



Cisco AsyncOS 8.0.1 for Email ユーザ ガイド

2013 年 10 月 28 日

【注意】シスコ製品をご使用になる前に、安全上の注意
(www.cisco.com/jp/go/safety_warning/)をご確認ください。

本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco AsyncOS 8.0.1 for Email ユーザガイド
© 2013 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Cisco 電子メール セキュリティ アプライアンスをご使用前に 1-1

- 今回のリリースでの変更点 1-1
- 詳細情報の入手先 1-5
 - マニュアル 1-6
 - トレーニングと認定試験 1-6
 - Knowledge Base 1-6
 - Cisco サポート コミュニティ 1-7
 - シスコのテクニカル サポート 1-7
 - サードパーティ コントリビュータ 1-8
 - マニュアルに関するフィードバック 1-8
- Cisco 電子メール セキュリティ アプライアンスの概要 1-8
 - サポートされる言語 1-9

CHAPTER 2

概要 2-1

- Web ベースのグラフィカル ユーザ インターフェイス (GUI) 2-1
 - ブラウザ要件 2-1
 - GUI へのアクセス 2-2
 - アクティブなセッションの表示 2-5
- コマンドライン インターフェイス (CLI) 2-5
 - コマンドライン インターフェイスの表記法 2-6
 - 汎用 CLI コマンド 2-9

CHAPTER 3

セットアップおよび設置 3-1

- 設置計画 3-1
 - 計画決定に影響を与える情報の確認 3-1
 - ネットワーク境界に Cisco アプライアンスを配置する 3-1
 - DNS への Cisco アプライアンスの登録 3-2
 - インストール シナリオ 3-3
- Cisco アプライアンスのネットワークへの物理接続 3-4
 - 設定シナリオ 3-4
- システム セットアップの準備 3-7
 - アプライアンスへの接続方式の決定 3-8
 - ネットワーク アドレスと IP アドレスの割り当ての決定 3-9
 - セットアップ情報の収集 3-10

- システム セットアップ ウィザードの使用方法 3-12
 - Web ベースのグラフィカル ユーザ インターフェイス (GUI) の利用 3-13
 - Web ベースのシステム セットアップ ウィザードを使用した基本設定の定義 3-14
 - Active Directory への接続の設定 3-22
 - 次の手順 3-23
 - コマンドライン インターフェイス (CLI) へのアクセス 3-23
 - コマンドライン インターフェイス (CLI) システム セットアップ ウィザードの実行 3-23
 - エンタープライズ ゲートウェイとしてシステムを設定 3-37
 - 設定と次の手順の確認 3-37

CHAPTER 4

- 電子メール パイプラインの理解 4-1
 - 電子メール パイプラインの概要 4-1
 - 電子メール パイプラインのフロー 4-1
 - 着信および受信 4-4
 - ホスト アクセス テーブル (HAT)、送信者グループ、およびメール フロー ポリシー 4-4
 - Received: ヘッダー 4-5
 - デフォルト ドメイン 4-5
 - バウンス検証 4-5
 - ドメイン マップ 4-5
 - 受信者アクセス テーブル (RAT) 4-6
 - エイリアス テーブル 4-6
 - LDAP 受信者の受け入れ 4-6
 - SMTP Call-Ahead 受信者検証 4-6
 - ワーク キューとルーティング 4-6
 - 電子メール パイプラインとセキュリティ サービス 4-7
 - LDAP 受信者の受け入れ 4-7
 - マスカレードまたは LDAP マスカレード 4-8
 - LDAP ルーティング 4-8
 - メッセージ フィルタ 4-8
 - 電子メール セキュリティ マネージャ (受信者単位のスキャン) 4-8
 - 隔離 4-10
 - 配信 4-10
 - 仮想ゲートウェイ 4-10
 - 配信制限 4-10
 - ドメインベースの制限値 4-11
 - ドメインベースのルーティング 4-11
 - グローバル配信停止 4-11

バウンス制限 4-11

CHAPTER 5

電子メールを受信するためのゲートウェイの設定 5-1

- 電子メールを受信するためのゲートウェイ設定の概要 5-1
- リスナーの使用 5-2
- リスナーのグローバル設定 5-5
 - 複数のエンコーディングが含まれるメッセージの設定 : localeconfig 5-7
- GUI からのリスナーの作成による接続要求のリッスン 5-8
 - 部分ドメイン、デフォルト ドメイン、不正な形式の MAIL FROM 5-12
- CLI からのリスナーの作成による接続要求のリッスン 5-13
 - HAT の詳細パラメータ 5-14
- エンタープライズ ゲートウェイ構成 5-15

CHAPTER 6

レピュテーション フィルタリング 6-1

- レピュテーション フィルタリングの概要 6-1
- SenderBase レピュテーション サービス 6-1
 - SenderBase レピュテーション スコア (SBRs) 6-2
 - SenderBase レピュテーション フィルタの仕組み 6-3
 - さまざまなレピュテーション フィルタリング手法の推奨設定 6-4
- リスナーのレピュテーション フィルタリング スコアのしきい値の編集 6-5
 - SBRs を使用したレピュテーション フィルタリングのテスト 6-6
 - SenderBase レピュテーション サービスのステータスのモニタリング 6-7
- メッセージの件名への低い SBRs スコアの入力 6-7

CHAPTER 7

ホスト アクセス テーブル (HAT) を使用した接続を許可するホストの定義 7-1

- 接続を許可するホストの定義の概要 7-1
 - デフォルト HAT エントリ 7-2
- 送信者グループへのリモート ホストの定義 7-3
 - 送信者グループの構文 7-4
 - ネットワーク オーナー、ドメイン、IP アドレスで定義される送信者グループ 7-5
 - SenderBase レピュテーション スコアを使用した送信者グループの定義 7-6
 - DNS リストにクエリーを実行することで定義された送信者グループ 7-7
- メール フロー ポリシーを使用した電子メール送信者のアクセス ルールの定義 7-8
 - HAT 変数の構文 7-9
- 定義済みの送信者グループとメール フロー ポリシーの理解 7-11
- 送信者グループからのメッセージの同様の処理 7-13
 - メッセージ処理の送信者グループの作成 7-13
 - 既存の送信者グループに送信者を追加できます。 7-14

- 着信接続のために実行するルールの順序の並べ替え 7-14
- 送信者の検索 7-15
 - メール フロー ポリシーを使用した着信メッセージのルールの定義 7-15
 - メール フロー ポリシーのデフォルト値の定義 7-20
- ホスト アクセス テーブルの設定の使用 7-21
 - 外部ファイルへの ホスト アクセス テーブル設定のエクスポート 7-21
 - 外部ファイルからのホスト アクセス テーブル設定のインポート 7-21
- 着信接続ルールへの送信者アドレス リストの使用 7-22
- SenderBase 設定とメール フロー ポリシー 7-23
 - SenderBase クエリーのタイムアウト 7-23
 - HAT Significant Bits 機能 7-24
- 送信者の検証 7-28
 - 送信者検証 : ホスト 7-28
 - 送信者検証 : エンベロープ送信者 7-29
 - 送信者検証の実装 — 設定例 7-31
 - 未検証送信者からのメッセージの設定テスト 7-36
 - 送信者検証とロギング 7-37
 - CLI でのホスト DNS 検証のイネーブル化 7-38

CHAPTER 8

- ドメイン名または受信者アドレスに基づく接続の許可または拒否 8-1
 - 受信者のアドレスに基づく接続の許可または拒否の概要 8-1
 - 受信者アクセス テーブル (RAT) の概要 8-2
 - RAT へのアクセス 8-2
 - デフォルトの RAT エントリの編集 8-2
 - ドメインおよびユーザ 8-3
 - メッセージを受け入れるドメインおよびユーザの追加 8-3
 - 受信者アクセス テーブルでのドメインおよびユーザの順序の入れ替え 8-5
 - 受信者アクセス テーブルの外部ファイルへのエクスポート 8-6
 - 受信者アクセス テーブルの外部ファイルからのインポート 8-6

CHAPTER 9

- メッセージ フィルタを使用した電子メール ポリシーの適用 9-1
 - 概要 9-1
 - メッセージ フィルタのコンポーネント 9-2
 - メッセージ フィルタ ルール 9-2
 - メッセージ フィルタ アクション 9-2
 - メッセージ フィルタの構文例 9-3
 - メッセージ フィルタ処理 9-4
 - メッセージ フィルタの順番 9-4

メッセージ ヘッダー ルールおよび評価	9-5
メッセージ本文と メッセージ添付ファイル	9-5
コンテンツ スキャンの一致のしきい値	9-6
メッセージ フィルタ内の AND テストと OR テスト	9-8
メッセージ フィルタ ルール	9-9
フィルタ ルールの概要の表	9-9
ルールで使用する正規表現	9-16
スマート ID	9-20
メッセージ フィルタ ルールの例	9-21
メッセージ フィルタ アクション	9-43
フィルタ アクション一覧表	9-43
アクション変数	9-49
該当コンテンツの表示	9-51
メッセージ フィルタ アクションの例	9-52
添付ファイルのスキャン	9-67
添付ファイルのスキャンで使用するメッセージ フィルタ	9-68
イメージ分析	9-69
イメージ分析スキャン エンジンの設定	9-69
イメージ分析結果に基づいたアクション実行のメッセージ フィルタの設定	9-73
通知	9-75
添付ファイルのスキャン メッセージ フィルタの例	9-75
CLI を使用したメッセージ フィルタの管理	9-79
新しいメッセージ フィルタの作成	9-80
メッセージ フィルタの削除	9-80
メッセージ フィルタの移動	9-80
メッセージ フィルタのアクティベーションとディアクティベーション	9-81
メッセージ フィルタのインポート	9-84
メッセージ フィルタのエクスポート	9-85
非 ASCII 文字セットの表示	9-85
メッセージ フィルタ リストの表示	9-85
メッセージ フィルタの詳細の表示	9-86
フィルタ ログ サブスクリプションの設定	9-86
スキャン パラメータの変更	9-88
メッセージのエンコードの変更	9-92
サンプル メッセージ フィルタの作成	9-94
メッセージ フィルタの例	9-100
オープンリレー防止フィルタ	9-100
ポリシー強制フィルタ	9-101
ルーティングおよびドメイン スプーフィング	9-105

CHAPTER 10

メール ポリシー 10-1

- メール ポリシーの概要 10-1
- メール ポリシーをユーザ単位で適用する方法 10-2
- 着信処理および発信メッセージの異なる処理 10-2
- メール ポリシーへのユーザの一致 10-3
 - 最初に一致したものの勝ち 10-3
 - ポリシー マッチングの例 10-4
- メッセージ分裂 10-5
 - 管理例外 10-6
- メール ポリシーの設定 10-6
 - 着信または発信メッセージのデフォルトのメールポリシーの設定 10-7
 - 送信者および受信者のグループのメール ポリシーの作成 10-8
 - 送信者または受信者に適用するポリシーの検索 10-9

CHAPTER 11

コンテンツ フィルタ 11-1

- コンテンツ フィルタの概要 11-1
- コンテンツ フィルタの仕組み 11-1
 - コンテンツ フィルタを使用したメッセージ コンテンツのスキャン方法 11-2
 - コンテンツ フィルタの条件 11-2
 - コンテンツ フィルタのアクション 11-10
 - アクション変数 11-16
- コンテンツに基づくメッセージのフィルタリング 11-18
 - コンテンツ フィルタの作成 11-18
 - デフォルトでのすべての受信者のコンテンツ フィルタのイネーブル化 11-19
 - 特定のユーザ グループに対するメッセージへのコンテンツ フィルタの適用 11-20
 - GUI でのコンテンツ フィルタの設定に関する注意事項 11-20

CHAPTER 12

アンチウイルス 12-1

- アンチウイルス スキャンの概要 12-1
 - 評価キー 12-2
 - 複数のアンチウイルス スキャンエンジンによるメッセージのスキャン 12-2
- Sophos Anti-Virus フィルタリング 12-2
 - ウイルス検出エンジン 12-3
 - ウイルス スキャン 12-3
 - 検出方法 12-3
 - ウイルスの記述 12-4
 - Sophos アラート 12-4
 - ウイルスが発見された場合 12-5

McAfee Anti-Virus フィルタリング	12-5
ウイルス シグニチャとのパターン照合	12-5
暗号化されたポリモーフィック型ウイルスの検出	12-5
発見的分析	12-6
ウイルスが発見された場合	12-6
アプライアンスでのウイルスのスキャンの設定方法	12-6
ウイルス スキャンのイネーブル化およびグローバル設定の構成	12-7
ユーザのウイルス スキャン アクションの設定	12-7
送信者および受信者のグループごとのアンチウイルス ポリシーの設定	12-13
アンチウイルス設定に関する注意事項	12-14
アンチウイルス アクションのフロー ダイアグラム	12-16
アンチウイルス スキャンをテストするためにアプライアンスにメールを送信する	12-17
ウイルス定義ファイルの更新	12-19
HTTP を使用した Anti-Virus アップデートの取得について	12-19
アップデート サーバの設定	12-19
モニタリングおよび手動での Anti-Virus アップデート チェック	12-20
アプライアンスでのアンチウイルス ファイルの更新の確認	12-21

CHAPTER 13

アンチスパム 13-1

スパム対策スキャンの概要	13-1
スパム対策ソリューション	13-2
メッセージがスパムかどうかスキャンするためのアプライアンスの設定方法	13-2
IronPort Anti-Spam フィルタリング	13-3
評価キー	13-3
Cisco Anti-Spam : 概要	13-4
IronPort Anti-Spam スキャンの設定	13-5
CiscoIntelligent Multi-Scan フィルタリング	13-6
Cisco Intelligent Multi-Scan の設定	13-7
スパム対策ポリシーの定義	13-8
陽性および陽性と疑わしいスパムのしきい値の理解	13-10
設定例 : 陽性と判定されたスパムと、陽性と疑わしいスパムとのアクション	13-11
正規の送信元からの不要なマーケティング メッセージ	13-11
異なるメール ポリシーでの異なるスパム対策スキャン エンジンのイネーブル化 : 設定例	13-12
スパム フィルタからのアプライアンス生成メッセージの保護	13-13
スパム対策スキャン中に追加されるヘッダー	13-14
誤って分類されたメッセージの Cisco Systems への報告	13-14
着信リレー構成における送信者の IP アドレスの決定	13-14

着信リレーを使用した環境例	13-15
着信リレーを使用するアプライアンスの設定	13-16
着信リレーが機能にどのように影響するか	13-21
使用するヘッダーを指定するログの設定	13-23
モニタリング ルールのアップデート	13-23
スパム対策のテスト	13-24
Cisco スパム対策をテストするためのアプライアンスへのメールの送信	13-24
スパム対策の性能をテストしない方法	13-25

CHAPTER 14

アウトブレイク フィルタ	14-1
アウトブレイク フィルタの概要	14-1
アウトブレイク フィルタの動作	14-2
メッセージの遅延、リダイレクトおよび修正	14-2
脅威カテゴリ	14-2
Cisco Security Intelligence Operations	14-3
Context Adaptive Scanning Engine	14-4
メッセージの遅延	14-4
URL のリダイレクト	14-4
メッセージの変更	14-5
ルールのタイプ : アダプティブ ルールおよびアウトブレイク ルール	14-6
アウトブレイク	14-7
脅威レベル	14-7
アウトブレイク フィルタの機能概要	14-8
動的隔離	14-9
アウトブレイク フィルタの管理 (GUI)	14-11
アウトブレイク フィルタのグローバル設定の構成	14-12
アウトブレイク フィルタ ルール	14-14
アウトブレイク フィルタ機能とメール ポリシー	14-14
アウトブレイク フィルタ機能とアウトブレイク隔離	14-19
アウトブレイク フィルタのモニタリング	14-21
アウトブレイク フィルタ レポート	14-21
アウトブレイク フィルタの概要とルール リスト	14-21
アウトブレイク隔離	14-21
アラート、SNMP トラップ、およびアウトブレイク フィルタ	14-22
アウトブレイク フィルタ機能のトラブルシューティング	14-22

CHAPTER 15

データ消失防止	15-1
データ消失防止の概要	15-1
DLP スキャン プロセスの概要	15-2

データ消失防止の動作	15-2
DLP 配置オプション	15-3
データ消失防止のシステム要件	15-4
RSA メール DLP	15-4
RSA メール DLP を使用した導入の場合のデータ消失防止をセットアップする方法	15-4
データ消失防止のイネーブル化 (RSA Email DLP)	15-5
RSA Email DLP の DLP ポリシー	15-6
DLP ポリシーの説明	15-6
定義済み DLP ポリシー テンプレート	15-6
ウィザードを使用して RSA メール DLP を設定する方法	15-7
事前定義されたテンプレートを使用した DLP ポリシーの作成	15-8
カスタム DLP ポリシーの作成 (詳細)	15-9
コンテンツ照合分類子を使用した拒否されたコンテンツの定義について	15-10
DLP ポリシーのメッセージのフィルタリング	15-19
違反の重大度の評価について	15-20
違反との一致に対する Email DLP ポリシーの順序の調整	15-21
発信メール ポリシーとの DLP ポリシーの関連付け	15-21
DLP ポリシーの編集または削除に関する重要な情報	15-23
RSA Enterprise Manager	15-23
Enterprise Manager と電子メール セキュリティ アプライアンスの連携方法	15-23
Enterprise Manager のマニュアル	15-24
RSA Enterprise Manager の導入における展開データ消失防止のセットアップ方法	15-24
RSA メール DLP から RSA Enterprise Manager への移行	15-30
Enterprise Manager の DLP ポリシー更新の確認	15-31
RSA Enterprise Manager と言語サポート	15-32
クラスタ化されたアプライアンスでの Enterprise Manager の使用	15-32
Enterprise Manager 導入におけるポリシーの削除とディセーブル化について	15-32
電子メール セキュリティ アプライアンスと Enterprise Manager 間の接続の切断	15-33
Enterprise Manager から RSA メール DLP への切り替え	15-33
メッセージ アクション	15-33
DLP 違反アクション (メッセージ アクション) に対して実行するアクションの定義	15-34
メッセージ アクションの表示および編集	15-35
DLP 通知のドラフト	15-36
メッセージ トラッキングの機密 DLP データの表示または非表示	15-38
DLP エンジンおよびコンテンツ照合分類子の更新について	15-39
RSA DLP エンジンの現在のバージョンの決定	15-39

- DLP 更新に関する警告 15-40
- DLP エンジンとコンテンツ照合分類子の手動による更新 15-40
- 自動アップデートの有効化（推奨されません） 15-40
- 一元化された（クラスタ化された）アプライアンスの DLP 更新 15-41
- DLP 更新のロールバック 15-41
- DLP インシデントのメッセージとデータの使用 15-42
- トラブルシューティング データ消失防止 15-43
- Enterprise Manager は電子メール セキュリティ アプライアンスとの接続を解除し
ます。 15-43

CHAPTER 16

Cisco Email Encryption 16-1

- Cisco Email Encryption の概要 16-1
 - サポート対象の Web ブラウザ 16-1
- ローカル キー サーバで暗号化する方法 16-2
 - 暗号化ワークフロー 16-2
- 電子メール セキュリティ アプライアンスを使用したメッセージの暗号化 16-3
 - 電子メール セキュリティ アプライアンスでのメッセージの暗号化のイネーブル化 16-4
 - キー サービスによる暗号化メッセージの処理方法の設定 16-4
 - PXE エンジンの最新バージョンへの更新 16-7
- 暗号化するメッセージの決定 16-7
 - TLS 接続を暗号化の代わりに使用 16-8
 - コンテンツ フィルタを使用したメッセージの暗号化と即時配信 16-8
 - コンテンツ フィルタを使用した配信時のメッセージの暗号化 16-9
- メッセージへの暗号化ヘッダーの追加 16-11
 - 暗号化ヘッダー 16-11
 - 暗号化ヘッダーの例 16-13

CHAPTER 17

電子メール認証 17-1

- 電子メール認証の概要 17-1
- DomainKeys と DKIM 認証 17-1
 - AsyncOS の DomainKeys および DKIM 署名 17-2
- DomainKeys および DKIM 署名の設定 17-3
 - 署名キー 17-3
 - 公開キー 17-4
 - ドメイン プロファイル 17-4
 - 送信メールの署名のイネーブル化 17-5
 - バウンスおよび遅延メッセージの署名のイネーブル化 17-6
 - DomainKeys/DKIM 署名の設定（GUI） 17-6
 - ドメイン キーとロギング 17-15

DKIM 署名を使用した受信メッセージの確認方法	17-15
AsyncOS による DKIM 検証チェック	17-15
DKIM の検証プロファイルの管理	17-16
メール フロー ポリシーでの DKIM 検証の設定	17-19
DKIM 検証済みメールのアクションの設定	17-19
SPF および SIDF 検証の概要	17-20
SPF/SIDF を使用して受信メッセージの確認方法	17-22
SPF と SIDF のイネーブル化	17-22
SPF/SIDF 検証済みメールに対して実行するアクションの決定	17-29
検証結果	17-29
CLI での spf-status フィルタ ルールの使用	17-30
GUI での spf-status コンテンツ フィルタ ルール	17-31
spf-passed フィルタ ルールの使用	17-31
SPF/SIDF 結果のテスト	17-32
SPF/SIDF 結果の基本の詳細度のテスト	17-32
SPF/SIDF 結果の高い詳細度のテスト	17-32

CHAPTER 18**テキスト リソース 18-1**

テキスト リソースの概要	18-1
コンテンツ ディクショナリ	18-1
テキスト リソース	18-2
メッセージの免責事項スタンプ	18-2
コンテンツ ディクショナリ	18-2
ディクショナリの内容	18-2
テキスト ファイルとしてディクショナリをインポートおよびエクスポートする方 法	18-3
ディクショナリの追加	18-4
ディクショナリの削除	18-5
ディクショナリのインポート	18-5
ディクショナリのエクスポート	18-6
コンテンツ ディクショナリ フィルタ ルールの使用方法およびテスト方法	18-6
ディクショナリの照合フィルタ ルール	18-6
テキスト リソースについて	18-8
テキスト ファイルとしてテキスト リソースをインポートおよびエクスポートする	18-8
テキスト リソース管理の概要	18-9
テキスト リソースの追加	18-9
テキスト リソースの削除	18-9
テキスト リソースのインポート	18-10
テキスト リソースのエクスポート	18-10

- HTML ベースのテキスト リソースの概要 18-11
- テキスト リソースの使用 18-12
 - 免責事項テンプレート 18-12
 - 免責事項スタンプと複数エンコード方式 18-16
 - 通知テンプレート 18-19
 - アンチウイルス通知テンプレート 18-20
 - バウンス通知および暗号化失敗通知テンプレート 18-22
 - 暗号化通知テンプレート 18-23

CHAPTER 19

SMTP サーバを使用した受信者の検証 19-1

- SMTP Call-Ahead 受信者検証の概要 19-1
- SMTP Call-Ahead 受信者検証のワークフロー 19-1
- 外部 SMTP サーバを使用した受信者の検証方法 19-3
 - Call-Ahead サーバ プロファイルの設定 19-3
- リスナーでの SMTP サーバ経由の着信メールの検証のイネーブル化 19-6
- LDAP ルーティング クエリーの設定 19-6
- SMTP Call-Ahead クエリーのルーティング 19-7
- 特定のユーザまたはグループの SMTP Call-Ahead 検証のバイパス 19-8

CHAPTER 20

他の MTA との暗号化通信 20-1

- 他の MTA との暗号化通信の概要 20-1
 - TLS を使用した SMTP カンバセーションの暗号化方法 20-2
- 証明書の取得 20-2
 - 中間証明書 20-3
 - 証明書と集中管理 20-3
 - GUI を使用した自己署名証明書の作成 20-3
 - GUI を使用した証明書のインポート 20-5
 - 自己署名証明書の作成または CLI を使用した証明書のインポート 20-5
 - GUI を使用した証明書のエクスポート 20-5
- リスナー HAT の TLS のイネーブル化 20-6
 - GUI を使用したパブリックまたはプライベートのリスナーへの TLS 接続のための証明書の割り当て 20-7
 - CLI を使用したパブリックまたはプライベートのリスナーへの TLS 接続のための証明書の割り当て 20-7
 - ロギング 20-7
 - GUI の例：リスナーの HAT の TLS 設定の変更 20-7
 - CLI 例：リスナーの HAT の TLS 設定の変更 20-8
- 配信時の TLS および証明書検証のイネーブル化 20-9
 - 要求された TLS 接続が失敗した場合のアラートの送信 20-11

ロギング	20-11
CLI の例	20-12
認証局のリストの管理	20-15
プレインストールされたの認証局リストの参照	20-16
システム認証局リストのディセーブル化	20-16
カスタム認証局リストのインポート	20-16
認証局リストのエクスポート	20-17
HTTPS の証明書のイネーブル化	20-17

CHAPTER 21

ルーティングおよび配信機能の設定	21-1
ローカル ドメインの電子メールのルーティング	21-1
SMTP ルートの概要	21-2
デフォルトの SMTP ルート	21-2
SMTP ルートの定義	21-2
SMTP ルートの制限	21-3
SMTP ルートと DNS	21-3
SMTP ルートおよびアラート	21-4
SMTP ルート、メール配信、およびメッセージ分裂	21-4
SMTP ルートと発信 SMTP 認証	21-4
GUI を使用した発信電子メール送信の SMTP ルート管理	21-4
アドレスの書き換え	21-6
エイリアス テーブルの作成	21-7
マスカレードの設定	21-16
ドメイン マップ機能	21-28
バウンスした電子メールの処理	21-36
配信不可能な電子メールの処理	21-36
新しいバウンス プロファイルの作成	21-40
リスナーへのバウンス プロファイルの適用	21-41
送信先コントロールによる電子メール配信の管理	21-43
メール配信に使用するインターフェイスの決定	21-43
デフォルトの配信制限	21-44
[送信先コントロール (Destination Controls)] の使用	21-44
Cisco バウンス検証	21-51
概要 : タギングと Cisco バウンス検証	21-52
タグなしのバウンスされたメッセージの合法的受け入れ	21-53
バウンス Cisco 検証を使用してバウンス メッセージ ストームを防止	21-54
電子メール配信パラメータの設定	21-56

Virtual Gateway™ テクノロジーを使用してすべてのホストされたドメインでの構成のメール ゲートウェイ 21-59

概要 21-59

Virtual Gateway アドレスの設定 21-59

Virtual Gateway アドレスのモニタリング 21-67

Virtual Gateway アドレスごとの配信接続の管理 21-67

[グローバル配信停止 (Global Unsubscribe)] 機能の使用 21-68

確認 : 電子メール パイプライン 21-73

CHAPTER 22

LDAP クエリー 22-1

LDAP クエリーの概要 22-1

LDAP クエリーの概要 22-2

LDAP と AsyncOS との連携の仕組み 22-3

Cisco IronPort アプライアンスを LDAP サーバと連携させるための設定 22-4

LDAP サーバに関する情報を保存する LDAP サーバ プロファイルの作成 22-5

LDAP サーバのテスト 22-7

特定のリスナーで実行するための LDAP クエリーのイネーブル化 22-7

Microsoft Exchange 5.5 に対する拡張サポート 22-9

LDAP クエリーに関する作業 22-12

LDAP サーバへの匿名のバインドをクライアントに許可する 22-14

LDAP クエリーのテスト 22-17

LDAP サーバへの接続のトラブルシューティング 22-18

受信者検証で受け入れクエリーを使用する 22-19

Lotus Notes の場合の受け入れクエリーの設定 22-20

複数ターゲット アドレスへのメール送信にルーティング クエリーを使用する 22-20

エンベロップ送信者を書き換えるためのマスカレード クエリーの使用 22-21

「フレンドリ名」のマスカレード 22-22

受信者がグループメンバーであるかどうかを指定するグループ LDAP クエリーの使用 22-23

グループ クエリーの設定 22-23

例 : グループ クエリーを使用してスパムとウイルスのチェックをスキップする 22-25

特定のドメインヘルペティングするためのドメイン ベース クエリーの使用 22-26

ドメインベース クエリーの作成 22-27

一連の LDAP クエリーを実行するためのチェーン クエリーの使用 22-28

チェーン クエリーの作成 22-29

LDAP によるディレクトリ ハーベスト攻撃防止 22-29

SMTP カンバセーション中のディレクトリ ハーベスト攻撃防止 22-30

ワーク キュー内でのディレクトリ ハーベスト攻撃防止 22-31

SMTP 認証を行うための AsyncOS の設定 22-32

SMTP 認証の設定	22-33
SMTP 認証クエリーの設定	22-34
第 2 の SMTP サーバ経由での SMTP 認証 (転送を使用する SMTP Auth)	22-35
LDAP を使用する SMTP 認証	22-36
クライアント認証を使用した SMTP セッションの認証	22-39
発信 SMTP 認証	22-39
ロギングと SMTP 認証	22-40
ユーザの外部 LDAP 認証の設定	22-40
ユーザ アカウント クエリー	22-41
グループ メンバーシップ クエリー	22-41
Cisco IronPort スпам隔離内のエンド ユーザ認証	22-43
Active Directory エンドユーザ認証の設定の例	22-43
OpenLDAP エンドユーザ認証の設定の例	22-44
スパム隔離のエイリアス統合のクエリー	22-44
Active Directory エイリアス統合の設定の例	22-45
OpenLDAP エイリアス統合の設定の例	22-45
RSA Enterprise Manager の送信者のユーザ識別名の特定	22-45
ユーザの識別名の設定例	22-46
AsyncOS を複数の LDAP サーバと連携させるための設定	22-46
サーバとクエリーのテスト	22-46
フェールオーバー	22-46
ロード バランシング	22-47

CHAPTER 23

クライアント証明書を使用した SMTP セッションの認証	23-49
証明書と SMTP 認証の概要	23-49
クライアント証明書でのユーザの認証方法	23-50
SMTP 認証 LDAP クエリーでのユーザの認証方法	23-50
クライアント認証が無効な場合の LDAP SMTP 認証クエリーでのユーザの認証方法	23-50
クライアント証明書の有効性の確認	23-51
LDAP ディレクトリを使用したユーザの認証	23-52
クライアント証明書を使用した TLS 経由の SMTP 接続の認証	23-52
アプライアンスからの TLS 接続の確立	23-53
無効にされた証明書のリストの更新	23-54

CHAPTER 24

FIPS 管理	24-1
FIPS 管理の概要	24-1
FIPS 管理の概要	24-1

[アプライアンスの FIPS モードへの切り替え](#) 24-2
[証明書およびキーの管理](#) 24-2
[DKIM 署名と検証のキーの管理](#) 24-3
 [DKIM: 署名](#) 24-3
 [DKIM の検証](#) 24-4

CHAPTER 25

[メッセージ トラッキング](#) 25-1
 [メッセージ トラッキングの概要](#) 25-1
 [メッセージ トラッキングのイネーブル化](#) 25-1
 [メッセージの検索](#) 25-2
 [メッセージ トラッキングの検索結果の使用](#) 25-4
 [有効なメッセージ トラッキング データの検査](#) 25-6
 [メッセージ トラッキングおよびアップグレードについて](#) 25-7

CHAPTER 26

[電子メール セキュリティ モニタの使用方法](#) 26-1
 [電子メール セキュリティ モニタの概要](#) 26-1
 [電子メール セキュリティ モニタ ページ](#) 26-2
 [検索と電子メール セキュリティ モニタ](#) 26-3
 [レポートに含まれるメッセージの詳細の表示](#) 26-4
 [\[マイレポート \(My Reports\)\] ページ](#) 26-4
 [\[概要 \(Overview\)\] ページ](#) 26-5
 [\[受信メール \(Incoming Mail\)\] ページ](#) 26-9
 [送信先 \(Outgoing Destinations\)](#) 26-17
 [送信メッセージ送信者 \(Outgoing Senders\)](#) 26-18
 [\[送信処理ステータス \(Delivery Status\)\] ページ](#) 26-19
 [\[内部ユーザ \(Internal Users\)\] ページ](#) 26-21
 [\[DLP インシデント \(DLP Incidents\)\] ページ](#) 26-22
 [\[コンテンツ フィルタ \(Content Filters\)\] ページ](#) 26-25
 [\[アウトブレイク フィルタ \(Outbreak Filters\)\] ページ](#) 26-26
 [\[ウイルス タイプ \(Virus Types\)\] ページ](#) 26-28
 [\[TLS 接続 \(TLS Connections\)\] ページ](#) 26-30
 [\[受信 SMTP 認証 \(Inbound SMTP Authentication\)\] ページ](#) 26-31
 [\[レート制限 \(Rate Limits\)\] ページ](#) 26-33
 [\[システム容量 \(System Capacity\)\] ページ](#) 26-34
 [\[システム ステータス \(System Status\)\] ページ](#) 26-40
 [CSV データの取得](#) 26-42
 [レポートの概要](#) 26-44
 [スケジュール設定されたレポートの種類](#) 26-44

レポート用返信アドレスの設定	26-45
レポートの管理	26-45
スケジュール設定されたレポート	26-45
アーカイブ済みのレポート	26-47
電子メール レポートのトラブルシューティング	26-48

CHAPTER 27

隔離 27-1

隔離の概要	27-1
隔離のタイプ	27-2
ローカル隔離	27-3
ポリシー、ウイルス、およびアウトブレイク隔離の管理	27-3
ポリシー、ウイルス、およびアウトブレイク隔離に対するディスク領域の割り当て	27-3
隔離エリアのメッセージ保存期間	27-4
自動的に処理された隔離メッセージのデフォルト アクション	27-5
システムが作成した隔離の設定の確認	27-5
ポリシー隔離の作成	27-6
ポリシー、ウイルス、アウトブレイク隔離の設定の編集方法	27-7
フィルタおよびメッセージ アクションに割り当てる隔離を決定する	27-7
ポリシー隔離の削除について	27-8
隔離のステータス、容量、アクティビティのモニタリング	27-8
ポリシー隔離のパフォーマンス	27-9
隔離のディスク領域の使用状況についてのアラート	27-9
ポリシー隔離とロギング	27-9
メッセージ処理作業の他のユーザへの分配	27-10
クラスタ設定におけるポリシー、ウイルス、およびアウトブレイク隔離について	27-11
ポリシー、ウイルス、アウトブレイク隔離の設定の集約方法	27-11
ポリシー、ウイルス、またはアウトブレイク隔離のメッセージの操作	27-11
隔離エリア内のメッセージの表示	27-11
ポリシー、ウイルスおよびアウトブレイク隔離のメッセージの検索	27-12
手動で隔離メッセージを処理	27-13
複数の隔離エリアにあるメッセージ	27-14
メッセージの詳細およびメッセージ内容の表示	27-15
隔離されたメッセージの再スキャンについて	27-18
アウトブレイク隔離	27-18
スパム隔離の概要	27-19
スパム隔離の設定	27-19
スパム隔離へのメッセージの送信方法	27-20
ローカルのスパム隔離のイネーブル化とディセーブル化	27-20
ローカルのスパム隔離から外部の隔離への移行	27-21

スパム隔離の設定	27-22
ローカルのスパム隔離の設定	27-23
外部のスパム隔離の設定	27-27
Web ブラウザからスパム隔離へのアクセスのイネーブル化	27-28
スパムを隔離するためのメール ポリシーの設定	27-29
導入上の考慮事項	27-29
スパム隔離内のメッセージの管理	27-33
スパム隔離内でのメッセージの検索	27-34
スパム隔離内のメッセージの表示	27-34
スパム隔離内のメッセージの配信	27-35
スパム隔離からのメッセージの削除	27-35
送信者に基づいて電子メール配信を制御するセーフリストおよびブロックを使用	27-36
セーフリスト/ブロックリスト データベース	27-36
セーフリストとブロックリストの作成およびメンテナンス	27-36
セーフリストとブロックリストのメッセージ配信	27-37
セーフリストとブロックリストの作成およびメンテナンスの概要	27-37
セーフリストとブロックリストを設定するためのエンド ユーザ作業	27-40

CHAPTER 28

管理タスクの分散 28-1

ユーザ アカウントを使用する作業	28-1
ユーザの管理	28-3
委任管理のためのカスタム ユーザ ロールの管理	28-7
[アカウント権限 (Account Privileges)] ページ	28-8
アクセス権限の割り当て	28-9
カスタム ユーザ ロールの定義	28-14
ユーザ アカウント追加時のカスタム ユーザ ロールの定義	28-14
カスタム ユーザ ロールの責任のアップデート	28-15
カスタム ユーザ ロールの編集	28-16
カスタム ユーザ ロールの複製	28-16
カスタム ユーザ ロールの削除	28-16
パスワード	28-17
パスワードの変更	28-17
ユーザ アカウントのロックおよびロック解除	28-17
制限的なユーザ アカウントとパスワードの設定値の設定	28-18
外部認証 (External Authentication)	28-21
電子メール セキュリティ アプライアンスの設定	28-24
ログイン バナーの追加	28-26
セキュア シェル (SSH) キーの管理	28-27
リモート SSH コマンド実行	28-29

CHAPTER 29

システム管理 29-1

- Cisco アプライアンスの管理 29-1
 - Cisco アプライアンスのシャットダウンおよび再起動 29-2
 - 電子メールの受信と配信の一時停止 29-2
 - 一時停止している電子メールの受信と配信の再開 29-3
 - CLI を使用したアプライアンスのオフライン化 29-3
 - 出荷時の初期状態へのリセット 29-3
 - AsyncOS のバージョン情報の表示 29-5
- ライセンス キー 29-5
 - ライセンス キーの追加および管理 29-5
 - ライセンス キーのダウンロードとアクティベーションの自動化 29-6
 - 期限切れライセンス キー 29-6
- Cisco 電子メール セキュリティ仮想アプライアンスのライセンス 29-6
- 設定ファイルファイルの管理 29-7
 - GUI を使用した設定ファイルの管理 29-8
 - 設定ファイル用の CLI コマンド 29-11
- AsyncOS のアップグレード 29-15
 - AsyncOS のアップグレードの準備 29-15
 - GUI からの AsyncOS のアップグレード 29-15
- アップグレードおよびアップデートをダウンロードするための設定 29-18
 - Cisco IronPort サーバからのアップグレードおよびアップデートのダウンロード 29-19
 - ローカル サーバからのアップグレードおよびアップデート 29-20
- サービスのアップデート 29-22
 - プロキシ サーバを経由したアップデート 29-22
 - アップグレードおよびアップデートをダウンロードするためのサーバ設定 29-22
- リモート電源管理のイネーブル化 29-24
- AsyncOS の以前のバージョンへの復元 29-25
 - 利用可能なバージョン 29-26
 - 復元の影響に関する重要な注意事項 29-26
 - AsyncOS の復元 29-26
- アプライアンスに生成されるメッセージの返信アドレスの設定 29-29
- アラート 29-30
 - アラートの概要 29-30
 - Cisco AutoSupport 29-32
 - アラート メッセージ 29-32
 - アラート受信者の追加 29-33
 - アラート設定値の設定 29-34
 - トップ アラートの表示 29-34

アラート リスト	29-35
ネットワーク設定値の変更	29-52
システム ホスト名の変更	29-52
ドメイン ネーム システム (DNS) 設定値の設定	29-53
TCP/IP トラフィック ルートの設定	29-55
デフォルト ゲートウェイの設定	29-57
システム時刻	29-57
時間帯の選択	29-57
時刻設定の編集	29-58
ビューのカスタマイズ	29-59
お気に入りページの使用	29-59
ユーザ プリファレンスの設定	29-59

CHAPTER 30

CLI による管理およびモニタリング 30-1

CLI を使用した管理およびモニタリングの概要	30-1
使用可能なモニタリング コンポーネントの読み取り	30-2
イベント カウンタの読み取り	30-2
システム ゲージの読み取り	30-4
配信およびバウンスされたメッセージのレートの読み取り	30-6
CLI を使用したモニタリング	30-6
電子メール ステータスのモニタリング	30-7
詳細な電子メール ステータスのモニタリング	30-9
メール ホストのステータスのモニタリング	30-12
電子メール キューの構成の確認	30-16
リアルタイム アクティビティの表示	30-17
着信電子メール接続のモニタリング	30-20
DNS ステータスの確認	30-22
電子メール モニタリング カウンタのリセット	30-23
アクティブな TCP/IP サービスの識別	30-24
電子メール キューの管理	30-24
キュー内の受信者の削除	30-24
キュー内の受信者のバウンス	30-26
キュー内のメッセージのリダイレクト	30-28
キュー内の受信者に基づいたメッセージの表示	30-29
電子メール配信の一時停止	30-31
電子メール配信の再開	30-32
電子メールの受信の一時停止	30-32
電子メールの受信の再開	30-33
電子メールの配信と受信の再開	30-34

電子メールの即時配信スケジュール	30-34
ワーク キューの休止	30-35
古いメッセージの検索およびアーカイブ	30-37
システム内のメッセージのトラッキング	30-38
SNMP モニタリング	30-39
MIB ファイル	30-40
ハードウェア オブジェクト	30-40
SNMP トラップ	30-42

CHAPTER 31**SenderBase Network Participation 31-1**

SenderBase Network Participation の概要	31-1
SenderBase との統計の共有	31-1
よくあるご質問	31-2

CHAPTER 32**GUI でのその他の作業 32-7**

Cisco グラフィカル ユーザ インターフェイス (GUI)	32-7
インターフェイスでの GUI のイネーブル化	32-7
GUI のシステム情報	32-11
GUI からの XML ステータスの収集	32-12

CHAPTER 33**高度なネットワーク構成 33-1**

イーサネット インターフェイスのメディア設定	33-1
etherconfig を使ったイーサネット インターフェイスのメディア設定の編集	33-1
ネットワーク インターフェイス カードのペアリング / チーミング	33-3
NIC ペアの名前	33-4
NIC ペアリング / チーミングの設定とテスト	33-4
NIC ペアリングの確認	33-9
仮想ローカル エリア ネットワーク (VLAN)	33-9
VLAN と物理ポート	33-10
VLAN の管理	33-11
Direct Server Return	33-16
Direct Server Return のイネーブル化	33-16
イーサネット インターフェイスの最大伝送単位	33-21

CHAPTER 34**ロギング 34-1**

概要	34-1
ログ ファイルおよびログ サブスクリプションについて	34-1
ログ タイプ	34-2

ログ取得方法	34-7
ログ タイプ	34-9
ログ ファイル内のタイムスタンプ	34-9
IronPort テキスト メール ログの使用	34-10
IronPort 配信ログの使用	34-16
IronPort バウンス ログの使用	34-18
IronPort ステータス ログの使用	34-20
IronPort ドメイン デバッグ ログの使用	34-23
IronPort インジェクション デバッグ ログの使用	34-24
IronPort システム ログの使用	34-25
IronPort CLI 監査ログの使用	34-26
IronPort FTP サーバ ログの使用	34-27
IronPort HTTP ログの使用	34-28
IronPort NTP ログの使用	34-29
スキャン ログの使用	34-29
IronPort アンチスパムの使用	34-30
IronPort アンチウイルス ログの使用	34-30
IronPort スпам隔離ログの使用	34-31
IronPort スпам隔離 GUI ログの使用	34-31
IronPort LDAP デバッグ ログの使用	34-32
セーフリスト/ブロックリスト ログの使用	34-33
レポートニング ログの使用	34-34
レポートニング クエリー ログの使用	34-35
アップデート ログの使用	34-36
トラッキング ログについて	34-37
認証ログの使用	34-38
コンフィギュレーション履歴ログの使用	34-38
ログ サブスクリプション	34-39
ログ サブスクリプションの設定	34-40
GUI でのログ サブスクリプションの作成	34-41
ロギングに対するグローバル設定	34-41
ログ サブスクリプションのロールオーバー	34-44
GUI での最近のログ エントリの表示	34-47
CLI での最近のログ エントリの表示 (tail コマンド)	34-48
ホスト キーの設定	34-50

CHAPTER 35

クラスタを使用した中央集中型管理	35-1
クラスタを使用した中央集中型管理の概要	35-1
クラスタの要件	35-2

クラスタの構成	35-2
初期設定	35-3
クラスタの作成とクラスタへの参加	35-4
clusterconfig コマンド	35-4
グループの追加	35-10
クラスタの管理	35-11
CLI でのクラスタの管理	35-11
設定のコピーと移動	35-12
新しい設定の実験	35-12
クラスタからの脱退（削除）	35-13
クラスタ内のマシンのアップグレード	35-13
設定ファイル コマンド	35-14
CLI コマンドのサポート	35-14
すべてのコマンドがクラスタに対応	35-14
制限コマンド	35-15
GUI でのクラスタの管理	35-16
クラスタ通信	35-19
DNS とホスト名の解決	35-19
クラスタ通信のセキュリティ	35-20
クラスタの整合性	35-21
切断 / 再接続	35-21
互いに依存する設定	35-22
ベスト プラクティスとよくあるご質問	35-24
ベスト プラクティス	35-24
セットアップと設定に関する質問	35-27
一般的な質問	35-28
ネットワークに関する質問	35-28
計画と設定	35-29

CHAPTER 36

テストとトラブルシューティング	36-1
テスト メッセージを使用したメール フローのデバッグ : トレース	36-1
アプライアンスのテストにリスナーを使用	36-13
ネットワークのトラブルシューティング	36-17
アプライアンスのネットワーク接続テスト	36-18
リスナーのトラブルシューティング	36-23
アプライアンスからの電子メール配信のトラブルシューティング	36-25
パフォーマンスのトラブルシューティング	36-27
アプライアンスの電源のリモート リセット	36-28

テクニカル サポートの使用	36-29
サポート事例を開くまたは更新する	36-29
シスコのテクニカル サポート担当者のリモート アクセスのイネーブル化	36-30
パケット キャプチャの実行	36-33

CHAPTER 37

D-Mode を使用した発信メール配信アプライアンスの最適化 37-1

機能の概要：最適化された発信配信の D-Mode	37-1
D-Mode-enabled アプライアンス特有の機能	37-1
D-Mode-enabled アプライアンスでディセーブルになっている標準機能	37-2
D-Mode-enabled アプライアンスに適用される標準機能	37-2
最適化された発信メール配信のアプライアンスの設定	37-3
リソースを節約するバウンス設定の指定	37-3
IronPort Mail Merge (IPMM) を使用した大量のメールの送信	37-4
IronPort Mail Merge の概要	37-4
Mail Merge 機能の利点	37-5
Mail Merge の使用	37-5
コマンドの説明	37-8
変数定義に関する注意事項	37-8
IPMM カンバセーションの例	37-9

CHAPTER 38

Cisco コンテンツ セキュリティ管理アプライアンスの集中型サービス 38-1

Cisco コンテンツ セキュリティ管理アプライアンス サービスの概要	38-1
ネットワーク プランニング	38-2
メール フローおよび外部スパム隔離	38-2
外部スパム隔離の設定	38-3
一元化されたポリシー、ウイルス、アウトブレイク隔離について	38-4
一元化されたポリシー、ウイルス、およびアウトブレイク隔離	38-4
ポリシー、ウイルス、アウトブレイク隔離の移行について	38-5
一元化されたポリシー、ウイルス、アウトブレイク隔離	38-5
一元化されたポリシー、ウイルス、アウトブレイク隔離のディセーブル化について	38-7
一元化されたポリシー、ウイルス、アウトブレイク隔離のトラブルシューティング	38-8
中央集中型レポートの設定	38-8
中央集中型メッセージ トラッキングの設定	38-9
中央集中型サービスの使用方法	38-10

APPENDIX A

アプライアンスへのアクセス A-1

IP インターフェイス	A-1
電子メール セキュリティ アプライアンス への FTP アクセス設定	A-2

secure copy (scp) アクセス	A-4
シリアル接続による電子メール セキュリティ アプライアンスへのアクセス	A-5

APPENDIX B

ネットワーク アドレスと IP アドレスの割り当て	B-1
イーサネット インターフェイス	B-1
IP アドレスとネットマスクの選択	B-1
インターフェイスの設定例	B-2
IP アドレス、インターフェイス、およびルーティング	B-3
まとめ	B-3
Cisco アプライアンスの接続時の戦略	B-3

APPENDIX C

メール ポリシーとコンテンツ フィルタの例	C-1
受信メールポリシーの概要	C-1
メール ポリシーへのアクセス	C-1
着信メッセージのデフォルトのアンチスパム ポリシーの設定	C-3
送信者および受信者のグループのメール ポリシーの作成	C-4
送信者および受信者のグループごとのメール ポリシーの作成	C-7
メール ポリシーでの送信者または受信者の検索	C-11
コンテンツに基づくメッセージのフィルタリング	C-12
各受信者のグループごとのコンテンツ フィルタの適用	C-15
GUI でのコンテンツ フィルタの設定に関する注意事項	C-18

APPENDIX D

ファイアウォール情報	D-1
-------------------	------------

APPENDIX E

End User License Agreement	E-1
Cisco Systems End User License Agreement	E-1
Supplemental End User License Agreement for Cisco Systems Content Security Software	E-8

GLOSSARY**INDEX**



CHAPTER 1

Cisco 電子メール セキュリティ アプライアンスをご使用の前に

- 「今回のリリースでの変更点」 (P.1-1)
- 「詳細情報の入手先」 (P.1-5)
- 「Cisco 電子メール セキュリティ アプライアンスの概要」 (P.1-8)

今回のリリースでの変更点

ここでは、AsyncOS for Email Security 8.0 の新機能および拡張機能について説明します。このリリースの詳細については、製品リリース ノートを参照してください。リリース ノートは、次の URL の Cisco カスタマー サポート ページから入手できます。


<http://www.cisco.com/web/ironport/index.html>

以前のリリースのリリース ノートで、前に追加された機能および拡張機能を参照することが役に立つ場合もあります。[サポート ポータル (Support Portal)] で該当するリリース ノートを参照するには、適切なアプライアンスのマニュアル ページの [旧リリース (Earlier Releases)] のリンクをクリックします。

機能	説明
リリース 8.0.1 の新機能：	
新しいハードウェアのサポート	このリリースでは、新しい C380 および C680 アプライアンスがサポートされます。
リモート電源管理	この機能は、C380 および C680 ハードウェアでのみ使用可能です。 アプライアンスのシャーシの電源をリモートでリセットできます。 この機能は、必要なときに使用できるように、事前に設定しておく必要があります。 詳細については、「リモート電源管理のイネーブル化」 (P.29-24) および「アプライアンスの電源のリモートリセット」 (P.36-28) を参照してください。
データの損失防止設定の機能拡張	カスタム DLP ポリシーに対して作成したカスタム コンテンツ照合分類子を再利用できるようになりました。

機能	説明
リリース 8.0.0 の新機能	
Cisco E メール セキュリティ仮想アプライアンス	<p>シスコは、所有するネットワーク上でホストできる仮想マシンとして Cisco 電子メール セキュリティ アプライアンスを提供します。</p> <p>仮想アプライアンスは、シスコと Cisco UCS サーバ（ブレードまたはラックマウント）ハードウェア プラットフォームが動作している VMware ESXi バージョン 4.x から購入した個別のライセンスが必要です。</p> <p>『Cisco Content Security Virtual Appliance Installation Guide』には、仮想アプライアンスの要件の詳細情報が含まれます。</p> <p>使用できる仮想アプライアンス モデルのリストについては、『Cisco Content Security Virtual Appliance Installation Guide』またはリリース ノートを参照してください。</p> <p>これには、メール用の AsyncOs への次の変更が含まれます。</p> <ul style="list-style-type: none"> 電子メール セキュリティ仮想アプライアンスのライセンスは、ネットワーク内に複数の仮想アプライアンスを複製し、実行することができます。 仮想アプライアンスのライセンスをインストールするための <code>loadlicense</code> CLI コマンド。複数の仮想アプライアンスに同じライセンスを使用できます。 ライセンス キーは仮想アプライアンスのライセンスに含まれています。ライセンス キーはライセンスと同時に期限切れになります。新しいライセンス キーを購入すると、新しい仮想アプライアンスのライセンスをダウンロードおよびインストールする必要があります。 仮想アプライアンスのライセンスにライセンス キーが含まれているため、シスコのスパム対策またはアウトブレイク フィルタなどの AsyncOS 機能の 30 日間評価はありません。 仮想アプライアンスのライセンスをインストールする前に、テクニカル サポートは利用できません。 バージョン、<code>ipcheck</code>、および <code>supportrequest</code> CLI コマンドは、そこに含まれている仮想アプライアンスの情報に更新されています。 仮想アプライアンスの誤設定に対する新しいアラートとログがあります。 <p>物理/仮想アプライアンス間のその他の相違点については、必要な場合にこのガイドに表示されます。</p>

機能	説明
集中型ポリシー、ウイルスおよびアウトブレイク隔離	<p>次の隔離は、まとめて Cisco コンテンツ セキュリティ管理アプライアンス に中央集中化できます。</p> <ul style="list-style-type: none"> • アンチウイルス • アウトブレイク • 以下で捕捉されるメッセージに使用するポリシー隔離 <ul style="list-style-type: none"> – メッセージ フィルタ – コンテンツ フィルタ – データ消失防止ポリシー <p>これらの隔離の中央集中化には次の利点があります。</p> <ul style="list-style-type: none"> • 管理者は複数の電子メール セキュリティ アプライアンスで隔離されたメッセージを 1 か所で管理できます。 • 隔離されたメッセージは、セキュリティ リスクを減らすために、DMZ の代わりに、ファイアウォールの内側に保存されます。 • 一元化された隔離は、Cisco コンテンツ セキュリティ管理アプライアンスの標準のバック アップ機能を使用して実行できます。 <p>詳細については、第 27 章「隔離」を参照してください。</p>
クライアント認証を使用した SMTP セッション認証	<p>電子メールセキュリティアプライアンスとユーザのメールアプリケーション間の SMTP セッションを認証するクライアント証明書に対応します。</p> <p>ユーザがメールアプリケーションに共通の Access Card (CAC) を使用する組織はこの機能を使って、CAC と ActivClient のミドルウェアアプリケーションがアプライアンスに配信する証明書を要求するように電子メールセキュリティアプライアンスを設定できます。</p> <p>この機能には、次の更新が含まれます。</p> <ul style="list-style-type: none"> • 新しい LDAP クエリーはユーザのメールクライアントと電子メールセキュリティアプライアンス間の SMTP セッションを認証するクライアント証明書の有効性を検査します。 • アプライアンスがユーザのメールアプリケーションがアプライアンスに接続する SMTP Auth コマンドを使用するかどうかを判断できる SMTP Auth LDAP クエリーへの更新。 • SMTP 認証プロファイルの新しい証明書タイプ。 • 新しい TLS パラメータが、メールフローポリシーに追加されました。[クライアント証明書の検証 (Verify Client Certificate)] • アプライアンスが証明書の確認の一部として、ユーザの証明書が無効になっていないかを確認する、失効した証明書のリスト ([Certificate Revocation List (証明書失効リスト)])。 <p>詳細については、第 23 章「クライアント証明書を使用した SMTP セッションの認証」を参照してください。</p>

機能	説明
FIPS 140-2 Level 1 の準拠	<p>Cisco 電子メール セキュリティ アプライアンスは FIPS 140-2 Level 1 標準に準拠するために CiscoSSL の暗号化ツール キット、GGSG 承認された暗号スイートを 使用します。CiscoSSL には OpenSSL、FIPS 準拠のシスコの共通の暗号化モジュールの拡張バージョンが含まれます。</p> <p>管理者は FIPS モードを <code>fipsconfig CLI</code> コマンドを使用してオンまたはオフにできます。</p> <p>アプライアンスが FIPS モードの場合、CiscoSSL を使用する他、AsyncOS 8.0 for Email には次の機能拡張があります。</p> <ul style="list-style-type: none"> • AsyncOS は FIPS モードのアプライアンスで使用される証明書のタイプとキーを制限します。 • AsyncOS は SCP によるログのプッシュを含む着信と発信接続用に SSH プロトコルのバージョン 1 のサポートをドロップしました。 • DKIM 署名の RSA キーは、1024、1536、および 2048 ビットのみです。DKIM 検証は FIPS 準拠ではない証明書の <code>permfail</code> を返します。 • 電子メール セキュリティ アプライアンスのシリアル ポートセッションはポートへの接続が終了してから 30 分後にタイムアウトします。 • 次のアプライアンスとその他のサーバ間の通信は、FIPS 準拠の LDAP を含めたりリモート メール ホスト、Cisco サーバ、および Web インターフェイスです。 • 通信に CiscoSSL を使用する必要のない機能、またはカスタマー データを送信しない機能は FIPS 準拠である必要はありません。これらの機能には、他のクラスタ化されたアプライアンス、RSA Enterprise Manager (DLP)、シスコの更新サーバ、暗号化が含まれます。 <p>(注) FIPS 準拠の一部として、AsyncOS for Email は SSH バージョン 1 をサポートしません。</p> <p> 警告 AsyncOS 7.3 からアップグレードした場合、アプライアンスは FIPS モードでは実行されません。アップグレード後に新しい証明書とキーをインポートまたは生成する必要があります。</p> <p>FIPS は物理/仮想電子メール セキュリティ アプライアンスで使用できます。詳細については、第 24 章「FIPS 管理」を参照してください。</p>
お気に入りリスト	<p>すぐにアクセスできるお気に入りページのメニューに、よく使うページを追加します。</p> <p>詳細については、「お気に入りページの使用」(P.29-59) を参照してください。</p>
バックグラウンドでのダウンロードのアップグレード	<p>アップグレードをバックグラウンドでダウンロードして、後でインストールできます。これにより、サービスの中断を最小限に抑えることができます。</p> <p>詳細については、「GUI からの AsyncOS のアップグレード」(P.29-15) を参照してください。</p>

機能	説明
レポート作成機能の拡張	<p>レポート作成機能の拡張により、以下が可能になりました。</p> <ul style="list-style-type: none"> よく参照するチャートと表のカスタム レポート ページを作成します。 [データ消失防止 (Data Loss Prevention)] または [コンテンツ フィルタリング (Content Filtering)] ポリシーに違反するメッセージの [メッセージ トラッキング (Message Tracking)] データを表示するには、レポートのリンクをクリックします。この機能拡張により、こうした違反の調査パターンと根本原因を簡素化します。 <p>詳細については、第 26 章「電子メール セキュリティ モニタの使用法」を参照してください。</p>
メッセージ トラッキング機能拡張	<ul style="list-style-type: none"> メッセージ トラッキングから UTF-8 で符号化されたサブジェクトを含むメッセージを検索できます。 メッセージ トラッキングの検索を隔離されたメッセージに限定できます メッセージ トラッキングの検索結果とメッセージの詳細には、メッセージが存在する隔離のメッセージ詳細ページへのリンクが含まれます。 メッセージ トラッキング クエリーが 1000 件以上のメッセージを返した場合、他のツールを使用して分析するために、カンマ区切り形式のファイルとしてクエリーに一致する、最大 50,000 のメッセージをエクスポートできます。 <p>詳細については、第 25 章「メッセージ トラッキング」を参照してください。</p>
より柔軟なパスワードの長さのサポート	<p>ゼロ文字を含め、任意の長さのアプライアンスのパスワードがサポートされるようになりました。</p> <p>詳細については、「パスワード」(P.28-17) を参照してください。</p>
SNMP トラップの改善	<p>linkUp および linkDown の SNMP トラップは、標準 RFC 実装 (RFC-3418) に置き換えられました。</p>
機能拡張を更新する DLP エンジン	<p>アプライアンスは構成によって DLP ポリシーから自動または手動で使用されている DLP エンジンとコンテンツ照合分類子をダウンロードして更新できるようになりました。アプライアンスの RSA DLP エンジンとコンテンツ照合分類子を更新するための設定は、[セキュリティ サービス (Security Services)] > [データ消失防止 (Data Loss Prevention)] の [設定 (Settings)] ページからアクセスできます。</p> <p>詳細については、「DLP エンジンおよびコンテンツ照合分類子の更新について」(P.15-39) を参照してください。</p>
スパム隔離の改善	<p>スパム隔離の検索結果は簡単に表示できるようになりました。これにはメッセージ トラッキングの詳細へのリンクが含まれます。</p> <p>詳細については、第 27 章「隔離」を参照してください。</p>

詳細情報の入手先

シスコは、Cisco 電子メール セキュリティ アプライアンスについての理解を深めて頂くために次の資料を提供しています。

マニュアル

マニュアルは、PDF ファイルおよび HTML ファイルとして配布されます。このマニュアルの電子バージョンは、Cisco IronPort カスタマー サポート サイトで入手できます。また、右上の [ヘルプとサポート (Help and Support)] をクリックすることにより、アプライアンスの GUI からユーザ ガイドの HTML オンライン ヘルプ バージョンに直接アクセスできます。

Cisco 電子メール セキュリティ アプライアンスのマニュアル セットには次のマニュアルおよびマニュアルが含まれます。

- リリース ノート
- 電子メール セキュリティ アプライアンスのクイック スタート ガイド
- 『Cisco AsyncOS for Email Security User Guide』 (このマニュアル)
- 『Cisco Content Security Virtual Appliance Installation Guide』
- 『Cisco AsyncOS CLI Reference Guide』

このアプライアンスの関連資料は、

http://www.cisco.com/en/US/products/ps10154/tsd_products_support_series_home.html から入手できます。

トレーニングと認定試験

シスコでは、技術者、パートナー、学生など、それぞれのニーズに合わせた、さまざまなトレーニング プログラムおよびトレーニング コースを用意しています。日本のトレーニングと認定試験の情報については、以下の Web サイトをご覧ください。

<http://www.cisco.com/web/JP/event/index.html>

Knowledge Base

Customer Support Portal の Cisco Knowledge Base には、次の URL からアクセスできます。

<http://www.cisco.com/web/ironport/knowledgebase.html>



(注)

サイトにアクセスするには Cisco.com のユーザ ID が必要です。Cisco.com のユーザ ID をお持ちでない場合は、<https://tools.cisco.com/RPF/register/register.do> で登録できます。

Knowledge Base には、Cisco 製品に関する豊富な情報が用意されています。

通常、記事は次のカテゴリのいずれかに分類されています。

- **How-To** これらの記事では、Cisco 製品の使用方法について説明します。たとえば、How-To の記事では、アプライアンス用データベースのバックアップをとり、復元する手順について説明します。
- **問題と解決策** 問題と解決策の項目では、Cisco 製品の発生時に発生する可能性がある特定のエラーや問題に対処します。たとえば、問題と解決策の記事では、製品の新しいバージョンへのアップグレード時に特定のエラーメッセージが表示された場合の対応方法について説明します。
- **参考資料** 参考資料の項目では、特定のハードウェアに関連するエラー コードなどの情報を一覧表示します。

- **トラブルシューティング** トラブルシューティングの記事は、Cisco 製品に関する一般的な問題の分析方法および解決方法について説明します。たとえば、トラブルシューティングの記事は、DNS で問題が発生した場合に従う手順を提供します。

ナレッジ ベース内の各記事には、一意の回答 ID 番号がつけられています。

Cisco サポート コミュニティ

Cisco サポート コミュニティは、Cisco のお客様、パートナー、および従業員のオンライン フォーラムです。電子メールおよび Web セキュリティに関する一般的な問題や、特定の Cisco 製品に関する技術情報について話し合う場を提供します。このフォーラムにトピックを投稿して質問したり、他の Cisco ユーザと情報を共有したりできます。

Customer Support Portal の Cisco サポート コミュニティには、次の URL からアクセスします。

- 電子メール セキュリティと関連管理
<https://supportforums.cisco.com/community/netpro/security/email>
- Web セキュリティと関連管理 :
<https://supportforums.cisco.com/community/netpro/security/web>

シスコのテクニカル サポート

次の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。

<http://www.cisco.com/en/US/support/index.html>

以下を含むさまざまな作業にこの Web サイトが役立ちます。

- テクニカル サポートを受ける
- ソフトウェアをダウンロードする
- セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける
- ツールおよびリソースへアクセスする
 - Product Alert の受信登録
 - Field Notice の受信登録
 - Bug Toolkit を使用した既知の問題の検索
- Networking Professionals (NetPro) コミュニティで、技術関連のディスカッションに参加する
- トレーニング リソースへアクセスする
- TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する

Japan テクニカル サポート Web サイトでは、Technical Support Web サイト (<http://www.cisco.com/cisco/web/support/index.html>) の、利用頻度の高いドキュメントを日本語で提供しています。

Japan テクニカル サポート Web サイトには、次の URL からアクセスしてください。

<http://www.cisco.com/cisco/web/JP/support/index.html>

サードパーティ コントリビュータ

Cisco AsyncOS 内に含まれる一部のソフトウェアは、FreeBSD Inc.、Stichting Mathematisch Centrum、Corporation for National Research Initiatives Inc.、および他のサードパーティ コントリビュータのソフトウェア使用許諾契約の条項、通知、および条件に基づいて配布されています。これらすべての契約条件は、Cisco ライセンス契約に含まれています。

これらの契約内容の全文は次の URL を参照してください。

https://support.ironport.com/3rdparty/AsyncOS_User_Guide-1-1.html

Cisco AsyncOS 内の一部のソフトウェアは、Tobi Oetiker の書面による同意を得て、RRDtool を基にしています。

このマニュアルには、Dell Computer Corporation の許可を得て複製された内容が一部含まれています。このマニュアルには、McAfee の許可を得て複製された内容が一部含まれています。このマニュアルには、Sophos の許可を得て複製された内容が一部含まれています。

マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、HTML ドキュメント内のフィードバックフォームよりご連絡ください。ご協力をよろしくお願いいたします。

Cisco 電子メール セキュリティ アプライアンスの概要

Cisco AsyncOS のオペレーティング システムには、次の機能が含まれます。

- SenderBase レピュテーション フィルタと Cisco Anti-Spam を統合した独自のマルチレイヤ アプローチによるゲートウェイでの**スパム対策**。
- Sophos および McAfee ウイルス対策スキャン エンジンによるゲートウェイでの**ウイルス対策**。
- 新しいアップデートが適用されるまで危険なメッセージを隔離し、新しいメッセージ脅威に対する脆弱性を削減する、新しいウイルス、詐欺、およびフィッシングの拡散に対する Cisco の独自保護機能である**アウトブレイク フィルタ**。
- 隔離されたスパムおよび陽性と疑わしいスパムへのエンドユーザ アクセスを提供する、オンボックスまたはオフボックスの**スパム隔離**。
- **電子メール認証** Cisco AsyncOS は、発信メールに対する DomainKeys および DomainKeys Identified Mail (DKIM) の署名の他に、着信メールに対する Sender Policy Framework (SPF)、Sender ID Framework (SIDF)、DKIM の検証など、さまざまな形式の電子メール認証をサポートします。
- **Cisco 電子メール暗号化**。HIPAA、GLBA、および同様の規制要求に対応するために発信メールを暗号化できます。これを行うには、電子メール セキュリティ アプライアンスで暗号化ポリシーを設定し、ローカル キー サーバまたはホステッド キー サービスを使用してメッセージを暗号化します。
- アプライアンス上のすべての電子メール セキュリティ サービスおよびアプリケーションを管理する、単一で包括的なダッシュボードである**電子メール セキュリティ マネージャ**。電子メール セキュリティ マネージャは、ユーザ グループに基づいて電子メール セキュリティを実施でき、インバウンドとアウトバウンドの独立したポリシーを使用して、Cisco レピュテーション フィルタ、アウトブレイク フィルタ、アンチスパム、アンチウイルス、および電子メール コンテンツ ポリシーを管理できます。

- 電子メール ポリシーに違反したメッセージを保持する**オンボックス隔離エリア**。隔離はアウトブレイク フィルタ機能とシームレスに連携します。
- **オンボックスのメッセージトラッキング**。AsyncOS for Email には、電子メール セキュリティ アプライアンスが処理するメッセージのステータスの検索が容易にできる、オンボックスのメッセージトラッキング機能があります。
- 企業のすべての電子メール トラフィックを全体的に確認できる、すべてのインバウンドおよびアウトバウンドの電子メールに対する**メールフロー モニタ機能**。
- 送信者の IP アドレス、IP アドレス範囲、またはドメインに基づいた、インバウンドの送信者の**アクセス コントロール**。
- 広範な**メッセージフィルタリング** テクノロジーを使用して、社内ポリシーを順守させ、企業のインフラストラクチャを出入りする特定のメッセージに作用させることができます。フィルタルールでは、メッセージまたは添付ファイルの内容、ネットワークに関する情報、メッセージエンベロープ、メッセージヘッダー、またはメッセージ本文に基づいてメッセージを識別します。フィルタアクションでは、メッセージをドロップ、バウンス、アーカイブ、ブラインドカーボンコピー、または変更したり、通知を生成したりできます。
- **セキュアな SMTP over Transport Layer Security 経由のメッセージの暗号化**により、企業のインフラストラクチャとその他の信頼できるホストとの間でやりとりされるメッセージが暗号化されるようになります。
- **Virtual Gateway™** テクノロジーにより、Cisco アプライアンスは、単一サーバ内で複数の電子メール ゲートウェイとして機能できるため、さまざまな送信元またはキャンペーンの電子メールを、それぞれ独立した IP アドレスを通して送信するように分配できます。これにより、1 つの IP アドレスに影響する配信可能量の問題が、他の IP アドレスに及ばないようにします。

AsyncOS for Email は、メッセージを受け入れて配信するために、RFC 2821 準拠の Simple Mail Transfer Protocol (SMTP; シンプル メール転送プロトコル) をサポートします。

レポート作成コマンド、モニタリング コマンド、およびコンフィギュレーション コマンドのほとんどは、HTTP 経由でも HTTPS 経由でも Web ベースの GUI から使用できます。さらに、セキュア シェル (SSH)、Telnet、または直接シリアル接続でアクセスするインタラクティブなコマンドライン インターフェイス (CLI) がシステムに用意されています。

また、複数の 電子メール セキュリティ アプライアンス のレポート、トラッキング、および隔離管理を統合するように Cisco コンテンツ セキュリティ管理アプライアンス を設定できます。

サポートされる言語

AsyncOS は次の言語のいずれかで GUI および CLI を表示できます。

- 英語
- フランス語
- スペイン語
- ドイツ語
- イタリア語
- 韓国語
- 日本語
- ポルトガル語 (ブラジル)
- 中国語 (繁体字および簡体字)
- ロシア語



CHAPTER 2

概要

- 「Web ベースのグラフィカル ユーザ インターフェイス (GUI)」 (P.2-1)
- 「コマンドライン インターフェイス (CLI)」 (P.2-5)

Web ベースのグラフィカル ユーザ インターフェイス (GUI)

Web ベースのグラフィカル ユーザ インターフェイス (GUI) とコマンドライン インターフェイス (CLI) の両方を使用して Cisco アプライアンスを管理できます。GUI には、システムの設定およびモニタに必要な機能のほとんど含まれています。ただし、すべての CLI コマンドが GUI から使用できるわけではありません。一部の機能は CLI からのみ使用できます。

ブラウザ要件

Web ベースの UI にアクセスするには、ブラウザが JavaScript およびクッキーをサポートし、受け入れが有効になっている必要があります。さらに、Cascading Style Sheet (CSS) を含む HTML ページをレンダリングする必要があります。



(注)

AsyncOS 5.5 からは、Web ベースの UI は、Yahoo! User Interface (YUI) ライブラリからライブラリを組み込んでいます。これは、リッチでインタラクティブな Web アプリケーションを構築するための、JavaScript で記述されたユーティリティおよびコントロールのセットです。この変更の目的は、Web ベース UI のユーザ操作性を改善することです。

YUI ライブラリは、一般的に使用されているほとんどのブラウザをサポートしています。また、YUI ライブラリは、ブラウザサポートに対する包括的で公開されたアプローチを取り、「A グレード」ブラウザとして指定されたすべてのブラウザでコンポーネントが問題なく動作することを表明しています。格付けされたブラウザのサポートについては、次の URL を参照してください。

<http://developer.yahoo.com/yui/articles/gbs/>

Cisco は、Web ベース UI へのアクセスに次のリストの A グレード ブラウザを使用してシスコの Web アプリケーションをテストしているため、これらのブラウザを推奨します。

- Firefox 3.6
- Windows XP および Vista : Internet Explorer 7 および 8
- Windows 7 : Internet Explorer 8 および 9、Google Chrome、Firefox 4
- Mac OS X : Safari 4 以降、Firefox 4

GUI へのアクセス時には、複数のブラウザ ウィンドウまたはタブを同時に使用して、Cisco アプライアンスに変更を行わないように注意してください。GUI セッションおよび CLI セッションも同時に使用しないでください。同時に使用すると、予期しない動作が生じ、サポートの対象外になります。

インターフェイスの一部のボタンまたはリンクからは追加のウィンドウがオープンされるため、GUI を使用するには、ブラウザのポップアップ ブロックの設定が必要な場合があります。

GUI へのアクセス

デフォルトで、システムは管理インターフェイス (Cisco C60/600/650/660/670、C30/300/350/360/370、および X1000/1050/1060/1070 アプライアンスの場合) またはデータ 1 (Cisco C10/100/150/160) インターフェイスで HTTP がイネーブルに設定された状態で出荷されます。詳細については、「[インターフェイスでの GUI のイネーブル化](#)」(P.32-7) を参照してください。

新規システムの GUI にアクセスするには、次の URL にアクセスします。

<http://192.168.42.42>

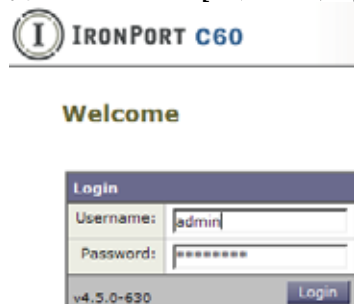
ログイン ページが表示されたら、デフォルトのユーザ名とパスワードを使用してシステムにログインします。

工場出荷時のデフォルト ユーザ名とパスワード

- ユーザ名 : `admin`
- パスワード : `ironport`

次に例を示します。

図 2-1 [ログイン (Login)] 画面



新規 (以前のリリースの AsyncOS からのアップグレードではなく) システムの場合は、システム セットアップ ウィザードへ自動的にリダイレクトされます。

初期システム セットアップ時に、インターフェイスの IP アドレスと、このインターフェイスの HTTP サービス、HTTPS サービス、またはその両方を実行するかどうかを選択します。インターフェイスの HTTP サービス、HTTPS サービス、またはその両方がイネーブルに設定されている場合は、サポートしている任意のブラウザを使用し、ブラウザのロケーションフィールド（「アドレス バー」）に URL として IP インターフェイスの IP アドレスまたはホスト名を入力して GUI を表示できます。

次に例を示します。

`http://192.168.1.1` または

`https://192.168.1.1` または

`http://mail3.example.com` または

`https://mail3.example.com`



(注)

インターフェイスの HTTPS がイネーブルに設定されている（かつ HTTP 要求がセキュア サービスにリダイレクトされていない）場合は、「`https://`」のプレフィックスを使用して GUI にアクセスすることに留意してください。

ログイン

GUI にアクセスするすべてのユーザは、ログインが必要です。ユーザ名とパスワードを入力してから [ログイン (Login)] をクリックして GUI にアクセスします。サポートされる Web ブラウザを使用する必要があります。「[ブラウザ要件 \(P.2-1\)](#)」を参照してください。admin アカウントまたは作成済みの特定のユーザ アカウントを使用してログインできます 詳細については、「[ユーザの追加 \(P.28-4\)](#)」を参照してください。

ログインしたら、[モニタ (Monitor)] > [受信メールの概要 (Incoming Mail Overview)] ページが表示されます。

GUI セクションおよび基本ナビゲーション

GUI は、Cisco アプライアンスの機能に対応する、[モニタ (Monitor)]、[メール ポリシー (Mail Policies)]、[セキュリティ サービス (Security Services)]、[ネットワーク (Network)]、および [システム管理 (System Administration)] のメニューで構成されています。以降の章では、各セクション内のページで実行するタスクなど、各セクションについて説明します。



(注)

GUI のオンライン ヘルプは、GUI 内のどのページからも使用できます。オンライン ヘルプにアクセスするには、ページの右上にある [ヘルプ (Help)] > [オンライン ヘルプ (Online Help)] リンクをクリックします。

各メイン セクション ([モニタ (Monitor)]、[メール ポリシー (Mail Policies)]、[セキュリティ サービス (Security Services)]、[ネットワーク (Network)]、および [システム管理 (System Administration)]) のメニュー見出しをクリックして、インターフェイスのセクション内をナビゲートします。各メニュー内にあるのが、情報やアクティビティをさらにグループ化するサブセクションです。たとえば、[セキュリティ サービス (Security Services)] セクションには、[スパム対策 (Anti-Spam)] ページを表示する [スパム対策 (Anti-Spam)] セクションがあります。GUI の特定のページを参照する場合、マニュアルではそれに沿ってメニュー名に続けて矢印とページ名を表記して使います。たとえば、[セキュリティ サービス (Security Services)] > [SenderBase] です。

[モニタ (Monitor)] メニュー

[モニタ (Monitor)] セクションには、メールフロー モニタ機能 (概要、着信メール、発信先、発信者、配信ステータス、内部ユーザ、コンテンツ フィルタ、ウイルス拡散、ウイルス タイプ、システム容量、システム ステータス)、ローカル隔離と外部隔離、およびスケジュール済みレポートの各機能のページがあります。このメニューからメッセージ トラッキングにもアクセスできます。

[メール ポリシー (Mail Policies)] メニュー

[メール ポリシー (Mail Policies)] セクションには、電子メール セキュリティ マネージャ機能 (メール ポリシーおよびコンテンツ フィルタを含む)、ホスト アクセス テーブル (HAT) と受信者アクセス テーブル (RAT) 設定、送信先コントロール、バウンス検証、DomainKeys、テキストリソース、およびディクショナリのページがあります。

[セキュリティ サービス (Security Services)] メニュー

[セキュリティ サービス (Security Services)] セクションには、アンチスパム、アンチウイルス、Cisco 電子メール暗号化、アウトブレイク フィルタ、および SenderBase Network Participation の各機能のグローバル設定を行うためのページがあります。このメニューからは、レポート作成、メッセージ トラッキング、外部スパム隔離の機能もイネーブルにします。

[ネットワーク (Network)] メニュー

[ネットワーク (Network)] セクションには、IP インターフェイス、リスナー、SMTP ルート、DNS、ルーティング、バウンス プロファイル、SMTP 認証、および着信リレーを作成および管理するページがあります。

[システム管理 (System Administration)] メニュー

[システム管理 (System Administration)] セクションには、トレース、アラート、ユーザ管理、LDAP、ログ サブスクリプション、リターンアドレス、システム時刻、設定ファイル管理、ライセンス キー設定、ライセンス キー、シャットダウン/再起動、アップグレード、およびシステム セットアップ ウィザードの各機能のページがあります。

集中管理

集中管理機能を使用し、クラスタをイネーブルにしている場合は、クラスタ内のマシンを参照し、クラスタ、グループ、マシン間での設定の作成、削除、コピー、および移動 (つまり、`clustermode` コマンドおよび `clusterset` コマンドと同等の内容) を GUI 内から実行できます。

詳細については、「[GUI でのクラスタの管理](#)」(P.35-16) を参照してください。

[変更を確定 (Commit Changes)] ボタン

GUI の確定モデルは、CLI で使用されている「明示的な確定」モデルと同じです。詳細については、「[設定変更の確定](#)」(P.2-9) を参照してください。重要: GUI で設定を変更する際は、[変更を確定 (Commit Changes)] ボタンをクリックして、それらの変更を明示的に確定する必要があります。このボタンは、保存する必要のある未確定の変更がある場合に表示されます。

図 2-2 【変更を確定 (Commit Changes)】ボタン

Commit Changes »

【変更を確定 (Commit Changes)】ボタンをクリックして表示されたページでは、コメントを追加し変更を確定したり、最新の確定 (CLI の `clear` コマンドと同等。「設定変更のクリア」(P.2-10) を参照) の後に行われた変更をすべて中止したり、キャンセルすることができます。

図 2-3 確定された変更の確認
Uncommitted Changes

アクティブなセッションの表示

GUI から、現在電子メールセキュリティ アプライアンスにログインしているすべてのユーザとセッションの情報を表示できます。

これらのアクティブなセッションを表示するには、ページの右上にある [オプション (Options)] > [アクティブなセッション (Active Sessions)] をクリックします。

[アクティブなセッション (Active Sessions)] ページで、ユーザ名、ユーザ ロール、ログイン時間、アイドル時間、コマンドラインからのログインか、GUI からのログインかを表示できます。

図 2-4 アクティブなセッション
Active Sessions

Active Sessions for esa01-vmml-tpub.qa					
Username	Role	Login Time ▼	Idle Time	Remote Host	Interface
susan1	DLP Administrator*	17 Mar 2011 22:00 (GMT)	1 min 55 secs	173.37.1.34	GUI
admin	Administrator	17 Mar 2011 22:00 (GMT)	1 min 47 secs	173.37.1.34	GUI

* Custom User Role for delegated administration of web policies.

コマンドライン インターフェイス (CLI)

Cisco AsyncOS のコマンドライン インターフェイスは、Cisco アプライアンスを設定およびモニタするために設計されたインタラクティブなインターフェイスです。引数を指定しても指定しなくても、コマンド名を入力すると、コマンドが起動されます。引数を指定せずにコマンドを入力した場合は、必要な情報を要求するプロンプトが表示されます。

コマンドライン インターフェイスには、SSH または Telnet のサービスがイネーブルに設定されている IP インターフェイスで SSH または Telnet 経由、またはシリアル ポートで端末エミュレーションソフトウェアを使用してアクセスできます。工場出荷時のデフォルトでは、管理ポートに SSH および Telnet が設定されています。これらのサービスをディセーブルにするには、`interfaceconfig` コマンドを使用します。

特定の CLI コマンドの詳細については、『Cisco AsyncOS CLI Reference Guide』を参照してください。

コマンドライン インターフェイスの表記法

ここでは、AsyncOS CLI のルールおよび表記法について説明します。

コマンド プロンプト

最上位のコマンド プロンプトは、完全修飾ホスト名に続いて大なり (>) 記号とスペース 1 つで構成されます。次に例を示します。

```
mail3.example.com>
```

アプライアンスが集中管理機能を使用したクラスタの一部として設定されている場合、CLI のプロンプトが変わって現在のモードを示します。次に例を示します。

```
(Cluster Americas) >
```

または

```
(Machine losangeles.example.com) >
```

詳細については、「[集中管理](#)」(P.2-4) を参照してください。

コマンドを実行すると、CLI によりユーザの入力が要求されます。CLI がユーザの入力を待機している場合は、コマンド プロンプトとして、角カッコ ([]) で囲まれたデフォルト入力値の後に大なり (>) 記号が表示されます。デフォルトの入力値がない場合、コマンド プロンプトのカッコ内は空です。

次に例を示します。

```
Please create a fully-qualified hostname for this Gateway
```

```
(Ex: "mail3.example.com"):
```

```
[ ]> mail3.example.com
```

デフォルト設定がある場合は、コマンド プロンプトのカッコ内にその設定が表示されます。次に例を示します。

```
Ethernet interface:
```

1. Data 1
2. Data 2
3. Management

```
[1]> 1
```

デフォルト設定が表示される場合に Return を入力すると、デフォルト値を入力したことになります。

```
Ethernet interface:
```

1. Data 1
2. Data 2
3. Management

```
[1]> (type Return)
```

コマンド構文

インタラクティブ モードで動作中の場合、CLI コマンド構文は、空白スペースを含めず、引数やパラメータも指定しない単一コマンドで構成されます。次に例を示します。

```
mail3.example.com> systemsetup
```

選択リスト

入力できる複数の選択肢がある場合、コマンドによっては番号付きリストを使用します。プロンプトで選択する番号を入力します。

次に例を示します。

```
Log level:  
1. Error  
2. Warning  
3. Information  
4. Debug  
5. Trace  
[3]> 3
```

Yes/No クエリー

yes または no のオプションがある場合、質問はデフォルト値（カッコ内表示）を付けて表示されます。**Y**、**N**、**Yes**、または **No** で返答できます。大文字小文字の区別はありません。

次に例を示します。

```
Do you want to enable FTP on this interface? [Y]> n
```

サブコマンド

コマンドによっては、サブコマンドを使用する場合があります。サブコマンドには、NEW、EDIT、および DELETE などの命令があります。EDIT および DELETE の機能の場合、これらのコマンドは、システムですでに設定されているレコードのリストを提供します。

次に例を示します。

```
mail3.example.com> interfaceconfig  
  
Currently configured interfaces:  
  
1. Management (192.168.42.42/24: mail3.example.com)  
  
Choose the operation you want to perform:  
  
- NEW - Create a new interface.  
  
- EDIT - Modify an interface.
```

```
- GROUPS - Define interface groups.  
- DELETE - Remove an interface.  
  
[]>
```

サブコマンド内からメイン コマンドに戻るには、空のプロンプトで **Enter** または **Return** を入力します。

エスケープ

サブコマンド内でいつでも **Ctrl+C** キーボードショートカットを使用して、すぐに最上位の CLI に戻ることができます。

履歴

CLI は、セッション中に入力するすべてのコマンドの履歴を保持します。最近使用したコマンドの実行リストをスクロールするには、キーボードの **↑** および **↓** の矢印キーを使用するか、**Ctrl+P** キーと **Ctrl+N** キーを組み合わせで使用します。

```
mail3.example.com> (type the Up arrow key)
```

```
mail3.example.com> interfaceconfig (type the Up arrow key)
```

```
mail3.example.com> topin (type the Down arrow key)
```

コマンドの補完

Cisco AsyncOS CLI は、コマンドの補完をサポートします。あるコマンドの先頭数文字を入力して **Tab** キーを入力すると、CLI によって一意のコマンドのストリングが補完されます。入力した文字がコマンドの中で一意ではない場合、CLI はそのセットを「絞り込み」ます。次に例を示します。

```
mail3.example.com> set (type the Tab key)  
setgateway, sethostname, setttime, settz  
mail3.example.com> seth (typing the Tab again completes the entry with sethostname)
```

CLI の履歴およびファイルの補完機能では、**Enter** または **Return** を入力してコマンドを起動する必要があります。

設定の変更

電子メール操作を通常どおり継続しながら、Cisco AsyncOS に対する設定変更を行えます。

設定変更は、次の処理を行うまでは有効になりません。

1. コマンド プロンプトで **commit** コマンドを発行します。
2. **commit** コマンドに必要な入力値を指定します。
3. CLI で **commit** 処理の確認を受け取ります。

確定されていない設定に対する変更は記録されますが、commit コマンドが実行されるまでは有効になりません。



(注) AsyncOS のすべてのコマンドが、commit コマンドの実行を必要とするわけではありません。変更を有効にする前に確定を行う必要があるコマンドの概要については、『Cisco AsyncOS CLI Reference Guide』を参照してください。

CLI セッションの終了、システムのシャットダウン、再起動、障害、または clear コマンドの発行により、確定されていない変更はクリアされます。

汎用 CLI コマンド

この項では、変更の確定またはクリア、ヘルプへのアクセス、およびコマンドライン インターフェイスの終了に使用するコマンドについて説明します。

設定変更の確定

Cisco アプライアンスに対する設定変更の保存には、commit コマンドが重要です。設定変更の多くは、commit コマンドを入力するまで有効になりません。(変更内容を有効にするために commit コマンドを使用する必要がないコマンドも少数あります。commit コマンドは、commit コマンドまたは clear コマンドが最後に発行されてから、Cisco AsyncOS に対して行われた設定変更に適用されます。コメントとして最大 255 文字を使用できます。変更内容は、タイムスタンプとともに確認を受け取るまでは、確定されたものとして認められません。

commit コマンドの後のコメントの入力は任意です。

```
mail3.example.com> commit
```

```
Please enter some comments describing your changes:
```

```
[ ]> Changed "psinet" IP Interface to a different IP address
```

```
Changes committed: Wed Jan 01 12:00:01 2003
```



(注) 変更を正常に確定するには、最上位のコマンドプロンプトになっている必要があります。コマンドライン階層の1つ上のレベルに移動するには、空のプロンプトで Return を入力します。

設定変更のクリア

`clear` コマンドは、`commit` コマンドまたは `clear` コマンドが最後に発行されてから、Cisco AsyncOS の設定に対して行われた変更内容があればクリアします。

```
mail3.example.com> clear
```

```
Are you sure you want to clear all changes since the last commit? [Y]> y
```

```
Changes cleared: Mon Jan 01 12:00:01 2003
```

```
mail3.example.com>
```

コンフィギュレーション変更のロールバック

`rollbackconfig` コマンドは最新の確定済みの設定を 10 個表示し、ロールバックするものを 1 つ選択できます。

管理者だけがこのコマンドを使用できます。



(注)

このコマンドは、クラスタ化されたアプライアンス上では動作しません。以前のバージョンの AsyncOS に戻した場合は、アプライアンスは設定を復元できません。

```
mail.example.com> rollbackconfig
```

```
Previous Commits :
```

Committed On	User	Description

1. Wed Sep 19 22:03:10 2012	admin	Enabled anti-spam
2. Wed Sep 19 21:51:14 2012	admin	Updated envelope encry...
3. Wed Sep 19 18:50:41 2012	admin	

```
Enter the number of the config to revert to.
```

```
[1]> 1
```



```
Reverted to Wed Sep 19 18:50:41 2012      admin

Do you want to commit this configuration now?[N]> y

Committed the changes successfully
```

コマンドライン インターフェイス セッションの終了

quit コマンドを実行すると、CLI アプリケーションからログアウトします。確定されていない設定変更はクリアされます。quit コマンドは電子メール操作には影響しません。ログアウトはログ ファイルに記録されます (exit の入力、quit の入力と同じです)。

```
mail3.example.com> quit

Configuration changes entered but not committed.  Exiting will lose changes.

Type 'commit' at the command prompt to commit changes.

Are you sure you wish to exit?  [N]> y
```

コマンドライン インターフェイスでのヘルプの検索

help コマンドを実行すると、使用可能なすべての CLI コマンドが表示され、各コマンドの簡単な説明を参照できます。help コマンドは、コマンド プロンプトで help と入力するか、疑問符 (?) を 1 つ入力して実行できます。

```
mail3.example.com> help
```




CHAPTER 3

セットアップおよび設置

- 「設置計画」 (P.3-1)
- 「Cisco アプライアンスのネットワークへの物理接続」 (P.3-4)
- 「システム セットアップの準備」 (P.3-7)
- 「システム セットアップ ウィザードの使用方法」 (P.3-12)
- 「設定と次の手順の確認」 (P.3-37)

設置計画

計画決定に影響を与える情報の確認

- 仮想電子メール セキュリティ アプライアンスを設定する場合は、この章に進む前に『*Cisco Virtual Security Appliance Installation Guide*』を参照してください。
- Cisco M-Series アプライアンスを設定する場合は、第 38 章「Cisco コンテンツ セキュリティ管理 アプライアンスの集中型サービス」を参照してください。
- インフラストラクチャへのアプライアンスの配置に影響する可能性のある一部の機能について、設置前に第 4 章「電子メール パイプラインの理解」を参照することを推奨します

ネットワーク境界に Cisco アプライアンスを配置する

お使いの電子メール セキュリティ アプライアンスが、Mail Exchange (MX) とも呼ばれる SMTP ゲートウェイとして機能するように設計されています。最適な結果を得るために、機能によっては、アプライアンスが電子メールを送受信するためにインターネットに直接アクセスできる IP アドレス（つまり、外部 IP アドレス）を割り当てられた最初のマシンである必要があります。

受信者ごとのレピュテーション フィルタリング、アンチスパム、アンチウイルス、およびウイルス アウトブレイク フィルタの機能（「SenderBase レピュテーション サービス」 (P.6-1)、「IronPort Anti-Spam フィルタリング」 (P.13-3)、「Sophos Anti-Virus フィルタリング」 (P.12-2)、および「アウトブレイク フィルタ」 (P.14-1) を参照）は、インターネットからおよび内部ネットワークからのメッセージの直接のフローを扱うことを目的としています。企業が送受信するすべての電子メール トラフィックに対するポリシー施行（「接続を許可するホストの定義の概要」 (P.7-1)）のためにアプライアンスを設定できます。

Cisco アプライアンスは、パブリック インターネットを介してアクセス可能なことと、電子メール インフラストラクチャの「第1 ホップ」であることの両方を満たすことを確認します。別の MTA をネットワーク境界に配置してすべての外部接続を処理させると、電子メール セキュリティ アプライアンスで送信者の IP アドレスを判別できなくなります。送信者の IP アドレスは、メール フロー モニタで送信元を識別および区別したり、SenderBase レピュテーション サービスに送信者の SenderBase レピュテーション スコア (SBRs) を問い合わせたり、Cisco Anti-Spam 機能およびアウトブレイク フィルタ機能の有効性を高めたりするために必要です。



(注)

インターネットから電子メールを受信する最初のマシンとして IronPort アプライアンスを設定できない場合でも、IronPort アプライアンスで使用可能なセキュリティ サービスの一部は利用できます。詳細については、「着信リレー構成における送信者の IP アドレスの決定」(P.13-14) を参照してください。

Cisco アプライアンスを SMTP ゲートウェイとして使用することにより、次の機能が実現されます。

- メール フロー モニタ機能 (第 26 章「電子メール セキュリティ モニタの使用法」を参照) により、内部および外部の両方の送信者から企業に着信するすべての電子メール トラフィックを把握できます。
- ルーティング、エイリアシング、およびマスカレードを対象とする LDAP クエリー (第 22 章「LDAP クエリー」を参照) では、ディレクトリ インフラストラクチャを統合でき、更新を単純化できます。
- エイリアス テーブル (「エイリアス テーブルの作成」(P.21-7) を参照)、ドメイン ベースのルーティング (「ドメイン マップ機能」(P.21-28) を参照)、およびマスカレード (「マスカレードの設定」(P.21-16) を参照) などの一般的なツールによって、オープンソースの MTA からの移行が簡単になります。

DNS への Cisco アプライアンスの登録

不正な電子メール送信者は、次の攻撃対象を探してパブリック DNS レコードを積極的に検索します。Cisco Anti-Spam、アウトブレイク フィルタ、McAfee Antivirus および Sophos Anti-Virus のすべての機能を利用するために、Cisco アプライアンスが DNS に登録されていることを確認します。

Cisco アプライアンスを DNS に登録するには、アプライアンスのホスト名を IP アドレスにマッピングする A レコードおよびパブリック ドメインをアプライアンスのホスト名にマッピングする MX レコードを作成します。ドメインのプライマリ MTA またはバックアップ MTA のいずれかとして Cisco アプライアンスをアドバタイズするように MX レコードのプライオリティを指定する必要があります。

次の例では、MX レコードに大きいプライオリティ値 (20) が指定されているため、Cisco アプライアンス (IronPort.example.com) は、ドメイン example.com のバックアップ MTA です。言い換えると、数値が大きいほど、MTA のプライオリティは低くなります。

```
$ host -t mx example.com

example.com mail is handled (pri=10) by mail.example.com

example.com mail is handled (pri=20) by ironport.example.com
```

Cisco アプライアンスを DNS に登録するという事は、MX レコードのプライオリティに設定する値に関係なく、スパム攻撃にさらされることを意味します。ただし、ウイルス攻撃でバックアップ MTA がターゲットになることはまれです。したがって、アンチウイルス エンジンの性能を徹底的に評価するには、Cisco アプライアンスの MX レコードのプライオリティに、他の MTA のプライオリティ以上の値を設定します。

インストール シナリオ

Cisco アプライアンスを既存のネットワーク インフラストラクチャに設置する方法は複数あります。大部分のお客様のネットワーク コンフィギュレーションは、以降のシナリオで表現されています。ネットワーク コンフィギュレーションが多少異なっており、設置計画の支援を必要とする場合は、Cisco カスタマー サポートにお問い合わせください（「[シスコのテクニカル サポート](#)」(P.1-7) を参照）。

設定の概要

次の図は、エンタープライズ ネットワーク 環境における Cisco アプライアンスの一般的な設置方法を示します。



いくつかのシナリオでは、Cisco アプライアンスはネットワークの DMZ 内に配置されます。その場合は、Cisco アプライアンスとグループウェア サーバの間にさらにファイアウォールを設置しています。

次のネットワーク シナリオを説明します。

- ファイアウォールの内側：リスナー 2 個の設定（[図 3-1 \(P.3-6\)](#)）

実際のインフラストラクチャと最も一致する設定を選択してください。その後、「[システム セットアップの準備](#)」(P.3-7) に進んでください。

着信

- 指定したローカル ドメイン宛ての着信メールは受け入れられます
- その他のドメインはすべて拒否されます。
- 外部システムは、ローカル ドメイン宛て電子メールを転送するために Cisco アプライアンスに直接接続し、Cisco アプライアンスは、SMTP ルートを介して、そのメールを適切なグループウェア サーバ (Exchange™、Groupwise™、Domino™ など) にリレーします（「[ローカル ドメインの電子メールのルーティング](#)」(P.21-1) を参照）。

発信

- 内部ユーザが送信した発信メールは、グループウェア サーバによって Cisco アプライアンスにルーティングされます。
- Cisco アプライアンスでは、プライベート リスナーのホスト アクセス テーブルの設定値に基づいてアウトバウンド電子メールを受け入れます（詳細については、「[リスナーの使用](#)」(P.5-2) を参照してください）。

イーサネット インターフェイス

これらの設定では、Cisco アプライアンスにある使用可能なイーサネット インターフェイスのうち 1 つだけを必要とします。ただし、イーサネット インターフェイスを 2 つ設定すると、内部ネットワークを外部インターネット ネットワーク接続と分離できます。

使用可能なインターフェイスに対する複数 IP アドレスの割り当ての詳細については、「[Virtual Gateway™ テクノロジー](#)を使用してすべてのホストされたドメインでの構成のメール ゲートウェイ (P.21-59) および付録 B 「ネットワーク アドレスと IP アドレスの割り当て」を参照してください。



(注)

Cisco X1060/1070、C660/670、および C360/370 電子メール セキュリティ アプライアンスには、デフォルトで、使用可能なイーサネット インターフェイスが 3 つあります。Cisco C160/170 電子メール セキュリティ アプライアンスには、使用可能なイーサネット インターフェイスが 2 つあります。

拡張設定

図 3-1 および図 3-2 に示す設定に加え、次の設定も可能です。

- 中央集中管理機能を使用する複数 Cisco アプライアンス。第 35 章「[クラスタを使用した中央集中型管理](#)」を参照してください。
- Cisco アプライアンスの 2 つのイーサネット インターフェイスを NIC ペ어링機能によって「チーム化」することによるネットワーク インターフェイス カード レベルでの冗長性 第 33 章「[高度なネットワーク構成](#)」を参照してください。

ファイアウォール設定値 (NAT、ポート)

SMTP サービスおよび DNS サービスでは、インターネットにアクセスする必要があります。他のサービスも場合によってはファイアウォール ポートを開く必要があります。詳細については、[付録 D 「ファイアウォール情報」](#)を参照してください。

Cisco アプライアンスのネットワークへの物理接続

設定シナリオ

Cisco アプライアンスの一般的な設定シナリオは次のとおりです。

- **イーサネット インターフェイス**：大部分のネットワーク環境では、Cisco アプライアンスにある使用可能な 3 つのイーサネット インターフェイスのうち 1 つだけを必要とします。ただし、イーサネット インターフェイスを 2 つ設定すると、内部ネットワークを外部インターネット ネットワーク接続と分離できます。
- **パブリック リスナー (着信電子メール)**：パブリック リスナーでは、多数の外部ホストからの接続を受け入れ、一定の数の内部グループウェア サーバにメッセージを振り向けます。
 - ホスト アクセス テーブル (HAT) の設定値に基づいて外部メール ホストからの接続を受け入れます。HAT は、デフォルトでは、すべての外部メール ホストからの接続を受け入れるように設定されています。
 - 受信者アクセス テーブル (RAT) で指定されているローカル ドメイン宛ての着信メールに限って受け入れます。その他のドメインはすべて拒否されます。

- SMTP ルートの定義に従って、適切な内部グループウェア サーバにメールをリレーします。
- **プライベート リスナー (発信電子メール)** : プライベート リスナーは、一定の数の内部グループウェア サーバからの接続を受け入れ、多数の外部メール ホストにメッセージを振り向けます。
 - 内部グループウェア サーバは、Cisco C-Series または X-Series アプライアンスに発信メールをルーティングするように設定されます。
 - Cisco アプライアンスは、HAT の設定値に基づいて、内部グループウェア サーバからの接続を受け入れます。HAT は、デフォルトでは、すべての内部メール ホストからの接続を受け入れるように設定されています。

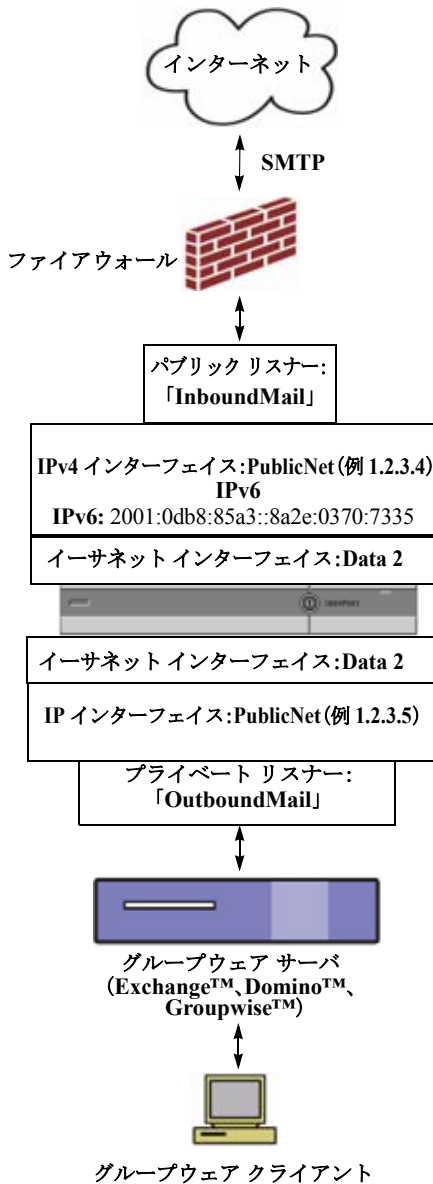
着信メールと発信メールの分離

着信と発信の電子メール トラフィックを個別のリスナーおよび個別の IP アドレスで分離できます。インターネット プロトコル バージョン 4 (IPv4) およびバージョン 6 (IPv6) アドレスを使用できます。ただし、アプライアンスのシステム セットアップ ウィザードでは、次の設定を持つ初期設定をサポートしています。

- **個別の物理インターフェイスに設定された 2 個の論理 IPv4 アドレスおよび 2 個の IPv6 アドレス上の 2 つの個別リスナー**
 - 着信と発信のトラフィックの分離
 - IPv4 アドレスおよび IPv6 アドレスを各リスナーに割り当てることができます。
- **1 つの物理インターフェイスに設定された 1 つの論理 IPv4 アドレス上の 1 つのリスナー**
 - 着信と発信の両トラフィックの組み合わせ
 - IPv4 アドレスおよび IPv6 アドレスの両方ともリスナーに割り当てることができます。

リスナー 1 つと 2 つの両方の設定に対するコンフィギュレーション ワークシートが以下にあります (「[セットアップ情報の収集](#)」(P.3-10) を参照)。大部分の設定シナリオは、次の 3 つの図のいずれかで表現されます。

図 3-1 ファイアウォールの内側のシナリオ：リスナー 2 個の設定



注：

- リスナー x 2
- IPv4 アドレス x 2
- IPv6 アドレス x 2
- イーサネット インターフェイス x 1 または 2 (表示されるインターフェイスは 1 個のみ)
- 設定済みの SMTP ルート

インバウンド リスナー：「InboundMail」（パブリック）

- IPv4 アドレス：1.2.3.4
- IPv6 アドレス：
2001:0db8:85a3::8a2e:0370:7334
- Data 2 インターフェイスのリスナーでポート 25 をリッスン
- HAT（すべてを受け入れ）
- RAT（ローカル ドメイン宛てメールを受け入れ、その他すべてを拒否）

アウトバウンド リスナー：「OutboundMail」（プライベート）

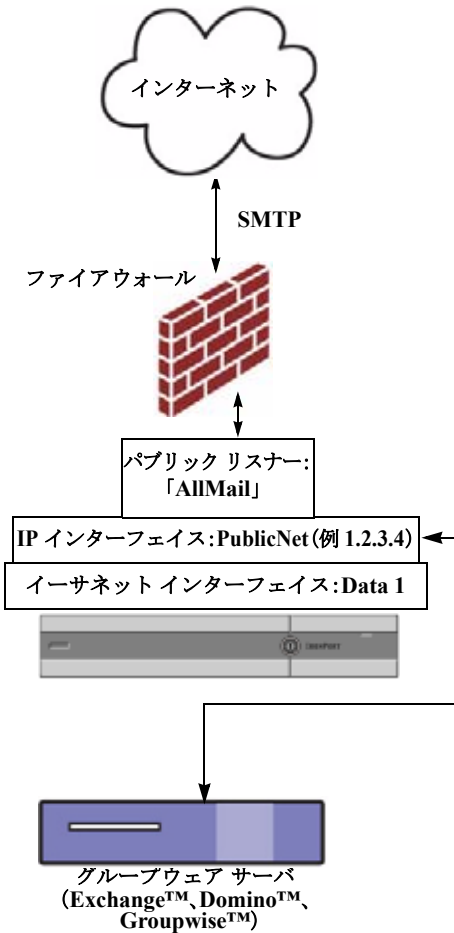
- IP アドレス：1.2.3.5
- IPv6 アドレス：
2001:0db8:85a3::8a2e:0370:7335
- Data 2 インターフェイスのリスナーでポート 25 をリッスン
- HAT（ローカル ドメイン宛てをリレー、その他すべてを拒否）

インターネット ルート サーバまたは内部 DNS サーバを使用するように DNS を設定可能

SMTP ルートでは、適切なグループウェア サーバにメールを振り向け

適切なサービスと Cisco アプライアンスの双方向の通信用にファイアウォール ポートをオープン

図 3-2 リスナー 1 個の設定



注:

- リスナー x 1
- IP アドレス x 1
- イーサネット インターフェイス x 1
- 設定済みの SMTP ルート

インバウンド リスナー: 「InboundMail」 (パブリック)

- IP アドレス: 1.2.3.4
- Data 2 インターフェイスのリスナーでポート 25 をリッスン
- HAT (すべてを受け入れ) では、RELAYLIST にあるグループウェア サーバ用のエントリが組み込まれます。
- RAT (ローカル ドメイン宛てメールを受け入れ、その他すべてを拒否)

インターネット ルート サーバまたは内部 DNS サーバを使用するように DNS を設定可能

SMTP ルートでは、適切なグループウェア サーバにメールを振り向け

適切なサービスと Cisco アプライアンスの双方向の通信用にファイアウォール ポートをオープン

システム セットアップの準備

	操作内容	追加情報
ステップ1	アプライアンスへの接続方法を決定します。	「アプライアンスへの接続方式の決定」(P.3-8) を参照してください。
ステップ2	ネットワーク アドレスと IP アドレスの割り当てを決定します。 すでにアプライアンスをネットワークに配線済みの場合は、Cisco アプライアンスのデフォルト IP アドレスが、ネットワーク上の他の IP アドレスと競合していないことを確認します。	「ネットワーク アドレスと IP アドレスの割り当ての決定」(P.3-9)
ステップ3	システム セットアップに関する情報を収集します。	「セットアップ情報の収集」(P.3-10) を参照してください。

	操作内容	追加情報
ステップ4	アプライアンスの最新の製品リリースノートを確認してください。	「 マニュアル 」(P.1-6) のリンクから、リリース ノートを手に入れます。
ステップ5	アプライアンスを開梱し、物理的にラックに設置し、オンにします。	アプライアンスについては、『 クイックスタート ガイド 』を参照してください。このガイドは、「 マニュアル 」(P.1-6) のリンクから入手できます。
ステップ6	Web ベース インターフェイスおよびコマンドライン インターフェイス (CLI) を使用してアプライアンスにアクセスします。	<ul style="list-style-type: none"> Web ブラウザを起動し、アプライアンスの IP アドレスを入力します または 「コマンドライン インターフェイス (CLI) システム セットアップ ウィザードの実行」(P.3-23) を参照してください。
ステップ7	仮想電子メール セキュリティ アプライアンスをセットアップする場合は、お使いの仮想アプライアンスのライセンスをロードしてください。	loadlicense コマンドを使用します。詳細については、「 マニュアル 」(P.1-6) のリンクから利用できる『 Cisco Virtual Security Appliance Installation Guide 』を参照してください。
ステップ8	システムの基本設定を行います。	「 システム セットアップ ウィザードの使用法 」(P.3-12) を参照してください。

アプライアンスへの接続方式の決定

Cisco アプライアンスを環境に正常にセットアップするには、Cisco アプライアンスをネットワークに接続する方法に関する重要なネットワーク情報をネットワーク管理者から収集する必要があります。

アプライアンスへの接続

初期セットアップ時に、次の 2 つのいずれかの方式で、アプライアンスに接続できます。

表 3-1 アプライアンスに接続するオプション

イーサネット	PC とネットワークの間およびネットワークと Cisco 管理ポートの間のイーサネット接続です。工場出荷時に Management ポートに割り当てられている IPv4 アドレスは 192.168.42.42 です。ご使用のネットワーク コンフィギュレーションで使用可能であれば、この方法による接続が手軽です。
シリアル	シリアル通信によって PC と Cisco シリアル コンソール ポートが接続されます。イーサネット方式を使用できない場合は、コンピュータとアプライアンスをシリアル同士でストレート接続すると、代替ネットワーク設定値を Management ポートに適用できるまでの代用になります。ピン割り当については、「 シリアル接続による電子メール セキュリティ アプライアンスへのアクセス 」(P.A-5) を参照してください。シリアル ポートの通信設定値は次のとおりです。 Bits per second : 9600 データ ビット : 8 パリティ : なし ストップビット : 1 フロー制御 : ハードウェア



(注)

初期接続方式は、最終的な方式でないことに留意してください。このプロセスは、初期設定だけに適用されます。ネットワーク設定値を後で変更して、別の接続方式を使用できます（詳細については、[付録 A 「アプライアンスへのアクセス」](#)を参照してください）。アプライアンスを利用するための管理者権限が異なる、複数のユーザ アカウントを作成することもできます（詳細については、「[ユーザの追加](#)」(P.28-4)を参照してください）。

ネットワーク アドレスと IP アドレスの割り当ての決定

IPv4 アドレスと IPv6 アドレスの両方を使用できます。

管理およびデータ ポート用のデフォルト IP アドレス

(Cisco X1060/1070、C660/670、および C360/370 アプライアンスの) 管理ポートまたは (Cisco C160/170 アプライアンスの) データ 1 ポートで事前に設定される IP アドレスは、192.168.42.42 です。

電子メールを受信および配信するネットワーク接続の選択

大部分のユーザは、Cisco アプライアンスから 2 つのネットワークに接続することによって、アプライアンス上の 2 つの Data イーサネット ポートを利用します。

- プライベート ネットワークでは、内部システム宛てのメッセージを受け入れて配信します。
- パブリック ネットワークでは、インターネット宛てのメッセージを受け入れて配信します。

1 つの Data ポートだけを両方の機能に使用するユーザもいます。Management イーサネット ポートでは任意の機能をサポートできますが、グラフィカル ユーザ インターフェイスとコマンドライン インターフェイスを利用するために事前設定されています。

物理イーサネット ポートへの論理 IP アドレスのバインド

着信と発信の電子メール トラフィックを個別のリスナーおよび個別の IP アドレスで分離できます。インターネット プロトコル バージョン 4 (IPv4) およびバージョン 6 (IPv6) アドレスを使用できます。ただし、アプライアンスのシステム セットアップ ウィザードでは、次の設定を持つ初期設定をサポートしています。

- 個別の物理インターフェイスに設定された 2 個の論理 IPv4 アドレスおよび 2 個の IPv6 アドレス上の 2 つの個別リスナー
 - 着信と発信のトラフィックの分離
 - IPv4 アドレスおよび IPv6 アドレスを各リスナーに割り当てることができます。
- 1 つの物理インターフェイスに設定された 1 つの論理 IPv4 アドレス上の 1 つのリスナー
 - 着信と発信の両トラフィックの組み合わせ
 - IPv4 アドレスおよび IPv6 アドレスの両方ともリスナーに割り当てることができます。

電子メール セキュリティ アプライアンスは、1 つのリスナーで IPv4 アドレスと IPv6 アドレスの両方をサポートできます。リスナーは両方のアドレスでメール受け入れます。リスナーの設定はすべて、IPv4 と IPv6 両方のアドレスに適用されます。

接続用ネットワーク設定値の選択

使用することを選択した各イーサネット ポートに関する次のネットワーク情報が必要になります。

- IP アドレス (IPv4 または IPv6、あるいはその両方)
- CIDR 形式の IPv4 アドレスのネットマスク
- CIDR 形式の IPv6 アドレスのプレフィックス

さらに、ネットワーク全体に関する次の情報も必要になります。

- ネットワークのデフォルト ルータ (ゲートウェイ) の IP アドレス
- DNS サーバの IP アドレスおよびホスト名 (インターネット ルート サーバを使用する場合は不要)
- NTP サーバのホスト名または IP アドレス (Cisco のタイム サーバを使用する場合は不要)

詳細については、[付録 B「ネットワーク アドレスと IP アドレスの割り当て」](#)を参照してください。



(注)

インターネットと Cisco アプライアンスの間でファイアウォールを稼働しているネットワークの場合には、Cisco アプライアンスを正常に機能させるために、特定のポートを開ける必要がある場合があります。詳細については、[付録 D「ファイアウォール情報」](#)を参照してください。

セットアップ情報の収集

これで、システム セットアップ ウィザードで必要な内容を選択するための要件および戦略が判明したため、この項を参照しながら次の表を使用して、システムのセットアップに関する情報を収集してください。

ネットワークおよび IP アドレスの詳細については、[付録 B「ネットワーク アドレスと IP アドレスの割り当て」](#)を参照してください。Cisco M-Series アプライアンスを設定する場合は、[第 38 章「Cisco コンテンツ セキュリティ管理アプライアンスの集中型サービス」](#)を参照してください。

表 3-2 システム セットアップ ワークシート：2 個のリスナーによる電子メール トラフィックの分離

システム設定 (System Settings)	
デフォルトのシステム ホスト名 : (Default System Hostname:)	
システム アラート メール の送信先 : (Email System Alerts To:)	
定期レポートの送信先 : (Deliver Scheduled Reports To:)	
タイムゾーン情報 (Time Zone Information:)	
NTP サーバ : (NTP Server:)	
管理者パスワード : (Admin Password:)	
SenderBase ネットワークに参加 : (SenderBase Network Participation:)	イネーブル/ディセーブル
オートサポート : (AutoSupport:)	イネーブル/ディセーブル
ネットワーク インテグレーション (Network Integration)	
ゲートウェイ : (Gateway:)	
DNS: (インターネットまたは独自指定)	
インターフェイス (Interfaces)	
データ 1 ポート (Data 1 Port)	

表 3-2 システム セットアップ ワークシート : 2 個のリスナーによる電子メール トラフィックの分離

IPv4 アドレス/ネットマスク : (IPv4 Address / Netmask:)		
IPv6 アドレス/プレフィックス : (IPv6 Address / Prefix:)		
完全なホスト名 : (Fully Qualified Hostname:)		
受信メールの受け入れ : (Accept Incoming Mail:)	ドメイン (Domain)	宛先 (Destination)
外部への送信メールを中継 : (Relay Outgoing Mail:)	システム (System)	
データ 2 ポート (Data 2 Port)		
IPv4 アドレス/ネットマスク : (IPv4 Address / Netmask:)		
IPv6 アドレス/プレフィックス : (IPv6 Address / Prefix:)		
完全なホスト名 : (Fully Qualified Hostname:)		
受信メールの受け入れ : (Accept Incoming Mail:)	ドメイン (Domain)	宛先 (Destination)
外部への送信メールを中継 : (Relay Outgoing Mail:)	システム (System)	
管理ポート (Management Port)		
IP アドレス : (IP Address:)		
ネットワーク マスク : (Network Mask:)		
IPv6 アドレス : (IPv6 Address:)		
プレフィックス : (Prefix:)		
完全なホスト名 : (Fully Qualified Hostname:)		
受信メールの受け入れ : (Accept Incoming Mail:)	ドメイン (Domain)	宛先 (Destination)
外部への送信メールを中継 : (Relay Outgoing Mail:)	システム (System)	
メッセージ セキュリティ (Message Security)		
SenderBase レピュテーション フィルタ : (SenderBase Reputation Filtering:)	イネーブル/ディセーブル	
Anti-Spam Scanning Engine	なし /IronPort	
McAfee Anti-Virus Scanning Engine	イネーブル/ディセーブル	
Sophos Anti-Virus Scanning Engine	イネーブル/ディセーブル	
アウトブレイク フィルタ (Outbreak Filters)	イネーブル/ディセーブル	

表 3-3 システム セットアップ ワークシート : 1 個のリスナーをすべての電子メール トラフィックに使用

システム設定 (System Settings)	
デフォルトのシステム ホスト名 : (Default System Hostname:)	
システム アラート メール の送信先 : (Email System Alerts To:)	
定期レポートの送信先 : (Deliver Scheduled Reports To:)	
タイムゾーン : (Time Zone:)	
NTP サーバ : (NTP Server:)	

表 3-3 システム セットアップ ワークシート: 1 個のリスナーをすべての電子メール トラフィックに使用 (続き)

管理者パスワード : (Admin Password:)		
SenderBase ネットワークに参加 : (SenderBase Network Participation:)	イネーブル/ディセーブル	
オートサポート : (AutoSupport:)	イネーブル/ディセーブル	
ネットワーク インテグレーション (Network Integration)		
ゲートウェイ : (Gateway:)		
DNS: (インターネットまたは独自指定)		
インターフェイス (Interfaces)		
データ 2 ポート (Data 2 Port)		
IPv4 アドレス/ネットマスク : (IPv4 Address / Netmask:)		
IPv6 アドレス/プレフィックス : (IPv6 Address / Prefix:)		
完全なホスト名 : (Fully Qualified Hostname:)		
受信メールの受け入れ : (Accept Incoming Mail:)	ドメイン (Domain)	宛先 (Destination)
外部への送信メールを中継 : (Relay Outgoing Mail:)	システム (System)	
データ 1 ポート (Data 1 Port)		
IPv4 アドレス/ネットマスク : (IPv4 Address / Netmask:)		
IPv6 アドレス/プレフィックス : (IPv6 Address / Prefix:)		
完全なホスト名 : (Fully Qualified Hostname:)		
メッセージ セキュリティ (Message Security)		
SenderBase レピュテーション フィルタ : (SenderBase Reputation Filtering:)	イネーブル/ディセーブル	
Anti-Spam Scanning Engine	なし /IronPort	
McAfee Anti-Virus Scanning Engine	イネーブル/ディセーブル	
Sophos Anti-Virus Scanning Engine	イネーブル/ディセーブル	
アウトブレイク フィルタ (Outbreak Filters)	イネーブル/ディセーブル	

システム セットアップ ウィザードの使用法

初期セットアップではシステム セットアップ ウィザードを使用して、設定に漏れがないようにする必要があります。後で、システム セットアップ ウィザードで利用できないカスタム オプションを設定できます。

ブラウザまたはコマンドライン インターフェイス (CLI) を使用して、システム設定ウィザードを実行できます。詳細については、「[Web ベースのグラフィカル ユーザ インターフェイス \(GUI\) の利用 \(P.3-13\)](#)」または「[コマンドライン インターフェイス \(CLI\) システム セットアップ ウィザードの実行 \(P.3-23\)](#)」を参照してください。

開始する前に、「[システム セットアップの準備 \(P.3-7\)](#)」にある前提条件をクリアします。



警告

仮想電子メール セキュリティ アプライアンスをセットアップする場合は、システム セットアップ ウィザードを実行する前に、仮想アプライアンスのライセンスをロードするために `loadlicense` のコマンドを使用する必要があります。詳細については、『*Cisco Virtual Security Appliance Installation Guide*』を参照してください。



警告

システム セットアップ ウィザードでは、システムを完全に再設定します。システム セットアップ ウィザードは、アプライアンスをまったく初めて設置する場合か、既存の設定を上書きする場合に限り使用してください。



注意

Cisco アプライアンスは出荷時に、すべてのシステムの管理ポートがデフォルト IP アドレス 192.168.42.42 に設定されています。ただし、theData 1 ポートを代わりに使用する C160/C170 システムを除きます。Cisco アプライアンスをネットワークに接続する前に、他の装置の IP アドレスが、この工場出荷時のデフォルト設定と競合していないことを確認してください。Cisco M-Series アプライアンスを設定する場合は、「Cisco コンテンツ セキュリティ管理アプライアンスの集中型サービス」(P.38-1)を参照してください。

工場出荷時の設定を持つ Cisco アプライアンスをネットワークに複数接続する場合は、各 Cisco アプライアンスのデフォルト IP アドレスを順に再設定しながら、1 台ずつ追加してください。

Web ベースのグラフィカル ユーザ インターフェイス (GUI) の利用

Web ベースのグラフィカル ユーザ インターフェイス (GUI) を利用するには、Web ブラウザを開き、192.168.42.42 を表示します。

ログイン画面が表示されます。

図 3-3 アプライアンスへのログイン

Welcome



下記のユーザ名およびパスワードを入力してアプライアンスにログインします。

工場出荷時のデフォルト ユーザ名とパスワード

- ユーザ名 : `admin`
- パスワード : `ironport`



(注)

セッションがタイムアウトした場合は、ユーザ名とパスワードの再入力が必要です。システム セットアップ ウィザードの実行中にセッションがタイムアウトした場合は、最初からやり直す必要があります。

Web ベースのシステム セットアップ ウィザードを使用した基本設定の定義

手順

-
- ステップ 1** システム セットアップ ウィザードの起動
- 「Web ベースのグラフィカル ユーザ インターフェイス (GUI) の利用」(P.3-13) に記載されている方法で、グラフィカル ユーザ インターフェイスにログインします。
 - 新規のシステム (先行リリースの AsyncOS からのアップグレードなし) の場合は、ブラウザがシステム セットアップ ウィザードに自動的にリダイレクトされます。
 - それ以外の場合は、[システム管理 (System Administration)] タブで、左方のリンク リストから [システム セットアップ ウィザード (System Setup Wizard)] をクリックします。
- ステップ 2** 開始
- ライセンス契約書の参照と受諾
- ステップ 3** システム
- アプライアンスのホスト名の設定
 - アラート設定値、レポート配信設定値、および AutoSupport の設定
 - システム時刻設定値および NTP サーバの設定
 - admin パスワードのリセット
 - SenderBase Network Participation のイネーブル化
- ステップ 4** ネットワーク
- デフォルト ルータおよび DNS 設定値の定義
 - 次のようなネットワーク インターフェイスのイネーブル化および設定
 - 着信メールの設定 (インバウンド リスナー)
 - SMTP ルートの定義 (任意)
 - 発信メール (アウトバウンド リスナー) の設定およびアプライアンスを介してメールをリレーできるシステムの定義 (任意)
- ステップ 5** セキュリティ
- SenderBase レピュテーション フィルタリングのイネーブル化
 - アンチスパム サービスのイネーブル化
 - Cisco スпам隔離のイネーブル化
 - Anti-Virus サービスのイネーブル化
 - アウトブレイク フィルタサービスのイネーブル化
- ステップ 6** レビュー
- セットアップのレビューおよび設定のインストール
 - 手順の最後に表示されるプロンプト
- ステップ 7** 変更点の確定
- 確定するまで、変更は有効になりません。
-

手順 1 : 開始

ライセンス契約書の参照から開始します。ライセンス契約書を参照し、同意する場合は、同意することを示すボックスをオンにし、[セットアップの開始 (Begin Setup)] をクリックして続行します。

契約書の文面は次の場所でも参照できます。

<https://support.ironport.com/license/eula.html>

手順 2 : システム

ホスト名の設定

Cisco アプライアンスの完全修飾ホスト名を定義します。この名前は、ネットワーク管理者が割り当てる必要があります。

システム アラートの設定

ユーザの介入を必要とするシステム エラーが発生した場合、Cisco AsyncOS では、電子メールでアラート メッセージを送信します。このアラートの送信先として使用する電子メール アドレス (複数可) を入力します。

システム アラートを受信する電子メール アドレスを 1 つ以上追加する必要があります。単一の電子メール アドレスか、カンマで区切った複数アドレスを入力します。当初、この電子メール受信者は、ディレクトリ獲得攻撃対策アラート以外のすべてのタイプおよびすべてのレベルのアラートを受信します。後で、アラート コンフィギュレーションをさらに詳細化できます。詳細については、「アラート」(P.29-30) を参照してください。

レポート配信の設定

デフォルトのスケジュール済みレポートの送信先にするアドレスを入力します。この値を空白にしても、スケジュール済みレポートは引き続き実行されます。スケジュール済みレポートは配信されませんが、アプライアンス上にアーカイブされます。

時間の設定

Cisco アプライアンス上の時間帯を設定して、メッセージ ヘッダーおよびログ ファイルのタイムスタンプが正確になるようにします。ドロップダウン メニューを使用して時間帯を見つけるか、GMT オフセットによって時間帯を定義します (詳細については、「GMT オフセットの選択」(P.29-58) を参照してください)。

システム クロック時刻は、後で手動によって設定するか、Network Time Protocol (NTP; ネットワーク タイム プロトコル) を使用してネットワーク上またはインターネット上の他のサーバと時刻を同期することもできます。デフォルトでは、Cisco Systems のタイム サーバ (time.IronPort.com) と時刻を同期するエントリ 1 つが、Cisco アプライアンスにすでに設定されています。

パスワードの設定

admin アカウントのパスワードを設定します。この手順は必須です。Cisco AsyncOS の admin アカウントのパスワードを変更する場合、新しいパスワードは、6 文字以上でなければなりません。パスワードは、必ず安全な場所に保管してください。

SenderBase ネットワークへの参加

SenderBase は、電子メール管理者による送信者の調査、電子メールの正規送信元の識別、およびスパム送信者のブロックに役立つように設計された、電子メールのレピュテーション サービスです。

SenderBase ネットワークへの参加に同意した場合、シスコは、組織の電子メール トラフィックを集約した統計情報を収集します。これには、メッセージ属性の要約データおよび Cisco アプライアンスがどのように各種メッセージを処理したかに関する情報のみが含まれています。たとえば、シスコは、メッセージの本文もメッセージの件名も収集しません。個人を特定できる情報や、組織を特定する情報は、機密情報として扱われます。収集されるデータの例など、SenderBase の詳細については、[共有対象データの詳細については、[ここをクリック \(Click here for more information about what data is being shared\)](#)] リンクをクリックしてください（「よくあるご質問」(P.31-2) を参照）。

SenderBase ネットワークに参加する場合は、[メールをベースとする脅威の特定、排除を目的として、IronPort がメールの匿名統計を収集および SenderBase に対しレポートすることを許可 (Allow IronPort to gather anonymous statistics on email and report them to SenderBase in order to identify and stop email-based threats)] の横のボックスをオンにし、[承認 (Accept)] をクリックします。

詳細については、第 31 章「[SenderBase Network Participation](#)」を参照してください。

AutoSupport のイネーブル化

CiscoAutoSupport 機能（デフォルトでイネーブル）では、ご使用の Cisco アプライアンスに関する問題を Cisco カスタマー サポート チームが認識しておくことで、適切なサポートを提供できるようにします。（詳細については、「[Cisco AutoSupport](#)」(P.29-32) を参照してください）。

[次へ (Next)] をクリックして続行します。

手順 3 : ネットワーク

手順 3 では、デフォルト ルータ（ゲートウェイ）を定義し、DNS 設定値を設定してから、Data 1 インターフェイス、Data 2 インターフェイス、および Management インターフェイスを設定することにより、電子メールの受信やリレーを行うようにアプライアンスをセットアップします。

DNS とデフォルト ゲートウェイの設定

ネットワーク上のデフォルト ルータ（ゲートウェイ）の IP アドレスを入力します。IPv4 アドレス、IPv6 アドレス、またはその両方を使用できます。

次に、Domain Name Service (DNS) 設定値を設定します。Cisco AsyncOS には、インターネットのルート サーバに直接問い合わせできる、高性能な内部 DNS リゾルバ/キャッシュが組み込まれていますが、指定した DNS サーバを使用することもできます。独自のサーバを使用する場合は、各 DNS サーバの IP アドレスおよびホスト名を指定する必要があります。システム セットアップ ウィザードから入力できる DNS サーバは 4 台までです。入力した DNS サーバの初期プライオリティは 0 になっていることに注意してください。詳細については、「[ドメイン ネーム システム \(DNS\) 設定値の設定](#)」(P.29-53) を参照してください。



(注)

アプライアンスでは、着信接続のための DNS ルックアップを実行するために、稼働中の DNS サーバを利用する必要があります。アプライアンスをセットアップするときにアプライアンスからアクセス可能な稼働中の DNS サーバを指定できない場合は、[インターネット ルート DNS サーバを使用 (Use Internet Root DNS Server)] を選択するか、Management インターフェイスの IP アドレスを一時的に指定することを回避策として、システム セットアップ ウィザードを完了できます。

ネットワーク インターフェイスの設定

Cisco アプライアンスには、マシンの物理ポートに関連付けられたネットワーク インターフェイスがあります。たとえば、C660/670、C360/370、および X1060/1070 アプライアンスでは、3 個の物理イーサネット インターフェイスが使用可能です。C160/170 アプライアンスでは、2 個の物理イーサネット インターフェイスが使用可能です。

インターフェイスを使用するには、[有効 (Enable)] チェックボックスをオンにし、IP アドレス、ネットワーク マスク、および完全修飾ホスト名を指定します。入力する IP アドレスは、DNS レコードに反映されている、インバウンド メール用のアドレスである必要があります。通常、このアドレスには、DNS で MX レコードと関連付けられています。IPv4 アドレス、IPv6 アドレス、またはその両方を使用できます。両方使用すると、インターフェイスは両方のタイプの接続を受け入れます。

各インターフェイスは、メールを受け入れる (着信)、電子メールをリレーする (発信)、またはアプライアンスを管理するように設定できます。セットアップ時は、このいずれかに制限されます。通常は、インターフェイスの 1 つを着信用、1 つを発信用、および 1 つをアプライアンス管理用に使用します。C160/170 アプライアンスでは、1 つのインターフェイスを着信と発信の両方のメール用に使用し、もう 1 つのインターフェイスを管理用に使用することが一般的です。

インターフェイスの 1 つは、電子メールの受信用に設定する必要があります。

アプライアンスのいずれかの物理イーサネット インターフェイスに論理 IP アドレスを割り当てて、設定します。Data 1 イーサネット ポートと Data 2 イーサネット ポートの両方を使用する場合は、両方の接続に対してこの情報が必要です。

C660/670、C360/370、および X1060/1070 をご利用のお客様：Cisco では、パブリック リスナーを介してインバウンド電子メールを受信するためにインターネットに直接接続するように物理イーサネット ポートの 1 つを使用し、プライベート リスナーを介してアウトバウンド電子メールをリレーするために内部ネットワークに直接接続するようもう 1 つの物理イーサネット ポートを使用することを推奨しています。

C160/170 をご利用のお客様：通常は、インバウンド電子メールの受信とアウトバウンド電子メールのリレーの両方のために、リスナー 1 つの物理イーサネット ポート 1 つだけが、システム セットアップ ウィザードによって設定されます。

「物理イーサネット ポートへの論理 IP アドレスのバインド」(P.3-9) を参照してください。

次の情報が必要です。

- ネットワーク管理者によって割り当てられた **IP アドレス**。IPv4 アドレス、IPv6 アドレス、またはその両方を使用できます。
- IPv4 アドレスの場合：インターフェイスの**ネットマスク**。AsyncOS は、CIDR 形式の netmask だけを受け入れます。たとえば、255.255.255.0 サブネットの /24 など。
IPv6 アドレスの場合：CIDR 形式の**プレフィックス**。64 ビット プレフィックスの /64 など。
- (任意) IP アドレスの完全修飾ホスト名。



(注)

同じサブネットに含まれる IP アドレスを、別々の物理イーサネット インターフェイスには設定できません。ネットワークおよび IP アドレスのコンフィギュレーションの詳細については、付録 B「ネットワーク アドレスと IP アドレスの割り当て」を参照してください。

メールの受け入れ

メールを受け入れるようにインターフェイスを設定する場合は、次の内容を定義します。

- 受け入れるメールの宛先のドメイン
- 各ドメインの宛先 (SMTP ルート) (任意)

[受信メールの受け入れ (Accept Incoming Mail)] のチェックボックスをオンにし、メールを受け入れるインターフェイスを設定します。受け入れるメールのドメインの名前を入力します。

[宛先 (Destination)] を入力します。これは、SMTP ルートまたは指定したドメイン宛ての電子メールをルーティングするマシンの名前です。

これは、最初の SMTP ルート エントリです。SMTP ルート テーブルを使用すると、入力する各ドメイン宛てのすべての電子メール (受信者アクセス テーブル (RAT) エントリとも呼ぶ) を特定の Mail Exchange (MX) ホストにリダイレクトできます。標準インストールの場合、SMTP ルート テーブルでは、特定のグループウェア サーバ (たとえば、Microsoft Exchange) やインフラストラクチャの電子メール配信における次のホップを定義します。

たとえば、ドメイン example.com かそのすべてのサブドメイン .example.com のいずれか宛てメールを受け入れた場合に、グループウェア サーバ exchange.example.com にルーティングするよう指定するルートを定義できます。

ドメインおよび宛先は、複数入力できます。ドメインをさらに追加するには、[行を追加 (Add Row)] をクリックします。行を削除するには、ゴミ箱アイコンをクリックします。



(注)

この手順での SMTP ルートの設定は任意です。SMTP ルートを定義していない場合は、リスナーが受信した着信メールの配信ホストの検索と決定に、DNS が使用されます (「ローカル ドメインの電子メールのルーティング」(P.21-1) を参照)。

ドメインを受信者アクセス テーブルに少なくとも 1 つ追加する必要があります。ドメイン、たとえば、example.com を入力します。example.net のいずれかのサブドメイン宛てのメールとも必ず一致させるために、ドメイン名の他に .example.net も受信者アクセス テーブルに入力します。詳細については、「受信者アドレスの定義」(P.8-4) を参照してください。

メール リレー (任意)

メールをリレーするようにインターフェイスを設定するときは、アプライアンスを介して電子メールのリレーを許可するよう、システムを定義します。

リスナーのホストアクセス テーブルにある RELAYLIST 内のエントリを使用します。詳細については、「送信者グループの構文」(P.7-4) を参照してください。

[外部への送信メールを中継 (Relay Outgoing Mail)] のチェックボックスをオンにし、メールをリレーするインターフェイスを設定します。アプライアンスを介してメールをリレーできるホストを入力します。

アウトバウンド メールをリレーするようにインターフェイスを設定すると、そのインターフェイスを使用するパブリック リスナーが設定されている場合を除き、そのインターフェイスの SSH がシステム セットアップ ウィザードによってオンにされます。

次の例では、IPv4 アドレスの 2 個のインターフェイスが作成されます。

- 192.168.42.42 は、引き続き Management インターフェイスに設定されます。
- 192.168.1.1 は、Data 1 イーサネット インターフェイスでイネーブルになります。example.com で終わるドメイン宛てのメールを受け入れるように設定されており、exchange.example.com 宛ての SMTP ルートが定義されています。
- 192.168.2.1 は、Data 2 イーサネット インターフェイスでイネーブルになります。exchange.example.com からのメールをリレーするように設定されます。



(注)

次の例は、X1060/1070、C660/670、および C360/370 アプライアンスに該当します。C160/170 アプライアンスの場合は、着信と発信の両方のメール用に Data 2 インターフェイスを設定し、アプライアンス管理用に Data 1 インターフェイスを設定することが一般的です（「C160/170 の設置」(P.3-19) を参照）。

図 3-4 ネットワーク インターフェイス : Management および追加のインターフェイス x 2 (トラフィックの分離)

<input checked="" type="checkbox"/> Enable Data 1 Interface	
<i>This interface is typically configured to accept mail.</i>	
IPv4 Address / Netmask:	1.1.1.1/24
IPv6 Address / Prefix:	2001:db8:1::4/64
Fully Qualified Hostname:	<input type="text"/>
<i>Fully qualified hostname for this appliance</i>	
Accept Incoming Mail:	<input type="checkbox"/> Accept mail on this interface
Relay Outgoing Mail:	<input type="checkbox"/> Relay mail on this interface
<input checked="" type="checkbox"/> Enable Data 2 Interface	
<i>This interface is typically configured to relay mail.</i>	
IPv4 Address / Netmask:	1.1.1.2/24
IPv6 Address / Prefix:	2001:db8:1::4/64
Fully Qualified Hostname:	<input type="text"/>
<i>Fully qualified hostname for this appliance</i>	
Accept Incoming Mail:	<input type="checkbox"/> Accept mail on this interface
Relay Outgoing Mail:	<input type="checkbox"/> Relay mail on this interface
<input checked="" type="checkbox"/> Enable Management Interface	
<i>This interface is typically configured for system administration.</i>	
IPv4 Address / Netmask:	1.1.1.2/24
IPv6 Address / Prefix:	2001:db8:1::4/64
Fully Qualified Hostname:	mail.example.com
<i>Fully qualified hostname for this appliance</i>	
Accept Incoming Mail:	<input type="checkbox"/> Accept mail on this interface
Relay Outgoing Mail:	<input type="checkbox"/> Relay mail on this interface

C160/170 の設置

すべての電子メール トラフィック用に単一の IP アドレスを設定する場合（トラフィックの分離なし）、システム セットアップ ウィザードの手順 3 は次のようになります。

図 3-5 ネットワーク インターフェイス : 着信と発信の (分離されない) トラフィック用に 1 つの IP アドレス

The screenshot shows the 'Interfaces' configuration screen. At the top, there is a diagram of a network interface card with two ports labeled 'Data 2' and 'Data 1'. Below this, the configuration is divided into two sections: 'Enable Data 2 Interface' and 'Enable Data 1 Interface'.

Enable Data 2 Interface:

- IP Address: 192.168.1.1
- Network Mask: 255.255.255.0
- Fully Qualified Hostname: mail.example.com
- Accept Incoming Mail: Accept mail on this interface

Domain	Destination
example.com	exchange.example.com
example: company.com	i.e. An Exchange or Notes server
- Relay Outgoing Mail: Relay mail on this interface

System
exchange.example.com
example: company.com

Enable Data 1 Interface:

- IP Address: 192.168.42.42
- Network Mask: 255.255.255.0
- Fully Qualified Hostname: mail.example.com
- Accept Incoming Mail: Accept mail on this interface
- Relay Outgoing Mail: Relay mail on this interface

[次へ (Next)] をクリックして続行します。

手順 4 : セキュリティ

手順 4 では、アンチスパム設定値およびアンチウイルス設定値を設定します。アンチスパム オプションには、SenderBase レピュテーション フィルタリングとアンチスパム スキャン エンジンの選択が含まれます。アンチウイルスについては、アウトブレイク フィルタおよび Sophos または McAfee のアンチウイルス スキャンをイネーブルにできます。

SenderBase レピュテーション フィルタリングのイネーブル化

SenderBase レピュテーション サービスは、スタンドアロンのアンチスパム ソリューションとしても使用できますが、Cisco Anti-Spam など、コンテンツ ベースのアンチスパム システムの有効性を高めることを主な目的としています。

SenderBase レピュテーション サービス (<http://www.SenderBase.org>) には、リモート ホストの接続 IP アドレスに基づいて、陽性と疑わしいスパムをユーザが拒否したり、制限したりするための正確で柔軟な方法が備わっています。SenderBase レピュテーション サービスは、特定の送信元からのメッセージがスパムである確率に基づく評点を返します。SenderBase レピュテーション サービスは、電子メール メッセージの量をグローバルに表示して、電子メールの送信元の識別とグループ化を容易にする方法でデータを編成している点で独特です。SenderBase レピュテーション フィルタリングをイネーブルにすることを強く推奨しています。

イネーブルにした SenderBase レピュテーション フィルタリングは、着信 (受け入れ) リスナーで適用されます。

アンチスパム スキャンのイネーブル化

Cisco アプライアンスには、Cisco Anti-Spam ソフトウェアの 30 日間評価キーが付属している場合があります。システム セットアップ ウィザードのこの部分では、アプライアンスで Cisco Anti-Spam をグローバルでイネーブルにすることを選択できます。アンチスパム サービスをイネーブルにしないことも選択できます。

アンチスパム サービスをイネーブルにする場合は、スパムおよび陽性と疑わしいスパム メッセージをローカル Cisco スпам隔離エリアに送信するように、AsyncOS を設定できます。Cisco スпам隔離は、アプライアンスのエンドユーザ隔離として機能します。エンドユーザのアクセス権を設定していない場合は、管理者だけが隔離を利用できます。

アプライアンスで使用可能なすべての Cisco Anti-Spam 設定オプションについては、第 13 章「アンチスパム」を参照してください。「隔離」(P.27-1)を参照してください。

アンチウイルス スキャンのイネーブル化

Cisco アプライアンスには、Sophos Anti-Virus または McAfee Anti-Virus スキャン エンジンの 30 日間評価キーが付属している場合があります。システム セットアップ ウィザードのこの部分では、アプライアンスでアンチウイルス スキャン エンジンをグローバルでイネーブルにすることを選択できます。

アンチウイルス スキャン エンジンをイネーブルにすると、デフォルトの着信メール ポリシーおよびデフォルトの発信メール ポリシーの両方についてイネーブルになります。Cisco アプライアンスでは、メールをスキャンしてウイルスを検出しますが、感染した添付ファイルの修復は行いません。アプライアンスでは、感染したメッセージをドロップします。

アプライアンスで使用可能なすべてのアンチウイルス コンフィギュレーション オプションについては、第 12 章「アンチウイルス」を参照してください。

アウトブレイク フィルタのイネーブル化

Cisco アプライアンスには、アウトブレイク フィルタの 30 日間評価キーが付属している場合があります。アウトブレイク フィルタは、従来のアンチウイルス セキュリティ サービスが新しいウイルス シグニチャ ファイルで更新されるまで、疑わしいメッセージを隔離することで、新種ウイルスの発生に対する「第一の防衛ライン」になります。

詳細については、第 14 章「アウトブレイク フィルタ」を参照してください。

[次へ (Next)] をクリックして続行します。

手順 5 : レビュー

設定情報のサマリーが表示されます。[システム設定 (System Settings)]、[ネットワーク インテグレーション (Network Integration)]、および [メッセージ セキュリティ (Message Security)] の情報は、[前へ (Previous)] ボタンをクリックするか、各セクションの右上にある対応する [編集 (Edit)] リンクをクリックすることによって編集できます。変更を加える手順まで戻った場合は、再度このレビュー ページに至るまで、残りの手順を進める必要があります。以前に入力した設定は、すべて残っています。

表示されている情報が要件を満たしていれば、[この設定をインストール (Install This Configuration)] をクリックします。

確認のダイアログが表示されます。[インストール (Install)] をクリックして、新しい設定をインストールします。

これで、Cisco アプライアンスは、電子メールを送信できる状態になりました。



(注)

アプライアンスへの接続に使用するインターフェイス (X1060/1070、C660/670、および C360/370 システムの Management インターフェイスまたは C160/170 システムの Data 1 インターフェイス) の IP アドレスをデフォルトから変更した場合は、[インストール (Install)] をクリックすると、現在の URL (http://192.168.42.42) への接続が失われます。ただし、ブラウザは、新しい IP アドレスにリダイレクトされます。

システム セットアップが完了すると、複数のアラート メッセージが送信されます。詳細については、「即時アラート」(P.3-36) を参照してください。

Active Directory への接続の設定

システム セットアップ ウィザードによって電子メールセキュリティ アプライアンスに設定が正しくインストールされると、Active Directory Wizard が表示されます。ネットワークで Active Directory サーバを稼働している場合は、Active Directory Wizard を使用して、Active Directory サーバ用の LDAP サーバプロファイルの設定と、受信者検証用リスナーの割り当てを行う必要があります。Active Directory を使用していないか、後で設定する場合は、[このステップをスキップ (Skip this Step)] をクリックします。Active Directory Wizard は、[システム管理 (System Administration)] > [Active Directory ウィザード (Active Directory Wizard)] ページで実行できます。Active Directory およびその他の LDAP プロファイルは、[システム管理 (System Administration)] > [LDAP] ページでも設定できます。

Active Directory Wizard では、認証方式、ポート、ベース DN、および SSL をサポートするかどうかなど、LDAP サーバプロファイルの作成に必要なシステム情報を取得します。Active Directory Wizard では、LDAP サーバプロファイル用の LDAP の受け入れクエリーおよびグループクエリーも作成します。

Active Directory Wizard によって LDAP サーバプロファイルが作成されてから、[システム管理 (System Administration)] > [LDAP] ページを使用して新規プロファイルを表示し、さらに変更を加えます。

手順

- ステップ 1** [Active Directory ウィザード (Active Directory Wizard)] ページで [Active Directory ウィザードを実行 (Run Active Directory Wizard)] をクリックします。
- ステップ 2** Active Directory サーバのホスト名を入力します。
- ステップ 3** 認証要求のためのユーザ名およびパスワードを入力します。
- ステップ 4** [次へ (Next)] をクリックして続行します。
Active Directory サーバへの接続が Active Directory Wizard によってテストされます。成功すると、[ディレクトリ設定のテスト (Test Directory Settings)] ページが表示されます。
- ステップ 5** Active Directory に存在すると判明している電子メールアドレスを入力し、[テスト (Test)] をクリックすることによって、ディレクトリ設定値をテストします。結果が [接続ステータス (Connection Status)] フィールドに表示されます。
- ステップ 6** [完了 (Done)] をクリックします。

次の手順

Active Directory Wizard と連携するようにアプライアンスを正常に設定するか、処理をスキップすると、[システム セットアップの次のステップ (System Setup Next Steps)] ページが表示されます。

[システム セットアップの次のステップ (System Setup Next Steps)] ページのリンクをクリックして、Cisco アプライアンスの設定を続行します。

コマンドライン インターフェイス (CLI) へのアクセス

CLI へのアクセスは、「アプライアンスへの接続」(P.3-8) で選択した管理接続方式によって異なります。工場出荷時のデフォルト ユーザ名およびパスワードを次に示します。当初は、admin ユーザ アカウントだけが CLI にアクセスできます。admin アカウントを介してコマンドライン インターフェイスに初回アクセスしたうえで、さまざまな許可レベルの他のユーザを追加できます (ユーザの追加については、「ユーザの追加」(P.28-4) を参照してください)。システム セットアップ ウィザードで、admin アカウントのパスワードを変更するよう要求されます。admin アカウントのパスワードは、password コマンドを使用して、任意の時点で直接再設定することもできます。

イーサネットを介して接続する場合は、工場出荷時のデフォルト IP アドレスの 192.168.42.42 を使用して SSH セッションまたは Telnet セッションを開始します。SSH は、ポート 22 を使用するように設定されています。Telnet は、ポート 23 を使用するように設定されています。下記のユーザ名とパスワードを入力します。

シリアル接続を介して接続する場合は、パーソナル コンピュータのシリアル ケーブルが接続されている通信ポートを使用して端末セッションを開始します。「アプライアンスへの接続」(P.3-8) に示されているシリアル ポートの設定値を使用してください。下記のユーザ名とパスワードを入力します。

下記のユーザ名およびパスワードを入力してアプライアンスにログインします。

工場出荷時のデフォルト ユーザ名とパスワード

- ユーザ名 : admin
- パスワード : ironport

次の例を参考にしてください。

```
login: admin
password: ironport
```

コマンドライン インターフェイス (CLI) システム セットアップ ウィザードの実行

CLI バージョンのシステム セットアップ ウィザードの手順は、基本的に GUI バージョン同様ですが、次のわずかな例外があります。

- CLI バージョンには、Web インターフェイスをイネーブルにするプロンプトが含まれています。
- CLI バージョンでは、作成する各リスナーのデフォルト メール フロー ポリシーを編集できます。
- CLI バージョンには、グローバルなアンチウイルス セキュリティ設定値およびアウトブレイク フィルタ セキュリティ設定値を設定するためのプロンプトが含まれています。
- CLI バージョンでは、システム セットアップの完了後に LDAP プロファイルを作成することを指示されません。ldapconfig コマンドを使用して LDAP プロファイルを作成してください。

システム セットアップ ウィザードを実行するには、コマンドプロンプトで `systemsetup` と入力します。

```
IronPort> systemsetup
```

システムを再設定するようシステム セットアップ ウィザードから警告が出されます。アプライアンスをまったく初めて設置する場合か、既存の設定を完全に上書きする場合は、この質問に [はい (Yes)] と回答します。

```
WARNING: The system setup wizard will completely delete any existing
```

```
'listeners' and all associated settings including the 'Host Access Table' - mail
operations may be interrupted.
```

```
Are you sure you wish to continue? [Y]> Y
```



(注)

以降のシステム セットアップ手順については、次で説明します。CLI バージョンのシステム セットアップ ウィザード対話の例には、「[Web ベースのシステム セットアップ ウィザードを使用した基本設定の定義](#)」(P.3-14) で説明した GUI バージョンのシステム セットアップ ウィザードから逸脱する部分だけを含めてあります。

admin パスワードの変更

まず、AsyncOS の admin アカウントのパスワードを変更します。続行するには、現在のパスワードを入力する必要があります。新しいパスワードは 6 文字以上の長さである必要があります。パスワードは、必ず安全な場所に保管してください。パスワードの変更は、システム セットアップ プロセスを終了した時点で有効になります。

ライセンス契約書の受諾

表示されるソフトウェア使用許諾契約を参照して受諾します。

ホスト名の設定

次に、Cisco アプライアンスの完全修飾ホスト名を定義します。この名前は、ネットワーク管理者が割り当てる必要があります。

論理 IP インターフェイスの割り当てと設定

次の手順では、Management (X1000/1050/1060/1070、C60/600/650/660/670、および C30/300/350/360/370 アプライアンス) または Data 1 (C10/100/150/160 アプライアンス) 物理イーサネット インターフェイス上に論理 IP インターフェイスの割り当てと設定を行います。続いて、アプライアンス上で使用可能な他の任意の物理イーサネット インターフェイス上に論理 IP インターフェイスを設定するよう指示されます。

各イーサネット インターフェイスに複数の IP インターフェイスを割り当てることができます。IP インターフェイスは、IP アドレスおよびホスト名を物理イーサネット インターフェイスと関連付ける論理構成概念です。Data 1 と Data 2 の両方のイーサネット ポートを使用する場合は、両方の接続用に IP アドレスとホスト名が必要です。

X1060/1070、C660/670、および C360/370 をご利用のお客様：Cisco では、パブリック リスナーを介してインバウンド電子メールを受信するためにインターネットに直接接続するように物理イーサネット ポートの 1 つを使用し、プライベート リスナーを介してアウトバウンド電子メールをリレーするために内部ネットワークに直接接続するようにもう 1 つの物理イーサネット ポートを使用することを推奨しています。

C160/170 をご利用のお客様：デフォルトでは、インバウンド電子メールの受信とアウトバウンド電子メールのリレーの両方のために、リスナー 1 つの物理イーサネット ポート 1 つだけが、systemsetup コマンドによって設定されます。



(注) アウトバウンド メールをリレーするようにインターフェイスを設定すると、そのインターフェイスを使用するパブリック リスナーが設定されている場合を除き、そのインターフェイスの SSH がシステムによってオンにされます。

次の情報が必要です。

- 後でその IP インターフェイスを参照するために作成した名前 (ニックネーム)。たとえば、イーサネット ポートの 1 つをプライベート ネットワーク用に使用し、もう 1 つをパブリック ネットワーク用にしている場合は、それぞれ PrivateNet および PublicNet などの名前を付けます。



(注) インターフェイス用に定義する名前では、大文字と小文字が区別されます。AsyncOS では、2 つの同じインターフェイス名を作成することはできません。たとえば、Privatenet および PrivateNet という名前は、異なる (一意の) 2 つの名前であると見なされます。

- ネットワーク管理者によって割り当てられた IP アドレス。これは、IPv4 アドレスまたは IPv6 アドレスにできます。1 つの IP インターフェイスに両方のタイプの IP アドレスを割り当てることができます。
- インターフェイスのネットマスク。ネットマスクは、CIDR 形式である必要があります。たとえば、255.255.255.0 サブネットでは /24 を使用します。



(注) 同じサブネットに含まれる IP アドレスを、別々の物理イーサネット インターフェイスには設定できません。ネットワークおよび IP アドレスのコンフィギュレーションの詳細については、付録 B 「ネットワーク アドレスと IP アドレスの割り当て」を参照してください。



(注) C10/100 をご利用のお客様は、Data 2 インターフェイスを先に設定します。

デフォルト ゲートウェイの指定

systemsetup コマンドの次の部分では、ネットワークのデフォルト ルータ (ゲートウェイ) の IP アドレスを入力します。

Web インターフェイスのイネーブル化

systemsetup コマンドの次の部分では、アプライアンス (Management イーサネット インターフェイス) の Web インターフェイスをイネーブルにします。Secure HTTP (https) を介して Web インターフェイスを実行することもできます。HTTPS を使用する場合は、独自の証明書を上ロードするまで、デモ証明書が使用されます。詳細については、「HTTPS の証明書のイネーブル化」(P.20-17) を参照してください。

DNS 設定値の設定

次に、Domain Name Service (DNS) 設定値を設定します。Cisco AsyncOS には、インターネットのルート サーバに直接問い合わせできる、高性能な内部 DNS リゾルバ/キャッシュが組み込まれていますが、独自の DNS サーバを使用することもできます。独自のサーバを使用する場合は、各 DNS サーバの IP アドレスおよびホスト名を指定する必要があります。必要な数の DNS サーバを入力できます (各サーバのプライオリティは 0 になります)。デフォルトでは、独自の DNS サーバのアドレスを入力するよう、systemsetup から示されます。

リスナーの作成

特定の IP インターフェイスに対して設定される、インバウンド電子メール処理サービスをリスナーによって管理します。リスナーは、内部システムまたはインターネットのいずれかから Cisco アプライアンスに着信する電子メールだけに適用されます。Cisco AsyncOS は、メッセージを受け入れて受信者のホストにリレーするために、リスナーを使用してメッセージが満たす必要のある基準を指定します。リスナーは、上記で指定した IP アドレス用に実行されている電子メール リスナーであると見なすことができます (「SMTP デーモン」と見なすことさえ可能)。

X1060/1070、C660/670、および C360/370 をご利用のお客様：デフォルトでは、パブリックとプライベートのリスナー 1 つずつの合計 2 つのリスナーが systemsetup コマンドによって設定されます (使用可能なリスナー タイプの詳細については、「電子メールを受信するためのゲートウェイの設定」(P.5-1) を参照してください)。

C160/170 をご利用のお客様：デフォルトでは、インターネットからのメールの受信と内部ネットワークからの電子メールのリレーの両方に対応するパブリック リスナー 1 つが systemsetup コマンドによって設定されます。「C10/100/150/160 のリスナーの例」(P.3-30) を参照してください。

リスナーを定義するときは、次の属性を指定します。

- 後でそのリスナーを参照するために作成した名前 (ニックネーム)。たとえば、インターネットに配信される、内部システムからの電子メールを受け入れるリスナーには、OutboundMail などの名前を付けます。
- 電子メールの受信に使用する、systemsetup コマンドで先に作成したいずれかの IP インターフェイス。
- 電子メールのルーティング先にするマシンの名前 (パブリック リスナーのみ)。(これは、最初の smtproutes エントリです。「ローカル ドメインの電子メールのルーティング」(P.21-1) を参照してください)。
- パブリック リスナーで SenderBase Reputation Score (SBRS; SenderBase レピュテーション スコア) に基づくフィルタリングをイネーブルにするかどうか。イネーブルにする場合は、[保守的 (Conservative)]、[適度 (Moderate)]、または [アグレッシブ (Aggressive)] から設定値を選択することも指示されます。
- ホストごとのレート制限：1 時間あたりにリモート ホストから受信する受信者の最大数 (パブリック リスナーのみ)。

- 受け入れる電子メールの宛先にされている受信者ドメインまたは特定のアドレス（パブリック リスナーの場合）、またはアプライアンスを介した電子メールのリレーを許可するシステム（プライベート リスナーの場合）。これらは、リスナーの受信者アクセス テーブルおよびホスト アクセス テーブルの最初のエントリです。詳細については、「送信者グループの構文」(P.7-4) および「メッセージを受け入れるドメインおよびユーザの追加」(P.8-3) を参照してください。

パブリック リスナー



(注) パブリック リスナーおよびプライベート リスナーを作成する次の例は、X1060/1070、C660/670、および C360/370 をご利用のお客様だけに適用されます。Cisco C160/170 をご利用のお客様は、次の「C10/100/150/160 のリスナーの例」(P.3-30) にスキップしてください。

systemsetup コマンドのこの例の部分では、PublicNet IP インターフェイスで実行されるように InboundMail というパブリック リスナーを設定します。続いて、ドメイン example.com 宛てのすべての電子メールを受け入れるように設定します。Mail Exchange exchange.example.com への初期 SMTP ルートを設定します。レート制限をイネーブルにし、パブリック リスナーに対して単一のホストから受信する 1 時間あたりの受信者の最大値に 4500 を指定します。



(注) 1 台のリモート ホストから 1 時間あたりに受信する最大受信者数に入力する値は、完全に自由裁量の値です。通常は、管理対象の電子メールを所有している企業の規模に比例します。たとえば、1 時間に 200 通のメッセージを送信する送信者は、「スパム送信者」（未承諾の大量電子メールの送信者）である可能性があります。10,000 人規模の会社に対するすべての電子メールを処理する Cisco アプライアンスを設定する場合は、単一のリモート ホストからの 1 時間あたりのメッセージが 200 通であっても、理にかなった値である可能性があります。対照的に、50 人規模の会社の場合に、1 時間あたり 200 通のメッセージを送信してくる送信者は、おそらく、明らかなスパム送信者です。パブリック リスナーで、企業へのインバウンド電子メールのレート制限をイネーブルにする（量を絞る）場合は、適切な値を選択してください。デフォルトのホスト アクセス ポリシーの詳細については、「送信者グループの構文」(P.7-4) を参照してください。

次に、リスナーのデフォルトのホスト アクセス ポリシーが受け入れられます。

```
You are now going to configure how the IronPort C60 accepts mail by
creating a "Listener".
```

```
Please create a name for this listener (Ex: "InboundMail"):
```

```
[1]> InboundMail
```

```
Please choose an IP interface for this Listener.
```

1. Management (192.168.42.42/24: mail3.example.com)
2. PrivateNet (192.168.1.1/24: mail3.example.com)
3. PublicNet (192.168.2.1/24: mail3.example.com)

```
[1]> 3
```

Enter the domains or specific addresses you want to accept mail for.

Hostnames such as "example.com" are allowed.

Partial hostnames such as ".example.com" are allowed.

Usernames such as "postmaster@" are allowed.

Full email addresses such as "joe@example.com" or "joe@[1.2.3.4]" are allowed.

Separate multiple addresses with commas.

```
[ ]> example.com
```

Would you like to configure SMTP routes for example.com? [Y]> **y**

Enter the destination mail server which you want mail for example.com to be delivered.
Separate multiple entries with commas.

```
[ ]> exchange.example.com
```

Do you want to enable rate limiting for this listener? (Rate limiting defines the maximum number of recipients per hour you are willing to receive from a remote domain.) [Y]> **y**

Enter the maximum number of recipients per hour to accept from a remote domain.

```
[ ]> 4500
```

Default Policy Parameters

=====

Maximum Message Size: 100M

Maximum Number Of Connections From A Single IP: 1,000

Maximum Number Of Messages Per Connection: 1,000

Maximum Number Of Recipients Per Message: 1,000

Maximum Number Of Recipients Per Hour: 4,500

Maximum Recipients Per Hour SMTP Response:

452 Too many recipients received this hour

```
Use SenderBase for Flow Control: Yes

Virus Detection Enabled: Yes

Allow TLS Connections: No

Would you like to change the default host access policy? [N]> n

Listener InboundMail created.

Defaults have been set for a Public listener.

Use the listenerconfig->EDIT command to customize the listener.

*****
```

プライベート リスナー

systemsetup コマンドのこの例の部分では、**PrivateNet IP** インターフェイスで実行されるように **OutboundMail** というプライベート リスナーを設定します。次に、ドメイン example.com に含まれる任意のホスト宛てのすべての電子メールをリレーするように設定します（エントリ .example.com の先頭のドットに注意してください）。

続いて、レート制限（イネーブルでない）のデフォルト値およびこのリスナーのデフォルト ホスト アクセス ポリシーが受け入れられます。

プライベート リスナーのデフォルト値は、先に作成したパブリック リスナーのデフォルト値と異なることに注意してください。詳細については、「[リスナーの使用](#)」(P.5-2) を参照してください。

```
Do you want to configure the C60 to relay mail for internal hosts? [Y]> y
```

```
Please create a name for this listener (Ex: "OutboundMail"):
```

```
[ ]> OutboundMail
```

```
Please choose an IP interface for this Listener.
```

1. Management (192.168.42.42/24: mail3.example.com)
2. PrivateNet (192.168.1.1/24: mail3.example.com)
3. PublicNet (192.168.2.1/24: mail3.example.com)

```
[1]> 2
```

```
Please specify the systems allowed to relay email through the IronPort C60.
```

```
Hostnames such as "example.com" are allowed.
```

Partial hostnames such as ".example.com" are allowed.

IP addresses, IP address ranges, and partial IP addresses are allowed.

Separate multiple entries with commas.

```
[ ]> .example.com
```

```
Do you want to enable rate limiting for this listener? (Rate limiting defines the
maximum number of recipients per hour you are willing to receive from a remote domain.)
[N]> n
```

Default Policy Parameters

=====

Maximum Message Size: 100M

Maximum Number Of Connections From A Single IP: 600

Maximum Number Of Messages Per Connection: 10,000

Maximum Number Of Recipients Per Message: 100,000

Maximum Number Of Recipients Per Hour: Disabled

Use SenderBase for Flow Control: No

Virus Detection Enabled: Yes

Allow TLS Connections: No

```
Would you like to change the default host access policy? [N]> n
```

Listener OutboundMail created.

Defaults have been set for a Private listener.

Use the listenerconfig->EDIT command to customize the listener.

C10/100/150/160 のリスナーの例



(注) リスナーを作成する次の例は、C160/170 をご利用のお客様だけに適用されます。

systemsetup コマンドのこの例の部分では、MailNet IP インターフェイスで実行されるように MailInterface というリスナーを設定します。続いて、ドメイン example.com 宛てのすべての電子メールを受け入れるように設定します。Mail Exchange exchange.example.com への初期 SMTP ルートを設定します。次に、ドメイン example.com に含まれる任意のホスト宛てのすべての電子メールをリレーするように同じリスナーを設定します（エントリ .example.com の先頭のドットに注意してください）。レート制限をイネーブルにし、パブリック リスナーに対して単一のホストから受信する 1 時間あたりの受信者の最大値に 450 を指定します。



(注)

1 台のリモート ホストから 1 時間あたりに受信する最大受信者数に入力する値は、完全に自由裁量の値です。通常は、管理対象の電子メールを所有している企業の規模に比例します。たとえば、1 時間に 200 通のメッセージを送信する送信者は、「スパム送信者」（未承諾の大量電子メールの送信者）である可能性があります。10,000 人規模の会社に対するすべての電子メールを処理する Cisco アプライアンスを設定する場合は、単一のリモート ホストからの 1 時間あたりのメッセージが 200 通であっても、理にかなった値である可能性があります。対照的に、50 人規模の会社の場合に、1 時間あたり 200 通のメッセージを送信してくる送信者は、おそらく、明らかなスパム送信者です。パブリック リスナーで、企業へのインバウンド電子メールのレート制限をイネーブルにする（量を絞る）場合は、適切な値を選択してください。デフォルトのホスト アクセス ポリシーの詳細については、「[送信者グループの構成](#)」(P.7-4) を参照してください。

次に、リスナーのデフォルトのホスト アクセス ポリシーが受け入れられます。

```
You are now going to configure how the IronPort C10 accepts mail by creating a "Listener".
```

```
Please create a name for this listener (Ex: "MailInterface"):
```

```
[1]> MailInterface
```

```
Please choose an IP interface for this Listener.
```

1. MailNet (10.1.1.1/24: mail3.example.com)
2. Management (192.168.42.42/24: mail3.example.com)

```
[1]> 1
```

```
Enter the domain names or specific email addresses you want to accept mail for.
```

```
Hostnames such as "example.com" are allowed.
```

```
Partial hostnames such as ".example.com" are allowed.
```

```
Usernames such as "postmaster@" are allowed.
```

```
Full email addresses such as "joe@example.com" or "joe@[1.2.3.4]" are allowed.
```

```
Separate multiple addresses with commas.
```

```
[ ]> example.com
```

```
Would you like to configure SMTP routes for example.com? [Y]> y
```

```
Enter the destination mail server where you want mail for example.com to be delivered.  
Separate multiple entries with commas.
```

```
[ ]> exchange.example.com
```

```
Please specify the systems allowed to relay email through the IronPort C10.
```

```
Hostnames such as "example.com" are allowed.
```

```
Partial hostnames such as ".example.com" are allowed.
```

```
IP addresses, IP address ranges, and partial IP addresses are allowed.
```

```
Separate multiple entries with commas.
```

```
[ ]> .example.com
```

```
Do you want to enable rate limiting for this listener? (Rate limiting defines the  
maximum number of recipients per hour you are willing to receive from a remote domain.)
```

```
[Y]> y
```

```
Enter the maximum number of recipients per hour to accept from a remote domain.
```

```
[ ]> 450
```

```
Default Policy Parameters
```

```
=====
```

```
Maximum Message Size: 10M
```

```
Maximum Number Of Connections From A Single IP: 50
```

```
Maximum Number Of Messages Per Connection: 100
```

```
Maximum Number Of Recipients Per Message: 100
```

```
Maximum Number Of Recipients Per Hour: 450
```

```
Maximum Recipients Per Hour SMTP Response:
```

```
452 Too many recipients received this hour

Use SenderBase for Flow Control: Yes

Spam Detection Enabled: Yes

Virus Detection Enabled: Yes

Allow TLS Connections: No

Would you like to change the default host access policy? [N]>

Listener MailInterface created.

Defaults have been set for a Public listener.

Use the listenerconfig->EDIT command to customize the listener.

*****
```



(注)

この `systemsetup` コマンドでは、C10/100 を利用しているお客様向けに、インバウンドとアウトバウンドの両方のメールに対してリスナー 1 つだけを設定するため、すべての発信メールがメールフローモニタ機能（通常はインバウンドメッセージに使用）で評価されます。第 26 章「電子メールセキュリティ モニタの使用法」を参照してください。

Cisco Anti-Spam のイネーブル化

Cisco アプライアンスには、Cisco Anti-Spam ソフトウェアの 30 日間有効な評価キーが付属していません。`systemsetup` コマンドのこの部分では、ライセンス契約書を受諾し、アプライアンスでグローバルに Cisco Anti-Spam をイネーブルにすることができます。

次に着信メール ポリシーに対する Cisco Anti-Spam スキャンをイネーブルにします。



(注)

ライセンス契約に合意しない場合、Cisco Anti-Spam はアプライアンスでイネーブルになりません。

アプライアンスで使用可能なすべての Cisco Anti-Spam 設定オプションについては、第 13 章「アンチスパム」を参照してください。

デフォルト アンチスパム スキャン エンジンの選択

複数のアンチスパム スキャン エンジンをイネーブルにした場合は、デフォルト着信メール ポリシーに対してイネーブルにするエンジンを選択するように示されます。

Cisco スпам隔離のイネーブル化

アンチスパム サービスをイネーブルにする場合は、スパム メッセージおよび陽性と疑わしいスパム メッセージをローカル Cisco スпам隔離エリアに送信するように、着信メール ポリシーをイネーブル できます。Cisco スпам隔離をイネーブルにすると、アプライアンスでエンドユーザ隔離もイネーブル になります。エンドユーザのアクセス権を設定していないうちは、管理者だけがエンドユーザ隔離を利用 できます。

「[スパム隔離の設定](#)」(P.27-19) を参照してください。

アンチウイルス スキャンのイネーブル化

Cisco アプライアンスには、ウイルス スキャン エンジンの 30 日間評価キーが付属しています。 systemsetup コマンドのこの部分では、1 つまたは複数のライセンス契約書を受諾し、アプライアンス でアンチウイルス スキャンをイネーブルにできます。アプライアンスでイネーブルにするアンチウイ ルス スキャン エンジンごとにライセンス契約を受諾する必要があります。

契約書を受諾すると、選択したアンチウイルス スキャン エンジンが着信メール ポリシーでイネーブル にされます。Cisco アプライアンスでは、着信メールをスキャンしてウイルスを検出しますが、感染し た添付ファイルの修復は行いません。アプライアンスでは、感染したメッセージをドロップします。

アプライアンスで使用可能なアンチウイルス コンフィギュレーション オプションについては、[第 12 章 「アンチウイルス」](#) を参照してください。

アウトブレイク フィルタおよび SenderBase 電子メール トラフィック モニタリング ネットワークのイネーブル化

続くこの手順では、SenderBase への参加とアウトブレイク フィルタの両方をイネーブルにするよう指 示されます。Cisco アプライアンスには、アウトブレイク フィルタの 30 日間評価キーが付属していま す。

アウトブレイク フィルタ

アウトブレイク フィルタは、従来のアンチウイルス セキュリティ サービスが新しいウイルス シグニ チャ ファイルで更新されるまで、疑わしいメッセージを隔離することで、新種ウイルスの発生に対す る「第一の防衛ライン」になります。アウトブレイク フィルタをイネーブルにした場合は、デフォルト 着信メール ポリシーでイネーブルになります。

アウトブレイク フィルタをイネーブルにする場合は、しきい値およびアウトブレイク フィルタ アラー トを受信するかどうかを入力します。アウトブレイク フィルタおよびしきい値の詳細については、「[ア ウトブレイク フィルタ](#)」(P.14-1) を参照してください。

SenderBase への参加

SenderBase は、電子メール管理者による送信者の調査、電子メールの正規送信元の識別、およびスパ ム送信者のブロックに役立つように設計された、電子メールのレピュテーション サービスです。

SenderBase 電子メール トラフィック モニタリング ネットワークへの参加に同意した場合は、組織宛 に送信された電子メールに関する集約された統計がシスコによって収集されます。メッセージ属性に関 する要約データと、さまざまなタイプのメッセージを Cisco アプライアンスで処理した方法に関する情 報が含まれます。

詳細については、[第 31 章 「SenderBase Network Participation」](#) を参照してください。

アラート設定値および AutoSupport の設定

ユーザの介入を必要とするシステム エラーが発生した場合、Cisco AsyncOS では、電子メールでアラート メッセージをユーザに送信します。システム アラートを受信する電子メール アドレスを 1 つ以上追加してください。複数のアドレスを指定する場合は、カンマで区切ります。入力した電子メールアドレスでは、当初、ディレクトリ獲得攻撃対策アラート以外のすべてのタイプおよびすべてのレベルのアラートを受信します。CLI で `alertconfig` コマンドを使用するか、GUI で [システム管理 (System Administration)] > [アラート (Alerts)] ページを使用することにより、後でアラート コンフィギュレーションを詳細化できます。詳細については、「アラート」(P.29-30) を参照してください。

Cisco AutoSupport 機能では、ご使用の Cisco アプライアンスに関する問題を Cisco カスタマー サポート チームが認識しておくことで、業界トップ水準のサポートを提供できます。IronPort サポート アラートおよび週ごとのステータスの更新をシスコに送信するには、[はい (Yes)] と回答します (詳細については、「Cisco AutoSupport」(P.29-32) を参照してください)。

スケジュール済みレポートの設定

デフォルトのスケジュール済みレポートの送信先にするアドレスを入力します。この値は空白にすることができ、その場合、レポートは、電子メールで送信される代わりに、アプライアンス上にアーカイブされます。

時刻設定値の設定

Cisco AsyncOS では、ネットワーク タイム プロトコル (NTP) を使用して、ネットワーク上またはインターネット上の他のサーバと時刻を同期するか、システム クロックを手動で設定することができます。Cisco アプライアンス上の時間帯を設定して、メッセージ ヘッダーおよびログ ファイルのタイムスタンプを正確にする必要もあります。Cisco Systems タイム サーバを使用して Cisco アプライアンス上の時刻を同期することもできます。

[大陸 (Continent)]、[国 (Country)]、および [タイムゾーン (Timezone)] を選択し、NTP を使用するかどうかと、使用する NTP サーバの名前を選択します。

変更の確定

最後に、手順全体で行った設定変更を確定するかどうかの確認が、システム セットアップ ウィザードから示されます。変更を確定する場合は、[はい (Yes)] と回答します。

システム セットアップ ウィザードを正常に完了すると、次のメッセージが表示されて、コマンド プロンプトが出されます。

```
Congratulations! System setup is complete. For advanced configuration, please refer to the User Guide.
```

```
mail3.example.com>
```

これで、Cisco アプライアンスは、電子メールを送信できる状態になりました。

設定のテスト

Cisco AsyncOS の設定をテストするために、`mailconfig` コマンドをすぐに使用して、`systemsetup` コマンドで作成したばかりのシステム コンフィギュレーション データを含むテスト電子メールを送信できます。

```
mail3.example.com> mailconfig
```

```
Please enter the email address to which you want to send
```

```
the configuration file. Separate multiple addresses with commas.
```

```
[ ]> user@example.com
```

```
The configuration file has been sent to user@example.com.
```

```
mail3.example.com>
```

利用可能なメールボックスに設定を送信して、システムでネットワーク上に電子メールを送信できることを確認します。

即時アラート

Cisco アプライアンスでは、ライセンス キーを使用して機能をイネーブルにします。`systemsetup` コマンドでリスナーを最初に作成した場合、Cisco Anti-Spam をイネーブルにした場合、Sophos または McAfee Anti-Virus をイネーブルにした場合、またはアウトブレイク フィルタをイネーブルにした場合は、アラートが生成されて、「手順 2：システム」(P.3-15) で指定したアドレスに送信されます。

キーの残り時間を定期的に通知するアラートです。次の例を参考にしてください。

```
Your "Receiving" key will expire in under 30 day(s). Please contact IronPort Customer Support.
```

```
Your "Sophos" key will expire in under 30 day(s). Please contact IronPort Customer Support.
```

```
Your "Outbreak Filters" key will expire in under 30 day(s). Please contact IronPort Customer Support.
```

30 日間の評価期間を超えて機能をイネーブルにする場合は、Cisco 営業担当者にお問い合わせください。キーの残り時間は、[システム管理 (System Administration)]> [ライセンス キー (Feature Keys)] ページからか、`featurekey` コマンドを発行することによって確認できます (詳細については、「ライセンス キー」(P.29-5) を参照してください)。

エンタープライズ ゲートウェイとしてシステムを設定

エンタープライズ ゲートウェイ（インターネットからの電子メールの受け入れ）としてシステムを設定する場合は、まずこの章を完了してから、詳細について第5章「電子メールを受信するためのゲートウェイの設定」を参照してください。

設定と次の手順の確認

システム セットアップが完了したため、Cisco アプライアンスによって電子メールが送信および受信されます。アンチウイルス、アンチスパム、およびウイルス アウトブレイク フィルタ セキュリティ機能をイネーブルにした場合は、着信メールおよび発信メールでスパムおよびウイルスのスキャンも行われます。

次の手順では、アプライアンスの設定をカスタマイズする方法を理解します。第4章「電子メール パイプラインの理解」では、システムでの電子メールのルーティング方法の詳細な概要を説明しています。各機能は、順次（上から下に）処理されます。各機能については、本書の残りの章で説明します。



CHAPTER 4

電子メールパイプラインの理解

- 「電子メールパイプラインの概要」(P.4-1)
- 「着信および受信」(P.4-4)
- 「ワークキューとルーティング」(P.4-6)
- 「配信」(P.4-10)

電子メールパイプラインの概要

電子メールパイプラインはCisco アプライアンスで処理されるため、電子メールフローです。これには3フェーズがあります：

- 受信：着信電子メールを受信するようにアプライアンスはリモートホストに接続されるため、設定された制限やその他の受信ポリシーに従います。たとえば、ホストがユーザのメールを送信できることを確認し、受信接続とメッセージ制限を適用し、メッセージの受信者を検証します。
- ワークキュー：アプライアンスは着信および発信メールを処理し、フィルタリング、セーフリスト/ブロックリストスキャン、スパム対策およびウイルス対策スキャン、アウトブレイクフィルタ、隔離などを実行します。
- 配信：発信電子メールを送信するようにアプライアンスは接続されるため、設定された配信制限とポリシーに従います。たとえば、発信接続制限を適用し、指定された配信不能メッセージを処理します。

電子メールパイプラインのフロー

図 4-1、図 4-2、および図 4-3 に、受信から配信へのルーティングまで、電子メールがシステムで処理される様子の概要を示します。各機能は順番に処理されます（上から下へ）。このパイプラインに含まれる機能の設定の大部分は、trace コマンドを使用してテストできます。

図 4-1 電子メールパイプライン：電子メール接続の受信

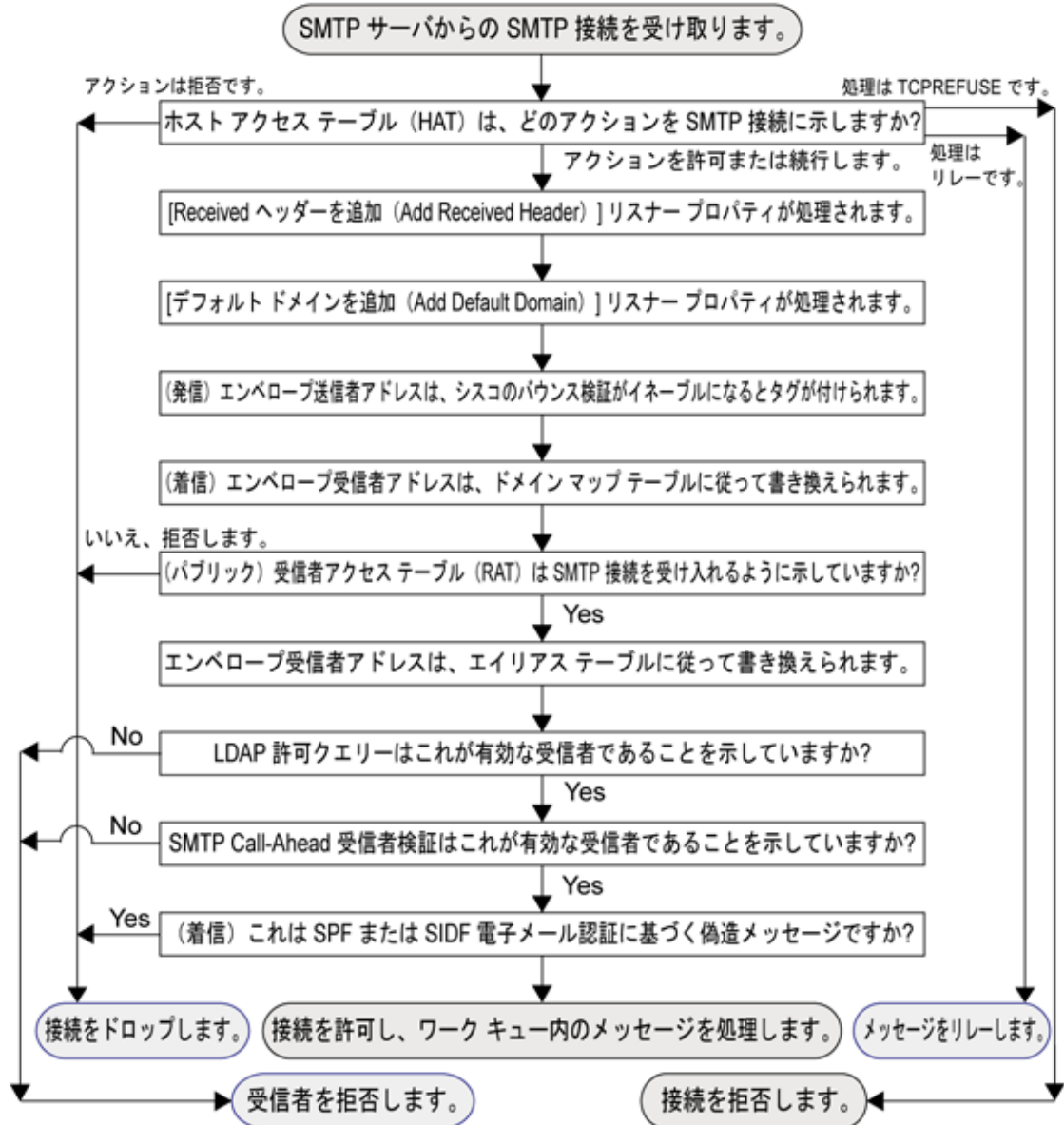
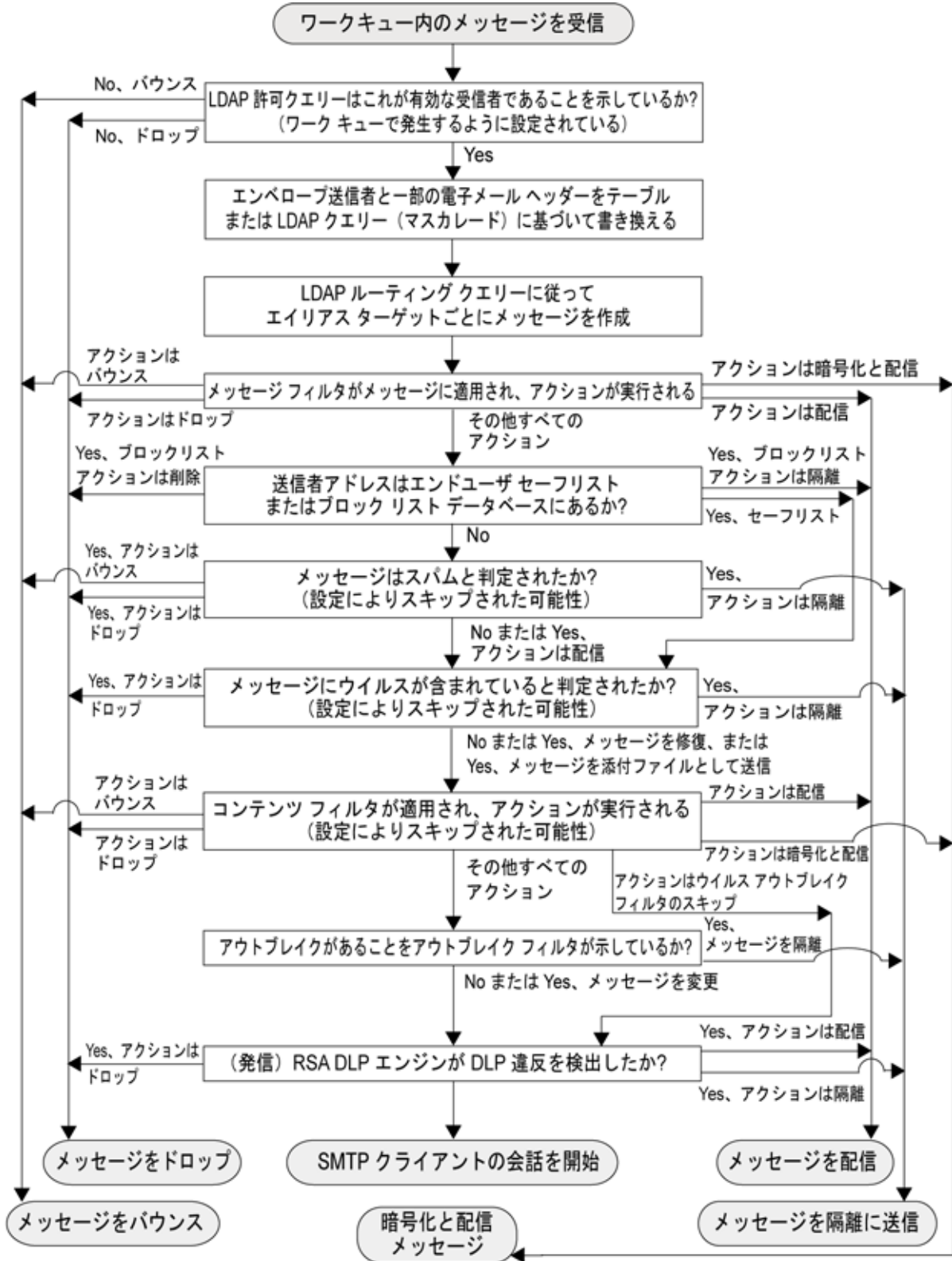
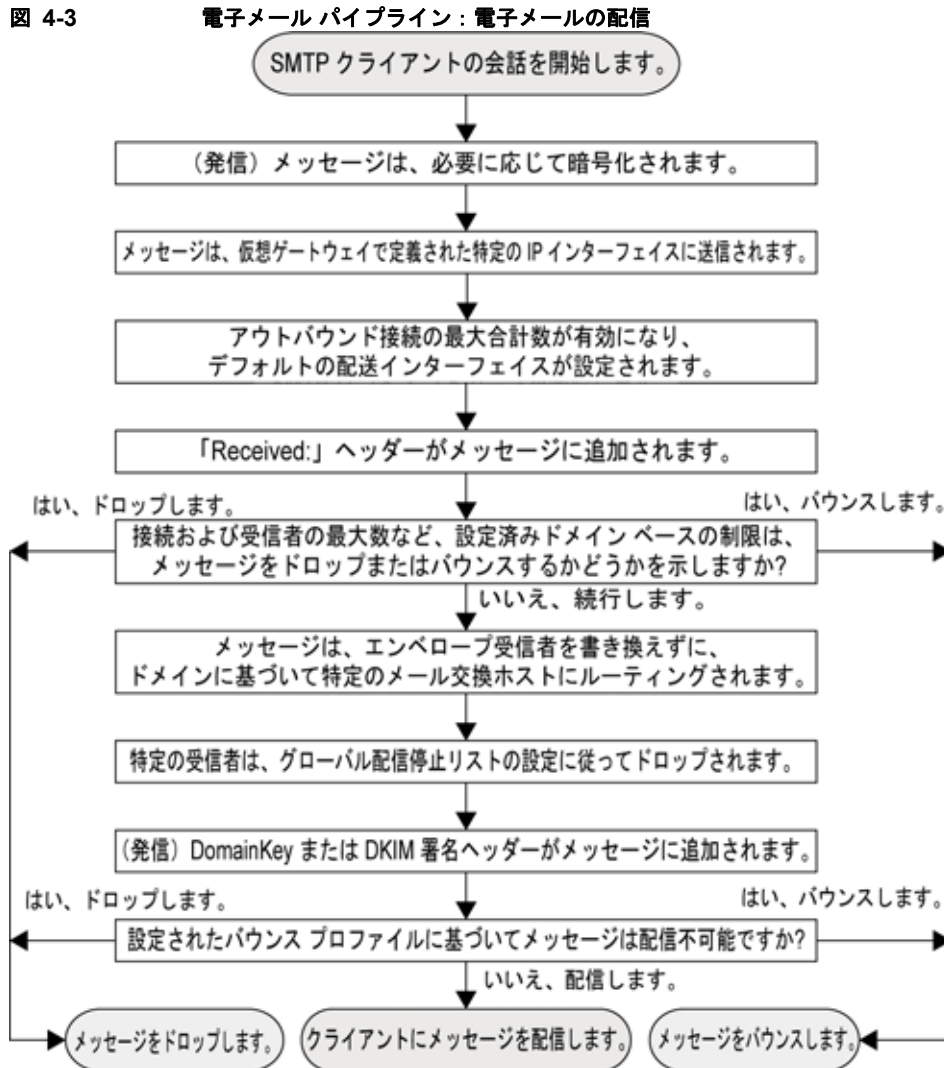


図 4-2 電子メールパイプライン：ワーク キュー





着信および受信

電子メールパイプラインの受信フェーズでは、送信者のホストからの初期接続が行われます。各メッセージのドメインを設定でき、受信者が検査されて、メッセージはワークキューに渡されます。

ホスト アクセス テーブル (HAT)、送信者グループ、およびメールフローポリシー

HAT では、リスナーへの接続を許可するホスト（つまり、電子メールの送信を許可するホスト）を指定できます。

送信者グループは、1 つまたは複数の送信者をグループに関連付けるために使用されるもので、メッセージフィルタおよびその他のメールフローポリシーを送信者グループに対して適用できます。メールフローポリシーは、一連の HAT パラメータ（アクセスルール、レート制限パラメータ、およびカスタム SMTP コードと応答）を表現する 1 つの方法です。

送信者グループおよびメールフローポリシーは合わせて、リスナーの HAT で定義されます。

送信者グループのホスト DNS 検証設定では、SMTP カンバセーションの前に未検証の送信者を分類し、さまざまな種類の未検証の送信者をさまざまな送信者グループに含めることができます。

SMTP カンバセーションに先立って、接続元のホストが送信者グループでホスト DNS 検証の対象になった一方で、エンベロープ送信者のドメイン部分はメールフローポリシーで DNS 検証されます。この検証は、SMTP カンバセーションの間に行われます。不正な形式のエンベロープ送信者を含むメッセージを無視できます。送信者検証例外テーブルにエントリを追加できます。このテーブルはメールの受け入れや拒否の基盤となるドメインと電子メールアドレスのリストで、エンベロープ送信者 DNS 検証設定値の影響は受けません。

レピュテーションフィルタリングでは、電子メール送信者を分類でき、Cisco SenderBase レピュテーションサービスによって決定された送信者の信頼性に基づいて電子メールインフラストラクチャの利用を制限できます。

詳細については、「[定義済みの送信者グループとメールフローポリシーの理解](#) (P.7-11) を参照してください。

Received: ヘッダー

`listenerconfig` コマンドを使用すると、リスナーで受信したすべてのメッセージに対して、デフォルトでは Received: ヘッダーを組み込まないようにリスナーを設定できます。

詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Customizing Listeners」の章の「Advanced Configuration Options」を参照してください。

デフォルト ドメイン

完全修飾ドメイン名を含んでいない送信者アドレスにデフォルトドメインを自動的に追加するようリスナーを設定できます。これらのアドレスを「素」アドレスとも呼びます（「joe」と「joe@example.com」など）。

詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Customizing Listeners」の章の「SMTP Address Parsing Options」を参照してください。

バウンス検証

発信メールには特別なキーがタグ付けされます。これにより、そのメールがバウンスとして送り返された場合は、そのタグを認識したうえでメールが配信されます。詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Delivery Features」の章の「IronPort Bounce Verification」を参照してください。

ドメインマップ

設定するリスナーごとにドメインマップテーブルを作成できます。ドメインマップテーブルに含まれているドメインと一致するメッセージでは、各受信者のエンベロープ受信者が書き換えられます。たとえば、joe@old.com -> joe@new.com です。

詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Delivery Features」の章の「The Domain Map Feature」を参照してください。

受信者アクセス テーブル (RAT)

インバウンド電子メールに限っては、Cisco アプライアンスでメールを受け入れるすべてのローカルドメインのリストを、RAT によって指定できます。

詳細については、「[受信者のアドレスに基づく接続の許可または拒否の概要 \(P.8-1\)](#)」を参照してください。

エイリアス テーブル

エイリアス テーブルを使用すると、1 人または複数の受信者にメッセージをリダイレクトできます。エイリアスはマッピング テーブルに格納されます。電子メールのエンベロップ受信者 (Envelope To または RCPT TO と呼ぶ) とエイリアス テーブルに定義されているエイリアスが一致すると、電子メールのエンベロップ受信者アドレスが書き換えられます。

エイリアス テーブルの詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Delivery Features」の章にある「Creating Alias Tables」を参照してください。

LDAP 受信者の受け入れ

既存の LDAP インフラストラクチャを使用して、着信メッセージの受信者電子メール アドレス (パブリック リスナー上) を SMTP カンバセーションまたはワークキュー内で処理する方法を定義できます。『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Customizing Listeners」の章の「Accept Queries」を参照してください。これにより、Cisco アプライアンスでは、独特な方法でディレクトリ獲得攻撃 (DHAP) に対処できます。システムでは、メッセージを受け入れて、SMTP カンバセーションまたはワークキューで LDAP 受け入れ検証を実行します。受信者が LDAP ディレクトリ内で見つからない場合に、遅延バウンスを実行するか、そのメッセージ全体をドロップするかを設定できます。

詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「LDAP Queries」の章を参照してください。

SMTP Call-Ahead 受信者検証

電子メールセキュリティ アプライアンスで SMTP Call-Ahead 受信者検証を設定すると、電子メールセキュリティ アプライアンスは、SMTP サーバに「事前に電話して」受信者を検証する間、送信側の MTA との SMTP 通信を中断します。Cisco アプライアンスが SMTP サーバに問い合わせると、SMTP サーバの応答が電子メールセキュリティ アプライアンスに返されます。電子メールセキュリティ アプライアンスは SMTP 通信を再開し、送信側の MTA に応答を送信し、SMTP サーバの応答 (および SMTP Call-Ahead プロファイルの設定) に基づいて接続を続行するかドロップします。

詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Validating Recipients Using an SMTP Server」の章を参照してください。

ワーク キューとルーティング

ワーク キューでは、配信フェーズに移動される前の受信メッセージを処理します。処理には、マスカレード、ルーティング、フィルタリング、セーフリスト/ブロックリスト スキャン、アンチスパムおよびアンチウイルス スキャン、アウトブレイク フィルタ、および隔離が含まれます。



(注) Data Loss Prevention (DLP) スキャンは、発信メッセージだけで使用可能です。DLP メッセージ スキャンが実行されるワーク キュー内の位置については、「[メッセージ分裂](#)」(P.10-5) を参照してください。

電子メールパイプラインとセキュリティ サービス

原則として、セキュリティ サービス (アンチスパム スキャン、アンチウイルス スキャン、およびアウトブレイク フィルタ) に対する変更は、すでにワーク キューにあるメッセージには影響しません。次に例を示します。

初めてパイプラインに入るメッセージについて、次のいずれかの理由により、アンチウイルス スキャンがバイパスされると仮定します。

- アプライアンスでグローバルにアンチウイルス スキャンがイネーブルにされていなかった。または、
- アンチウイルス スキャンをスキップするように HAT ポリシーで指定されていた。または、
- そのメッセージに対するアンチウイルス スキャンをバイパスさせるメッセージフィルタが存在していた。

この場合、アンチウイルス スキャンが再イネーブル化されているかどうかを問わず、隔離エリアから解放されるときにそのメッセージのアンチウイルス スキャンは行われません。ただし、メール ポリシーに基づいてアンチウイルス スキャンがバイパスされるメッセージの場合は、隔離エリアからの解放時にアンチウイルス スキャンが行われる可能性があります。メッセージが隔離エリアにある間に、メール ポリシーの設定値が変更される可能性があるためです。たとえば、メール ポリシーによってメッセージがアンチウイルス スキャンをバイパスし、隔離されている場合に、隔離エリアからの解放以前にメール ポリシーが更新されて、アンチウイルス スキャンが組み込まれた場合、そのメッセージは、隔離エリアからの解放時にアンチウイルス スキャンが行われます。

同様に、誤ってアンチスパム スキャンをグローバルに (または HAT で) ディセーブルにし、メールがワーク キューに入った後で気付いたとします。その時点でアンチスパムをイネーブルにしても、ワーク キューにあるメッセージについてはアンチスパム スキャンは行われません。

LDAP 受信者の受け入れ

既存の LDAP インフラストラクチャを使用して、着信メッセージの受信者電子メールアドレス (パブリック リスナー上) を SMTP カンバセーションまたはワークキュー内で処理する方法を定義できます。『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Customizing Listeners」の章の「Accept Queries」を参照してください。これにより、Cisco アプライアンスでは、独特な方法でディレクトリ獲得攻撃 (DHAP) に対処できます。システムでは、メッセージを受け入れて、SMTP カンバセーションまたはワーク キューで LDAP 受け入れ検証を実行します。受信者が LDAP ディレクトリ内で見つからない場合に、遅延バウンスを実行するか、そのメッセージ全体をドロップするかを設定できます。

詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「LDAP Queries」の章を参照してください。

マスカレードまたは LDAP マスカレード

マスカレードは、作成したテーブルに従って、エンベロープ送信者（送信者または MAIL FROM と呼ぶ）およびプライベートまたはパブリック リスナーによって処理される電子メールの To:、From:、CC: のヘッダーを書き換える機能です。スタティック マッピング テーブルと LDAP クエリーの 2 通りのうちいずれかによって、作成したリスナーごとに異なるマスカレード パラメータを指定できます。

スタティック マッピング テーブルによるマスカレードの詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Delivery Features」の章にある「Configuring Masquerading」を参照してください。

クエリーによるマスカレードの詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「LDAP Queries」の章を参照してください。

LDAP ルーティング

ネットワーク上の LDAP ディレクトリで使用可能な情報に基づいて、適切なアドレスやメール ホストにメッセージをルーティングするように Cisco アプライアンスを設定できます。

詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「LDAP Queries」を参照してください。

メッセージ フィルタ

メッセージ フィルタでは、受信直後のメッセージおよび添付ファイルの処理方法を記述した特別なルールを作成できます。フィルタ ルールでは、メッセージまたは添付ファイルの内容、ネットワークに関する情報、メッセージ エンベロープ、メッセージ ヘッダー、またはメッセージ本文に基づいてメッセージを識別します。フィルタ アクションでは、メッセージのドロップ、バウンス、アーカイブ、隔離、ブラインド カーボン コピー、または変更を行うことができます。

詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Using Message Filters to Enforce Email Policies」の章を参照してください。

複数受信者メッセージは、このフェーズの後に、電子メール セキュリティ マネージャに先立って「分裂」されます。メッセージの分裂とは、電子メール セキュリティ マネージャによる処理のために、単一の受信者を設定した電子メールの分裂版コピーを作成することを指します。

電子メール セキュリティ マネージャ（受信者単位のスキャン）

セーフリスト/ブロックリスト スキャン

エンドユーザ セーフリストおよびブロックリストは、エンドユーザによって作成されて、アンチスパム スキャンに先行して検査されるデータベースに格納されます。各エンドユーザは、常にスパムとして扱うか、決してスパムとして扱わないドメイン、サブドメイン、または電子メール アドレスを指定できます。送信者アドレスがエンドユーザ セーフリストに含まれている場合、アンチスパム スキャンはスキップされます。送信者アドレスがブロックリストに含まれている場合、メッセージは、管理者設定値に応じて隔離するかドロップすることができます。セーフリストおよびブロックリストの設定の詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Quarantines」の章を参照してください。

スパム対策

スパム対策機能は、Cisco Anti-Spam スキャンを行います。アンチスパム スキャンは、インターネット全体にわたるサーバ側のアンチスパム保護を提供します。アンチスパム スキャンでは、スパム攻撃によってユーザに不便が生じ、ネットワークが蹂躪されたり損傷したりする前に、スパム攻撃を活発に識別し、危険を除去します。その結果、ユーザのプライバシーを侵害することなく、ユーザの受信箱に届く前に、不要なメールを削除できます。

スパム対策スキャンは Cisco スパム隔離にメールを配信するように設定できます（オンボックスまたはオフボックス）。Cisco スパム隔離から解放されるメッセージは電子メールパイプラインで処理する以降のワークキューをとばし、宛先キューに直接進みます。

詳細については、第13章「アンチスパム」を参照してください。

アンチウイルス

Cisco アプライアンスには、統合されたウイルス スキャン エンジンが含まれています。「メールポリシー」ごとを基本に、メッセージおよび添付ファイルをスキャンしてウイルスを検出するように、アプライアンスを設定できます。ウイルスが検出された場合に次の処置を行うようにアプライアンスを設定できます。

- 添付ファイルの修復の試行
- 添付ファイルのドロップ
- 件名ヘッダーの変更
- 追加の X-Header の追加
- 異なるアドレスまたはメールホストへのメッセージの送信
- メッセージのアーカイブ
- メッセージの削除

メッセージが隔離エリア（「隔離」(P.4-10) を参照）から解放されると、ウイルスがスキャンされません。アンチウイルス スキャンの詳細については、第12章「アンチウイルス」を参照してください。

コンテンツ フィルタ

受信者ごとまたは送信者ごとを基準に、メッセージに適用するコンテンツ フィルタを作成できます。コンテンツ フィルタは、電子メールパイプラインで後ほど適用される点、つまり、1つのメッセージが、各電子メールセキュリティ マネージャ ポリシーに対応する個々の複数のメッセージに「分裂」された後で適用される点を除いては、メッセージ フィルタとほぼ同じです。コンテンツ フィルタ機能は、メッセージ フィルタ処理およびアンチスパムとアンチウイルス スキャンがメッセージに対して実行された後で適用されます。

コンテンツ フィルタの詳細については、「コンテンツ フィルタの概要」(P.11-1) を参照してください。

アウトブレイク フィルタ

Cisco のアウトブレイク フィルタ機能には、新たな拡散に対抗するための重要な第1層となるように活発に動作する特別なフィルタが含まれています。Cisco の発行するアウトブレイク ルールに基づいて、特定のファイルタイプの添付ファイルを持つメッセージを Outbreak という名前の隔離エリアに送信できます。

アウトブレイク隔離エリア内のメッセージは、他のすべての隔離エリア内のメッセージと同じように処理されます。隔離エリアおよびワークキューの詳細については、「[隔離](#)」(P.4-10)を参照してください。

詳細については、第 14 章「[アウトブレイク フィルタ](#)」を参照してください。

隔離

Cisco AsyncOS では、着信メッセージまたは発信メッセージをフィルタして、隔離エリアに入れることができます。隔離エリアは、メッセージの保持と処理に使用される特別なキュー、言い換えるとリポジトリです。隔離エリア内のメッセージは、隔離の設定方法に基づいて配信するか削除できます。

次のワークキュー機能では、メッセージを隔離エリアに送信できます。

- メッセージフィルタ
- アンチウイルス
- アウトブレイク フィルタ
- コンテンツ フィルタ

メッセージが隔離エリアから解放されると、ウイルスが再度スキャンされます。

詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「[Quarantines](#)」の章を参照してください。

配信

電子メールパイプラインの配信フェーズでは、接続の制限、バウンス、および受信者など、電子メール処理の最終フェーズを主とします。

仮想ゲートウェイ

Cisco Virtual Gateway テクノロジーを使用すると、Cisco アプライアンスを複数の Virtual Gateway アドレスに分割し、そのアドレスを使用して電子メールを送受信できます。各仮想ゲートウェイアドレスには、個別の IP アドレス、ホスト名、およびドメインと電子メール配信キューが割り当てられます。

詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「[Configuring Routing and Delivery Features](#)」の章の「[Using Virtual Gateway Technology](#)」を参照してください。

配信制限

配信時に使用する IP インターフェイスに基づく配信の制限およびアプライアンスでアウトバウンドメッセージ配信に適用する最大同時接続数を設定するには、`deliveryconfig` コマンドを使用します。

詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「[Configuring Routing and Delivery Features](#)」の章の「[Set Email Delivery Parameters](#)」を参照してください。

ドメインベースの制限値

各ドメインに対して、一定期間でシステムが超えることができない、接続および受信者の最大数を割り当てることができます。この「グッドネイバー」テーブルは、[メールポリシー (Mail Policies)] > [送信先コントロール (Destination Controls)] ページ (または `destconfig` コマンド) から定義します。

詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Delivery Features」の章の「Controlling Email Delivery」を参照してください。

ドメインベースのルーティング

エンベロープ受信者を書き換えることなく、特定のドメイン宛てのすべての電子メールを特定の Mail Exchange (MX) ホストにリダイレクトするには、[ネットワーク (Network)] > [SMTP ルート (SMTP Routes)] ページ (または `smtproutes` コマンド) を使用します。

詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Delivery Features」の章の「Routing Email for Local Domains」を参照してください。

グローバル配信停止

特定の受信者、受信者ドメイン、または IP アドレスに対する Cisco アプライアンスからのメッセージの配信を確実に停止するには、グローバル配信停止を使用します。グローバル配信停止をイネーブルにすると、すべての受信者アドレスが、グローバル配信停止対象のユーザ、ドメイン、電子メール アドレス、および IP アドレスのリストと照合されます。一致する電子メールは送信されません。

詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Delivery Features」の章の「Using Global Unsubscribe」を参照してください。

バウンス制限

作成する各リスナーのカンパシーションのハードバウンスおよびソフトバウンスを Cisco AsyncOS で処理する方法を設定するには、[ネットワーク (Network)] > [バウンスプロファイル (Bounce Profiles)] ページ (または `bounceconfig` コマンド) を使用します。バウンスプロファイルを作成し、各リスナーにプロファイルを適用するには、[ネットワーク (Network)] > [リスナー (Listeners)] ページ (または `listenerconfig` コマンド) を使用します。メッセージフィルタを使用して、特定のメッセージにバウンスプロファイルを割り当てることもできます。

バウンスプロファイルの詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Delivery Features」の章の「Directing Bounced Email」を参照してください。



CHAPTER 5

電子メールを受信するためのゲートウェイの設定

- 「電子メールを受信するためのゲートウェイ設定の概要」 (P.5-1)
- 「リスナーの使用」 (P.5-2)
- 「リスナーのグローバル設定」 (P.5-5)
- 「GUI からのリスナーの作成による接続要求のリッスン」 (P.5-8)
- 「CLI からのリスナーの作成による接続要求のリッスン」 (P.5-13)
- 「エンタープライズ ゲートウェイ構成」 (P.5-15)

電子メールを受信するためのゲートウェイ設定の概要

Cisco アプライアンスは、組織の電子メール ゲートウェイ、電子メール接続の提供、メッセージの受け入れ、それらの適切なシステムへのリレーといった機能をします。アプライアンスは、インターネットからユーザのネットワーク内の受信者ホストへ、ユーザのネットワーク内のシステムからインターネットに電子メール接続を提供できます。通常、電子メール接続要求は Simple Mail Transfer Protocol (SMTP; シンプル メール転送プロトコル) を使用します。アプライアンスは、SMTP 接続をデフォルトで提供し、SMTP ゲートウェイとして機能し、ネットワークのメール エクスチェンジまたは MX と呼ばれます。

アプライアンスは、着信 SMTP 接続要求を提供するためにリスナーを使用します。リスナーは、特定の IP インターフェイスで設定される電子メール処理サービスを記述します。リスナーは、インターネットまたはインターネットに到達しようとするユーザのネットワーク内のシステムから、アプライアンスに入る電子メールだけに適用されます。メッセージおよび接続が、メッセージを受け入れて受信者のホストにリレーするために満たす必要のある基準を、リスナーを使用して指定します。リスナーは、指定された各 IP アドレスを特定のポート上で実行する「SMTP デモン」として見なすことができます。また、リスナーは Cisco アプライアンスがアプライアンスにメールを送信しようとするシステムと通信する方法を定義します。

次のタイプのリスナーを作成できます。

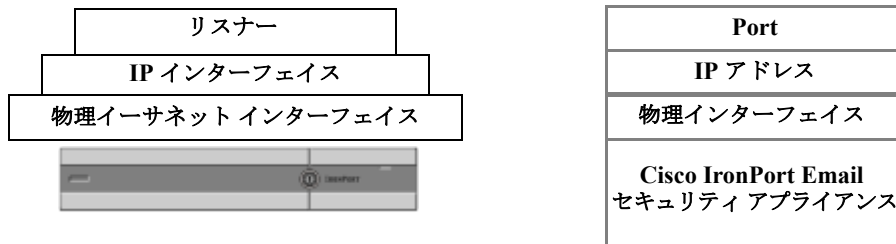
- **パブリック。** インターネットから着信するメール メッセージをリッスンし、受け入れます。パブリック リスナーは多数のホストからの接続を受信し、限られた数の受信者にメッセージを渡します。
- **プライベート。** ユーザのネットワーク内のシステムから (インターネット中でネットワークの外にいる受信者ではなく、通常内部グループウェアおよび電子メール サーバ (POP/IMAP) から)、電子メール メッセージをリッスンし、受け入れます。プライベート リスナーは、限られた (既知の) 数のホストからの接続を受信し、多数の受信者にメッセージを渡します。

リスナーを作成するときは、次の情報も指定します。

- **リスナーのプロパティ。**すべてのリスナーに適用するグローバル プロパティおよび各リスナーに固有のプロパティを定義します。たとえば、リスナーに使用する IP インターフェイスおよびポート、そしてこれがパブリックまたはプライベートのリスナーのどちらかを指定することができます。この方法の詳細については、「[リスナーの使用](#)」(P.5-2) を参照してください。
- **リスナーに接続が許可されているのはどのホストか。**リモート ホストからの着信接続を制御するルールを定義します。たとえば、リモート ホストを定義し、リスナーに接続できるかどうか定義できます。この方法の詳細については、「[ホスト アクセス テーブル \(HAT\) を使用した接続を許可するホストの定義](#)」(P.7-1) を参照してください。
- **(パブリック リスナーのみ) リスナーがメッセージを受け入れるローカル ドメイン。**どの受信者がパブリック リスナーによって許可されるかを定義します。たとえば、組織で以前 oldcompany.com ドメインを使用し、現在 currentcompany.com ドメインを使用していて、currentcompany.com および oldcompany.com の両方からメッセージを受け入れる場合があります。この方法の詳細については、「[ドメイン名または受信者アドレスに基づく接続の許可または拒否](#)」(P.8-1) を参照してください。

ホスト アクセス テーブルおよび受信者アクセス テーブルを含むリスナーでの設定は、リスナーが SMTP キャンペーション中に SMTP サーバと通信する方法に影響します。これによって、接続が閉じる前に Cisco アプライアンスがスパムを送信するホストをブロックできます。

図 5-1 リスナー、IP インターフェイス、物理イーサネット インターフェイスの関係



リスナーの使用

GUI の [ネットワーク (Network)] > [リスナー (Listeners)] ページまたは CLI の `listenerconfig` コマンドを使用してリスナーを設定します。

すべてのリスナーに適用されるグローバル設定を定義できます。詳細については、「[リスナーのグローバル設定](#)」(P.5-5) を参照してください。

Cisco アプライアンスでリスナーを使用および設定する場合は、次のルールとガイドラインに留意してください。

- 設定済みの IP インターフェイスごとに複数のリスナーを定義できますが、各リスナーは異なるポートを使用する必要があります。
- デフォルトでは、SMTP は電子メール接続を提供するためのメール プロトコルとしてリスナーに使用されます。ただし、Quick Mail Queuing Protocol (QMQP) を使用して電子メール接続を提供するために Cisco IronPort アプライアンスも設定できます。listenerconfig CLI コマンドを使用してこれを行います。
- リスナーは、インターネット プロトコル バージョン 4 (IPv4) およびバージョン 6 (IPv6) アドレスの両方をサポートします。単一のリスナーでどちらかのプロトコル バージョンまたは両方を使用できます。リスナーは、接続ホストとしてメール配信に同じプロトコル バージョンを使用し

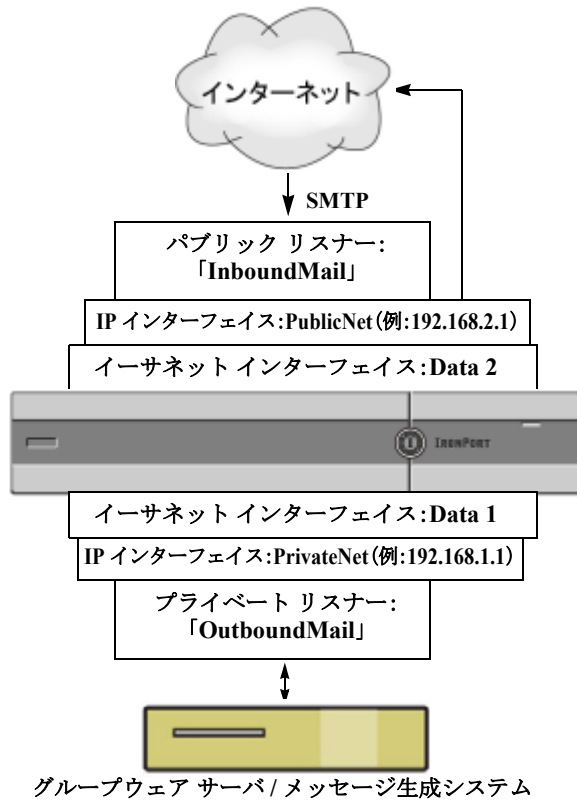
ます。たとえば、リスナーが IPv4 と IPv6 の両方に設定され、IPv6 を使用してホストに接続する場合、リスナーは IPv6 を使用します。ただし、リスナーが IPv6 アドレスのみの使用を設定されている場合は、IPv4 アドレスのみを使用するホストに接続できません。

- 少なくとも 1 つのリスナー（デフォルト値）がシステム セットアップ ウィザードの実行後にアプライアンス上に設定されます。ただし、リスナーを手動で作成する場合、AsyncOS ではこれらのデフォルト SBRS 値は使用されません。
- **C160/170 カスタマー**：システム セットアップ ウィザードでは、デフォルトで、インターネットからの電子メールの受信と内部ネットワークからの電子メールの中継の両方を行うための、1 つのパブリック リスナーを順を追って設定します。つまり、1 つのリスナーで両方の機能を実行できます。
- Cisco アプライアンスのテストおよびトラブルシューティングに利用するために、パブリックまたはプライベート リスナーの代わりに、「ブラックホール」タイプのリスナーを作成できます。ブラックホール リスナーの作成時に、メッセージを削除する前にそのメッセージをディスクに書き込むかどうかを選択します。（詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Testing and Troubleshooting」を参照してください）。メッセージを削除する前にディスクに書き込むと、受信レートおよびキューの速度の測定に役立ちます。メッセージをディスクに書き込まないリスナーは、メッセージ生成システムからの純粋な受信レートの測定に役立ちます。このリスナーのタイプは CLI の `listenerconfig` コマンドを使用した場合にだけ利用できます。

図 5-2 に、2 つ以上のイーサネット インターフェイスを持つ Cisco アプライアンス モデル上でシステム セットアップ ウィザードによって作成される一般的な電子メール ゲートウェイ構成を示します。2 つのリスナーが作成されます。あるインターフェイス上でインバウンド接続を使用可能にするためのパブリック リスナーと、別の IP インターフェイス上でアウトバウンド接続を使用可能にするためのプライベート リスナーです。

図 5-3 に、2 つだけイーサネット インターフェイスを持つ Cisco アプライアンス モデル上でシステム セットアップ ウィザードによって作成される一般的な電子メール ゲートウェイ構成を示します。インバウンド接続およびアウトバウンド接続の両方を提供するために、単一の IP インターフェイスで 1 つのリスナーが作成されます。

図 5-2 2つ以上のイーサネット インターフェイスを持つアプライアンス モデル上のパブリックおよびプライベート リスナー



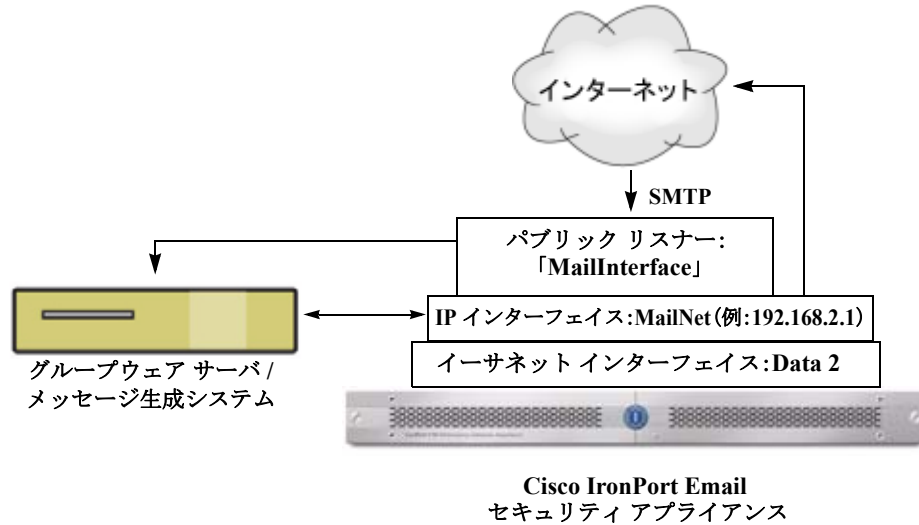
(注) このパブリック リスナーは、イーサネット インターフェイス Data2 上の IP インターフェイス PublicNet のポート 25 上で SMTP プロトコルを使用し、インターネットからのメッセージを受信します。IP インターフェイス PublicNet は、インターネット上の宛先ホストにメッセージを送信します。

Cisco IronPort Email セキュリティ アプライアンス

IP インターフェイス PrivateNet は、内部のメール ホストにメッセージを送信します。

(注) このプライベート リスナーは、イーサネット インターフェイス Data1 上の IP インターフェイス PrivateNet のポート 25 上で SMTP プロトコルを使用し、.example.com ドメインの内部システムからのメッセージを受信します。

図 5-3 2つだけイーサネットインターフェイスを持つアプライアンスモデル上のパブリックリスナー



- (注) このパブリックリスナーは、イーサネットインターフェイス Data2 上の IP インターフェイス PublicNet のポート 25 上で SMTP プロトコルを使用し、インターネットからのメッセージを受信し、.example.com ドメイン内の内部システムからのメッセージを中継します。IP インターフェイス MailNet は、インターネット上の宛先ホストと内部のメールホストにメッセージを送信します。

リスナーのグローバル設定

リスナーのグローバル設定は、Cisco アプライアンスで設定されたすべてのリスナーに影響します。リスナーが、インターネットプロトコルバージョン 4 (IPv4) およびバージョン 6 (IPv6) アドレスの両方を持つインターフェイスを使用する場合、リスナーの設定は IPv4 および IPv6 トラフィックの両方に適用されます。

手順

- ステップ 1 [ネットワーク (Network)] > [リスナー (Listeners)] を選択します。
- ステップ 2 [グローバル設定を編集 (Edit Global Settings)] をクリックします。

ステップ 3 次の表に定義された設定に変更します。

表 5-1 リスナー グローバル設定

グローバル設定	説明
最大同時接続数 (Maximum Concurrent Connections)	リスナーに同時に接続できる最大数を設定します。デフォルト値は 300 です。リスナーが IPv4 と IPv6 の両方の接続を受け入れる場合、接続数は 2 つの間で分配されます。たとえば最大同時接続数が 300 の場合、IPv4 および IPv6 接続の最大同時接続数が合計 300 を超えることはできません。
最大 TLS 同時接続数 (Maximum Concurrent TLS Connections)	すべてのリスナーでの同時 TLS 接続の最大数を設定します。デフォルト値は 100 です。リスナーが IPv4 と IPv6 の両方の TLS 接続を受け入れる場合、接続数は 2 つの間で分配されます。たとえば最大同時接続数が 100 の場合、IPv4 および IPv6 の TLS 接続の最大同時接続数が合計 100 を超えることはできません。
インジェクションカウンタリセット期間 (Injection Counters Reset Period)	インジェクション制御カウンタがリセットされた場合に調整できます。多数の IP アドレスのカウンタを管理している非常にビジーなシステムの場合、カウンタをより頻繁に (たとえば、60 分間隔ではなく 15 分間隔で) リセットするように設定します。これにより、データが管理不能なサイズにまで増大したり、システムのパフォーマンスに影響を与えたりすることを回避できます。 現在のデフォルト値は 1 時間です。最小 1 分 (60 秒) から最大 4 時間 (14,400 秒) までの期間を指定できます。 「 インジェクション制御期間 」(P.7-25) を参照してください。
受信接続のタイムアウトまでの待ち時間 (Timeout Period for Unsuccessful Inbound Connections)	AsyncOS が失敗した着信接続が閉じられるまでそのままの状態にする有効期間を設定します。 失敗した接続は SMTP カンパセーションとなり、正常なメッセージインジェクションが発生することなく、SMTP コマンドまたは ESMTP コマンドが発行され続けます。指定したタイムアウトが到達した場合、動作はエラーを送信し、接続を解除します。 「421 Timed out waiting for successful message injection, disconnecting.」 正常なメッセージインジェクションが発生するまで、接続に失敗したと見なされます。 パブリック リスナーの SMTP 接続にのみ使用できます。デフォルト値は 5 分です。

表 5-1 リスナー グローバル設定 (続き)

グローバル設定	説明
すべてのインバウンド接続の合計時間制限 (Total Time Limit for All Inbound Connections)	<p>AsyncOS が着信接続が閉じられるまでそのままの状態にする有効期間を設定します。</p> <p>この設定は、最大許容接続時間を適用することにより、システム リソースを保持するためのものです。この最大接続時間の約 80% が経過すると、次のメッセージが表示されます。</p> <p>「421 Exceeded allowable connection time, disconnecting.」</p> <p>アプライアンスは、接続が最大接続時間の 80% を超えると、接続がメッセージの途中で切断されることを防ぐために接続を切断しようとします。着信接続を最大接続時間の 80% に到達する期間開いている場合、発生する可能性がある問題です。時間制限を指定する場合、このしきい値に注意してください。</p> <p>パブリック リスナーの SMTP 接続にのみ使用できます。デフォルト値は 15 分です。</p>
HAT 遅延拒否 (HAT delayed rejections)	<p>メッセージ受信者レベルで HAT 拒否を実行するかどうかを設定します。デフォルトでは、HAT によって拒否された接続は SMTP カンパセーションの開始時にバナー メッセージをとまって終了されます。</p> <p>HAT 「拒否」設定で電子メールが拒否されると、AsyncOS では SMTP カンパセーションの開始時ではなく、メッセージ受信者レベル (RCPT TO) で拒否を実行できます。この方法でメッセージを拒否することで、メッセージの拒否が遅延されメッセージがバウンスするため、AsyncOS は拒否されたメッセージに関するより詳細な情報を取得できます。たとえば、ブロックされたメッセージのアドレスおよび各受信者のアドレスからメールを表示できます。また、HAT 拒否の遅延によって、MTA の送信が何度も再試行される可能性も小さくなります。</p> <p>HAT 遅延拒否をイネーブルにすると、次の動作が発生します。</p> <ul style="list-style-type: none"> • MAIL FROM コマンドが許可されるが、メッセージ オブジェクトは作成されない。 • 電子メールの送信のためのアクセスが拒否されたというメッセージが表示され、すべての RCPT TO コマンドが拒否される。 • SMTP AUTH を使用して MTA 送信が認証される場合、RELAY ポリシーが許可され、メールを通常どおりに送信できる。 <p>(注) CLI の listenerconfig --> setup コマンドからのみ設定できます。</p>

ステップ 4 変更内容を送信し、確定します。

複数のエンコーディングが含まれるメッセージの設定 : localeconfig

メッセージ処理中のメッセージのヘッダーおよびフッターのエンコードの変更に関する AsyncOS の動作を設定できます。この設定は GUI からは行えません。かわりに、CLI の localeconfig を使用して設定できます。

GUI からのリスナーの作成による接続要求のリスン

手順

ステップ 1 [ネットワーク (Network)] > [リスナー (Listener)] を選択します。

ステップ 2 [リスナーを追加 (Add Listener)] をクリックします。

ステップ 3 次の表に定義されている設定を設定します。

表 5-2 リスナーの設定

名前 (Name)	リスナーには、簡単に参照できるように一意の名前を付けてください。リスナー用に定義する名前では、大文字と小文字が区別されます。AsyncOS では、複数のリスナーに同一の名前を付けることはできません。
リスナーのタイプ (Type of Listener)	次のリスナー タイプのいずれかを選択します。 <ul style="list-style-type: none"> [パブリック (Public)]。パブリック リスナーには、インターネットから電子メールを受信するためのデフォルト特性が含まれます。 [プライベート (Private)]。プライベート リスナーは、プライベート (内部) ネットワークで使用することを目的としています。
インターフェイス (Interface)	リスナーを作成する設定済みアプライアンスの IP インターフェイスおよび TCP ポートを選択します。インターフェイスで使用する IP アドレスのバージョンによって、リスナーは IPv4 アドレス、IPv6 アドレス、または両方のバージョンからの接続を受け入れます。デフォルトでは、SMTP ではポート 25 を使用し、QMQP ではポート 628 を使用します。
バウンス プロファイル (Bounce Profile)	バウンス プロファイルを選択します (CLI の <code>bounceconfig</code> コマンドを使用して作成されたバウンス プロファイルがリストで使用可能です。「 新しいバウンス プロファイルの作成 」(P.21-40) を参照)。
免責条項を上配置 (Disclaimer Above)	電子メールの上または下に添付する免責条項を選択します ([メール ポリシー (Mail Policies)] > [テキスト リソース (Text Resources)] ページまたは CLI の <code>textconfig</code> コマンドで作成された文章がリストで使用可能です。『Cisco IronPort AsyncOS for Email Configuration Guide』の「Text Resources」の章を参照)。
免責条項を下配置 (Disclaimer Below)	電子メールの上または下に添付する免責条項を選択します ([メール ポリシー (Mail Policies)] > [テキスト リソース (Text Resources)] ページまたは CLI の <code>textconfig</code> コマンドで作成された文章がリストで使用可能です。『Cisco IronPort AsyncOS for Email Configuration Guide』の「Text Resources」の章を参照)。
SMTP 認証プロファイル (SMTP Authentication Profile)	SMTP 認証プロファイルを指定します。
証明書 (Certificate)	リスナーへの TLS 接続のための証明書を指定します ([ネットワーク (Network)] > [証明書 (Certificates)] ページまたは CLI の <code>certconfig</code> コマンドで追加された証明書がリストで使用可能です。「 他の MTA との暗号化通信の概要 」(P.20-1) を参照)。

ステップ 4 (任意) 次の表で定義される SMTP 「MAIL FROM」 および 「RCPT TO」 での解析の制御の設定を行います。

設定	説明
アドレス パーサー タイプ (Address Parser Type)	<p>次のパーサー タイプのいずれかを使用してアプライアンスが、RFC2821 規格にどの程度厳密に準拠するかを選択します。</p> <p>ストリクト モード :</p> <p>ストリクト モードは RFC 2821 に準拠します。ストリクト モードでは、アドレス解析が RFC 2821 の規格に準拠しますが、次の例外および追加機能があります。</p> <ul style="list-style-type: none"> 「MAIL FROM : <joe@example.com>」のように、コロンの後にスペースを挿入できます。 ドメイン名に下線を使用できます。 「MAIL FROM」 コマンドおよび 「RCPT TO」 コマンドでは、大文字と小文字が区別されます。 ピリオドは特殊な用途に使用できません (たとえば、RFC 2821 では 「J.D.」 のようなユーザ名を作成できません)。 <p>次の項で説明する追加オプションは、技術的に RFC 2821 に違反するため、イネーブルにできます。</p> <p>ルーズ モード :</p> <p>ルーズ解析は基本的に AsyncOS の以前のバージョンからの既存の動作です。電子メール アドレスの 「検索」 を最優先し、次のことを行います。</p> <ul style="list-style-type: none"> コメントの無視。ネストされたコメント (かっこで囲まれている) がサポートされ、それらは無視されます。 「RCPT TO」 コマンドおよび 「MAIL FROM」 コマンドで指定された電子メール アドレスの前後には山カッコが不要です。 複数のネストされた山カッコを使用できます (最も深いネストレベルの電子メール アドレスが検索される)。
8 ビット ユーザ名を許可 (Allow 8-bit User Names)	イネーブルにすると、(エスケープ処理なしで) アドレスのユーザ名部分に 8 ビットの文字を使用できます。
8 ビット ドメイン名を許可 (Allow 8-bit Domain Names)	イネーブルにすると、アドレスのドメイン部分に 8 ビットの文字を使用できます。

設定	説明
部分ドメインを許可 (Allow Partial Domains)	<p>イネーブルにすると、部分ドメインを使用できます。部分ドメインは完全なドメインではなく、ドットなしのドメインです。</p> <p>次のアドレスは、部分ドメインの例です。</p> <ul style="list-style-type: none"> • foo • foo@ • foo@bar <p>デフォルトのドメイン機能を正常に動作させるために、このオプションをイネーブルにする必要があります。</p> <p>[デフォルト ドメインを追加 (Add Default Domain)]: 完全修飾ドメイン名ではなく、デフォルトのドメインを電子メール アドレスに使用します。</p> <p>[SMTP アドレス解析オプション (SMTP Address Parsing options)]で [部分ドメインを許可 (Allow Partial Domains)]がイネーブルになっていない限り、このオプションはディセーブルです (「GUI からのリスナーの作成による接続要求のリスン」(P.5-8) を参照)。これは「デフォルト送信者ドメイン」を送信者のアドレスおよび完全修飾ドメイン名を含まない受信者のアドレスに追加することによって、リスナーがリレーする電子メールを変更する方法に影響します。(言い換えると、リスナーの「そのまま」アドレスの処理方法をカスタマイズできます)。</p> <p>従来のシステムで、送信者アドレスに企業のドメインを追加 (付加) せずに電子メールを送信する場合、これを使用してデフォルトの送信者ドメインを追加できます。たとえば、従来のシステムでは電子メールの送信者として自動的に文字列「joe」のみが入力された電子メールが作成されます。デフォルトの送信者ドメインを変更すると、「@yourdomain.com」が「joe」に付加され、完全修飾送信者名 joe@yourdomain.com が作成されます。</p>
ソース ルーティング (Source Routing)	<p>「MAIL FROM」アドレスおよび「RCPT TO」アドレスで送信元ルーティングが検出された場合の動作を決定します。送信元ルーティングは、複数の「@」文字を使用してルーティングを指定する、電子メール アドレスの特殊な形式です (例: @one.dom@two.dom:joe@three.dom)。「reject」を設定すると、アドレスは拒否されます。「strip」を設定すると、アドレスの送信元ルーティング部分が削除され、メッセージが通常どおり挿入されます。</p>
不明なアドレス文字 (Unknown Address Literals)	<p>システムで処理できないアドレス リテラルを受信したときの動作を決定します。現在は、IPv4 以外のすべてです。そのため、たとえば IPv6 アドレス リテラルの場合、プロトコル レベルで拒否するか、受信後すぐにハードバウンスを行うことができます。</p> <p>リテラルが含まれる受信者アドレスは即時ハードバウンスの原因となります。送信者アドレスは配信される場合があります。メッセージを配信できない場合、ハードバウンスがハードバウンスされます (二重ハードバウンス)。</p> <p>拒否された場合、送信者と受信者のアドレスがプロトコル レベルですぐに拒否されます。</p>
ユーザ名で次の文字を拒否 (Reject These Characters in User Names)	<p>文字 (たとえば、% や!) を含むユーザ名を入力すると、拒否されます。</p>

ステップ 5 (任意) 次の表に定義されているリスナーの動作をカスタマイズするための高度な設定を設定します。

設定	説明
最大同時接続数 (Maximum Concurrent Connections)	許可される最大接続数。
TCP リスン用キュー サイズ (TCP Listen Queue Size)	SMTP サーバが受け入れる前に AsyncOS で管理される接続のバックログ。
CR と LF の取り扱い (CR and LF Handling)	そのまの CR (復帰) 文字および LF (改行) 文字を含むメッセージの処理方法を選択します。 <ul style="list-style-type: none"> • [正常 (Clean)]。メッセージを許可しますが、そのまの CR 文字および LF 文字を CRLF 文字に変換します。 • [拒否 (Reject)]。メッセージを拒否します。 • [許可 (Allow)]。メッセージを許可します。
Received ヘッダーを追加 (Add Received Header)	すべての受信メールに Received ヘッダーを追加します。また、リスナーは各メッセージに Received: ヘッダーを追加してリレーする電子メールを変更します。Received: ヘッダーが含まれないようにするには、このオプションを使用してディセーブルにします。 <p>(注) Received: ヘッダーは、ワーク キューの処理ではメッセージに追加されません。このヘッダーは配信のためにメッセージがキューから出たときに追加されます。</p> <p>Received: ヘッダーをディセーブルにすると、インフラストラクチャの外部に送信されるすべてのメッセージで内部サーバの IP アドレスまたはホスト名が表示されることによって、ネットワークのトポロジが公開されないようにすることができます。Received: ヘッダーをディセーブルにする際には注意が必要です。</p>
SenderBase IP プロファイルを使用 (Use SenderBase IP Profiling)	[SenderBase IP プロファイルを使用 (SenderBase IP Profiling)] をイネーブルにするかどうかを選択し、次のように設定を行います。 <ul style="list-style-type: none"> • [クエリーのタイムアウト (Timeout for Queries)]。SenderBase レピュテーション サービスから照会される情報をアプライアンスがどのくらいの期間キャッシュするかを定義します。 • [接続ごとの SenderBase タイムアウト (SenderBase Timeout per Connection)]。SMTP 接続ごとの SenderBase 情報をアプライアンスがどのくらいの期間キャッシュするかを定義します。

ステップ 6 (任意) 次の表に定義されているこのリスナーに関連付けられた LDAP クエリーを制御する設定を行います。

リスナーの LDAP クエリーをイネーブルにするには、次の設定を使用します。このオプションを使用する前に、LDAP クエリーを作成しておく必要があります。クエリーの各タイプには、設定するための個別のサブセクションがあります。クエリーのタイプをクリックしてサブセクションを展開します。

LDAP クエリー作成の詳細については、「LDAP クエリー」(P.22-1) を参照してください。

クエリーのタイプ	説明
受け入れクエリー	<p>クエリーを受け入れるには、使用するクエリーをリストから選択します。LDAP Accept をワーク キューの処理中に実行するか、SMTP カンバセーションで実行するかを指定できます。</p> <p>ワーク キューの処理中に LDAP Accept を実行する場合、一致しない受信者に対する動作として、バウンスまたはドロップに指定します。</p> <p>SMTP カンバセーションで LDAP Accept を実行する場合、LDAP サーバに到達できない場合にメールを処理する方法を指定します。メッセージを許可するか、コードとカスタム応答で接続をドロップするかを選択できます。最後に、SMTP カンバセーションで Directory Harvest Attack Prevention (DHAP; ディレクトリ ハーベスト攻撃防止) しきい値に達した場合に接続をドロップするかどうかを選択します。</p> <p>SMTP カンバセーションで受信者の検証を行うと、複数の LDAP クエリー間の遅延を低減できます。したがって、対話形式の LDAP Accept をイネーブルにした場合、ディレクトリ サーバの負荷が増大することに注意してください。</p> <p>詳細については、「LDAP クエリーの概要」(P.22-1) を参照してください。</p>
ルーティング クエリー	<p>クエリーをルーティングするには、リストからクエリーを選択します。詳細については、「LDAP クエリーの概要」(P.22-1) を参照してください。</p>
マスカレード クエリー	<p>クエリーをマスカレードするには、リストからクエリーを選択して、From または CC ヘッダー アドレスといった、マスカレードするアドレスを選択します。</p> <p>詳細については、「LDAP クエリーの概要」(P.22-1) を参照してください。</p>
グループ クエリー	<p>クエリーをグループ化するには、リストからクエリーを選択します。詳細については、「LDAP クエリーの概要」(P.22-1) を参照してください。</p>

ステップ 7 変更内容を送信し、確定します。

部分ドメイン、デフォルト ドメイン、不正な形式の MAIL FROM

エンベロープ送信者検証をイネーブルにした場合、またはリスナーの SMTP アドレス解析オプションで部分ドメインの許可をディセーブルにした場合、リスナーのデフォルト ドメイン設定が使用されなくなります。

これらの機能は互いに排他的です。

CLI からのリスナーの作成による接続要求のリスン

表 5-3 に、リスナーの作成および編集に関連するタスクに使用する複数の listenerconfig サブコマンドを示します。

表 5-3 リスナーを作成するタスク

リスナーを作成するタスク	コマンドおよびサブコマンド	参考資料
新しいリスナーの作成	listenerconfig -> new	
リスナーのグローバル設定の編集	listenerconfig -> setup	「リスナーのグローバル設定」(P.5-5)
リスナーのバウンス プロファイルを指定	bounceconfig, listenerconfig -> edit -> bounceconfig	「新しいバウンス プロファイルの作成」(P.21-40)
リスナーへの免責条項の関連付け	textconfig, listenerconfig -> edit -> setup -> footer	『Cisco IronPort AsyncOS for Email Configuration Guide』で説明されています
SMTP 認証を設定	smtpauthconfig, listenerconfig -> smtpauth	
SMTP アドレス解析を設定	textconfig, listenerconfig -> edit -> setup -> address	
リスナーのデフォルトドメインを設定	listenerconfig -> edit -> setup -> defaultdomain	
Received: ヘッダーを電子メールに追加	listenerconfig -> edit -> setup -> received	
そのままの CR 文字および LF 文字を CRLF 文字に変更	listenerconfig -> edit -> setup -> cleansmtp	
ホスト アクセス テーブルを修正	listenerconfig -> edit -> hostaccess	『Cisco IronPort AsyncOS for Email Configuration Guide』で説明されています
ローカルドメインまたは特定のユーザ (RAT) への電子メールの受け入れ (パブリックリスナーのみ)	listenerconfig -> edit -> rcptaccess	『Cisco IronPort AsyncOS for Email Configuration Guide』で説明されています
リスナーの暗号化カンパセーション (TLS)	certconfig, settls, listenerconfig -> edit	「他の MTA との暗号化通信の概要」(P.20-1)
証明書の選択 (TLS)	listenerconfig -> edit -> certificate	「他の MTA との暗号化通信の概要」(P.20-1)

電子メールのルーティングおよび配信設定の詳細については、第 21 章「ルーティングおよび配信機能の設定」を参照してください。

HAT の詳細パラメータ

表 5-4 では、HAT の詳細パラメータの構文を定義しています。次の値は数値であり、後に **k** を追加してキロバイトで表すか、後に **m** を追加してメガバイトで表すことができます。文字のない値はバイトと見なされます。アスタリスク (*) でマーク付けされたパラメータでは、表 5-4 で示す変数構文がサポートされます。

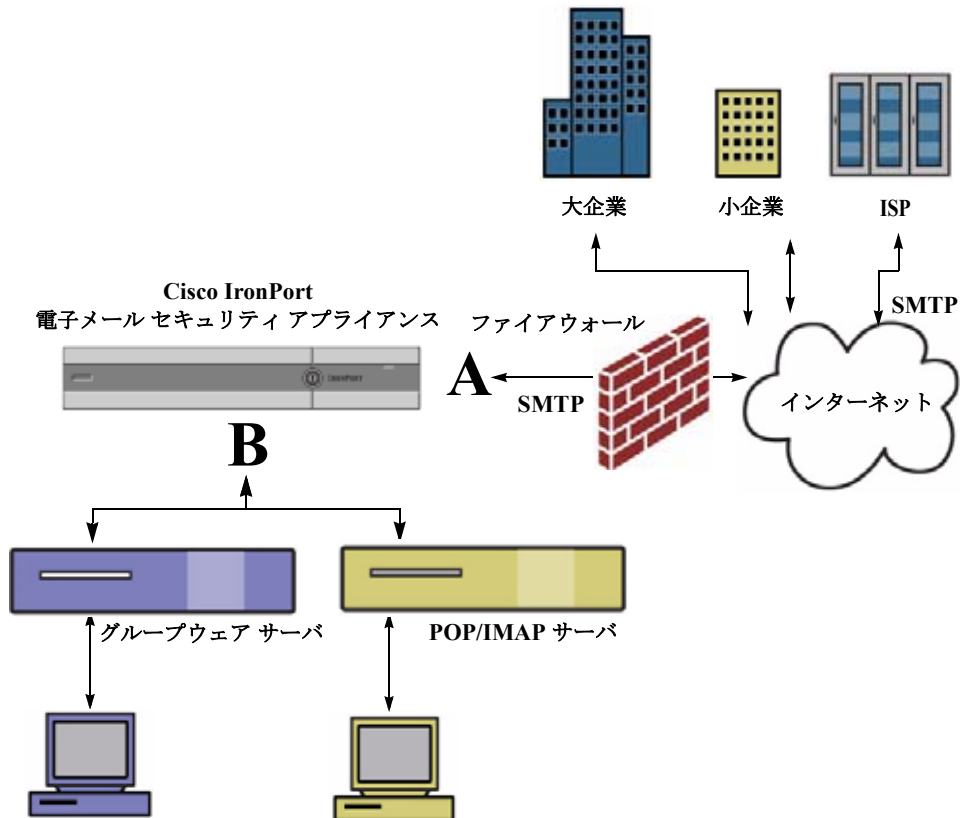
表 5-4 HAT 詳細パラメータの構文

パラメータ	構文	値	値の例
接続あたりの最大メッセージ数	max_msgs_per_session	番号	1000
メッセージあたりの最大受信者数	max_rcpts_per_msg	番号	10000 1k
最大メッセージ サイズ	max_message_size	番号	1048576 20M
このリスナーで可能な最大同時接続数	max_concurrency	番号	1000
SMTP バナー コード	smtp_banner_code	番号	220
SMTP バナー テキスト (*)	smtp_banner_text	文字列	Accepted
SMTP 拒否バナー コード	smtp_banner_code	番号	550
SMTP 拒否バナー テキスト (*)	smtp_banner_text	文字列	Rejected
SMTP バナーホスト名を上書き	use_override_hostname	on off default	default
	override_hostname	文字列	newhostname
TLS を使用	tls	on off required	on
スパム対策スキャンの使用	spam_check	on off	off
ウイルス スキャンの使用	virus_check	on off	off
1 時間あたりの最大受信者数	max_rcpts_per_hour	番号	5k
時間エラー コードあたりの最大受信者数	max_rcpts_per_hour_code	番号	452
時間テキストあたりの最大受信者数 (*)	max_rcpts_per_hour_text	文字列	Too many recipients
SenderBase を使用	use_sb	on off	on
SenderBase レピュテーション スコアの定義	sbrs[value1:value2]	-10.0 ~ 10.0	sbrs[-10:-7.5]
ディレクトリ獲得攻撃防御：1 時間あたりの無効な受信者の最大数	dhap_limit	番号	150

エンタープライズ ゲートウェイ構成

この設定では、エンタープライズ ゲートウェイの設定はインターネットからメールを受け取り、グループウェア サーバ、POP/IMAP サーバまたは他の MTA に電子メールをリレーします。エンタープライズ ゲートウェイは、それと同時に、グループウェア サーバおよびその他の電子メール サーバからの SMTP メッセージを受け付け、インターネット上の受信者に中継します。

図 5-4 エンタープライズ ゲートウェイのパブリック リスナーおよびプライベート リスナー



グループウェア クライアント POP/IMAP クライアント

この設定では、少なくとも 2 つのリスナーが必要です。

- インターネットからのメールだけを受け入れるように設定されたリスナー 1 つ
- 内部グループウェアおよび電子メール サーバ (POP/IMAP) からのメールだけを受け入れるように設定されたリスナー 1 つ

異なるパブリック ネットワークとプライベート ネットワーク用に個別のパブリック リスナーとプライベート リスナーを作成することで、セキュリティ、ポリシー強制、レポート、管理用に電子メールを区別できます。たとえば、パブリック リスナーで受信した電子メールは、設定されたアンチスパム エンジンおよびアンチウイルス スキャン エンジンによってデフォルトでスキャンされますが、プライベート リスナーで受信される電子メールはスキャンされません。

図 5-4 では、このエンタープライズ ゲートウェイ構成のアプライアンスで設定されたパブリック リスナー (A) 1 つとプライベート リスナー (B) 1 つを示します。



CHAPTER 6

レピュテーション フィルタリング

- 「レピュテーション フィルタリングの概要」 (P.6-1)
- 「SenderBase レピュテーション サービス」 (P.6-1)
- 「リスナーのレピュテーション フィルタリング スコアのしきい値の編集」 (P.6-5)
- 「メッセージの件名への低い SBRS スコアの入力」 (P.6-7)

レピュテーション フィルタリングの概要

レピュテーション フィルタリングはスパム保護の最初のレイヤで、Cisco SenderBase™ レピュテーション サービスにより決定される送信者の信頼性に基づいて、電子メール ゲートウェイからやってくるメッセージを制御できます。

Cisco アプライアンスは、既知または信頼性の高い送信者、つまりお客様やパートナーなどからのメッセージを受け取り、コンテンツ スキャンを一切実施しないでエンドユーザに直接配信できます。未知または信頼性の低い送信者からのメッセージは、アンチスパムおよびアンチウイルススキャンなどのコンテンツ スキャンの対象にできます。また、各送信者から受け入れるメッセージの数をスロットリングすることもできます。信頼性の最も低い電子メール送信者に対しては、設定に基づいて接続を拒否したり、その送信者からのメッセージを送り返したりできます。

SenderBase レピュテーション サービス

SenderBase Affiliate ネットワークからデータを使用する Cisco SenderBase レピュテーション サービスは、クレーム率およびメッセージ量の統計情報および公開ブラックリストや、オープンプロキシリストからのデータに基づいて、電子メール送信者に SenderBase レピュテーション スコアを割り当てます。SenderBase レピュテーション スコア サービスは、正当な送信者とスパム発信元を区別する際に役立ちます。レピュテーション スコアの低い送信者からのメッセージをブロックするしきい値を指定することも可能です。

Cisco IronPort SenderBase Security Network Web サイト (www.senderbase.org) では、最新の電子メールおよび Web ベースの脅威のグローバルな概要を提供して、国別の電子メール トラフィック量を表示し、IP アドレス、URI またはドメインに基づいたレピュテーション スコアを検索できます。



(注) SenderBase レピュテーション サービスは、現在の Anti-Spam ライセンス キーに限り使用可能です。

関連項目

- 「アウトブレイク フィルタ」 (P.14-1)

- 第 26 章「電子メール セキュリティ モニタの使用方法」

SenderBase レピュテーション スコア (SBRs)

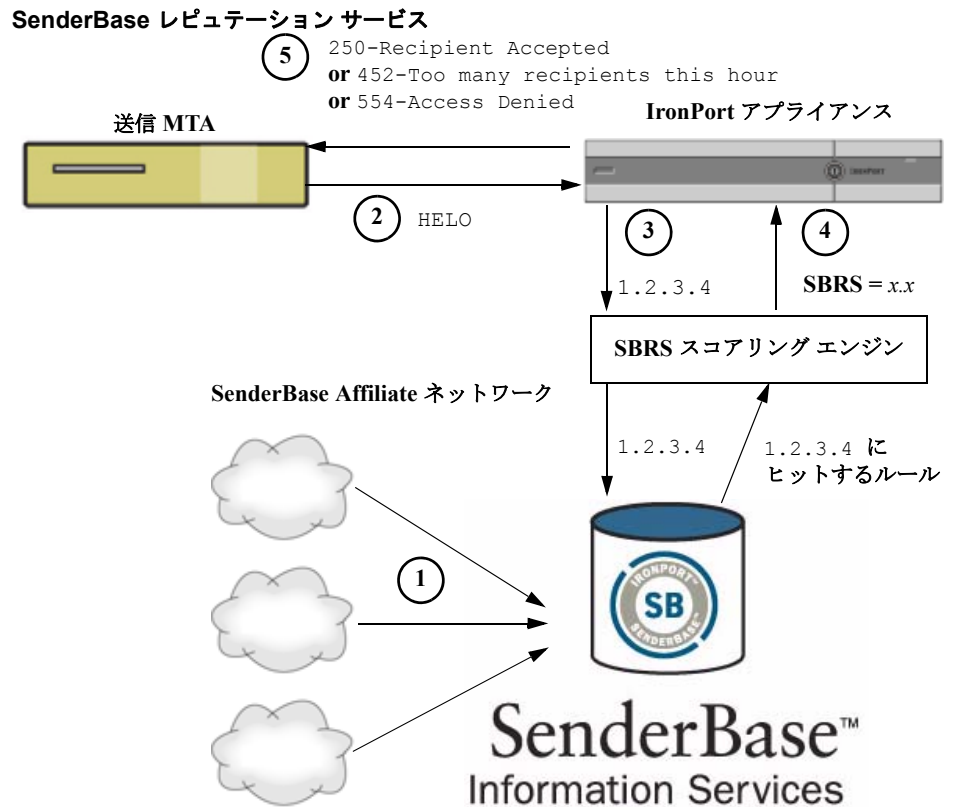
SenderBase Reputation Score (SBRs; SenderBase レピュテーション スコア) は、SenderBase レピュテーション サービスからの情報に基づいて、IP アドレスに割り当てられる数値です。SenderBase レピュテーション サービスは、25 個を超える公開ブラックリストおよびオープンプロキシリストのデータを集約し、さらにこのデータを SenderBase のグローバル データと組み合わせて、次のように -10.0 ~ +10.0 のスコアを割り当てます。

スコア	意味
-10.0	スパムの送信元である可能性が最も高い
0	中間か、または推奨を行うための十分な情報がない
+10.0	信頼できる送信者である可能性が最も高い

スコアが低いほど、メッセージがスパムである可能性は高くなります。スコアが -10.0 であれば、そのメッセージはスパムであると「保証」されていることを意味し、スコアが 10.0 であれば、そのメッセージは正規であると「保証」されていることを意味します。

SBRs を使用して、信頼性に基づいてメール フロー ポリシーを送信者に適用するように Cisco アプライアンスを設定します (メッセージ フィルタを作成して SenderBase レピュテーション スコアに「しきい値」を指定し、システムで処理されるメッセージにさらにアクションを実行できます。詳細については、「SenderBase レピュテーション ルール」(P.9-33) および「アンチスパム システムのバイパス アクション」(P.9-65) を参照してください。

図 6-1



- グローバルなクレーム データ
- グローバルな容量データ
- ブラックリスト
- オープン プロキシ リスト
- その他の SenderBase データ サービス

1. SenderBase Affiliate から、リアルタイムのグローバル データを送信します。
2. 送信 MTA により、Cisco アプライアンスとの接続が開始されます。
3. Cisco アプライアンスにより、接続 IP アドレスのグローバル データがチェックされます。
4. SenderBase レピュテーション サービスにより、このメッセージがスパムである可能性が計算され、SenderBase レピュテーション スコアが割り当てられます。
5. Cisco により、SenderBase レピュテーション スコアに基づいて応答が返されます。

SenderBase レピュテーション フィルタの仕組み

Cisco レピュテーション フィルタ テクノロジーは、Cisco アプライアンスで使用可能なその他のセキュリティ サービスの処理から、できる限り多くのメールを切り離すことを目的としています（「[電子メールパイプラインの理解](#)」(P.4-1) を参照）。

レピュテーション フィルタリングをイネーブルにすると、既知の悪質な送信者は、単純に拒否されま
す。世界で 2000 社から送信された既知の良好なメールは、false positive の可能性を低減するために、
自動的にフィルタを避けてルーティングされます。未知、または「灰色」の電子メールは、アンチスパ
ム スキャン エンジンにルーティングされます。レピュテーション フィルタは、この方法を使用して、
コンテンツ フィルタにかかる負荷を最大 50 % 低減できます。

図 6-2 レピュテーション フィルタリングの例



さまざまなレピュテーション フィルタリング手法の推奨設定

企業の目的に応じて、Conservative、Moderate、Aggressive のいずれかの方法を選択できます。

実現方法	特性	WHITELIST	BLACKLIST	SUSPECTLIST	UNKNOWNLIST
SenderBase レピュテーション スコア範囲					
Conservative	false positive はほ ぼ 0。良好なパ フォーマンス。	7 ~ 10	-10 ~ -4	-4 ~ -2	-2 ~ 7
Moderate (インストール時の デフォルト)	false positive は非 常に少ない。高パ フォーマンス。	SenderBase レ ピュテーション スコアは使用され ません。	-10 ~ -3	-3 ~ -1	-1 ~ +10
Aggressive	false positive はい くらか発生。パ フォーマンスは最 大。 このオプション は、ほとんどの メールをアンチス パム処理から切り 離します。	4 ~ 10	-10 ~ -2	-2 ~ -1	-1 ~ 4
メール フロー ポリシー					
すべての方式		信頼できる	ブロック	スロットル	承認

リスナーのレピュテーション フィルタリング スコアのしきい値の編集

デフォルトの SenderBase レピュテーション サービス (SBRs) スコアのしきい値を変更またはレピュテーション フィルタリングに送信者グループを追加する場合は、この手順を使用します。



(注)

SBRs スコアのしきい値に関連するその他の設定およびメール フロー ポリシー設定については、第 7 章「[ホスト アクセス テーブル \(HAT\) を使用した接続を許可するホストの定義](#)」に記載されています。

はじめる前に

- Cisco アプライアンスが、ローカル MX/MTA から電子メールを受信するように設定されている場合は、送信者の IP アドレスをマスクする可能性のあるアップストリーム ホストを識別します。詳細については、「[着信リレー構成における送信者の IP アドレスの決定](#)」(P.13-14) を参照してください。
- SenderBase レピュテーション スコア範囲について理解します。「[SenderBase レピュテーション スコアを使用した送信者グループの定義](#)」(P.7-6) を参照してください。
- 組織のフィルタリング方法を選択し、このアプローチの推奨設定を確認します。「[さまざまなレピュテーション フィルタリング手法の推奨設定](#)」(P.6-4) を参照してください。

手順

- ステップ 1** [メール ポリシー (Mail Policies)] > [HAT 概要 (HAT Overview)] を選択します。
- ステップ 2** [送信者グループ (リスナー) (Sender Groups (Listener))] メニューからパブリック リスナーを選択します。
- ステップ 3** 送信者グループのリンクをクリックします。
たとえば、「SUSPECTLIST」のリンクをクリックします。
- ステップ 4** [設定を編集 (Edit Settings)] をクリックします。
- ステップ 5** 送信者グループの SenderBase レピュテーション スコアの範囲を入力します。
たとえば、「WHITELIST」に 7.0 ~ 10 の範囲を入力します。
- ステップ 6** [送信 (Submit)] をクリックします。
- ステップ 7** 必要に応じてこのリスナーの各送信者グループに対し、繰り返し実行します。
- ステップ 8** 変更を確定します。

関連項目

- [第 7 章「ホスト アクセス テーブル \(HAT\) を使用した接続を許可するホストの定義](#)」
- [「メッセージがスパムかどうかスキャンするためのアプライアンスの設定方法](#)」(P.13-2)

SBRS を使用したレピュテーション フィルタリングのテスト

常時大量のスパムを受信しているか、または組織に対するスパムを受信するために「ダミー」のアカウントを特に設定していない限り、実装した SBRS ポリシーをただちにテストすることは困難です。ただし、表 6-1 に示すように、リスナーの HAT に SenderBase レピュテーション スコアによるレピュテーション フィルタリングのエントリを追加した場合は、インバウンドメールのうち「未分類」になるパーセンテージが低くなります。

ポリシーは、任意の SBRS で `trace` コマンドを使用してテストします。「[テストメッセージを使用したメールフローのデバッグ：トレース](#)」(P.36-1) を参照してください。trace コマンドは、GUI だけでなく CLI でも使用できます。

表 6-1 SBRS 実装の推奨メール フロー ポリシー

ポリシー名	主要な動作 (アクセス ルール)	パラメータ	値
\$BLOCKED	REJECT	None	
\$THROTTLED	ACCEPT	Maximum messages / session: Maximum recipients / message: Maximum message size: Maximum concurrent connections: Use Spam Detection: Use TLS: Maximum recipients / hour: Use SenderBase:	10 20 1 MB 10 ON OFF 20 (推奨) ON
\$ACCEPTED (パブリック リスナー)	ACCEPT	Maximum messages / session: Maximum recipients / message: Maximum message size: Maximum concurrent connections: Use Spam Detection: Use TLS: Use SenderBase:	1,000 1,000 100 MB 1,000 ON OFF ON
\$TRUSTED	ACCEPT	Maximum messages / session: Maximum recipients / message: Maximum message size: Maximum concurrent connections: Use Spam Detection: Use TLS: Maximum recipients / hour: Use SenderBase:	1,000 1,000 100 MB 1,000 OFF OFF -1 (ディセーブル) OFF



(注) STHROTTLED ポリシーでは、リモート ホストから受信する 1 時間あたりの最大受信者数は、デフォルトで 1 時間あたり 20 人に設定されています。この設定により、使用可能な最大スロットリングが制御されることに注意してください。このパラメータが厳しすぎる場合は、時間あたりの受信者数を増やすことができます。デフォルトのホスト アクセス ポリシーの詳細については、「[定義済みの送信者グループとメール フロー ポリシーの理解](#)」(P.7-11) を参照してください。

SenderBase レピュテーション サービスのステータスのモニタリング

[セキュリティ サービス (Security Services)]メニューの [SenderBase] ページには、Cisco アプライアンスから SenderBase Network Status Server および SenderBase レピュテーション スコア サービスに対して最後に実行したクエリーの接続ステータスおよびタイムスタンプが表示されます。SenderBase レピュテーション スコア サービスは、アプライアンスに SRBS スコアを送信します。SenderBase Network Server は、アプライアンスにメール送信元の IP アドレス、ドメイン、および組織についての情報を送信します。AsyncOS は、このデータをレポート作成および電子メール モニタリング機能に使用します。

図 6-3 [SenderBase] ページの [SenderBase ネットワークのステータス (SenderBase Network Status)]

SenderBase Network Status		
Type	Status	Last Status Check
SenderBase Network Server	up	Wed Sep 10 13:44:52 2008 PDT
SenderBase Reputation Score Service	up	Wed Sep 10 13:44:52 2008 PDT

CLI の sbstatus コマンドでも、同じ情報を表示できます。

メッセージの件名への低い SBRS スコアの入力

スロットリングを推奨しますが、SenderBase レピュテーション サービスを使用する別方法では、スパムの疑いのあるメッセージの件名行を変更します。このようにするには、表 6-2 に示すメッセージ フィルタを使用します。このフィルタは、reputation フィルタ ルールおよび strip-header および insert-header フィルタ アクションを使用して、SenderBase レピュテーション スコアが -2.0 未満のメッセージの件名行を、{Spam SBRS} のように表現される実際の SenderBase レピュテーション スコアを含む件名行に置き換えます。この例の *listener_name* を、ご使用のパブリック リスナーの名前に置き換えます (このテキストを切り取って filters コマンドのコマンドライン インターフェイスに直接貼り付けできるように、この行自体にピリオドが含まれています)。

表 6-2 件名ヘッダーを SBRs に変更するメッセージ フィルタ : 例 1

```
sbrs_filter:

if ((recv-inj == "listener_name" AND subject != "\\{Spam -?[0-9.]+\\}")

{

    insert-header("X-SBRs", "$REPUTATION");

    if (reputation <= -2.0)

    {

        strip-header("Subject");

        insert-header("Subject", "$Subject \\{Spam $REPUTATION\\}");

    }

}

.
```

関連項目

- [第 9 章「メッセージ フィルタを使用した電子メール ポリシーの適用」](#)。



CHAPTER 7

ホスト アクセス テーブル (HAT) を使用した 接続を許可するホストの定義

- 「接続を許可するホストの定義の概要」 (P.7-1)
- 「送信者グループへのリモート ホストの定義」 (P.7-3)
- 「メール フロー ポリシーを使用した電子メール送信者のアクセス ルールの定義」 (P.7-8)
- 「定義済みの送信者グループとメール フロー ポリシーの理解」 (P.7-11)
- 「送信者グループからのメッセージの同様の処理」 (P.7-13)
- 「ホスト アクセス テーブルの設定の使用」 (P.7-21)
- 「着信接続ルールへの送信者アドレス リストの使用」 (P.7-22)
- 「SenderBase 設定とメール フロー ポリシー」 (P.7-23)
- 「送信者の検証」 (P.7-28)

接続を許可するホストの定義の概要

設定されているすべてのリスナーに対して、リモート ホストからの着信接続を制御する一連の規則を定義します。たとえば、リモート ホストを定義し、リスナーに接続できるかどうか定義できます。AsyncOS では、ホスト アクセス テーブル (HAT) を使用してリスナーへの接続が許可されるホストを定義できます。

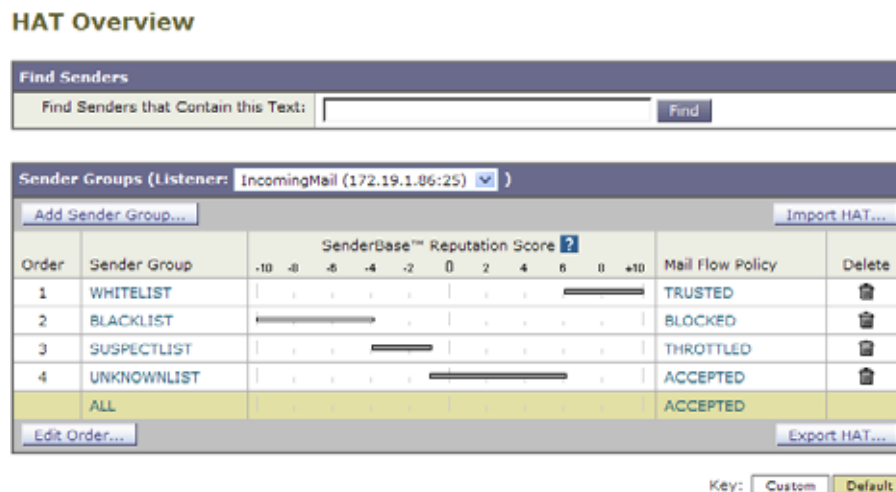
HAT は、リモート ホストからの着信接続を制御するリスナー用のルール セットを保持しています。設定されたどのリスナーにも独自の HAT があります。パブリック リスナーおよびプライベート リスナーの両方に HAT を設定します。

リモート ホストからの着信接続を制御するには、次の情報を定義します。

- **リモート ホスト** リモート ホストがリスナーに接続を試みる方法を定義します。リモート ホスト定義を送信者グループにグループ化します。たとえば、IP アドレスとホスト名の一部を使用して、送信者グループの複数のリモート ホストを定義できます。SenderBase レピュテーション スコアによってリモート ホストを定義できます。詳細については、「送信者グループへのリモート ホストの定義」 (P.7-3) を参照してください。
- **アクセル ルール** 送信者グループに定義されたリモート ホストがリスナーに接続するのを許可するのか、またどのような条件下なのかを定義できます。アクセス ルールは、メール フロー ポリシーを使って定義します。たとえば、特定の送信者グループのリスナーへの接続を許可するよう定義できますが、接続ごとに最大メッセージ数だけを許可します。詳細については、「メール フロー ポリシーを使用した電子メール送信者のアクセス ルールの定義」 (P.7-8) を参照してください。

[メール ポリシー (Mail Policies)] > [HAT 概要 (HAT Overview)] ページで、リスナーへの接続が許可されるホストを定義します。図 7-1 に、パブリック リスナーのデフォルトで定義された送信者グループとメール フロー ポリシーの [HAT 概要 (HAT Overview)] が表示されます。

図 7-1 [メール ポリシー (Mail Policies)] > [HAT 概要 (HAT Overview)] ページ - パブリック リスナー



リスナーが TCP 接続を受信すると、設定された送信者グループに対して送信元 IP アドレスを比較します。また、[HAT 概要 (HAT Overview)] ページにリストされている順序で送信者グループを評価します。一致が見つかり、設定済みのメール フロー ポリシーを接続に適用します。

リスナーを作成すると、AsyncOS は、リスナーに定義済みの送信者グループとメール フロー ポリシーを作成します。定義済みの送信者グループとメール フロー ポリシーを編集して新しい送信者グループとメール フロー ポリシーを作成できます。詳細については、「[定義済みの送信者グループとメール フロー ポリシーの理解](#)」(P.7-11) を参照してください。

ホストアクセス テーブルに格納されているすべての情報をファイルにエクスポートし、ファイルに格納されているホストアクセス テーブル情報をリスナー用のアプライアンスにインポートできます。このとき、設定されているすべてのホストアクセス テーブル情報は上書きされます。詳細については、「[ホストアクセス テーブルの設定の使用](#)」(P.7-21) を参照してください。

デフォルト HAT エントリ

HAT は、デフォルトでは、リスナーのタイプによって異なるアクションを実行するように定義されています。

- **パブリック リスナー。** HAT は、すべてのホストからの電子メールを受け入れるように設定されます。
- **プライベート リスナー。** HAT は、指定したホストからの電子メールをリレーし、他のすべてのホストを拒否するように設定されます。

[HAT 概要 (HAT Overview)] では、デフォルトのエントリに「ALL」という名前が付けられます。[メール ポリシー (Mail Policies)] > [HAT 概要 (HAT Overview)] ページですべての送信者グループのメール フロー ポリシーをクリックしてデフォルト エントリを編集できます。



(注)

指定したホスト以外のすべてのホストを拒否することで、`listenerconfig` コマンドと `systemsetup` コマンドでは、意図せずシステムを「オープン リレー」として設定することが防止されます。オープン リレー（「セキュアでないリレー」または「サードパーティ」リレーとも呼びます）は、第三者による電子メール メッセージのリレーを許す SMTP 電子メール サーバです。オープン リレーがあると、ローカル ユーザ向けでもローカル ユーザからでもない電子メールを処理することにより、非良心的な送信者がゲートウェイを通じて大量のスパムを送信することが可能になります。

送信者グループへのリモートホストの定義

リモートホストがリスナーに接続しようとする方法を定義できます。リモートホスト定義を送信者グループにグループ化します。送信者グループは、それらの送信者からの電子メールを処理するために定義されたリモートホストのリストです。

送信者グループは、次のもので識別される送信者のリストです。

- IP アドレス (IPv4 または IPv6)
- IP 範囲
- 具体的なホスト名またはドメイン名
- SenderBase レピュテーション サービスの「組織」分類
- SenderBase Reputation Score (SBRS; SenderBase レピュテーション スコア) の範囲 (またはスコアの欠如)
- DNS リスト クエリー応答

送信者グループの受け入れ可能なアドレスのリストの詳細については、「[送信者グループの構文](#)」(P.7-4) を参照してください。

SMTP サーバがアプライアンスとの SMTP 接続を試みると、リスナーは、送信者グループを順番に評価し、SenderBase レピュテーション スコア、ドメイン、または IP アドレスなどの送信者グループの任意の条件に一致する場合、送信者グループに接続を割り当てます。



(注)

二重 DNS ルックアップを実行することで、システムはリモートホストの IP アドレスの正当性を確保および検証します。これは、接続元ホストの IP アドレスに対する逆引き DNS (PTR) ルックアップと、それに続く PTR ルックアップ結果に対する正引き DNS (A) ルックアップからなります。その後、システムは A ルックアップの結果が PTR ルックアップの結果と一致するかどうかをチェックします。結果が一致しない場合、または A レコードが存在しない場合は、システムは IP アドレスのみを使用して HAT 内のエントリと照合します。

[メールポリシー (Mail Policies)] > [HAT 概要 (HAT Overview)] ページで送信者グループを定義します。

送信者グループの構文

表 7-1 HAT 内でのリモート ホストの定義 : 送信者グループの構文

構文	意味
n:n:n:n:n:n:n	IPv6 アドレス。先行ゼロを含める必要はありません。
n:n:n:n:n:n:n-n n:n:n:n:n:n:n n:n:n-n:n:n:n:n:n	IPv6 アドレスの範囲。先行ゼロを含める必要はありません。
n.n.n.n	フル (完全な) IPv4 アドレス
n.n.n. n.n.n n.n. n.n n. n	部分的な IPv4 アドレス
n.n.n.n-n n.n.n-n. n.n.n-n n.n-n. n.n-n n-n. n-n	IPv4 アドレスの範囲
yourhost.example.com	完全修飾ドメイン名
.partialhost	部分ホスト ドメイン内のすべてのもの
n/c n.n/c n.n.n/c n.n.n.n/c	IPv4 CIDR アドレス ブロック
n: n: n: n: n: n: n: n/c	IPv6 CIDR アドレス ブロック。先行ゼロを含める必要はありません
SBRS [n:n] SBRS [none]	SenderBase レピュテーション スコア。詳細については、「 SenderBase レピュテーション スコアを使用した送信者グループの定義 」(P.7-6) を参照してください。
SBO:n	SenderBase ネットワーク オーナー識別番号。詳細については、「 SenderBase レピュテーション スコアを使用した送信者グループの定義 」(P.7-6) を参照してください。
dnslist[dnserver.domain]	DNS リスト クエリー。詳細については、「 DNS リストにクエリーを実行することで定義された送信者グループ 」(P.7-7) を参照してください。
ALL	すべてのアドレスに一致する特殊なキーワード。これは、すべての送信者グループのみに適用され、常に含まれます (ただしリストされません)。

ネットワーク オーナー、ドメイン、IP アドレスで定義される送信者グループ

SMTP プロトコルには電子メールの送信者を認証するための方法が組み込まれていないため、大量の迷惑メールの送信者は、その身元を隠すためのいくつかの戦略を採用することに成功してきました。たとえば、メッセージのエンベロープ送信者アドレスのスプーフィング、偽造した HELO アドレスの使用、単なる異なるドメイン名のローテーションなどがあります。これにより、多数のメール管理者は、「この大量の電子メールは誰が送信しているのか」という基本的な質問を自問することになります。この質問に答えるために、SenderBase レピュテーション サービスは、接続元ホストの IP アドレスに基づいて身元ベースの情報を集約するための固有の階層を開発してきました。IP アドレスは、メッセージ中で偽造することがほとんど不可能な情報の 1 つです。

IP Address は、送信元メール ホストの IP アドレスとして定義します。電子メールセキュリティ アプライアンスは両方のインターネット プロトコルバージョン 4 (IPv4) および IP バージョン 6 (IPv6) アドレスをサポートします。

Domain は、指定した第 2 レベルドメイン名 (たとえば yahoo.com) を持つホスト名を使用するエンティティとして定義され、IP アドレスに対する逆引き (PTR) ルックアップによって決定されます。

Network Owner は、IP アドレスのブロックを管理するエンティティ (通常は会社) として定義され、American Registry for Internet Numbers (ARIN) などのグローバル レジストリやその他のソースからの IP アドレス空間の割り当てに基づいて決定されます。

Organization は、ネットワーク オーナーの IP ブロック内のメール ゲートウェイの特定のグループを最も詳細に管理するエンティティとして定義され、SenderBase によって決定されます。Organization は Network Owner、Network Owner 内の部門、その Network Owner の顧客のいずれかになります。

HAT に基づくポリシーの設定

表 7-2 に、ネットワーク オーナーと組織の例をいくつか示します。

表 7-2 ネットワーク オーナーと組織の例

例の種類	ネットワーク オーナー	組織
ネットワーク サービス プロバイダー	Level 3 Communications	Macromedia Inc. AllOutDeals.com GreatOffers.com
電子メール サービス プロバイダー	GE	GE Appliances GE Capital GE Mortgage
商用送信者	The Motley Fool	The Motley Fool

ネットワーク オーナーの規模にはかなりの幅があるため、メール フロー ポリシーの基にする適切なエンティティは組織です。SenderBase レピュテーション サービスは、電子メールの送信元について組織レベルまで独自に理解しており、Cisco アプライアンスはそれを利用して、組織に基づいてポリシーを自動的に適用します。上の例で、ユーザがホスト アクセス テーブル (HAT) で「Level 3 Communications」を送信者グループとして指定した場合、SenderBase はそのネットワーク オーナーによって管理される個別の組織に基づいてポリシーを適用します。

たとえば、上記の表で、ユーザが Level 3 に対して時間あたりの受信者数の制限を 10 と入力した場合、Cisco アプライアンスは、Macromedia Inc.、Alloutdeals.com、および Greatoffers.com に対して最大 10 人の受信者を許可します (Level 3 ネットワーク オーナーに対しては時間あたり合計 30 人の受信者

になります)。このアプローチの利点は、これらの組織のいずれかがスパムを送信し始めても、Level 3 によって管理されているその他の組織には影響がないことです。これを、ネットワーク オーナー「The Motley Fool」の例と対比します。ユーザがレート制限を時間あたり 10 個の受信者に設定した場合、ネットワーク オーナー Motley Fool の合計の制限は、時間あたり 10 個の受信者になります。

Cisco メール フロー モニタ機能は、送信者を定義する方法の 1 つであり、送信者に関するメール フロー ポリシーの決定を作成するためのモニタリング ツールとなります。特定の送信者に関するメール フロー ポリシーの決定を作成するには、次のことを質問します。

- この送信者によって、どの IP アドレスが制御されているか。

インバウンド電子メールの処理を制御するためのメール フロー モニタ機能が使用する最初の情報が、この質問に対する答えになります。この答えは、SenderBase レピュテーション サービスにクエリーを実行することで得られます。SenderBase レピュテーション サービスは、送信者の相対的な規模に関する情報を提供します (SenderBase ネットワーク オーナーまたは SenderBase 組織)。この質問に答えるにあたり、次のことが仮定されます。

- 大規模な組織は、より多くの IP アドレスを管理し、より厳格な電子メールを送信する傾向があります。
- その規模に応じて、この送信者に接続数を全体でいくつ割り当てるべきか。
 - 大規模な組織は、より多くの IP アドレスを管理し、より厳格な電子メールを送信する傾向があります。そのため、アプライアンスへの接続をより多く割り当てる必要があります。
 - 多くの場合、大量の電子メールの送信元は、ISP、NSP、アウトソーシングされた電子メールの配信を管理する企業、迷惑メールの送信元です。ISP、NSP、アウトソーシングされた電子メールの配信を管理する企業は、多数の IP アドレスを管理する組織の例であり、アプライアンスへの接続をより多く割り当てる必要があります。通常、迷惑メールの送信者は、多数の IP アドレスを管理せず、少数の IP アドレスを通じて大量のメールを送信します。このような送信者には、アプライアンスへの接続をより少なく割り当てる必要があります。

メール フロー モニタ機能は、SenderBase ネットワーク オーナーと SenderBase 組織の差別化を使用して、SenderBase 内のロジックに基づき、送信者あたりに接続を割り当てる方法を決定します。メール フロー モニタ機能の使用の詳細については、『Cisco IronPort AsyncOS for Email Daily Management Guide』の「Using Email Security Monitor」の章を参照してください。

SenderBase レピュテーション スコアを使用した送信者グループの定義

Cisco アプライアンスは、Cisco SenderBase レピュテーション サービスに対してクエリーを実行して、送信者のレピュテーション スコア (SBRs) を決定できます。SBRs は、SenderBase レピュテーション サービスからの情報に基づき、IP アドレス、ドメイン、または組織に割り当てられた数値です。スコアの範囲は、表 7-3 に示すように、-10.0 ~ +10.0 です。

表 7-3 SenderBase レピュテーション スコアの定義

スコア	意味
-10.0	スパムの送信元である可能性が最も高い
0	中間か、または推奨を行うための十分な情報がない
+10.0	信頼できる送信者である可能性が最も高い
なし	この送信者のデータがない (一般にスパムの送信元)

SBRs を使用して、信頼性に基づいてメールフローポリシーを送信者に適用するように Cisco アプリアンスを設定します。たとえば、スコアが -7.5 未満のすべての送信者を拒否することが考えられます。これは、GUI を使用して実現するのが最も簡単です。「[メッセージ処理の送信者グループの作成](#)」(P.7-13) を参照してください。エクスポートした HAT をテキストファイルで編集する場合、SenderBase レピュテーション スコアを含めるための構文については表 7-4 を参照してください。

表 7-4 SenderBase レピュテーション スコアの構文

SBRs [n:n]	SenderBase レピュテーション スコア。送信者は、SenderBase レピュテーション サービスにクエリーを実行することで識別され、スコアは範囲内で定義されます。
SBRs[none]	SBRs がいないことを指定します (非常に新しいドメインには、まだ SenderBase レピュテーション スコアがない場合があります)。



(注) GUI を通じて HAT に追加されるネットワーク オーナーは、SBO:n という構文を使用します。ここで n は、SenderBase レピュテーション サービス内のネットワーク オーナーの一意の識別番号です。

SenderBase レピュテーション サービスにクエリーを実行するようにリスナーを設定するには、[ネットワーク (Network)] > [リスナー (Listeners)] ページを使用するか、CLI で listenerconfig -> setup コマンドを使用します。また、アプリアンスが SenderBase レピュテーション サービスにクエリーを実行するときに待つタイムアウト値を定義することもできます。その後、GUI の [メールポリシー (Mail Policies)] ページの値を使用するか、CLI の listenerconfig -> edit -> hostaccess コマンドを使用して、SenderBase レピュテーション サービスに対するルックアップを使用するさまざまなポリシーを設定できます。



(注) また、SenderBase レピュテーション スコアの「しきい値」を指定するメッセージフィルタを作成し、システムによって処理されたメッセージをさらに操作することもできます。詳細については、『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「SenderBase Reputation Rule」、「Bypass Anti-Spam System Action」、および「Bypass Anti-Virus System Action」を参照してください。

DNS リストにクエリーを実行することで定義された送信者グループ

リスナーの HAT では、特定の DNS リスト サーバに対するクエリーに一致するものとして送信者グループを定義することもできます。クエリーは、リモートクライアントの接続時に DNS を通じて実行されます。リモートリストにクエリーを実行する機能は、現在メッセージフィルタルールとしても存在しますが (『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「DNS List Rule」を参照)、メッセージの内容全体が受信されるのは一度だけです。

このメカニズムにより、グループ内で、DNS リストにクエリーを実行する送信者を設定し、それに合わせてメールフローポリシーを調整できます。たとえば、接続を拒否したり、接続元ドメインの振る舞いを制限したりできます。



(注) いくつかの DNS リストは、可変の応答 (たとえば「127.0.0.1」、「127.0.0.2」、「127.0.0.3」) を使用して、クエリー対象の IP アドレスに関するさまざまな事実を示すことができます。メッセージフィルタ DNS リストルール (『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「DNS List Rule」を参照) を使用すると、クエリーの結果をさまざまな値と比較できます。しかし、HAT 内で DNS リスト サーバにクエリーを実行する指定では、簡潔にするためにブール演算のみがサポートされています (つまり、IP アドレスがリストに現れるかどうか)。



(注) CLI のクエリーでは必ず角カッコを含めます。GUI で DNS リスト クエリーを指定する場合には角カッコは不要です。クエリーのテスト、DNS クエリーの一般的な設定、または現在の DNS リスト キャッシュのフラッシュを行うには、CLI で `dnslistconfig` コマンドを使用します。

このメカニズムは、「異常な」接続に加えて、「正常な」接続を識別するためにも使用できます。たとえば、`query.bondedsender.org` に対してクエリーを実行すると、その電子メール キャンペーンの健全性を保証するために Cisco Systems の Bonded Sender™ プログラムに供託金を積んだ接続元ホストが照合されます。デフォルトの WHITELIST の送信者グループを修正して Bonded Sender プログラムの DNS サーバにクエリーを実行し（積極的に供託金を抛出したこれら正規の電子メール送信者が一覧表示されます）、それに応じてメールフローポリシーを調整することもできます。

メールフローポリシーを使用した電子メール送信者のアクセス ルールの定義

メールフローポリシーでは SMTP カンバセーション中の送信者からリスナーへの電子メールメッセージのフローを制御または制限することができます。メールフローポリシーに次のパラメータタイプを定義することで SMTP カンバセーションを制御します。

- 接続ごとの最大メッセージ数などの接続パラメータ。
- 1 時間あたりの受信者の最大数など、レート制限パラメータ。
- SMTP カンバセーション中に通信するカスタム SMTP コードと応答を変更します。
- スпам検出の有効化。
- ウイルス保護の有効化。
- TLS を使った SMTP 接続の暗号化などの暗号化。
- DKIM を使った着信メールの確認などの認証パラメータ。

最後に、メールフローポリシーが、リモートホストからの接続に対し、次のいずれかのアクションを実行します。

- **承認 (ACCEPT)**。接続が許可された後、電子メールの許可がさらに受信者アクセステーブル（パブリックリスナーの場合）などのリスナーの設定によって制限されます。
- **拒否 (REJECT)**。接続は、最初は許可されますが、接続しようとするクライアントは、4XX または 5XX SMTP のステータスコードを取得します。どの電子メールも許可されません。



(注) また、SMTP カンバセーションの開始時ではなく、メッセージ受信者レベル (RCPT TO) でこの拒否を実行するように、AsyncOS を設定できます。この方法でメッセージを拒否することで、メッセージの拒否が遅延されメッセージがバウンスするため、AsyncOS は拒否されたメッセージに関するより詳細な情報を取得できます。この設定は、CLI の `listenerconfig > setup` コマンドから設定されます。詳細については、「[CLI からのリスナーの作成による接続要求のリスン](#)」(P.5-13) を参照してください。

- **TCPREFUSE TCP** レベルで接続は拒否されます。
- **リレー (RELAY)**。接続は許可されます。すべての受信者の受信は許可され、受信者アクセステーブルで制限されません。

- **継続 (CONTINUE)**。HAT 内のマッピングが無視され、HAT の処理が継続されます。着信接続が、CONTINUE でない後続のエントリに一致する場合、代わりにそのエントリが使用されます。CONTINUE ルールは、GUI での HAT の編集を容易にするために使用されます。詳細については、「メッセージ処理の送信者グループの作成」(P.7-13) を参照してください。

HAT 変数の構文

表 7-5 では、メール フロー ポリシーに対して定義されるカスタム SMTP およびレート制限バナーと組み合わせることも使用できる変数のセットを定義します。変数名の大文字と小文字は区別されません (つまり、\$group と \$Group は同じです)。

表 7-5 HAT 変数の構文

変数	定義
\$Group	HAT 内の一致した送信者グループの名前で置き換えられます。送信者グループに名前がない場合、「None」が表示されます。
\$Hostname	Cisco アプライアンスによって検証された場合にのみ、リモート ホスト名で置き換えられます。IP アドレスの逆引き DNS ルックアップが成功したもののホスト名が返されない場合、「None」が表示されます。逆引き DNS ルックアップが失敗した場合 (DNS サーバに到達できない場合や、DNS サーバが設定されていない場合)、「Unknown」が表示されます。
\$orgid	SenderBase 組織 ID (整数値) で置き換えられます。 Cisco アプライアンスが SenderBase 組織 ID を取得できないか、SenderBase レピュテーション サービスが値を返さなかった場合、「None」が表示されます。
\$RemoteIP	リモートクライアントの IP アドレスで置き換えられます。
\$HATEntry	リモートクライアントが一致した HAT のエントリで置き換えられます。

HAT 変数の使用



(注) これらの変数は、『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「Customizing Listeners」の章の表 1-3 に示されている高度な HAT パラメータ smtp_banner_text および max_rcpts_per_hour_text とともに使用できます。

これらの変数を使用し、\$TRUSTED ポリシー内で許可された接続のカスタム SMTP バナー応答テキストを GUI で編集できます。

図 7-2 HAT 変数の使用

Rate Limiting:	Max. Recipients Per Hour:	<input checked="" type="radio"/> Unlimited <input type="radio"/> <input type="text"/>
	Max. Recipients Per Hour Code:	<input type="text" value="452"/>
	Max. Recipients Per Hour Text:	Too many recipients received this hour from Host: \$hostname

または、CLI で次のように入力します。

```
Would you like to specify a custom SMTP response? [Y]> y
```

```
Enter the SMTP code to use in the response. 220 is the standard code.
```

```
[220]> 200
```

```
Enter your custom SMTP response. Press Enter on a blank line to finish.
```

```
You've connected from the hostname: $Hostname, IP address of: $RemoteIP, matched the group: $Group, $HATEntry and the SenderBase Organization: $OrgID.
```

HAT 変数のテスト

これらの変数をテストするには、既知の信頼できるマシンの IP アドレスを、Cisco アプライアンス上のリスナーの \$WHITELIST 送信者グループに追加します。その後、そのマシンから telnet で接続します。SMTP 応答中で変数の置き換えを確認できます。次に例を示します。

```
# telnet IP_address_of_IronPort_Appliance
```

```
220 hostname ESMTTP
```

```
200 You've connected from the hostname: hostname, IP address of:
IP-address_of_connecting_machine, matched the group: WHITELIST, 10.1.1.1 the SenderBase
Organization: OrgID.
```

定義済みの送信者グループとメール フロー ポリシーの理解

表 7-6 では、パブリック リスナーの作成時に設定される定義済みの送信者グループとメール フロー ポリシーをリストします。

表 7-6 パブリック リスナー用の定義済みの送信者グループとメール フロー ポリシー

定義済みの送信者グループ	説明	デフォルトで設定されるメール フロー ポリシー
WHITELIST	信頼する送信者を WHITELIST の送信者グループに追加します。メール フロー ポリシー \$TRUSTED は、信頼できる送信者からの電子メールのレート制限をイネーブルにせず、それらの送信者からの内容をアンチスパムまたはアンチウイルス ソフトウェアでスキャンしない場合に設定します。	\$TRUSTED
BLACKLIST	BLACKLIST 送信者グループ内の送信者は拒否されます (メール フロー ポリシー \$BLOCKED で設定されたパラメータにより)。このグループに送信者を追加すると、SMTP HELO コマンドで 5XX SMTP 応答が返され、それらのホストからの接続が拒否されます。	\$BLOCKED
SUSPECTLIST	送信者グループ SUSPECTLIST には、着信メールの速度をスロットリングする (低下させる) メール フロー ポリシーが含まれています。送信者が疑わしい場合、送信者グループ SUSPECTLIST に追加することで、メール フロー ポリシーにより次のことが指示されます。 <ul style="list-style-type: none"> レート制限により、セッションあたりの最大メッセージ数、メッセージあたりの最大受信者数、最大メッセージ サイズ、リモートホストから受け付ける最大同時接続数が制限されます。 リモートホストからの時間あたりの最大受信者数は 20 に設定されます。この設定は、使用可能な最大のスロットリングであることに注意してください。このパラメータが厳しすぎる場合は、時間あたりの受信者数を増やすことができます。 メッセージの内容はアンチスパム スキャンエンジンとアンチウイルス スキャンエンジンによってスキャンされます (これらの機能がシステムでイネーブルになっている場合)。 送信者に関する詳細情報を得るために、Cisco SenderBase レピュテーション サービスに対してクエリーが実行されます。 	\$THROTTLED

表 7-6 パブリック リスナー用の定義済みの送信者グループとメール フロー ポリシー (続き)

定義済みの送信者グループ	説明	デフォルトで設定されるメール フロー ポリシー
UNKNOWNLIST	送信者グループ UNKNOWNLIST は、特定の送信者に対して使用するメール フロー ポリシーが決まっていない場合に便利です。このグループのメール フロー ポリシーでは、このグループの送信者についてメールが許可されますが、Cisco Anti-Spam ソフトウェア (システムでイネーブされている場合)、アンチウイルス スキャン エンジン、および Cisco SenderBase レピュテーション サービスをすべて使用して、送信者とメッセージの内容に関する詳細情報を取得することが指示されます。このグループに属する送信者に対するレート制限もデフォルト値を使用してイネーブになります。ウイルス スキャン エンジンの詳細については、「 アンチウイルス スキャンの概要 」(P.12-1) を参照してください。SenderBase レピュテーション サービスの詳細については、「 SenderBase レピュテーション サービス 」(P.6-1) を参照してください。	\$ACCEPTED
ALL	その他すべての送信者に適用されるデフォルトの送信者グループ。詳細については、「 デフォルト HAT エントリ 」(P.7-2) を参照してください。	\$ACCEPTED

表 7-7 では、プライベート リスナーの作成時に設定される定義済みの送信者グループとメール フロー ポリシーをリストします。

表 7-7 プライベート リスナー用の定義済みの送信者グループとメール フロー ポリシー

定義済みの送信者グループ	説明	デフォルトで設定されるメール フロー ポリシー
RELAYLIST	中継を許可する必要があることがわかっている送信者を RELAYLIST 送信者グループに追加します。メール フロー ポリシー \$RELAYED は、中継を許可する送信者からの電子メールのレート制限を行わず、それらの送信者からの内容をアンチスパム スキャン エンジンまたはアンチウイルス ソフトウェアでスキャンしない場合に設定します。 (注) RELAYLIST 送信者グループにはシステム設定 ウィザードを実行したときに電子メールのリレーが許可されるシステムが含まれます。	\$RELAYED
ALL	その他すべての送信者に適用されるデフォルトの送信者グループ。詳細については、「 デフォルト HAT エントリ 」(P.7-2) を参照してください。	\$BLOCKED



(注) Ethernet ポートが 2 つしかないアプライアンス モデル Cisco のシステム設定ウィザードを実行すると、1 人のリスナーだけを作成するように促されます。また、内部システム用のメールのリレーに使用される \$RELAYED メール フロー ポリシーも含まれるパブリック リスナーを作成します。2 つ以上のイーサネット ポートを持つ Cisco アプライアンス モデルについては、RELAYLIST 送信者グループと \$RELAYED メール フロー ポリシーがプライベート リスナーだけに表示されます。

送信者グループからのメッセージの同様の処理

リスナーが送信者からのメッセージを処理する方法を設定するには、[メール ポリシー (Mail Policies)] > [HAT 概要 (HAT Overview)] と [メール フロー ポリシー (Mail Flow Policy)] ページで行います。これは、送信者グループとメール フロー ポリシーを作成、編集、および削除することにより行います。

メッセージ処理の送信者グループの作成

手順

- ステップ 1 [メール ポリシー (Mail Policies)] > [HAT 概要 (HAT Overview)] ページに移動します。
- ステップ 2 [リスナー (Listener)] フィールドに編集するリスナーを選択します。
- ステップ 3 [送信者グループを追加 (Add Sender Group)] をクリックします。
- ステップ 4 送信者グループの名前を入力します。
- ステップ 5 送信者グループのリストに配置する順序を選択します。
- ステップ 6 (任意) たとえば、送信者グループまたはその設定についての情報などのコメントを入力します。
- ステップ 7 この送信者グループを適用するメール フロー ポリシーを選択します。



(注) このグループに適用すべきメール フロー ポリシーがわからない場合 (またはまだメール フロー ポリシーが存在しない場合) は、デフォルトの「CONTINUE (no policy)」メール フロー ポリシーを使用します。

- ステップ 8 (任意) DNS リストを選択します。
- ステップ 9 (任意) SBRS に情報が無い送信者を含めます。これは「none」と呼ばれ、一般に疑いがあることを意味します。
- ステップ 10 (任意) DNS リストを入力します。
- ステップ 11 (任意) ホスト DNS 検証設定を構成します。
詳細については、「[送信者検証の実装 — 設定例](#)」(P.7-31) を参照してください。
- ステップ 12 グループを作成し、送信者を追加するには、[送信して送信者を追加 (Submit and Add Senders)] をクリックします。
- ステップ 13 IPv4 アドレス、IPv6 アドレス、またはホスト名を使用して送信者を入力します。送信者は、IP アドレスおよびホスト名の一部の範囲を含めることができます。



(注) 1 つの送信者グループに重複するエントリ (同じドメインまたは IP アドレス) を入力すると、重複は廃棄されます。

ステップ 14 (任意) コメントを入力します。

ステップ 15 変更内容を送信し、確定します。

関連項目

- 「リスナーのレピュテーション フィルタリング スコアのしきい値の編集」 (P.6-5)

既存の送信者グループに送信者を追加できます。

手順

ステップ 1 ドメイン、IP、またはネットワーク オーナー プロファイル ページで、[送信者グループに追加 (Add to Sender Group)] リンクをクリックします。

ステップ 2 各リスナーに対して定義されているリストから送信者グループを選択します。

ステップ 3 変更内容を送信し、確定します。



(注) ドメインを送信者グループに追加すると、実際には 2 つのドメインが GUI に表示されます。たとえば、ドメイン example.net を追加した場合、[送信者グループに追加 (Add to Sender Group)] ページには、example.net と .example.net が追加されます。2 つめのエントリがあることで、example.net のサブドメイン内のすべてのホストが送信者グループに追加されます。詳細については、「送信者グループの構文」 (P.7-4) を参照してください。



(注) 送信者グループに追加しようとしている送信者の 1 つ以上がその送信者グループにすでに存在する送信者と重複する場合、重複する送信者は追加されず、確認メッセージが表示されます。

ステップ 4 [保存 (Save)] をクリックして送信者を追加し、[受信メールの概要 (Incoming Mail Overview)] ページに戻ります。

関連項目

- 「スパム フィルタからのアプライアンス生成メッセージの保護」 (P.13-13)
- 「メッセージがスパムかどうかスキャンするためのアプライアンスの設定方法」 (P.13-2)

着信接続のために実行するルールの順序の並べ替え

リスナーに送信者グループを追加すると、送信者グループの順序を編集する必要があります。

リスナーに接続しようとするホストごとに、HAT は上から下へ順番に読み込まれます。接続元ホストにルールが一致する場合、その接続に対してすぐにアクションが実行されます。

手順

-
- ステップ 1** [メール ポリシー (Mail Policies)] > [HAT 概要 (HAT Overview)] ページに移動します。
- ステップ 2** [リスナー (Listener)] フィールドに編集するリスナーを選択します。
- ステップ 3** [順番を編集 (Edit Order)] をクリックします。
- ステップ 4** HAT の送信者グループの既存の行の新しい順序を入力します。
シスコはデフォルトの順序を維持することを推奨します (RELAYLIST (特定のハードウェア モデルのみ)、WHITELIST、BLACKLIST、SUSPECTLIST、UNKNOWNLIST)。
- ステップ 5** 変更内容を送信し、確定します。
-

送信者の検索

[HAT 概要 (HAT Overview)] ページの上部にある [送信者を検索 (Find Senders)] フィールドにテキストを入力することで送信者を検索できます。検索するテキストを入力し [検索 (Find)] をクリックします。

メール フロー ポリシーを使用した着信メッセージのルールの定義

メール フロー ポリシーを作成する前に、次のルールとガイドラインを考慮してください。

- [デフォルトを使用 (Use Default)] オプション ボタンがオンの場合、ポリシーのデフォルト値はグレー表示されます。デフォルト値を上書きするには、[オン (On)] オプション ボタンを選択して機能または設定をイネーブルにし、新たにアクセス可能になった値を変更します。デフォルト値を定義するには、「[メール フロー ポリシーのデフォルト値の定義](#)」(P.7-20) を参照してください。
- 一部のパラメータは特定の事前設定値に依存します (たとえば、ディレクトリ獲得攻撃の設定を行うには、LDAP 許可クエリーを設定しておく必要があります)。

手順

-
- ステップ 1** [メール ポリシー (Mail Policies)] > [メール フロー ポリシー (Mail Flow Policies)] ページに移動します。
- ステップ 2** [ポリシーを追加 (Add Policy)] をクリックします。
- ステップ 3** [表 7-8](#) の説明に従って情報を入力します。

表 7-8 メール フロー ポリシー パラメータ

パラメータ	説明
接続	
最大メッセージ サイズ (Maximum message size)	このリスナーが許可するメッセージの最大サイズ。最大メッセージ サイズの最小値は 1 KB です。
単一 IP からの最大同時接続数 (Maximum concurrent connections from a single IP)	単一の IP アドレスからこのリスナーに接続することが許可される最大同時接続数。

表 7-8 メール フロー ポリシー パラメータ (続き)

パラメータ	説明
接続あたりの最大メッセージ数 (Maximum messages per connection)	リモート ホストからの接続に対して、このリスナーを通じて送信できる最大メッセージ数。
メッセージあたりの最大受信者数 (Maximum recipients per message)	このホストから許可されるメッセージあたりの受信者の最大数。
SMTP バナー	
カスタム SMTP バナー コード (Custom SMTP Banner Code)	このリスナーとの接続が確立されたときに返される SMTP コード。
カスタム SMTP バナー テキスト (Custom SMTP Banner Text)	このリスナーとの接続が確立されたときに返される SMTP バナー テキスト。 (注) このフィールドには一部の変数を使用できます。詳細については、「 HAT 変数の構文 」(P.7-9) を参照してください。
カスタム SMTP 拒否バナーコード (Custom SMTP Reject Banner Code)	このリスナーにより接続が拒否されたときに返される SMTP コード。
カスタム SMTP 拒否バナーテキスト (Custom SMTP Reject Banner Text)	このリスナーにより接続が拒否されたときに返される SMTP バナー テキスト。
SMTP バナー ホスト名を上書き (Override SMTP Banner Host Name)	デフォルトでは、SMTP バナーをリモート ホストに表示するときに、リスナーのインターフェイスに関連付けられているホスト名が含まれます (たとえば、220- <i>hostname</i> ESMTPL)。ここに異なるホスト名を入力することで、このバナーを変更できます。また、ホスト名フィールドを空白のままにすることで、ホスト名をバナーに表示しないこともできます。
ホストのレート制限	
1 時間あたりの最大受信者数 (Max. Recipients per Hour)	このリスナーが 1 台のリモート ホストから受信する、時間あたりの最大受信者数。送信者 IP アドレスあたりの受信者の数は、グローバルに追跡されます。各リスナーは各レート制限のしきい値を追跡します。ただし、すべてのリスナーは単一のカウンタに対して検証するので、同じ IP アドレス (送信者) が複数のリスナーに接続されるとレート制限を超える可能性が高くなります。 (注) このフィールドには一部の変数を使用できます。詳細については、「 HAT 変数の構文 」(P.7-9) を参照してください。
時間コードあたりの最大受信者数 (Max. Recipients per Hour Code)	ホストが、このリスナーに対して定義されている時間あたりの最大受信者数を超えた場合に返される SMTP コード。
1 時間あたりの最大受信者数の超過テキスト (Max. Recipients Per Hour Exceeded Text)	ホストが、このリスナーに対して定義されている時間あたりの最大受信者数を超えた場合に返される SMTP バナー テキスト。
送信者のレート制限	

表 7-8 メール フロー ポリシー パラメータ (続き)

パラメータ	説明
時間間隔あたりの最大受信者数 (Max. Recipients per Time Interval)	このリスナーがメール送信者アドレスに基づいて一義的なエンベロープ送信者から受信する指定した期間中の最大受信者数はグローバルに追跡されます。各リスナーは各レート制限のしきい値を追跡します。ただし、すべてのリスナーは単一のカウンタに対して検証するので、同じメール送信者アドレスからのメッセージが複数のリスナーによって受信されるとレート制限を超える可能性が高くなります。 デフォルトの最大受信者数を使用するか、無制限の受信者を許可するか、または別の最大受信者数を指定するか選択します。 他のメール フロー ポリシーによってデフォルトで使用される、最大受信者数と時間間隔を指定するデフォルトのメール フロー ポリシー設定を使用します。時間間隔はデフォルトのメール フロー ポリシーを使用してしか指定できません。
送信者のレート制限超過エラー コード (Sender Rate Limit Exceeded Error Code)	SMTP コードは、エンベロープがこのリスナーに対して定義された時間間隔の最大受信者数を超えた場合に返されます。
送信者のレート制限超過エラー テキスト (Sender Rate Limit Exceeded Error Text)	SMTP バナー テキストは、エンベロープの送信者がこのリスナーに対して定義された時間間隔の最大受信者数を超えた場合に返されます。
例外 (Exceptions)	特定のエンベロープ送信者を定義されているレート制限から免除する場合は、そのエンベロープ送信者を含むアドレス リストを選択します。詳細については、「 着信接続ルールへの送信者アドレス リストの使用 」(P.7-22) を参照してください。
フロー制御	
フロー制御に SenderBase を使用 (Use SenderBase for Flow Control)	このリスナーに対する Cisco SenderBase 情報サービスでの「検索」をイネーブルにします
IP アドレスの類似性でグループ化：(有効ビット範囲 0 ~ 32) (Group by Similarity of IP Addresses: (significant bits<1/> 0-32))	リスナーのホスト アクセス テーブル (HAT) 内のエントリを大規模な CIDR ブロックで管理しつつ、IP アドレスごとに着信メールを追跡およびレート制限するために使用します。レート制限のために類似の IP アドレスをグループ化するための有効ビットの範囲 (0 ~ 32) を定義しつつ、その範囲内の IP アドレスごとに個別のカウンタを保持します。「Use SenderBase」をディセーブルにする必要があります。HAT の有効ビットの詳細については、『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「Configuring Routing and Delivery Features」の章の「HAT Significant Bits Feature」を参照してください。

表 7-8 メール フロー ポリシー パラメータ (続き)

パラメータ	説明
ディレクトリ獲得攻撃防御 (DHAP)	
ディレクトリ獲得攻撃防御 : 1 時間あたりの無効な受信者の最大数 (Directory Harvest Attack Prevention: Maximum Invalid Recipients Per Hour)	このリスナーがリモート ホストから受け取る無効な受信者の 1 時間あたりの最大数です。このしきい値は、RAT 拒否と SMTP コールアヘッドサーバプロファイル拒否の総数を表します。これは、無効な LDAP 受信者宛てのため SMTP カンバセーション中にドロップされたメッセージの総数と、ワーク キュー内でバウンスされたメッセージの合計です (関連付けられたリスナーの LDAP 承認設定に設定されたとおり)。LDAP 許可クエリーの DHAP の設定の詳細については、『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「LDAP Queries」を参照してください。
ディレクトリ獲得攻撃防御 : SMTP 対話内で DHAP しきい値に到達した場合、接続をドロップ (Directory Harvest Attack Prevention: Drop Connection if DHAP threshold is Reached within an SMTP Conversation)	Cisco アプライアンスは、無効な受信者のしきい値に達するとホストへの接続をドロップします。
Max. 時間コードあたりの無効な受信者の最大数 (Invalid Recipients Per Hour Code) :	接続をドロップするときに使用するコードを指定します。デフォルトのコードは 550 です。
Max. 時間テキストあたりの無効な受信者の最大数 (Invalid Recipients Per Hour Text) :	ドロップした接続に対して使用するテキストを指定します。デフォルトのテキストは「Too many invalid recipients」です。
SMTP 対話内で DHAP しきい値に到達した場合、接続をドロップ (Drop Connection if DHAP threshold is reached within an SMTP Conversation)	SMTP カンバセーション中に DHAP しきい値に達した場合の接続のドロップをイネーブルにします。
Max. 時間コードあたりの無効な受信者の最大数 (Invalid Recipients Per Hour Code) :	SMTP カンバセーション中の DHAP により接続をドロップするときに使用するコードを指定します。デフォルトのコードは 550 です。
Max. 時間テキストあたりの無効な受信者の最大数 (Invalid Recipients Per Hour Text) :	SMTP カンバセーション中の DHAP により接続をドロップするときに使用するテキストを指定します。
スパム検出	
アンチスパム スキャン (Anti-spam scanning)	このリスナー上でアンチスパム スキャンをイネーブルにします。
ウイルス検出	
アンチウイルス スキャン (Anti-virus scanning)	このリスナー上でアンチウイルス スキャンをイネーブルにします。

表 7-8 メールフローポリシーパラメータ (続き)

パラメータ	説明
暗号化と認証 (Encryption and Authentication)	
TLS	<p>このリスナーに対する SMTP カンバセーションのトランスポート レイヤセキュリティ (TLS) を拒否、推奨、必須します。</p> <p>[推奨 (Preferred)] を選択すると、ドメインおよび電子メールアドレスを指定するアドレス リストを選択することによって、特定のドメインまたは特定の電子メールアドレスを持つドメインのエンベロープ送信者に対して TLS を必須に設定できます。このリストのドメインまたはアドレスに一致するエンベロープ送信者が TLS を使用しない接続経路でメッセージを送信しようとする、アプライアンスは接続を拒否し、送信者は再び TLS を使用して送信を試みる必要があります。</p> <p>[クライアント証明書の検証 (Verify Client Certificate)] オプションは、クライアント認証が有効な場合、電子メールセキュリティアプライアンスがユーザのメールアプリケーションと TLS 接続を確立するように指示します。TLS 推奨設定にこのオプションを選択した場合、ユーザが証明書を持たない場合にもアプライアンスは非 TLS 接続を許可しますが、ユーザが無効な証明書を持つ場合は、接続を拒否します。TLS 必須設定の場合、このオプションを選択すると、アプライアンスが接続を許可するために有効な証明書が必要になります。</p> <p>アドレスリストの作成の詳細については、参照して「着信接続ルールへの送信者アドレスリストの使用」(P.7-22) ください。</p> <p>TLS 接続のクライアント証明書を使用する方法については、「アプライアンスからの TLS 接続の確立」(P.23-53) を参照してください。</p>
SMTP 認証 (SMTP Authentication)	リスナーに接続するリモート ホストからの SMTP 認証を許可、禁止、義務付けます。SMTP 認証については、『 <i>Cisco IronPort AsyncOS for Email Advanced Configuration Guide</i> 』の章の「LDAP Queries」で詳細を説明します。
TLS と SMTP 認証の両方が有効化されている場合: (If Both TLS and SMTP Authentication are enabled:)	TLS に SMTP 認証を提供するよう義務付けます。
DomainKeys 署名 (Domain Key Signing)	
ドメイン キー / DKIM 署名 (Domain Key/ DKIM Signing)	このリスナーでドメイン キーまたは DKIM 署名を有効にします。(承認およびリレーのみ)。
DKIM の検証 (DKIM Verification)	DKIM 検証をイネーブルにします。
SPF/SIDF の検証 (SPF/SIDF Verification)	
SPF/SIDF 検証をイネーブルにする (Enable SPF/SIDF Verification)	このリスナーで SPF/SIDF 署名をイネーブルにします。詳細については、『 <i>Cisco IronPort AsyncOS for Email Advanced Configuration Guide</i> 』の「Email Authentication」の章を参照してください。
準拠レベル (Conformance Level)	SPF/SIDF 準拠レベルを設定します。[SPF]、[SIDF]、[SIDF Compatible] のいずれかを選択します。詳細については、『 <i>Cisco IronPort AsyncOS for Email Advanced Configuration Guide</i> 』の「Email Authentication」の章を参照してください。

表 7-8 メールフロー ポリシー パラメータ (続き)

パラメータ	説明
「Resent-Sender:」または「Resent-From:」を使用した場合、PRA 検証結果をダウングレードする: (Downgrade PRA verification result if 'Resent-Sender:' or 'Resent-From:' were used:)	準拠レベルとして [SIDF 互換 (SIDF Compatible)] を選択した場合、メッセージ中に Resent-Sender: ヘッダーまたは Resent-From: ヘッダーが存在する場合に、PRA Identity 検証の結果 Pass を None にダウングレードするかどうかを設定します。このオプションはセキュリティ目的で選択します。
HELO テスト (HELO Test)	HELO ID に対してテストを実行するかどうかを設定します ([SPF] および [SIDF 互換 (SIDF Compatible)] 準拠レベルで使用します)。
タグなしバウンス (Untagged Bounces)	
タグなしバウンスを有効と見なす (Consider Untagged Bounces to be Valid)	バウンス検証タギング (の『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』「Configuring Routing and Delivery Features」の章で説明する) がイネーブルになっている場合にだけ適用されます。デフォルトでは、アプライアンスはタグのないバウンスを無効とみなし、バウンス検証の設定に応じて、バウンスを拒否するか、カスタム ヘッダーを追加します。タグの付いていないバウンスを有効とみなすことを選択した場合、アプライアンスはバウンスメッセージを受け入れます。
エンベロープ送信者の DNS 検証 (Envelope Sender DNS Verification)	
	「送信者の検証」(P.7-28) を参照してください。
例外テーブル (Exception Table)	
例外テーブルの使用 (Use Exception Table)	送信者検証ドメイン例外テーブルを使用します。例外テーブルは 1 つだけ使用できますが、メールフロー ポリシーごとにイネーブルにできます。詳細については、「送信者検証例外テーブル」(P.7-30) を参照してください。



(注) アンチスパムまたはアンチウイルス スキャンが HAT でグローバルにイネーブルの場合、メッセージはアンチスパムまたはアンチウイルス スキャンのために Cisco アプライアンスによって受け入れられると同時にフラグが付けられます。メッセージを許可した後にアンチスパムまたはアンチウイルス スキャンがディセーブルにされた場合、メッセージは、ワーク キューを出るときに引き続きスキャン対象になります。

ステップ 4 変更内容を送信し、確定します。

メールフローポリシーのデフォルト値の定義

手順

- ステップ 1** [メール ポリシー (Mail Policies)] > [メールフローポリシー (Mail Flow Policies)] をクリックします。
- ステップ 2** [リスナー (Listener)] フィールドに編集するリスナーを選択します。

- ステップ 3** 設定したメール フロー ポリシーの下の [デフォルト ポリシー パラメータ (Default Policy Parameters)] リンクをクリックします。
- ステップ 4** このリスナーのすべてのメール フロー ポリシーで使用するデフォルト値を定義します。
プロパティの詳細については、「[メール フロー ポリシーを使用した着信メッセージのルールの定義 \(P.7-15\)](#)」を参照してください。
- ステップ 5** 変更内容を送信し、確定します。

ホスト アクセス テーブルの設定の使用

ホストアクセス テーブルに格納されているすべての情報をファイルにエクスポートし、ファイルに格納されているホストアクセス テーブル情報をリスナー用のアプライアンスにインポートできます。このとき、既存のすべてのホストアクセス テーブル情報は上書きされます。

外部ファイルへの ホスト アクセス テーブル設定のエクスポート

手順

- ステップ 1** [メール ポリシー (Mail Policies)] > [HAT 概要 (HAT Overview)] ページに移動します。
- ステップ 2** [リスナー (Listener)] メニューで編集するリスナーを選択します。
- ステップ 3** [HAT をエクスポート (Export HAT)] をクリックします。
- ステップ 4** エクスポートする HAT のファイル名を入力します。これは、アプライアンスの設定ディレクトリに作成されるファイルの名前になります。
- ステップ 5** 変更内容を送信し、確定します。

外部ファイルからのホスト アクセス テーブル設定のインポート

HAT をインポートすると、既存のすべての HAT エントリが現在の HAT から削除されます。

手順

- ステップ 1** [メール ポリシー (Mail Policies)] > [HAT 概要 (HAT Overview)] ページに移動します。
- ステップ 2** [リスナー (Listener)] メニューで編集するリスナーを選択します。
- ステップ 3** [HAT をインポート (Import HAT)] をクリックします。
- ステップ 4** リストからファイルを選択します。



(注) インポートするファイルは、アプライアンスの configuration ディレクトリに存在する必要があります。

ステップ 5 [送信 (Submit)] をクリックします。既存のすべての HAT エントリを削除することを確認する警告メッセージが表示されます。

ステップ 6 [インポート (Import)] をクリックします。

ステップ 7 変更内容を確定します。

ファイルには「コメント」を格納できます。文字「#」で始まる行はコメントと見なされ、AsyncOS によって無視されます。次の例を参考にしてください。

```
# File exported by the GUI at 20060530T215438
```

```
$BLOCKED
```

```
REJECT {}
```

```
[ ... ]
```

着信接続ルールへの送信者アドレス リストの使用

メールフローポリシーは、レート制限の除外、および必須 TLS 接続などのエンベロープ送信者グループに適用する特定の設定にアドレスリストを使用できます。アドレスリストは、電子メールアドレス、ドメイン、部分ドメインおよび IP アドレスで構成できます。GUI で [メールポリシー (Mail Policies)] > [アドレスリスト (Address Lists)] のページを使用するか、または CLI の `addresslistconfig` コマンドを使用し、アドレスリストを作成できます。[アドレスリスト (Address Lists)] のページには、アドレスリストを使用するメールフローポリシーとともに、アプライアンスのすべてのアドレスリストが表示されます。

手順

ステップ 1 [メールポリシー (Mail Policies)] > [アドレスリスト (Address Lists)] を選択します。

ステップ 2 [アドレスリストの追加 (Add Address List)] をクリックします。

ステップ 3 アドレスリストの名前を入力します。

ステップ 4 アドレスリストの説明を入力します。

ステップ 5 追加するアドレスを入力します。次の形式を使用できます。

- 完全な電子メールアドレス : `user@example.com`
- 電子メールアドレスの一部 : `user@`
- 電子メールアドレスの IP アドレス : `@[1.2.3.4]`
- ドメインのすべてのユーザ : `@example.com`
- 部分ドメインのすべてのユーザ : `@.example.com`

ドメインおよび IP アドレスは @ 文字で開始する必要があることに注意してください。

カンマで電子メールアドレスを区切ります。新しい行を使ってアドレスを区切る場合、AsyncOS は自動的にエントリをカンマで区切られたリストに変換します。

ステップ 6 変更内容を送信し、確定します。

SenderBase 設定とメール フロー ポリシー

アプライアンスへの接続を分類し、メール フロー ポリシーを適用するには（レート制限が含まれる場合と含まれない場合がある）、リスナーは次の方法を使用します。

[分類 (Classification)] -> [送信者グループ (Sender Group)] -> [メール フロー ポリシー (Mail Flow Policy)] -> [レート制限 (Rate Limiting)]

詳細については、「[ネットワーク オーナー、ドメイン、IP アドレスで定義される送信者グループ \(P.7-5\)](#)」を参照してください。

「分類 (Classification)」段階では、送信側ホストの IP アドレスを使用して、(パブリック リスナーで受信した) 受信 SMTP セッションを送信者グループに分類します。送信者グループに関連付けられたメール フロー ポリシーには、レート制限をイネーブルにするパラメータがあります。(レート制限によって、セッションごとのメッセージの最大数、メッセージごとの受信者の最大数、メッセージの最大サイズ、リモート ホストから受け入れる同時接続の最大数が制限されます)。

通常、このプロセスでは、対応する名前の送信者グループの各送信者に対して受信者をカウントします。同じ時間帯に複数の送信者からメールを受信した場合、すべての送信者に対する受信者の合計数が制限値と比較されます。

このカウント方法には、次に示すいくつかの例外があります。

- ネットワーク オーナーによって分類が行われた場合、SenderBase レピュテーション サービスによってアドレスの大きなブロックが小さなブロックに自動的に分割されます。
このような小さな各ブロックに対して、受信者と受信者レート制限のカウントが別々に実行されず (通常、/24 CIDR ブロックと同じですが、必ずしも同じではありません)。
- HAT Significant Bits 機能を使用する場合について説明します。この場合、ポリシーに関連付けられた significant bits パラメータを適用して、大きなブロックのアドレスが小さなブロックに分割されます。

このパラメータは [メール フロー ポリシー (Mail Flow Policy)] -> [レート制限 (Rate Limiting)] フェーズに関連しています。送信者グループの IP アドレスの分類に使用する「network/bits」CIDR 表記法は、「bits」フィールドとは異なります。

デフォルトでは、SenderBase レピュテーション フィルタおよび IP プロファイリングのサポートが、パブリック リスナーに対してはイネーブルで、プライベート リスナーに対してはディセーブルです。

SenderBase クエリーのタイムアウト

リスナーを設定する場合、SenderBase レピュテーション サービスでクエリーを実行した情報をアプライアンスがキャッシュする時間を指定できます。その後、メール フロー ポリシーを設定する場合、SenderBase をイネーブルにし、メールのフローをリスナーに制御できます。

メール フロー ポリシーを設定する場合、[フロー制御に SenderBase を使用 (Use SenderBase for Flow Control)] 設定を使用した GUI のメール フロー ポリシーか、または `listenerconfig > hostaccess > edit` コマンドを使用した CLI で SenderBase をイネーブルにします。

HAT Significant Bits 機能

AsyncOS の 3.8.3 リリース以降では、大きな CIDR ブロック内のリスナーのホスト アクセス テーブル (HAT) の送信者グループ エントリを管理しながら、IP アドレス単位で受信メールの追跡およびレート制限を実行できます。たとえば、着信接続がホスト「10.1.1.0/24」と一致した場合、すべてのトラフィックを 1 つの大きなカウンタに集約するのではなく、範囲内の個別のアドレスに対してカウンタが生成されます。



(注) HAT ポリシーの significant bits オプションを有効にするには、HAT フロー制御オプションの「User SenderBase」をディセーブルにする必要があります (または、CLI の場合、listenerconfig -> setup コマンドで SenderBase 情報サービスをイネーブルにするための質問「Would you like to enable SenderBase Reputation Filters and IP Profiling support?」に **no** と回答します)。つまり、Hat Significant Bits 機能と SenderBase IP プロファイリング サポートのイネーブル化は相互に排他的です。

ほとんどの場合、この機能を使用して送信者グループを広く定義し (つまり、「10.1.1.0/24」や「10.1.0.0/16」のような IP アドレスの大きなグループ)、IP アドレスの小さなグループにメール フロー レート制限を狭く適用します。

HAT Significant Bits 機能は、次のようなシステムのコンポーネントに対応します。

HAT 設定

HAT の設定には、送信者グループとメール フロー ポリシーの 2 つの部分があります。送信者グループの設定では、送信者の IP アドレスの「分類」(送信者グループに入れる) 方法を定義します。メール フロー ポリシー設定では IP アドレスからの SMTP セッションの管理方法を定義します。この機能を使用すると、IP アドレスは「CIDR ブロックで分類された」(たとえば、10.1.1.0/24) 送信者グループとなり、個々のホスト (/32) として制御されます。これは「significant_bits」ポリシー設定を使用して実行されます。

Significant Bits HAT ポリシー オプション

HAT 構文では significant_bits 設定オプションを使用できます。HAT でデフォルト メール フロー ポリシーまたは特定のメール フロー ポリシーを編集する場合 (たとえば、listenerconfig -> edit -> hostaccess -> default コマンドを発行する場合)、次のような質問が表示されます。

- レート制限がイネーブルになっているか
 - フロー制御のための SenderBase の使用がディセーブルになっているか
 - Directory Harvest Attack Prevention (DHAP ディレクトリ ハーベスト攻撃防止) がメール フロー ポリシー (デフォルト メール フロー ポリシーまたは特定のメール フロー ポリシー) に対してイネーブルになっているか

次に例を示します。

```
Do you want to enable rate limiting per host? [N]> y
```

```
Enter the maximum number of recipients per hour from a remote host.
```

```
[ ]> 2345
```

Would you like to specify a custom SMTP limit exceeded response? [Y]> n

Would you like to use SenderBase for flow control by default? [N]> n

Would you like to group hosts by the similarity of their IP addresses? [N]> y

Enter the number of bits of IP address to treat as significant, from 0 to 32.

[24]>

また、この機能は [メール ポリシー (Mail Policies)] > [メール フロー ポリシー (Mail Flow Policies)] ページの GUI にも表示されます。

図 7-3 HAT Significant Bits 機能のイネーブル化

Rate Limiting:	Max. Recipients Per Hour:	<input checked="" type="radio"/> Unlimited <input type="radio"/> []
	Max. Recipients Per Hour Code:	452
	Max. Recipients Per Hour Text:	Too many recipients received this hour
Flow Control:	Use SenderBase for Flow Control:	<input checked="" type="radio"/> On <input type="radio"/> Off
	Group by Similarity of IP Addresses:	This Feature can only be used if Senderbase Flow Control is off. <input type="radio"/> Off <input type="radio"/> [] (significant bits 0-32)

フロー制御に SenderBase を使用するオプションが [オフ (OFF)] になっているか、または [ディレクトリ ハーベスト攻撃防止 (Directory Harvest Attack Prevention)] がイネーブルになっている場合、「significant bits」値は、接続している送信者の IP アドレスに適用され、結果的に CIDR 表記法が、HAT 内の定義済みの送信者グループと一致させるためのトークンとして使用されます。CIDR ブロックで囲まれた一番右のビットは、文字列の作成時に「ゼロ設定」になります。そのため、接続が IP アドレス 1.2.3.4 から確立され、significant_bits オプションが 24 に設定されたポリシーと一致する場合、結果として生じる CIDR ブロックは 1.2.3.0/24 になります。この機能を使用すると、HAT 送信者グループ エントリ (たとえば、10.1.1.0/24) には、グループに割り当てられたポリシー内の有効ビット エントリ (上記の例では、32) とは異なる数のネットワーク有効ビット (24) が存在する可能性があります。

インジェクション制御期間

インジェクション制御カウンタがリセットされた場合に調整できるグローバル設定オプションがあります。多数の IP アドレスのカウンタを管理している非常にビジーなシステムの場合、カウンタをより頻繁に (たとえば、60 分間隔ではなく 15 分間隔で) リセットするように設定します。これにより、データが管理不能なサイズにまで増大したり、システムのパフォーマンスに影響を与えたりすることを回避できます。

現在のデフォルト値は 3600 秒 (1 時間) です。最小 1 分 (60 秒) から最大 4 時間 (14,400 秒) までの期間を指定できます。

GUI でグローバル設定を使用してこの期間を調整します (詳細については、「リスナーのグローバル設定」(P.5-5) を参照してください)。

また、CLI の `listenerconfig -> setup` コマンドを使用してこの期間を調整することもできます。

```
mail3.example.com> listenerconfig
```

```
Currently configured listeners:
```

1. InboundMail (on PublicNet, 192.168.2.1) SMTP TCP Port 25 Public
2. OutboundMail (on PrivateNet, 192.168.1.1) SMTP TCP Port 25 Private

```
Choose the operation you want to perform:
```

- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.

```
[>] setup
```

```
Enter the global limit for concurrent connections to be allowed across all listeners.
```

```
[300]>
```

```
Enter the global limit for concurrent TLS connections to be allowed across all listeners.
```

```
[100]>
```

```
Enter the maximum number of message header lines. 0 indicates no limit.
```

```
[1000]>
```

1. Allow SenderBase to determine cache time (Recommended)
2. Don't cache SenderBase data.
3. Specify your own cache time.

```
[1]> 3
```

Enter the time, in seconds, to cache SenderBase data:

[300]>

Enter the rate at which injection control counters are reset.

[1h]> 15m

Enter the timeout for unsuccessful inbound connections.

[5m]>

Enter the maximum connection time for inbound connections.

[15m]>

What hostname should Received: headers be stamped with?

1. The hostname of the Virtual Gateway(tm) used for delivering the message
2. The hostname of the interface the message is received on

[2]>

The system will always add a Message-ID header to outgoing messages that don't already have one. Would you like to do the same for incoming messages? (Not recommended.) [N]>

By default connections with a HAT REJECT policy will be closed with a banner message at the start of the SMTP conversation. Would you like to do the rejection at the message recipient level instead for more detailed logging of rejected mail? [N]>

Currently configured listeners:

1. InboundMail (on PublicNet, 192.168.2.1) SMTP TCP Port 25 Public
2. OutboundMail (on PrivateNet, 192.168.1.1) SMTP TCP Port 25 Private

[1]>

送信者の検証

スパムや無用なメールは、多くの場合、DNS で解決できないドメインまたは IP アドレスを持つ送信者によって送信されます。DNS 検証とは、送信者に関する信頼できる情報を取得し、それに従ってメールを処理することを意味します。SMTP カンバセーションの前に送信者検証 (送信者の IP アドレスの DNS ルックアップに基づく接続のフィルタリング) を行うことは、Cisco アプライアンス上のメールパイプラインを介して処理されるジャンクメールの量を減らすことにも役立ちます。

未検証の送信者からのメールは自動的に廃棄されます。代わりに、AsyncOS には、未検証の送信者からのメールを処理する方法を決定する送信者検証設定があります。たとえば、SMTP カンバセーションの前に未検証の送信者からのすべてのメールを自動的にブロックしたり、未検証の送信者をスロットリングしたりするように Cisco アプライアンスを設定できます。

送信者検証機能は、次のコンポーネントで構成されます。

- **接続ホストの検証 (Verification of the connecting host)**。これは、SMTP カンバセーションの前に実行されます。詳細については、「[送信者検証：ホスト](#)」(P.7-28) を参照してください。
- **エンベロープ送信者のドメイン部分の検証 (Verification of the domain portion of the envelope sender)**。これは SMTP カンバセーションの中で実行されます。詳細については、「[送信者検証：エンベロープ送信者](#)」(P.7-29) を参照してください。

送信者検証：ホスト

送信者が未検証となる理由にはさまざまなものがあります。たとえば、DNS サーバが「ダウン」または応答しないか、ドメインが存在しないことが考えられます。送信者グループのホスト DNS 検証設定では、SMTP カンバセーションの前に未検証の送信者を分類し、さまざまな種類の未検証の送信者をさまざまな送信者グループに含めることができます。

Cisco アプライアンスは、着信メールについて、DNS を通じて接続元ホストの送信元ドメインを検証しようとしています。この検証は、SMTP カンバセーションの前に実行されます。ダブル DNS ルックアップの実行によって、リモートホストの IP アドレス (つまり、ドメイン) が取得され、有効性が検証されます。二重の DNS ルックアップは、接続元ホストの IP アドレスに対する逆引き DNS (PTR) ルックアップと、その後の PTR ルックアップの結果に対する正引き DNS (A) ルックアップからなります。その後、アプライアンスは A ルックアップの結果が PTR ルックアップの結果と一致するかどうかをチェックします。PTR ルックアップまたは A ルックアップが失敗するか、結果が一致しない場合、システムは IP アドレスのみを使用して HAT 内のエントリを照合し、送信者は未検証と見なされます。

未検証の送信者は、次のカテゴリに分類されます。

- 接続元ホストの PTR レコードが DNS に存在しない。
- DNS の一時的な障害により接続元ホストの PTR レコードのルックアップに失敗した。
- 接続元ホストの逆引き DNS ルックアップ (PTR) が正引き DNS ルックアップ (A) に一致しない。

送信者グループの [接続ホストの DNS 検証 (Connecting Host DNS Verification)] 設定を使用して、未検証の送信者に対する動作を指定できます («[送信者グループ SUSPECTLIST を使用した未検証の送信者からのメッセージのスロットリング](#)」(P.7-31) を参照)。

すべての送信者グループの送信者グループ設定でホスト DNS 検証をイネーブルにできますが、ホスト DNS 検証設定を送信者グループに追加するという事は、そのグループに未検証の送信者を含めることになるという点に注意してください。つまり、スパムやその他の無用なメールが含まれることとなります。そのため、これらの設定は、送信者を拒否またはスロットリングする送信者グループに対してのみイネーブルにすることを推奨します。たとえば、送信者グループ WHITELIST に対して DNS 検証を

イネーブルにすると、未検証の送信者からのメールが、WHITELIST 内の信頼できる送信者からのメールと同じように扱われることを意味します (メールフロー ポリシーの設定内容に応じて、アンチスパムまたはアンチウイルス チェック、レート制限などのバイパスを含みます)。

送信者検証 : エンベロープ送信者

エンベロープ送信者検証を使用すると、エンベロープ送信者のドメイン部分が DNS で検証されます (エンベロープ送信者のドメインが解決されるか。エンベロープ送信者のドメインの A レコードまたは MX レコードが DNS に存在するか)。タイムアウトや DNS サーバの障害など、DNS でのルックアップで一時的なエラー条件が発生した場合、ドメインは解決されません。これに対し、ドメインをルックアップしようとしたときに明確な「domain does not exist」ステータスが返された場合、ドメインは存在しません。この検証が SMTP カンパセーションの中で実行されるのに対し、ホスト DNS 検証はカンパセーションが開始される前に実行され、接続元 SMTP サーバの IP アドレスに適用されます。

詳細 : AsyncOS は、送信者のアドレスのドメインに対して MX レコードクエリーを実行します。次に AsyncOS は、MX レコードのルックアップの結果に基づいて、A レコードのルックアップを行います。DNS サーバが「NXDOMAIN」(このドメインのレコードがない) を返した場合、AsyncOS はそのドメインが存在しないものとして扱います。これは「Envelope Senders whose domain does not exist」のカテゴリに分類されます。NXDOMAIN は、ルート ネーム サーバがこのドメインの権威ネームサーバを提供していないことを意味する場合があります。

しかし、DNS サーバが「SERVFAIL」を返した場合、「Envelope Senders whose domain does not resolve」として分類されます。SERVFAIL は、ドメインが存在するものの、DNS にレコードのルックアップで一時的な問題があることを意味します。

スパマーなどの不法なメール送信者が使用する一般的な手法は、MAIL FROM 情報 (エンベロープ送信者内) を偽造し、受け付けられた未検証の送信者からのメールが処理されるようにすることです。これにより、MAIL FROM アドレスに送信されたバウンス メッセージが配信不能になるため、問題が生じる可能性があります。エンベロープ送信者検証を使用すると、不正な形式の (ただし空白ではない) MAIL FROM を拒否するように Cisco アプライアンスを設定できます。

各メールフロー ポリシーで、次のことが可能です。

- エンベロープ送信者の DNS 検証をイネーブルにする。
- 不正な形式のエンベロープ送信者に対し、カスタム SMTP コードと応答を渡す。エンベロープ送信者の DNS 検証をイネーブルにした場合、不正な形式のエンベロープ送信者はブロックされます。
- 解決されないエンベロープ送信者ドメインに対しカスタム応答を渡す。
- DNS に存在しないエンベロープ送信者ドメインに対しカスタム応答を渡す。

送信者検証例外テーブルを使用して、ドメインまたはアドレスのリストを格納し、そこからのメールを自動的に許可または拒否することができます (「送信者検証例外テーブル」(P.7-30) を参照)。送信者検証例外テーブルは、エンベロープ送信者検証とは独立してイネーブルにできます。そのため、たとえば、例外テーブルで指定した特別なアドレスやドメインを、エンベロープ送信者検証をイネーブルにすることなく拒否できます。また、内部ドメインまたはテスト ドメインからのメールを、他の方法で検証されない場合でも常に許可することもできます。

ほとんどのスパムは未検証の送信者から受信されますが、未検証の送信者からのメールを受け付けることが必要な理由があります。たとえば、すべての正規の電子メールを DNS ルックアップで検証できるわけではありません。一時的な DNS サーバの問題により送信者を検証できないことがあります。

未検証の送信者からのメール送信が試みられた場合、送信者検証例外テーブルとメールフロー ポリシーのエンベロープ送信者 DNS 検証設定を使用して、SMTP カンパセーション中にエンベロープ送信者が分類されます。たとえば、DNS に存在しないために検証されない送信元ドメインからのメールを

受け付けてスロットリングすることができます。いったんそのメールを受け付けた後、MAIL FROM の形式が不正なメッセージは、カスタマイズ可能な SMTP コードと応答で拒否されます。これは SMTP カンバセーションの中で実行されます。

任意のメール フロー ポリシーに対し、メール フロー ポリシー設定中で、エンベロープ送信者の DNS 検証 (ドメイン例外テーブルを含む) をイネーブルにできます。これには、GUI または CLI (`listenerconfig -> edit -> hostaccess -> <policy>`) を使用します。

部分ドメイン、デフォルト ドメイン、不正な形式の MAIL FROM

エンベロープ送信者検証をイネーブルにするか、リスナーの SMTP アドレス解析オプションで部分ドメインの許可をディセーブルにすると (『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「Customizing Listeners」の章の「SMTP Address Parsing Options」の項を参照)、そのリスナーのデフォルト ドメイン設定は使用されなくなります。

これらの機能は互いに排他的です。

カスタム SMTP コードと応答

エンベロープ送信者の形式が不正なメッセージ、DNS に存在しないエンベロープ送信者、DNS クエリーで解決できない (DNS サーバがダウンしているなど) エンベロープ送信者に対し、SMTP コードと応答メッセージを指定できます。

SMTP 応答には変数 `$EnvelopeSender` を含めることができます。これは、カスタム応答を送信するときエンベロープ送信者の値に展開されます。

一般には「Domain does not exist」結果は永続的ですが、これを一時的な状態にすることができます。そのようなケースを扱うために、「保守的な」ユーザは、エラー コードをデフォルトの 5XX から 4XX に変更できます。

送信者検証例外テーブル

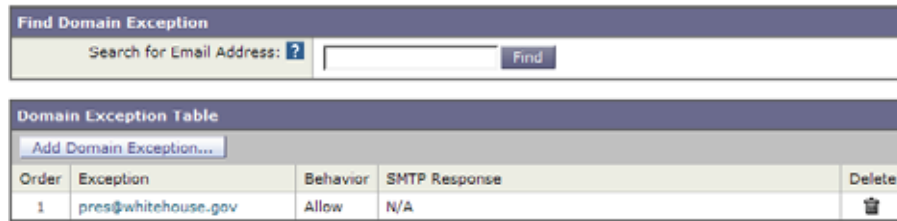
送信者検証例外テーブルは、SMTP カンバセーション中に自動的に許可または拒否されるドメインまたは電子メール アドレスのリストです。また、拒否されるドメインについて、オプションの SMTP コードと拒否応答を指定することもできます。Cisco アプライアンスあたりの送信者検証例外テーブルは 1 つのみであり、メール フロー ポリシーごとにイネーブルにされます。

送信者検証例外テーブルは、明らかに偽物であるものの、形式が正しいドメインまたは電子メール アドレスをリストし、そこからのメールを拒否するために使用できます。たとえば、形式が正しい MAIL FROM `pres@whitehouse.gov` を送信者検証例外テーブルに格納し、自動的に拒否するように設定できます。また、内部ドメインやテスト ドメインなど、自動的に許可するドメインをリストすることもできます。これは、受信者アクセス テーブル (RAT) で行われるエンベロープ受信者 (SMTP RCPT TO コマンド) 処理に似ています。

送信者検証例外テーブルは、GUI の [メール ポリシー (Mail Policies)] > [例外テーブル (Exception Table)] ページ (または CLI の `exceptionconfig` コマンド) で定義された後、GUI (『メール フロー ポリシー ACCEPTED を使用した未検証送信者への送信メッセージの定義』(P.7-34) を参照) または CLI (『Cisco AsyncOS CLI Reference Guide』を参照) でポリシーごとにイネーブルにされます。

送信者検証例外テーブルのエントリの構文は次のとおりです。

図 7-4 例外テーブルのリスト
Exception Table



例外テーブルの変更については「送信者の電子メール アドレスに基づいた送信者検証ルールからの未検証送信者の除外」(P.7-35) を参照してください。

送信者検証の実装 — 設定例

ここでは、ホストとエンベロープ送信者検証の典型的で保守的な実装の例を示します。

この例では、ホスト送信者検証を実装するときに、既存の送信者グループ SUSPECTLIST とメール フロー ポリシー THROTTLED により、逆引き DNS ルックアップが一致しない接続元ホストからのメールがスロットリングされます。

新しい送信者グループ (UNVERIFIED) と新しいメール フロー ポリシー (THROTTLEMORE) が作成されます。検証されない接続元ホストからのメールは、SMTP カンパセーションの前にスロットリングされます (送信者グループ UNVERIFIED とより積極的なメール フロー ポリシー THROTTLEMORE が使用されます)。

メール フロー ポリシー ACCEPTED に対してエンベロープ送信者検証がイネーブルにされます。

表 7-9 に、送信者検証を実装するための推奨される設定を示します。

表 7-9 送信者検証：推奨される設定

送信者グループ	ポリシー	内容
UNVERIFIED	THROTTLEMORE	SMTP カンパセーションの前。 接続元ホストの PTR レコードが DNS に存在しない。
SUSPECTLIST	THROTTLED	接続元ホストの逆引き DNS ルックアップ (PTR) が正引き DNS ルックアップ (A) に一致しない。
	ACCEPTED	SMTP カンパセーション中のエンベロープ送信者検証。 - 形式が不正な MAIL FROM:。 - エンベロープ送信者が DNS に存在しない。 - エンベロープ送信者が DNS で解決されない。

送信者グループ SUSPECTLIST を使用した未検証の送信者からのメッセージのスロットリング

手順

ステップ 1 [メール ポリシー (Mail Policies)] > [HAT 概要 (HAT Overview)] を選択します。

ステップ 2 送信者グループのリストで [SUSPECTLIST] をクリックします。

図 7-5 [HAT 概要 (HAT Overview)] ページ

HAT Overview

Find Senders

Find Senders that Contain this Text: Find

Sender Groups (Listener: IncomingMail (172.19.0.86:25))

Add Sender Group... Import HAT...

Order	Sender Group	SenderBase™ Reputation Score ?	Mail Flow Policy	Delete
1	WHITELIST	TRUSTED	🗑️
2	BLACKLIST	BLOCKED	🗑️
3	SUSPECTLIST	THROTTLED	🗑️
4	UNKNOWNLIST	ACCEPTED	🗑️
	ALL	ACCEPTED	

Edit Order... Export HAT...

ステップ 3 [設定を編集 (Edit Settings)] をクリックします。

図 7-6 送信者グループ : SUSPECTLIST : [設定を編集 (Edit Settings)]

Sender Group Settings

Comment: Suspicious senders are throttled

Policy: THROTTLED

SBRs (Optional): -4.0 to -1.0
 Include SBRs Scores of "None"
 Recommended for suspected senders only.

DNS Lists (Optional): ?

Connecting Host DNS Verification:

Connecting host PTR record does not exist in DNS.
 Connecting host PTR record lookup fails due to temporary DNS failure.
 Connecting host reverse DNS lookup (PTR) does not match the forward DNS lookup (A).

Cancel Submit

ステップ 4 リストから [スロットル (THROTTLED)] ポリシーを選択します。

ステップ 5 [接続ホストの DNS 検証 (Connecting Host DNS Verification)] 中の [接続ホスト逆引き DNS 検索 (PTR) が転送 DNS 検索 (A) と一致しない (Connecting host reverse DNS lookup (PTR) does not match the forward DNS lookup (A))] チェックボックスをオンにします。

ステップ 6 変更内容を送信し、確定します。

逆引き DNS ルックアップが失敗した送信者は送信者グループ SUSPECTLIST に一致し、メールフロー ポリシー THROTTLED のデフォルト アクションが実行されます。



(注) また、CLI でホスト DNS 検証を設定することもできます。詳細については、「CLI でのホスト DNS 検証のイネーブル化」(P.7-38) を参照してください。

未検証の送信者へのより厳格なスロットリング設定の実行

手順

- ステップ 1** まず、新しいメールフロー ポリシーを作成し（この例では THROTTLEMORE という名前を付けます）、より厳格なスロットリング設定を行います。
- [メールフロー ポリシー (Mail Flow Policies)] ページで [ポリシーを追加 (Add Policy)] をクリックします。
 - メールフロー ポリシーの名前を入力し、[接続動作 (Connection Behavior)] として [承認 (Accept)] を選択します。
 - メールをスロットリングするようにポリシーを設定します。
 - 変更内容を送信し、確定します。
- ステップ 2** 次に、新しい送信者グループを作成し（この例では、UNVERIFIED という名前を付けます）、THROTTLEMORE ポリシーを使用するように設定します。
- [HAT 概要 (HAT Overview)] ページで [送信者グループを追加 (Add Sender Group)] をクリックします。

図 7-7 [送信者グループを追加 (Add Sender Group)] : THROTTLEMORE

Add Sender Group to IncomingMail (192.168.0.1:25)

Sender Group Settings	
Name:	UNVERIFIED
Order:	5
Comment:	Throttle when host record is not in DNS
Policy:	THROTTLEMORE
SBR5 (Optional):	<input type="checkbox"/> to <input type="checkbox"/> <input type="checkbox"/> Include SBR5 Scores of "None" <i>Recommended for suspected senders only.</i>
DNS Lists (Optional):	?
Connecting Host DNS Verification:	<input checked="" type="checkbox"/> Connecting host PTR record does not exist in DNS. <input type="checkbox"/> Connecting host PTR record lookup fails due to temporary DNS failure. <input type="checkbox"/> Connecting host reverse DNS lookup (PTR) does not match the forward DNS lookup (A).

Cancel Submit Submit and Add Senders >>

- リストから [THROTTLEMORE] ポリシーを選択します。
- [接続ホストの DNS 検証 (Connecting Host DNS Verification)] 中の [接続ホストの PTR レコードが DNS に存在しません (Connecting host PTR record does not exist in DNS)] チェックボックスをオンにします。
- 変更内容を送信し、確定します。

図 7-8 HAT 概要 (HAT Overview)

HAT Overview

The screenshot shows the 'HAT Overview' interface. At the top, there is a 'Find Senders' section with a search box and a 'Find' button. Below that, the 'Sender Groups (Listener: IncomingMail (172.19.0.86:25))' section is visible. It includes buttons for 'Add Sender Group...' and 'Import HAT...'. The main part of the interface is a table with the following columns: Order, Sender Group, SenderBase™ Reputation Score (with a scale from -10 to +10), Mail Flow Policy, and Delete. The table lists five sender groups: WHITELIST (score 10, policy TRUSTED), BLACKLIST (score -10, policy BLOCKED), SUSPECTLIST (score -5, policy THROTTLED), UNVERIFIED (score -2, policy THROTTLEMORE), and UNKNOWNLIST (score 0, policy ACCEPTED). There is also an 'ALL' group with a score of 0 and policy ACCEPTED. At the bottom, there are buttons for 'Edit Order...' and 'Export HAT...', and a 'Key: Custom Default' indicator.

Order	Sender Group	SenderBase™ Reputation Score	Mail Flow Policy	Delete
1	WHITELIST	10	TRUSTED	
2	BLACKLIST	-10	BLOCKED	
3	SUSPECTLIST	-5	THROTTLED	
4	UNVERIFIED	-2	THROTTLEMORE	
5	UNKNOWNLIST	0	ACCEPTED	
	ALL	0	ACCEPTED	

メール フロー ポリシー ACCEPTED を使用した未検証送信者への送信メッセージの定義

手順

- ステップ 1 [メール ポリシー (Mail Policies)] > [メールフロー ポリシー (Mail Flow Policies)] を選択します。
- ステップ 2 [メールフロー ポリシー (Mail Flow Policies)] ページで、メールフロー ポリシー [承認 (ACCEPTED)] をクリックします。
- ステップ 3 メールフロー ポリシーの最後にスクロールします。

図 7-9 メール フロー ポリシー ACCEPTED のエンベロップ送信者の DNS 検証の設定

The screenshot shows the configuration page for 'Envelope Sender DNS Verification'. At the top, there are radio buttons for 'Use Default (Off)', 'On', and 'Off', with 'On' selected. Below this, there are three sections for defining SMTP codes and text for different error conditions:

- Malformed Envelope Senders:** SMTP Code: 553, SMTP Text: #5.5.4 Domain required for sender address
- Envelope Senders whose domain does not resolve:** SMTP Code: 451, SMTP Text: #4.1.3 Domain of sender address <\$Envelo
- Envelope Senders whose domain does not exist:** SMTP Code: 553, SMTP Text: #5.1.8 Domain of sender address <\$Envelo

 At the bottom, there are radio buttons for 'Use Exception Table: Use Default (Off)', 'On', and 'Off', with 'On' selected.

- ステップ 4 [オン (On)] を選択し、このメールフロー ポリシーに対するエンベロップ送信者の DNS 検証をイネーブルにします。
- ステップ 5 カスタム SMTP コードと応答を定義することもできます。
- ステップ 6 [例外テーブルを使用 (Use Exception Table)] で [オン (On)] を選択することで、ドメイン例外テーブルをイネーブルにします。

ステップ 7 変更内容を送信し、確定します。

送信者の電子メール アドレスに基づいた送信者検証ルールからの未検証送信者の除外

手順

ステップ 1 [メール ポリシー (Mail Policies)] > [例外テーブル (Exception Table)] を選択します。



(注) 例外テーブルは、[例外テーブルを使用 (Use Exception Table)] がイネーブルに設定されているすべてのメールフロー ポリシーにグローバルに適用されます。

ステップ 2 [メール ポリシー (Mail Policies)] > [例外テーブル (Exception Table)] ページで [ドメイン例外を追加 (Add Domain Exception)] をクリックします。

ステップ 3 電子メール アドレスを入力します。具体的なアドレス (pres@whitehouse.gov)、名前 (user@)、ドメイン (@example.com または @.example.com)、または IP アドレスを角カッコで囲んだアドレス (user@[192.168.23.1]) を入力できます。

ステップ 4 そのアドレスからのメッセージを許可するか拒否するかを指定します。メールを拒否する場合、SMTP コードとカスタム応答を指定することもできます。

ステップ 5 変更内容を送信し、確定します。

送信者検証例外テーブル内でのアドレスの検索

手順

ステップ 1 [例外テーブル (Exception Table)] ページの [ドメイン例外の検索 (Find Domain Exception)] セクションに電子メール アドレスを入力します。

ステップ 2 [検索 (Find)] をクリックします。

図 7-10 例外テーブル中の一致エントリの検索

Exception Table

The screenshot shows a web interface for managing exception tables. At the top, there is a search bar titled "Find Domain Exception" with the text "Search for Email Address: ?" and a text input field containing "mjones@partner.com" and a "Find" button. Below this is a table titled "Domain Exception Table" with a button "Add Domain Exception...". The table has five columns: "Order", "Exception", "Behavior", "SMTP Response", and "Delete".

Order	Exception	Behavior	SMTP Response	Delete
1	pres@whitehouse.gov	Reject	553, Envelope sender <\${EnvelopeSender}> rej...	
2	@partner.com	Allow	N/A	

テーブル中のいずれかのエントリにアドレスが一致した場合、最初に一致したエントリが表示されます。

図 7-11 例外テーブル中の一致エントリの一覧表示

Exception Table

Find Domain Exception				
Search for Email Address: ?		mjones@partner.com		Find
Domain Exceptions Matching "mjones@partner.com"				
Show All Domain Exceptions				
Order	Exception	Behavior	SMTP Response	Delete
2	@partner.com	Allow	N/A	

未検証送信者からのメッセージの設定テスト

これで送信者検証設定を完了したため、Cisco アプライアンスの動作を確認できます。
DNS 関連の設定のテストは、本書の範囲を超えていることに注意してください。

形式が不正な MAIL FROM 送信者アドレスのテスト メッセージの送信

THROTTLED ポリシーのさまざまな DNS 関連の設定をテストすることは難しい場合がありますが、形式が不正な MAIL FROM 設定をテストできます。

手順

- ステップ 1** Cisco アプライアンスへの Telnet セッションを開きます。
- ステップ 2** SMTP コマンドを使用して、形式が不正な MAIL FROM (ドメインなしの「admin」など) を使用したテストメッセージを送信します。



(注) デフォルト ドメインを使用するか、メールを送受信するときに部分ドメインを明示的に許可するように Cisco アプライアンスを設定した場合や、アドレス解析をイネーブにした場合は (『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「Customizing Listeners」を参照)、ドメインがないかドメインの形式が正しくない電子メールを作成、送信、受信できない場合があります。

- ステップ 3** メッセージが拒否されることを確認します。

```
# telnet IP_address_of_IronPort_Appliance_port

220 hostname ESMTTP

helo example.com

250 hostname

mail from: admin

553 #5.5.4 Domain required for sender address
```


SMTP コードと応答が、メール フロー ポリシー THROTTLED のエンベロープ送信者検証設定で設定したものになっていることを確認します。

送信者検証ルールから除外するアドレスからのメッセージの送信

送信者検証例外テーブルに列挙されている電子メール アドレスからのメールに対し、エンベロープ送信者検証が実行されないことを確認するには、次の手順を実行します。

手順

- ステップ 1** アドレス `admin@zzzaazz.com` を、例外テーブルに動作「Allow」で追加します。
- ステップ 2** 変更内容を確定します。
- ステップ 3** Cisco アプライアンスへの Telnet セッションを開きます。
- ステップ 4** SMTP コマンドを使用して、送信者検証例外テーブルに入力した電子メール アドレス (`admin@zzzaazz.com`) からテスト メッセージを送信します。
- ステップ 5** メッセージが許可されることを確認します。

```
# telnet IP_address_of_IronPort_Appliance port

220 hostname ESMTP

helo example.com

250 hostname

mail from: admin@zzzaazz.com

250 sender <admin@zzzaazz.com> ok
```

その電子メール アドレスを送信者検証例外テーブルから削除すると、エンベロープ送信者のドメイン部分が DNS で検証されないため、その送信者からのメールが拒否されます。

送信者検証とロギング

次のログ エントリは、送信者検証の判断例を示します。

エンベロープ送信者検証

形式が不正なエンベロープ送信者

```
Thu Aug 10 10:14:10 2006 Info: ICID 3248 Address: <user> sender rejected, envelope sender domain missing
```

ドメインが存在しない (NXDOMAIN)

```
Wed Aug 9 15:39:47 2006 Info: ICID 1424 Address: <user@domain.com> sender rejected,
envelope sender domain does not exist
```

ドメインが解決されない (SERVFAIL)

```
Wed Aug 9 15:44:27 2006 Info: ICID 1425 Address: <user@domain.com> sender rejected,
envelope sender domain could not be resolved
```

CLI でのホスト DNS 検証のイネーブル化

CLI でホスト DNS 検証をイネーブルにするには、`listenerconfig > edit > hostaccess` コマンドを使用します。詳細については、『*Cisco AsyncOS CLI Reference Guide*』を参照してください。

表 7-10 に、未検証の送信者の種類と対応する CLI 設定を示します。

表 7-10 送信者グループ設定と対応する CLI 値

接続元ホストの DNS 検証	同等の CLI 設定
接続元ホストの PTR レコードが DNS に存在しない。	<code>nx.domain</code>
DNS の一時的な障害により接続元ホストの PTR レコードのルックアップに失敗した。	<code>serv.fail</code>
接続元ホストの逆引き DNS ルックアップ (PTR) が正引き DNS ルックアップ (A) に一致しない。	<code>not.double.verified</code>



CHAPTER 8

ドメイン名または受信者アドレスに基づく接続の許可または拒否

- 「受信者のアドレスに基づく接続の許可または拒否の概要」 (P.8-1)
- 「ドメインおよびユーザ」 (P.8-3)

受信者のアドレスに基づく接続の許可または拒否の概要

AsyncOS は各パブリック リスナーが受信者アドレスの許可および拒否操作を管理するために Recipient Access Table (RAT; 受信者アクセス テーブル) を使用します。受信者アドレスには次のものが含まれます。

- ドメイン
- 電子メール アドレス
- 電子メール アドレスのグループ

システム セットアップ ウィザードは、少なくとも 1 つのパブリック リスナー (デフォルト値) をアプライアンス上で設定するように管理者に指示します。セットアップ時にパブリック リスナーを設定すると、メールを受け入れるデフォルトのローカル ドメインまたは特定のアドレスを指定します。これらのローカル ドメインまたは特定のアドレスは、パブリック リスナーの RAT の最初のエントリです。

各パブリック リスナーのデフォルトのエントリである [その他の受信者 (All Other Recipients)] は、すべての受信者からの電子メールを拒否します。管理者は、アプライアンスがメッセージを許可するすべてのローカル ドメインを定義します。任意で、アプライアンスがメッセージを許可または拒否する特定のユーザも定義できます。AsyncOS では、受信者アクセス テーブル (RAT) を使用して適切なローカル ドメインと特定のユーザを定義することができます。

複数ドメインのメッセージを受け入れるように、リスナーの設定が必要になる場合があります。たとえば、組織で以前 oldcompanyname.com ドメインを使用し、現在 currentcompanyname.com ドメインを使用していて、currentcompanyname.com および oldcompanyname.com の両方からメッセージを受け入れる場合があります。この場合、両方のローカル ドメインをパブリック リスナーの RAT に含めます。

((注) ドメイン マップ機能はあるドメインから別のドメインにメッセージをマップできます。『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「Configuring Routing and Domain Features」の章とドメイン マップ機能の項を参照してください)。

受信者アクセス テーブル (RAT) の概要

受信者アクセス テーブルは、パブリック リスナーが許可する受信者を定義します。少なくとも、テーブルはアドレスおよびそのアドレスを受け入れるか拒否するかを指定します。

[受信者アクセス テーブル (RAT) (Recipient Access Table (RAT))] ページには、RAT 内のエントリの一覧が、その順序、デフォルトのアクション、エントリが LDAP 許可クエリーをバイパスするように設定されているかどうかとともに表示されます。

RAT へのアクセス

GUI

ステップ 1 [メールポリシー (Mail Policies)] > [受信者アクセス テーブル (RAT) (Recipient Access Table (RAT))] に移動します。

CLI

ステップ 1 listenerconfig コマンドと edit -> rcptaccess -> new サブコマンドを使用します。

デフォルトの RAT エントリの編集

はじめる前に

- パブリック リスナーを設定します。
- インターネット上に、オープン リレーを作成しないように、編集の計画には注意が必要です。オープンリレー (「セキュアでないリレー」または「サードパーティ リレー」とも呼びます) は、第三者による電子メール メッセージのリレーを許す SMTP 電子メール サーバです。オープン リレーがあると、ローカル ユーザ向けでもローカル ユーザからでもないメールを処理することにより、非良心的な送信者がゲートウェイを通じて大量のスパムを送信することが可能になります。デフォルトでは、RAT はすべての受信者を拒否し、オープン リレーが作成されないようにします。
- デフォルトのエントリを RAT から削除できないことに注意してください。

手順

ステップ 1 [メールポリシー (Mail Policies)] > [受信者アクセス テーブル (RAT) (Recipient Access Table (RAT))] に移動します。

ステップ 2 [その他の受信者 (All Other Recipients)] をクリックします。

ドメインおよびユーザ

RAT を使用してメッセージを受け入れるドメインを変更する

アプライアンスがメッセージを許可するすべてのローカル ドメインおよび特定のユーザを設定するには、[メールポリシー (Mail Policies)] > [受信者アクセス テーブル (RAT) (Recipient Access Table (RAT))] ページを使用します。このページでは、次の作業を実行できます。

- RAT 内のエントリの追加、削除、変更。
- エントリの順序の変更。
- RAT エントリのテキスト ファイルへのエクスポート。
- RAT エントリのテキスト ファイルからのインポート。テキスト ファイルからのインポートは、既存のエントリを上書きします。

メッセージを受け入れるドメインおよびユーザの追加

手順

-
- ステップ 1** [メールポリシー (Mail Policies)] > [受信者アクセス テーブル (RAT) (Recipient Access Table (RAT))] ページに移動します。
 - ステップ 2** [リスナーの概要 (Overview for Listener)] フィールドで編集するリスナーを選択します。
 - ステップ 3** [受信者を追加 (Add Recipient)] をクリックします。
 - ステップ 4** エントリの順序を選択します。
 - ステップ 5** 受信者のアドレスを入力します。
 - ステップ 6** 受信者を許可するか拒否するかを選択します。
 - ステップ 7** (任意) 受信者に対する LDAP 許可クエリーをバイパスすることを選択します。
 - ステップ 8** (任意) このエントリに対してカスタム SMTP 応答を使用します。
 - a.** [カスタム SMTP 応答 (Custom SMTP Response)] で [はい (Yes)] を選択します。
 - b.** SMTP 応答コードとテキストを入力します。その受信者に対する RCPT TO コマンドへの SMTP 応答を含めます。
 - ステップ 9** (任意) [受信コントロールのバイパス (Bypass Receiving Control)] で [はい (Yes)] を選択して、スロットリングのバイパスを選択します。
 - ステップ 10** 変更内容を送信し、確定します。
-

関連項目

- 「[受信者アドレスの定義](#)」 (P.8-4)
- 「[特別な受信者での LDAP 許可のバイパス](#)」 (P.8-4)

受信者アドレスの定義

RAT では、受信者または受信者のグループを定義できます。受信者は、完全な電子メール アドレス、ドメイン、部分ドメイン、ユーザ名、または IP アドレスで定義できます。

[IPv4 address]	ホストの特定のインターネット プロトコル バージョン 4 (IPv4) アドレス。IP アドレスは文字「[]」で囲む必要があることに注意してください。
[IPv6 address]	ホストの特定のインターネット プロトコル バージョン 6 (IPv6) アドレス。IP アドレスは文字「[]」で囲む必要があることに注意してください。
division.example.com	完全修飾ドメイン名。
.partialhost	「partialhost」ドメイン内のすべて。
user@domain	完全な電子メール アドレス。
user@	指定したユーザ名を含むすべてのアドレス。
user@[IP_address]	特定の IPv4 または IPv6 アドレスのユーザ名。IP アドレスは文字「[]」で囲む必要があることに注意してください。 「user@[IP_address]」(角カッコ文字なし) は有効なアドレスではないことに注意してください。有効なアドレスを作成するために、メッセージを受信したときに角カッコが追加され、受信者が RAT で一致するかどうかに影響が出ることがあります。



(注)

GUI のシステム セットアップ ウィザードの手順 4 でドメインを受信者アクセス テーブルに追加する場合 (「手順 3 : ネットワーク」(P.3-16) を参照)、サブドメインを指定するための別のエントリを追加することを検討してください。たとえば、ドメイン example.net を入力する場合、.example.net も入力したほうがよい場合があります。第 2 のエントリにより、example.net のすべてのサブドメイン宛のメールが受信者アクセス テーブルに一致するようになります。RAT で .example.com のみを指定した場合、.example.com のすべてのサブドメイン宛のメールを許可しますが、サブドメインがない完全な電子メール アドレス受信者 (たとえば joe@example.com) 宛のメールは許可されません。

特別な受信者での LDAP 許可のバイパス

LDAP 許可クエリーを設定する場合、特定の受信者について許可クエリーをバイパスすることが必要な場合があります。この機能は、customer@example.com のように、ある受信者宛に受信した電子メールについて、LDAP クエリーの中で遅延させたりキューに格納したりしないことが望ましい場合に便利です。

LDAP 許可クエリーの前にワーク キュー内で受信者アドレスを書き換えるように設定した場合 (エイリアシングまたはドメイン マップの使用など)、書き換えられたアドレスは LDAP 許可クエリーをバイパスしません。たとえば、エイリアス テーブルを使用して customer@example.com を bob@example.com および sue@example.com にマップします。customer@example.com について LDAP 許可のバイパスを設定した場合、エイリアシングが実行された後に、bob@example.com および sue@example.com に対して LDAP 許可クエリーが実行されます。

GUI で LDAP 許可をバイパスするように設定するには、RAT エントリを追加または編集するときに [この受信者の LDAP アクセプトクエリーをバイパスする (Bypass LDAP Accept Queries for this Recipient)] を選択します。

CLI で LDAP 許可クエリーをバイパスするように設定するには、`listenerconfig -> edit -> rcptaccess` コマンドを使用して受信者を入力するときに、次の質問に「yes」と答えます。

```
Would you like to bypass LDAP ACCEPT for this entry? [Y]> y
```

LDAP 許可をバイパスするように RAT エントリを設定する場合、RAT エントリの順序が、受信者アドレスの一致のしかたに影響を与えることに注意してください。条件を満たす最初の RAT エントリを使用して受信者アドレスが一致します。たとえば、RAT エントリ `postmaster@ironport.com` と `ironport.com` があるとします。`postmaster@ironport.com` のエントリについては LDAP 許可クエリーをバイパスするように設定し、`ironport.com` のエントリを ACCEPT に設定します。`postmaster@ironport.com` 宛のメールを受信した場合、LDAP 許可がバイパスされるのは、`postmaster@ironport.com` のエントリが `ironport.com` のエントリよりも前にある場合のみです。`ironport.com` のエントリが `postmaster@ironport.com` のエントリの前にある場合、RAT はこのエントリを介して受信者アドレスと一致し、ACCEPT アクションが適用されます。

特別な受信者でのスロットリングのバイパス

受信者エントリで、リスナーでイネーブルになっているスロットリング制御メカニズムを受信者がバイパスすることを指定できます。

この機能は、特定の受信者のメッセージを制限しない場合に便利です。たとえば、多くのユーザは、メール フロー ポリシーで定義されている受信制御に基づいて送信元ドメインがスロットリングされている場合でも、リスナー上でアドレス「`postmaster@domain`」の電子メールを受信します。リスナーの RAT 中で受信制御をバイパスするようにこの受信者を指定することで、同じドメイン中の他の受信者用のメール フロー ポリシーを保持しつつ、リスナーは受信者「`postmaster@domain`」の無制限のメッセージを受信できます。受信者は、送信元ドメインが制限されている場合に、システムが保持している時間あたりの受信者のカウンタでカウントされません。

GUI で特定の受信者が受信制御をバイパスするように指定するには、RAT エントリを追加または編集するときに、[受信コントロールのバイパス (Bypass Receiving Control)] 設定で [はい (Yes)] を選択します。

CLI で特定の受信者が受信制御をバイパスするように指定するには、`listenerconfig -> edit -> rcptaccess` コマンドを使用して受信者を入力するときに、次の質問に「yes」と答えます。

```
Would you like to bypass receiving control for this entry? [N]> y
```

受信者アクセス テーブルでのドメインおよびユーザの順序の入れ替え

手順

-
- ステップ 1 [メールポリシー (Mail Policies)] > [受信者アクセス テーブル (RAT) (Recipient Access Table (RAT))] ページに移動します。
 - ステップ 2 [リスナーの概要 (Overview for Listener)] フィールドで編集するリスナーを選択します。
 - ステップ 3 [順番を編集 (Edit Order)] をクリックします。
 - ステップ 4 [順番 (Order)] 列の値を調整して順序を変更します。
 - ステップ 5 変更内容を送信し、確定します。
-

受信者アクセス テーブルの外部ファイルへのエクスポート

手順

-
- ステップ 1** [メールポリシー (Mail Policies)] > [受信者アクセス テーブル (RAT) (Recipient Access Table (RAT))] ページに移動します。
 - ステップ 2** [リスナーの概要 (Overview for Listener)] フィールドで編集するリスナーを選択します。
 - ステップ 3** [RAT をエクスポート (Export RAT)] をクリックします。
 - ステップ 4** エクスポートするエントリのファイル名を入力します。
これは、アプライアンスの設定ディレクトリに作成されるファイルの名前になります。
 - ステップ 5** 変更内容を送信し、確定します。
-

受信者アクセス テーブルの外部ファイルからのインポート

テキスト ファイルから受信者アクセス テーブル エントリをインポートすると、既存のすべてのエントリが受信者アクセス テーブルから削除されます。

手順

-
- ステップ 1** [メールポリシー (Mail Policies)] > [受信者アクセス テーブル (RAT) (Recipient Access Table (RAT))] ページに移動します。
 - ステップ 2** [リスナーの概要 (Overview for Listener)] フィールドで編集するリスナーを選択します。
 - ステップ 3** [RAT をインポート (Import RAT)] をクリックします。
 - ステップ 4** リストからファイルを選択します。
AsyncOS は、アプライアンス上の configuration ディレクトリに存在するテキスト ファイルの一覧を表示します。
 - ステップ 5** [送信 (Submit)] をクリックします。
既存の受信者アクセス テーブル エントリをすべて削除することを確認する警告メッセージが表示されます。
 - ステップ 6** [インポート (Import)] をクリックします。
 - ステップ 7** 変更内容を確定します。

ファイルには「コメント」を格納できます。文字「#」で始まる行はコメントと見なされ、AsyncOS によって無視されます。次に例を示します。

```
# File exported by the GUI at 20060530T220526

.example.com  ACCEPT

ALL  REJECT
```



CHAPTER 9

メッセージフィルタを使用した電子メールポリシーの適用

Cisco アプライアンスは、詳細なコンテンツ スキャンおよびメッセージ フィルタリング テクノロジーを備えているため、会社のネットワークに参加または退出するときに、会社のポリシーを適用して、特定のメッセージを処理することができます。

この章では、ポリシーの適用のために使用可能な機能（コンテンツ スキャン エンジン、メッセージ フィルタ、添付ファイル フィルタ、コンテンツ ディクショナリ）の強力な組み合わせについて説明します。

この章は、次の内容で構成されています。

- 「概要」 (P.9-1)
- 「メッセージフィルタのコンポーネント」 (P.9-2)
- 「メッセージフィルタ処理」 (P.9-4)
- 「メッセージフィルタ ルール」 (P.9-9)
- 「メッセージフィルタ アクション」 (P.9-43)
- 「添付ファイルのスキャン」 (P.9-67)
- 「CLI を使用したメッセージ フィルタの管理」 (P.9-79)
- 「メッセージ フィルタの例」 (P.9-100)

概要

メッセージ フィルタにより、Cisco アプライアンスでメッセージを受信したときに、それらを処理する方法を記述した特別なルールを作成できます。メッセージ フィルタは、特定の種類の電子メール メッセージに指定の特別な処理を施す必要があることを指定します。Cisco メッセージ フィルタは、指定の単語に対してメッセージ内容をスキャンすることによって社内メール ポリシーを適用することができます。この章は、次の内容で構成されています。

- **メッセージ フィルタのコンポーネント。**メッセージ フィルタにより、メッセージの受信時にそれらを処理する方法を記述した特別なルールを作成できます。フィルタ ルールでは、メッセージまたは添付ファイルの内容、ネットワークに関する情報、メッセージ エンベロープ、メッセージ ヘッダー、またはメッセージ本文に基づいてメッセージを識別します。フィルタ アクションにより、通知を生成したり、メッセージのドロップ、バウンス、アーカイブ、ブラインドカーボンコピー、変更を行ったりすることができます。詳細については、「[メッセージ フィルタのコンポーネント](#)」 (P.9-2) を参照してください。

- **メッセージフィルタの処理。** AsyncOS がメッセージフィルタを処理する場合、AsyncOS がスキャンする内容、処理の順番、実行されるアクションは、メッセージフィルタの順番、メッセージの内容を変更した可能性のある事前の処理、メッセージの MIME 構造、コンテンツ マッチング用に設定されたしきい値スコア、クエリーの構造などのいくつかの要因に基づきます。詳細については、「[メッセージフィルタ処理](#)」(P.9-4) を参照してください。
- **メッセージフィルタ ルール。** 各フィルタには、フィルタで処理できる一連のメッセージを定義するルールがあります。メッセージフィルタを作成する場合、それらのルールを定義します。詳細については、「[メッセージフィルタ ルール](#)」(P.9-9) を参照してください。
- **メッセージフィルタのアクション。** 各フィルタには、ルールで true に評価された場合に、メッセージに対して実行するアクションがあります。実行できるアクションには、最終アクション (メッセージの配信、ドロップ、バウンスなど)、またはメッセージをさらに処理できる非最終アクション (ヘッダーの除去や挿入など) の 2 つのタイプのアクションがあります。詳細については、「[メッセージフィルタ アクション](#)」(P.9-43) を参照してください。
- **添付ファイル スキャン メッセージフィルタ。** 添付ファイル スキャン メッセージフィルタを使用して、会社のポリシーと整合しないメッセージから添付ファイルを除去できます。元のメッセージはそのまま配信することができます。添付ファイルは、それらの特定のタイプ、フィンガープリント、内容に基づいてフィルタできます。イメージアナライザを使用して、イメージ添付ファイルをスキャンすることもできます。イメージアナライザは、肌の色、本文サイズ、曲率を測定して、グラフィックに不適切な内容が含まれている可能性を判断するアルゴリズムを作成します。詳細については、「[添付ファイルのスキャン](#)」(P.9-67) を参照してください。
- **CLI を使用したメッセージフィルタの管理。** CLI は、メッセージフィルタを操作するためのコマンドを受け入れます。たとえば、メッセージフィルタのリストを表示、並び替え、インポート、エクスポートする必要がある場合があります。詳細については、「[CLI を使用したメッセージフィルタの管理](#)」(P.9-79) を参照してください。
- **メッセージフィルタの例。** この項では、実際のフィルタの例を示し、各フィルタについて簡単に説明します。詳細については、「[メッセージフィルタの例](#)」(P.9-100) を参照してください。

メッセージフィルタのコンポーネント

メッセージフィルタにより、メッセージの受信時にそれら処理する方法を記述した特別なルールを作成できます。メッセージフィルタは、メッセージフィルタ ルールとメッセージフィルタ アクションから構成されます。

メッセージフィルタ ルール

メッセージフィルタ ルールによって、フィルタで処理するメッセージを判断します。ルールは、論理結合子 AND、OR、NOT を使用して組み合わせることで、複雑なテストを作成できます。ルール式は、かっこを使用してグループ化することもできます。

メッセージフィルタ アクション

メッセージフィルタの目的は、選択されたメッセージに対してアクションを実行することです。

アクションには、次の 2 つのタイプがあります。

- **最終アクション** (deliver、drop、bounce など) はメッセージの処理を終了し、後続のフィルタによるさらなる処理を許可しません。
- **非最終アクション**は、メッセージをさらに処理することを許可するアクションを実行します。



(注) 非最終メッセージフィルタアクションは、累積的です。各フィルタが異なるアクションを指定する複数のフィルタにメッセージが一致する場合、すべてのアクションが累積され、適用されます。ただし、同じアクションを指定する複数のフィルタにメッセージが一致する場合、前のアクションが上書きされ、最後のフィルタアクションが適用されます。

メッセージフィルタの構文例

フィルタ仕様の直観的な意味は次のようになります。

メッセージがルールに一致する場合、順番にアクションが適用されます。else 句が存在する場合、メッセージがルールに一致しない場合に else 句内のアクションが実行されます。

指定したフィルタ名によって、フィルタをアクティブ、非アクティブ、削除する場合に、フィルタが管理しやすくなります。

メッセージフィルタでは次の構文を使用します。

構文例	目的
<code>expedite:</code>	フィルタ名
<code>if (recv-listener == 'InboundMail' or recv-int == 'notmain')</code>	ルールの指定
<code>{ alt-src-host('outbound1'); skip-filters(); }</code>	アクションの指定
<code>else { alt-src-host('outbound2'); }</code>	任意の代替アクションの指定

代替アクションは省略できることに注意してください。

構文例	目的
<code>expedite2:</code>	フィルタ名
<code>if ((not (recv-listener == 'InboundMail')) and (not (recv-int == 'notmain')))</code>	ルールの指定
<code>{ alt-src-host('outbound2'); skip-filters(); }</code>	アクションの指定

複数のフィルタを順番に1つずつ並べて1つのテキストファイルにまとめることができます。

単一引用符または二重引用符で、フィルタの値を囲む必要があります。単一引用符または二重引用符は、値の両側に等しく組み合わせる必要があります。たとえば、式

`notify('customer-care@example.com')` と `notify("customer-care@example.com")` はどちらも有効ですが、式 `notify("customer-care@example.com')` は構文エラーが発生します。

「#」文字で始まる行はコメントと見なされ、無視されます。ただし、それらは `filters -> detail` によってフィルタを表示して確認できるように、AsyncOS で保持されません。

メッセージフィルタ処理

AsyncOS はメッセージフィルタを処理する場合、AsyncOS がスキャンする内容、処理の順番、実行するアクションは、次のいくつかの要因に基づきます。

- **メッセージフィルタの順番。**メッセージフィルタは、順序付けられたリストで維持されます。メッセージの処理時に、AsyncOS は各メッセージフィルタをそれらがリストに表示されている順番で適用します。最終アクションが行われた場合、そのメッセージに対して、それ以上のアクションは実行されません。詳細については、「[メッセージフィルタの順番](#)」(P.9-4) を参照してください。
- **事前処理。**メッセージフィルタが評価される前に、AsyncOS メッセージに対して実行されるアクションによって、ヘッダーが追加または削除されることがあります。AsyncOS は、処理時にメッセージに存在するヘッダーに対してメッセージフィルタプロセスを実行します。詳細については、「[メッセージヘッダー ルールおよび評価](#)」(P.9-5) を参照してください。
- **メッセージの MIME 構造。**メッセージの MIME 構造によって、「本文」として扱われるメッセージの部分と「添付ファイル」として扱われるメッセージの部分が判断されます。多くのメッセージフィルタは、メッセージの本文部分のみに、または添付ファイル部分のみに作用するように設定されます。詳細については、「[メッセージ本文とメッセージ添付ファイル](#)」(P.9-5) を参照してください。
- **正規表現に設定されるしきい値スコア。**正規表現に一致させる場合、フィルタアクションが実行されるまでに、一致が発生しなければならない回数を集計する「スコア」を設定します。これにより、さまざまな用語に対する応答の重み付けをすることができます。詳細については、「[コンテンツ スキャンの一致のしきい値](#)」(P.9-6) を参照してください。
- **クエリーの構造。**メッセージフィルタ内で、AND または OR テストを評価する場合、AsyncOS は不要なテストを評価しません。さらに、システムは左から右にテストを評価しないことに注意することが重要です。代わりに、AND および OR テストが評価される場合、最も価値の低いテストが最初に評価されます。詳細については、「[メッセージフィルタ内の AND テストと OR テスト](#)」(P.9-8) を参照してください。

メッセージフィルタの順番

メッセージフィルタは順序付けられたリストに維持され、リスト内のそれらの位置によって番号付けされます。メッセージの処理時に、メッセージフィルタが割り振られた番号順で適用されます。そのため、9 番のフィルタがメッセージに対してすでに最終アクション（バウンスなど）を実行した場合、30 番のフィルタは、メッセージの送信元ホストを変更する機会がありません。リストのフィルタの位置は、システム ユーザ インターフェイスによって変更できます。ファイルからインポートされたフィルタは、インポートされたファイル内のそれらの相対的順序に基づきます。

最終アクション後、そのメッセージに対して、それ以上のアクションは実行されません。

メッセージがフィルタルールに一致していても、次のいずれかの理由で、フィルタがそのメッセージに対して作用しないことがあります。

- フィルタが非アクティブである。
- フィルタが無効である。
- フィルタが、メッセージの最終アクションを実行した前のフィルタに取って代わられた。

メッセージヘッダールールおよび評価

フィルタは、ヘッダールールを適用する場合に、元のメッセージのヘッダーではなく、「処理済み」ヘッダーを評価します。つまり、

- 前に実行されたアクションによって、ヘッダーが追加された場合、後続のすべてのヘッダールールによって、それを照合できるようになります。
- 前に実行されたアクションによって、ヘッダーが取り除かれた場合、後続のすべてのヘッダールールで、それを照合できなくなります。
- 前に実行されたアクションによって、ヘッダーが変更された場合、後続のすべてのヘッダールールで、元のメッセージヘッダーではなく、変更済みのヘッダーが評価されます。

この動作は、メッセージフィルタとコンテンツフィルタの両方に共通です。

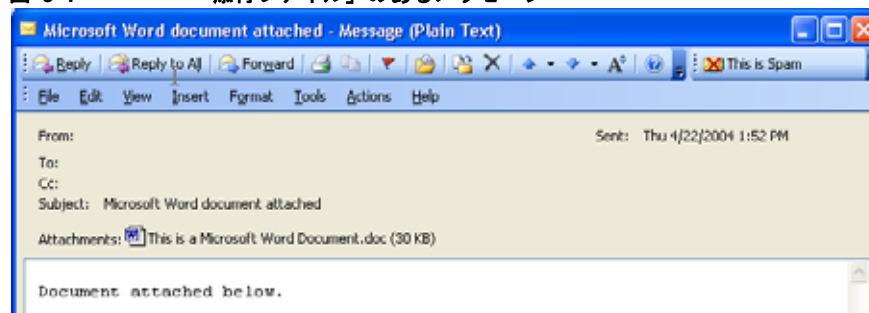
メッセージ本文とメッセージ添付ファイル

電子メールメッセージは、複数の部分から構成されます。RFCでは、メッセージのヘッダーの後に続くすべてのものをマルチパート「メッセージ本文」として規定していますが、多くのユーザはまだメッセージの「本文」と「添付ファイル」を別々のものと捉えています。body-variable または attachment-variable という Cisco メッセージフィルタを使用する場合、Cisco アプライアンスはほとんどのユーザが「本文」と「添付ファイル」として考える部分を、多くの MUA がそれらを別々にレンダリングしようと試みるのと同じように区別しようとします。

body-variable または attachment-variable メッセージフィルタルールを書く目的では、メッセージヘッダーの後のすべてのものがメッセージ本文と見なされ、その内容は本文内にある MIME 部分の最初のテキスト部分と見なされます。そのコンテンツの後のすべてのもの（つまり、追加の MIME 部分）は添付ファイルと見なされます。AsyncOS はメッセージのさまざまな MIME 部分を評価し、添付ファイルとして処理されるファイルの部分を識別します。

たとえば、[図 9-1](#) に、Microsoft Outlook MUA のメッセージを示します。ここでは「Document attached below.」という言葉がプレーンテキストのメッセージ本文として表示され、ドキュメント「This is a Microsoft Word document.doc」が添付ファイルとして表示されています。多くのユーザが電子メールをこのように捉えている（最初の部分がプレーンテキストで 2 番目の部分がバイナリファイルであるマルチパートメッセージとしてではなく）ため、Cisco は、メッセージの「本文」（最初のプレーンテキスト部分）と対照的に、.doc ファイル部分（実質的に 2 番目の MIME 部分）を区別して処理するルールを作成するために、メッセージフィルタで「添付ファイル」という用語を使用しています。ただし、RFC 1521 および 1522 で使われている用語によると、メッセージの本文はすべての MIME 部分から構成されます。

図 9-1 「添付ファイル」のあるメッセージ



Cisco アプライアンスは、マルチパートメッセージの本文と添付ファイルを区別しているため、body-variable または attachment-variable メッセージフィルタルールを使用して、期待する動作を達成するために、注意する必要があるいくつかの状況があります。

- テキスト部分が1つのメッセージ（つまり、「Content-Type: text/plain」または「Content-Type: text/html」のヘッダーを含むメッセージ）がある場合、Cisco アプライアンスはメッセージ全体を本文と見なします。コンテンツタイプが異なる場合、Cisco アプライアンスは、それを単一の添付ファイルと見なします。
- エンコードされたファイル（`uuencoded` など）は電子メールメッセージの本文に含まれます。これが発生した場合、エンコードされたファイルは添付ファイルとして扱われ、抽出およびスキャンされ、残りのテキストがテキスト本文として見なされます。
- 単一のテキスト以外の部分は常に添付ファイルと見なされます。たとえば、`.zip` ファイルのみで構成されるメッセージは、添付ファイルと見なされます。

コンテンツ スキャンの一致のしきい値

メッセージ本文または添付ファイル内のパターンを検索するフィルタ ルールを追加する場合、パターンが見つかる必要がある回数の最初のしきい値を指定できます。AsyncOS はメッセージをスキャンすると、メッセージおよび添付ファイルに見つかった一致の数の「スコア」を集計します。最小しきい値に満たない場合、正規表現は `true` と評価されません。このしきい値は次のフィルタ ルールに指定できます。

- `body-contains`
- `only-body-contains`
- `attachment-contains`
- `every-attachment-contains`
- `dictionary-match`
- `attachment-dictionary-match`

`drop-attachments-where-contains` アクションにしきい値を指定することもできます。



(注)

ヘッダーまたはエンベロープの受信者と送信者をスキャンするフィルタ ルールにしきい値を指定できません。

しきい値の構文

出現最小回数のしきい値を指定するには、パターンと、`true` と評価するために必要な一致の最小数を指定します。

```
if(<filter rule>(<pattern>,<minimum threshold>){
```

たとえば、`body-contains` フィルタ ルールで、値「`Company Confidential`」が少なくとも2回見つかる必要があることを指定するには、次の構文を使用します。

```
if(body-contains('Company Confidential',2)){
```

デフォルトで、AsyncOS がコンテンツ スキャン フィルタを保存する場合、フィルタをコンパイルし、しきい値が割り当てられていない場合、1のしきい値を割り当てます。

コンテンツ ディクショナリの値に対して、パターン マッチの最小数を指定することもできます。コンテンツ ディクショナリの詳細については、「テキストリソース」の章を参照してください。

メッセージ本文と添付ファイルのしきい値スコア

電子メールメッセージは、複数の部分から構成されることがあります。メッセージ本文または添付ファイル内のパターンを検索するフィルタ ルールのしきい値を指定すると、AsyncOS は、メッセージ部分と添付ファイルの一致の数をカウントして、しきい値「スコア」を判断します。メッセージフィルタで特定の MIME 部分を指定しない限り (attachment-contains フィルタ ルールなど)、AsyncOS はメッセージのすべての部分で見つかった一致を合計し、一致の合計がしきい値に達しているかどうかを判断します。たとえば、しきい値が 2 の body-contains メッセージフィルタがあるとします。本文に 1 つの一致があり、添付ファイルに 1 つの一致があるメッセージを受信します。AsyncOS がこのメッセージを採点した場合、合計が 2 つの一致になり、しきい値スコアを満たしていると判断します。

同様に、複数の添付ファイルがある場合、AsyncOS は添付ファイルごとにスコアを合計して、一致のスコアを判断します。たとえば、しきい値が 3 の attachment-contains フィルタ ルールがあるとします。2 つの添付ファイルがあるメッセージを受信し、各添付ファイルに 2 つの一致が含まれます。AsyncOS はこのメッセージを 4 つの一致と採点し、しきい値スコアを満たされていると判断します。

しきい値スコア マルチパート/代替 MIME 部分

カウントの重複を避けるため、同じコンテンツの 2 つの表現 (プレーンテキストと HTML) がある場合、AsyncOS は重複した部分からの一致を合計しません。代わりに、各部分の一致を比較して、最高値を選択します。AsyncOS はこの値をマルチパートメッセージの他の部分からのスコアに追加して、合計スコアを作成します。

たとえば、body-contains フィルタ ルールを設定し、しきい値を 4 に設定します。プレーンテキスト、HTML、および 2 つの添付ファイルを含むメッセージを受信します。メッセージは次のような構造を使用します。

```
multipart/mixed

    multipart/alternative

        text/plain

        text/html

    application/octet-stream

    application/octet-stream
```

body-contains フィルタ ルールは、メッセージの text/plain および text/html 部分を最初に採点して、このメッセージのスコアを判断します。次に、これらのスコアの結果を比較し、結果から最高のスコアを選択します。さらに、この結果を各添付ファイルからのスコアに追加して、最終スコアを判断します。メッセージに次の数の一致があるとします。

```
multipart/mixed

    multipart/alternative

        text/plain (2 matches)

        text/html (2 matches)
```

```
application/octet-stream (1 match)

application/octet-stream
```

AsyncOS は text/plain と text/html 部分の一致を比較するため、スコア 3 を返します。これは、フィルタ ルールをトリガーする最小しきい値を満たしていません。

コンテンツ ディクショナリを使用したしきい値のスコアリング

コンテンツ ディクショナリを使用すると、用語の「重み」を設定して、より簡単に特定の用語でフィルタ アクションをトリガーできます。たとえば、「bank」という用語ではメッセージフィルタをトリガーせず、「bank」の後に「account」という用語があり、さらに ABA ルーティング番号が含まれていれば、フィルタ アクションをトリガーする必要があるとします。これを実現するには、重みを設定したディクショナリを使用して、特定の用語または用語の組み合わせの重要度を高くします。コンテンツ ディクショナリを使うメッセージフィルタがフィルタ ルールの一致を評価する場合、コンテンツ ディクショナリの重みを使用して最終的なスコアを決定します。たとえば、次のコンテンツと重みを指定してコンテンツ ディクショナリを作成したとします。

表 9-1 コンテンツ ディクショナリの例

用語/スマート ID	重み
ABA Routing Number	3
Account	2
Bank	1

このコンテンツ ディクショナリを dictionary-match または attachment-dictionary-match メッセージフィルタ ルールに関連付けると、AsyncOS はメッセージ内で検出された一致する用語の各インスタンスの合計「スコア」に、この用語の重みを追加します。たとえば、メッセージ本文に用語「account」のインスタンスが 3 つ含まれているメッセージの合計スコアに、値 6 が追加されます。メッセージフィルタのしきい値が 6 に設定されている場合、AsyncOS はこのしきい値スコアが満たされたと判断します。または、各用語のインスタンスが 1 つずつ含まれている場合も合計値は 6 になり、このスコアによってフィルタ アクションがトリガーされます。

メッセージフィルタ内の AND テストと OR テスト

メッセージフィルタ内で、AND または OR テストを評価する場合、AsyncOS は不要なテストを評価しません。したがって、たとえば、一方の AND テストが false の場合、もう一方のテストは評価されません。テストは左から右に評価されるわけではないため、注意してください。代わりに、AND および OR テストが評価される場合、最も価値の低いテストが最初に評価されます。たとえば、次のフィルタでは、remote-ip テストが必ず最初に評価されます。その理由は、rcpt-to-group テストよりもコストが低いからです（一般に、LDAP テストのほうがコストが高くなります）。

```
andTestFilter:

if (remote-ip == "192.168.100.100" AND rcpt-to-group == "GROUP")

{ ... }
```


最もコストの低いテストが最初に実行されるため、項目の順序を入れ替えても影響はありません。テストの実行順序を保証する必要がある場合は、if 文をネストさせてください。この方法は、できる限りコストの高いテストを避けるためにも推奨します。

```
expensiveAvoid:

if (<simple tests>

    { if (<expensive test>)

        { <action> }

    }
```

次に、もう少し複雑な例で説明します。

```
if (test1 AND test2 AND test3) { ... }
```

システムは左から右に式をグループ化するため、次のようになります。

```
if ((test1 AND test2) AND test3) { ... }
```

この場合、最初に (test1 AND test2) のコストと test3 のコストを比較してから、最初に 2 番めの AND を評価します。3 つのテストすべてで同じコストがかかる場合、test3 が最初に実行されます。これは、(test1 AND test2) のコストが 2 倍になるためです。

メッセージフィルタ ルール

各メッセージフィルタには、フィルタを適用できるメッセージのコレクションを定義するルールが含まれています。フィルタルールを定義して、true を返すメッセージへのフィルタアクションを定義します。

フィルタ ルールの概要の表

表 9-2 に、メッセージフィルタで使用できるルールをまとめます。

表 9-2 メッセージフィルタ ルール

ルール	構文	説明
件名ヘッダー (Subject Header)	subject	件名ヘッダーが特定のパターンと一致しているか。「件名ルール」(P.9-22) を参照してください。
本文サイズ (Body Size)	body-size	本文のサイズは一定の範囲内か。「本文サイズルール」(P.9-25) を参照してください。
エンベロープ送信者 (Envelope Sender)	mail-from	エンベロープ送信者 (Envelope From, <MAIL FROM>) が指定したパターンと一致しているか。「エンベロープ送信者ルール」(P.9-23) を参照してください。

表 9-2 メッセージフィルタルール (続き)

ルール	構文	説明
グループ内のエンベロープ送信者 (Envelope Sender in Group)	mail-from-group	エンベロープ送信者 (Envelope From <MAIL FROM>) が、指定した LDAP グループ内に存在するか。「グループ内エンベロープ送信者ルール」(P.9-24) を参照してください。
送信者グループ (Sender Group)	sendergroup	どの送信者グループが、リスナーのホストアクセステーブル (HAT) に一致するか。「送信者グループルール」(P.9-24) を参照してください。
エンベロープ受信者 (Envelope Recipient)	rcpt-to	エンベロープ受信者 (Envelope To, <RCPT TO>) が指定したパターンと一致しているか。「エンベロープ受信者ルール」(P.9-22) を参照してください。 注: rcpt-to ルールはメッセージベースです。メッセージに複数の受信者が設定されている場合、いずれか 1 人の受信者がルールと一致していれば、指定した処理がすべての受信者に対するメッセージに適用されます。
グループ内のエンベロープ受信者 (Envelope Recipient in Group)	rcpt-to-group	エンベロープ受信者 (Envelope To, <RCPT TO>) が、指定した LDAP グループ内に存在するか。「グループ内エンベロープ受信者ルール」(P.9-23) を参照してください。 注: rcpt-to-group ルールはメッセージベースです。メッセージに複数の受信者がある場合、グループの受信者が 1 人だけ検出されれば、指定されたアクションがメッセージのすべての受信者に適用されます。
リモート IP (Remote IP)	remote-ip	リモートホストから送信されたメッセージは、指定した IP アドレスまたは IP ブロックに一致しているか。「リモート IP ルール」(P.9-25) を参照してください。
受信インターフェイス (Receiving Interface)	recv-int	メッセージは、指定された受信インターフェイス経由で届いたか。「受信 IP インターフェイスルール」(P.9-26) を参照してください。
受信リスナー (Receiving Listener)	recv-listener	メッセージは、指定されたリスナー経由で届いたか。「受信リスナールール」(P.9-26) を参照してください。
日付 (Date)	date	現在時刻は特定の日時の前か後か。「日付ルール」(P.9-26) を参照してください。
ヘッダー (Header)	header(<string>)	メッセージに特定のヘッダーが含まれているか。ヘッダーの値が特定のパターンと一致しているか。「ヘッダールール」(P.9-27) を参照してください。

表 9-2 メッセージフィルタ ルール (続き)

ルール	構文	説明
ランダム (Random)	<code>random(<integer>)</code>	ランダム番号は一定の範囲内か。「乱数ルール」(P.9-28)を参照してください。
受信者数 (Recipient Count)	<code>rcpt-count</code>	この電子メールの受信者の人数。「受信者数ルール」(P.9-28)を参照してください。
アドレス数 (Address Count)	<code>addr-count()</code>	受信者の累積数。 このフィルタは、エンベロープの受信者ではなくメッセージ本文のヘッダーに対して機能する点が <code>rcpt-count</code> フィルタ ルールと異なります。「アドレス数ルール」(P.9-29)を参照してください。
SPF ステータス (SPF Status)	<code>spf-status</code>	SPF 検証ステータスの値。このフィルタ ルールでは、さまざまな SPF 検証結果をクエリーできます。有効な SPF/SIDF 戻り値ごとに異なるアクションを入力できます。「SPF-Status ルール」(P.9-35)を参照してください。
SPF 合格 (SPF Passed)	<code>spf-passed</code>	SPF/SIDF 検証に合格したか。このフィルタ ルールは SPF/SIDF 結果をブール値として一般化します。「SPF-Passed ルール」(P.9-37)を参照してください。
イメージ評価 (Image verdict)	<code>image-verdict</code>	イメージ スキャンの評価の結果。このフィルタ ルールを使用して、さまざまなイメージ分析の評価について問い合わせることができます。「イメージ分析」(P.9-69)を参照してください。
ワークキュー数 (Workqueue count)	<code>workqueue-count</code>	ワーク キュー数と指定した値の比較結果 (等しい、多い、少ない)。「workqueue-count ルール」(P.9-37)を参照してください。
本文スキャン (Body Scanning)	<code>body-contains(<regular expression>)</code>	指定したパターンと一致するテキストまたは添付ファイルがメッセージに含まれているか。パターンの発生回数が、しきい値で指定した最小回数以上である必要があります。 エンジンは、配信ステータス部分と関連する添付ファイルをスキャンします。 「本文スキャン ルール」(P.9-29)を参照してください。
本文スキャン (Body Scanning)	<code>only-body-contains(<regular expression>)</code>	指定したパターンと一致するテキストがメッセージ本文に含まれているか。パターンの発生回数が、しきい値で指定した最小回数以上である必要があります。添付ファイルはスキャンされません。「本文スキャン」(P.9-29)を参照してください。
暗号化検出 (Encryption Detection)	<code>encrypted</code>	メッセージは暗号化されているか。「暗号化検出ルール」(P.9-30)を参照してください。

表 9-2 メッセージフィルタルール (続き)

ルール	構文	説明
添付ファイル名 (Attachment Filename) ^a	attachment-filename	指定したパターンと一致するファイル名の添付ファイルがメッセージに含まれているか。「添付ファイル名ルール」(P.9-31)を参照してください。
添付ファイルタイプ (Attachment Type) ^a	attachment-type	特定の MIME タイプの添付ファイルがメッセージに含まれているか。「添付ファイルタイプルール」(P.9-31)を参照してください。
添付ファイルのファイルタイプ (Attachment File Type) ^a	attachment-filetype	フィンガープリントに基づく特定のパターンと一致するファイルタイプの添付ファイルがメッセージに含まれているか (UNIX の file コマンドと同様)。添付ファイルが Excel または Word ドキュメントである場合、埋め込みファイルタイプの .exe、.dll、.bmp、.tiff、.pcx、.gif、.jpeg、png、および Photoshop イメージを検索することもできます。 有効なフィルタを作成するには、ファイルタイプを引用符で囲む必要があります。一重引用符または二重引用符を使用できます。たとえば、.exe 添付ファイルを検索するには、次の構文を使用します。 <pre>if (attachment-filetype == "exe")</pre> 詳細については、「添付ファイルのスキャンメッセージフィルタの例」(P.9-75)を参照してください。
添付ファイル MIME タイプ (Attachment MIME Type) ^a	attachment-mimetype	特定の MIME タイプの添付ファイルがメッセージに含まれているか。このルールは attachment-type ルールに似ていますが、MIME 添付ファイルで指定された MIME タイプのみが評価される点が異なります。(明示的にファイルタイプが指定されていない場合、アプリケーションはファイルの拡張子からファイルのタイプを推測しようとしません)。「添付ファイルのスキャンメッセージフィルタの例」(P.9-75)を参照してください。
保護された添付ファイル (Attachment Protected)	attachment-protected	パスワード保護された添付ファイルがメッセージに含まれているか。「保護された添付ファイルの隔離」(P.9-78)を参照してください。

表 9-2 メッセージフィルタ ルール (続き)

ルール	構文	説明
保護されていない添付ファイル (Attachment Unprotected)	attachment-unprotected	<p>attachment-unprotected フィルタ条件は、保護されていない添付ファイルをスキャン エンジンが検出した場合に true を返します。スキャン エンジンが添付ファイルを読み取ることができた場合、そのファイルは保護されていないと見なされます。zip ファイルに保護されていないメンバが含まれている場合、その zip ファイルは保護されていないと見なされます。</p> <p>注： attachment-unprotected フィルタ条件と attachment-protected フィルタ条件は、相互に排他的ではありません。同じ添付ファイルのスキャンすると、両方のフィルタ条件で true が返される場合があります。これは、たとえば、zip ファイルに保護されたメンバと保護されていないメンバの両方が含まれている場合に発生します。</p> <p>「保護されていない添付ファイルの検出」(P.9-78) を参照してください。</p>
添付ファイルのスキャン (Attachment Scanning) ^a	attachment-contains (<regular expression>)	<p>指定したパターンと一致するテキストまたは別の添付ファイルが、メッセージの添付ファイルに含まれているか。パターンの発生回数が、しきい値で指定した最小回数以上である必要があります。</p> <p>このルールは body-contains () ルールと似ていますが、このルールでは、メッセージの全体の「本文」をスキャンしないようにします。つまり、ユーザが添付ファイルとして表示する場合だけスキャンします。「添付ファイルのスキャンメッセージフィルタの例」(P.9-75) を参照してください。</p>
添付ファイルのスキャン (Attachment Scanning)	attachment-binary-contains (<regular expression>)	<p>指定したパターンと一致するバイナリ データが存在する添付ファイルがメッセージに含まれているか。</p> <p>このルールは attachment-contains () ルールに似ていますが、バイナリ データ内のパターンのみを検索します。</p>
添付ファイルのスキャン (Attachment Scanning)	every-attachment-contains (<regular expression>)	<p>このメッセージのすべての添付ファイルに、特定のパターンと一致するテキストが含まれているか。対象のテキストがすべての添付ファイル内に存在する必要があります。つまり実際に実行されるアクションは、各添付ファイルに対する「attachment-contains ()」の論理 AND 演算です。本文はスキャンされません。パターンの発生回数が、しきい値で指定した最小回数以上である必要があります。</p> <p>「添付ファイルのスキャンメッセージフィルタの例」(P.9-75) を参照してください。</p>

表 9-2 メッセージフィルタルール (続き)

ルール	構文	説明
添付ファイルのサイズ (Attachment Size) ^a	attachment-size	メッセージに含まれている添付ファイルのサイズが特定の範囲内に収まっているか。このルールは body-size ルールに似ていますが、メッセージの「本文」全体のスキャンを避けるよう試みます。つまり、ユーザが添付ファイルとして表示する場合だけスキャンします。このサイズは、デコードする前に評価されます。「添付ファイルのスキャンメッセージフィルタの例」(P.9-75)を参照してください。
公開ブラックリスト (Public Blacklists)	dnslist(<query server>)	送信者の IP アドレスがパブリック ブラックリスト サーバ (RBL) 内に存在するか。「DNS リストルール」(P.9-32)を参照してください。
SenderBase レピュテーション (SenderBase Reputation)	reputation	送信者の SenderBase レピュテーション スコアの値。「SenderBase レピュテーションルール」(P.9-33)を参照してください。
SenderBase レピュテーションなし (No SenderBase Reputation)	no-reputation	SenderBase レピュテーションが「None」の場合に使用します。「SenderBase レピュテーションルール」(P.9-33)を参照してください。
ディクショナリ (Dictionary) ^b	dictionary-match(<dictionary_name>)	メッセージ本文に、dictionary_name で指定した名前のコンテンツ ディクショナリの正規表現または用語が含まれているかどうかを判別します。パターンの発生回数が、しきい値で指定した最小回数以上である必要があります。「辞書ルール」(P.9-34)を参照してください。
添付ディクショナリー致 (Attachment Dictionary Match)	attachment-dictionary-match(<dictionary_name>)	添付ファイルに、dictionary_name で指定した名前のコンテンツ ディクショナリの正規表現が含まれているかどうかを判別します。パターンの発生回数が、しきい値で指定した最小回数以上である必要があります。「辞書ルール」(P.9-34)を参照してください。
件名ディクショナリー致 (Subject Dictionary Match)	subject-dictionary-match(<dictionary_name>)	件名ヘッダーに、dictionary_name で指定した名前のコンテンツ ディクショナリの正規表現または用語が含まれているかどうかを判別します。「辞書ルール」(P.9-34)を参照してください。
ヘッダー ディクショナリー致 (Header Dictionary Match)	header-dictionary-match(<dictionary_name>, <header>)	指定したヘッダー (大文字と小文字を区別) に、dictionary_name で指定した名前のコンテンツ ディクショナリの正規表現または用語が含まれているかどうかを判別します。「辞書ルール」(P.9-34)を参照してください。

表 9-2 メッセージフィルタ ルール (続き)

ルール	構文	説明
本文ディクショナリー一致 (Body Dictionary Match)	<code>body-dictionary-match(<dictionary_name>)</code>	このフィルタ条件は、辞書の用語がメッセージ本文に含まれていれば <code>true</code> を返します。このフィルタの検索対象となるのは、添付ファイルと見なされていない MIME 部分内の用語です。また、ユーザが定義したしきい値が満たされた場合も <code>true</code> を返します (デフォルトのしきい値は 1 です)。「辞書ルール」(P.9-34) を参照してください。
エンベロープ受信者ディクショナリー一致 (Envelope Recipient Dictionary Match)	<code>rcpt-to-dictionary-match(<dictionary_name>)</code>	エンベロープ受信者に、 <code>dictionary_name</code> で指定した名前のコンテンツ ディクショナリーの正規表現または用語が含まれているかどうかを判別します。「辞書ルール」(P.9-34) を参照してください。
エンベロープ送信者ディクショナリー一致 (Envelope Sender Dictionary Match)	<code>mail-from-dictionary-match(<dictionary_name>)</code>	エンベロープ送信者に、 <code>dictionary_name</code> で指定した名前のコンテンツ ディクショナリーの正規表現または用語が含まれているかどうかを判別します。「辞書ルール」(P.9-34) を参照してください。
SMTP 認証済みユーザー一致 (SMTP Authenticated User Match)	<code>smtp-auth-id-matches(<target> [, <sieve-char>])</code>	エンベロープ送信者のアドレスとメッセージヘッダーのアドレスが、送信者の認証済み SMTP ユーザ ID と一致するかどうかを判別します。「SMTP Authenticated User Match ルール」(P.9-38) を参照してください。
True	<code>true</code>	すべてのメッセージと一致します。「true ルール」(P.9-21) を参照してください。
有効 (Valid)	<code>valid</code>	メッセージに解析不能または無効な MIME 部分がある場合に <code>false</code> を返し、それ以外の場合は <code>true</code> を返します。「valid ルール」(P.9-21) を参照してください。
署名済み (Signed)	<code>signed</code>	メッセージが署名済みであるかどうかを判別します。「signed ルール」(P.9-40) を参照してください。
署名証明書 (Signed Certificate)	<code>signed-certificate(<field> [<operator> <regular expression>])</code>	メッセージ署名者または X.509 証明書発行者が特定のパターンと一致するかどうかを判別します。「Signed Certificate ルール」(P.9-40) を参照してください。

- 添付ファイルのフィルタリングについては、「添付ファイルのスキャン」(P.9-67) を参照してください。
- コンテンツ ディクショナリーの詳細については、「Text Resources」の章で説明しています。

Cisco アプライアンスに送信されるメッセージはいずれも、すべてのメッセージフィルタで順番に処理されますが、最終アクションを指定した場合はそのアクションによりメッセージに対する以降の処理が停止されます。(「メッセージフィルタアクション」(P.9-2) を参照してください)。フィルタはすべてのメッセージに適用することもでき、ルールは論理接続子 (AND、OR、NOT) を使用して結合することもできます。

ルールで使用する正規表現

ルールの定義に使用するアトミックテストの一部では、**正規表現照合**を行います。正規表現は複雑になる場合があります。次の表は、メッセージフィルタルールで正規表現を適用する場合の目安として使用してください。

表 9-3 ルールで使用する正規表現

正規表現 (abc)	フィルタルールでの正規表現が文字列と一致すると判断されるのは、正規表現の一連の指示が文字列のいずれかの部分と一致する場合です。 たとえば、正規表現「Georg」は「George Of The Jungle」、「Georgy Porgy」、「La Meson Georgette」、「Georg」の各文字列と一致します。
キャラクタ (^) ドル記号 (\$)	ドル記号 (\$) を含むルールは文字列の末尾のみと一致し、キャラクタ (^) を含むルールは文字列の先頭のみと一致します。 たとえば、正規表現「^Georg\$」は文字列「Georg」のみと一致します。 空のヘッダーを検索するには、「"^\\$"」と指定します。
文字、空白、アットマーク (@)	文字、空白、アットマーク (@) を含むルールは、当該の文字自体と完全に一致します。 たとえば、正規表現「^George@admin\$」は文字列「George@admin」のみと一致します。
ピリオド (.)	ピリオド (.) を含むルールは任意の 1 文字（改行を除く）と一致します。 たとえば、「^...admin\$」という正規表現は「macadmin」および「sunadmin」の各文字列とは一致しますが、「win32admin」とは一致しません。
アスタリスク (*)	アスタリスク (*) を含むルールは、「直前に指定されている文字が 0 回を含む任意の回数繰り返されている文字」と一致します。ピリオドとアスタリスクが続く場合 (.*)、任意の文字（改行を除く）と一致します。 たとえば、「^P.*Piper\$」という正規表現は、「PPiper」、「Peter Piper」、「P.Piper」、「Penelope Penny Piper」のどの文字列とも一致します。
円記号 (\)	円記号は特殊文字のエスケープに使用します。したがって、\. と続けると、ピリオドそのもののみ一致し、\\$ はドル記号のみ一致し、\^ はキャレット記号のみ一致します。たとえば、「^ik\.ac\.uk\$」は「ik.ac.uk」という文字列のみと一致します。 重要： 円記号はパーサーでも特殊なエスケープ文字として使用します。そのため、正規表現で円記号を使用する場合、2 つの円記号が必要です。解析後には「実際に」使用される円記号 1 つのみが残り、正規表現システムに渡されます。上記の例を照合する場合は「^ik\\.ac\\.uk\$」と入力することになります。

表 9-3 ルールで使用する正規表現（続き）

大文字と小文字を区別しない (?i)	トークン (?i) は、正規表現の残りの部分で大文字と小文字が区別されないことを表します。このトークンを、大文字と小文字を区別する正規表現の先頭に配置すると、大文字と小文字が一切区別されない照合が行われます。 たとえば、「(?i)viagra」という正規表現は、「viagra」、「vIaGrA」、「VIAGRA」と一致します。
繰り返し回数 {min,max}	1つ前のトークンの繰り返し回数を指定する正規表現表記がサポートされています。 たとえば、「fo{2,3}」は「foo」および「fooo」とは一致しますが、「fo」や「fofo」とは一致しません。 if(header('To') == "^.{500,}") というステートメントは、500文字以上が使用されている「To」ヘッダーを検索します。
論理和 ()	代替、つまり「or」演算子に相当します。A と B が正規表現の場合、「A B」は A と B のいずれかに一致する文字列と一致します。 たとえば、「foo bar」という表現は foo や bar とは一致しますが、foobar とは一致しません。

メッセージのフィルタリングでの正規表現の使用

フィルタを使用して、ASCII 以外の形式でエンコードされているメッセージの内容（ヘッダーと本文）の文字列とパターンを検索できます。具体的には、本システムでは次の場所にある非 ASCII 文字を検索する正規表現 (regex) を使用できます。

- メッセージヘッダー
- MIME 添付ファイル名の文字列
- メッセージ本文
 - MIME ヘッダーがない本文（従来の形式の電子メール）
 - エンコードを示す MIME ヘッダーがあり、MIME 部分がない本文
 - エンコードが指定されているマルチパート MIME メッセージ
 - 上記の本文のうち、MIME ヘッダーでエンコードが指定されていないもの

メッセージまたは本文の任意の部分（添付ファイルを含む）の照合に正規表現を使用できます。添付ファイルのタイプとして HTML、MS Word、Excel など多数のタイプを対象にできます。対象となる文字セットとして、gb2312、HZ、EUC、JIS、Shift-JIS、Big5、Unicode などがあります。正規表現のメッセージフィルタルールを作成するには、コンテンツ フィルタ GUI を使用するか、テキストエディタでファイルを作成してからシステムにインポートします。詳細については、「[CLI を使用したメッセージフィルタの管理](#)」(P.9-79) および「[スキャンパラメータの変更](#)」(P.9-88) を参照してください。

正規表現の使用に関するガイドライン

プレフィックスではなく文字列全体を照合する場合は、正規表現の先頭にキャレット (^)、末尾にドル記号 (\$) をそれぞれ配置する必要があります。

効率的なフィルタの作成

次の例は、同じ処理を行う2つのフィルタですが、最初の例の方がCPUの使用率が高くなります。2番目のフィルタの方が効率的な正規表現を使用しています。

```
attachment-filter: if (recv-listener == "Inbound") AND
((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((((
"\\.386$") OR (attachment-filename == "\\exe$") OR (attachment-filename == "\\ad$")
OR (attachment-filename == "\\ade$")) OR (attachment-filename == "\\adp$")) OR
(attachment-filename == "\\asp$")) OR (attachment-filename == "\\bas$")) OR
(attachment-filename == "\\bat$")) OR (attachment-filename == "\\chm$")) OR
(attachment-filename == "\\cmd$")) OR (attachment-filename == "\\com$")) OR
(attachment-filename == "\\cpl$")) OR (attachment-filename == "\\crt$")) OR
(attachment-filename == "\\exe$")) OR (attachment-filename == "\\hlp$")) OR
(attachment-filename == "\\hta$")) OR (attachment-filename == "\\inf$")) OR
(attachment-filename == "\\ins$")) OR (attachment-filename == "\\isp$")) OR
(attachment-filename == "\\js$")) OR (attachment-filename == "\\jse$")) OR
(attachment-filename == "\\lnk$")) OR (attachment-filename == "\\mdb$")) OR
(attachment-filename == "\\mde$")) OR (attachment-filename == "\\msc$")) OR
(attachment-filename == "\\msi$")) OR (attachment-filename == "\\msp$")) OR
(attachment-filename == "\\mst$")) OR (attachment-filename == "\\pcd$")) OR
(attachment-filename == "\\pif$")) OR (attachment-filename == "\\reg$")) OR
(attachment-filename == "\\scr$")) OR (attachment-filename == "\\sct$")) OR
(attachment-filename == "\\shb$")) OR (attachment-filename == "\\shs$")) OR
(attachment-filename == "\\url$")) OR (attachment-filename == "\\vb$")) OR
(attachment-filename == "\\vbe$")) OR (attachment-filename == "\\vbs$")) OR
(attachment-filename == "\\vss$")) OR (attachment-filename == "\\vst$")) OR
(attachment-filename == "\\vsw$")) OR (attachment-filename == "\\ws$")) OR
(attachment-filename == "\\wsc$")) OR (attachment-filename == "\\wsf$")) OR
(attachment-filename == "\\wsh$")) { bounce(); }
```

この例では、AsyncOS は正規表現エンジンを30回（添付ファイルタイプとrecv-listenerのそれぞれに1回ずつ）起動する必要があります。

かわりに、次のようなフィルタを作成します。

```
attachment-filter: if (recv-listener == "Inbound") AND (attachment-filename ==
"\\. (386|exe|ad|ade|adp|asp|bas|bat|chm|cmd|com|cpl|crt|exe|hlp|hta|inf|ins|isp|js|jse|l
nk|mdb|mde|mde|msc|msi|msp|mst|pcd|pif|reg|scr|sct|shb|shs|url|vb|vbe|vbs|vss|vst|vsw|ws|wsc
|wsf|wsh)$") {

    bounce ();

}
```

正規表現エンジンの起動回数は2回だけで、「()」の追加やスペルの誤りについて心配する必要がなくなるためフィルタの管理も大幅に簡単になります。また、最初の例に比べてCPUオーバーヘッドが低下します。

PDF と正規表現

PDF の生成方法によっては、スペースや改行がないことがあります。このような場合、スキャンエンジンは、ページ内の単語の位置に基づき、論理的なスペースと改行の挿入を試みます。たとえば、1つの単語の中に複数のフォントやフォントサイズが混在する場合、生成される PDF コードからスキャンエンジンが単語と改行を判別するのが難しくなります。このように生成された PDF ファイルで正規表現による照合を行うと、スキャンエンジンは予期しない結果を返す場合があります。

たとえば、PowerPoint 文書に挿入した単語の中に、単語内の文字ごとに異なるフォントやフォントサイズが設定されているものがあるとします。このアプリケーションから生成された PDF をスキャンエンジンが読み取ると、論理的なスペースと改行が挿入されます。PDF の構造が原因で、「callout」という単語が「call out」や「c a l lout」と解釈される場合があります。このレンダリング結果を正規表現「callout」で照合しようとする、一致なしと判断されます。

スマート ID

メッセージの内容をスキャンするメッセージルールを使用する場合、スマート ID を使用するとデータ内の特定のパターンを検出できます。

スマート ID で、データ内の次のパターンを検出できます。

- クレジットカード番号
- 米国 社会保障番号
- CUSIP ナンバー
- ABA ナンバー

フィルタでスマート ID を使用するには、本文または添付ファイルのコンテンツをスキャンするフィルタルールで次のキーワードを使用します。

表 9-4 メッセージフィルタのスマート ID

キーワード	スマート ID	説明
*credit	クレジットカード番号	14、15、および 16 桁のクレジットカード番号を識別します。 (注) スマート ID では enRoute および JCB カードは識別されません。
*aba	ABA 送金番号	ABA 送金番号を識別します。
*ssn	社会保障番号	米国 社会保障番号を識別します。 *ssn スマート ID はダッシュ、ピリオド、スペースがある社会保障番号を識別します。
*cusip	CUSIP 番号	CUSIP 番号を識別します。

スマート ID の構文

フィルタルールでスマート ID を使用する場合、次の例のように、本文または添付ファイルをスキャンするフィルタルールの中でスマート ID キーワードを引用符で囲みます。

```
ID_Credit_Cards:
if(body-contains("*credit")){
```

```
notify("legaldept@example.com");  
  
}  
.
```

また、コンテンツディクショナリの一部としてコンテンツフィルタ内でスマートIDを使用することもできます。



(注) スマートIDキーワードは通常の正規表現や他のキーワードと組み合わせて使用できません。たとえば、「*credit|*ssn」というパターンは有効ではありません。



(注) *ssn スマートIDによる誤判定を防ぐため、*ssn スマートIDは他のフィルタ条件とあわせて使用すると有用な場合があります。たとえば、「only-body-contains」フィルタ条件を使用することができます。この場合、検索文字列がメッセージ本文のすべてのMIME部分に存在する場合のみ式がtrueであると判定されます。たとえば、次のようなフィルタを作成できます。

```
SSN-nohtml: if only-body-contains("*ssn") { duplicate-quarantine("Policy");}
```

メッセージフィルタルールの例

次のセクションでは、メッセージフィルタの使用例を照会します。

true ルール

true ルールはすべてのメッセージと一致します。たとえば、次のルールはテスト対象となるすべてのメッセージについて、IP インターフェイスを external に変更します。

```
externalFilter:  
  
  if (true)  
  
  {  
  
    alt-src-host('external');  
  
  }
```

valid ルール

valid ルールは、メッセージに解析不能または無効な MIME 部分が含まれている場合に false を返し、それ以外の場合は true を返します。たとえば、次のルールはテスト対象のメッセージのうち解析不能なメッセージをすべてドロップします。

```
not-valid-mime:  
  
  if not valid
```

```
{
    drop();
}
```

件名ルール

subject ルールは、件名ヘッダーの値が指定した正規表現と一致するメッセージを選択します。

たとえば、次のフィルタは、件名が「Make Money」という語句で始まるすべてのメッセージを廃棄します。

```
scamFilter:
    if (subject == '^Make Money')
    {
        drop();
    }
```

ヘッダーの値で検索する非 ASCII 文字を指定することができます。

ヘッダーに関する操作を行う場合、ヘッダーの現在の値には処理中に行われた変更（メッセージのヘッダーの追加、削除、変更を行うフィルタ処理など）が含まれている点に注意してください。詳細については、「[メッセージヘッダールールおよび評価](#)」(P.9-5)を参照してください。

次のフィルタは、ヘッダーが空の場合、またはメッセージにヘッダーがない場合に true を返します。

```
EmptySubject_To_filter:
if (header('Subject') != ".") OR
    (header('To') != ".") {
    drop();
}
```



(注)

このフィルタは Subject ヘッダーと To ヘッダーが空の場合に true を返しますが、ヘッダーがない場合も true を返します。指定したヘッダーがメッセージ内にない場合でも、このフィルタは true を返します。

エンベロープ受信者ルール

rcpt-to ルールは、いずれかのエンベロープ受信者が指定した正規表現と一致するメッセージを選択します。たとえば、次のフィルタは「scarface」という文字列を含む電子メールアドレス宛てに送信されたすべてのメッセージをドロップします。



(注) rcpt-to ルールで使用する正規表現では、大文字と小文字は区別されません。

```
scarfaceFilter:

    if (rcpt-to == 'scarface')

    {

        drop();

    }
```



(注) rcpt-to ルールはメッセージに基づいています。メッセージに複数の受信者が設定されている場合、いずれか1人の受信者がルールと一致していれば、指定した処理がすべての受信者に対するメッセージに適用されます。

グループ内エンベロープ受信者ルール

rcpt-to-group ルールは、いずれかのエンベロープ受信者が指定した LDAP グループのメンバであるメッセージを選択します。たとえば、次のフィルタは「ExpiredAccounts」という LDAP グループ内の電子メールアドレス宛てに送信されたすべてのメッセージをドロップします。

```
expiredFilter:

    if (rcpt-to-group == 'ExpiredAccounts')

    {

        drop();

    }
```



(注) rcpt-to-group ルールはメッセージに基づいています。メッセージに複数の受信者が設定されている場合、いずれか1人の受信者がルールと一致していれば、指定した処理がすべての受信者に対するメッセージに適用されます。

エンベロープ送信者ルール

mail-from ルールは、エンベロープ送信者が指定した正規表現と一致するメッセージを選択します。たとえば、次のフィルタを実行すると admin@yourdomain.com により送信されたすべてのメッセージがただちに出力されます。



(注)

mail-from ルールで使用する正規表現では、大文字と小文字は区別されません。次の例では、ピリオドがエスケープ処理されています。

```
kremFilter:

    if (mail-from == '^admin@yourdomain\\.com$')

    {

    skip-filters();

    }
```

グループ内エンベロープ送信者ルール

mail-from-group ルールは、エンベロープ送信者が演算子の右辺で指定した LDAP グループに属している（不一致を検索する場合は、送信者の電子メールアドレスが指定した LDAP グループに属していない）メッセージを選択します。たとえば、次のフィルタを実行すると、「KnownSenders」という LDAP グループの電子メールアドレスにより送信されたすべてのメッセージがただちに出力されます。

```
SenderLDAPGroupFilter:

    if (mail-from-group == 'KnownSenders')

    {

    skip-filters();

    }
```

送信者グループルール

sendergroup メッセージフィルタは、リスナーのホスト アクセス テーブル (HAT) でどの送信者グループが一致するかに基づいて、メッセージを選択します。このルールは「==」（一致を検索する場合）または「!=」（不一致を検索する場合）を使用して、指定した正規表現（式の右辺）との一致をテストします。たとえば、次のメッセージフィルタルールは、メッセージの送信者グループが正規表現「Internal」と一致する場合に true を返し、その場合はメッセージを代替メールホストに送信します。

```
senderGroupFilter:

    if (sendergroup == "Internal")

    {

        alt-mailhost("[172.17.0.1]");

    }
```


本文サイズ ルール

本文サイズとはメッセージのサイズのことで、ヘッダーと添付ファイルも含まれます。body-size ルールは、指定に従い本文のサイズを特定の数値を比較します。たとえば、次のフィルタは本文サイズが 5 メガバイトを超えるすべてのメッセージをバウンスします。

```
BigFilter:

    if (body-size > 5M)

    {

        bounce();

    }
```

body-size を使用すると次のような比較ができます。

例	比較の種類
body-size < 10M	より小さい
body-size <= 10M	以下
body-size > 10M	より大きい
body-size >= 10M	以上
body-size == 10M	等しい
body-size != 10M	等しくない

サイズ指定にはサフィクスを使用すると便利です。

数量	説明
10b	10 バイト（「10」に同じ）
13k	13 キロバイト
5M	5 メガバイト
40G	40 ギガバイト（注：Cisco では 100 メガバイトを超えるメッセージを処理できません）

リモート IP ルール

remote-ip ルールは、メッセージを送信したホストの IP アドレスが特定のパターンと一致するかどうかを確認するためのテストを実行します。IP アドレスは、インターネットプロトコルバージョン 4 (IPv4) またはインターネットプロトコルバージョン 6 (IPv6) を指定できます。IP アドレスのパターンは、「送信者グループの構文」で説明している **allowed hosts** 表記（SBO、SBRs、dnslist の各表記と特殊キーワード ALL を除く）を使用して指定されます。

allowed hosts 表記では、IP アドレス（ホスト名ではない）の順序と数値での範囲のみを指定できます。たとえば、次のフィルタは 10.1.1.x（x は 50、51、52、53、54、55 のいずれか）の形式の IP アドレスから送信されていないすべてのメッセージをバウンスします。

```
notMineFilter:

    if (remote-ip != '10.1.1.50-55')
```

```

{
    bounce ();
}

```

受信リスナー ルール

recv-listener ルールは、名前付きリスナーで受信したメッセージを選択します。リスナー名は、現在システム上で設定されているリスナーのいずれかのニックネームである必要があります。たとえば、次のフィルタを実行すると、expedite という名前のリスナーから受信したすべてのメッセージがただちに出力されます。

```

expediteFilter:

    if (recv-listener == 'expedite')

    {

        skip-filters ();

    }

```

受信 IP インターフェイス ルール

recv-int ルールは、名前付きインターフェイス経由で受信したメッセージを選択します。インターフェイス名は、現在システムに設定されているインターフェイスのいずれかのニックネームである必要があります。たとえば、次のフィルタは、outside という名前のインターフェイスから受信したすべてのメッセージをバウンスします。

```

outsideFilter:

    if (recv-int == 'outside')

    {

        bounce ();

    }

```

日付ルール

date ルールは、現在の日時と指定した時刻を照合します。date ルールは *MM/DD/YYYY hh:mm:ss* という形式のタイムスタンプがある文字列との比較を行います。このルールは、特定の日時（米国形式）の前または後に実行する処理を指定する場合に便利です。（米国以外の日付形式を使用しているメッセージを検索する場合は問題が発生することがあります）。次のフィルタは、2003年7月28日の午後1時より後に campaign1@yourdomain.com から送信されたすべてのメッセージをバウンスします。

```

TimeOutFilter:

    if ((date > '07/28/2003 13:00:00') and (mail-from ==

```

```
'campaign1@yourdomain\\.com'))  
  
{  
  
    bounce();  
  
}
```



(注)

date ルールを \$Date メッセージフィルタ処理変数と混同しないようにしてください。

ヘッダー ルール

header() ルールは、メッセージヘッダーがかっこ内で引用されている特定のヘッダー ("ヘッダー名") と一致するかどうかを確認します。このルールは subject ルールと同様に正規表現と比較することもできますが、比較を行わずに使用することもできます。この場合、メッセージにそのヘッダーがあれば「true」、なければ「false」となります。たとえば、次の例ではヘッダー X-Sample の有無、およびこのヘッダーの値に「sample text」という文字列が含まれているかどうかを確認しています。一致する場合は、メッセージがバウンスされます。

FooHeaderFilter:

```
if (header('X-Sample') == 'sample text')  
  
{  
  
    bounce();  
  
}
```

ヘッダーの値で検索する非 ASCII 文字を指定することができます。

次の例では、比較を行わずにヘッダー ルールを適用しています。この場合、ヘッダー X-DeleteMe が見つかったら、そのヘッダーがメッセージから削除されます。

DeleteMeHeaderFilter:

```
if header('X-DeleteMe')  
  
{  
  
    strip-header('X-DeleteMe');  
  
}
```

ヘッダーに関する操作を行う場合、ヘッダーの現在の値には処理中に行われた変更 (メッセージのヘッダーの追加、削除、変更を行うフィルタ処理など) が含まれている点に注意してください。詳細については、「[メッセージヘッダールールおよび評価](#)」(P.9-5) を参照してください。

乱数ルール

random ルールは、0 から N-1 (N はルール名の後のかっこで指定される整数値) までの乱数を生成します。このルールでは header() ルールと同様に比較を行うこともできますが、「単項」形式で単独使用することもできます。単項形式では、生成された乱数が 0 でない場合に true と評価されます。たとえば、次のフィルタはいずれも内容としては同じもので、2 分の 1 の確率で Virtual Gateway アドレス A が選択され、残り 2 分の 1 の確率で Virtual Gateway アドレス B が選択されます。

```
load_balance_a:

    if (random(10) < 5) {

        alt-src-host('interface_a');

    } else {

        alt-src-host('interface_b');

    }
```

```
load_balance_b:

    if (random(2)) {

        alt-src-host('interface_a');

    } else {

        alt-src-host('interface_b');

    }
```

受信者数ルール

rcpt-count ルールは、body-size ルールと同様に、メッセージの受信者の数を整数値と比較します。このルールを使用すると、ユーザが一度に多数のユーザに電子メールを送信することを防止でき、また大規模なメール送信キャンペーンが特定の Virtual Gateway アドレス経由で行われるようにすることができます。次の例では、受信者数が 100 件を超える電子メールが特定の Virtual Gateway アドレスを経由して送信されます。

```
large_list_filter:

    if (rcpt-count > 100) {

        alt-src-host('mass_mailing_interface');

    }
```

アドレス数ルール

`addr-count()` メッセージフィルタルールは、1つ以上のヘッダー文字列を対象に、各行の受信者数を計算し、受信者の累積数をレポートします。このフィルタは、エンベロープの受信者ではなくメッセージ本文のヘッダーに対して機能する点が `rcpt-count` フィルタルールと異なります。次の例では、このフィルタルールにより長い受信者リストが「`undisclosed-recipients`」というエイリアスに置き換えられています。

```
count: if (addr-count("To", "Cc") > 30) {  
  
    strip-header("To");  
  
    strip-header("Cc");  
  
    insert-header("To", "undisclosed-recipients");  
  
}
```

本文スキャンルール

`body-contains()` ルールは、受信する電子メールとその添付ファイルをスキャンし、パラメータで定義された特定のパターンの有無を確認します。これには、配信ステータス部および関連付けられている添付ファイルが含まれます。`body-contains()` ルールでは複数行を対象とした照合は行われません。スキャンのロジックを CLI の `scanconfig` コマンドで変更することにより、スキャンの対象となる、またはスキャンの対象から除外する MIM タイプを定義できます。また、スキャン結果を `true` と評価するために検出する必要がある一致の最小数を指定することもできます。

デフォルトでは、MIME タイプが `video/*`、`audio/*`、`image/*` 以外であるすべての添付ファイルがスキャンされます。複数のファイルが含まれている `.zip`、`.bzip`、`.compress`、`.tar`、`.gzip` の各アーカイブ添付ファイルがスキャンされます。スキャン対象となる、「ネストされた」アーカイブ添付ファイル (`.zip` に格納されている `.zip` など) の数を設定できます。

`scanconfig` コマンドを使用して添付ファイルのスキャン処理を設定する方法の例などの詳細については、「[スキャンパラメータの変更](#)」(P.9-88) を参照してください。

本文スキャン

AsyncOS が本文スキャンを実行する場合、正規表現を使用して本文のテキストと添付ファイルをスキャンします。式には最小しきい値を指定することができ、スキャンエンジンがこの最小回数だけ正規表現との一致を検出すると、この式は `true` と評価されます。

AsyncOS はメッセージの各種の MIME 部分を評価し、テキスト形式になっているすべての MIME 部分をスキャンします。最初の部分で MIME タイプがテキストに指定されている場合、AsyncOS はテキスト部分を識別します。AsyncOS はメッセージで指定されたエンコードに基づいてエンコードを決定し、テキストを Unicode に変換します。その後、Unicode 領域で正規表現を検索します。メッセージでエンコードが指定されていない場合は、`scanconfig` コマンドで指定されたエンコードが使用されません。

メッセージのスキャン時に AsyncOS が MIME 部分を評価する方法の詳細については、「[メッセージ本文とメッセージ添付ファイル](#)」(P.9-5) を参照してください。

MIME 部分がテキストでない場合、AsyncOS は `.zip` または `.tar` からファイルを抽出するか、圧縮されたファイルを抽出します。データを抽出した後、スキャンエンジンはファイルのエンコードを識別し、ファイルのデータを Unicode 形式で返します。その後、AsyncOS は Unicode 領域で正規表現を検索します。

次の例では、本文のテキストと添付ファイルで「Company Confidential」という文字列を検索しています。この例では、最小しきい値が2件に設定されているため、スキャンエンジンがこの文字列を2件以上検出すると、該当するメッセージをすべてバウンスし、法務部門に通知します。

ConfidentialFilter:

```
if (body-contains('Company Confidential',2)) {
    notify ('legaldept@example.domain');
    bounce();
}
```

メッセージの本文のみをスキャンする場合は、`only-body-contains` を使用します。

disclaimer:

```
if (not only-body-contains('[dD]disclaimer',1)) {
    notify('hresource@example.com');
}
```

暗号化検出ルール

`encrypted` ルールは、メッセージの内容に暗号化データが存在するかどうかを調査します。このルールは暗号化データのデコードは行わず、メッセージの内容に暗号化データが存在するかどうかのみを調査します。このルールは、ユーザが暗号化された電子メールを送信できないようにする場合に便利です。



(注)

暗号化されたルールは、メッセージの内容の暗号化されたデータのみを検出できます。暗号化された添付ファイルは検出しません。

`encrypted` は `true` ルールと同様に、パラメータを使用せず、比較も行いません。暗号化されたデータが検出された場合に `true`、検出されなかった場合に `false` を返します。この機能を実行するにはメッセージのスキャンが必要になるため、`scanconfig` コマンドで定義されたスキャン設定が使用されます。オプションの設定の詳細については、「[スキャンパラメータの変更](#)」(P.9-88)を参照してください。

次のフィルタは、リスナー経由で送信されたすべての電子メールを確認し、メッセージに暗号化されたデータが含まれる場合は、該当するメッセージが BCC で法務部門宛てに送信され、バウンスされません。

prevent_encrypted_data:

```
if (encrypted) {
    bcc ('legaldept@example.domain');
    bounce();
}
```

添付ファイルタイプルール

attachment-type ルールはメッセージ内の各添付ファイルの MIME タイプを確認し、指定されたパターンと一致するかどうかを判別します。このパターンは scanconfig コマンドで使用する形式（「[スキャンパラメータの変更](#)」(P.9-88) を参照）と同じ形式である必要があります。スラッシュ (/) の右の一方でアスタリスクをワイルドカードとして使用できます。メッセージの添付ファイルがここで指定した MIME タイプと一致する場合、このルールは「true」を返します。

この機能を実行するにはメッセージのスキャンが必要となるため、scanconfig コマンドで指定されたすべてのオプション（「[スキャンパラメータの変更](#)」(P.9-88) を参照）が適用されます。

メッセージの添付ファイルを操作するために使用できるメッセージフィルタ ルールの詳細については、「[添付ファイルのスキャン](#)」(P.9-67) を参照してください。

次のフィルタは、リスナー経由で送信されたすべての電子メールを確認し、MIME タイプが video/* である添付ファイルがメッセージに含まれる場合は、該当するメッセージがバウンスされます。

```
bounce_video_clips:

    if (attachment-type == 'video/*') {

        bounce();

    }
```

添付ファイル名ルール

attachment-filename ルールはメッセージ内の各添付ファイルの名前を確認し、指定されたパターンと一致するかどうかを判別します。この比較では大文字と小文字は区別されます。この比較ではスペースの有無も区別されるため、ファイル名の末尾にスペースがある状態でエンコードされていると、フィルタはその添付ファイルをスキップします。メッセージの添付ファイルのいずれかが指定したファイル名と一致すると、このルールは true を返します。

次の点に注意してください。

- 各添付ファイルの名前は MIME ヘッダーからキャプチャされます。MIME ヘッダーにあるファイル名の末尾にはスペースがある場合があります。
- 添付ファイルがアーカイブの場合、Cisco はアーカイブの内部からファイル名を取得し、scanconfig ルール（「[スキャンパラメータの変更](#)」(P.9-88) を参照）を適用します。
 - 添付ファイルが 1 個の圧縮ファイル（拡張子を問わず）である場合、アーカイブであるとは見なされず、この圧縮ファイルの名前は取得されません。つまり、このファイルは attachment-filename ルールでは処理されません。このようなファイルの例としては、gzip で圧縮された実行可能ファイル (.exe) などがあります。
 - 添付ファイルが単独の圧縮ファイルである場合 (foo.exe.gz など)、正規表現を使用して圧縮ファイル内の特定のファイルタイプを検索します。「[添付ファイル名とアーカイブファイル内の単独の圧縮ファイル](#)」(P.9-32) を参照してください。

メッセージの添付ファイルを操作するために使用できるメッセージフィルタ ルールの詳細については、「[添付ファイルのスキャン](#)」(P.9-67) を参照してください。

次のフィルタは、リスナー経由で送信されたすべての電子メールを確認し、ファイル名が *.mp3 である添付ファイルがメッセージに含まれる場合は、該当するメッセージがバウンスされます。

```
block_mp3s:

    if (attachment-filename == '(?i)\\.mp3$') {

        bounce();

    }
```

添付ファイル名とアーカイブファイル内の単独の圧縮ファイル

次に、アーカイブ (gzip で作成したものなど) にある単独の圧縮ファイルの照合する例を示します。

```
quarantine_gzipped_exe_or_pif:

if (attachment-filename == '(?i)\\. (exe|pif) ($|.gz$)') {

    quarantine("Policy");

}
```

DNS リストルール

`dnslist()` ルールは、クエリーに DNSBL 方式 (「ip4r ルックアップ」とも呼ばれます) を使用するパブリック DNS リストサーバを照会します。着信接続の IP アドレスは反転され (IP が 1.2.3.4 の場合は 4.3.2.1 になり)、かっこ内のサーバ名にプレフィックスとして追加されます (サーバ名の先頭がピリオドでない場合は、サーバ名とプレフィックスを区切るためのピリオドが追加されます)。DNS クエリーが生成され、システムには DNS 失敗応答 (接続の IP アドレスがサーバのリストにないことを示す) または IP アドレス (アドレスが見つかったことを示す) が返されます。返される IP アドレスは通常、127.0.0.x (x は 0 ~ 255 のうちほぼすべての数) の形式になります (IP アドレス範囲は許可されていません)。一部のサーバは、リスト生成の理由に基づいてそれぞれ異なる数字を返しますが、それ以外のサーバはすべての一致に対して同じ結果を返します。

`dnslist()` は、`header()` ルールと同様に、単項または二項比較で使用できます。単独では、応答を受信すると `true` を返し、応答がない場合 (DNS サーバが到達不能の場合など) は `false` を返します。

次のフィルタを実行すると、送信者が Cisco Bonded Sender 情報サービス プログラムにボンドされている場合、そのメッセージがただちに出力されます。

```
whitelist_bondedsender:

    if (dnslist('query.bondedsender.org')) {

        skip-filters();

    }
```

オプションで、等式 (==) または不等式 (!=) を使用して結果を文字列と比較することもできます。

次のフィルタは、サーバから「127.0.0.2」が返されるメッセージをドロップします。応答がそれ以外の内容であれば、このルールは `false` を返し、フィルタは無視されます。

```
blacklist:

    if (dnslist('dnsbl.example.domain') == '127.0.0.2') {

        drop();

    }
```

SenderBase レピュテーション ルール

reputation ルールは、SenderBase レピュテーション スコアを他の値と比較して確認します。>、==、<= などのすべての比較演算子を使用できます。メッセージに SenderBase レピュテーション スコアがない場合（これまでスコアがまったく確認されていないか、SenderBase レピュテーション サービス クエリー サーバから応答を取得できなかった場合）、レピュテーション スコアとの比較はすべて失敗します（数値がいずれかの値より大きいまたは小さい、いずれかの値と等しいまたは等しくないという判別ができません）。次に説明する no-reputation ルールを使用すると、SBRS スコアが「none」であるかどうかを確認できます。次の例では、SenderBase レピュテーション サービスから返されるレピュテーション スコアがしきい値の -7.5 を下回る場合に、メッセージの「Subject:」行の先頭に「*** BadRep ***」が付加されます。

```
note_bad_reps:

    if (reputation < -7.5) {

        strip-header ('Subject');

        insert-header ('Subject', '*** BadRep $Reputation *** $Subject');

    }
```

詳細については、「レピュテーション フィルタリング」の章を参照してください。[「アンチスパム システムのバイパス アクション」\(P.9-65\)](#) も参照してください。

SenderBase レピュテーション ルールによる値は -10 ~ 10 ですが、NONE という値が返される場合もあります。NONE について特に確認が必要な場合は、no-reputation ルールを使用します。

```
none_rep:

    if (no-reputation) {

        strip-header ('Subject');

        insert-header ('Subject', '*** Reputation = NONE *** $Subject');

    }
```

辞書ルール

`dictionary-match(<dictionary_name>)` ルールは、*dictionary_name* で指定した名前の辞書にある正規表現または用語がメッセージ本文にあれば `true` と評価します。辞書が存在しない場合は、このルールは `false` と評価します。辞書の定義の詳細については（大文字と小文字の区別や単語境界の設定など）、「テキストリソース」の章を参照してください。

次のフィルタは、Cisco が「`secret_words`」という辞書にある単語を含むメッセージをスキャンすると、管理者にブラインドカーボンコピーを送信します。

```
copy_codenames:

    if (dictionary-match ('secret_words')) {

        bcc('administrator@example.com');

    }
```

次の例では、メッセージ本文に「`secret_words`」という辞書の単語がある場合、`Policy` という名の隔離エリアにメッセージが送信されます。`only-body-contains` 条件とは異なり、`body-dictionary-match` 条件ではすべてのコンテンツ部分がそれぞれ辞書と一致している必要はありません。各コンテンツ部分のスコア（マルチパート/代替部分も考慮されます）は合計されます。

```
quarantine_data_loss_prevention:

    if (body-dictionary-match ('secret_words'))

    {

        quarantine('Policy');

    }
```

次のフィルタでは、件名が指定した辞書にある単語と一致すると隔離されます。

```
quarantine_policy_subject:

    if (subject-dictionary-match ('gTest'))

    {

        quarantine('Policy');

    }
```

次の例では、「`To`」ヘッダーの電子メールアドレスを照合し、管理者にブラインドコピーを送信しています。

```
headerTest:

    if (header-dictionary-match ('competitorsList', 'to'))

    {
```

```
bcc('administrator@example.com');  
  
}
```

attachment-dictionary-match(<dictionary_name>) ルールは上記の dictionary-match ルールと同様に機能しますが、検索対象は添付ファイルです。

次のフィルタでは、メッセージの添付ファイルに「secret_words」という辞書にあるいずれかの単語が含まれていると、そのメッセージが Policy という隔離エリアに送信されます。

```
quarantine_codenames_attachment:  
  
if (attachment-dictionary-match ('secret_words'))  
  
{  
  
    quarantine('Policy');  
  
}
```

header-dictionary-match(<dictionary_name>, <header>) ルールは上記の dictionary-match ルールと同様に機能しますが、検索対象は <header> で指定したヘッダーです。ヘッダー名の大文字と小文字は区別されないため、たとえば「subject」でも「Subject」でも機能します。

次のフィルタでは、メッセージの「cc」ヘッダーに「ex_employees」という辞書にあるいずれかの単語が含まれていると、そのメッセージが Policy という隔離エリアに送信されます。

```
quarantine_codenames_attachment:  
  
if (header-dictionary-match ('ex_employees', 'cc'))  
  
{  
  
    quarantine('Policy');  
  
}
```

辞書用語内でワイルドカードを使用することができます。電子メールアドレスのピリオドをエスケープする必要はありません。

SPF-Status ルール

SPF/SIDF 検証されたメールを受信する場合、SPF/SIDF 検証の結果によって異なるアクションを実行することが必要になる場合があります。spf-status ルールを使用すると、複数の SPF 検証結果との照合が可能になります。詳細については、「[検証結果](#)」(P.17-29) を参照してください。

SPF/SIDF 検証結果との照合を行うには、次の構文を使用します。

```
if (spf-status == "Pass")
```

1つの条件で複数の状態判定に対してチェックする場合、次の構文を使用できます。

```
if (spf-status == "PermError, TempError")
```

さらに、次の構文を使用して、HELO、MAIL FROM、PRA ID に対して検証結果をチェックすることもできます。

```
if (spf-status("pra") == "Fail")
```

次の、spf-status フィルタの使用例を示します。

```
skip-spam-check-for-verified-senders:
```

```
    if (sendergroup == "TRUSTED" and spf-status == "Pass"){  
        skip-spamcheck();  
    }
```

```
quarantine-spf-failed-mail:
```

```
    if (spf-status("pra") == "Fail") {  
        if (spf-status("mailfrom") == "Fail"){  
            # completely malicious mail  
            quarantine("Policy");  
        } else {  
            if(spf-status("mailfrom") == "SoftFail") {  
                # malicious mail, but tempting  
                quarantine("Policy");  
            }  
        }  
    } else {  
        if(spf-status("pra") == "SoftFail"){  
            if (spf-status("mailfrom") == "Fail"  
                or spf-status("mailfrom") == "SoftFail"){  
                # malicious mail, but tempting  
                quarantine("Policy");  
            }  
        }  
    }
```

```
    }  
  }  
}  
  
stamp-mail-with-spf-verification-error:  
  
  if (spf-status("pra") == "PermError, TempError"  
      or spf-status("mailfrom") == "PermError, TempError"  
      or spf-status("helo") == "PermError, TempError"){  
    # permanent error - stamp message subject  
    strip-header("Subject");  
    insert-header("Subject", "[POTENTIAL PHISHING] $Subject"); }  
.  
.
```

SPF-Passed ルール

次の例に、`spf-passed` とマークされていない電子メールを隔離するために使用する `spf-passed` ルールを示します。

```
quarantine-spf-unauthorized-mail:  
  
  if (not spf-passed) {  
    quarantine("Policy");  
  }  
.
```



(注)

`spf-status` ルールと異なり `spf-passed` ルールは SPF/SIDF 検証値を簡単なブール値に単純化します。次の検証結果は、`spf-passed` ルールに合格していないものとして扱われます。None、Neutral、Softfail、TempError、PermError、Fail。より詳細な結果に基づいて、メッセージへのアクションを実行するには、`spf-status` ルールを使用します。

workqueue-count ルール

`workqueue-count` ルールは、ワークキュー数を特定の値と照合します。>、==、<= などのすべての比較演算子を使用できます。

次のフィルタは、ワークキュー数を確認し、指定した値より多ければスパムの確認を省略します。

```
wqfull:

if (workqueue-count > 1000) {

    skip-spamcheck();

}
```

SPF/SIDF の詳細については、「[SPF および SIDF 検証の概要](#)」(P.17-20) を参照してください。

SMTP Authenticated User Match ルール

Cisco アプライアンスがメッセージの送信に SMTP 認証を使用している場合、`smtp-auth-id-matches` (<target> [, <sieve-char>]) ルールはメッセージのヘッダーとエンベロープ送信者を送信者の SMTP 認証ユーザ ID と照合し、スプーフィングされたヘッダーを含む送信メッセージを識別します。このフィルタを使用すると、なりすましの可能性のあるメッセージを隔離またはブロックできます。

`smtp-auth-id-matches` ルールは、SMTP 認証 ID を次の比較対象と比較します。

比較対象	説明
*EnvelopeFrom	SMTP 対話のエンベロープ送信者のアドレス (MAIL FROM) を比較します。
*FromAddress	From ヘッダーから解析されたアドレスを比較します。From ヘッダーには複数のアドレスを使用できるため、そのうち 1 つが一致すれば一致と見なされます。
*Sender	Sender ヘッダーで指定されているアドレスを比較します。
*Any	ID にかかわらず、認証済み SMTP セッション中に作成されたメッセージと一致します。
*None	認証済み SMTP セッション中に作成されなかったメッセージと一致します。認証がオプションの場合に便利です (推奨)。

フィルタによる照合は厳密ではありません。大文字と小文字は区別されません。オプションで `sieve-char` パラメータが指定されている場合、特定の文字の後に続くアドレスの最後の部分は比較時に無視されます。たとえば、パラメータに「+」が含まれている場合、アドレス `joe+folder@example.com` のうち「+」より後の部分がフィルタでは無視されます。アドレスが `joe+smith+folder@example.com` の場合は、「+folder」のみが無視されます。SMTP 認証ユーザ ID 文字列が単純なユーザ名で、完全修飾電子メールアドレスでない場合は、比較対象のユーザ名部分のみが照合されます。ドメイン部分は別のルールで検証する必要があります。

また、`$SMTPAuthID` 変数を使用して SMTP 認証ユーザ ID をヘッダーに挿入することができます。

次の表は、SMTP 認証 ID と電子メールの比較の例で、`smtp-auth-id-matches` フィルタ ルールによる比較で一致するかどうかを示しています。

SMTP 認証 ID	ふるい文字	比較するアドレス	一致の可否
someuser		otheruser@example.com	No
someuser		someuser@example.com	Yes

SMTP 認証 ID	ふるい文字	比較するアドレス	一致の可否
someuser		someuser@another.com	Yes
SomeUser		someuser@example.com	Yes
someuser		someuser+folder@example.com	No
someuser	+	someuser+folder@example.com	Yes
someuser@example.com		someuser@forged.com	No
someuser@example.com		someuser@example.com	Yes
SomeUser@example.com		someuser@example.com	Yes

次のフィルタは、認証済み SMTP セッション中に作成されたすべてのメッセージを確認し、From ヘッダーのアドレスとエンベロープ送信者が SMTP 認証ユーザ ID と一致するか検証します。アドレスと ID が一致すると、フィルタはドメインを許可します。一致しない場合、アプライアンスはメッセージを隔離します。

```
Msg_Authentication:
```

```
if (smtp-auth-id-matches("*Any"))
{
    # Always include the original authentication credentials in a
    # special header.
    insert-header("X-Auth-ID", "$SMTPAuthID");

    if (smtp-auth-id-matches("*FromAddress", "+") and
        smtp-auth-id-matches("*EnvelopeFrom", "+"))
    {
        # Username matches. Verify the domain
        if header('from') != "(?i)@(?:(example\\.com|alternate\\.com))" or
            mail-from != "(?i)@(?:(example\\.com|alternate\\.com))"
        {
            # User has specified a domain which cannot be authenticated
            quarantine("forged");
        }
    }
} else {
    # User claims to be an completely different user
    quarantine("forged");
}
```

```

    }
}

```

signed ルール

signed ルールはメッセージの署名を確認します。このルールは、メッセージの署名の有無を示すブール値を返します。このルールは、署名が ASN.1 DER エンコーディングルールに従っているか、および CMS 署名データ型構造 (RFC 3852、セクション 5.1) に準拠しているかを評価します。署名がコンテンツと一致するかどうかは検証されず、証明書の有効性も確認されません。

次の例では、signed ルールを使用してヘッダーを署名済みメッセージに挿入します。

```
signedcheck: if signed { insert-header("X-Signed", "True"); }
```

次の例では、signed ルールを使用して、特定の送信者グループから受信した未署名のメッセージの添付ファイルをドロップします。

```
Signed: if ((sendergroup == "NOTTRUSTED") AND NOT signed) {

    html-convert();

    if (attachment_size > 0)
    {
        drop_attachments("");
    }
}

```

Signed Certificate ルール

signed-certificate ルールは、X.509 証明書発行者またはメッセージ署名者が、指定した正規表現と一致している S/MIME メッセージを選択します。このルールが対応しているのは X.509 証明書のみです。

このルールの構文は signed-certificate (<field> [<operator> <regular expression>]) です。各項目の内容は次のとおりです。

- <field> : 引用符で囲まれた文字列 "issuer" (発行者) または "signer" (署名者)。
- <operator> : == または !=。
- <regular expression> : 発行者または署名者を照合するための値。

メッセージに複数の署名が使用されている場合、いずれかの発行者または署名者が正規表現と一致すると true が返されます。このルールを一番短い形で signed-certificate("issuer") および signed-certificate("signer") のように指定すると、S/MIME メッセージに発行者または署名者が設定されている場合に true が返されます。

署名者

メッセージ署名者に関して、このルールは X.509 証明書の `subjectAltName` 拡張から `rfc822Name` 名のシーケンスを抽出します。署名証明書に `subjectAltName` フィールドがない場合、またはこのフィールドに `rfc822Name` 名がない場合、`signed-certificate("signer")` ルールは `false` を返します。まれではありますが、`rfc822Name` 名が複数使用されている場合、このルールはすべての名前を正規表現と照合しようと試み、最初に一致した時点で `true` を返します。

発行者

発行者は X.509 証明書の空でない識別名です。AsyncOS は証明書から発行者を取得し、LDAP-UTF8 Unicode 文字列に変換します。次の例を参考にしてください。

- `C=US,S=CA,O=IronPort`
- `C=US,CN=Bob Smith`

X.509 証明書では発行者フィールドが必要なため、`signed-certificate("issuer")` は S/MIME メッセージに X.509 証明書があるかどうかを評価します。

正規表現でのエスケープ処理

LDAP-UTF8 では、正規表現で使用できるエスケープ方式が定義されています。LDAP-UTF8 での文字のエスケープ処理の詳細については、『*Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names*』（<http://www.ietf.org/rfc/rfc4514.txt>）を参照してください。

`signed-certificate` ルールでのエスケープ ルールは、LDAP-UTF8 で定義されたエスケープ ルールとは異なり、エスケープ処理が必要な文字のみをエスケープします。LDAP-UTF8 では、エスケープ処理なしで表示できる文字をオプションでエスケープすることができます。たとえば、次の 2 つの文字列は、LDAP-UTF8 のエスケープ ルールではいずれも「`Example, Inc.`」を正しく表すものとされます。

- `Example\, Inc.`
- `Example\,\ Inc\.`

一方で、`signed-certificate` ルールでは「`Example\, Inc.`」のみが一致します。スペースやピリオドのエスケープ処理は LDAP-UTF8 では許可されていますが、必要ではないため、正規表現では許可されません。`signed-certificate` ルールで使用する正規表現を作成する場合は、エスケープ処理がなくても表示できる文字はエスケープしないでください。

\$CertificateSigners アクション変数

アクション変数 `$CertificateSigners` は、署名証明書の `subjectAltName` 要素から取得した、カンマ区切り形式の署名者のリストです。1 人の署名者に複数の電子メールアドレスがある場合、重複を除去した上でリストに収録されます。

たとえば、Alice が自分の 2 つの証明書でメッセージに署名したとします。Bob は自分の 1 つの証明書でメッセージに署名しています。すべての証明書は 1 件の社内機関により発行されています。メッセージが S/MIME スキャンを通過すると、抽出されるデータには 3 つの項目が含まれます。

```
[
  {
    'issuer': 'CN=Auth,O=Example\, Inc.',
    'signer': ['alice@example.com', 'al@private.example.com']
  }
]
```

```

    },
    {
      'issuer': 'CN=Auth,O=Example\, Inc.',
      'signer': ['alice@example.com', 'al@private.example.com']
    },
    {
      'issuer': 'CN=Auth,O=Example\, Inc.',
      'signer': ['bob@example.com', 'bob@private.example.com']
    }
  ]

```

\$CertificateSigners 変数は次のように拡張されます。

```
"alice@example.com, al@private.example.com, bob@example.com, bob@private.example.com"
```

例

次の例では、証明書発行者が米国にいる場合、新しいヘッダーが挿入されます。

```

Issuer: if signed-certificate("issuer") == "(?i)C=US" {
    insert-header("X-Test", "US issuer");
}

```

次の例では、署名者のドメインが **example.com** でない場合、管理者に通知されます。

```

NotOurSigners: if signed-certificate("signer") AND
    signed-certificate("signer") != "example\\.com$" {
    notify("admin@example.com");
}

```

次の例では、メッセージに **X.509** 証明書がある場合、ヘッダーが追加されます。

```

AnyX509: if signed-certificate ("issuer") {
    insert-header("X-Test", "X.509 present");
}

```

次の例では、メッセージの証明書に署名者がいない場合、ヘッダーが追加されます。

```
NoSigner: if not signed-certificate ("signer") {
    insert-header("X-Test", "Old X.509?");
}
```

メッセージフィルタアクション

メッセージフィルタの目的は、選択されたメッセージに対してアクションを実行することです。

アクションには、次の2つのタイプがあります。

- **最終アクション** (deliver、drop、bounce など) はメッセージの処理を終了し、後続のフィルタによるさらなる処理を許可しません。
- **非最終アクション**は、メッセージをさらに処理することを許可するアクションを実行します。

非最終メッセージフィルタアクションは、累積的です。各フィルタが異なるアクションを指定する複数のフィルタにメッセージが一致する場合、すべてのアクションが累積され、適用されます。ただし、同じアクションを指定する複数のフィルタにメッセージが一致する場合、前のアクションが上書きされ、最後のフィルタアクションが適用されます。

フィルタアクション一覧表

メッセージフィルタでは次の表 9-5 に示すアクションを電子メールメッセージに適用できます。

表 9-5 メッセージフィルタアクション

アクション	構文	説明
送信元ホストの変更	alt-src-host	メッセージの送信に使用する送信元ホスト名と IP インターフェイス (Virtual Gateway アドレス) を変更します。「送信元ホスト (Virtual Gateway アドレス) 変更アクション」(P.9-60) を参照してください。
受信者の変更	alt-rcpt-to	メッセージの受信者を変更します。「受信者変更アクション」(P.9-59) を参照してください。
メールホストの変更	alt-mailhost	メッセージの送信先メールホストを変更します。「配信ホスト変更アクション」(P.9-59) を参照してください。
通知	notify	メッセージに関する報告を別の受信者に送信します。「通知およびコピー通知アクション」(P.9-54) を参照してください。
コピーの通知	notify-copy	notify アクションと同様ですが、bcc-scan のようにコピーを送信します。「通知およびコピー通知アクション」(P.9-54) を参照してください。
BCC	bcc	メッセージをコピーし (メッセージレプリケーション)、このコピーを匿名で別の受信者に送信します。「ブライントカーボンコピーアクション」(P.9-56) を参照してください。

表 9-5 メッセージフィルタアクション (続き)

アクション	構文	説明
BCC (スキャン処理あり)	bcc-scan	メッセージを秘密で他の受信者に送信し、そのメッセージを新しいメッセージであるかのようにワークキューで処理します。「 ブラインドカーボンコピーアクション 」(P.9-56)を参照してください。
アーカイブ	archive	メッセージを mbox 形式のファイルにアーカイブします。「 アーカイブアクション 」(P.9-61)を参照してください。
隔離	quarantine (<i>quarantine_name</i>)	<i>quarantine_name</i> で指定した隔離エリアにメッセージを送信するようフラグを設定します。「 隔離および複製アクション 」(P.9-58)を参照してください。
複製 (隔離)	duplicate-quarantine(<i>quarantine_name</i>)	指定された隔離エリアにメッセージのコピーを送信します。「 隔離および複製アクション 」(P.9-58)を参照してください。
ヘッダーの削除	strip-header	メッセージの配信前に、指定したヘッダーをメッセージから削除します。「 ヘッダー削除アクション 」(P.9-62)を参照してください。
ヘッダーの挿入	insert-header	メッセージの配信前に、ヘッダーと値の対をメッセージに挿入します。「 ヘッダー挿入アクション 」(P.9-62)を参照してください。
ヘッダーテキストの編集	edit-header-text	指定したヘッダーテキストを、フィルタ条件として指定した文字列に置き換えます。「 ヘッダーテキスト編集アクション 」(P.9-63)を参照してください。
本文の編集	edit-body-text()	メッセージ本文から正規表現に一致する部分を削除し、指定したテキストに置き換えます。このフィルタは、メッセージ本文内の URL などの特定のコンテンツを削除および置換する場合に使用できます。「 本文編集アクション 」(P.9-63)を参照してください。
HTML の変換	html-convert()	メッセージ本文から HTML タグを削除し、メッセージのプレーンテキスト部分を残します。このフィルタは、メッセージ内のすべての HTML テキストをプレーンテキストに変換する場合に使用します。「 HTML 変換アクション 」(P.9-64)。
バウンス プロファイルの割り当て	bounce-profile	特定のバウンス プロファイルをメッセージに割り当てます。「 バウンス プロファイルアクション 」(P.9-65)を参照してください。
アンチスパムシステムのバイパス	skip-spamcheck	Cisco システムのアンチスパムシステムがメッセージに適用されないようにします。「 アンチスパムシステムのバイパスアクション 」(P.9-65)を参照してください。
アンチウイルスシステムのバイパス	skip-viruscheck	Cisco システムのアンチウイルスシステムがメッセージに適用されないようにします。「 アンチウイルスシステムのバイパスアクション 」(P.9-66)を参照してください。
ウイルスアウトブレイクフィルタのスキニング処理のスキップ	skip-vofcheck	このメッセージがウイルスアウトブレイクフィルタでスキニング処理されないようにします。「 アンチウイルスシステムのバイパスアクション 」(P.9-66)を参照してください。

表 9-5 メッセージフィルタアクション (続き)

アクション	構文	説明
添付ファイルのドロップ (名前別)	drop-attachments-by-name	メッセージの添付ファイルのうち、指定した正規表現と一致する名前のファイルをすべてドロップします。アーカイブ形式の添付ファイル (zip、tar) 内に該当するファイルがある場合、この添付ファイルはドロップされます。「添付ファイルのスキャンメッセージフィルタの例」(P.9-75) を参照してください。
添付ファイルのドロップ (タイプ別)	drop-attachments-by-type	メッセージの添付ファイルのうち、指定した MIME タイプまたはファイル拡張子に該当する MIME タイプのファイルをすべてドロップします。アーカイブ形式の添付ファイル (zip、tar) 内に該当するファイルがある場合、この添付ファイルはドロップされます。「添付ファイルのスキャンメッセージフィルタの例」(P.9-75) を参照してください。
添付ファイルのドロップ (ファイルタイプ別)	drop-attachments-by-filetype	メッセージの添付ファイルのうち、指定したファイルの「フィンガープリント」と一致するファイルをすべてドロップします。アーカイブ形式の添付ファイル (zip、tar) 内に該当するファイルがある場合、この添付ファイルはドロップされます。詳細については、「添付ファイルのスキャン」(P.9-67) を参照してください。
添付ファイルのドロップ (MIME タイプ別)	drop-attachments-by-mimetype	メッセージの添付ファイルのうち、特定の MIME タイプのファイルをすべてドロップします。このアクションではファイル拡張子による MIME タイプの判別は行われず、アーカイブの内容の確認もされません。「添付ファイルのスキャンメッセージフィルタの例」(P.9-75) を参照してください。
添付ファイルのドロップ (サイズ別)	drop-attachments-by-size	メッセージの添付ファイルのうち、ロー エンコード形式で指定したサイズ (バイト単位) 以上のサイズであるファイルをすべてドロップします。アーカイブや圧縮ファイルの場合、このアクションでは非圧縮状態でのサイズは計測されず、デコードを行う前実際の添付ファイルのサイズが計測されます。「添付ファイルのスキャンメッセージフィルタの例」(P.9-75) を参照してください。
添付ファイルのドロップ (内容別)	drop-attachments-where-contains	<p>メッセージの添付ファイルのうち、指定した正規表現を含むファイルをすべてドロップします。パターンの発生回数が、しきい値で指定した最小回数以上である必要があります。アーカイブファイル (zip、tar) は、中に含まれているファイルのいずれかが正規表現と一致する場合にドロップされます。「添付ファイルのスキャンメッセージフィルタの例」(P.9-75) を参照してください。</p> <p>オプション コメントは、ドロップされた添付ファイルの置換に使用されるテキストを変更します。添付ファイルのフッターは、単純にメッセージに追加されるだけです。</p>

表 9-5 メッセージフィルタアクション (続き)

アクション	構文	説明
添付ファイルのドロップ (辞書との一致別)	drop-attachments-where-dictionary-match	辞書の用語との一致に基づいて添付ファイルを削除します。添付ファイルであると判断される MIME 部分の用語が辞書の用語と一致する場合 (かつ、ユーザ定義のしきい値に達している場合)、添付ファイルが電子メールから削除されます。「添付ファイルのスキャンメッセージフィルタの例」(P.9-75) を参照してください。
フッターの追加	add-footer (footer-name)	メッセージのフッターとして免責条項を追加します。詳細については、「テキストリソース」の章の「メッセージ免責事項スタンプ」を参照してください。
見出しの追加	add-heading (heading-name)	メッセージの見出しとして免責条項を追加します。詳細については、「テキストリソース」の章の「メッセージ免責事項スタンプ」を参照してください。
配信時の暗号化	encrypt-deferred	配信時にメッセージを暗号化します。メッセージはそのまま次の処理に進み、すべての処理が完了した時点で暗号化され、配信されます。
メッセージタグの追加	tag-message (tag-name)	RSA Email DLP ポリシー フィルタリングで使用するカスタム用語をメッセージに追加します。RSA Email DLP ポリシーを設定して、スキャン対象をメッセージタグがあるメッセージに限定することができます。メッセージタグは受信者側では表示されません。「メッセージタグ追加アクション」(P.9-66) と「データ消失防止」の章を参照してください。
ログ エントリの追加	log-entry	カスタマイズしたテキストを、IronPort テキスト メール ログに INFO レベルで追加します。このテキストにはアクション変数を使用することができます。ログ エントリはメッセージトラッキングに表示されます。「ログ エントリ追加アクション」(P.9-67) を参照してください。
* 残りのメッセージフィルタをスキップ	skip-filters	メッセージに対して他のメッセージフィルタによる処理は行われず、メッセージは電子メールパイプラインをそのまま通過します。「残りのメッセージフィルタをスキップ」アクション (P.9-52) を参照してください。
* メッセージのドロップ	drop	メッセージをドロップし、廃棄します。「ドロップアクション」(P.9-53) を参照してください。
* メッセージのバウンス	bounce	メッセージを送信者に戻します。「バウンスアクション」(P.9-53) を参照してください。
* すぐに暗号化して配信	encrypt	発信メッセージの暗号化に Cisco 電子メール暗号化を使用します。「暗号化アクション」(P.9-53) を参照してください。

* 最終アクション

添付ファイルグループ

特定のファイルタイプ (「exe」など) や一般的な添付ファイルのグループを attachment-filetype ルールや drop-attachments-by-filetype ルールで指定できます。AsyncOS は添付ファイルを表 9-6 に記載されているグループに分類します。

特定のファイルタイプの添付ファイルを含まないメッセージと照合させる `!=` 演算子を使うメッセージフィルタを作成する場合は、フィルタで除外するファイルタイプの添付ファイルが少なくとも1つあると、フィルタはメッセージへのアクションを実行しません。たとえば、次のフィルタは `.exe` ファイルタイプではない添付ファイルを含むメッセージをドロップします。

```
exe_check: if (attachment-filetype != "exe") {
    drop();
}
```

メッセージに複数の添付ファイルがある場合、電子メールセキュリティアプライアンスは他の添付ファイルが `.exe` ファイルでない場合でも、添付ファイルの少なくとも1つが `.exe` ファイルの場合はメッセージをドロップしません。

表 9-6 添付ファイルグループ

添付ファイルグループ名	スキャン対象のファイルタイプ
ドキュメント (Document)	<ul style="list-style-type: none"> • doc • mdb • mpp • ole • pdf • ppt • rtf • wps • x-wmf • xls
実行ファイル (Executable)	<ul style="list-style-type: none"> • exe • java • msi • pif <p>(注) Executable グループをフィルタリングすると、<code>.dll</code> ファイルと <code>.scr</code> ファイルもスキャンされます。これらのファイルタイプは個別にスキャンできません。</p>

表 9-6 添付ファイルグループ (続き)

添付ファイルグループ名	スキャン対象のファイルタイプ
圧縮 (Compressed)	<ul style="list-style-type: none"> • ace (ACE アーカイバ圧縮ファイル) • arc (SQUASH 圧縮アーカイブ) • arj (Robert Jung ARJ 圧縮アーカイブ) • binhex • bz (Bzip 圧縮ファイル) • bz2 (Bzip 圧縮ファイル) • cab (Microsoft キャビネット ファイル) • gzip* (圧縮ファイル - UNIX gzip) • lha (圧縮アーカイブ [LHA/LHARC/LHZ]) • rar (圧縮アーカイブ) • sit (圧縮アーカイブ - Macintosh ファイル [Stuffit]) • tar* (圧縮アーカイブ) • unix (UNIX 圧縮アーカイブ) • zip* (圧縮アーカイブ - Windows) • zoo (ZOO 圧縮アーカイブ ファイル) <p>* これらのファイルは「本文スキャン」の対象にすることができます。</p>
テキスト (Text)	<ul style="list-style-type: none"> • txt • html • xml

表 9-6 添付ファイルグループ (続き)

添付ファイルグループ名	スキャン対象のファイルタイプ
イメージ (Image)	<ul style="list-style-type: none"> • bmp • cur • gif • ico • jpeg • pcx • png • psd • psp • tga • tiff
メディア (Media)	<ul style="list-style-type: none"> • aac • aiff • asf • avi • flash • midi • mov • mp3 • mpeg • ogg • ram • snd • wav • wma • wmv

アクション変数

`bcc()`、`bcc-scan()`、`notify()`、`notify-copy()`、`add-footer()`、`add-heading()`、`insert-headers()` の各アクションには、アクションの実行時に元のメッセージの情報に自動的に置き換えられる所定の変数を使用しているパラメータがあります。これらの特殊な変数をアクション変数といいます。Cisco アプライアンスでは次のアクション変数がサポートされています。

表 9-7 メッセージフィルタアクション変数

変数	構文	説明
すべてのヘッダー (All Headers)	<code>\$AllHeaders</code>	メッセージのヘッダーを返します。
本文サイズ (Body Size)	<code>\$BodySize</code>	メッセージのサイズをバイト単位で返します。

表 9-7 メッセージフィルタアクション変数 (続き)

変数	構文	説明
証明書の署名者 (Certificate Signers)	\$CertificateSigners	署名付き証明書の subjectAltName 要素から取得した署名者を返します。詳細については、「\$CertificateSigners アクション変数」(P.9-41) を参照してください。
日付 (Date)	\$Date	現在の日付を MM/DD/YYYY 形式で返します。
ドロップされたファイル名 (Dropped File Name)	\$dropped_filename	直近にドロップされたファイル名のみを返します。
ドロップされたファイル名 (Dropped File Names)	\$dropped_filenames	ドロップされたファイルのリストを表示します (\$filenames と同様です)。
ドロップされたファイルタイプ (Dropped File Types)	\$dropped_filetypes	ドロップされたファイルのタイプを表示します (\$filenames と同様です)。
エンベロープ送信者 (Envelope Sender)	\$EnvelopeFrom	メッセージのエンベロープ送信者 (Envelope From、<MAIL FROM>) を返します。
エンベロープ受信者 (Envelope Recipients)	\$EnvelopeRecipients	メッセージのすべてのエンベロープ受信者 (Envelope To、<RCPT TO>) を返します。
ファイル名 (File Names)	\$filenames	メッセージの添付ファイルの名前のリストをカンマ区切りで返します。
ファイルサイズ (File Sizes)	\$filesizes	メッセージの添付ファイルのサイズのリストをカンマ区切りで返します。
ファイルタイプ (File Types)	\$filetypes	メッセージの添付ファイルのタイプのリストをカンマ区切りで返します。
フィルタ名 (Filter Name)	\$FilterName	処理中のフィルタの名前を返します。
GMTTimeStamp	\$GMTTimeStamp	メッセージの Received: 行に表示される現在の日時を GMT 形式で返します。
HAT グループ名 (HAT Group Name)	\$Group	メッセージの送信時に送信者が属していた送信者グループの名前を返します。送信者グループに名前がない場合は、文字列「>Unknown<」が挿入されます。
一致した内容 (Matched Content)	\$MatchedContent	スキャンフィルタルール (body-contains などのフィルタルールやコンテンツディクショナリを含む) をトリガーした内容を返します。
メールフローポリシー (Mail Flow Policy)	\$Policy	メッセージの送信時に送信者に適用された HAT ポリシーの名前を返します。事前に定義されているポリシー名が使用されていない場合、文字列「>Unknown<」が挿入されます。

表 9-7 メッセージフィルタアクション変数 (続き)

変数	構文	説明
ヘッダー (Header)	<code>\$Header['string']</code>	引用符で囲まれたヘッダーの値を返します (元のメッセージに該当するヘッダーがある場合)。二重引用符が使用される場合もあります。
ホスト名 (Hostname)	<code>\$Hostname</code>	Cisco アプライアンスのホスト名を返します。
内部メッセージ ID (Internal Message ID)	<code>\$MID</code>	内部でメッセージを識別するため使用されているメッセージ ID (MID) を返します。RFC822 「Message-Id」の値とは異なるため注意してください (「Message-Id」を取得するには <code>\$Header</code> を使用します)。
受信リスナー (Receiving Listener)	<code>\$RecvListener</code>	メッセージを受信したリスナーのニックネームに置き換えられます。
受信インターフェイス (Receiving Interface)	<code>\$RecvInt</code>	メッセージを受信したインターフェイスのニックネームを返します。
リモート IP アドレス (Remote IP Address)	<code>\$RemoteIP</code>	Cisco アプライアンスにメッセージを送信したシステムの IP アドレスを返します。
リモート ホスト アドレス (Remote Host Address)	<code>\$remotehost</code>	Cisco アプライアンスにメッセージを送信したシステムのホスト名を返します。
SenderBase レピュテーションスコア (SenderBase Reputation Score)	<code>\$Reputation</code>	送信者の SenderBase レピュテーションスコアを返します。レピュテーションスコアがない場合は「None」に置き換えられます。
件名 (Subject)	<code>\$Subject</code>	メッセージの件名を返します。
時間 (Time)	<code>\$Time</code>	現在地の時間帯での現在時刻を返します。
タイムスタンプ (Timestamp)	<code>\$Timestamp</code>	メッセージの Received: 行に表示される現在の日時を現在地の時間帯に従って返します。

非 ASCII 文字セットとメッセージフィルタアクション変数

このシステムでは、ISO-2022 スタイル文字コード (ヘッダー値で使用されるエンコードのスタイル) を含むアクション変数の拡張をサポートしています。また、通知内で多言語テキストを使用できます。これらの内容が統合されて通知が生成され、UTF-8 形式の、引用符で囲まれた印刷可能なメッセージとして送信されます。

該当コンテンツの表示

Attachment Content 条件、Message Body または Attachment 条件、Message 本文条件、または Attachment 内容条件と一致するメッセージに対して隔離アクションを設定した場合、隔離されたメッセージ内の一致した内容を表示できます。メッセージ本文を表示すると、該当内容が黄色で強調表示されます。また、`$MatchedContent` アクション変数を使用して、一致した内容をメッセージの件名に含めることができます。

メッセージフィルタまたはコンテンツフィルタのルールをトリガーしたローカル隔離内のメッセージを表示すると、フィルタアクションを実際にはトリガーしなかった内容が（フィルタアクションをトリガーした内容とともに）GUIで表示されることがあります。GUIの表示は、該当コンテンツを特定するための目安として使用するもので、該当コンテンツの完全なリストであるとは限りません。この現象が発生するのは、GUIでコンテンツの照合に使用しているロジックがフィルタと比べて厳密でないためです。この問題はメッセージ本文での検索についてのみ発生します。メッセージの各部分について、一致する文字列と関連するフィルタルールのリストが記載された表は正確です。

図 9-2 ポリシー隔離エリア内で表示された一致内容



メッセージフィルタアクションの例

「残りのメッセージフィルタをスキップ」アクション

skip-filters アクションを実行すると、メッセージフィルタによるメッセージの処理がスキップされ、メッセージは電子メールパイプラインを通過します。アプライアンスでアンチスパムスキャンとアンチウイルススキャンが使用できる場合、skip-filters アクションを実行したメッセージはこれらのスキャンの対象となります。skip-filters アクションは、メッセージフィルタのデフォルトの最終アクションです。

次のフィルタは、customer@example.com に通知を送信し、boss@admin 宛てのメッセージをただちに送信します。

```
bossFilter:
    if(rcpt-to == 'boss@admin$')
    {
        notify('customer@example.com');

        skip-filters();
    }
```

ドロップアクション

drop アクションを実行すると、メッセージは送信されずに廃棄されます。メッセージは送信者には戻されず、メッセージの本来の宛先にも送信されず、それ以外の処理も一切行われません。

次のフィルタは、まず `george@whitehouse.gov` に通知を送信し、その後件名が「SPAM」で始まるメッセージを廃棄します。

```
spamFilter:

    if(subject == '^SPAM.*')

    {

        notify('george@whitehouse.gov');

        drop();

    }
```

バウンスアクション

bounce アクションは、メッセージを送信者（エンベロープ送信者）に戻し、それ以降の処理は行いません。

次のフィルタは、`@yahoo\\.com` で終わる電子メールアドレスから送信されたすべてのメッセージを戻します（バウンスします）。

```
yahooFilter:

    if(mail-from == '@yahoo\\.com$')

    {

        bounce();

    }
```

暗号化アクション

encrypt アクションは、設定された暗号化プロファイルを使用して、電子メール受信者に暗号化されたメッセージを送信します。

次のフィルタは、メッセージの件名に `[encrypt]` という語句が含まれている場合に、そのメッセージを暗号化します。

```
Encrypt_Filter:

    if ( subject == '\\[encrypt\\]' )

    {

        encrypt('My_Encryption_Profile');

    }
```



(注)

このフィルタアクションを使用するには、ネットワークに Cisco Exryption アプライアンスがあるか、ホストキーサービスが設定されている必要があります。また、このフィルタアクションを使用するには、暗号化プロファイルの設定が必要です。

通知およびコピー通知アクション

notify および notify-copy アクションは、指定した電子メールに対して、メッセージの概要を電子メールで送信します。notify-copy アクションは、bcc-scan アクションと同様に、元のメッセージのコピーも送信します。通知概要には次の内容が含まれます。

- メッセージのメール転送プロトコル対話から取得したエンベロープ送信者およびエンベロープ受信者 (MAIL FROM および RCPT TO) 指定の内容。
- メッセージのヘッダー。
- メッセージを検出したメッセージフィルタの名前。

受信者、件名行、送信元アドレス、通知テンプレートを指定できます。次のフィルタは、サイズが 4 MB を超えるメッセージを選択し、一致するメッセージのそれぞれについて通知メッセージを admin@example.com に送信し、最後にメッセージを廃棄します。

```
bigFilter:
```

```
    if(body-size >= 4M)
    {
        notify('admin@example.com');
        drop();
    }
```

または

```
bigFilterCopy:
```

```
    if(body-size >= 4M)
    {
        notify-copy('admin@example.com');
        drop();
    }
```

エンベロープ受信者パラメータとして、有効な任意の電子メールアドレス（上の例では `admin@example.com`）を指定できます。また、メッセージのすべてのエンベロープ受信者を指定するアクション変数 `$EnvelopeRecipients`（「アクション変数」(P.9-49) を参照）を指定することもできます。

```
bigFilter:

    if(body-size >= 4M)

    {

        notify('$EnvelopeRecipients');

        drop();

    }
```

`notify` アクションでは最大で3つのオプション引数を使用でき、件名ヘッダー、エンベロープ送信者、通知メッセージに使用する定義済みテキストリソースを指定できます。これらのパラメータはこの順序で指定する必要があるため、エンベロープ送信者を設定する場合や通知テンプレートを指定する場合は件名を指定する必要があります。

件名パラメータにはアクション変数（「アクション変数」(P.9-49) を参照）を指定できます。この変数は元のメッセージから取得したデータで置き換えられます。デフォルトでは、件名は「`Message Notification`」に設定されています。

エンベロープ送信者パラメータとして、有効な任意の電子メールアドレスを指定できます。また、メッセージのリターンパスを元のメッセージと同じに設定する `$EnvelopeFrom` アクション変数を指定することもできます。

通知テンプレートパラメータは、既存の通知テンプレートの名前になります。詳細については、「通知」(P.9-75) を参照してください。

次の例は前の例を拡張したのですが、件名が「`[bigFilter] Message too large`」となるように変更し、リターンパスを元の送信者に設定し、「`message.too.large`」テンプレートを_using_しています。

```
bigFilter:

    if (body-size >= 4M)

    {

        notify('admin@example.com', '[FilterName] Message too large',

            '$EnvelopeFrom', 'message.too.large');

        drop();

    }
```

また、`$MatchedContent` アクション変数を使用して、送信者または管理者にコンテンツフィルタがトリガーされたことを通知することもできます。`$MatchedContent` アクション変数は、フィルタをトリガーしたコンテンツを表示します。たとえば、次のフィルタは、電子メールに ABA アカウント情報が含まれる場合に、管理者に通知します。

```
ABA_filter:

if (body-contains ('*aba')){

notify('admin@example.com', '[${MatchedContent}]Account Information Displayed');

}
```

通知テンプレート

[テキストリソース (Text Resources)] ページまたは `textconfig CLI` コマンドを使用して、`notify()` および `notify-copy()` アクションで使用するテキストリソースとなるカスタム通知テンプレートを設定できます。カスタム通知テンプレートを作成しない場合、デフォルトのテンプレートが使用されます。デフォルトのテンプレートにはメッセージヘッダーが含まれますが、デフォルトではカスタム通知テンプレートにはメッセージヘッダーは含まれません。カスタム通知にメッセージヘッダーを含めるには、`$AllHeaders` アクション変数を使用します。

詳細については、「テキストリソース」の章を参照してください。

次の例では、メッセージのサイズが大きい場合に次のフィルタがトリガーされると、本来の受信者に対して、メッセージが大きすぎることを示す電子メールが送信されます。

```
bigFilter:

if (body-size >= 4M)

{

    notify('${EnvelopeRecipients}', '[${FilterName}] Message too large',

        '${EnvelopeFrom}', 'message.too.large');

    drop();

}
```

ブラインドカーボンコピーアクション

`bcc` アクションは、メッセージの無記名コピーを、指定した受信者に送信します。この処理はメッセージレプリケーションとも呼ばれています。元のメッセージにはコピーに関する通知は含まれず、無記名コピーが受信者にバウンスされることはないため、メッセージの元の送信者と受信者はコピーが送信されたことを関知しない場合があります。

次のフィルタは、johnny から sue に送信されるメッセージのそれぞれについて、ブラインドカーボンコピーを mom@home.org に送信します。

```
momFilter:

if ((mail-from == '^johnny$') and (rcpt-to == '^sue$'))
```



```
{
    bcc('mom@home.org');
}
```

bcc アクションでは最大で 3 つのオプション引数を使用でき、コピーしたメッセージに使用する件名ヘッダーとエンベロープ送信者、および alt-mailhost を指定できます。これらのパラメータはこの順序で指定する必要があるため、エンベロープ送信者を設定する場合は件名を指定する必要があります。

件名パラメータにはアクション変数（「アクション変数」(P.9-49) を参照）を指定できます。この変数は元のメッセージから取得したデータで置き換えられます。デフォルトでは、元のメッセージの件名（\$Subject と同じ内容）が設定されます。

エンベロープ送信者パラメータとして、有効な任意の電子メールアドレスを指定できます。また、メッセージのリターンパスを元のメッセージと同じに設定する \$EnvelopeFrom アクション変数を指定することもできます。

次の例は前の例を拡張したもので、件名は「[Bcc] <元の件名>」に設定され、リターンパスは badbounce@home.org に設定されています。

```
momFilter:
    if ((mail-from == '^johnny$') and (rcpt-to == '^sue$'))
    {
        bcc('mom@home.org', '[Bcc] $Subject', 'badbounce@home.org');
    }
```

4 番目のパラメータは alt-mailhost です。

```
momFilterAltM:
    if ((mail-from == '^johnny$') and (rcpt-to == '^sue$'))
    {
        bcc('mom@home.org', '[Bcc] $Subject', '$EnvelopeFrom',
            'momaltmailserver.example.com');
    }
```



警告

Bcc()、notify()、bounce() の各フィルタアクションを実行すると、ネットワーク内にウイルスが侵入する場合があります。ブラインドカーボンコピーフィルタアクションは、元のメッセージの完全なコピーであるメッセージを新規作成します。通知フィルタアクションは、元のメッセージのヘッダーを含むメッセージを新規作成します。まれにはありますが、ヘッダーにウイルスが含まれている場合があります。バウンスフィルタアクションは、元のメッセージの最初の 10 キロバイトを含むメッセージを新規作成します。3 つのうちいずれの場合についても、新しいメッセージはアンチウイルススキャンやアンチスパムスキャンの処理対象とはなりません。

複数のホストに送信する場合は、`bcc()` アクションを複数回呼び出すことができます。

```
multiplealthosts:

  if (recv-listener == "IncomingMail")

  {

    insert-header('X-ORIGINAL-IP', '$remote_ip');

    bcc ('$EnvelopeRecipients', '$Subject', '$EnvelopeFrom', '10.2.3.4');

    bcc ('$EnvelopeRecipients', '$Subject', '$EnvelopeFrom', '10.2.3.5');

    bcc ('$EnvelopeRecipients', '$Subject', '$EnvelopeFrom', '10.2.3.6');

  }

```

`bcc-scan()` アクション

`bcc-scan` アクションは `bcc` アクションと同様に機能しますが、送信されるメッセージは新しいメッセージとして扱われるため、電子メールパイプライン全体を経由して送信されます。

```
momFilter:

  if ((mail-from == '^johnny$') and (rcpt-to == '^sue$'))

  {

    bcc-scan ('mom@home.org');

  }

```

隔離および複製アクション

`quarantine('隔離エリア名')` アクションは、隔離エリアと呼ばれるキューに入れるメッセージにフラグを設定します。隔離についての詳細については、「隔離」の章を参照してください。

`duplicate-quarantine('隔離エリア名')` アクションを実行すると、メッセージのコピーが指定されている隔離エリアにただちに配置されます。隔離エリア名の大文字と小文字は区別されます。

隔離フラグの付けられたメッセージは、電子メールパイプラインの残りの処理を続けます。メッセージがパイプラインの末尾に到達すると、メッセージに1つ以上の隔離に関するフラグが設定されていれば、該当するキューに入ります。それ以外の場合は配信されます。メッセージがパイプラインの末尾に到達しなければ、隔離エリアには配置されません。

したがって、メッセージフィルタに `quarantine()` アクションがあり、その後に `bounce()` または `drop()` アクションが続く場合、最後のアクションによりメッセージはパイプラインの末尾に到達しないため、メッセージは隔離エリアに配置されません。メッセージフィルタに隔離アクションが含まれる場合も同様ですが、メッセージはアンチスパムまたはアンチウイルス スキャン、またはコンテンツフィルタによりドロップされます。`skip-filters()` アクションによりメッセージは残りのメッセージフィルタをとばしますが、コンテンツフィルタが適用される場合があります。たとえば、メッセージフィルタがメッセージに隔離フラグを設定し、同時に最後の `skip_filters()` アクションも設定している場合、電子メールパイプラインの他のアクションによりメッセージがドロップされる場合を除き、メッセージは残りのメッセージフィルタをすべてスキップした上で隔離されます。

次の例では、メッセージに「secret_word」という辞書にあるいずれかの単語が含まれていると、そのメッセージは Policy 隔離エリアに送信されます。

```
quarantine_codenames:

    if (dictionary-match ('secret_words'))

        {

            quarantine('Policy');

        }
```

次の例では、ある会社に .mp3 ファイル形式の添付ファイルをすべてドロップする公式ポリシーがあるものと仮定しています。受信メッセージに .mp3 形式の添付ファイルがある場合、この添付ファイルは削除され、残りのメッセージ（本文と他の添付ファイル）は本来の受信者に送信されます。元のメッセージにすべての添付ファイルが添付されているコピーが隔離（Policy 隔離エリアに送信）されます。ブロックされた添付ファイルを受信する必要がある場合、本来の受信者はメッセージを隔離エリアから解放するよう要求することができます。

```
strip_all_mp3s:

    if (attachment-filename == '(?i)\\.mp3$') {

        duplicate-quarantine('Policy');

        drop-attachments-by-name ('(?i)\\.mp3$');

    }
```

受信者変更アクション

alt-rcpt-to アクションは、メッセージの配信時にメッセージのすべての受信者を指定した受信者に変更します。

次のフィルタは、エンベロープ受信者のアドレスに .freelist.com が含まれているすべてのメッセージを送信し、そのメッセージの受信者を system-lists@myhost.com に変更します。

```
freelistFilter:

    if(rcpt-to == '\\.freelist\\.com$')

        {

            alt-rcpt-to('system-lists@myhost.com');

        }
```

配信ホスト変更アクション

alt-mailhost アクションは、選択したメッセージのすべての受信者の IP アドレスを、指定した数値 IP アドレスまたはホスト名に変更します。



(注)

alt-mailhost アクションを実行すると、アンチスパム スキャンによりスパムと分類されたメッセージが隔離されないようにすることができます。alt-mailhost アクションは隔離アクションに優先して実行され、指定したメール ホストにメッセージを送信します。

次のフィルタは、すべての受信者について、受信者のアドレスをホスト example.com に変更します。

```
localRedirectFilter:

    if(true)
    {

        alt-mailhost('example.com');

    }
```

これにより、joe@anywhere.com に送信されるメッセージの Envelope To アドレスが joe@anywhere.com になり、メッセージは example.com のメールホストに送信されます。smtproutes コマンドで指定された追加ルーティング情報は、引き続きメッセージのルーティングに適用されます。[「ローカルドメインの電子メールのルーティング」\(P.21-1\)](#) を参照。



(注)

alt-mailhost アクションではポート番号を指定できません。この操作を行うには、かわりに SMTP ルートを追加します。

次のフィルタは、すべてのメッセージを 192.168.12.5 にリダイレクトします。

```
local2Filter:

    if(true)
    {

        alt-mailhost('192.168.12.5');

    }
```

送信元ホスト (Virtual Gateway アドレス) 変更アクション

alt-src-host アクションは、メッセージの送信元ホストを指定した送信元に変更します。送信元ホストは、メッセージの送信元となる IP インターフェイス、または IP インターフェイスのグループにより構成されます。IP インターフェイスのグループが選択された場合、システムは電子メールの配信時に、グループ内のすべての IP インターフェイスを送信元インターフェイスとして使用する処理を繰り返します。つまり、これにより 1 台の Cisco 電子メールセキュリティ アプライアンスに複数の Virtual Gateway アドレスを設定できます。詳細については、[「Virtual Gateway™ テクノロジーを使用してすべてのホストされたドメインでの構成のメール ゲートウェイ」\(P.21-59\)](#) を参照してください。

IP インターフェイスは、システムで現在設定されている IP インターフェイスまたはインターフェイスのグループにしか変更できません。次のフィルタは、IP アドレスが 1.2.3.4 であるリモート ホストから受信したすべてのメッセージに対して、発信（配信）IP インターフェイス `outbound2` を使用する Virtual Gateway を作成します。

```
externalFilter:

    if(remote-ip == '1.2.3.4')

    {

        alt-src-host('outbound2');

    }

}
```

次のフィルタは、IP アドレスが 1.2.3.4 であるリモート ホストから受信したすべてのメッセージに対して、IP インターフェイスのグループ `Group1` を使用します。

```
groupFilter:

    if(remote-ip == '1.2.3.4')

    {

        alt-src-host('Group1');

    }

}
```

アーカイブ アクション

archive アクションは、元のメッセージ（すべてのメッセージ ヘッダーと受信者を含む）のコピーを、アプライアンス上の `mbox` 形式のファイルに保存します。このアクションでは、メッセージを保存するログ ファイルの名前がパラメータとして使用されます。システムはフィルタの作成時に、指定したファイル名で自動的にログ サブスクリプションを作成します。また、既存のフィルタ ログ ファイルを指定することもできます。フィルタとフィルタ ログ ファイルの作成後は、`filters -> logconfig` サブコマンドでフィルタ ログ オプションを編集できます。



(注)

`logconfig` コマンドは `filters` のサブコマンドです。このサブコマンドの完全な説明については、「[CLI を使用したメッセージフィルタの管理](#)」(P.9-79) を参照してください。

`mbox` 形式は標準の UNIX メールボックス形式で、メッセージを簡単に表示するためのユーティリティが多数用意されています。大部分の UNIX システムでは、「`mail -f mbox.filename`」と入力するとファイルを表示できます。`mbox` 形式はプレーン テキストであるため、普通のテキスト エディタを使用してメッセージの内容を表示することができます。

次の例では、エンベロープ送信者が `joesmith@yourdomain.com` と一致する場合に、メッセージのコピーが `joesmith` というログに保存されます。

```
logJoeSmithFilter:

    if(mail-from == '^joesmith@yourdomain\\.com$')
```

```
{  
  
    archive('joesmith');  
  
}
```

ヘッダー削除アクション

strip-header アクションは、メッセージの特定のヘッダーを調べ、配信する前に該当する行をメッセージから削除します。ヘッダーが複数ある場合は、ヘッダーのすべてのインスタンス（「Received:」ヘッダーなど）が削除されます。

次の例では、すべてのメッセージで送信前に X-DeleteMe ヘッダーが削除されます。

```
stripXDeleteMeFilter:  
  
    if (true)  
  
    {  
  
        strip-header('X-DeleteMe');  
  
    }
```

ヘッダーに関する操作を行う場合、ヘッダーの現在の値には処理中に行われた変更（メッセージのヘッダーの追加、削除、変更を行うフィルタ処理など）が含まれている点に注意してください。詳細については、「[メッセージヘッダールールおよび評価](#)」(P.9-5) を参照してください。

ヘッダー挿入アクション

insert-header アクションは、メッセージに新しいヘッダーを挿入します。AsyncOS は、挿入したヘッダーが規格を満たしているかどうかを検証しません。生成されるメッセージが電子メールのインターネット規格を満たしているかどうかは、ユーザが自分で確認する必要があります。

次の例では、X-Company というヘッダーがメッセージにない場合に、このヘッダーに My Company Name という値が設定されます。

```
addXCompanyFilter:  
  
    if (not header('X-Company'))  
  
    {  
  
        insert-header('X-Company', 'My Company Name');  
  
    }
```

insert-header() アクションでは、ヘッダーのテキストに非 ASCII 文字を使用できます。ただし、ヘッダー名には（規格遵守のため）ASCII 文字しか使用できません。可読性を最大限に高めるため、トランスポート エンコードは Quoted-Printable となります。



(注)

strip-headers アクションと insert-header アクションを組み合わせることにより、元のメッセージにある任意のメッセージヘッダーを書き換えることができます。場合によっては、同じヘッダーを複数回使用することができます (Received: など)、それ以外の場合は同じヘッダーを複数回使用すると MUA が混乱する場合があります (Subject: ヘッダーを複数回使用する場合など)。

ヘッダーに関する操作を行う場合、ヘッダーの現在の値には処理中に行われた変更 (メッセージのヘッダーの追加、削除、変更を行うフィルタ処理など) が含まれている点に注意してください。詳細については、「[メッセージヘッダールールおよび評価](#)」(P.9-5) を参照してください。

ヘッダーテキスト編集アクション

edit-header-text アクションを実行すると、正規表現の置換機能を使用して、指定したヘッダーテキストを書き換えることができます。このフィルタはヘッダー内で正規表現と一致するテキストを検索し、指定した正規表現に置き換えます。

たとえば、電子メールに次のような件名ヘッダーがあるものとします。

```
Subject: SCAN Marketing Messages
```

次のフィルタは、「SCAN」というテキストを削除し、「Marketing Messages」というテキストをヘッダー内に残します。

```
Remove_SCAN: if true
{
    edit-header-text ('Subject', '^SCAN\s*', '');
}
```

フィルタはメッセージを処理した後、次のヘッダーを返します。

```
Subject: Marketing Messages
```

本文編集アクション

edit-body-text() メッセージフィルタの機能は Edit-Header-Text() フィルタと同様ですが、メッセージのヘッダーではなく本文が処理対象です。

edit-body-text() メッセージフィルタは次の構文を使用します。最初のパラメータは検索のための正規表現で、2 番目のパラメータは置換のためのテキストです。

```
Example: if true {
edit-body-text("parameter 1",
"parameter 2");
}
```

edit-body-text() メッセージフィルタはメッセージ本文のみが処理対象です。特定の MIME 部分がメッセージの「本文」と見なされるか「添付ファイル」と見なされるかの詳細については、「[メッセージ本文とメッセージ添付ファイル](#)」(P.9-5) を参照してください。

次の例では、メッセージから URL が削除され、「URL REMOVED」というテキストに置き換えられています。

```
URL_Replaced: if true {

    edit-body-text("(?i)(?:https?|ftp)://[^\s">]+", "URL REMOVED");

}
```

次の例では、メッセージの本文から社会保障番号が削除され、「XXX-XX-XXXX」というテキストに置き換えられています。

```
ssn: if true {

    edit-body-text("(?!000)(?:[0-6]\\d{2}|7(?:[0-6]\\d|7[012]))([
-]?) (?!00) \\d\\d\\d\\1 (?!0000) \\d{4}",

    "XXX-XX-XXXX");

}
```



(注)

現時点では、edit-body-text() フィルタではスマート ID を使用できません。

HTML 変換アクション

RFC 2822 では電子メールメッセージのテキスト形式が規定されていますが、RFC 2822 メッセージ内の他のコンテンツのトランスポートを実現するための拡張機能 (MIME など) があります。AsyncOS は html-convert() メッセージフィルタを使用して、次の構文により HTML をプレーンテキストに変換できます。

```
Convert_HTML_Filter:

if (true)

{

html-convert();

}
```

Cisco メッセージフィルタは、特定の MIME 部分がメッセージの「本文」であるか「添付ファイル」であるかを判別します。html-convert() メッセージフィルタはメッセージ本文のみが処理対象です。メッセージの本文と添付ファイルの詳細については、「[メッセージ本文とメッセージ添付ファイル](#)」(P.9-5) を参照してください。

html-convert() フィルタが文書内の HTML を削除する方式は、形式によって異なります。

メッセージがプレーン テキスト (`text/plain`) である場合、メッセージは変更されずにフィルタを通過します。メッセージが単純な HTML メッセージ (`text/html`) である場合、すべての HTML タグはメッセージから削除され、残りの本文が HTML メッセージにかわり使用されます。各行の再フォーマットは行われず、HTML がプレーンテキストになることはありません。構造が MIME (multipart/alternative 構造) で、同じコンテンツに `text/plain` 部分と `text/html` 部分が含まれている場合、フィルタはメッセージの `text/html` 部分を削除して `text/plain` 部分を残します。その他の MIME タイプ (multipart/mixed など) では、すべての HTML 本文部分のタグが削除され、メッセージに再挿入されます。

メッセージフィルタでは、`html-convert()` フィルタ アクションは処理対象のメッセージにタグを設定するだけで、メッセージ構造の変更はただちには行われません。メッセージの変更は、すべての処理が完了した後に行われます。これにより、変更前に他のフィルタ アクションが元のメッセージを処理することができます。

バウンス プロファイル アクション

`bounce-profile` アクションは、設定済みのバウンス プロファイルをメッセージに割り当てます。「[バウンスした電子メールの処理](#)」(P.21-36) を参照)。メッセージを配信できない場合、バウンス プロファイルで設定されたバウンス オプションが使用されます。この機能は、リスナーの設定から割り当てられているバウンス プロファイル (割り当てられている場合) に優先して適用されます。

次のフィルタの例では、送信される電子メールのうち、ヘッダーに「`X-Bounce-Profile: fastbounce`」があるすべての電子メールにバウンス プロファイル「`fastbounce`」が割り当てられます。

```
fastbounce:

    if (header ('X-Bounce-Profile') == 'fastbounce') {

        bounce-profile ('fastbounce');

    }
```

アンチスパム システムのバイパス アクション

`skip-spamcheck` アクションは、システムに設定されたコンテンツベースのアンチスパム フィルタリングをすべてバイパスするようシステムに指示します。コンテンツベースのアンチスパム フィルタリングが設定されていない場合、またはメッセージがあらかじめスパム スキャンの対象に設定されていない場合は、このアクションを実行してもメッセージに影響はありません。

次の例では、メッセージの `SenderBase` レピュテーション スコアが高い場合に、メッセージに対するコンテンツベースのアンチスパム フィルタリングがバイパスされます。

```
whitelist_on_reputation:

    if (reputation > 7.5)

    {

        skip-spamcheck ();

    }
```

関連項目

- 「[メッセージがスパムかどうかスキャンするためのアプライアンスの設定方法](#)」(P.13-2)

- 「スパムフィルタからのアプライアンス生成メッセージの保護」(P.13-13)

アンチウイルスシステムのバイパスアクション

skip-viruscheck アクションは、システムに設定されたウイルス保護システムをすべてバイパスするようシステムに指示します。アンチウイルスシステムが設定されていない場合、またはメッセージがあらかじめウイルススキャンの対象に設定されていない場合は、このアクションを実行してもメッセージに影響はありません。

次の例では、「private_listener」というリスナーで受信したメッセージに対して、アンチスパムシステムとアンチウイルスシステムによる処理がバイパスされています。

```
internal_mail_is_safe:

    if (recv-listener == 'private_listener')

    {

        skip-spamcheck();

        skip-viruscheck();

    }
```

ウイルスアウトブレイクフィルタのスキャン処理バイパスアクション

skip-vofcheck アクションは、メッセージのウイルスアウトブレイクフィルタによるスキャン処理がバイパスされるようシステムに指示します。ウイルスアウトブレイクフィルタのスキャン処理がイネーブルになっていない場合、このアクションを実行してもメッセージに影響はありません。

次の例では、「private_listener」というリスナーで受信したメッセージに対して、ウイルスアウトブレイクフィルタのスキャン処理がバイパスされています。

```
internal_mail_is_safe:

    if (recv-listener == 'private_listener') Outbreak Filters

    {

        skip-vofcheck();

    }
```

メッセージタグ追加アクション

tag-message アクションは、RSA Email DLP ポリシーフィルタリングで使用するカスタム用語を送信メッセージに挿入します。RSA Email DLP ポリシーを設定して、スキャン対象をメッセージタグがあるメッセージに限定することができます。メッセージタグは受信者側では表示されません。タグ名には、[a-zA-Z0-9_-.] の範囲の文字のうち任意のものを組み合わせて使用できます。

メッセージのフィルタリングに使用する DLP ポリシーの設定の詳細については、「データ消失防止」の章を参照してください。

次の例では、件名に「[Encrypt]」が含まれるメッセージにメッセージタグを挿入しています。Cisco Email Encryption が使用できる場合は、メッセージの配信前にメッセージをこのメッセージタグで暗号化する DLP ポリシーを作成できます。

```
Tag_Message:

    if (subject == '^\[Encrypt\]')

    {

        tag-message('Encrypt-And-Deliver');

    }
```

ログ エントリ追加アクション

log-entry アクションは、カスタマイズしたテキストを、IronPort テキスト メール ログに INFO レベルで追加します。このテキストにはアクション変数を使用することができます。このアクションを使用すると、デバッグ時に便利なテキストや、メッセージフィルタがアクションを実行した理由に関する情報を挿入できます。ログ エントリはメッセージ トラッキングにも表示されます。

次の例では、メッセージに会社の機密情報が含まれていると判断されたためメッセージがバウンスされたことを示すログ エントリが挿入されます。

```
CompanyConfidential:

    if (body-contains('Company Confidential'))

    {

        log-entry('Message may have contained confidential information.');
```

```
        bounce();

    }
```

添付ファイルのスキャン

AsyncOS は企業ポリシーに準拠していないメッセージの添付ファイルを削除でき、一方で元のメッセージはそのまま配信することができます。

添付ファイルのフィルタリングは、特定のファイル タイプ、フィンガープリント、添付ファイルの内容に基づいて行うことができます。フィンガープリントを使用して添付ファイルの正確な種類を判別することにより、ユーザは悪意のある添付ファイルの拡張子 (.exe など) を一般的な拡張子 (.doc など) に変更して、名前が変更されたファイルが添付ファイル フィルタを通過できるようにすることができます。

添付ファイルのコンテンツをスキャンすると、Stellent 添付ファイル スキャン エンジン は添付ファイルからデータを抽出し、正規表現による検索を実行します。添付ファイルのデータとメタデータの両方が検査対象となります。Excel または Word 文書をスキャンする場合、添付ファイル スキャン エンジン は .exe、.dll、.bmp、.tiff、.pcx、.gif、.jpeg、.png、Photoshop 画像の各埋め込みファイルも検出できます。

添付ファイルのスキャンで使用するメッセージフィルタ

表 9-8 に記載されているメッセージフィルタは最終でないアクションです。(添付ファイルはドロップされ、メッセージの処理が続行されます)。

オプションのコメントは、フッターのようにメッセージに追加されるテキストで、メッセージフィルタアクション変数(「添付ファイルのスキャンメッセージフィルタの例」(P.9-75)を参照)を使用することもできます。

表 9-8 添付ファイルのスキャンで使用するメッセージフィルタアクション

アクション	構文	説明
添付ファイルのドロップ (名前別)	drop-attachments-by-name (<i><regular expression></i> [, <i><optional comment></i>])	メッセージの添付ファイルのうち、指定した正規表現と一致する名前のファイルをすべてドロップします。アーカイブ形式の添付ファイル(zip、tar)内に該当するファイルがある場合、この添付ファイルはドロップされます。「添付ファイルのスキャンメッセージフィルタの例」(P.9-75)を参照してください。
添付ファイルのドロップ (タイプ別)	drop-attachments-by-type (<i><MIME type></i> [, <i><optional comment></i>])	メッセージの添付ファイルのうち、指定したMIMEタイプまたはファイル拡張子に該当するMIMEタイプのファイルをすべてドロップします。アーカイブ形式の添付ファイル(zip、tar)内に該当するファイルがある場合、この添付ファイルはドロップされます。
添付ファイルのドロップ (ファイルタイプ別)	drop-attachments-by-filetype (<i><fingerprint name></i> [, <i><optional comment></i>])	メッセージの添付ファイルのうち、指定したファイルの「フィンガープリント」と一致するファイルをすべてドロップします。アーカイブ形式の添付ファイル(zip、tar)内に該当するファイルがある場合、この添付ファイルはドロップされます。詳細については、「表 9-6 添付ファイルグループ」(P.9-47)を参照してください。
添付ファイルのドロップ (MIMEタイプ別)	drop-attachments-by-mimetype (<i><MIME type></i> [, <i><optional comment></i>])	メッセージの添付ファイルのうち、特定のMIMEタイプのファイルをすべてドロップします。このアクションではファイル拡張子によるMIMEタイプの判別は行われず、アーカイブの内容の確認もされません。
添付ファイルのドロップ (サイズ別)	drop-attachments-by-size (<i><number></i> [, <i><optional comment></i>])	メッセージの添付ファイルのうち、ローエンコード形式で指定したサイズ(バイト単位)以上のサイズであるファイルをすべてドロップします。アーカイブファイルまたは圧縮ファイルの場合、このアクションは、圧縮前のサイズを検証せず、実際の自体のサイズが計測されません。

表 9-8 添付ファイルのスキャンで使用するメッセージ フィルタ アクション (続き)

アクション	構文	説明
添付ファイルのスキャン	drop-attachments-where-contains (<regular expression>[, <optional comment>])	メッセージの添付ファイルのうち、指定した正規表現を含むファイルをすべてドロップします。アーカイブ ファイル (zip、tar) は、中に含まれているファイルのいずれかが正規表現と一致する場合にドロップされます。
添付ファイルのドロップ (辞書との一致別)	drop-attachments-where-dictionary-match(<dictionary name>)	このフィルタ アクションは、辞書の用語との一致に基づいて添付ファイルを削除します。添付ファイルであると判断される MIME 部分の用語が辞書の用語と一致する場合 (かつ、ユーザ定義のしきい値に達している場合)、添付ファイルが電子メールから削除されます。「添付ファイルのスキャン メッセージ フィルタの例」(P.9-75) を参照してください。

イメージ分析

メッセージによってはイメージを含むものがあり、適切でないコンテンツがないかスキャンすることが必要になる場合があります。イメージ分析エンジンを使用すると、電子メール内の適切でないコンテンツを検索できます。イメージ分析は、アンチウイルスおよびアンチスパム スキャン エンジンの補完または代替を目的とするものではありません。この機能は、電子メール内の適切でないコンテンツを特定することにより、許容範囲での使用を促進するためのものです。イメージ分析スキャン エンジンを使用すると、メールの隔離と分析、および傾向の認識ができます。

AsyncOS でイメージ分析を設定すると、イメージ分析フィルタ ルールを使用して、疑わしい電子メールや適切でない電子メールに対してアクションを実行することができます。イメージ スキャンでは、JPEG、BMP、PNG、TIFF、GIF、TGA、ICO、PCX の各添付ファイルのタイプをスキャンできます。イメージアナライザは、スキンカラー、本体サイズ、曲率を測定するアルゴリズムを使用し、画像に適切でないコンテンツが含まれる可能性を判定します。イメージ添付ファイルをスキャンすると、Cisco フィンガープリントによりファイル タイプが特定され、イメージアナライザはイメージ コンテンツを分析するアルゴリズムを使用します。イメージが別のファイルに埋め込まれている場合、Stellent スキャン エンジンによりファイルが抽出されます。Stellent スキャン エンジンは、Word、Excel、PowerPoint 文書などの各種のファイル タイプからイメージを抽出できます。イメージ分析の結果は、メッセージ全体で計算されます。メッセージにイメージがない場合、メッセージのスコアは 0 となります。これは分析結果が「Clean」であることを表します。そのため、イメージがないメッセージに対する分析結果は「Clean」となります。



(注)

PDF ファイルのイメージは抽出されません。

イメージ分析スキャン エンジンの設定

GUI からイメージ分析をイネーブル化するには、次の手順を実行します。

手順

- ステップ 1** [セキュリティ サービス (Security Services)] > [IronPort イメージ分析 (IronPort Image Analysis)] の順に進みます。

ステップ 2 [有効 (Enable)] をクリックします。

成功したことを示すメッセージが表示され、分析結果設定が表示されます。

**図 9-3 Cisco イメージ分析の概要
IronPort Image Analysis**

IronPort Image Analysis Overview			
IronPort Image Analysis:	Enabled		
Image Analysis Sensitivity:	65		
Skip Images:	Enabled, 100 pixels		
Verdict Ranges:	CLEAN	SUSPECT	INAPPROPRIATE
	0 - 49	50 - 74	75 - 100
Edit Settings...			

イメージ分析フィルタ ルールを使用すると、次の各分析結果に基づいてアクションを決定できます。

- [正常 (Clean)]: イメージに適切でないコンテンツはありません。イメージ分析の結果はメッセージ全体で計算されるため、イメージがないメッセージをスキャンすると分析結果は [正常 (Clean)] となります。
- [疑わしい (Suspect)]: イメージに適切でないコンテンツがある可能性があります。
- [不適切 (Inappropriate)]: イメージに適切でないコンテンツがあります。

これらの計算結果には、イメージアナライザのアルゴリズムにより、適切でないコンテンツがある可能性を示す数値が割り当てられます。

次の値が推奨されます。

- [正常 (Clean)]: 0 ~ 49
- [疑わしい (Suspect)]: 50 ~ 74
- [不適切 (Inappropriate)]: 75 ~ 100

精度を設定することによりイメージ スキャンを微調整できます。これにより、誤判定を減らすことができます。たとえば、誤判定が発生している場合は、精度を低くします。逆に、イメージ スキャンで適切でないコンテンツが検出されていない場合は、精度を高く設定します。精度設定は 0 (一切検出しない) と 100 (精度が最高である) の間の値です。デフォルトの精度の 65 に設定することを推奨します。

イメージ分析の調整

手順

ステップ 1 [セキュリティ サービス (Security Services)] > [IronPort イメージ分析 (IronPort Image Analysis)] の順に進みます。

ステップ 2 [設定を編集 (Edit Settings)] をクリックします。

図 9-4 IronPort イメージ分析設定の編集 (Edit IronPort Image Analysis Settings)

ステップ 3 イメージ分析の精度を設定します。デフォルトの精度の 65 に設定することを推奨します。

ステップ 4 [正常 (Clean)]、[疑わしい (Suspect)]、および[不適切 (Inappropriate)] の評価を設定します。

値の範囲を設定する場合、値が重ならないようにしてください。また、すべて整数を使用してください。

ステップ 5 任意で、最小サイズの要件を満たさないイメージのスキャンをバイパスするように、AsyncOS を設定します (推奨)。デフォルトで、この設定は 100 ピクセルに設定されています。100 ピクセル未満のイメージをスキャンすると、誤検知が発生する可能性があります。

imageanalysisconfig コマンドを使用して、CLI からイメージ分析設定をイネーブルにすることもできます。

```
test.com> imageanalysisconfig
```

```
IronPort Image Analysis: Enabled
```

```
Image Analysis Sensitivity: 65
```

```
Verdict Ranges: Clean (0-49), Suspect(50-74), Inappropriate (75+)
```

```
Skip small images with size less than 100 pixels (width or height)
```

```
Choose the operation you want to perform:
```

```
- SETUP - Configure IronPort Image Analysis.
```

```
[ ]> setup
```

```
IronPort Image Analysis: Enabled
```

```
Would you like to use IronPort Image Analysis? [Y]>
```

Define the image analysis sensitivity. Enter a value between 0 (least sensitive) and 100 (most sensitive). As sensitivity increases, so does the false positive rate. The default setting of 65 is recommended.

[65]>

Define the range for a CLEAN verdict. Enter the upper bound of the CLEAN range by entering a value between 0 and 98. The default setting of 49 is recommended.

[49]>

Define the range for a SUSPECT verdict. Enter the upper bound of the SUSPECT range by entering a value between 50 and 99. The default setting of 74 is recommended.

[74]>

Would you like to skip scanning of images smaller than a specific size? [Y]>

Please enter minimum image size to scan in pixels, representing either height or width of a given image.

[100]>

特定のメッセージのレピュテーションスコアの表示

特定のメッセージのレピュテーションスコアを確認するには、メールログを参照します。メールログにはイメージ名またはファイル名、特定のメッセージの添付ファイルのスコアが表示されます。また、ログにはファイル内のイメージがスキャン可能かどうかについての情報も表示されます。このログには、各イメージではなく、各メッセージの添付ファイルの結果に関する情報が表示されます。たとえば、メッセージに JPEG イメージを含む zip ファイルが添付されていた場合、ログのエントリには JPEG の名前ではなく、zip ファイルの名前が表示されます。また、zip ファイルに複数のイメージが含まれている場合、ログ エントリにはすべてのイメージの最大スコアが表示されます。「unscannable」の通知は、いずれかのイメージがスキャンできないことを意味します。

ログには、スコアがどのように特定の評価 ([clean]、[suspect]、または [inappropriate]) に反映されるかに関する情報はありません。ただし、メールログを使用して特定のメッセージの配信を追跡できるため、メッセージに対して実行されたアクションによって、メールに不適切なイメージまたは疑わしいイメージが含まれていたかがわかります。

たとえば、次のメールログでは、イメージ分析スキャンの結果、メッセージフィルタルールによってドロップされた添付ファイルを示しています。

```
Thu Apr 3 08:17:56 2009 Debug: MID 154 IronPort Image Analysis: image 'Unscannable.jpg'
is unscannable.
```

```
Thu Apr 3 08:17:56 2009 Info: MID 154 IronPort Image Analysis: attachment
'Unscannable.jpg' score 0 unscannable
```

```
Thu Apr 3 08:17:56 2009 Info: MID 6 rewritten to MID 7 by
drop-attachments-where-image-verdict filter 'f-001'
```

```
Thu Apr 3 08:17:56 2009 Info: Message finished MID 6 done
```

イメージ分析結果に基づいたアクション実行のメッセージフィルタの設定

イメージ分析をイネーブルにしたら、メッセージフィルタを作成して、さまざまなメッセージの評価に対してさまざまなアクションを実行する必要があります。たとえば、問題ないと評価されたメッセージを配信し、不適切なコンテンツを含むと判断されたメッセージを隔離する必要があります。



(注)

シスコでは、不適切または疑わしいと評価されたメッセージをドロップまたはバウンスしないことを推奨します。代わりに、後で確認してトレンド分析について把握するために、違反したメッセージのコピーを隔離します。

次のフィルタは、コンテンツが不適切または疑わしい場合にタグを付けられるメッセージを示しています。

```
image_analysis: if image-verdict == "inappropriate" {

strip-header("Subject");

insert-header("Subject", "[inappropriate image] $Subject");

}

else {

if image-verdict == "suspect" {

strip-header("Subject");

insert-header("Subject", "[suspect image] $Subject");

}

}
```

イメージ分析の評価に基づいて添付ファイルを除去するコンテンツフィルタの作成

イメージ分析をイネーブルにすると、コンテンツフィルタを作成してイメージ分析の評価に基づいて添付ファイルを削除するか、さまざまなメッセージの評価に対してさまざまなアクションを実行するようにフィルタを設定できます。たとえば、不適切なコンテンツを含むメッセージを隔離することに決定したとします。

イメージ分析の評価に基づいて添付ファイルを削除するには、次の手順を実行します。

手順

-
- ステップ 1** [メールポリシー (Mail Policies)] > [受信コンテンツフィルタ (Incoming Content Filters)] をクリックします。
 - ステップ 2** [フィルタを追加 (Add Filter)] をクリックします。
 - ステップ 3** コンテンツフィルタの名前を入力します。
 - ステップ 4** [アクション (Actions)] で、[アクションを追加 (Add Action)] をクリックします。
 - ステップ 5** [ファイル情報によって添付ファイルを除去 (Strip Attachment by File Info)] で、[イメージ分析判定 (Image Analysis Verdict is)] をクリックします。
 - ステップ 6** 次のイメージ分析の評価から選択します。
 - 疑わしい (Suspect)
 - 不適切 (Inappropriate)
 - 不適切もしくは疑わしい (Suspect or Inappropriate)
 - スキャン不可 (Unscannable)
 - 正常 (Clean)
-

イメージ分析の評価に基づくアクションを設定するには、次の手順を実行します。

手順

-
- ステップ 1** [メールポリシー (Mail Policies)] > [受信コンテンツフィルタ (Incoming Content Filters)] をクリックします。
 - ステップ 2** [フィルタを追加 (Add Filter)] をクリックします。
 - ステップ 3** コンテンツフィルタの名前を入力します。
 - ステップ 4** [条件 (Conditions)] で、[条件を追加 (Add Condition)] をクリックします。
 - ステップ 5** [添付ファイルのファイル情報 (Attachment File Info)] で、[イメージ分析判定 (Image Analysis Verdict)] をクリックします。
 - ステップ 6** 次のいずれかの評価を選択します。
 - 疑わしい (Suspect)
 - 不適切 (Inappropriate)
 - 不適切もしくは疑わしい (Suspect or Inappropriate)
 - スキャン不可 (Unscannable)
 - 正常 (Clean)
 - ステップ 7** [アクションを追加 (Add Action)] をクリックします。

ステップ 8 イメージ分析の評価に基づいてメッセージに対して実行するアクションを選択します。

ステップ 9 変更内容を送信し、確定します。

通知

GUI の [テキスト リソース (Text Resources)] ページまたは `textconfig` CLI コマンドを使用して、カスタム通知テンプレートをテキスト リソースとして設定することもできます。これも、添付ファイルのフィルタ ルールと組み合わせて使用すると便利なツールです。通知テンプレートは非 ASCII 文字をサポートしています (テンプレートを作成するとき、エンコードを選択するように要求されます)。

次の例では、最初に `textconfig` コマンドを使用して、`strip.mp3` という名前の通知テンプレートを作成します。これは、通知メッセージの本文に挿入されます。次に、添付ファイルのフィルタ ルールを作成し、`.mp3` ファイルがメッセージから削除された場合、予定していた受信者宛てに `.mp3` ファイルが削除されたことを通知する電子メールが送信されるように設定できます。

```
drop-mp3s:

if (attachment-type == '*/mp3')

{ drop-attachments-by-filetype('Media');

    notify ('$EnvelopeRecipients', 'Your mp3 has been removed', '$EnvelopeFrom',
    'strip.mp3');

}
```

詳細については、「[通知およびコピー通知アクション](#)」(P.9-54) を参照してください。

添付ファイルのスキャン メッセージ フィルタの例

次に、添付ファイルに対して実行されるアクションの例を示します。

ヘッダーの挿入

この例では、添付ファイルに指定したコンテンツが含まれている場合に、AsyncOS がヘッダーを挿入します。

次の例では、あるキーワードが含まれるかどうか、メッセージのすべての添付ファイルをスキャンします。すべての添付ファイルにキーワードが存在する場合、カスタムの X-Header が挿入されます。

```
attach_disclaim:

if (every-attachment-contains('[dD]isclaimer')) {

    insert-header("X-Example-Approval", "AttachOK");

}
```

次の例では、特定のバイナリ データのパターンがあるかどうか、添付ファイルのスキャンします。フィルタは attachment-binary-contains フィルタ ルールを使用して、PDF ドキュメントが暗号化されていることを示すパターンを検索します。バイナリ データ内にそのパターンが存在する場合、カスタム ヘッダーが挿入されます。

```
match_PDF_Encrypt:

if (attachment-filetype == 'pdf' AND

attachment-binary-contains('/Encrypt')){

strip-header ('Subject');

insert-header ('Subject', '[Encrypted] $Subject');

}
```

ファイルタイプによる添付ファイルのドロップ

次の例では、添付ファイルの「executable」グループ (.exe、.dll、および .scr) がメッセージから削除され、削除されたファイルの名前を列挙するテキストがメッセージに追加されます (\$dropped_filename アクション変数を使用)。drop-attachments-by-filetype アクションは添付ファイルを確認し、3 文字のファイル拡張子だけではなく、ファイルのフィンガープリントに基づいて添付ファイルを削除します。1 つのファイルタイプ (「mpeg」) を指定したり、あるファイルタイプのすべてのメンバ (「Media」) を参照したりできます。

```
strip_all_exes: if (true) {

drop-attachments-by-filetype ('Executable', "Removed attachment:

$dropped_filename");

}
```

次の例では、エンベロープ送信者がドメイン example.com 内に存在しないメッセージから、同じ「executable」グループの添付ファイル (.exe、.dll、および .scr) が、削除されます。

```
strip_inbound_exes: if (mail-from != "@example\\.com$") {

drop-attachments-by-filetype ('Executable');

}
```

次の例では、エンベロープ送信者がドメイン example.com 内に存在しないメッセージから、ファイルタイプの特定のメンバ (「wmf」) および同じ「executable」グループの添付ファイル (.exe、.dll、および .scr) が削除されます。

```
strip_inbound_exes_and_wmf: if (mail-from != "@example\\.com$") {

drop-attachments-by-filetype ('Executable');
```

```
drop-attachments-by-filetype ('x-wmf');
}
```

次の例では、添付ファイルの「executable」事前定義グループが、より多くの添付ファイルの名前を含むように拡張されています。（このアクションでは、添付ファイルのファイルタイプは確認されません）。

```
strip_all_dangerous: if (true) {
    drop-attachments-by-filetype ('Executable');
    drop-attachments-by-name ('(?:i)\\. (cmd|pif|bat)$');
}
```

drop-attachments-by-name アクションでは、非 ASCII 文字をサポートしています。



(注)

drop-attachments-by-name アクションは、MIME ヘッダーでキャプチャされたファイル名に対して正規表現照合を実行します。MIME ヘッダーからキャプチャされたファイル名は、最後にスペースが存在する場合があります。

次の例では、添付ファイルがメッセージに .exe 実行ファイルのファイルタイプでない場合はドロップされます。ただし、フィルタは、除外するファイルタイプを備えた少なくとも1つの添付ファイルがあるメッセージへのアクションを実行しません。たとえば、次のフィルタは .exe ファイルタイプではない添付ファイルを含むメッセージをドロップします。

```
exe_check: if (attachment-filetype != "exe") {
    drop();
}
```

メッセージに複数の添付ファイルがある場合、電子メールセキュリティ アプライアンスは他の添付ファイルが .exe ファイルでない場合でも、添付ファイルの少なくとも1つが .exe ファイルの場合はメッセージをドロップしません。

ディクショナリの一致による添付ファイルのドロップ

この drop-attachments-where-dictionary-match アクションでは、ディクショナリの用語との一致に基づいて、添付ファイルを削除します。添付ファイルであると判断される MIME 部分の用語が辞書の用語と一致する場合（かつ、ユーザ定義のしきい値に達している場合）、添付ファイルが電子メールから削除されます。次の例では、「secret_words」ディクショナリ内の単語が添付ファイル内で検出されると、添付ファイルが削除されます。一致のしきい値は1に設定されている点に注意してください。

```
Data_Loss_Prevention: if (true) {
```

```
drop-attachments-where-dictionary-match("secret_words", 1);  
}
```

保護された添付ファイルの隔離

attachment-protected フィルタでは、メッセージ内の添付ファイルがパスワード保護されているかをテストします。受信メールに対してこのフィルタを使用して、添付ファイルがスキャン可能かどうかを確認できます。この定義に従い、1つの暗号化されたメンバと複数の暗号化されていないメンバーを含む zip ファイルは、保護されていると見なされます。同様に、オープンパスワードが設定されていない PDF ファイルは、コピーや印刷がパスワード保護されていたとしても、保護されているとは見なされません。次の例では、保護された添付ファイルが隔離エリア「Policy」に送信されます。

```
quarantine_protected:  
  
if attachment-protected  
{  
  
quarantine("Policy");  
}
```

保護されていない添付ファイルの検出

attachment-unprotected フィルタは、メッセージ内の添付ファイルがパスワード保護されていないかをテストします。このメッセージフィルタは、attachment-protected フィルタと補完関係にあります。このフィルタを送信メールに使用して、保護されていないメールを検出することができます。次の例では、AsyncOS が送信リスナーで保護されていない添付ファイルを検出し、メッセージを隔離しています。

```
quarantine_unprotected:  
  
if attachment-unprotected  
{  
  
quarantine("Policy");  
}
```

CLI を使用したメッセージフィルタの管理

CLI を使用して、メッセージフィルタの追加、削除、アクティブ化/非アクティブ化、インポート/エクスポート、ログ オプションの設定が可能です。次の表で、コマンドとサブコマンドについてまとめて説明します。

表 9-9 メッセージフィルタ サブコマンド

構文	説明
filters	メイン コマンド。このコマンドは対話形式で、詳細情報を入力するよう要求されま す（たとえば、new、delete、import など）。
new	新しいフィルタを作成します。場所を指定しない場合、現在のシーケンスにフィル タが追加されます。場所を指定した場合、シーケンスの特定の場所にフィルタが挿 入されます。詳細については、「 新しいメッセージフィルタの作成 」(P.9-80) を参 照してください。
delete	名前またはシーケンス番号を指定して、フィルタを削除します。詳細については、 「 メッセージフィルタの削除 」(P.9-80) を参照してください。
move	既存のフィルタを並べ替えます。詳細については、「 メッセージフィルタの移動 (P.9-80) を参照してください。
set	フィルタをアクティブまたは非アクティブ状態に設定します。詳細については、 「 メッセージフィルタのアクティベーションとディアクティベーション 」(P.9-81) を参照してください。
import	フィルタの現在のセットを、ファイル（アプライアンスの /configuration ディレク トリ）内に保存されている新しいセットに置き換えます。詳細については、「 メッ セージフィルタのインポート 」(P.9-84) を参照してください。
export	フィルタの現在のセットを（アプライアンスの /configuration ディレクトリ内の） ファイルにエクスポートします。詳細については、「 メッセージフィルタのエクス ポート 」(P.9-85) を参照してください。
list	1 つ以上のフィルタに関する情報を一覧表示します。詳細については、「 メッセージ フィルタ リストの表示 」(P.9-85) を参照してください。
detail	特定のフィルタに関する詳細情報（フィルタ ルール自体の本文など）を出力しま す。詳細については、「 メッセージフィルタの詳細の表示 」(P.9-86) を参照してく ださい。
logconfig	フィルタの logconfig サブメニューを入力すると、archive() フィルタ アクション からログ サブスクリプションを編集できます。詳細については、「 フィルタ ログ サ ブスクリプションの設定 」(P.9-86) を参照してください。



(注) フィルタを有効にするには、commit コマンドを発行する必要があります。

パラメータには、次の 3 つのタイプがあります。

表 9-10 フィルタ管理パラメータ

seqnum	フィルタのリスト内の位置に基づいてフィルタを表す整数です。たとえば、seqnum が 2 の場合、リスト内の 2 番目のフィルタを表します。
--------	---

表 9-10 フィルタ管理パラメータ (続き)

filename	フィルタの表示名。
range	range は、複数のフィルタを表す場合に使用することがあり、「X-Y」の形式で表されます。X と Y は、範囲を指定するための最初と最後の <i>seqnums</i> です。たとえば、「2-4」は、2、3、4 番目の位置にあるフィルタを表します。X または Y のいずれかを省略すると、無制限のリストを表します。たとえば、「-4」は最初から 4 つのフィルタを表し、「2-」は、先頭以外のすべてのフィルタを表します。キーワード <i>all</i> を使用して、フィルタリスト内のすべてのフィルタを表すこともできます。

新しいメッセージフィルタの作成

```
new [seqnum|filename|last]
```

新しいフィルタを挿入する位置を指定します。省略するか、キーワード *last* を指定すると、入力されたフィルタがフィルタリストの最後に追加されます。シーケンス番号は連続させる必要があります。現在のリストの範囲を越える *seqnum* は入力できません。不明な *filename* を入力すると、有効な *filename*、*seqnum*、または *last* を入力するように求められます。

フィルタを入力したら、手動でフィルタスクリプトを入力する必要があります。入力を終了したら、その行自体にピリオド (.) を入力してエントリを終了します。

次の条件ではエラーが発生します。

- シーケンス番号が現在のシーケンス番号の範囲を越えている。
- フィルタに付けた *filename* が一意ではない。
- フィルタに付けた *filename* が予約語である。
- フィルタに構文エラーが発生している。
- インターフェイスなど、存在しないシステムリソースを参照するアクションを実行するフィルタ。

メッセージフィルタの削除

```
delete [seqnum|filename|range]
```

指定したフィルタを削除します。

次の条件ではエラーが発生します。

- 指定した名前のフィルタが存在しない。
- 指定したシーケンス番号のフィルタが存在しない。

メッセージフィルタの移動

```
move [seqnum|filename|range seqnum|last]
```

最初のパラメータで指定したフィルタを、2 番目のパラメータで指定した場所に移動します。2 番目のパラメータがキーワード *last* である場合、フィルタはフィルタリストの最後に移動されます。複数のフィルタを移動する場合、それらのフィルタの相対的な順序は変わりません。

次の条件ではエラーが発生します。

- 指定した名前のフィルタが存在しない。

- 指定したシーケンス番号のフィルタが存在しない。
- シーケンス番号が現在のシーケンス番号の範囲を越えている。
- 移動してもシーケンスが変更されない。

メッセージフィルタのアクティベーションとディアクティベーション

指定されるメッセージフィルタは、*active* または *inactive* のいずれかであり、さらに *valid* または *invalid* のいずれかです。メッセージフィルタは、*active* と *valid* の両方の状態である場合にのみ処理に使用されます。CLI を通じて、既存のフィルタを *active* から *inactive* に変更します（その後、再び戻します）。存在しない（または削除された）リスナーまたはインターフェイスを参照している場合、そのフィルタは *invalid* です。



(注)

フィルタが *inactive* であるかどうかは、構文から判断できます。AsyncOS では、*inactive* であるフィルタのフィルタ名に続くコロンが、感嘆符に変更されます。フィルタを入力またはインポートするときはこの構文を使用すると、AsyncOS はフィルタを *inactive* としてマークします。

たとえば、次のように無害な「filterstatus」という名前のフィルタを入力します。filter -> set サブコマンドを使用して、このフィルタを *inactive* にします。フィルタの詳細が表示され、コロンが感嘆符に変わっている点に注目してください（以下の例で、太字で示されています）。

```
mail3.example.com> filters
```

```
Choose the operation you want to perform:
```

```
- NEW - Create a new filter.
```

```
- IMPORT - Import a filter script from a file.
```

```
[> new
```

```
Enter filter script. Enter '.' on its own line to end.
```

```
filterstatus: if true(skip-filters());
```

```
.
```

```
1 filters added.
```

```
Choose the operation you want to perform:
```

```
- NEW - Create a new filter.
```

```
- DELETE - Remove a filter.
```

```
- IMPORT - Import a filter script from a file.
```

- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.

```
[> list
```

```
Num Active Valid Name
```

```
1 Y Y filterstatus
```

```
Choose the operation you want to perform:
```

- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.

```
[> set
```

```
Enter the filter name, number, or range:
```

```
[all]> all
```

```
Enter the attribute to set:
```

```
[active]> inactive
```

```
1 filters updated.
```

```
Choose the operation you want to perform:
```

- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.

```
[> detail
```

```
Enter the filter name, number, or range:
```

```
[> all
```

```
Num Active Valid Name
  1   N     Y  filterstatus
filterstatus! if (true) {
  skip-filters();
}
```

```
Choose the operation you want to perform:
```

```

- NEW - Create a new filter.

- DELETE - Remove a filter.

- IMPORT - Import a filter script from a file.

- EXPORT - Export filters to a file

- MOVE - Move a filter to a different position.

- SET - Set a filter attribute.

- LIST - List the filters.

- DETAIL - Get detailed information on the filters.

- LOGCONFIG - Configure log subscriptions used by filters.

- ROLLOVERNOW - Roll over a filter log file.

[]>

```

メッセージフィルタのアクティベーションまたはディアクティベーション

```
set [seqnum|filename|range] active|inactive
```

指定したフィルタを指定した状態に設定します。状態のルールは次のとおりです。

- **active** : 選択したフィルタの状態を **active** に設定します。
- **inactive** : 選択したフィルタの状態を **inactive** に設定します。

次の条件ではエラーが発生します。

- 指定した *filename* のフィルタが存在しない。
- 指定したシーケンス番号のフィルタが存在しない。



(注)

inactive であるフィルタは、構文からも判断できます。ラベル（フィルタ名）の後のコロンが、感嘆符 (!) に変更されます。CLI から手動で入力された、またはインポートされたフィルタにこの構文が含まれる場合、自動的に **inactive** とマークされます。たとえば、`mailfrompm!` が、`mailfrompm:` の代わりに表示されます。

メッセージフィルタのインポート

```
import filename
```

処理されるフィルタを含むファイルの名前です。このファイルは、アプライアンスの FTP/SCP ルートディレクトリの **configuration** ディレクトリ内に存在する必要があります (`interfaceconfig` コマンドを使用してインターフェイスの FTP/SCP アクセスをイネーブしている場合)。ファイルは取り込まれて解析され、エラーが存在すれば報告されます。現在のフィルタ セット内に存在するすべてのフィルタは、インポートされたフィルタに置き換わります。詳細については、[付録 A 「アプライアンスへのアクセス」](#) を参照してください。現在のフィルタ リストをエクスポートし ([「メッセージフィルタのエクスポート」 \(P.9-85\)](#) を参照)、そのファイルを編集してインポートすることを推奨します。

メッセージフィルタをインポートする場合、使用するエンコードを選択するよう求められます。

次の条件ではエラーが発生します。

- ファイルが存在しない。
- フィルタ名が一意ではない。
- フィルタに付けた *filename* が予約語である。
- フィルタに構文エラーが発生している。
- インターフェイスなど、存在しないシステム リソースを参照するアクションを実行するフィルタ。

メッセージフィルタのエクスポート

```
export filename [seqnum|filename|range]
```

既存のフィルタ セットを、アプライアンスの FTP/SCP ルート ディレクトリにある **configuration** ディレクトリ内のファイルに所定の形式で出力します。詳細については、[付録 A 「アプライアンスへのアクセス」](#) を参照してください。

メッセージフィルタをエクスポートする場合、使用するエンコードを選択するよう求められます。

次の条件ではエラーが発生します。

- 指定した名前のフィルタが存在しない。
- 指定したシーケンス番号のフィルタが存在しない。

非 ASCII 文字セットの表示

このシステムでは、CLI で非 ASCII 文字が UTF-8 で表示されます。お使いのターミナル/ディスプレイが UTF-8 をサポートしていない場合、フィルタが正常に表示されません。

フィルタ内の非 ASCII 文字を管理する最も良い方法は、フィルタをテキスト ファイルで編集してから、そのテキスト ファイルをアプライアンスにインポートすることです（[「メッセージフィルタのインポート」](#) (P.9-84) を参照）。

メッセージフィルタ リストの表示

```
list [seqnum|filename|range]
```

指定したフィルタの本文を出力せずに、概要を表形式で表示します。表示される情報は次のとおりです。

- フィルタ名
- フィルタ シーケンス番号
- フィルタの active/inactive 状態
- フィルタの valid/invalid 状態

次の条件ではエラーが発生します。

- 範囲の指定が不正です。

メッセージフィルタの詳細の表示

```
detail [seqnum|filtname|range]
```

フィルタの本文や追加の状態情報など、指定したフィルタの情報をすべて表示します。

フィルタ ログ サブスクリプションの設定

```
logconfig
```

サブメニューを入力し、`archive()` アクションによって生成されたメールボックス ファイルのフィルタ ログ オプションを設定できます。これらのオプションは、通常の `logconfig` コマンドで使用されるオプションとよく似ていますが、ログを参照するフィルタを追加または削除することによってのみ、ログを作成または削除できます。

各フィルタ ログ サブスクリプションには次のデフォルト値が設定されています。この値は、`logconfig` サブコマンドを使用して変更できます。

- 取得方法 : FTP Poll
- ファイル サイズ : 10MB
- ファイルの最大数 : 10

詳細については、「ロギング」の章を参照してください。

```
mail3.example.com> filters
```

```
Choose the operation you want to perform:
```

- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.

```
[> logconfig
```

```
Currently configured logs:
```

```
1. "joesmith" Type: "Filter Logs" Retrieval: FTP Poll
```

```
Choose the operation you want to perform:
```

```
- EDIT - Modify a log setting.
```

```
[> edit
```

```
Enter the number of the log you wish to edit.
```

```
[> 1
```

```
Choose the method to retrieve the logs.
```

```
1. FTP Poll
```

```
2. FTP Push
```

```
3. SCP Push
```

```
[1]> 1
```

```
Please enter the filename for the log:
```

```
[joesmith.mbox]>
```

```
Please enter the maximum file size:
```

```
[10485760]>
```

```
Please enter the maximum number of files:
```

```
[10]>
```

```
Currently configured logs:
```

```
1. "joesmith" Type: "Filter Logs" Retrieval: FTP Poll
```

```
Enter "EDIT" to modify or press Enter to go back.
```

```
[>
```

スキャンパラメータの変更

scanconfig コマンドは、スキャンでスキップするタイプなど、本文と添付ファイルのスキャン動作を制御します。



(注)

zip などの圧縮ファイルに含まれる MIME タイプをスキャンする場合、スキャンリストに「compressed」または「zip」または「application/zip」リストを含める必要があります。

scanconfig の使用

次の例では、scanconfig コマンドで次のパラメータを設定します。

- video/*、audio/*、image/* の MIME タイプは、コンテンツをスキャンされません。
- ネストされた（再帰的な）アーカイブ添付ファイルは、最大 10 レベルまでスキャンされます。（デフォルトは 5 レベル）。
- スキャンされる添付ファイルの最大サイズは、25 MB です。これより大きいファイルはすべてスキップされます（デフォルトは 5 MB）。
- 添付ファイルのメタデータ スキャンをイネーブルにします。スキャンエンジンが添付ファイルをスキャンするとき、メタデータを正規表現でスキャンします。これはデフォルトの設定です。
- 添付ファイルのスキャンのタイムアウトは、60 秒に設定されます。デフォルトは 30 秒です。
- スキャンされなかった添付ファイルは、検索パターンに一致しないと見なされます。（デフォルトの動作）。
- メッセージの application/(x-)pkcs7-mime（符号化署名）部分は、multipart/signed（クリア署名）に変換され、メッセージのコンテンツが処理されます。デフォルトでは、符号化署名されたメッセージは変換されません。



(注)

[assume the attachment matches the search pattern] を「Y」に設定すると、スキャンできないメッセージはメッセージフィルタルールによって true と評価されます。これにより、ディクショナリに一致しないメッセージの隔離など、予想外の動作が発生することがあります。このようなメッセージは、コンテンツが正しくスキャンできないという理由で隔離されていました。

```
mail3.example.com> scanconfig
```

```
There are currently 5 attachment type mappings configured to be SKIPPED.
```

```
Choose the operation you want to perform:
```

- NEW - Add a new entry.
- DELETE - Remove an entry.
- SETUP - Configure scanning behavior.
- IMPORT - Load mappings from a file.

- EXPORT - Save mappings to a file.
- PRINT - Display the list.
- CLEAR - Remove all entries.
- SMIME - Configure S/MIME unpacking.

[1]> **setup**

1. Scan only attachments with MIME types or fingerprints in the list.
2. Skip attachments with MIME types or fingerprints in the list.

Choose one:

[2]> **2**

Enter the maximum depth of attachment recursion to scan:

[5]> **10**

Enter the maximum size of attachment to scan:

[5242880]> **10m**

Do you want to scan attachment metadata? [Y]> **Y**

Enter the attachment scanning timeout (in seconds):

[30]> **60**

If a message has attachments that were not scanned for any reason (e.g. because of size, depth limits, or scanning timeout), assume the attachment matches the search pattern?
[N]>

If a message could not be deconstructed into its component parts in order to remove specified attachments, the system should:

1. Deliver
2. Bounce

3. Drop

[1]> 1

Configure encoding to use when none is specified for plain body text or anything with MIME type plain/text or plain/html.

1. US-ASCII
2. Unicode (UTF-8)
3. Unicode (UTF-16)
4. Western European/Latin-1 (ISO 8859-1)
5. Western European/Latin-1 (Windows CP1252)
6. Traditional Chinese (Big 5)
7. Simplified Chinese (GB 2312)
8. Simplified Chinese (HZ GB 2312)
9. Korean (ISO 2022-KR)
10. Korean (KS-C-5601/EUC-KR)
11. Japanese (Shift-JIS (X0123))
12. Japanese (ISO-2022-JP)
13. Japanese (EUC)

[1]>

Scan behavior changed.

There are currently 5 attachment type mappings configured to be SKIPPED.

Choose the operation you want to perform:

- NEW - Add a new entry.
- DELETE - Remove an entry.
- SETUP - Configure scanning behavior.
- IMPORT - Load mappings from a file.

- EXPORT - Save mappings to a file.
- PRINT - Display the list.
- CLEAR - Remove all entries.
- SMIME - Configure S/MIME unpacking.

[> **SMIME**

Do you want to convert opaque-signed messages to clear-signed? This will provide the clear text content for various blades to process. [N]> Y

There are currently 5 attachment type mappings configured to be SKIPPED.

Choose the operation you want to perform:

- NEW - Add a new entry.
- DELETE - Remove an entry.
- SETUP - Configure scanning behavior.
- IMPORT - Load mappings from a file.
- EXPORT - Save mappings to a file.
- PRINT - Display the list.
- CLEAR - Remove all entries.
- SMIME - Configure S/MIME unpacking.

[> **print**

1. Fingerprint Image
2. Fingerprint Media
3. MIME Type audio/*
4. MIME Type image/*
5. MIME Type video/*

```
There are currently 5 attachment type mappings configured to be SKIPPED.
```

```
Choose the operation you want to perform:
```

- NEW - Add a new entry.
- DELETE - Remove an entry.
- SETUP - Configure scanning behavior.
- IMPORT - Load mappings from a file.
- EXPORT - Save mappings to a file.
- PRINT - Display the list.
- CLEAR - Remove all entries.
- SMIME - Configure S/MIME unpacking.

```
[ ]>
```

メッセージのエンコードの変更

localeconfig コマンドを使用して、メッセージ処理中のメッセージのヘッダーおよびフッターのエンコードの変更に関する AsyncOS の動作を設定できます。

```
example.com> localeconfig
```

```
Behavior when modifying headers: Use encoding of message body
```

```
Behavior for untagged non-ASCII headers: Impose encoding of message body
```

```
Behavior for mismatched footer or heading encoding: Only try encoding from  
message body
```

```
Choose the operation you want to perform:
```

- SETUP - Configure multi-lingual settings.

```
[ ]> setup
```

```
If a header is modified, encode the new header in the same encoding as
```

the message body? (Some MUAs incorrectly handle headers encoded in a different encoding than the body. However, encoding a modified header in the same encoding as the message body may cause certain characters in the modified header to be lost.) [Y]>

If a non-ASCII header is not properly tagged with a character set and is being used or modified, impose the encoding of the body on the header during processing and final representation of the message?

(Many MUAs create non-RFC-compliant headers that are then handled in an undefined way. Some MUAs handle headers encoded in character sets

that differ from that of the main body in an incorrect way. Imposing the encoding of the body on the header may encode

the header more precisely. This will be used to interpret the content of headers for processing, it will not modify or rewrite the header

unless that is done explicitly as part of the processing.) [Y]>

Footers or headings are added in-line with the message body whenever possible. However, if the footer or heading is encoded differently than the message body, and if imposing a single encoding will cause loss of characters, it will be added as an attachment. The system will always try to use the message body's encoding for the footer or heading. If that fails, and if the message body's encoding is US-ASCII, the system can try to edit the message body to use the footer's or heading's encoding. Should the system try to impose the footer's or headings's encoding on the message body? [N]> **y**

Behavior when modifying headers: Use encoding of message body

Behavior for untagged non-ASCII headers: Impose encoding of message body. Behavior for mismatched footer or heading encoding: Try both

body and footer or heading encodings

```
Choose the operation you want to perform:
```

```
- SETUP - Configure multi-lingual settings.
```

最初のプロンプトは、ヘッダーが（たとえばフィルタによって）変更されていた場合、メッセージヘッダーのエンコードをメッセージ本文に一致するように変更するかどうかを指定します。

2番目のプロンプトは、ヘッダーの文字セットが適切にタグで指定されていない場合、ヘッダーに対してメッセージ本文のエンコードを強制する必要があるかどうかを制御します。

3番目のプロンプトは、免責事項のスタンプ（および複数のエンコード）がメッセージ本文でどのように機能するかを制御するために使用されます。詳細については、「テキストリソース」の章の「免責事項スタンプと複数エンコード方式」を参照してください。

サンプルメッセージフィルタの作成

次の例では、`filter` コマンドを使用して新しいフィルタを3つ作成します。

- 最初のフィルタの名前は、**big_messages** です。これは `body-size` ルールを使用して、10 MB より大きいメッセージをドロップします。
- 2番目のフィルタの名前は、**no_mp3s** です。これは `attachment-filename` ルールを使用して、`.mp3` ファイル拡張子が付いた添付ファイルを含むメッセージをドロップします。
- 3番目のフィルタの名前は、**mailfrompm** です。これは `mail-from` ルールを使用して、`postmaster@example.com` からのメールをすべて調べ、`administrator@example.com` のブラインドカーボンコピーを作成します。

`filter -> list` サブコマンドを使用し、フィルタのリストを表示して、フィルタがアクティブで有効であることを確認します。次に、`move` サブコマンドを使用して、最初と最後のフィルタの位置を入れ替えます。最後に、変更を確定してフィルタを有効にします。

```
mail3.example.com> filters
```

```
Choose the operation you want to perform:
```

```
- NEW - Create a new filter.
```

```
- IMPORT - Import a filter script from a file.
```

```
[> new
```

```
Enter filter script. Enter '.' on its own line to end.
```

```
big_messages:
```

```
    if (body-size >= 10M) {
```

```
        drop();
    }
.
1 filters added.

Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.

[ ]> new

Enter filter script. Enter '.' on its own line to end.

no_mp3s:
    if (attachment-filename == '(?i)\\.mp3$') {
        drop();
    }
.
1 filters added.

Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
```

- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.

```
[> new
```

Enter filter script. Enter '.' on its own line to end.

```
mailfrompm:
```

```
    if (mail-from == "^postmaster$")
        { bcc ("administrator@example.com");}
```

```
.
```

```
1 filters added.
```

Choose the operation you want to perform:

- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.

```
[> list
```



```
Num Active Valid Name
  1   Y      Y   big_messages
  2   Y      Y   no_mp3s
  3   Y      Y   mailfrompm
```

Choose the operation you want to perform:

- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.

```
[> move
```

Enter the filter name, number, or range to move:

```
[> 1
```

Enter the target filter position number or name:

```
[> last
```

```
1 filters moved.
```

Choose the operation you want to perform:

- NEW - Create a new filter.

- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.

```
[> list
```

```
Num Active Valid Name
```

```
1 Y Y no_mp3s
2 Y Y mailfrompm
3 Y Y big_messages
```

```
Choose the operation you want to perform:
```

- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.

```
[> move
```

```
Enter the filter name, number, or range to move:
```

```
[ ]> 2
```

```
Enter the target filter position number or name:
```

```
[ ]> 1
```

```
1 filters moved.
```

```
Choose the operation you want to perform:
```

- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.

```
[ ]> list
```

```
Num Active Valid Name
  1   Y      Y  mailfrompm
  2   Y      Y  no_mp3s
  3   Y      Y  big_messages
```

```
Choose the operation you want to perform:
```

- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.

```

- EXPORT - Export filters to a file

- MOVE - Move a filter to a different position.

- SET - Set a filter attribute.

- LIST - List the filters.

- DETAIL - Get detailed information on the filters.

- LOGCONFIG - Configure log subscriptions used by filters.

- ROLLOVERNOW - Roll over a filter log file.

[]>

```

```
mail3.example.com> commit
```

```
Please enter some comments describing your changes:
```

```
[]> entered and enabled 3 filters: no_mp3s, mailfrompm, big_messages
```

メッセージフィルタの例

この項では、実際のフィルタの例を示し、各フィルタについて簡単に説明します。

オープンリレー防止フィルタ

このフィルタは、次のように、%、余分な @、および ! 文字が電子メールアドレスに含まれるメッセージをバウンスします。

- user%otherdomain@validdomain
- user@otherdomain@validdomain:
- domain!user@validdomain

```
sourceRouted:
```

```
if (rcpt-to == "(%|@|!)(.*)@") {

    bounce();

}
```

Cisco アプライアンスは、従来の Sendmail/Qmail システムを活用するためによく使用される、このようなサードパーティ製のリレーハックの影響を受けません。これらの記号の多く（% など）は正当な電子メールアドレスの一部である可能性があるため、Cisco アプライアンスはこれらを有効なアドレスとして受け入れ、設定済みの受信者リストと照合し、次の内部サーバに渡します。Cisco アプライアンスは、これらのメッセージを外部にリレーしません。

このようなフィルタは、このタイプのメッセージをリレーできるように誤って設定されたオープンソース MTA を使用しているユーザを保護するために所定の場所に設定されます。



(注) このようなタイプのアドレスを処理するように、リスナーを設定することもできます。詳細については、「[GUI からのリスナーの作成による接続要求のリッスン](#)」(P.5-8) を参照してください。

ポリシー強制フィルタ

件名に基づき通知するフィルタ

このフィルタは、件名に特定の用語が含まれているかどうかに基づいて通知を送信します。

```
search_for_sensitive_content:

if (Subject == "(?i)plaintiff|lawsuit|judge" ) {

    notify ("admin@company.com");

}
```

競合他社に送信されたメールの BCC およびスキャン

このフィルタは、競合他社に送信されたメッセージをスキャンし、ブラインドコピーを作成します。ディクショナリと `header-dictionary-match()` ルールを使用して、柔軟性の高い競合他社のリストを指定できます（「[辞書ルール](#)」(P.9-34) を参照）。

```
competitorFilter:

if (rcpt-to == '@competitor1.com|@competitor2.com') {

    bcc-scan('legal@example.com');

}
```

特定のユーザをブロックするフィルタ

このフィルタを使用すると、特定のアドレスからの電子メールをブロックします。

```
block_harrasing_user:

if (mail-from == "ex-employee@hotmail\\.com") {

    notify ("admin@company.com");

}
```

```

    drop ();
}

```

メッセージのアーカイブおよびドロップ フィルタ

ファイルタイプが一致するメッセージのみをログ記録およびドロップします。

```

drop_attachments:

if (mail-from != "user@example.com") AND (attachment-filename ==

'(?i)\.(asp|bas|bat|cmd|cpl|exe|hta|ins|isp|js)$')

{

    archive("Drop_Attachments");

    insert-header("X-Filter", "Dropped by: $FilterName MID: $MID");
    drop-attachments-by-name("\.(asp|bas|bat|cmd|cpl|exe|hta|ins|isp|js)$");

}

```

大きい「To:」ヘッダーのフィルタ

「To」ヘッダーが非常に大きいメッセージを検索します。

archive() 行を使用して適切なアクションを検証し、drop() をイネーブルまたはディセーブルにして安全性を高めます。

```

toTooBig:

if(header('To') == "^.{500,}") {

    archive('tooTooBigdropped');

    drop();

}

```

空白の「From:」フィルタ

空白の「From」ヘッダーを特定します。

このフィルタは、「from」アドレスが空白であるさまざまな形式に対応できます。

```

blank_mail_from_stop:

if (recv-listener == "InboundMail" AND header("From") == "^$|<\s*>") {

    drop ();

}

```

また、Envelope From が空欄のメッセージをドロップする場合は、次のフィルタを使用します。

```
blank_mail_from_stop:

if (recv-listener == "InboundMail" AND (mail-from == "^$|<\\s*>" OR header ("From") ==
"^$|<\\s*>"))

{

    drop ();

}
```

SRBS フィルタ

SenderBase レピュテーション フィルタ:

```
note_bad_reps:

if (reputation < -2) {

    strip-header ('Subject');

    insert-header ('Subject', '***BadRep $Reputation *** $Subject');

}
```

SRBS フィルタの変更

特定のドメインの SenderBase Reputation Score (SBRs; SenderBase レピュテーション スコア) しきい値を変更します。

```
mod_sbrs:

if ( (rcpt-count == 1) AND (rcpt-to == "@domain\\.com$") AND (reputation < -2) ) {

    drop ();

}
```

ファイル名の正規表現フィルタ

このフィルタは、メッセージ本文のサイズの範囲を指定し、正規表現に一致する添付ファイルを検索します (このパターンに一致するファイル名は、「readme.zip」、「readme.exe」、「attach.exe」、など)。

```
filename_filter:

if ((body-size >= 9k) AND (body-size <= 20k)) {

    if (body-contains "(?i)(readme|attach|information)\\. (zip|exe)$") {

        drop ();

    }

}
```

```

    }
}

```

ヘッダー内の SenderBase レピュテーション スコアの表示フィルタ

ヘッダーのログが記録されるので、メール ログで表示できます（「ロギング」の章を参照）。

```

Check_SBRs:

if (true) {

    insert-header('X-SBRs', '$Reputation');

}

```

ポリシーのヘッダーへの挿入フィルタ

どのメールフローポリシーが接続を受け入れたかを示します。

```

Policy_Tracker:

if (true) {

    insert-header ('X-HAT', 'Sender Group $Group, Policy $Policy applied.');
```

多数の受信者のバウンス フィルタ

3 つ以上の固有ドメインから 50 人を超える受信者が指定されている発信メールメッセージをすべてバウンスします。

```

bounce_high_rcpt_count:

if ( (rcpt-count > 49) AND (rcpt-to != "@example\\.com$") ) {

    bounce-profile ("too_many_rcpt_bounce"); bounce ();

}

```


ルーティングおよびドメインスプーフィング

仮想ゲートウェイフィルタの使用

仮想ゲートウェイを使用してトラフィックを区分します。システムに2つのインターフェイス「public1」と「public2」が存在するとします。デフォルトの配信インターフェイスは「public1」です。これにより、発信トラフィックはすべて2番目のインターフェイスを介すように強制されます。バウンスおよびその他同様のタイプのメールはフィルタを通過しないため、そのようなメールは public1 から配信されます。

```
virtual_gateways:

if (recv-listener == "OutboundMail") {

    alt-src-host ("public2");

}
```

配信とリスナーのフィルタに対する同じリスナーの使用

配信と受信に同じリスナーを使用します。このフィルタでは、パブリックリスナー「listener1」で受信したメッセージを、インターフェイス「listener1」から送信できます（設定したパブリックインジェクタごとに、固有のフィルタをセットアップする必要があります）。

```
same_listener:

if (recv-inj == 'listener1') {

    alt-src-host('listener1');

}
```

単一のリスナーのフィルタ

単一のリスナーでフィルタを機能させます。たとえば、システム全体で実行するのではなく、メッセージフィルタを処理する専用のリスナーを指定します。

```
textfilter-new:

if (recv-inj == 'inbound' and body-contains("some spammy message")) {

    alt-rcpt-to ("spam.quarantine@spam.example.com");

}
```

スプーフィングドメインのドロップフィルタ（単一のリスナー）

スプーフィングドメイン（内部のアドレスからであると偽り、単一のリスナーで機能する）が使用されている電子メールをドロップします。以下のIPアドレスは、架空のドメイン（mycompany.com）を表しています。

```
DomainSpoofered:

if (mail-from == "mycompany\\.com$") {

    if ((remote-ip != "1.2.") AND (remote-ip != "3.4. ")) {

        drop();

    }

}
```

スプーフィングドメインのドロップフィルタ（複数のリスナー）

前述と同じですが、複数のリスナーを使用して動作します。

```
domain_spoof:

if ((recv-listener == "Inbound") and (mail-from == "@mycompany\\.com")) {

archive('domain_spoof');

drop ();

}
```

別のスプーフィングドメインのドロップフィルタ

概要：ドメインスプーフィング対策フィルタ：

```
reject_domain_spoof:

if (recv-listener == "MailListener") {

    insert-header("X-Group", "$Group");

    if ((mail-from == "@test\\.mycompany\\.com") AND (header("X-Group") != "RELAYLIST")) {

        notify("me@here.com");

        drop();

        strip-header("X-Group");

    }

}
```

ルーピングの検出フィルタ

このフィルタを使用して、メールループを発生させている要因を検出、停止、および判断します。このフィルタは、Exchange サーバまたはそれ以外の場所で発生している構成の問題を判断するために役立ちます。

```
External_Loop_Count:

if (header("X-ExtLoop1")) {

    if (header("X-ExtLoopCount2")) {

        if (header("X-ExtLoopCount3")) {

            if (header("X-ExtLoopCount4")) {

                if (header("X-ExtLoopCount5")) {

                    if (header("X-ExtLoopCount6")) {

                        if (header("X-ExtLoopCount7")) {

                            if (header("X-ExtLoopCount8")) {

                                if (header("X-ExtLoopCount9")) {

                                    notify ('joe@example.com');

                                    drop();

                                }

                                else {insert-header("X-ExtLoopCount9", "from
                                    $RemoteIP");}}

                                else {insert-header("X-ExtLoopCount8", "from $RemoteIP");}}

                                else {insert-header("X-ExtLoopCount7", "from $RemoteIP");}}

                                else {insert-header("X-ExtLoopCount6", "from $RemoteIP");}}

                                else {insert-header("X-ExtLoopCount5", "from $RemoteIP");}}

                                else {insert-header("X-ExtLoopCount4", "from $RemoteIP");}}

                                else {insert-header("X-ExtLoopCount3", "from $RemoteIP");}}

                            else {insert-header("X-ExtLoopCount2", "from $RemoteIP");}}

                        else {insert-header("X-ExtLoop1", "1"); }

                    }

                }

            }

        }

    }

}
```



(注) デフォルトでは、AsyncOS は自動的にメールのループを検出し、100 回ループしたメッセージをドロップします。



CHAPTER 10

メール ポリシー

- 「メール ポリシーの概要」 (P.10-1)
- 「メール ポリシーをユーザ単位で適用する方法」 (P.10-2)
- 「着信処理および発信メッセージの異なる処理」 (P.10-2)
- 「メール ポリシーへのユーザの一致」 (P.10-3)
- 「メッセージ分裂」 (P.10-5)
- 「メール ポリシーの設定」 (P.10-6)

メール ポリシーの概要

電子メール セキュリティ アプライアンスはメール ポリシーを使用して、組織とユーザとの間で送信されるメッセージについての組織のポリシーを適用します。これらは、組織が社内のネットワークに入ったり出たりして欲しくない、疑わしい、機密な、または悪意のあるコンテンツのタイプを指定する一連のルールです。このコンテンツは次のようなものがあります。

- スпам
- 問題のないマーケティング メッセージ
- ウイルス
- フィッシングおよび他のメール攻撃のターゲット
- 機密企業データ
- 個人情報

組織内の異なるユーザ グループの個別のセキュリティ ニーズを満たすために複数のポリシーを作成できます。電子メール セキュリティ アプライアンスはこれらのポリシーに定義されているルールを使用して各メッセージをスキャンし、必要に応じて、ユーザを保護するアクションを実行します。たとえば、ポリシーは、スパムの疑いのあるメッセージが幹部に配信されないようにするとともに、そのコンテンツについて警告する件名に変更して IT スタッフへの配信を許可することができます。システム管理者グループ以外のすべてのユーザで、危険な実行可能プログラムの添付ファイルをドロップします。

メール ポリシーをユーザ単位で適用する方法

	操作内容	詳細
ステップ 1	電子メール セキュリティ アプライアンスが着信または発信メッセージに使用するコンテンツ スキャン機能をイネーブルにします。	この機能で、次の 1 つ以上をイネーブル化し、設定できます。 <ul style="list-style-type: none"> 「アンチウイルス」 「アンチスパム」 「アウトブレイク フィルタ」 「データ消失防止」(発信メッセージのみ) 「コンテンツ フィルタ」
ステップ 2	(任意) 特定のデータを含むメッセージに対して実行するアクションの場合にコンテンツ フィルタを作成します。	第 11 章「コンテンツ フィルタ」を参照してください。
ステップ 3	(任意) メール ポリシーのルールが適用されるユーザを指定する LDAP グループ クエリーを定義します。	「受信者がグループ メンバーであるかどうかを指定するグループ LDAP クエリーの使用」(P.22-23)を参照してください。
ステップ 4	(任意) 着信または発信メッセージのデフォルトのメール ポリシーを定義します。	「着信または発信メッセージのデフォルトのメールポリシーの設定」(P.10-7)を参照してください。
ステップ 5	ユーザ特定のメール ポリシーを設定するユーザ グループを定義します。	着信または発信メール ポリシーを作成します。 詳細については、「メール ポリシーの設定」(P.10-6)を参照してください。
ステップ 6	コンテンツ セキュリティ機能とアプライアンスがメッセージに対して実行するコンテンツ フィルタ アクションを設定します。	メール ポリシーの異なるコンテンツのセキュリティ機能を設定します。 <ul style="list-style-type: none"> コンテンツ フィルタ (Content Filters) : 「特定のユーザ グループに対するメッセージへのコンテンツ フィルタの適用」(P.11-20) 「ユーザのウイルス スキャン アクションの設定」(P.12-7) ウイルス対策 (Anti-Virus) : スパム対策 (Anti-Spam) : 「スパム対策ポリシーの定義」(P.13-8) アウトブレイク フィルタ (Outbreak Filters) : 「アウトブレイク フィルタ機能とメール ポリシー」(P.14-14) データ消失防止 (Data Loss Prevention) : 「発信メール ポリシーを使用した送信者および受信者への DLP ポリシーの割り当て」(P.15-22) および 「Enterprise Manager 導入の DLP ポリシーに発信メール ポリシーを関連付ける方法について」(P.15-30)。

着信処理および発信メッセージの異なる処理

電子メールセキュリティ アプライアンスはメッセージコンテンツセキュリティに 2 つの異なるメールポリシーのセットを使用します。

- メッセージの着信メッセージポリシーは、リスナーの ACCEPT HAT ポリシーに一致する接続から受信したメッセージです。
- メッセージの発信メッセージポリシーは、リスナーの RELAY HAT ポリシーに一致する接続からのメッセージです。この接続には、SMTP AUTH で認証された任意の接続が含まれます。

異なるポリシーのセットを持つことで、ユーザに送信またはユーザから送信されたメッセージに対し異なるセキュリティルールを定義することができます。GUI の [メール ポリシー (Mail Policies)] > [着信メール ポリシー (Incoming Mail Policies)] または [発信メール ポリシー (Outgoing Mail Policies)] ページを使用、または CLI の `policyconfig` コマンドを使用して、これらのポリシーを管理します。



(注) データ消失防止スキャンは、発信メッセージにだけしか実行できません。



(注) 特定のインストールでは、Cisco アプライアンスを経由する「内部」メールは、すべての受信者が内部アドレスにアドレス指定されている場合でも、発信と見なされます。たとえばシステムセットアップウィザードは、Cisco C160/170 カスタマーのデフォルトで、着信電子メールの受信および発信電子メールのリレー用に、1つのリスナーに物理イーサネットポートを1つだけ設定します。

メール ポリシーへのユーザの一致

メッセージがアプライアンスによって受信されると同時に、電子メールセキュリティアプライアンスは、メッセージが着信か発信かによって、各メッセージ受信者と送信者を着信または発信メッセージポリシー テーブルのメール ポリシーに一致させようとします。

マッチングは、受信者のアドレスまたは送信者のアドレスのいずれかに基づいて行われます。

- 受信者アドレスは、エンベロープ受信者アドレスと一致します。

受信者アドレスが一致すると、入力された受信者アドレスは、電子メールパイプラインの先行部分による処理後の最終アドレスです。たとえば、イーサブルの場合、デフォルトドメイン、LDAP ルーティングまたはマスカレード、エイリアステーブル、ドメインマップ、メッセージフィルタ機能はエンベロープ受信者アドレスを書き換えることができ、メッセージがメールポリシーに一致するかどうかに影響することがあります。

- 送信者アドレスは、次のアドレスに一致します。
 - エンベロープ送信者 (RFC821 MAIL FROM アドレス)
 - RFC822 From: ヘッダーのアドレス
 - RFC822 Reply-To: ヘッダーのアドレス

アドレス マッチングは、完全な電子メールアドレス、ユーザ、ドメインまたは部分的なドメインのいずれか、あるいは LDAP グループメンバーシップで行われます。

最初に一致したものの勝ち

各ユーザは（送信者または受信者）トップダウン方式の適切なメールポリシー テーブルで定義したメールポリシーごとに評価されます。

ユーザごとに、最初に一致したポリシーが適用されます。ユーザが特定のポリシーと一致しない場合、ユーザは自動的にテーブルのデフォルトポリシーと一致します。

送信者アドレスに基づいて一致する場合、メッセージの残りのすべての受信者がそのポリシーに一致します。(これは、メッセージごとに存在する送信者が 1 人だけのためです)。

ポリシー マッチングの例

次の例では、ポリシー テーブルがどのように上から順にマッチングされるかを説明します。

次の表 10-1 に示す着信メールの電子メール セキュリティ ポリシーの表では、着信メッセージはさまざまなポリシーとマッチングされます。

表 10-1 ポリシー マッチングの例

順番	ポリシー名	ユーザ
1	special_people	受信者: joe@example.com 受信者: ann@example.com
2	from_lawyers	送信者: @lawfirm.com
3	acquired_domains	受信者: @newdomain.com 受信者: @anotherexample.com
4	engineering	受信者: PublicLDAP.ldapgroup: engineers
5	sales_team	受信者: jim@ 受信者: john@ 受信者: larry@
	デフォルト ポリシー	(全ユーザ)

例 1

送信者 bill@lawfirm.com から受信者 jim@example.com に送信されるメッセージはポリシー #2 と一致します。これは、送信者 (@lawfirm.com) と一致するユーザの説明が受信者 (jim@) と一致するユーザ説明よりテーブル内で先に来るからです。

例 2

送信者 joe@yahoo.com は、3 人の受信者、john@example.com、jane@newdomain.com および bill@example.com に着信メッセージを送信します。

- 受信者 jane@newdomain.com へのメッセージは、ポリシー #3 で定義されたスパム対策、ウイルス対策、アウトブレイク フィルタおよびコンテンツ フィルタを受信します。
- 受信者 john@example.com へのメッセージはポリシー #5 で定義されている設定を受信します。
- 受信者 bill@example.com はエンジニアリング LDAP クエリーに一致しないため、メッセージはデフォルト ポリシーで定義された設定を受け取ります。

次の例では、受信者が複数あるメッセージでメッセージ分裂がどのように発生するかについて示します。詳細については、「[メッセージ分裂](#)」(P.10-5) を参照してください。

例 3

送信者 bill@lawfirm.com は、受信者 ann@example.com および larry@example.com にメッセージを送信します。

- 受信者 `ann@example.com` は、ポリシー #1 で定義されているスパム対策、ウイルス対策、アウトブレイク フィルタおよびコンテンツ フィルタを受信します。
- 受信者 `larry@example.com` は、ポリシー #2 で定義されているスパム対策、ウイルス対策、アウトブレイク フィルタおよびコンテンツ フィルタを受信します。これは、表内で、送信者 (`@lawfirm.com`) が、受信者 (`jim@`) と一致するユーザ説明よりも前に示されているためです。

メッセージ分裂

インテリジェントなメッセージ分裂は、受信者に基づいたコンテンツの異なるセキュリティ ルールを複数の受信者に対するメッセージに個別に適用できるメカニズムです。





各受信者は、該当するメール ポリシー テーブル（着信または発信）の各ポリシーに対して上から順に評価されます。

メッセージに一致する各ポリシーは、これらの受信者に新しいメッセージを作成します。このプロセスが、「メッセージ分裂」と定義されます。

- 一部の受信者が異なるポリシーと一致する場合、受信者は一致したポリシーに基づいてグループ化され、メッセージは一致したポリシー数と同数のメッセージに分裂されます。これらの受信者は、それぞれ適切な「分裂先」に設定されます。
- すべての受信者が同じポリシーと一致する場合、メッセージは分裂されません。反対に、最も多くの分裂が行われるのは、単一のメッセージがメッセージ受信者 1 人 1 人に分裂される場合です。
- 各メッセージ分裂は、スパム対策、ウイルス対策、DLP スキャン（発信メッセージのみ）、アウトブレイク フィルタおよびコンテンツ フィルタにより電子メール パイプラインで個別に処理されます。

表 10-2 に、電子メール パイプラインでメッセージが分裂されるポイントを示します。

表 10-2 電子メール パイプラインでのメッセージ分裂

ワークキュー	メッセージ フィルタ (filters)	電子メールセキュリティ マネージャ ポリシー (受信者 1 人あたり)	↓  すべての受信者のメッセージ
	スパム対策 (antispamconfig、antispamupdate)		メッセージは、メッセージ フィルタ処理直後の、スパム対策処理前に分裂されます。
	ウイルス対策 (antivirusconfig、antivirusupdate)		 すべての受信者のメッセージ ポリシー 1 と一致
	コンテンツ フィルタ (policyconfig -> filters)		 すべての受信者のメッセージ ポリシー 2 と一致
	アウトブレイク フィルタ (outbreakconfig、outbreakflush、outbreakstatus、outbreakupdate)		 その他のすべての受信者のメッセージ (デフォルト ポリシーと一致)
	データ消失防止 (policyconfig)		(注) DLP スキャンは、発信メッセージだけに実行されます。



(注)

新しい MID (メッセージ ID) が、各メッセージ分裂用に作成されます (たとえば、MID 1 は、MID 2 および MID 3 になります)。詳細については、『Cisco IronPort AsyncOS for Email Daily Management Guide』の「Logging」の章を参照してください。また、トレース機能は、メッセージを分裂したポリシーを示します。

電子メール セキュリティ マネージャ ポリシーのポリシー マッチングおよびメッセージ分裂は、アプライアンスで使用できるメッセージ処理の管理に影響を与えます。

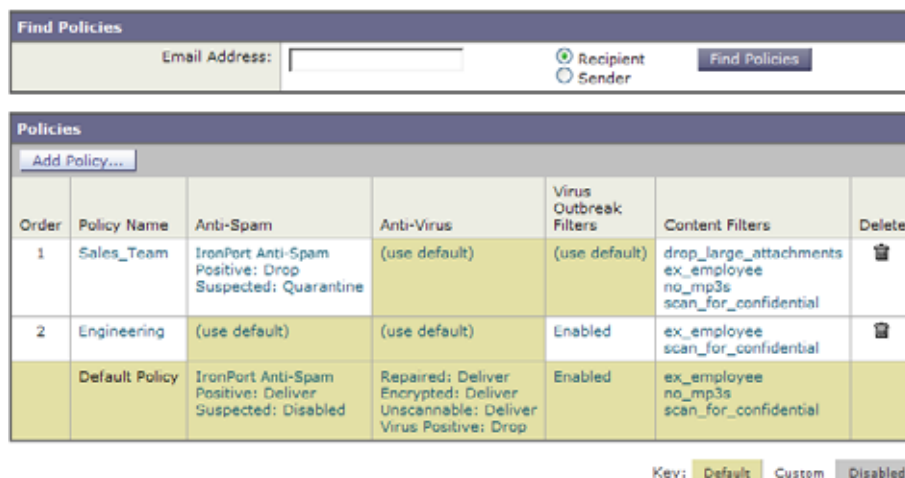
管理例外

各分裂メッセージの反復処理はパフォーマンスに影響するため、シスコは**管理例外**単位で十分なコンテンツ セキュリティ ルールを設定することを推奨します。つまり、組織のニーズを評価し、大多数のメッセージがデフォルト ポリシーで処理され、少数のメッセージが、追加の「例外」ポリシーで処理されるように機能を設定します。このようにすることで、メッセージ分裂が最小化され、ワークキューの各分裂メッセージの処理により受けるシステム パフォーマンスの影響が少なくなります。

メール ポリシーの設定

図 10-1 は、電子メール セキュリティ アプライアンスが異なるユーザ グループを、特定のスパム対策、ウイルス対策、アウトブレイク フィルタ、DLP およびコンテンツ フィルタ セキュリティ設定にどのようにマッピングするかを示します。

図 10-1 GUI の電子メール セキュリティ マネージャ ポリシーの概要
Incoming Mail Policies



Order	Policy Name	Anti-Spam	Anti-Virus	Virus Outbreak Filters	Content Filters	Delete
1	Sales_Team	IronPort Anti-Spam Positive: Drop Suspected: Quarantine	(use default)	(use default)	drop_large_attachments ex_employee no_mp3s scan_for_confidential	
2	Engineering	(use default)	(use default)	Enabled	ex_employee scan_for_confidential	
	Default Policy	IronPort Anti-Spam Positive: Deliver Suspected: Disabled	Repaired: Deliver Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	Enabled	ex_employee no_mp3s scan_for_confidential	

Key: Default Custom Disabled

着信または発信メッセージのデフォルトのメールポリシーの設定

デフォルトのメール ポリシーは他のメール ポリシーに該当しないメッセージに適用されます。他のポリシーが設定されていない場合、デフォルト ポリシーはすべてのメッセージに適用されます。

はじめる前に

個々のセキュリティ サービスをメール ポリシーに定義する方法を理解します。

- コンテンツ フィルタ (Content Filters) : 「特定のユーザ グループに対するメッセージへのコンテンツ フィルタの適用」 (P.11-20)
- 「ユーザのウイルス スキャン アクションの設定」 (P.12-7) ウイルス対策 (Anti-Virus) :
- スпам対策 (Anti-Spam) : 「スパム対策ポリシーの定義」 (P.13-8)
- アウトブレイク フィルタ (Outbreak Filters) : 「アウトブレイク フィルタ機能とメール ポリシー」 (P.14-14)
- データ消失防止 (Data Loss Prevention) : 「デフォルトの発信メール ポリシーとの DLP ポリシーの関連付け」 (P.15-22) および 「Enterprise Manager 導入の DLP ポリシーに発信メール ポリシーを関連付ける方法について」 (P.15-30)。

手順

- ステップ 1** [メール ポリシー (Mail Policies)] > [着信メール ポリシー (Incoming Mail Policies)]
または
[メール ポリシー (Mail Policies)] > [送信メール ポリシー (Outgoing Mail Policies)] を選択します。
- ステップ 2** デフォルトのメール ポリシーに設定するセキュリティ サービスのリンクをクリックします。
次のコンテンツ セキュリティ サービスのタイプを使用できます。
- コンテンツ フィルタ (Content Filters)
 - スпам対策 (Anti-Spam)

- ウイルス対策 (Anti-Virus)
- データ消失防止 (Data Loss Prevention) (発信メールポリシーのみ)
- アウトブレイク フィルタ (Outbreak Filters)



(注) デフォルトのセキュリティ サービス設定の場合、このページの最初の設定では、ポリシーでサービスがイネーブルになるかどうかを定義します。[無効 (Disable)] をクリックして、サービスをディセーブルにできます。

- ステップ 3** セキュリティ サービスの設定値を設定します。
- ステップ 4** [送信 (Submit)] をクリックします。
- ステップ 5** 変更内容を送信し、確定します。

送信者および受信者のグループのメールポリシーの作成

はじめる前に

- 個々のセキュリティ サービスをメールポリシーに定義する方法を理解します。
 - コンテンツ フィルタ (Content Filters) : 「特定のユーザグループに対するメッセージへのコンテンツフィルタの適用」 (P.11-20)
 - 「ユーザのウイルス スキャンアクションの設定」 (P.12-7) ウイルス対策 (Anti-Virus) :
 - スпам対策 (Anti-Spam) : 「スパム対策ポリシーの定義」 (P.13-8)
 - アウトブレイク フィルタ (Outbreak Filters) : 「アウトブレイク フィルタ機能とメールポリシー」 (P.14-14)
 - データ消失防止 (Data Loss Prevention) : 「発信メールポリシーを使用した送信者および受信者への DLP ポリシーの割り当て」 (P.15-22) および 「Enterprise Manager 導入の DLP ポリシーに発信メールポリシーを関連付ける方法について」 (P.15-30)。
- 各受信者は、適切なテーブル (着信または発信) の各ポリシーに対して上から順に評価されます。詳細については、「最初に一致したものの勝ち」 (P.10-3) を参照してください。
- (任意) メールポリシーの管理を担当する委任管理者を定義します。委任管理者は、ポリシーのアンチスパム、アンチウイルス、アウトブレイク フィルタの設定を編集し、ポリシーのコンテンツ フィルタを有効化または無効化できます。オペレータおよび管理者のみがメールポリシーの名前または送信者、受信者、またはグループを変更できます。メールポリシーへのフルアクセス権があるカスタム ユーザ ロールはメールポリシーに自動的に割り当てられます。

手順

- ステップ 1** [メールポリシー (Mail Policies)] > [着信メールポリシー (Incoming Mail Policies)] または [メールポリシー (Mail Policies)] > [送信メールポリシー (Outgoing Mail Policies)] を選択します。
- ステップ 2** [ポリシーを追加 (Add Policy)] ボタンをクリックして、新しいポリシーの作成を開始します。
- ステップ 3** メールポリシーの名前と説明を入力します。

ステップ 4 (任意) [編集可能なユーザ (役割) (Editable by (Roles))] のリンクをクリックし、メールポリシーの管理を担当する委任管理者のカスタム ユーザ役割を選択します。

ステップ 5 ポリシーのユーザを定義します。

ポリシーを適用するユーザが送信者なのか、受信者なのかを次の方法で定義します。

- 完全な電子メールアドレス (Full email address) : user@example.com
- 電子メールアドレスの一部 (Partial email address) : user@
- ドメインのすべてのユーザ (All users in a domain) : @example.com
- 部分ドメインのすべてのユーザ (All users in a partial domain) : @.example.com
- LDAP クエリーとのマッチング (By matching an LDAP Query)



(注) ユーザの入力は、AsyncOS の GUI および CLI の両方で、大文字と小文字が区別されます。たとえば、ユーザの受信者 Joe@ を入力すると、joe@example.com に送信されるメッセージが一致します。

ステップ 6 [追加 (Add)] ボタンをクリックして、[現在のユーザ (Current Users)] リストにユーザを追加します。

ポリシーには、送信者、受信者および LDAP クエリーを組み合わせることができます。

[削除 (Remove)] ボタンを使用すると、定義されているユーザを現在のユーザのリストから削除できます。

ステップ 7 ユーザの追加が完了したら、[送信 (Submit)] をクリックします。

ステップ 8 メールポリシーを設定するコンテンツ セキュリティ サービスのリンクをクリックします。

次のコンテンツ セキュリティ サービスのタイプを使用できます。

- コンテンツ フィルタ (Content Filters)
- スпам対策 (Anti-Spam)
- ウイルス対策 (Anti-Virus)
- データ消失防止 (Data Loss Prevention) (発信メールポリシーのみ)
- アウトブレイク フィルタ (Outbreak Filters)

ステップ 9 ドロップダウン リストから、デフォルト設定を使用する代わりに、ポリシーの設定をカスタマイズするオプションを選択します。

ステップ 10 セキュリティ サービスの設定をカスタマイズします。

ステップ 11 [送信 (Submit)] をクリックします。

ステップ 12 変更内容を送信し、確定します。

関連項目

- 「メッセージがスパムかどうかスキャンするためのアプライアンスの設定方法」(P.13-2)

送信者または受信者に適用するポリシーの検索

すでに着信または発信メールポリシーに定義されているユーザを検索するには、[ポリシー検索 (Find Policies)] セクションを使用します。

たとえば、bob@example.com と入力して、[ポリシー検索 (Find Policies)] ボタンをクリックし、ポリシーに一致する定義済みのユーザが含まれるポリシーを表示します。

図 10-2 ポリシーでのユーザの検索

Find Policies

Email Address:
 Recipient
 Sender
 Find Policies

Results: Email Address "Recipient: bob@example.com" is defined in the following policies:

- Engineering
- Default Policy (all users)

Policies matching "bob@example.com"

Add Policy... Show All Policies

Order	Policy Name	Anti-Spam	Anti-Virus	Content Filters	Outbreak Filters	Delete
2	Engineering	(use default)	(use default)	(use default)	Retention Time: Virus: 1 day Other: 4 hours	🗑️
	Default Policy	IronPort Anti-Spam Positive: Quarantine Suspected: Quarantine Marketing Messages: Disabled	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	Disabled	Retention Time: Virus: 1 day	

そのポリシーのユーザを編集するには、ポリシーの名前をクリックします。

ユーザを検索する場合、デフォルト ポリシーは常に表示されるため注意してください。これは、定義上、送信者または受信者が設定されているポリシーと一致しない場合、デフォルトのポリシーが必ず一致するためです。

管理例外

前述の 2 つの例で示されている手順を使用して、*管理例外*に基づいたポリシーの作成および設定を開始できます。つまり、組織のニーズを評価した後で、メッセージの大部分がデフォルト ポリシーで処理されるように、ポリシーを設定できます。また、必要に応じて、異なるポリシーを管理して、特定のユーザまたはユーザ グループの追加「例外」ポリシーを作成できます。このようにすることで、メッセージ分裂が最小化され、ワーク キューの各分裂メッセージの処理により受けるシステム パフォーマンスの影響が少なくなります。

スパム、ウイルスおよびポリシー実行に対する組織またはユーザの許容値に基づいて、ポリシーを定義できます。表 10-3 (P.10-10) に、ポリシーの例をいくつか示します。「積極的な」ポリシーでは、エンドユーザのメールボックスに到達するスパムおよびウイルスの量が最小限に抑えられます。「保守的な」ポリシーでは、誤検出を回避し、ポリシーに関係なく、ユーザによるメッセージの見落としを防ぐことができます。

表 10-3 積極的および保守的な電子メール セキュリティ マネージャ設定

	積極的な設定	保守的な設定
スパム対策 (Anti-Spam)	陽性と判定されたスパム：ドロップ 陽性と疑わしいスパム：隔離 マーケティング メール：メッセージの件名の前に「[Marketing]」が追加されて配信	陽性と判定されたスパム：隔離 陽性と疑わしいスパム：メッセージの件名の前に「[Suspected Spam]」が追加されて配信 マーケティング メール：ディセーブル

表 10-3 積極的および保守的な電子メール セキュリティ マネージャ設定 (続き)

ウイルス対策 (Anti-Virus)	修復されたメッセージ：配信 暗号化されたメッセージ：ドロップ スキャンできないメッセージ：ドロップ 感染メッセージ：ドロップ	修復されたメッセージ：配信 暗号化されたメッセージ：隔離 スキャンできないメッセージ：隔離 感染メッセージ：ドロップ
ウイルス フィルタ (Virus Filters)	イネーブル、バイパスできる特定のファイル名拡張子またはドメインなし すべてのメッセージのメッセージ変更の有効化	バイパスできるファイル名拡張子またはドメインの有効化 未署名のメッセージのメッセージ変更の有効化



CHAPTER 11

コンテンツ フィルタ

- 「コンテンツ フィルタの概要」 (P.11-1)
- 「コンテンツ フィルタの仕組み」 (P.11-1)
- 「コンテンツに基づくメッセージのフィルタリング」 (P.11-18)

コンテンツ フィルタの概要

後で検査するためにコンテンツで隔離が必要な場合、企業ポリシーで特定のメッセージを配信前に暗号化する場合、または任意の理由で、電子メール セキュリティ アプライアンスがコンテンツによって特別な処理が必要なメッセージを受診することがあります。これらは、アンチウイルス スキャンまたは DLP などの他のコンテンツ セキュリティ機能が処理できない場合に問題になります。アプライアンスはこのようなコンテンツをスキャンし、メッセージに対して適切なアクションを実行するために、コンテンツ フィルタを使用します。

コンテンツ フィルタの仕組み

コンテンツ フィルタはメッセージ フィルタと似ていますが、メッセージ フィルタ処理およびアンチスパムとアンチウイルス スキャンがメッセージに対して実行された後で適用されます。電子メール セキュリティ アプライアンスは、ユーザ（送信者または受信者）単位でメッセージをスキャンするためにコンテンツ フィルタを使用します。コンテンツ フィルタは、電子メール パイプラインで後ほど適用される点、つまり、1つのメッセージが、各メール ポリシーに対応する個々の複数のメッセージに「分裂」された後で適用される点を除いては、メッセージ フィルタとほぼ同じです。（詳細については、「[メッセージ分裂](#)」 (P.10-5) を参照してください）。コンテンツ フィルタ機能は、メッセージ フィルタ処理およびアンチスパムとアンチウイルス スキャンがメッセージに対して実行された後で適用されません。

コンテンツ フィルタは着信メッセージまたは発信メッセージのどちらかのスキャンに限定されます。両方のメッセージをスキャンするフィルタを定義することはできません。電子メール セキュリティ アプライアンスでは、各メッセージ タイプに対してそれぞれコンテンツ フィルタの「マスター リスト」があります。またマスター リストは、アプライアンスがどの順序でコンテンツ フィルタを実行するかを決定します。ただし個々のメール ポリシーは、メッセージがポリシーに一致するときに、実行される特定のフィルタを決定します。

AsyncOS には、「ルール ビルダ」ページがあります。このページでは、4つの要素を使用してコンテンツ フィルタを簡単に作成できます。

- アプライアンスがメッセージをスキャンするためのコンテンツ フィルタを使用するときに発生する条件 (任意)

- アプライアンスがメッセージに実行するアクション (必須)
- メッセージを変更した場合に、アプライアンスがメッセージに追加できるアクション変数 (任意)

コンテンツ フィルタを使用したメッセージ コンテンツのスキャン方法

表 11-1 コンテンツ フィルタを使用したメッセージ コンテンツのスキャン方法

	操作内容	追加情報
ステップ 1	(任意) コンテンツ フィルタがサポートする機能を定義します。	コンテンツ フィルタで使用する次の項目を作成します。 <ul style="list-style-type: none"> • 暗号化プロファイル • 免責事項テンプレート • 通知テンプレート • Policy 隔離
ステップ 2	着信または発信コンテンツ フィルタを定義します。	コンテンツ フィルタは 3 つの部分から構成されています。 <ul style="list-style-type: none"> • コンテンツ フィルタの条件 (任意) • コンテンツ フィルタのアクション • アクション変数 (任意) 「コンテンツ フィルタの作成」 (P.11-18)
ステップ 3	コンテンツ セキュリティ ルールを設定するユーザ グループを定義します。	着信または発信メール ポリシーを作成します。
ステップ 4	フィルタを使用する着信または発信メッセージのユーザのグループにコンテンツ フィルタを割り当てます。	第 10 章「メール ポリシー」 を参照してください。

コンテンツ フィルタの条件

条件は、電子メール セキュリティ アプライアンスが関連するメール ポリシーに一致するメッセージ フィルタを使用するかどうかを決定する「トリガー」です。コンテンツ フィルタの条件の指定はオプションです。条件のないコンテンツ フィルタは関連するメール ポリシーに一致するすべてのメッセージに適用されます。

コンテンツ フィルタの条件では、メッセージ本文または添付ファイルで特定のパターンを検索するフィルタ ルールを追加する場合、パターンが検出される回数の最小しきい値を指定できます。AsyncOS はメッセージをスキャンすると、メッセージおよび添付ファイルに見つかった一致の数の「スコア」を集計します。最小しきい値に満たない場合、正規表現は true と評価されません。このしきい値は、テキスト、スマート ID、またはコンテンツ デictionary の用語に対して指定できます。

各フィルタには、複数の条件を定義できます。複数の条件が定義されている場合、条件を論理 OR (「次の任意の条件...」) または論理 AND (「次のすべての条件」) のいずれかで結合するかを選択できます。

表 11-2 コンテンツ フィルタの条件

条件	説明
(条件なし)	コンテンツ フィルタでの条件の指定はオプションです。条件が指定されていない場合、true ルールが適用されます。true ルールはすべてのメッセージに一致し、必ずアクションが実行されます。
メッセージ本文あるいは添付ファイル (Message Body or Attachments)	<p>[テキストを含む (Contains text)] : メッセージ本文に、特定のパターンと一致するテキストまたは添付ファイルが含まれているかどうかを判別します。</p> <p>[スマート識別子を含む (Contains smart identifier)] : メッセージ本文または添付ファイルのコンテンツが、スマート ID と一致するかどうかを判別します。</p> <p>[コンテンツ辞書の単語を含む (Contains term in content dictionary)] : メッセージ本文に、<dictionary name> という名前のコンテンツ ディクショナリのいずれかの正規表現または用語が含まれているかどうかを判別します。</p> <p>このオプションをイネーブルにするには、ディクショナリがすでに作成されている必要があります。「コンテンツ ディクショナリ」(P.18-2) を参照してください。</p> <p>(注) ディクショナリに関連する条件は、1 つ以上のディクショナリがイネーブルにされている場合だけ使用できます。コンテンツ ディクショナリの作成の詳細については、「コンテンツ ディクショナリ」(P.18-2) を参照してください。</p> <p>[要求された一致数 (Number of matches required)] : true と評価するためにルールで必要な一致数を指定します。このしきい値は、テキスト、スマート ID、またはコンテンツ ディクショナリの用語に対して指定できます。</p> <p>これには、配信ステータス部および関連付けられている添付ファイルが含まれます。</p>

表 11-2 コンテンツ フィルタの条件 (続き)

条件	説明
メッセージ本文 (Message Body)	<p>[テキストを含む (Contains text)] : メッセージ本文に、特定のパターンと一致するテキストが含まれているかどうかを判別します。</p> <p>[スマート識別子を含む (Contains smart identifier)] : メッセージ本文のコンテンツが、スマート ID と一致するかどうかを判別します。スマート ID は、次のパターンを検出できます。</p> <ul style="list-style-type: none"> • クレジット カード番号 • U.S. 社会保障番号 • Committee on Uniform Security Identification Procedures (CUSIP) 番号 • American Banking Association (ABA; 米国銀行協会) ルーティング番号 <p>[コンテンツ辞書の単語を含む (Contains term in content dictionary)] : メッセージ本文に、<dictionary name> という名前のコンテンツ ディクショナリのいずれかの正規表現または用語が含まれているかどうかを判別します。</p> <p>このオプションをイネーブルにするには、ディクショナリがすでに作成されている必要があります。「コンテンツ ディクショナリ」(P.18-2) を参照してください。</p> <p>(注) ディクショナリに関連する条件は、1 つ以上のディクショナリがイネーブルにされている場合だけ使用できます。コンテンツ ディクショナリの作成の詳細については、「コンテンツ ディクショナリ」(P.18-2) を参照してください。</p> <p>[要求された一致数 (Number of matches required)] : true と評価するためにルールで必要な一致数を指定します。このしきい値は、テキストまたはスマート ID に対して指定できます。</p> <p>このルールは、メッセージの本文だけに適用されます。添付ファイルまたはヘッダーは含まれません。</p>
メッセージ サイズ (Message Size)	<p>本文サイズが、指定範囲内にあるかどうかを判別します。本文サイズとはメッセージのサイズのこと、ヘッダーと添付ファイルも含まれます。本文サイズルールは、本文サイズが指定数と比較されるメッセージを選択します。</p>

表 11-2 コンテンツ フィルタの条件 (続き)

条件	説明
添付ファイルの内容 (Attachment Content)	<p>[テキストを含む (Contains text)] : 指定したパターンと一致するテキストまたは別の添付ファイルが、メッセージの添付ファイルに含まれているか。このルールは <code>body-contains()</code> ルールと似ていますが、このルールでは、メッセージの全体の「本文」をスキャンしないようにします。つまり、ユーザが添付ファイルとして表示する場合だけスキャンします。</p> <p>[スマート識別子を含む (Contains a smart identifier)] : メッセージ添付ファイルの内容が、指定されたスマート ID と一致するかどうかを判別します。</p> <p>[コンテンツ辞書の単語を含む (Contains terms in content dictionary)] : 添付ファイルに、<code><dictionary name></code> という名前のコンテンツ ディクショナリのいずれかの正規表現または用語が含まれているかどうかを判別します。ディクショナリ用語を検索するには、ディクショナリがすでに作成されている必要があります。「コンテンツ ディクショナリ」(P.18-2) を参照してください。</p> <p>(注) ディクショナリに関連する条件は、1 つ以上のディクショナリがイネーブルにされている場合だけ使用できます。コンテンツ ディクショナリの作成の詳細については、「コンテンツ ディクショナリ」(P.18-2) を参照してください。</p> <p>[要求された一致数 (Number of matches required)] : <code>true</code> と評価するためにルールで必要な一致数を指定します。このしきい値は、テキスト、スマート ID またはコンテンツ ディクショナリの一致回数に対して指定できます。</p>

表 11-2 コンテンツ フィルタの条件 (続き)

条件	説明
添付ファイルのファイル情報 (Attachment File Info)	<p>[ファイル名 (Filename)]: メッセージに、ファイル名が特定のパターンと一致する添付ファイルがあるかどうかを判別します。</p> <p>[コンテンツ辞書の単語を含むファイル名 (Filename contains term in content dictionary)]: メッセージに、<dictionary name> という名前のコンテンツ ディクショナリのいずれかの正規表現または用語が含まれるファイル名の添付ファイルがあるかどうかを判別します。</p> <p>このオプションをイネーブルにするには、ディクショナリがすでに作成されている必要があります。「コンテンツ ディクショナリ」(P.18-2)を参照してください。</p> <p>(注) ディクショナリに関連する条件は、1 つ以上のディクショナリがイネーブルにされている場合だけ使用できます。コンテンツ ディクショナリの作成の詳細については、「コンテンツ ディクショナリ」(P.18-2)を参照してください。</p> <p>[ファイル タイプ (File type)]: メッセージに、フィンガープリントに基づいて特定のパターンと一致するファイル タイプの添付ファイルがあるかどうかを判別します (UNIX file コマンドと似ています)。</p> <p>[MIME タイプ (MIME type)]: メッセージに、特定の MIME タイプの添付ファイルがあるかどうかを判別します。このルールは attachment-type ルールに似ていますが、MIME 添付ファイルで指定された MIME タイプのみが評価される点が異なります。(アプライアンスは、タイプが明示的に指定されていない場合、拡張子からファイルのタイプを「予測」することはありません)。</p> <p>[イメージ分析 (Image Analysis)]: メッセージに、指定されているイメージ判定と一致するイメージ添付ファイルがあるかどうかを判別します。有効なイメージ分析判定には、[疑わしい (Suspect)]、[不適切 (Inappropriate)]、[不適切もしくは疑わしい (Suspect or Inappropriate)]、[スキャン不可 (Unscannable)]または[正常 (Clean)]があります。</p>
添付ファイル保護 (Attachment Protection)	<p>[パスワードで保護されたまたは暗号化された添付ファイルが添付されている (Contains an attachment that is password-protected or encrypted)]:</p> <p>(この条件は、たとえば、スキャンできない可能性がある添付ファイルを識別する場合に使用します)。</p> <p>[パスワードで保護されたまたは暗号化された添付ファイルが添付されていない (Contains an attachment that is NOT password-protected or encrypted)]:</p>

表 11-2 コンテンツ フィルタの条件 (続き)

条件	説明
件名ヘッダー (Subject Header)	<p>[件名ヘッダー (Subject Header)] : 件名ヘッダーに、特定のパターンが含まれているかどうかを判別します。</p> <p>[コンテンツ辞書の単語を含む (Contains terms in content dictionary)] : 件名ヘッダーに、<dictionary name> という名前のコンテンツ ディクショナリのいずれかの正規表現または用語が含まれているかどうかを判別します。</p> <p>ディクショナリ用語を検索するには、ディクショナリがすでに作成されている必要があります。「コンテンツ ディクショナリ」(P.18-2) を参照してください。</p> <p>(注) ディクショナリに関連する条件は、1 つ以上のディクショナリがイネーブルにされている場合だけ使用できます。コンテンツ ディクショナリの作成の詳細については、「コンテンツ ディクショナリ」(P.18-2) を参照してください。</p>
その他のヘッダー (Other Header)	<p>[ヘッダー名 (Header name)] : メッセージに、特定のヘッダーが含まれているかどうかを判別します。</p> <p>[ヘッダーの値 (Header value)] : ヘッダーの値が、特定のパターンと一致するかどうかを判別します。</p> <p>[ヘッダーの値がコンテンツ辞書内の単語を含みます (Header value contains terms in the content dictionary)] : 指定されたヘッダーに、<dictionary name> という名前のコンテンツ ディクショナリのいずれかの正規表現または用語が含まれているかどうかを判別します。</p> <p>ディクショナリ用語を検索するには、ディクショナリがすでに作成されている必要があります。「コンテンツ ディクショナリ」(P.18-2) を参照してください。</p> <p>(注) ディクショナリに関連する条件は、1 つ以上のディクショナリがイネーブルにされている場合だけ使用できます。コンテンツ ディクショナリの作成の詳細については、「コンテンツ ディクショナリ」(P.18-2) を参照してください。</p>

表 11-2 コンテンツ フィルタの条件 (続き)

条件	説明
エンベロープ送信者 (Envelope Sender)	<p>[エンベロープ送信者 (Envelope Sender)]: エンベロープ送信者 (Envelope From, <MAIL FROM>) が指定したパターンと一致しているか。</p> <p>[LDAP グループに一致 (Matches LDAP group)]: エンベロープ送信者 (つまり、Envelope From, <MAIL FROM>) が、特定の LDAP グループに含まれるかどうかを判別します。</p> <p>[コンテンツ辞書の単語を含む (Contains term in content dictionary)]: エンベロープ送信者に、<dictionary name> という名前のコンテンツ ディクショナリのいずれかの正規表現または用語が含まれているかどうかを判別します。</p> <p>ディクショナリ用語を検索するには、ディクショナリがすでに作成されている必要があります。「コンテンツ ディクショナリ」(P.18-2) を参照してください。</p> <p>(注) ディクショナリに関連する条件は、1 つ以上のディクショナリがイネーブルにされている場合だけ使用できます。コンテンツ ディクショナリの作成の詳細については、「コンテンツ ディクショナリ」(P.18-2) を参照してください。</p>

表 11-2 コンテンツ フィルタの条件 (続き)

条件	説明
エンベロープ受信者 (Envelope Recipient)	<p>[エンベロープ受信者 (Envelope Recipient)] : エンベロープ受信者 (Envelope To, <RCPT TO>) が指定したパターンと一致しているか。</p> <p>[LDAP グループに一致 (Matches LDAP group)] : エンベロープ受信者 (Envelope To, <RCPT TO>) が、指定した LDAP グループ内に存在するか。</p> <p>[コンテンツ辞書の単語を含む (Contains term in content dictionary)] : エンベロープ受信者に、<dictionary name> という名前のコンテンツ ディクショナリのいずれかの正規表現または用語が含まれているかどうかを判別します。</p> <p>ディクショナリ用語を検索するには、ディクショナリがすでに作成されている必要があります。「コンテンツ ディクショナリ」(P.18-2) を参照してください。</p> <p>(注) ディクショナリに関連する条件は、1 つ以上のディクショナリがイネーブルにされている場合だけ使用できます。コンテンツ ディクショナリの作成の詳細については、「コンテンツ ディクショナリ」(P.18-2) を参照してください。</p> <p>(注) [エンベロープ受信者 (Envelope Recipient)] ルールは、メッセージ単位です。メッセージに複数の受信者がある場合、グループの受信者が 1 人だけ検出されれば、指定されたアクションがメッセージのすべての受信者に適用されます。</p> <p>エンベロープ送信者 (Envelope From <MAIL FROM>) が、指定した LDAP グループ内に存在するか。</p>
受信リスナー (Receiving Listener)	メッセージは、指定されたリスナー経由で届いたか。リスナー名は、システムで現在設定されているリスナーの名前でなければなりません。
リモート IP (Remote IP)	リモート ホストから送信されたメッセージは、指定した IP アドレスまたは IP ブロックに一致しているか。[リモート IP (Remote IP)] ルールは、メッセージを送信したホストの IP アドレスが特定のパターンと一致するかどうかをテストします。これは、インターネット プロトコル バージョン 4 (IPv4) またはバージョン 6 (IPv6) アドレスを指定できます。IP アドレス パターンは、「 送信者グループの構文 」(P.7-4) で説明されている、許可されたホスト表記を使用して指定されます。ただし、SBO、SBRs、dnslist 表記および特殊キーワード ALL を除きます。
レピュテーション スコア (Reputation Score)	送信者の SenderBase レピュテーション スコアを検証します。[レピュテーション スコア (Reputation Score)] は、別の値に対する SenderBase レピュテーション スコアをチェックします。

表 11-2 コンテンツ フィルタの条件 (続き)

条件	説明
DKIM 認証 (DKIM Authentication)	DKIM 認証に合格したか、部分的に検証されたか、一時的に検証不可能として返されたか、失敗したか、DKIM 結果が返されていないかどうかを判別します。
SPF 検証 (SPF Verification)	SPF 検証ステータスを判別します。このフィルタ ルールでは、さまざまな SPF 検証結果をクエリーできます。SPF 検証の詳細については、『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「Email Authentication」を参照してください。

コンテンツ フィルタのアクション

アクションは、電子メールセキュリティ アプライアンスがコンテンツ フィルタの条件に一致するメッセージに行うことです。メッセージの変更、隔離またはドロップなどさまざまなタイプのアクションが用意されています。メッセージで配信またはドロップといった「最終アクション」が実行されることで、電子メールセキュリティ アプライアンスで強制的にアクションが即時実行され、アウトブレイク フィルタまたは DLP スキャンなどのその後のすべての処理が実施されません。

各コンテンツ フィルタには、少なくとも 1 つのアクションを定義する必要があります。

アクションは、順序に従いメッセージで実行されるため、コンテンツ フィルタの複数のアクションを定義する場合、アクションの順序を考慮します。

Attachment Content 条件、Message Body または Attachment 条件、Message 本文条件、または Attachment 内容条件と一致するメッセージに対して隔離アクションを設定した場合、隔離されたメッセージ内の一致した内容を表示できます。メッセージ本文を表示すると、該当内容が黄色で強調表示されます。また、\$MatchedContent アクション変数を使用して、一致した内容をメッセージの件名に含めることができます。詳細については、『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』を参照してください。

フィルタごとに定義できる最終アクションは 1 つだけです。最終アクションは、リストの最後のアクションです。バウンス、配信、およびドロップは、最終アクションです。コンテンツ フィルタのアクションを入力する場合、GUI および CLI により、最終アクションが強制的に最後に配置されます。

表 11-3 コンテンツ フィルタのアクション

アクション	説明
隔離	<p>[隔離 (Quarantine)] : いずれかの Policy 隔離エリアに保持されるメッセージにフラグを付けます。</p> <p>[重複するメッセージ (Duplicate message)] : メッセージのコピーを指定された隔離エリアに送信して、オリジナル メッセージの処理を続行します。任意の追加アクションが、オリジナル メッセージに適用されます。</p>
配信時の暗号化	<p>メッセージは、次の処理段階に進みます。すべての処理が完了すると、メッセージが暗号化され、配信されます。</p> <p>[暗号化ルール (Encryption rule)] : メッセージを常に暗号化するか、TLS 接続を介した送信試行が最初に失敗した場合だけ暗号化します。詳細については、「TLS 接続を暗号化の代わりに使用」(P.16-8) を参照してください。</p> <p>[暗号化プロファイル (Encryption Profile)] : 処理が完了したら、指定された暗号化プロファイルを使用してメッセージを暗号化し、メッセージを配信します。このアクションは、Cisco 暗号化アプライアンスまたはホステッドキー サービスとともに使用します。</p> <p>[件名 (Subject)] : 暗号化されたメッセージの件名です。デフォルトでは、この値は、\$Subject です。</p>

表 11-3 コンテンツ フィルタのアクション (続き)

アクション	説明
内容によって添付ファイルを除去	<p>[次を含む添付ファイル (Attachment contains)]: 正規表現を含むメッセージのすべての添付ファイルをドロップします。アーカイブ ファイル (zip、tar) は、中に含まれているファイルのいずれかが正規表現と一致する場合にドロップされます。</p> <p>[スマート識別子を含む (Contains smart identifier)]: 指定されたスマート ID を含むメッセージのすべての添付ファイルをドロップします。</p> <p>[コンテンツ辞書の単語を含む添付ファイル (Attachment contains terms in the content dictionary)]: 添付ファイルに、<dictionary name> という名前のコンテンツ デictionary のいずれかの正規表現または用語が含まれているかどうかを判別します。</p> <p>[要求された一致数 (Number of matches required)]: true と評価するためにルールで必要な一致数を指定します。このしきい値は、テキスト、スマート ID またはコンテンツ デictionary の一致回数に対して指定できます。</p> <p>[メッセージ差し替え (Replacement message)]: オプション コメントは、ドロップされた添付ファイルの置換に使用されるテキストを変更します。添付ファイルのフッターは、単純にメッセージに追加されるだけです。</p>

表 11-3 コンテンツ フィルタのアクション (続き)

アクション	説明
ファイル情報によって添付ファイルを除去	<p>[ファイル名 (File name)]: 指定された正規表現とファイル名が一致するメッセージのすべての添付ファイルをドロップします。アーカイブ形式の添付ファイル (zip、tar) 内に該当するファイルがある場合、この添付ファイルはドロップされます。</p> <p>[ファイル サイズ (File size)]: メッセージの添付ファイルのうち、ローエンコード形式で指定したサイズ (バイト単位) 以上のサイズであるファイルをすべてドロップします。アーカイブ ファイルまたは圧縮ファイルの場合、このアクションは、圧縮前のサイズを検証せず、実際の自体のサイズが計測されます。</p> <p>[ファイル タイプ (File type)]: メッセージの添付ファイルのうち、指定したファイルの「フィンガープリント」と一致するファイルをすべてドロップします。アーカイブ形式の添付ファイル (zip、tar) 内に該当するファイルがある場合、この添付ファイルはドロップされます。</p> <p>[MIME タイプ (MIME type)]: メッセージの添付ファイルのうち、特定の MIME タイプのファイルをすべてドロップします。</p> <p>[イメージ分析判定 (Image Analysis Verdict)]: 指定されたイメージ判定と一致するイメージ添付ファイルをドロップします。有効なイメージ分析判定には、[疑わしい (Suspect)]、[不適切 (Inappropriate)]、[不適切もしくは疑わしい (Suspect or Inappropriate)]、[スキャン不可 (Unscannable)] または [正常 (Clean)] があります。</p> <p>[メッセージ差し替え (Replacement message)]: オプション コメントは、ドロップされた添付ファイルの置換に使用されるテキストを変更します。添付ファイルのフッターは、単純にメッセージに追加されるだけです。</p>
免責条項文の追加	<p>[上に配置 (Above)]: メッセージ上部に免責事項を追加します (ヘッダー)。</p> <p>[下に配置 (Below)]: メッセージ下部に免責事項を追加します (フッター)。</p> <p>(注) このコンテンツ フィルタ アクションを使用するには、免責事項テキストをすでに作成している必要があります。</p> <p>詳細については、「免責事項テンプレート」(P.18-12) を参照してください。</p>
アウトブレイク フィルタによるスキャンのスキップ	<p>メッセージに対してアウトブレイク フィルタによるスキャンをスキップします。</p>

表 11-3 コンテンツ フィルタのアクション (続き)

アクション	説明
DKIM 署名のバイパス	メッセージに対して DKIM 署名をバイパスします。
コピー (Bcc:) を送信	[電子メール アドレス (Email addresses)] : 指定受信者にメッセージを匿名でコピーします。 [件名 (Subject)] : コピーされたメッセージの件名を追加します。 [リターン パス (オプション) (Return path (optional))] : リターン パスを指定します。 [代替メールホスト (オプション) (Alternate mail host (optional))] : 代替メール ホストを指定します。
通知	[通知 (Notify)] : 指定された受信者にこのメッセージを報告します。オプションで送信者および受信者に通知できます。 [件名 (Subject)] : コピーされたメッセージの件名を追加します。 [リターン パス (オプション) (Return path (optional))] : リターン パスを指定します。 [テンプレート利用 (Use template)] : 作成したテンプレートからテンプレートを選択します。 [オリジナル メッセージを添付ファイルとして含めます (Include original message as an attachment)] : オリジナル メッセージを添付ファイルとして追加します。
受信者を変更	[電子メール アドレス (Email Address)] : メッセージの受信者を指定電子メールアドレスに変更します。
代替送信ホストにメッセージを送信	[メール ホスト (Mail host)] : メッセージの宛先メール ホストを指定メール ホストに変更します。 (注) このアクションは、アンチスパム スキャン エンジンによりスパムとして分類されたメッセージが隔離されないようにします。このアクションは、隔離を無効にして、指定メール ホストに送信します。
IP インターフェイスから送信	[次の IP インターフェイスから送信 (Send from IP interface)] : 指定 IP インターフェイスから送信します。[IP インターフェイスから送信 (Deliver from IP Interface)] アクションは、メッセージのソース ホストを指定ソースに変更します。ソース ホストは、メッセージが配信される IP インターフェイスで構成されます。
ヘッダーの除去	[ヘッダー名 (Header name)] : 指定ヘッダーを配信前にメッセージから削除します。

表 11-3 コンテンツ フィルタのアクション (続き)

アクション	説明
ヘッダーの追加/編集	<p>メッセージに新しいヘッダーを挿入または既存のヘッダーを変更します。</p> <p>[ヘッダー名 (Header name)]: 新規または既存のヘッダーの名前。</p> <p>[新しいヘッダーの値を指定 (Specify value of new header)]: 新しいヘッダーの値を配信前にメッセージに挿入します。</p> <p>[既存のヘッダーの値の前に付加 (Prepend to the Value of Existing Header)]: 配信前に既存のヘッダーの前に値を追加します。</p> <p>[既存のヘッダーの値の後ろに付加 (Append to the Value of Existing Heade)]: 配信前に既存のヘッダーの後ろに値を追加します。</p> <p>[既存のヘッダーの値から検索して置換 (Search & Replace from the Value of Existing Header)]: [検索対象 (Search for)] フィールドに、既存のヘッダーで置き換える値を見つけるための検索語を入力します。ヘッダーに挿入する値を [次で置換 (Replace with)] フィールドに入力します。値を検索するために正規表現を使用できます。ヘッダーから値を削除する場合は、[次で置換 (Replace with)] フィールドを空白のままにしてください。</p>
メッセージ タグの追加	<p>RSA Email DLP ポリシー フィルタリングで使用するカスタム用語をメッセージに挿入します。RSA Email DLP ポリシーを設定して、スキャン対象をメッセージ タグがあるメッセージに限定することができます。メッセージ タグは受信者側では表示されません。DLP ポリシーでのメッセージ タグの使用については、「RSA Email DLP の DLP ポリシー」(P.15-6) を参照してください。</p>
ログ エントリの追加	<p>カスタマイズされたテキストを INFO レベルで IronPort Text Mail ログに挿入します。このテキストにはアクション変数を使用することができます。ログ エントリはメッセージ トラッキングにも表示されます。</p>
暗号化して今すぐ配信 (最終アクション)	<p>メッセージを暗号化および配信し、その後の任意の処理をスキップします。</p> <p>[暗号化ルール (Encryption rule)]: メッセージを常に暗号化するか、TLS 接続を介した送信試行が最初に失敗した場合だけ暗号化します。詳細については、「TLS 接続を暗号化の代わりに使用」(P.16-8) を参照してください。</p> <p>[暗号化プロファイル (Encryption Profile)]: 指定された暗号化プロファイルを使用してメッセージを暗号化し、メッセージを配信します。このアクションは、Cisco 暗号化アプライアンスまたはホステッド キー サービスとともに使用します。</p> <p>[件名 (Subject)]: 暗号化されたメッセージの件名です。デフォルトでは、この値は、\$Subject です。</p>
バウンスする (最終アクション)	<p>メッセージを送信者に戻します。</p>

表 11-3 コンテンツ フィルタのアクション (続き)

アクション	説明
残りのコンテンツ フィルタをスキップ (最終アクション)	メッセージを次の処理段階に配信し、その後の任意のコンテンツ フィルタをスキップします。設定に応じて、メッセージが受信者に配信されるか、隔離が実行されるか、アウトブレイク フィルタによるスキャンが開始されます。
ドロップする (最終アクション)	メッセージをドロップして廃棄します。

アクション変数

コンテンツ フィルタにより処理されるメッセージに追加されるヘッダーには、アクション実行時にオリジナル メッセージの情報に自動的に置換される変数を含めることができます。これらの特殊な変数をアクション変数といいます。Cisco アプライアンスでは次のアクション変数がサポートされています。

表 11-4 アクション変数

変数	構文	説明
すべてのヘッダー (All Headers)	<code>\$AllHeaders</code>	メッセージ ヘッダーに置き換えられます。
本文サイズ (Body Size)	<code>\$BodySize</code>	メッセージのサイズ (バイト単位) に置き換えられます。
日付 (Date)	<code>\$Date</code>	現在の日付 (MM/DD/YYYY 形式) に置き換えられます。
ドロップされたファイル名 (Dropped File Name)	<code>\$dropped_filename</code>	直近にドロップされたファイル名のみを返します。
ドロップされたファイル名 (Dropped File Names)	<code>\$dropped_filenames</code>	<code>\$filenames</code> と同様に、ドロップされたファイルのリストを表示します。
ドロップされたファイル タイプ (Dropped File Types)	<code>\$dropped_filetypes</code>	<code>\$filetypes</code> と同様に、ドロップされたファイル タイプのリストを表示します。
エンベロープ送信者 (Envelope Sender)	<code>\$envelopefrom</code> or <code>\$envelopesender</code>	メッセージのエンベロープ送信者 (Envelope From、<MAIL FROM>) に置き換えられます。
エンベロープ受信者 (Envelope Recipients)	<code>\$EnvelopeRecipients</code>	メッセージのエンベロープ受信者すべて (Envelope To、<RCPT TO>) に置き換えられます。
ファイル名 (File Names)	<code>\$filenames</code>	メッセージの添付ファイルのファイル名を示すカンマ区切りリストに置き換えられます。
ファイル サイズ (File Sizes)	<code>\$filesizes</code>	メッセージの添付ファイルのファイル サイズを示すカンマ区切りリストに置き換えられます。
ファイル タイプ (File Types)	<code>\$filetypes</code>	メッセージの添付ファイルのファイル タイプを示すカンマ区切りリストに置き換えられます。

表 11-4 アクション変数 (続き)

変数	構文	説明
フィルタ名 (Filter Name)	<code>\$FilterName</code>	処理されるフィルタの名前に置き換えられます。
GMTimeStamp	<code>\$GMTimeStamp</code>	現在の時刻および日付 (GMT) に置き換えられます。電子メール メッセージの Received: 行で見られる形式と同様です。
HAT グループ名 (HAT Group Name)	<code>\$Group</code>	メッセージのインジェクト時に、送信者が一致する送信者グループの名前に置き換えられます。送信者グループに名前がない場合は、文字列「>Unknown<」が挿入されます。
メール フロー ポリシー (Mail Flow Policy)	<code>\$Policy</code>	メッセージのインジェクト時に、送信者に適用した HAT ポリシーの名前に置き換えられます。事前に定義されているポリシー名が使用されていない場合、文字列「>Unknown<」が挿入されます。
一致した内容 (Matched Content)	<code>\$MatchedContent</code>	コンテンツ スキャン フィルタをトリガーした 1 つ以上の値に置き換えられます。Matched Content は、コンテンツ ディクショナリ マッチング、スマート ID または正規表現マッチングにすることができます。
ヘッダー (Header)	<code>\$Header['string']</code>	元のメッセージに一致するヘッダーが含まれる場合、引用符付きヘッダーの値に置き換えられます。二重引用符が使用される場合もあります。
ホスト名 (Hostname)	<code>\$Hostname</code>	Cisco アプライアンスのホスト名に置き換えられます。
内部メッセージ ID (Internal Message ID)	<code>\$MID</code>	メッセージを識別するために内部的に使用されるメッセージ ID または「MID」に置き換えられます。RFC822「Message-Id」の値とは異なるため注意してください (「Message-Id」を取得するには \$Header を使用します)。
受信リスナー (Receiving Listener)	<code>\$RecvListener</code>	メッセージを受信したリスナーのニックネームに置き換えられます。
受信インターフェイス (Receiving Interface)	<code>\$RecvInt</code>	メッセージを受信したインターフェイスのニックネームに置き換えられます。
リモート IP アドレス (Remote IP Address)	<code>\$RemoteIP</code>	メッセージを Cisco アプライアンスに送信したシステム IP アドレスに置き換えられます。
リモート ホスト アドレス (Remote Host Address)	<code>\$remotehost</code>	メッセージを Cisco アプライアンスに送信したシステムのホスト名に置き換えられます。
SenderBase レピュテーションスコア (SenderBase Reputation Score)	<code>\$Reputation</code>	送信者の SenderBase レピュテーションスコアに置き換えられます。レピュテーションスコアがない場合は「None」に置き換えられます。

表 11-4 アクション変数 (続き)

変数	構文	説明
件名 (Subject)	\$Subject	メッセージの件名に置き換えられます。
時間 (Time)	\$Time	現在の時刻 (ローカル時間帯) に置き換えられます。
タイムスタンプ (Timestamp)	\$Timestamp	現在の時刻および日付 (ローカル時間帯) に置き換えられます。電子メール メッセージの Received: 行で見られる形式と同様です。

コンテンツに基づくメッセージのフィルタリング

コンテンツ フィルタの作成

はじめる前に

- コンテンツ フィルタに一致するメッセージを暗号化する場合は、暗号化プロファイルを作成します。
- 一致メッセージに免責事項を追加する場合は、免責事項の生成に使用する免責事項テンプレートを作成します。
- 一致するメッセージについてユーザに通知メッセージを送信する場合は、通知を生成するための通知テンプレートを作成します。
- メッセージを隔離する場合は、これらのメッセージに対する新しい Policy 隔離を作成するか、または既存のものを使用します。

手順

- ステップ 1** [メール ポリシー (Mail Policies)] > [受信メール ポリシー (Incoming Mail Policies)]
または
[メール ポリシー (Mail Policies)] > [送信メール ポリシー (Outgoing Mail Policies)] をクリックします。
- ステップ 2** [フィルタを追加 (Add Filter)] をクリックします。
- ステップ 3** フィルタの名前と説明を入力します。
- ステップ 4** (相互参照) [編集可能なユーザ (役割) (Editable By (Roles))] リンクをクリックして、ポリシーの管理者を選択し、[OK] をクリックします。
ポリシー管理者ユーザ ロールに属する委任管理者はこのコンテンツ フィルタを編集し、自身のメールポリシーで使用できます。
- ステップ 5** (任意) フィルタをトリガーするための条件を追加します。
 - a. [条件を追加 (Add Condition)] をクリックします。
 - b. 条件のタイプを選択します。
 - c. 条件のルールを定義します。
 - d. [OK] をクリックします。

- e. フィルタに追加する追加条件について、上記の手順を繰り返して行ってください。コンテンツ フィルタに複数の条件を定義する場合、コンテンツ フィルタが一致したと見なされるために、定義されるアクションのすべて（論理 AND）、または定義されたいずれかのアクション（論理 OR）の適用が必要かどうかを定義できます。



(注) 条件を追加しない場合、アプライアンスはフィルタに関連するメール ポリシーの 1 つと一致するあらゆるメッセージにコンテンツ フィルタのアクションを実行します。

- ステップ 6** フィルタの条件に一致するメッセージに対して実行するアプライアンスのアクションを追加します。
- [アクションを追加 (Add Action)] をクリックします。
 - アクション タイプを選択します。
 - アクションを定義します。
 - [OK] をクリックします。
 - アプライアンスに実行する追加のアクションについて、上記の手順を繰り返して行ってください。
 - 複数のアクションに対して、アプライアンスがメッセージに適用する順序でアクションを配置します。フィルタごとに 1 個だけ「最終」アクションがあり、AsyncOS は自動的に最終アクションを順番の最後に移動します。
- ステップ 7** 変更内容を送信し、確定します。

次の作業

- デフォルトの着信または発信メール ポリシーでコンテンツ フィルタをイネーブルにできます。
- 特定のユーザ グループのメール ポリシーのコンテンツ フィルタをイネーブルにできます。

デフォルトでのすべての受信者のコンテンツ フィルタのイネーブル化

手順

- ステップ 1** [メール ポリシー (Mail Policies)] > [受信メール ポリシー (Incoming Mail Policies)] または [メール ポリシー (Mail Policies)] > [送信メール ポリシー (Outgoing Mail Policies)] をクリックします。
- ステップ 2** デフォルト ポリシー行のコンテンツ フィルタ セキュリティ サービスのリンクをクリックします
- ステップ 3** コンテンツ フィルタ セキュリティ サービス ページで、[コンテンツ フィルタリング: デフォルト ポリシー (Content Filtering for Default Policy)] の値を [コンテンツ フィルタを無効にする (Disable Content Filters)] から [コンテンツ フィルタを有効にする (設定をカスタマイズ) (Enable Content Filters (Customize settings))] に変更します。
- マスター リストで定義されているコンテンツ フィルタ（「[コンテンツ フィルタの概要](#)」(P.11-1) で作成されたフィルタ）が、このページに表示されます。値を [コンテンツ フィルタを有効にする (設定をカスタマイズ) (Enable Content Filters (Customize settings))] に変更すると、各フィルタのチェックボックスがイネーブルになります。
- ステップ 4** イネーブルにする個々のコンテンツ フィルタの [有効 (Enable)] チェックボックスをオンにします。

ステップ 5 変更内容を送信し、確定します。

特定のユーザ グループに対するメッセージへのコンテンツ フィルタの適用

はじめる前に

- ユーザ グループのメッセージに対してコンテンツ フィルタを使用する場合、着信または発信メール ポリシーを作成します。詳細については、「[送信者および受信者のグループのメール ポリシーの作成](#)」(P.10-8) を参照してください。

手順

-
- ステップ 1** [メール ポリシー (Mail Policies)] > [受信メール ポリシー (Incoming Mail Policies)]
または
[メール ポリシー (Mail Policies)] > [送信メール ポリシー (Outgoing Mail Policies)] をクリックします。
- ステップ 2** コンテンツ フィルタに適用するメール ポリシーのコンテンツ フィルタ セキュリティ サービス ([コンテンツ フィルタ (Content Filters)] 列) のリンクをクリックします。
- ステップ 3** コンテンツ フィルタ セキュリティ サービス ページで、[ポリシーのコンテンツ フィルタリング : エンジニアリング (Content Filtering for Policy: Engineering)] の値を [コンテンツ フィルタを有効にする (デフォルトのメール ポリシー設定を継承) (Enable Content Filtering (Inherit default policy settings))] から [コンテンツ フィルタを有効にする (設定をカスタマイズ) (Enable Content Filters (Customize settings))] に変更します。
- ステップ 4** ユーザが使用するコンテンツ フィルタのチェックボックスを選択します。
- ステップ 5** 変更内容を送信し、確定します。
-

GUI でのコンテンツ フィルタの設定に関する注意事項

- コンテンツ フィルタを作成するときに条件を指定する必要はありません。アクションが定義されていない場合、定義されるアクションは常にルールに適用されます (条件を指定しないことは、`true()` メッセージ フィルタ ルールを使用することと同じで、コンテンツ フィルタがポリシーに適用される場合、すべてのメッセージがマッチングされます)。
- カスタム ユーザ ロールをコンテンツ フィルタに割り当てていない場合、パブリックのコンテンツ フィルタになり、メール ポリシーの任意の委任管理者が使用できます。委任管理者とコンテンツ フィルタの詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Common Administrative Tasks」の章を参照してください。
- 管理者とオペレータは、コンテンツ フィルタがカスタム ユーザ ロールに割り当てられていない場合でも、アプライアンスのすべてのコンテンツ フィルタを表示および編集できます。
- フィルタ ルールおよびアクションのテキストを入力する場合、正規表現照合において、次のメタ文字に特殊な意味があります。`^ $ * + ? { [] \ | ()`
正規表現を使用しない場合、「\」(バックスラッシュ) を使用して、これらの任意の文字をエスケープする必要があります。たとえば、「*Warning*」と入力します。

- 「benign」コンテンツ フィルタを作成して、メッセージ分裂およびコンテンツ フィルタをテストできます。たとえば、唯一のアクションが「配信」であるコンテンツ フィルタを作成できます。このコンテンツ フィルタは、メール処理に影響を与えませんが、このフィルタを使用して、電子メールセキュリティ マネージャ ポリシー処理が、システムの他の要素（たとえば、メール ログ）に影響を与えているかテストできます。
- 逆に、着信または発信コンテンツ フィルタの「マスター リスト」の概念を使用して、アプライアンスにより処理されるすべてのメールのメッセージ処理に即時に影響を与える、非常に優れた、広範囲に及ぶコンテンツ フィルタを作成できます。このコンテンツ フィルタは次のように作成できます。
 - [受信コンテンツ フィルタ (Incoming Content Filters)] または [送信コンテンツ フィルタ (Outgoing Content Filters)] ページを使用して、順序が 1 の新しいコンテンツ フィルタを作成します。
 - [受信メール ポリシー (Incoming Mail Policies)] または [送信メール ポリシー (Outgoing Mail Policies)] ページを使用して、デフォルト ポリシーの新しいコンテンツ フィルタをイネーブルにします。
 - 残りすべてのポリシーでこのコンテンツ フィルタをイネーブルにします。
- コンテンツ フィルタで使用できる [Bcc:] および [隔離 (Quarantine)] アクションは、作成する隔離エリアの保持設定に役に立ちます（詳細については、第 27 章「隔離」を参照してください）。メッセージがすぐにはシステムからリリースされないようにするため（つまり、隔離エリアの割り当てディスク領域がすぐにいっぱいにならないようにするため）、ポリシー隔離とのメールフローをシミュレートするフィルタを作成できます。
- scanconfig コマンドと同じ設定が使用されるため、「Entire Message」条件は、メッセージのヘッダーをスキャンしません。「Entire Message」を選択すると、メッセージ本文および添付ファイルだけがスキャンされます。特定のヘッダー情報を検索するには、「Subject」または「Header」条件を使用します。
- LDAP クエリーによるユーザの設定は、アプライアンスで LDAP サーバが設定されている場合（つまり、ldapconfig コマンドを使用して特定の文字列を含む特定の LDAP サーバをクエリーするようにアプライアンスが設定されている場合）だけ GUI に表示されます。
- リソースが事前に定義されていないため、コンテンツ フィルタ ルール ビルダのいくつかのセクションは、GUI に表示されません。たとえば、通知テンプレートおよびメッセージ免責事項は、[テキスト リソース (Text Resources)] ページまたは CLI の textconfig コマンドを使用して事前に設定されていない場合、オプションとして表示されません。
- コンテンツ フィルタ機能は、次の文字エンコーディングのテキストを認識し、これらを追加およびスキャンできます。
 - Unicode (UTF-8)
 - Unicode (UTF-16)
 - Western European/Latin-1 (ISO 8859-1)
 - Western European/Latin-1 (Windows CP1252)
 - 中国語 (繁体字) (Big 5)
 - 中国語 (簡体字) (GB 2312)
 - 中国語 (簡体字) (HZ GB 2312)
 - 韓国語 (ISO 2022-KR)
 - 韓国語 (KS-C-5601/EUC-KR)
 - 日本語 (Shift-JIS (X0123))
 - 日本語 (ISO-2022-JP)









- 日本語 (EUC)

複数の文字セットを 1 つのコンテンツ フィルタ内で組み合わせてマッチングできます。複数の文字エンコーディングでのテキストの表示および入力については、Web ブラウザのマニュアルを参照してください。ほとんどのブラウザでは、複数の文字セットを同時にレンダリングできます。

- 着信または発信コンテンツ フィルタの要約ページで、[説明 (Description)]、[ルール (Rules)] および [ポリシー (Policies)] のリンクを使用して、コンテンツ フィルタに提供されているビューを変更します。
 - [説明 (Description)] ビューには、各コンテンツ フィルタの説明フィールドに入力したテキストが表示されます (これはデフォルト ビューです)。
 - [ルール (Rules)] ビューには、ルール ビルダ ページにより構築されたルールおよび正規表現が表示されます。
 - [ポリシー (Policies)] ビューには、イネーブルにされている各コンテンツ フィルタのポリシーが表示されます。

図 11-1 コンテンツ フィルタの [説明 (Description)]、[ルール (Rules)] および [ポリシー (Policy)] を切り替えるリンクの使用

Incoming Content Filters

Filters				
Add Filter...				
Order	Filter Name	Description Rules Policies	Duplicate	Delete
1	scan_for_confidential	scan_for_confidential: if (body-contains("confidential")) { quarantine ("Policy"); bcc ("hr@example.com", "[message matched confidential filter]"); }		
2	no_mp3s	no_mp3s: if (true) { drop-attachments-by-filetype("mp3", "mp3 deleted"); }		
3	ex_employee	ex_employee: if (rcpt-to == "^doug@") { notify-copy ("%EnvelopeSender", "message bounced for ex-employee of example.com"); bounce(); }		
4	drop_large_attachments	drop_large_attachments: if (true) { drop-attachments-by-size(5242880, "This attachment was too big"); }		



CHAPTER 12

アンチウイルス

- 「アンチウイルス スキャンの概要」 (P.12-1)
- 「Sophos Anti-Virus フィルタリング」 (P.12-2)
- 「McAfee Anti-Virus フィルタリング」 (P.12-5)
- 「アプライアンスでのウイルスのスキャンの設定方法」 (P.12-6)
- 「アンチウイルス スキャンをテストするためにアプライアンスにメールを送信する」 (P.12-17)
- 「ウイルス定義ファイルの更新」 (P.12-19)

アンチウイルス スキャンの概要

Cisco アプライアンスには、サードパーティの企業の Sophos および McAfee の統合されたウイルス スキャン エンジンが含まれます。Cisco アプライアンスのライセンス キーを取得して、これらのウイルス スキャン エンジンのいずれかまたは両方を使用してメッセージのウイルスをスキャンし、どちらかのアンチウイルス スキャン エンジンを使用してウイルスをスキャンするようにアプライアンスを設定できます。

McAfee および Sophos のエンジンには、特定のポイントでのファイルのスキャン、ファイルで発見されたデータとウイルス定義のパターン照合と処理、エミュレーション環境でのウイルス コードの復号化および実行、新しいウイルスを認識するための発見的手法の適用、および正規ファイルからの感染コードの削除に必要なプログラム ロジックが含まれています。

(一致する着信または発信メール ポリシーに基づいて) メッセージのウイルスをスキャンし、ウイルスが見つかった場合はメッセージに対してさまざまなアクション (たとえば、ウイルスの発見されたメッセージの「修復」、件名ヘッダーの変更、X-Header の追加、代替アドレスまたはメールホストへのメッセージの送信、メッセージのアーカイブ、またはメッセージの削除など) を実行するようにアプライアンスを設定できます。

ウイルス スキャンをイネーブルにした場合は、アンチスパム スキャンの直後に、アプライアンス上の「ワーク キュー」でウイルス スキャンが実行されます (「電子メール パイプラインとセキュリティ サービス」 (P.4-7) を参照)。

デフォルトでは、ウイルス スキャンはデフォルトの着信および発信メール ポリシーに対してイネーブルになります。

評価キー

Cisco アプライアンスには、使用可能な各アンチウイルス スキャン エンジンに対して 30 日間有効な評価キーが同梱されています。評価キーは、システム セットアップ ウィザードまたは [セキュリティ サービス (Security Services)] > [Sophos] または [McAfee ウイルス対策 (McAfee Anti-Virus)] ページのライセンス契約書にアクセスするか (GUI)、または `antivirusconfig` または `systemsetup` コマンドを実行して (CLI) イネーブルにします。デフォルトでは、ライセンス契約書に同意すると、アンチウイルス スキャン エンジンはデフォルトの着信および発信メール ポリシーに対してただちにイネーブルになります。30 日間の評価期間後もこの機能をイネーブルにする場合の詳細については、Cisco の営業担当者にお問い合わせください。残りの評価期間は、[システム管理 (System Administration)] > [ライセンス キー (Feature Keys)] ページを表示するか、または `featurekey` コマンドを発行することによって確認できます (詳細については、「[ライセンス キー](#)」(P.29-5) を参照してください)。

複数のアンチウイルス スキャンエンジンによるメッセージのスキャン

AsyncOS は、複数のアンチウイルス スキャン エンジンによるメッセージのスキャン (マルチレイヤ アンチウイルス スキャン) をサポートしています。メール ポリシーごとに、ライセンスを受けたアンチウイルス スキャン エンジンのいずれかまたは両方を使用するように Cisco アプライアンスを設定できます。たとえば、経営幹部用のメール ポリシーを作成し、そのポリシーでは Sophos および McAfee の両方のエンジンを使用してメールをスキャンするように設定することもできます。

複数のスキャン エンジンでメッセージをスキャンすることにより、Sophos および McAfee のアンチウイルス スキャン エンジン双方の利点を組み合わせた「多重防衛」が実現します。各エンジンともに業界をリードするアンチウイルス捕捉率を誇りますが、各エンジンは別々のテクノロジー基盤 ([「McAfee Anti-Virus フィルタリング」](#) (P.12-5) および [「Sophos Anti-Virus フィルタリング」](#) (P.12-2) を参照) に依存してウイルスを検出しているため、マルチスキャン方式を使用することで、より効果が高まります。複数のスキャン エンジンを使用することで、システム スループットが低下する場合があります。詳細は、Cisco のサポート担当者にお問い合わせください。

ウイルス スキャンの順序は設定できません。マルチレイヤ アンチウイルス スキャンをイネーブルにした場合、最初に McAfee エンジンによるウイルス スキャンが実行され、次に Sophos エンジンによるウイルス スキャンが実行されます。McAfee エンジンがメッセージはウイルスに感染していないと判断した場合は、Sophos エンジンはさらにメッセージをスキャンして、別の保護層を追加します。McAfee エンジンがメッセージはウイルスを含んでいると判断した場合は、Cisco アプライアンスは Sophos によるスキャンをスキップし、構成した設定に応じてウイルス メッセージに対してアクションを実行します。

Sophos Anti-Virus フィルタリング

Cisco アプライアンスには、Sophos の総合的なウイルス スキャン テクノロジーが含まれています。Sophos Anti-Virus は、プラットフォーム間のアンチウイルス保護、検出、および除去を提供します。

Sophos Anti-Virus は、ファイルをスキャンしてウイルス、トロイの木馬、およびワームを検出するウイルス検出エンジンを提供します。これらのプログラムは、「悪意のあるソフトウェア」を意味するマルウェアと総称されます。アンチウイルス スキャナは、すべてのタイプのマルウェアに共通する相似点を利用して、ウイルスだけでなく、すべてのタイプの悪意のあるソフトウェアを検出および削除します。

ウイルス検出エンジン

Sophos ウイルス検出エンジンは、Sophos Anti-Virus テクノロジーの中心的役割を担います。このエンジンは、Microsoft の Component Object Model (COM; コンポーネント オブジェクト モデル) と同様の、多くのオブジェクトと明確に定義されたインターフェイスで構成された独自のアーキテクチャを使用します。エンジンで使用されるモジュラ ファイリング システムは、それぞれが異なる「ストレージ クラス」(たとえばファイル タイプなど) を処理する、個別の内蔵型動的ライブラリに基づいています。この方法では、タイプに関係なく汎用のデータ ソースにウイルス スキャン操作を適用できます。

エンジンは、データのロードおよび検索に特化したテクノロジーにより、非常に高速なスキャンを実現できます。次の機能が内蔵されています。

- ポリモーフィック型ウイルスを検出するためのフル コード エミュレータ。
- アーカイブ ファイル内をスキャンするためのオンライン解凍プログラム。
- マクロ ウイルスを検出および駆除するための OLE2 エンジン。

Cisco アプライアンスは、SAV インターフェイスを使用してウイルス エンジンを統合しています。

ウイルス スキャン

大まかにいうと、エンジンのスキャン機能は、検索する場所を特定する分類子と、検索する対象を特定するウイルス データベースという 2 つの重要なコンポーネントの高性能な組み合わせにより管理されています。エンジンは、識別子に依存せずに、タイプでファイルを分類します。

ウイルス エンジンは、システムが受信したメッセージの本文および添付ファイルでウイルスを検索しますが、スキャンの実行方法の決定には、添付ファイルのタイプが役立ちます。たとえば、メッセージの添付ファイルが実行ファイルであれば、エンジンは実行コードの開始場所が記述されているヘッダーを調べて、その場所を検索します。ファイルが Word ドキュメントであれば、エンジンはマクロ ストリームを調べます。MIME ファイル (メール メッセージに使用される形式) であれば、添付ファイルが保存されている場所を調べます。

検出方法

ウイルスの検出方法は、ウイルスのタイプに応じて異なります。スキャン処理中に、エンジンは各ファイルを分析してタイプを特定してから、該当する手法を適用します。すべての方法の根幹には、特定のタイプの命令または特定の命令の順序を検索するという基本概念があります。

パターン照合

パターン照合の手法では、エンジンは特定のコード シーケンスを知っており、そのコード シーケンスと完全一致するコードをウイルスとして特定します。たいていの場合、エンジンは既知のウイルス コードのシーケンスに類似した (必ずしも完全に同一である必要はありません) コードのシーケンスを検索します。スキャン実行中にファイルを比較する対象となる記述を作成する際、Sophos のウイルス研究者達は、エンジンが (次で説明する発見的手法を使用して) オリジナルのウイルスだけでなく、後の派生的なウイルスも発見できるように、識別コードを可能な限り一般的なものに維持することに努めています。

発見的手法

ウイルス エンジンには、基本的なパターン照合手法と発見的手法（特定のルールではなく一般的なルールを使用する手法）を組み合わせることで、Sophos の研究者があるファミリーの 1 種類のウイルスしか分析していなかったとしても、そのファミリーの複数のウイルスを検出できます。この手法では、記述を 1 つ作成すれば、ウイルスの複数の派生形を捕らえることができます。Sophos は、発見的手法にその他の手法を加味することで、false positive の発生を最低限に抑えています。

エミュレーション

エミュレーションは、ポリモーフィック型ウイルスに対して、ウイルス エンジンによって適用される手法です。ポリモーフィック型ウイルスは、ウイルスを隠す目的のために、ウイルス自体を別の形に変更する暗号化されたウイルスです。明らかな定型的ウイルス コードは存在せず、拡散するたびにウイルス自体が別の形に暗号化されます。このウイルスは、実行されたときに自己復号化します。ウイルス 検出エンジンのエミュレータは、DOS または Windows 実行ファイルに使用されますが、ポリモーフィック型マクロは Sophos のウイルス記述言語で記述された検出コードによって発見されます。

この復号化の出力は実際のウイルス コードであり、エミュレータで実行された後に Sophos のウイルス 検出エンジンによって検出されるのは、この出力です。

スキャン用にエンジンに送信された実行ファイルは、エミュレータ内で実行されます。エミュレータでは、ウイルス本文の復号化がメモリに書き込まれ、これに応じて復号化が追跡されます。通常、ウイルスの侵入ポイントはファイルのフロントエンドにあり、最初に実行される部分です。ほとんどの場合、ウイルスであることを認識するためには、ウイルス本文のほんのわずかな部分を復号化するだけで十分です。クリーンな実行ファイルの多くは、数個の命令をエミュレートするだけでエミュレーションを停止して、負担を軽減します。

エミュレータは制限された領域で実行されるため、コードがウイルスであるとわかっていても、アプライアンスに感染することはありません。

ウイルスの記述

Sophos は、他の信用されているアンチウイルス企業と毎月ウイルスを交換しています。さらに、顧客から毎月数千の疑わしいファイルが直接 Sophos に送られ、そのうち約 30 % はウイルスであると判明しています。各サンプルは、非常にセキュアなウイルス ラボで厳しく分析され、ウイルスかどうか判断されます。Sophos は、新しく発見された各ウイルスまたはウイルスのグループに対して、記述を作成します。

Sophos アラート

Sophos Anti-Virus スキャンをイネーブルにしているお客様に対して、Sophos のサイト (<http://www.sophos.com/virusinfo/notifications/>) から Sophos アラートを購読することを推奨しています。

購読して Sophos から直接アラートを受け取ることにより、最新のウイルスの発生および利用可能な解決方法が確実に通知されます。

ウイルスが発見された場合

ウイルスが検出されたら、Sophos Anti-Virus はファイルを修復（駆除）できます。通常、Sophos Anti-Virus は、ウイルスが発見されたファイルをすべて修復でき、修復後はそのファイルをリスクなく使用できます。的確なアクションは、ウイルスに応じて異なります。

駆除の場合は、必ずしもファイルを元の状態に戻せるとは限らないため、ある程度の制限が生じる場合があります。一部のウイルスは実行プログラムの一部を上書きしてしまうため、元に戻せません。この場合は、修復できない添付ファイルを含むメッセージをどのように処理するかを定義します。これらの設定は、Email Security 機能 ([メール ポリシー (Mail Policies)] > [受信メール ポリシー (Incoming Mail Policies)] または [送信メール ポリシー (Outgoing Mail Policies)] ページ (GUI) または `policyconfig -> antivirus` コマンド (CLI)) を使用して受信者ごとに構成できます。これらの設定の構成に関する詳細については、「[ユーザのウイルス スキャン アクションの設定](#)」(P.12-7) を参照してください。

McAfee Anti-Virus フィルタリング

McAfee® スキャン エンジンは、次の処理を行います。

- ファイルのデータとウイルス シグニチャをパターン照合することにより、ファイルをスキャンします。
- エミュレーション環境でウイルス コードを復号化および実行します。
- 発見の手法を適用して新しいウイルスを認識します。
- ファイルから感染性のコードを削除します。

ウイルス シグニチャとのパターン照合

McAfee は、アンチウイルス定義 (DAT) ファイルをスキャン エンジンで使用して、特定のウイルス、ウイルスのタイプ、またはその他の潜在的に望ましくないソフトウェアを検出します。また、ファイル内の既知の場所を開始点としてウイルス固有の特徴を検索することにより、単純なウイルスを検出できます。多くの場合、ファイルのほんの一部を検索するだけで、ファイルがウイルスに感染していないと判断できます。

暗号化されたポリモーフィック型ウイルスの検出

複雑なウイルスは、次の 2 つの一般的な手法を使用して、シグニチャ スキャンによる検出を回避します。

- **暗号化**。ウイルス内部のデータは、アンチウイルス スキャナがメッセージまたはウイルスのコンピュータ コードを判読できないように、暗号化されます。ウイルスがアクティブになると、ウイルス自体が自発的に実行バージョンに変化し、自己実行します。
- **ポリモーフィック化**。この処理は暗号化に似ていますが、ウイルスが自己複製する際に、その形が変わる点で暗号化とは異なります。

このようなウイルスに対抗するために、エンジンはエミュレーションと呼ばれる手法を使用します。エンジンは、ファイルにこのようなウイルスが含まれていると疑った場合、ウイルスが他に害を及ぼすことなく自己実行して、本来の形が判読できる状態まで自分自身をデコードする人工的な環境を作成します。その後、エンジンは通常どおりウイルス シグニチャをスキャンして、ウイルスを特定します。

発見的分析

新しいウイルスの署名は未知であるため、ウイルス シグニチャを使用するだけでは、新しいウイルスは検出できません。そのため、エンジンは追加で発見的分析という手法を使用します。

ウイルスを運ぶプログラム、ドキュメント、または電子メール メッセージには、多くの場合、特異な特徴があります。これらは、自発的にファイルの変更を試行したり、メール クライアントを起動したり、またはその他の方法を使用して自己複製します。エンジンはプログラム コードを分析して、この種のコンピュータ命令を検出します。また、エンジンは、アクションを実行する前にユーザの入力を求めたりするようなウイルスらしくない正規の動作も検索して、誤ったアラームを発行しないようにしています。

このような手法を使用することで、エンジンは多くの新しいウイルスを検出できます。

ウイルスが発見された場合

ウイルスが検出されたら、McAfee はファイルを修復（駆除）できます。通常、McAfee は、ウイルスが発見されたファイルをすべて修復でき、修復後はそのファイルをリスクなく使用できます。的確なアクションは、ウイルスに応じて異なります。

ファイルの駆除の場合は、必ずしもファイルを元の状態に戻せるとは限らないため、時折、ある程度の制限が生じる場合があります。一部のウイルスは実行プログラムの一部を上書きしてしまうため、元に戻せません。この場合は、修復できない添付ファイルを含むメッセージをどのように処理するかを定義します。これらの設定は、Email Security 機能 ([メール ポリシー (Mail Policies)] > [受信メール ポリシー (Incoming Mail Policies)] または [送信メール ポリシー (Outgoing Mail Policies)] ページ (GUI) または `policyconfig -> antivirus` コマンド (CLI)) を使用して受信者ごとに構成できます。これらの設定の構成に関する詳細については、「[ユーザのウイルス スキヤンアクションの設定 \(P.12-7\)](#)」を参照してください。

アプライアンスでのウイルスのスキヤンの設定方法

表 12-1 メッセージのウイルスのスキヤン方法

	操作内容	追加情報
ステップ 1	電子メール セキュリティ アプライアンスでアンチウイルス スキヤンをイネーブルにします。	「 ウイルス スキヤンのイネーブル化およびグローバル設定の構成 (P.12-7) 」
ステップ 2	メッセージのウイルスをスキヤンするユーザグループを定義します。	「 送信者および受信者のグループのメール ポリシーの作成 (P.10-8) 」
ステップ 3	(任意) ウイルス隔離でのメッセージの処理方法を設定します。	「 ポリシー隔離の作成 (P.27-6) 」
ステップ 4	アプライアンスでのウイルスに感染したメッセージを処理方法を決定します。	「 ユーザのウイルス スキヤンアクションの設定 (P.12-7) 」
ステップ 5	定義したユーザグループに対するアンチウイルス スキヤンのルールを設定します。	「 送信者および受信者のグループごとのアンチウイルス ポリシーの設定 (P.12-13) 」
ステップ 6	(任意) 設定をテストするために電子メールメッセージを送信します。	「 アンチウイルス スキヤンをテストするためにアプライアンスにメールを送信する (P.12-17) 」

ウイルス スキャンのイネーブル化およびグローバル設定の構成

ウイルス スキャン エンジン は、システム セットアップ ウィザード を実行したときにイネーブルになった可能性があります。これにかかわらず、次の手順で設定をします。



(注) ライセンス キーによって、Sophos、McAfee、またはその両方をイネーブルにできます。

手順

ステップ 1 [セキュリティ サービス (Security Services)] > [McAfee] ページに移動します。

または

[セキュリティ サービス (Security Services)] > [Sophos] ページに移動します。

ステップ 2 [有効 (Enable)] をクリックします。



(注) [有効 (Enable)] をクリックすると、アプライアンスで機能がグローバルにイネーブルになります。ただし、後で [メール ポリシー (Mail Policies)] で受信者ごとの設定をイネーブルにする必要があります。

ステップ 3 ライセンス契約書を読み、ページの最後までスクロールしてから [承認 (Accept)] をクリックして契約に同意します。

ステップ 4 [グローバル設定を編集 (Edit Global Settings)] をクリックします。

ステップ 5 ウイルス スキャンの最大タイムアウト値を選択します。

システムがメッセージに対するアンチウイルス スキャンの実行を停止する、タイムアウト値を設定します。デフォルト値は 60 秒です。

ステップ 6 変更内容を送信し、確定します。

次の作業

アンチウイルス設定を受信者ごとに設定します。「[ユーザのウイルス スキャン アクションの設定 \(P.12-7\)](#)」を参照してください。

ユーザのウイルス スキャン アクションの設定

Cisco アプライアンスに統合されているウイルス スキャン エンジン は、[電子メールセキュリティマネージャ (Email Security Manager)] 機能を使用して設定したポリシー (設定オプション) に基づいて、着信および発信メール メッセージのウイルスを処理します。アンチウイルス アクションは、[メールセキュリティ機能 (Email Security Feature)] ([メール ポリシー (Mail Policies)] > [受信メールポリシー (Incoming Mail Policies)] または [送信メールポリシー (Outgoing Mail Policies)] ページ (GUI) または `policyconfig > antivirus` コマンド (CLI)) を使用して受信者ごとにイネーブルにします。

メッセージ スキャン設定

- [ウイルス スキャンのみ (Scan for Viruses Only)] :

システムにより処理されるメッセージには、ウイルス スキヤンが実行されます。感染している添付ファイルがあっても、修復は試行されません。ウイルスが含まれるメッセージまたは修復できなかったメッセージについて、添付ファイルをドロップしてメールを配信するかどうかを選択できます。

- [ウイルスをスキヤンして修復 (Scan and Repair Viruses)] :

システムにより処理されるメッセージには、ウイルス スキヤンが実行されます。添付ファイルにウイルスが発見された場合は、システムは添付ファイルの「修復」を試行します。

- [添付ファイルをドロップ (Dropping Attachments)] :

感染した添付ファイルをドロップするように選択できます。

アンチウイルス スキヤン エンジンにより、メッセージの添付ファイルがスキヤンされ感染したファイルがドロップされると、代わりに「Removed Attachment」という名前の新しいファイルが添付されます。この添付ファイルのタイプはテキストまたはプレーンで、次の内容が含まれています。

This attachment contained a virus and was stripped.

Filename: *filename*

Content-Type: *application/filetype*

悪質な添付ファイルによりメッセージが感染していたため、ユーザのメッセージに何らかの修正が加えられた場合は、必ずユーザに通知されます。二次的な通知アクションを設定することもできます（「通知の送信」(P.12-11) を参照）。感染した添付ファイルをドロップするように選択した場合は、通知アクションにより、ユーザにメッセージが修正されたことを通知する必要はありません。

- [X-IronPort-AV ヘッダー (X-IronPort-AV Header)] :

アプライアンスのアンチウイルス スキヤン エンジンにより処理されたすべてのメッセージには、X-IronPort-AV: というヘッダーが追加されます。このヘッダーは、特に「スキヤンできない」と見なされたメッセージについて、アンチウイルス設定に関する問題をデバッグする際の追加情報となります。X-IronPort-AV ヘッダーをスキヤンされたメッセージに含めるかどうかは、切り替えることができます。このヘッダーを含めることを推奨します。

メッセージ処理設定

ウイルス スキヤン エンジンは、リスナーにより受信される 4 つの独立したメッセージクラスについて、それぞれ別々のアクションを実行して処理するように設定できます。図 12-1 に、ウイルス スキヤン エンジンがイネーブルになっている場合にシステムが実行するアクションをまとめています。

次の各メッセージタイプについて、それぞれ実行するアクションを選択できます。アクションについては後述します（「メッセージ処理アクションの設定の構成」(P.12-9) を参照）。たとえば、ウイルスに感染したメッセージについて、感染した添付ファイルがドロップされ、電子メールの件名が変更されて、カスタム アラートがメッセージの受信者に送信されるように、アンチウイルスを設定できます。

修復されたメッセージの処理

メッセージが完全にスキヤンされ、すべてのウイルスが修復または削除された場合は、そのメッセージは修復されたと見なされます。これらのメッセージはそのまま配信されます。

暗号化されたメッセージの処理

メッセージ内に暗号化または保護されたフィールドがあるために、エンジンがスキヤンを完了できなかった場合は、そのメッセージは暗号化されていると見なされます。暗号化されているとマークされたメッセージも、修復可能です。

暗号化検出のメッセージ フィルタ ルール (「暗号化検出ルール」(P.9-30) を参照) と、「暗号化された」メッセージに対するウイルス スキヤン アクションの違いに注意してください。暗号化メッセージ フィルタ ルールは、PGP または S/MIME で暗号化されたすべてのメッセージを「true」と評価します。暗号化ルールで検出できるのは、PGP および S/MIME で暗号化されたデータのみです。パスワードで保護された ZIP ファイル、もしくは暗号化されたコンテンツを含む Microsoft Word または Excel ドキュメントは検出できません。ウイルス スキヤン エンジンは、パスワードで保護されたメッセージまたは添付ファイルはすべて「暗号化されている」と見なします。



(注)

AsyncOS バージョン 3.8 以前からアップグレードして、Sophos Anti-Virus スキヤンを設定する場合は、アップグレード後に [暗号化されたメッセージの処理 (Encrypted Message Handling)] の項を設定する必要があります。

スキヤンできないメッセージの処理

スキヤン タイムアウト値に到達した場合、または内部エラーによりエンジンが使用不可能になった場合は、メッセージはスキヤンできないと見なされます。スキヤンできないとマークされたメッセージも、修復可能です。

ウイルスに感染したメッセージの処理

システムが添付ファイルをドロップできない、またはメッセージを完全に修復できない場合があります。このような場合は、依然としてウイルスが含まれるメッセージのシステムでの処理方法を設定できます。

暗号化メッセージ、スキヤンできないメッセージ、およびウイルス メッセージの設定オプションは、どれも同じです。

メッセージ処理アクションの設定の構成

適用するアクション

暗号化されたメッセージ、スキヤンできないメッセージ、またはウイルス陽性のメッセージの各タイプについて、全般的にどのアクションを実行するか (メッセージをドロップする、新しいメッセージの添付ファイルとしてメッセージを配信する、メッセージをそのまま配信する、またはメッセージをアンチウイルス隔離エリアに送信する (「隔離およびアンチウイルス スキヤン」(P.12-10) を参照)) を選択します。

感染したメッセージを新しいメッセージの添付ファイルとして配信するようにアプライアンスを設定すると、受信者がオリジナルの感染した添付ファイルをどのように処理するか、選択できるようになります。

メッセージをそのまま配信するか、またはメッセージを新しいメッセージの添付ファイルとして配信することを選択した場合は、追加で次の処理を設定できます。

- メッセージの件名の変更
- オリジナル メッセージのアーカイブ

- 一般的な通知の送信
次のアクションは、GUI の [詳細 (Advanced)] セクションから実行できます。
- メッセージへのカスタム ヘッダーの追加
- メッセージ受信者の変更
- 代替宛先ホストへのメッセージの送信
- カスタムのアラート通知の送信 (受信者宛でのみ)



(注) これらのアクションは、相互に排他的ではありません。ユーザのグループのさまざまな処理ニーズに合わせて、さまざまな着信または発信ポリシーで、これらのアクションを数個またはすべてを、さまざまに組み合わせることができます。これらのオプションを使用した、さまざまなスキャン ポリシーの定義に関する詳細については、後述のセクションおよび「[アンチウイルス設定に関する注意事項](#)」(P.12-14) を参照してください。



(注) 修復されたメッセージに対する拡張オプションは、[カスタム ヘッダーを追加 (Add custom header)] および [カスタム アラート通知を送信 (Send custom alert notification)] の 2 つのみです。その他すべてのメッセージタイプについては、すべての拡張オプションにアクセスできます。

隔離およびアンチウイルス スキャン

隔離フラグの付けられたメッセージは、電子メール パイプラインの残りの処理を継続します。メッセージがパイプラインの末尾に到達すると、メッセージに 1 つ以上の隔離に関するフラグが設定されていれば、該当するキューに入ります。メッセージがパイプラインの末尾に到達しなければ、隔離エリアには配置されません。

たとえば、コンテンツ フィルタはメッセージをドロップまたは返送する場合がありますが、その場合、メッセージは隔離されません。

メッセージの件名ヘッダーの変更

特定のテキスト文字列を前後に追加することで、識別されたメッセージを変更すると、ユーザがより簡単に識別されたメッセージを判別したり、ソートしたりできるようになります。



(注) [メッセージの件名を修正 (Modify message subject)] フィールドでは、空白は無視されません。このフィールドに入力したテキストの後ろまたは前にスペース追加することで、オリジナルのメッセージ件名と、追加テキストを分けることができます (追加テキストをオリジナルの件名の前に追加する場合は追加テキストの前、オリジナルの件名の後ろに追加する場合は追加テキストの後ろにスペースを追加します)。たとえば、[WARNING: VIRUS REMOVED] というテキストをオリジナルの件名の前に追加する場合は、この後ろに数個のスペースを追加します。

デフォルトのテキストは次のとおりです。

表 12-2 アンチウイルス件名変更のデフォルト件名行テキスト

判断	件名に追加されるデフォルトのテキスト
暗号化されている	[WARNING: MESSAGE ENCRYPTED]
感染している	[WARNING: VIRUS DETECTED]

表 12-2 アンチウイルス件名変更のデフォルト件名行テキスト (続き)

修復されている	[WARNING: VIRUS REMOVED]
スキュン不可	[WARNING: A/V UNSCANNABLE]

複数のステートが該当するメッセージについては、アプライアンスがメッセージに対して実行したアクションをユーザに知らせる、複数部分で構成された通知メッセージが作成されます (たとえば、ユーザに対してはメッセージがウイルスを修復されていると通知されていても、メッセージの他の部分は暗号化されている場合があります)。

オリジナル メッセージのアーカイブ

システムにより、ウイルスが含まれている (または含まれている可能性がある) と判断されたメッセージは、「avarchive」ディレクトリにアーカイブできます。この形式は、mbox 形式のログ ファイルです。「Anti-Virus Archive」ログ サブスクリプションを設定して、ウイルスが含まれているメッセージまたは完全にスキュンできなかったメッセージをアーカイブする必要があります。詳細については、第 34 章「ロギング」を参照してください。



(注) GUI では、場合により [詳細 (Advanced)] リンクをクリックして [オリジナルのメッセージをアーカイブ (Archive original message)] を表示する必要があります。

通知の送信

システムにより、メッセージにウイルスが含まれていると識別されたときに、デフォルトの通知を送信者、受信者、およびその他のユーザまたはそのいずれかに送信できます。その他のユーザを通知対象に指定する場合は、複数のアドレスをコンマで区切ります (CLI および GUI の両方)。デフォルトの通知、メッセージは次のとおりです。

表 12-3 アンチウイルス通知のデフォルト通知

判断	通知
修復されている	The following virus(es) was detected in a mail message: <virus name(s)> Actions taken: Infected attachment dropped. (または Infected attachment repaired.)
暗号化されている	The following message could not be fully scanned by the anti-virus engine due to encryption.
スキュン不可	The following message could not be fully scanned by the anti-virus engine.
感染している	The following unrepairable virus(es) was detected in a mail message: <virus name(s)>.

メッセージへのカスタム ヘッダーの追加

アンチウイルス スキュン エンジンによってスキュンされたすべてのメッセージに追加する、追加のカスタム ヘッダーを定義できます。[はい (Yes)] をクリックし、ヘッダー名およびテキストを定義します。

また、skip-viruscheck アクションを使用するフィルタを作成して、特定のメッセージはウイルス スキュンを回避するようにもできます。「アンチウイルス システムのバイパス アクション」(P.9-66) を参照してください。

メッセージ受信者の変更

メッセージの受信者を変更して、メッセージが別のアドレスに送信されるようにできます。[はい (Yes)] をクリックして、新しい受信者のアドレスを入力します。

代替宛先ホストへのメッセージの送信

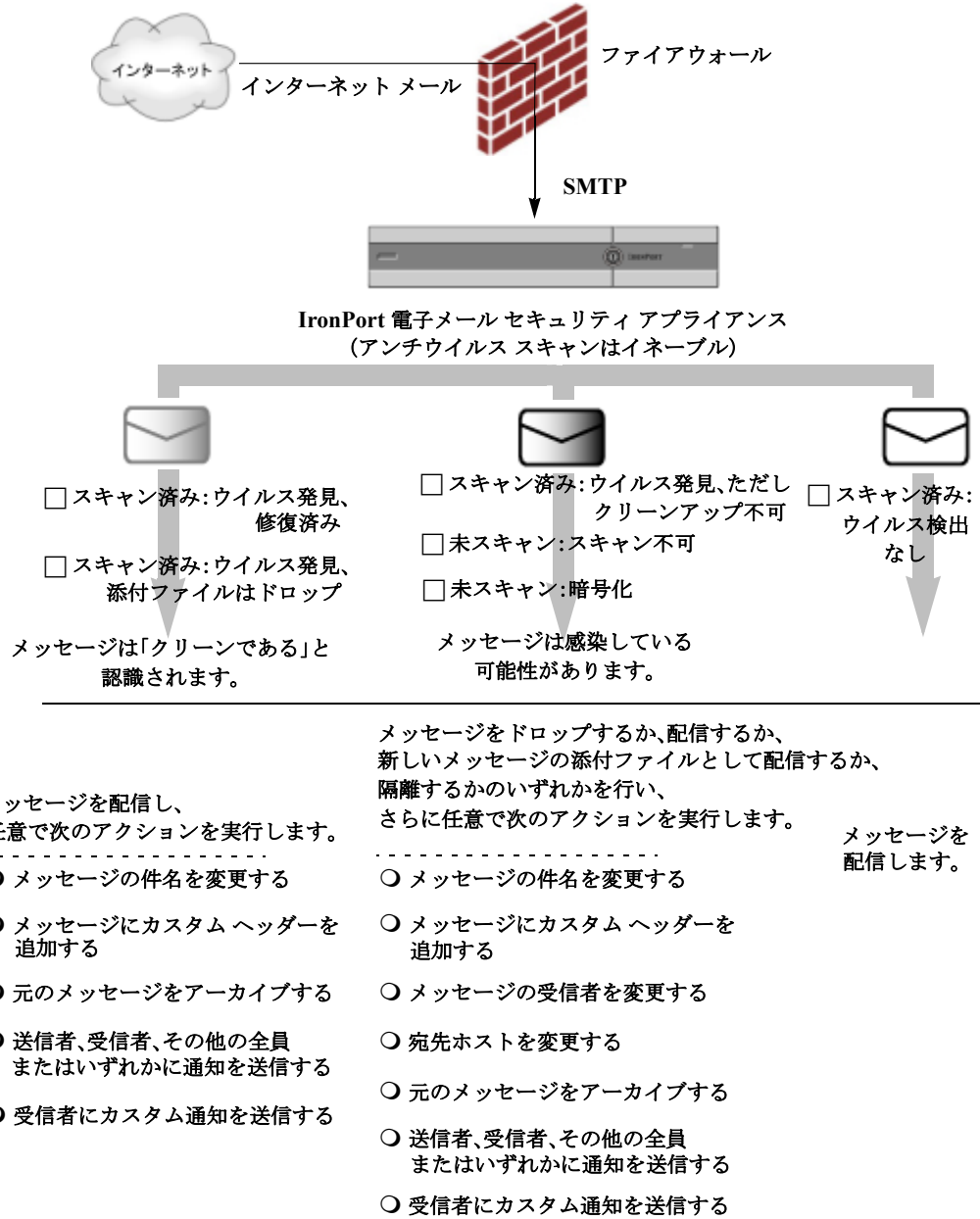
暗号化されたメッセージ、スキャンできないメッセージ、またはウイルスに感染したメッセージについて、異なる受信者または宛先ホストに通知を送信するように選択できます。[はい (Yes)] をクリックして代替アドレスまたはホストを入力します。

たとえば、疑わしいメッセージを管理者のメールボックスまたは専用のメール サーバに送信して、後で調査することができます。受信者が複数のメッセージの場合は、代替受信者に送信されるコピーは 1 つのみです。

カスタムのアラート通知の送信（受信者宛てのみ）

受信者にカスタム通知を送信できます。そのためには、この設定を構成する前に、まずカスタム通知を作成する必要があります。詳細については、「[テキストリソースについて](#)」(P.18-8) を参照してください。

図 12-1 ウイルス スキヤンを実行したメッセージの処理に関するオプション



(注)

デフォルトでは、アンチウイルス スキヤンは、WHITELIST 送信者グループが参照するパブリック リスナーの \$TRUSTED メール フロー ポリシーでイネーブルになっています。「[メール フロー ポリシーを使用した電子メール送信者のアクセス ルールの定義](#)」(P.7-8) を参照してください。

送信者および受信者のグループごとのアンチウイルス ポリシーの設定

メール ポリシーのユーザごとのアンチウイルス設定を編集する処理は、着信メールと発信メールで基本的に同じです。

個々のポリシー（デフォルト以外）には、[デフォルトを使用（Use Default）] 設定値という追加のフィールドがあります。この設定は、デフォルトのメール ポリシー設定を継承するように選択します。

アンチウイルス アクションは、[受信メール ポリシー（Incoming Mail Policies）] または [送信メール ポリシー（Outgoing Mail Policies）] を使用して受信者ごとにイネーブルにします。GUI または CLI の `policyconfig > antivirus` コマンドを使用してメール ポリシーを設定できます。アンチウイルス設定をグローバルにイネーブルにした後は、作成した各メール ポリシーに対して、これらのアクションを別々に設定します。さまざまなメール ポリシーに対して、異なるアクションを設定できます。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [受信メール ポリシー（Incoming Mail Policies）] または [送信メール ポリシー（Outgoing Mail Policies）] ページに移動します。

ステップ 2 ポリシーを設定するアンチウイルス セキュリティ サービスのリンクをクリックします。



(注) デフォルト ポリシーの設定を編集するには、デフォルト行のリンクをクリックします。

ステップ 3 [はい（Yes）] または [デフォルトを使用（Use Default）] をクリックして、そのポリシーのアンチウイルス スキャンをイネーブルにします。

このページの最初の設定値は、そのポリシーに対してサービスがイネーブルであるかどうかを定義します。[無効（Disable）] をクリックしてすべてのサービスをディセーブルにできます。

デフォルト以外のメール ポリシーでは、[はい（Yes）] を選択することで、[修復されたメッセージ（Repaired Messages）]、[暗号化されたメッセージ（Encrypted Messages）]、[スキャン不能なメッセージ（Unscannable Messages）]、および [ウイルス感染したメッセージ（Virus Infected Messages）] 領域内の各フィールドがイネーブルになります。

ステップ 4 アンチウイルス スキャン エンジンを選択します。McAfee または Sophos のエンジンを選択できます。

ステップ 5 [メッセージのスキャン（Message Scanning）] 設定を構成します。

詳細については、「[メッセージ スキャン設定](#)（P.12-7）を参照してください。

ステップ 6 [修復されたメッセージ（Repaired Messages）]、[暗号化されたメッセージ（Encrypted Messages）]、[スキャン不能なメッセージ（Unscannable Messages）]、および [ウイルス感染したメッセージ（Virus Infected Messages）] の設定を構成します。

「[メッセージ処理設定](#)（P.12-8） および 「[メッセージ処理アクションの設定の構成](#)（P.12-9）を参照してください。

ステップ 7 [送信（Submit）] をクリックします。

ステップ 8 変更内容を確定します。

アンチウイルス設定に関する注意事項

添付ファイルのドロップ フラグにより、アンチウイルス スキャンの動作は大きく異なります。システムが、[ウイルスが検出され修復できない場合、感染した添付ファイルをドロップする（Drop infected attachments if a virus is found and it could not be repaired）] ように設定されている場合は、ウイルス性またはスキャンできない MIME 部分はすべてメッセージから削除されます。そのため、アンチウイルス スキャンの出力は、ほとんど常にクリーンなメッセージになります。GUI ペインに表示された [スキャン不能なメッセージ（Unscannable Messages）] で定義されるアクションは、実行されることはほとんどありません。

[ウイルス スキヤンのみ (Scan for Viruses only)] の環境では、これらのアクションは悪質なメッセージ部分をドロップすることで、メッセージを「クリーンに」します。RFC822 ヘッダーに限り、RFC822 ヘッダー自体が攻撃された、またはその他の問題に遭遇した場合は、スキヤンできなかった場合のアクションが実行されます。ただし、アンチウイルス スキヤンが [ウイルス スキヤンのみ (Scan for Viruses only)] に設定されていながら、[ウイルスが検出され修復できない場合、感染した添付ファイルをドロップする (Drop infected attachments if a virus is found and it could not be repaired)] が選択されていない場合は、スキヤンできなかった場合のアクションが実行される可能性は非常に高くなります。

表 12-4 に、一般的なアンチウイルス設定オプションを示します。

表 12-4 一般的なアンチウイルス設定オプションの表示

状況	アンチウイルス設定
<p>ウイルスが広範囲に発生</p> <p>ウイルス性のメッセージは単純にシステムからドロップされ、他の処理が実行されることはほとんどありません。</p>	<p>添付ファイルのドロップ：しない。</p> <p>スキヤン：Scan-Only。</p> <p>クリーンアップされたメッセージ：配信する。</p> <p>スキヤンできないメッセージ：メッセージをドロップする。</p> <p>暗号化されたメッセージ：管理者に送るか隔離して、後で確認する。</p> <p>ウイルス性のメッセージ：メッセージをドロップする。</p>
<p>リベラルなポリシー</p> <p>できる限り多くのドキュメントを送信します。</p>	<p>添付ファイルのドロップ：する。</p> <p>スキヤン：Scan and Repair。</p> <p>クリーンアップされたメッセージ：[VIRUS REMOVED] として配信する。</p> <p>スキヤンできないメッセージ：添付ファイルとして転送する。</p> <p>暗号化されたメッセージ：マークして転送する。</p> <p>ウイルス性のメッセージ：隔離するか、マークして転送する。</p>

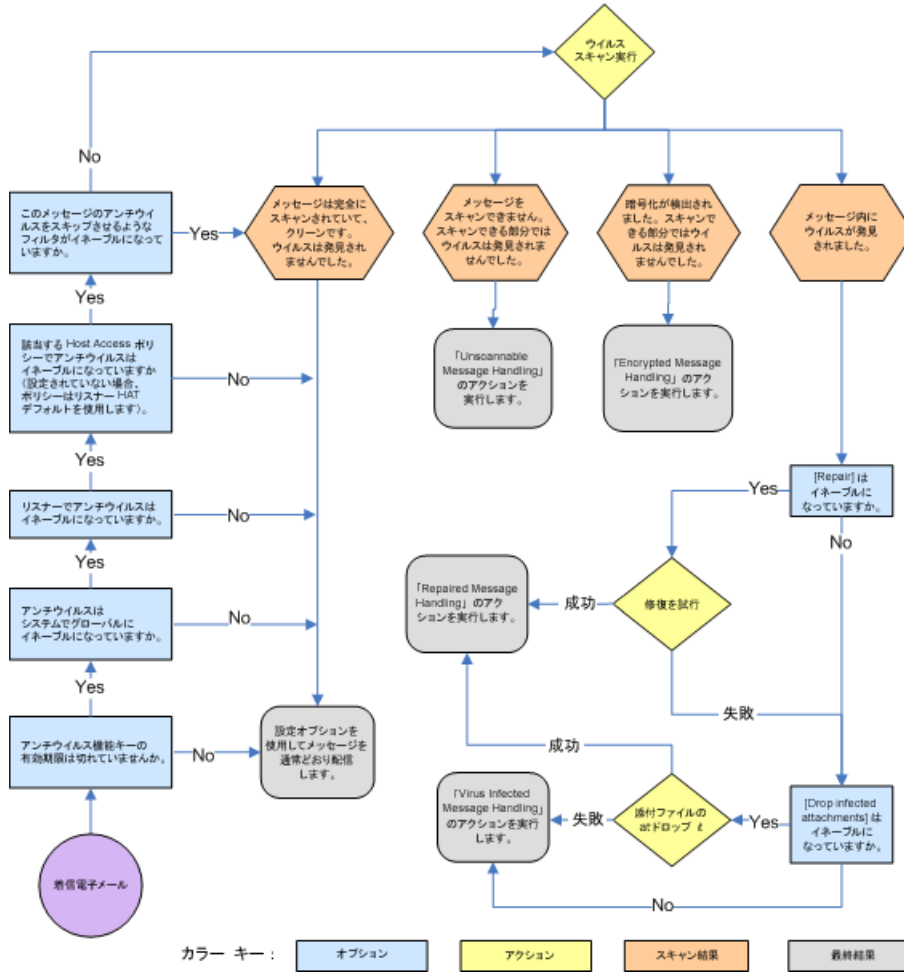
表 12-4 一般的なアンチウイルス設定オプションの表示 (続き)

より保守的なポリシー	<p>添付ファイルのドロップ：する。</p> <p>スキヤン：Scan and Repair。</p> <p>クリーンアップされたメッセージ：[VIRUS REMOVED] として配信する</p> <p>(より慎重なポリシーでは、クリーンアップしたメッセージをアーカイブします)。</p> <p>スキヤンできないメッセージ：通知を送る、隔離する、またはドロップしてアーカイブする。</p> <p>暗号化されたメッセージ：マークして転送する、またはスキヤンできないメッセージとして処理する。</p> <p>ウイルス性のメッセージ：アーカイブしてドロップする。</p>
<p>保守的なポリシーでレビューを実施する</p> <p>ウイルス メッセージの可能性のあるものは、後で管理者が内容を確認できるように、隔離メールボックスに送信されます。</p>	<p>添付ファイルのドロップ：しない。</p> <p>スキヤン：Scan-Only。</p> <p>クリーンアップされたメッセージ：配信する (通常、このアクションは実行されません)。</p> <p>スキヤンできないメッセージ：添付ファイル、alt-src-host、または alt-rcpt-to アクションとして転送する。</p> <p>暗号化されたメッセージ：スキヤンできないメッセージとして処理する。</p> <p>ウイルス性のメッセージ：隔離するか管理者に転送する。</p>

アンチウイルス アクションのフロー ダイアグラム

図 12-2 (P.12-17) に、アンチウイルス アクションおよびオプションが、アプライアンスで処理されるメッセージにどのように影響を及ぼすかを示します。

図 12-2 アンチウイルス アクションのフロー ダイアグラム



(注)

マルチレイヤ アンチウイルス スキャンを設定した場合は、Cisco アプライアンスは最初に McAfee エンジンでウイルス スキャンを実行し、次に Sophos エンジンでウイルス スキャンを実行します。アプライアンスは、McAfee エンジンがウイルスを検出しない限りは、両方のエンジンを使用してメッセージをスキャンします。McAfee エンジンがウイルスを検出した場合は、Cisco アプライアンスは、メール ポリシーで定義されたアンチウイルス アクション（修復、隔離など）を実行します。

アンチウイルス スキャンをテストするためにアプライアンスにメールを送信する

手順

ステップ 1 メール ポリシーのウイルス スキャンをイネーブルにします。

■ アンチウイルス スキャンをテストするためにアプライアンスにメールを送信する

[セキュリティ サービス (Security Services)] > [Sophos] または [McAfee ウイルス対策 (McAfee Anti-Virus)] ページ、または `antivirusconfig` コマンドを使用してグローバル設定を行ってから、[電子メールセキュリティマネージャ (Email Security Manager)] ページ (GUI) または `policyconfig` の `antivirus` サブコマンドを使用して、特定のメール ポリシーの設定を構成します。

ステップ 2 標準のテキスト エディタを開き、次の文字列をスペースまたは改行を使用せず、1 行で入力します。

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```



(注) 上記の行は、テキスト エディタ ウィンドウで 1 行で表示される必要があります。そのため、必ずテキスト エディタのウィンドウは最大にして、改行はすべて削除します。また、テストメッセージ開始部の「X5O...」には、数字の「0」ではなく必ず文字の「O」を入力します。

このマニュアルをコンピュータでお読みの場合は、PDF ファイルまたは HTML ファイルから直接この行をコピーして、テキスト エディタに貼ることができます。この行をコピーする場合は、必ずすべての余分な復帰文字またはスペースを削除します。

ステップ 3 ファイルを `EICAR.COM` という名前で保存します。
ファイルのサイズは 68 ~ 70 バイトになります。



(注) このファイルはウイルスではありません。拡散したり、他のファイルに感染したり、またはコンピュータに害を与えたりするものではありません。ただし、他のユーザにアラームを与えないために、テストを終了したらこのファイルは削除してください。

ステップ 4 ファイル `EICAR.COM` を電子メール メッセージに添付して、ステップ 1 で設定したメール ポリシーに一致するリスナーに送信します。

テストメッセージで指定した受信者が、リスナーで許可されることを確認します (詳細については、「[メッセージを受け入れるドメインおよびユーザの追加](#)」(P.8-3) を参照してください)。

Cisco 以外のゲートウェイ (たとえば Microsoft Exchange サーバ) で発信メールに対するウイルス スキャン ソフトウェアをインストールしている場合は、ファイルを電子メールで送信することが難しいことがあるため、注意してください。



(注) テスト ファイルは、常に修復不可能としてスキャンされます。

ステップ 5 リスナー上のウイルス スキャンに設定したアクションを評価して、そのアクションがイネーブルであり、予想どおりに動作していることを確認します。

これは、次のいずれかのアクションを実行することで、最も簡単に達成できます。

- ウイルス スキャンを、[スキャンして修復 (Scan and Repair)] モードまたは [スキャンのみ (Scan Only)] モードにして、添付ファイルをドロップしないように設定します。

EICAR テスト ファイルを添付ファイルとした電子メールを送信します。

実行されたアクションが、[ウイルス感染したメッセージ (Virus Infected Messages)] の処理で設定した内容 (「[ウイルスに感染したメッセージの処理](#)」(P.12-9) の設定) と一致していることを確認します。

- ウイルス スキャンを、[スキャンして修復 (Scan and Repair)] モードまたは [スキャンのみ (Scan Only)] モードにして、添付ファイルをドロップするように設定します。

EICAR テスト ファイルを添付ファイルとした電子メールを送信します。

実行されたアクションが、[修復されたメッセージ (Repaired Messages)] の処理で設定した内容 (「修復されたメッセージの処理」(P.12-8) の設定) と一致していることを確認します。

アンチウイルス スキャンのテスト用ウイルス ファイルの取得に関する詳細については、次の URL を参照してください。

http://www.eicar.org/anti_virus_test_file.htm

このページでは、ダウンロード可能な 4 つのファイルを提供しています。クライアント側にウイルス スキャン ソフトウェアをインストールしている場合は、これらのファイルをダウンロードして抽出するのは難しいため、注意してください。

ウイルス定義ファイルの更新

- HTTP を使用した Anti-Virus アップデートの取得について
- アップデート サーバの設定
- モニタリングおよび手動での Anti-Virus アップデート チェック
- アプライアンスでのアンチウイルス ファイルの更新の確認

HTTP を使用した Anti-Virus アップデートの取得について

Sophos および McAfee は新たに識別されたウイルスのウイルス定義を頻繁にアップデートします。これらの更新は、アプライアンスに渡す必要があります。

デフォルトでは、Cisco アプライアンスは、5 分ごとにアップデートをチェックするように設定されています。Sophos および McAfee のアンチウイルス エンジンの場合は、サーバは動的 Web サイトからアップデートします。

アップデートをアプライアンスにダウンロードしている間は、アップデートのタイムアウトにはなりません。アップデートのダウンロードが長時間中断すると、ダウンロードがタイムアウトします。

システムがタイムアウトせずに、アップデートが完了するまで待機する最大時間は、アンチウイルス アップデート間隔より 1 分短い値に定義された、動的な値です ([セキュリティ サービス (Security Services)] > [サービスのアップデート (Service Updates)]) で定義されています。この設定値は、接続速度の遅いアプライアンスが、完了まで 10 分を超える大きいアップデートをダウンロードする場合に役立ちます。

アップデート サーバの設定

[セキュリティ サービス (Security Services)] > [サービスのアップデート (Service Updates)] ページでウイルス更新設定を設定できます。たとえば、システムがアンチウイルスの更新を受ける方法や更新を確認する頻度を設定できます。追加設定に関する詳細については、「サービスのアップデート」(P.29-22) を参照してください。

モニタリングおよび手動での Anti-Virus アップデート チェック

[セキュリティ サービス (Security Services)] > [Sophos] または [McAfee] ページまたは CLI の `antivirusstatus` コマンドを使用して、アプライアンスに最新のアンチウイルス エンジンおよび識別ファイルがインストールされていることを確認し、いつ最終のアップデートが実行されたか確認できます。

また、手動でアップデートを実行することもできます。

GUI を使用した手動での Anti-Virus エンジンの更新

手順

-
- ステップ 1** [セキュリティ サービス (Security Services)] > [Sophos ウイルス対策 (Sophos Anti-Virus)] または [McAfee ウイルス対策 (McAfee Anti-Virus)] ページに移動します。
- ステップ 2** [現在の McAfee/Sophos ウイルス対策ファイル (Current McAfee/Sophos Anti-Virus Files)] テーブルで、[今すぐ更新 (Update Now)] をクリックします。
- アプライアンスは最新のアップデートを確認してダウンロードします。
-

CLI を使用した手動での Anti-Virus エンジンの更新

CLI の `antivirusstatus` コマンドを使用してウイルス ファイルのステータスをチェックし、`antivirusupdate` コマンドを使用してアップデートを手動でチェックします。

```
example.com> antivirusstatus

Choose the operation you want to perform:

- MCAFEE - Display McAfee Anti-Virus version information
- SOPHOS - Display Sophos Anti-Virus version information

> sophos

SAV Engine Version      3.2.07.286_4.58
  IDE Serial            0
  Last Engine Update    Base Version
  Last IDE Update       Never updated

example.com> antivirusupdate

Choose the operation you want to perform:

- MCAFEE - Request updates for McAfee Anti-Virus
- SOPHOS - Request updates for Sophos Anti-Virus

>sophos
```

```
Requesting check for new Sophos Anti-Virus updates
```

```
example.com>
```

アプライアンスでのアンチウイルス ファイルの更新の確認

アップデート ログを表示して、アンチウイルス ファイルが、すべて正常にダウンロード、抽出、またはアップデートされたことを確認できます。アップデート ログ サブスクリプションの最終的なエントリを表示して、ウイルス アップデートが取得できていることを確認するには、`tail` コマンドを使用します。



CHAPTER 13

アンチスパム

- 「スパム対策スキャンの概要」 (P.13-1)
- 「メッセージがスパムかどうかスキャンするためのアプライアンスの設定方法」 (P.13-2)
- 「IronPort Anti-Spam フィルタリング」 (P.13-3)
- 「CiscoIntelligent Multi-Scan フィルタリング」 (P.13-6)
- 「スパム対策ポリシーの定義」 (P.13-8)
- 「スパム フィルタからのアプライアンス生成メッセージの保護」 (P.13-13)
- 「スパム対策スキャン中に追加されるヘッダー」 (P.13-14)
- 「誤って分類されたメッセージの Cisco Systems への報告」 (P.13-14)
- 「着信リレー構成における送信者の IP アドレスの決定」 (P.13-14)
- 「モニタリング ルールのアップデート」 (P.13-23)
- 「スパム対策のテスト」 (P.13-24)

スパム対策スキャンの概要

スパム対策プロセスは、設定するメール ポリシーに基づいて着信（および発信）のメールの電子メールをスキャンします。

- 1 つ以上のスキャン エンジンがフィルタ モジュールによってメッセージをスキャンします。
- スキャン エンジンは、各メッセージにスコアを割り当てます。スコアが高いほど、メッセージがスパムである可能性が高くなります。
- スコアに基づいて、各メッセージは次のいずれかに分類されます。
 - スパムでない
 - 正規の送信元からの不要なマーケティング電子メール
 - 疑わしいスパム
 - 確定されたスパム
- 結果に基づいてアクションが実行されます。

確定されたスパム、陽性と疑わしいスパム、または不要なマーケティング メッセージとして識別されたメッセージに対して実行されるアクションは、相互に排他的ではありません。ユーザのグループのさまざまな処理ニーズに合わせて、さまざまな着信または発信ポリシーで、これらのアクションの数個またはすべてを、さまざまに組み合わせることができます。同じポリシーで、陽性と

判定されたスパムと陽性と疑わしいスパムを別々に扱うことができます。たとえば、陽性と判定されたスパムであるメッセージをドロップする一方で、陽性と疑わしいスパムメッセージを隔離する必要がある場合があります。

各メール ポリシーで、カテゴリの複数のしきい値を指定し、各カテゴリに対して実行するアクションを指定できます。異なるメール ポリシーに異なるユーザを割り当て、各ポリシーに対して異なるスキャン エンジン、スパム定義しきい値、スパム処理アクションを定義できます。



(注) スпам対策スキャンの適用方法および適用時期の詳細については、「電子メールパイプラインとセキュリティ サービス」(P.4-7) を参照してください。

スパム対策ソリューション

Cisco アプライアンスは次のスパム対策ソリューションを提供します。

- 「IronPort Anti-Spam フィルタリング」(P.13-3)
- 「CiscoIntelligent Multi-Scan フィルタリング」(P.13-6)

Cisco アプライアンスの両方のソリューションを認可して有効化できますが、特定のメール ポリシーでは 1 つしか使用できません。ユーザのグループごとに異なるスパム対策ソリューションを指定できません。

メッセージがスパムかどうかスキャンするためのアプライアンスの設定方法

	操作内容	詳細
ステップ 1	電子メール セキュリティ アプライアンスのスパム対策スキャンをイネーブルにします。 (注) この表の残りの手順は、両方のスキャン エンジンにオプションに適用されます。	Cisco IronPort Anti-Spam および Intelligent Multi-Scan の両方のライセンス キーがある場合は、アプライアンスの両方のソリューションをイネーブルにできます。 <ul style="list-style-type: none"> • 「IronPort Anti-Spam フィルタリング」(P.13-3) • 「CiscoIntelligent Multi-Scan フィルタリング」(P.13-6)
ステップ 2	ローカルの電子メール セキュリティ アプライアンスからスパムを隔離するか、または、セキュリティ管理アプライアンスの外部隔離を使用するかどうかを設定します。	<ul style="list-style-type: none"> • 「スパム隔離の設定」(P.27-19) • 「外部スパム隔離の設定」(P.38-3)
ステップ 3	メッセージのスパムをスキャンするユーザ グループを定義します。	「送信者および受信者のグループのメール ポリシーの作成」(P.10-8)
ステップ 4	定義したユーザ グループのスパム対策スキャン ルールを設定します。	「スパム対策ポリシーの定義」(P.13-8)
ステップ 5	特定のメッセージに Cisco Anti-Spam スキャンをとばして、skip-spamcheck アクションを使用するメッセージ フィルタを作成します。	「アンチスパム システムのバイパス アクション」(P.9-65)

	操作内容	詳細
ステップ6	(推奨) SenderBase レピュテーション スコアに基づいて接続を拒否しない場合でも、SenderBase レピュテーション スコアを各受信メール フロー ポリシーにイネーブルにします。	各受信メール フロー ポリシー用に、[フロー制御に SenderBase を使用 (Use SenderBase for Flow Control)] がオンになっていることを確認します。 「メール フロー ポリシーを使用した着信メッセージのルールの定義」(P.7-15) を参照してください。
ステップ7	電子メール セキュリティ アプライアンス が着信電子メールを受信するために外部送信者に直接接続しない代わりに、メール交換、メール転送エージェント、ネットワークの他のマシンからメッセージを受信する場合は、リレーされた着信メッセージに元の送信者の IP アドレスが含まれていることを確認します。	「着信リレー構成における送信者の IP アドレスの決定」(P.13-14)
ステップ8	アプライアンスで正しく生成されたアラートや他のメッセージがスパムとして間違えて識別されないようにします。	「スパム フィルタからのアプライアンス生成メッセージの保護」(P.13-13)
ステップ9	設定をテストします。	「スパム対策のテスト」(P.13-24)
ステップ10	(任意) サービスの更新を設定します (スパム対策ルールも含め)。	両方のスパム対策ソリューションのスキャン ルールが Cisco 更新サーバからデフォルトで取得されます。 <ul style="list-style-type: none"> 「サービスのアップデート」(P.29-22) 「プロキシ サーバを経由したアップデート」(P.29-22) 「アップグレードおよびアップデートをダウンロードするためのサーバ設定」(P.29-22)

IronPort Anti-Spam フィルタリング

評価キー

Cisco アプライアンスには、Cisco Anti-Spam ソフトウェアの 30 日間有効な評価キーが付属しています。このキーは、システム セットアップ ウィザードまたは [セキュリティ サービス (Security Services)] > [IronPort Anti-Spam] ページ (GUI) か、systemsetup コマンドまたは antispamconfig コマンド (CLI) で、ライセンス契約書を受諾して初めてイネーブルになります。ライセンス契約書に同意すると、デフォルトの着信メール ポリシーに対してデフォルトで Cisco Anti-Spam がイネーブルになります。設定した管理者アドレス (システム設定ウィザード、「手順 2 : システム」(P.3-15) を参照) に対して、Cisco Anti-Spam のライセンスの期限が 30 日後に切れることを通知するアラートの送信も行われます。アラートは、期限切れの 30、15、5、および 0 日前に送信されます。30 日間の評価期間後もこの機能をイネーブルにする場合の詳細については、Cisco の営業担当者にお問い合わせください。残りの評価期間は、[システム管理 (System Administration)] > [ライセンス キー (Feature Keys)] ページを表示するか、または featurekey コマンドを発行することによって確認できます (詳細については、「ライセンス キー」(P.29-5) を参照してください)。

Cisco Anti-Spam : 概要

IronPort Anti-Spam では、スパム、フィッシング、ゾンビ攻撃などの既知のあらゆる脅威に対応するだけでなく、「419」詐欺など検出が難しく、少量で、短期間の電子メール脅威にも対応します。さらに、IronPort Anti-Spam では、ダウンロード URL または実行ファイルを介して不正なコンテンツを配布するスパム攻撃など、新しい脅威や混合された脅威を識別します。

これらの脅威を特定するには、IronPort Anti-Spam はそのメッセージ コンテンツの完全なコンテキスト、メッセージの構築方法、送信者のレピュテーション、メッセージでなどによりアドバタイズされる Web サイトのレピュテーションを検査します。IronPort Anti-Spam は世界最大の電子メールおよび Web モニタリング ネットワークである SenderBase を最大限に活用する電子メールおよび Web レピュテーション データを組み合わせて、開始と同時に新しい攻撃を検出します。

IronPort Anti-Spam は次の分野における 100,000 以上のメッセージ属性を分析します。

- 電子メール レピュテーション：このメッセージの送信者は誰か。
- メッセージの内容：このメッセージに含まれている内容は何か。
- メッセージ構造：このメッセージはどのように構築されているか。
- Web レピュテーション：遷移先はどこか。

多角的な関係を分析することにより、精度を維持しながら、システムは多様な脅威を検出できます。たとえば、正規金融機関から送信されたと断言する内容を持ちながら、消費者向けのブロードバンド ネットワークに属している IP アドレスから送信されたメッセージや、ゾンビ PC によってホストされている URL を含むメッセージは、疑わしいメッセージであると見なされます。これとは対照的に、肯定的なレピュテーションが与えられている製薬会社からのメッセージは、スパムとの関連性が強い単語を含んでいたとしても、スパムであるとタグ付けされません。

国際地域のスパムのスキャン

Cisco Anti-Spam は世界的に有効な、ロケール固有コンテンツ対応の脅威検出技術を使用します。また、リージョナル ルール プロファイルを使用して特定の地域のスパム対策スキャンを最適化できます。

- 米国以外の特定の地域から大量のスパムを受信すると、リージョナル ルール プロファイルを使用してその地域のスパムを停止することもできます。

たとえば、中国および台湾で受信するスパムでは、繁体字および簡体字の割合が高くなります。中国語のリージョナル ルールは、このタイプのスパムに合わせて最適化されています。主に中国本土、台湾、香港のメールを受信する場合、シスコでは、スパム対策エンジンに含まれる中国のリージョナル ルール プロファイルを使用することを強く推奨しています。

- スパムが米国または他の特定の地域から主に来る場合、スパムの他のタイプの検出率を低下する可能性があるため、リージョナル ルールをイネーブルにしないでください。これは、リージョナル ルール プロファイルが特定地域向けスパム対策エンジンを最適化するためです。

IronPort Anti-Spam スキャンを設定するときにリージョナル ルール プロファイルをイネーブルにできます。

関連項目

- 「IronPort Anti-Spam スキャンの設定」(P.13-5)

IronPort Anti-Spam スキャンの設定



(注)

IronPort Anti-Spam をシステム セットアップ時にイネーブルにすると、グローバル設定のデフォルト値を使用し、デフォルトの着信メール ポリシーでイネーブルにされます。

はじめる前に

- リージョナル スキャンを使用するかどうかを設定します。「[国際地域のスパムのスキャン](#)」(P.13-4) を参照してください。

手順

- ステップ 1** [セキュリティ サービス (Security Services)] > [IronPort Anti-Spam] を選択します。
- ステップ 2** システム セットアップ ウィザードで [IronPort Anti-Spam] をイネーブルにしなかった場合：
 - [有効 (Enable)] をクリックします。
 - ライセンス契約書ページの下部にスクロールし、[承認 (Accept)] をクリックしてライセンス契約に合意します。
- ステップ 3** [グローバル設定を編集 (Edit Global Settings)] をクリックします。
- ステップ 4** [IronPort Anti-Spam スキャンを有効にする (Enable IronPort Anti-Spam Scanning)] チェックボックスを選択します。

このボックスをオンにすると、アプライアンスの機能がグローバルにイネーブルになります。
- ステップ 5** スпам送信者から続々と送信される大量メッセージをスキャンする能力を備えながらも、アプライアンスのスループット最適化を図るため、Cisco Anti-Spam によるメッセージのスキャンのしきい値を設定します。

オプション	説明
メッセージの スキャンのし きい値 (Message Scanning Thresholds)	<p>a. [次の件数未満のメッセージを常にスキャンする (Always scan messages smaller than)] に値を入力します。推奨値は 512 Kb 以下です。「初期終了」の場合を除き、<i>always scan</i> サイズより小さいメッセージは完全にスキャンします。このサイズより大きいメッセージは、<i>never scan</i> サイズより小さい場合、部分的にスキャンします。</p> <p><i>always scan</i> メッセージ サイズは 3 MB を超えないようにしてください。値が大きくなると、パフォーマンスが低下する可能性があります。</p> <p>b. [次の件数を超えるメッセージはスキャンしない (Never scan messages larger than)] に値を入力します。推奨値は 1024 Kb 以下です。このサイズより大きいメッセージは Cisco Anti-Spam によってスキャンされず、<code>X-IronPort-Anti-Spam-Filtered: true</code> というヘッダーはメッセージに追加されません。</p> <p><i>never scan</i> メッセージ サイズは 10 MB を超えないようにしてください。値が大きくなると、パフォーマンスが低下する可能性があります。</p> <p><i>always scan</i> サイズより大きいか、または <i>never scan</i> サイズより小さいメッセージについては、限定的な高速スキャンを実行します。</p> <p>(注) アウトブレイク フィルタの最大メッセージ サイズが Cisco Anti-Spam の <i>always scan</i> メッセージよりも大きい場合、アウトブレイク フィルタの最大サイズよりも小さいメッセージは完全にスキャンされます。</p>
1 つのメッセ ージのスキャン のタイムアウト (Timeout for Scanning Single Message)	<p>メッセージをスキャンするときにタイムアウトを待機する秒数を入力します。</p> <p>1 ~ 120 の整数を入力します。デフォルト値は 60 秒です。</p>
リージョナル スキャン (Regional Scanning)	<p>リージョナル スキャンをイネーブルまたはディセーブルにしたり、該当する場合は地域を選択します。</p> <p>指定した地域から大量の電子メールを受信した場合にのみこの機能をイネーブルにします。この機能では特定のリージョンに合わせてアンチスパム エンジンが最適化されるため、他のタイプのスパムについては検出率の低下を招くおそれがあります。</p>

ステップ 6 変更内容を送信し、確定します。

CiscoIntelligent Multi-Scan フィルタリング

CiscoIntelligent Multi-Scan では、Cisco Anti-Spam を含めた複数のスキャン対策エンジンを組み込むことにより、多層スパム対策ソリューションを実現しています。

Cisco Intelligent Multi-Scan によって処理された場合：

- メッセージは、サードパーティ製スパム対策エンジンによって最初にスキャンされます。
- Cisco Intelligent Multi-Scan は次に、メッセージおよびサードパーティ製エンジンによる判定を Cisco Anti-Spam に渡されて、最終判定が下されます。

- Cisco Anti-Spam がスキャンを実行した後、結合された複数のスキャン スコアを AsyncOS に返します。
- Cisco スпам対策の低い誤検出率を維持したまま、サードパーティ製スキャン エンジンおよび Cisco Anti-Spam 結果を組み合わせることで、より多くのスパムが検出されます。

Cisco Intelligent Multi-Scan で使用されるスキャン エンジンの順序は設定できません。Cisco Anti-Spam は、常に最後にメッセージをスキャンするエンジンであり、サードパーティ製エンジンによってスパムであると判定されたメッセージを Cisco Intelligent Multi-Scan がスキップすることはありません。

Cisco Intelligent Multi-Scan を持つ複数のスキャンを使用すると、システムのスループットが低下する場合があります。詳細については、Cisco サポート担当者にお問い合わせください。



(注)

Intelligent Multi-Scan ライセンス キーによって、アプライアンスで Cisco Anti-Spam もイネーブルになります。その結果、メール ポリシーで Cisco Intelligent Multi-Scan または Cisco Anti-Spam のいずれかをイネーブルにできるようになります。

Cisco Intelligent Multi-Scan の設定



(注)

Cisco Intelligent Multi-Scan をシステム セットアップ時にイネーブルにすると、グローバル設定のデフォルト値を使用し、デフォルトの着信メール ポリシーでイネーブルにされます。

はじめる前に

この機能のライセンス キーをアクティブにします。「[ライセンス キー](#)」(P.29-5) を参照してください。これを行なった場合にだけ [IronPort Intelligent Multi-Scan] オプションが表示されます。

手順

- ステップ 1** [セキュリティ サービス (Security Services)] > [IronPort Multi-Scan] を選択します。
- ステップ 2** システム セットアップ ウィザードで Cisco Intelligent Multi-Scan を有効にしていない場合：
 - a. [有効 (Enable)] をクリックします。
 - b. ライセンス契約書ページの下部にスクロールし、[承認 (Accept)] をクリックしてライセンス契約に合意します。
- ステップ 3** [グローバル設定を編集 (Edit Global Settings)] をクリックします。
- ステップ 4** [IronPort インテリジェント マルチスキャンを有効にする (Enable IronPort Intelligent Multi-Scan)] チェックボックスを選択します。
このボックスをオンにすると、アプライアンスの機能がグローバルにイネーブルになります。ただし、メール ポリシーの受信者ごとの設定値をイネーブルにする必要は、引き続きあります。
- ステップ 5** Cisco IronPort Intelligent Multi-Scan でスキャンする最大メッセージ サイズの値を選択します。
デフォルト値は 128 Kb です。このサイズより大きいメッセージは、Cisco Intelligent Multi-Scan でスキャンされません。
- ステップ 6** メッセージをスキャンするときにタイムアウトを待機する秒数を入力します。

秒数を指定する場合は、1 ~ 120 の整数を入力します。デフォルト値は 60 秒です。

大部分のユーザでは、スキャンする最大メッセージ サイズもタイムアウト値も変更する必要がありません。最大メッセージ サイズの設定を小さくして、アプライアンス スループットを最適化できる可能性があります。

ステップ 7 変更内容を送信し、確定します。

スパム対策ポリシーの定義

各メール ポリシーで、スパムと見なされるメッセージと、これらのメッセージで行われるアクションを指定します。また、ポリシーが適されるメッセージをスキャンするエンジンを指定します。

デフォルトの着信および発信メール ポリシーに対して、異なる設定を設定できます。別のユーザに異なるスパム対策ポリシーが必要な場合は、異なるスパム対策設定を持つ複数のメール ポリシーを使用します。ポリシーごとに 1 つのスパム対策ソリューションだけをイネーブルにできます。同じポリシーに両方をイネーブルにすることはできません。

はじめる前に

- 「メッセージがスパムかどうかスキャンするためのアプライアンスの設定方法」(P.13-2) のテーブルの、ここまでのすべてのステップを実行します。
- 次の概念を十分に理解してください。
 - 「陽性および陽性と疑わしいスパムのしきい値の理解」(P.13-10)
 - 「設定例：陽性と判定されたスパムと、陽性と疑わしいスパムとのアクション」(P.13-11)
 - 「正規の送信元からの不要なマーケティング メッセージ」(P.13-11)
 - 複数のスパム対策ソリューションをイネーブルにした場合：「異なるメール ポリシーでの異なるスパム対策スキャン エンジンのイネーブル化：設定例」(P.13-12)
 - 「スパム対策スキャン中に追加されるヘッダー」(P.13-14)
- 「スパム対策アーカイブ」ログにスパムをアーカイブする場合は、「ロギング」(P.34-1) も参照してください。
- 代替メール ホストにメッセージを送信する場合は、「配信ホスト変更アクション」(P.9-59) も参照してください。

手順

- ステップ 1** [メール ポリシー (Mail Policies)] > [着信メール ポリシー (Incoming Mail Policies)] ページに移動します。
- または
- ステップ 2** [メール ポリシー (Mail Policies)] > [発信メール ポリシー (Outgoing Mail Policies)] ページに移動します。
- ステップ 3** 任意のメール ポリシーの [スパム対策 (Anti-Spam)] カラムでリンクをクリックします。
- ステップ 4** [このポリシーの Anti-Spam スキャンを有効にする (Enable Anti-Spam Scanning for this Policy)] セクションでは、ユーザがポリシーで使用するスパム対策ソリューションを選択します。
- 表示されるオプションは、有効にしたスパム対策スキャン ソリューションに基づきます。

デフォルト以外のメール ポリシーの場合、デフォルトのポリシーを使用すると、そのページの他のオプションはディセーブルになります。

このメール ポリシーに対してスパム対策スキャンをまとめてディセーブルにすることもできます。

ステップ 5 陽性と判定されたスパムと陽性と疑わしいスパムおよびマーケティング メッセージを設定します。

オプション	説明
陽性と疑わしいスパムのスキャンを有効にする (Enable Suspected Spam Scanning) マーケティング電子メールのスキャンを有効にする (Enable Marketing Email Scanning)	オプションを選択します。 陽性と判定されたスパムのスキャンはスパム対策スキャンが有効の場合は常に有効です。
このアクションをメッセージに適用する (Apply This Action to Message)	陽性と判定されたスパム、陽性と疑わしいスパム、または不要なマーケティング メッセージに対する全般的なアクションを選択します。 <ul style="list-style-type: none"> • 配信 (Deliver) • ドロップ (Drop) • バウンス (Bounce) • 隔離 (Quarantine)
(オプション) 代替ホストに送信 (Send to Alternate Host)	代替送信メール ホスト (SMTP ルートまたは DNS に示されているもの以外のメール サーバ) で識別されたメッセージを送信できます。 IP アドレスまたはホスト名を入力します。ホスト名を入力すると、Mail Exchange (MX) が最初に検索されます。キーが見つからない場合、DNS サーバの A レコードが使用されます (SMTP ルートと同じ)。 たとえば、追加の検査のサンドボックスのメール サーバなど、メッセージの方向を変更するにはこのオプションを使用します。 重要な追加情報については、「 配信ホスト変更アクション (P.9-59) 」を参照してください。
件名ヘテキストを追加 (Add Text to Subject)	特定のテキスト文字列を前または後に追加して、識別されたメッセージ上の件名のテキストを変更することにより、スパムおよび不要なマーケティング メッセージをユーザが識別およびソートしやすくなります。 <p>(注) このフィールドではスペースは無視されません。このフィールドに入力したテキストの後ろまたは前にスペース追加することで、オリジナルのメッセージ件名と、追加テキストを分けることができます (追加テキストをオリジナルの件名の前に追加する場合は追加テキストの前、オリジナルの件名の後ろに追加する場合は追加テキストの後ろにスペースを追加します)。たとえば付加した場合、少数の末尾にスペースを含むテキスト [SPAM] を追加します。</p> <p>(注) [件名ヘテキストを追加 (Add Text to Subject)] フィールドでは US-ASCII 文字だけが許可されます。</p>
[詳細オプション (Advanced Options)] (カスタム ヘッダーとメッセージ配信用)	

オプション	説明
(オプション) カスタムヘッダーを追加 (Add Custom Header)	識別されたメッセージにカスタム ヘッダーを追加できます。 [詳細 (Advanced)] をクリックし、ヘッダーと値を定義します。
(オプション) 代替エンベロープ受信者に送信 (Send to an Alternate Envelope Recipient)	識別されたメッセージを代替エンベロープ受信者アドレスに送信できます。 [詳細 (Advanced)] をクリックして代替アドレスを定義します。 たとえば、スパムであると識別されたメッセージを後で調査するために、管理者のメールボックスにルーティングできます。複数受信者メッセージの場合は、単一のコピーだけが代替受信者に送信されます。
アーカイブ メッセージ (Archive Message)	識別されたメッセージを「アンチスパム アーカイブ」ログにアーカイブできます。この形式は、mbox 形式のログ ファイルです。
スパムしきい値 (Spam Thresholds)	デフォルトのしきい値を使用するか、陽性と判定されたスパムのしきい値および陽性と疑わしいスパムの値を入力します。

ステップ 6 変更内容を送信し、確定します。

次の作業

発信メールのスパム対策スキャンをイネーブルにした場合は、特にプライベート リスナーに関連するホスト アクセス テーブルのスパム対策設定を確認します。「[メール フロー ポリシーを使用した電子メール送信者のアクセス ルールの定義](#)」(P.7-8) を参照してください。

関連項目

- 「[メッセージがスパムかどうかスキャンするためのアプライアンスの設定方法](#)」(P.13-2)

陽性および陽性と疑わしいスパムのしきい値の理解

メッセージがスパムであるかどうかを評価するときに、両方のスパム対策スキャン ソリューションは、メッセージの総合スパム評点に達するために何千ものルールを適用します。スコアは、メッセージをスパムとして見なすかどうかを決定するため、該当するメール ポリシーで指定されたしきい値と比較されます。

最高精度では、スパムとして陽性と識別する精度はデフォルトでかなり高く設定されています：90 ~ 100 の範囲のメッセージ スコアは、陽性と判定されたスパムであると見なされます。陽性と疑わしいスパムのデフォルトのしきい値は 50 です。

- 陽性と疑わしいスパムのしきい値未満のスコアを持つメッセージは正規のメッセージと見なされません。
- 陽性と疑わしいスパムのしきい値を超えているが、陽性と識別されたしきい値未満のメッセージは、スパムの疑いがあると見なされます。

各メール ポリシーで陽性および陽性と疑わしいスパムのしきい値をカスタマイズし、組織のスパムの許容レベルを反映するスパム対策ソリューションを設定できます。

50 ~ 99 の値に陽性と判定されたスパムのしきい値を変更できます。25 から陽性と判定されたスパムに指定した値までの範囲の任意の値に、陽性と疑わしいスパムのしきい値を変更できます。

しきい値を変更する場合：

- 低い番号（より積極的な設定）を指定すると、より多くのメッセージをスパムとして識別し、より多くの誤検出が生成される場合があります。これによって、ユーザがスパムを受けるリスクは低くなりますが、スパムとしてマークされた正規のメールを受けるリスクは高くなります。
- より高い数（より保守的な設定）を指定すると、より少ないメッセージをスパムとして識別し、より多くのスパムを配信する可能性があります。これによって、ユーザがスパムを受けるリスクは高くなりますが、正規のメールがスパムとして除かれるリスクは低くなります。理想的には、正しく設定した場合、メッセージの件名はそのメッセージがスパムである可能性が高いことを識別し、メッセージは配信されます。

陽性と判定されたスパムと陽性と疑わしいスパムに対して異なるアクションを定義できます。たとえば、「陽性と判定された」スパムをドロップしますが、「陽性と疑わしい」スパムは隔離します。

関連項目

- 「スパム対策ソリューション」(P.13-2)
- 「設定例：陽性と判定されたスパムと、陽性と疑わしいスパムとのアクション」(P.13-11)

設定例：陽性と判定されたスパムと、陽性と疑わしいスパムとのアクション

スパム	サンプル アクション (Aggressive)	サンプル アクション (Conservative)
陽性判定	ドロップ	<ul style="list-style-type: none"> • メッセージの件名に「[疑わしいスパム (Suspected Spam)]」を追加して配信、または • 隔離
陽性と疑わしい	メッセージの件名に「[疑わしいスパム (Suspected Spam)]」を追加して配信	メッセージの件名に「[疑わしいスパム (Suspected Spam)]」を追加して配信

積極的な例では、陽性と識別されたメッセージをドロップし、スパムの疑いのあるメッセージだけにタグを付けます。管理者およびエンドユーザは、着信メッセージの件名行を調べて、false positive でないかどうかを確認でき、管理者は必要に応じて、陽性と疑わしいスパムのしきい値を調整できます。

保守的な例では、陽性と判定されたスパムと陽性と疑わしいスパムは、件名を変更して通過されます。ユーザは、陽性と疑わしいスパムおよび陽性と判定されたスパムを削除できます。この方式は、1 番めの方式よりも保守的です。

メール ポリシーの積極的および保守的なポリシーの詳細については、「メール ポリシー」の章 (表 10-3 (P.10-10)) を参照してください。

正規の送信元からの不要なマーケティング メッセージ

スパム対策スキャン エンジンには、スパムと、正規の送信元からの不要なマーケティング メッセージとを区別できます。マーケティング メッセージはスパムと見なされませんが、組織やエンドユーザによっては、マーケティング メッセージを受信しないことを希望する場合があります。スパム同様、不要なマーケティング メッセージを配信、ドロップ、隔離、またはバウンスすることを選択できます。メッセージの件名にテキストを追加することによって、不要なマーケティング メッセージにタグを付け、マーケティングであることを識別することもできます。

異なるメール ポリシーでの異なるスパム対策スキャン エンジンのイネーブル化：設定例

システム セットアップ ウィザード（または CLI の `systemsetup` コマンド）を使用すると、Cisco Intelligent Multi-Scan または Cisco Anti-Spam エンジンのいずれかをイネーブルにするオプションが示されます。システム セットアップ中に両方をイネーブルにできませんが、システム セットアップが完了した後に [セキュリティ サービス (Security Services)] メニューを使用して、選択しなかったスパム対策ソリューションをイネーブルにできます。

システムのセットアップが終了すれば、[メール ポリシー (Mail Policies)] > [着信メール ポリシー (Incoming Mail Policies)] ページから着信メール ポリシー用のアンチスパム スキャン ソリューションを設定できます（スパム対策スキャンは発信メール ポリシーでは通常はディセーブルです）。ポリシーのスパム対策スキャンも無効にできます。

この例では、デフォルトのメール ポリシーおよび「パートナー」ポリシーでは、陽性スパムおよび陽性と疑わしいスパムの隔離に Cisco Anti-Spam スキャン エンジンを使用しています。

図 13-1 メール ポリシー - 受信者 1 人あたりのスパム対策エンジン

Incoming Mail Policies

Find Policies

Email Address: Recipient Sender Find Policies

Policies

Add Policy...

Order	Policy Name	Anti-Spam	Anti-Virus	Content Filters	Virus Outbreak Filters	Delete
1	Partners	(use default)	(use default)	(use default)	(use default)	
	Default Policy	IronPort Anti-Spam Positive: Quarantine Suspected: Quarantine	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	Disabled	Enabled	

Key: Default Custom Disabled

パートナーのポリシーを変更し、不要なマーケティング メッセージの Cisco Intelligent Multi-Scan とスキャンを使用するには、パートナーの行 ([デフォルトを使用 (Use Default)]) に対応する [スパム対策 (Anti-Spam)] カラムのエントリを指定します。

スキャン エンジンに Cisco Intelligent Multi-Scan を選択し、不要なマーケティング メッセージの検出を有効にする場合は [はい (Yes)] を選択します。不要なマーケティング メッセージの検出にデフォルト設定を使用します。

図 13-2 は、Cisco Intelligent Multi-Scan と不要なマーケティング メッセージの検出がポリシーでイネーブルに設定されていることを示します。

図 13-2 メールポリシー - Cisco Intelligent Multi-Scan のイネーブル化

変更の送信と確定後のメール ポリシーは次のようになります。

図 13-3 メール ポリシー - Intelligent Multi-Scan がイネーブルにされたポリシー

Incoming Mail Policies

Find Policies

Email Address: Recipient Sender

Order	Policy Name	Anti-Spam	Anti-Virus	Content Filters	Virus Outbreak Filters	Delete
1	Partners	IronPort Intelligent Multi-Scan Positive: Deliver Suspected: Deliver Marketing Messages: Deliver	(use default)	(use default)	(use default)	<input type="button" value="Delete"/>
	Default Policy	IronPort Anti-Spam Positive: Deliver Suspected: Deliver Marketing Messages: Disabled	Not Available	Disabled	Not Available	

Key:

スパム フィルタからのアプライアンス生成メッセージの保護

Cisco IronPort アプライアンスから自動送信された電子メール メッセージ（メール アラートおよびスケジュール レポートなど）には、誤ってスパムとして識別される可能性のある URL または他の情報が含まれることがあるため、確実に配信されるよう次を実行します。

スパム対策スキャンをバイパスする着信メール ポリシーにこれらのメッセージの送信者を含めます。「送信者および受信者のグループのメール ポリシーの作成」(P.10-8) および「アンチスパム システムのバイパス アクション」(P.9-65) を参照してください。

スパム対策スキャン中に追加されるヘッダー

- いずれかのスパム対策スキャン エンジンがメール ポリシーでイネーブルにされている場合、そのポリシーを通過した各メッセージは次のヘッダーをメッセージに追加します。

```
X-IronPort-Anti-Spam-Filtered: true
```

```
X-IronPort-Anti-Spam: result
```

2 番目のヘッダーには、メッセージのスキャンに使用されたルールとエンジンのバージョンを Cisco Support で識別するための情報が含まれます。結果の情報は、符号化された独自の情報であり、顧客による復号は可能ではありません。

- Cisco Intelligent Multi-Scan では、サードパーティ製スパム対策スキャン エンジンからのヘッダーも追加します。
- 陽性と判定されたスパム、陽性と疑わしいスパム、不要なマーケティング メールとして識別される特定のメール ポリシーのすべてのメッセージに追加する追加のカスタム ヘッダーを定義できます。「[スパム対策ポリシーの定義](#)」(P.13-8) を参照してください。

誤って分類されたメッセージの Cisco Systems への報告

分類が誤っていると思われるメッセージを、分析用に Cisco に報告できます。各メッセージは、専門家チームによってレビューされ、製品の精度と有効性を向上させるために使用されます。各メッセージは、RFC 822 添付ファイルとして、次のアドレスに転送してください。

- spam@access.ironport.com : 見逃されたスパムの報告用
- ham@access.ironport.com : false positive の報告用

送信のボリュームに対して、Cisco IronPort はお客様に個別のフィードバックや結果を提供できません。

誤って分類されたメッセージの報告の詳細については、Cisco ナレッジ ベースを参照するか、Cisco サポート プロバイダーにお問い合わせください。

着信リレー構成における送信者の IP アドレスの決定

1 つ以上のメール交換/転送エージェント (MX または MTA)、フィルタ サービスが Cisco アプライアンスと着信メールを送信する外部マシンとの間のネットワークのエッジに配置されている場合、アプライアンスは送信元マシンの IP アドレスを決定することはできません。代わりに、メールはローカル MX/MTA から送信されたように見えます。ただし、IronPort Anti-Spam および Cisco Intelligent Multi-Scan (SenderBase レピュテーション サービスを使用) は外部送信者の正確な IP アドレスに依存します。

ソリューションは、着信リレーを使用するようにアプライアンスを設定することです。Cisco アプライアンスに接続するすべての内部 MX/MTA の名前と IP アドレス、発信元 IP アドレスを保管するのに使用するヘッダーを指定します。

- 「[着信リレーを使用した環境例](#)」(P.13-15)
- 「[着信リレーを使用するアプライアンスの設定](#)」(P.13-16)
- 「[着信リレーが機能にどのように影響するか](#)」(P.13-21)
- 「[使用するヘッダーを指定するログの設定](#)」(P.13-23)

着信リレーを使用した環境例

図 13-4 に、きわめて基本的な着信リレーの例を示します。ローカル MX/MTA によってメールが Cisco アプライアンスにリレーされているため、IP アドレス 7.8.9.1 からのメールは IP アドレス 10.2.3.4 からのように見えます。

図 13-4 MX/MTA によるメールリレー：簡易

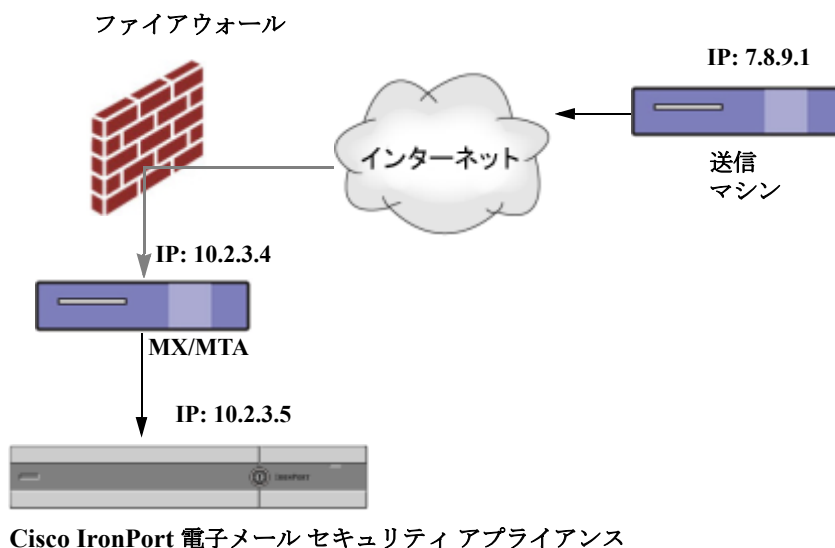
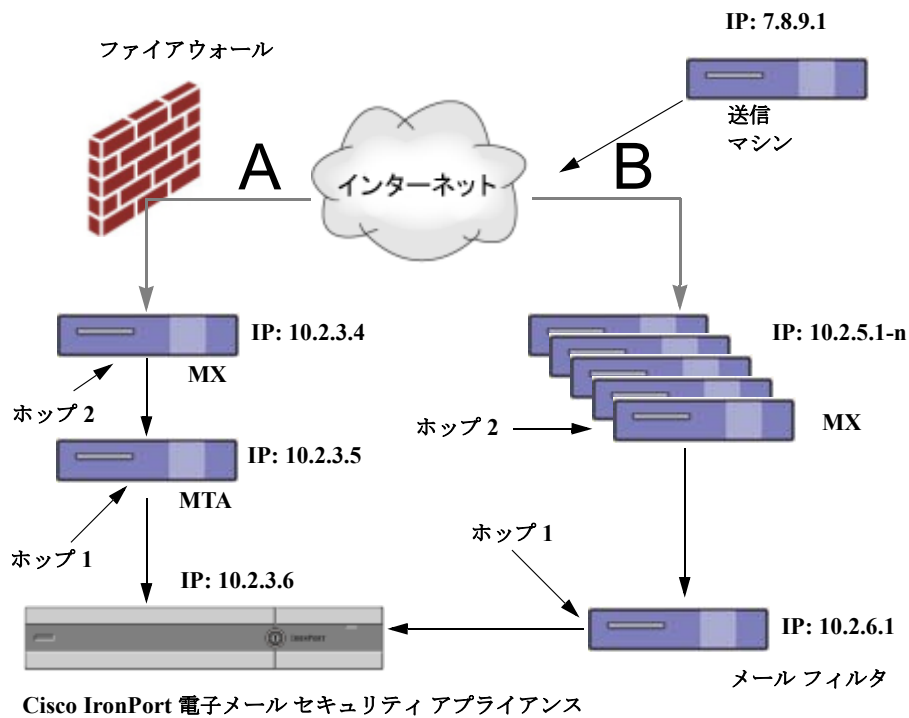


図 13-5 に別の 2 つの例を示します。この例は、少し複雑であり、ネットワーク内でのメールのリレー方法と、Cisco アプライアンスへの受け渡し前に実施できる、ネットワーク内の複数サーバにおけるメールの処理方法を示します。例 A では、7.8.9.1 からのメールがファイアウォールを通過し、MX および MTA で処理されてから、Cisco アプライアンスに配信されます。例 B では、7.8.9.1 からのメールがロード バランサまたは他のタイプのトラフィック シェーピング アプライアンスに送信され、一連の MX のいずれかに送信されてから、Cisco アプライアンスに配信されます。

図 13-5 MX/MTA によるメール リレー：拡張



着信リレーを使用するアプライアンスの設定

着信リレー機能のイネーブル化



(注) ローカル MX/MTA がメールを Cisco アプライアンスにリレーする場合のみ、着信リレー機能をイネーブルにしてください。

手順

- ステップ 1 [ネットワーク (Network)] > [着信リレー (Incoming Relays)] を選択します。
- ステップ 2 [有効 (Enable)] をクリックします。
- ステップ 3 変更内容を確定します。

着信リレーの追加

識別する着信リレーを追加します。

- 電子メールセキュリティアプライアンスに着信メッセージをリレーするネットワークの各マシン、および
- 元の外部送信者の IP アドレスが分類されるヘッダー。

はじめる前に

これらの前提条件を完了するために必要な情報は、「リレーされたメッセージのメッセージヘッダー」(P.13-18) を参照してください。

- 元の外部送信者の IP アドレスを識別するカスタムまたは Received ヘッダーを使用するかどうかを設定します。
- カスタム ヘッダーを使用する場合：
 - リレーされたメッセージの発信元 IP アドレスを分類する正確なヘッダーを設定します。
 - 各 MX、MTA、または元の外部送信元に接続している他のマシンは、受信メッセージに元の外部送信者のヘッダー名と IP アドレスを追加するには、そのマシンを設定します。

手順

-
- ステップ 1** [ネットワーク (Network)] > [着信リレー (Incoming Relays)] を選択します。
- ステップ 2** [リレーの追加 (Add Relay)] をクリックします。
- ステップ 3** このリレーの名前を入力します。
- ステップ 4** MTA、MX、またはリレー着信メッセージに 電子メールセキュリティ アプライアンス に接続している他のマシンの IP アドレスを入力します。

IPv4 または IPv6 アドレス、標準 CIDR 形式、または IP アドレス範囲を使用できます。たとえば、電子メールを受信する複数の MTA をネットワークのエッジに配置している場合に、すべての MTA を含む IP アドレスの範囲、たとえば 10.2.3.1/8 や 10.2.3.1-10 を入力する場合があります。

IPv6 アドレスの場合、AsyncOS は次の形式をサポートします。

- 2620:101:2004:4202::0-2620:101:2004:4202::ff
- 2620:101:2004:4202::
- 2620:101:2004:4202::23
- 2620:101:2004:4202::/64

- ステップ 5** 元の外部送信者の IP アドレスを識別するヘッダーを指定します。
- ヘッダーを入力する場合に、末尾のコロンを入力する必要はありません。
- a. ヘッダー タイプの選択：
 - カスタム ヘッダー (推奨) または Received ヘッダーを選択します。
 - b. カスタム ヘッダーの場合：
 - リレーされたメッセージに追加するリレー マシンを設定したヘッダー名を入力します。
 - 次に例を示します。
 - SenderIP
 - または
 - X-CustomHeader
 - c. Received ヘッダーの場合：
 - IP アドレスの前に配置される文字または文字列を入力します。IP アドレスを調査するホップ数を入力します。
- ステップ 6** 変更内容を送信し、確定します。
-

次の作業

次を行うことを検討します。

- DHAP の無制限のメッセージがあるメール フロー ポリシーを送信者グループにリレーするマシンを追加します。説明については、「[着信リレーおよびディレクトリ ハーベスト攻撃防止](#)」(P.13-21)を参照してください。
- トラッキングおよびトラブルシューティングを容易にするには、使用されるヘッダーを示すようにアプライアンスのロギングを設定します。「[使用するヘッダーを指定するログの設定](#)」(P.13-23)を参照してください。

関連項目

- 「[メッセージがスパムかどうかスキャンするためのアプライアンスの設定方法](#)」(P.13-2)

リレーされたメッセージのメッセージ ヘッダー

リレーされたメッセージの元の送信者の識別にヘッダーのタイプが次のいずれかを使用するようにアプライアンスを設定します：

- 「[カスタム ヘッダー](#)」(P.13-18)
- 「[Received ヘッダー](#)」(P.13-19)

カスタム ヘッダー

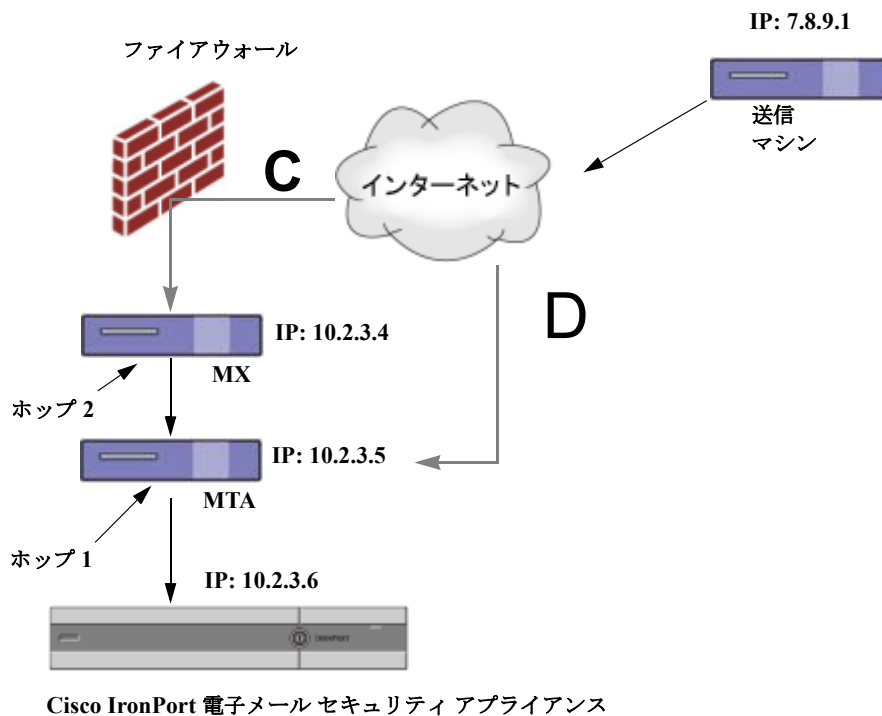
カスタム ヘッダーを使用して元の送信者を識別する推奨される方法です。元の送信者に接続するマシンでは、このカスタム ヘッダーを追加する必要があります。このヘッダーの値は、外部の送信マシンの IP アドレスになることが予想されます。次の例を参考にしてください。

```
SenderIP: 7.8.9.1
```

```
X-CustomHeader: 7.8.9.1
```

ローカル MX/MTA で不定ホップ数のメールを受信する場合は、カスタム ヘッダーを挿入することが、着信リレー機能をイネーブルにする唯一の方法です。たとえば、[図 13-6](#)では、パス C とパス D の両方が IP アドレス 10.2.3.5 まで至る一方で、パス C は 2 ホップ、パス D は 1 ホップです。この状況では、ホップ数が異なる場合があるため、カスタム ヘッダーを使用して、着信リレーが正しく設定されるようにする必要があります。

図 13-6 MX/MTA によるメール リレー：不定ホップ数



関連項目

- 「着信リレーの追加」(P.13-16)

Received ヘッダー

MX/MTA を設定する場合、送信 IP アドレスを含むカスタム ヘッダーの組み込みは選択肢になりません。着信リレー機能は、メッセージの「Received:」ヘッダーを調査することによって送信 IP アドレスの判別を試行するように設定できます。「Received:」ヘッダーを使用する方法は、ネットワーク ホップ数が常に一定である IP アドレスの場合に限り機能します。つまり、最初のホップにあるマシン (図 13-5 の 10.2.3.5) は、ネットワークのエッジからのホップ数が常に等しい必要があります。Cisco アプライアンスに接続しているマシンまでの着信メールのパスが異なる可能性がある場合 (したがって、図 13-6 で示したように、ホップ数が異なる場合) は、カスタム ヘッダーを使用する必要があります (「カスタム ヘッダー」(P.13-18) を参照)。

解析対象文字または文字列および逆行して検索するネットワーク ホップ数 (または Received: ヘッダー数) を指定します。ホップは、基本的に、メッセージがマシン間で転送されることを指します (Cisco アプライアンスによる受信はホップとしてカウントされません。詳細については、「使用するヘッダーを指定するログの設定」(P.13-23) を参照してください)。AsyncOS は、指定されたホップ数に対応する Received: ヘッダー内の解析対象文字または文字列の最初のオカレンスに続く最初の IP アドレスを参照します。たとえば、2 ホップを指定した場合は、Cisco アプライアンスから逆行して 2 つめの Received: ヘッダーが解析されます。解析対象文字も有効な IP アドレスも見つからない場合、Cisco アプライアンスは接続マシンの実際の IP アドレスを使用します。

次の例のメール ヘッダーの場合、左角カッコ (l) と 2 ホップを指定した場合は、外部マシンの IP アドレスは 7.8.9.1 です。ただし、右カッコ (r) および解析対象文字を指定した場合は、有効な IP アドレスが見つかりません。この場合、着信リレー機能はディセーブルであると見なされ、接続元マシンの IP (10.2.3.5) が使用されます。

図 13-5 の例における着信リレーは次のとおりです。

- パス A : 10.2.3.5 (Received ヘッダーを使用して 2 ホップ) および
- パス B : 10.2.6.1 (Received ヘッダーを使用して 2 ホップ)

表 13-1 に、図 13-5 同様、Cisco アプライアンスまで複数の移動ホップ数を持つメッセージの電子メールヘッダーの例を示します。この例は、受信者の受信箱に到着したメッセージで表示される、外部からのヘッダー (Cisco アプライアンスでは無視) を示します。指定するホップ数は 2 になります。

表 13-2 に、外部ヘッダーを除いて、同じ電子メールメッセージのヘッダーを示します。

表 13-1 一連の Received: ヘッダー (パス A 例 1)

1	Microsoft Mail Internet Headers Version 2.0 Received: from smemail.rand.org ([10.2.2.7]) by smmail5.customerdoamin.org with Microsoft SMTPSVC(5.0.2195.6713); Received: from ironport.customerdomain.org ([10.2.3.6]) by smemail.customerdoamin.org with Microsoft SMTPSVC(5.0.2195.6713);
2	Received: from mta.customerdomain.org ([10.2.3.5]) by ironport.customerdomain.org with ESMTTP; 21 Sep 2005 13:46:07 -0700
3	Received: from mx.customerdomain.org (mx.customerdomain.org) [10.2.3.4] by mta.customerdomain.org (8.12.11/8.12.11) with ESMTTP id j8LkKwU1008155 for <joefoo@customerdomain.org>
4	Received: from sending-machine.spamham.com (sending-machine.spamham.com [7.8.9.1]) by mx.customerdomain.org (Postfix) with ESMTTP id 4F3DA15AC22 for <joefoo@customerdomain.org>
5	Received: from linux1.thespammer.com (HELO linux1.thespammer.com) ([10.1.1.89]) by sending-machine.spamham.com with ESMTTP; Received: from exchange1.thespammer.com ([10.1.1.111]) by linux1.thespammer.com with Microsoft SMTPSVC(6.0.3790.1830); Subject: Would like a bigger paycheck? Date: Wed, 21 Sep 2005 13:46:07 -0700 From: "A.Sender" <asend@otherdomain.com> To: <joefoo@customerdomain.org>

表 13-1 についての注意事項は、次のとおりです。

- Cisco アプライアンスでは、これらのヘッダーを無視します。
- Cisco アプライアンスがメッセージを受信します (ホップとしてカウントされない)。
- 最初のホップ (着信リレー)。
- 第 2 ホップ。これは、送信 MTA です。仮想 IP アドレスは 7.8.9.1 です。
- Cisco アプライアンスでは、これらの Microsoft Exchange ヘッダーを無視します。

表 13-2 一連の Received: ヘッダー (パス A 例 2)

1	Received: from mta.customerdomain.org ([10.2.3.5]) by ironport.customerdomain.org with ESMTTP; 21 Sep 2005 13:46:07 -0700
2	Received: from mx.customerdomain.org (mx.customerdomain.org) [10.2.3.4] by mta.customerdomain.org (8.12.11/8.12.11) with ESMTTP id j8LkKwU1008155 for <joefoo@customerdomain.org>;
3	Received: from sending-machine.spamham.com (sending-machine.spamham.com [7.8.9.1]) by mx.customerdomain.org (Postfix) with ESMTTP id 4F3DA15AC22 for <joefoo@customerdomain.org>;

図 13-7 に、GUI の [リレーの追加 (Add Relay)] ページで設定されたパス A の着信リレーを示します。

図 13-7 Received ヘッダー付きで設定された着信リレー

Add Relay

Incoming Relay	
Name: ?	IncomingRelayOne
IP Address: ?	10.2.3.5
Header:	<input type="radio"/> Specify a custom header <input checked="" type="radio"/> Parse the "Received" header
	Begin parsing after: ? [] Hop: ? [2]

関連項目

- 「着信リレーの追加」 (P.13-16)

着信リレーが機能にどのように影響するか

- 「着信リレーとフィルタ」 (P.13-21)
- 「着信リレー、HAT、SBRs および送信者グループ」 (P.13-21)
- 「着信リレーおよびディレクトリ ハーベスト攻撃防止」 (P.13-21)
- 「着信リレーおよびトレース」 (P.13-22)
- 「着信リレーと電子メールセキュリティ モニタ (レポート)」 (P.13-22)
- 「着信リレーおよびメッセージ トラッキング」 (P.13-22)
- 「着信リレーとロギング」 (P.13-22)

着信リレーとフィルタ

着信リレー機能では、SenderBase レピュテーション サービスに関連するさまざまなフィルタ ルール (reputation、no-reputation) に正しい SenderBase レピュテーション スコアを提供します。

着信リレー、HAT、SBRs および送信者グループ

HAT ポリシー グループは、着信リレーからの情報は現在使用していません。ただし、着信リレー機能では SenderBase レピュテーション スコアを提供するため、メッセージフィルタおよび \$reputation 変数によって HAT ポリシー グループ機能をシミュレートできます。

着信リレーおよびディレクトリ ハーベスト攻撃防止

リモート ホストが、ネットワーク上で着信リレーとして使われている MX または MTA にメッセージを送ることでディレクトリ ハーベスト攻撃防止を試みる場合、アプライアンスは、ディレクトリ ハーベスト攻撃防止 (DHAP) がイネーブルに設定されたメール フロー ポリシーを持つ送信者グループにリレーが割り当てられていると、その着信リレーからの接続をドロップします。これは、リレーからす

すべてのメッセージが、正規のメッセージも含め電子メールセキュリティアプライアンスに接続されないよう防止します。アプライアンスはリモートホストが攻撃者であると認識できず、着信リレーとして機能する MX または MTA は攻撃元ホストからメールを受信し続けます。この問題を回避して、着信リレーからメッセージを受信し続けるために DHAP の無制限のメッセージがあるメールフローポリシーを送信者グループにリレーを追加します。

着信リレーおよびトレース

トレースは、送信元 IP アドレスのレピュテーションスコアの代わりに、結果の着信リレー側 SenderBase レピュテーションスコアを返します。

着信リレーと電子メールセキュリティ モニタ (レポート)

着信リレーを使用する場合

- 電子メールセキュリティ モニタ レポートには外部 IP および MX/MTA の両方のデータが含まれます。たとえば、外部マシン (IP 7.8.9.1) から内部 MX/MTA (IP 10.2.3.4) を介して 5 通の電子メールが送信された場合、[メールフロー サマリー (Mail Flow Summary)] には、IP 7.8.9.1 からの 5 個のメッセージに加えて、内部リレー MX/MTA (IP 10.2.3.5) からの 5 個のメッセージが表示されます。
- SenderBase レピュテーションスコアは電子メールセキュリティ モニタ レポートで正しく報告されません。送信者グループが正しく解決されない場合もあります。

着信リレーおよびメッセージ トラッキング

着信リレーを使用すると、メッセージ トラッキングの詳細ページに、元の外部送信者の IP アドレスおよびレピュテーションスコアの代わりに、メッセージのリレーの IP アドレスおよびリレー側 SenderBase レピュテーションスコアが表示されます。

着信リレーとロギング

次のログの例で、送信者の SenderBase レピュテーションスコアは、当初 1 行目に示されます。その後、着信リレーの処理が行われて、正しい SenderBase レピュテーションスコアが 5 行目に示されません。

1	Fri Apr 28 17:07:29 2006 Info: ICID 210158 ACCEPT SG UNKNOWNLIST match nx.domain SBRS rfc1918
2	Fri Apr 28 17:07:29 2006 Info: Start MID 201434 ICID 210158
3	Fri Apr 28 17:07:29 2006 Info: MID 201434 ICID 210158 From: <joe@sender.com>
4	Fri Apr 28 17:07:29 2006 Info: MID 201434 ICID 210158 RID 0 To: <mary@example.com>
5	Fri Apr 28 17:07:29 2006 Info: MID 201434 IncomingRelay(senderdotcom): Header Received found, IP 192.192.108.1 being used, SBRS 6.8
6	Fri Apr 28 17:07:29 2006 Info: MID 201434 Message-ID '<7.0.1.0.2.20060428170643.0451be40@sender.com>'
7	Fri Apr 28 17:07:29 2006 Info: MID 201434 Subject 'That report...'
8	Fri Apr 28 17:07:29 2006 Info: MID 201434 ready 2367 bytes from <joe@sender.com>
9	Fri Apr 28 17:07:29 2006 Info: MID 201434 matched all recipients for per-recipient policy DEFAULT in the inbound table

10	Fri Apr 28 17:07:34 2006 Info: ICID 210158 close
11	Fri Apr 28 17:07:35 2006 Info: MID 201434 using engine: CASE spam negative
12	Fri Apr 28 17:07:35 2006 Info: MID 201434 antivirus negative
13	Fri Apr 28 17:07:35 2006 Info: MID 201434 queued for delivery

着信リレーとメール ログ

次の例は、着信リレー情報を含む、一般的なログ エントリを示します。

```
Wed Aug 17 11:20:41 2005 Info: MID 58298 IncomingRelay(myrelay): Header Received found,
IP 192.168.230.120 being used
```

使用するヘッダーを指定するログの設定

Cisco アプライアンスでは、メッセージが受信された時点で存在していたヘッダーだけを検査します。したがって、ローカルで追加される追加のヘッダー（Microsoft Exchange のヘッダーなど）や、Cisco アプライアンスがメッセージを受信するときに追加する追加のヘッダーは、処理されません。使用されるヘッダーを特定する方法の 1 つは、使用するヘッダーを AsyncOS ログイングに含めるよう設定することです。

ヘッダーのログイング設定を設定するには、「[ログイングに対するグローバル設定](#)」(P.34-41) を参照してください。

モニタリング ルールのアップデート

使用許諾契約に同意すると、最新の Cisco Anti-Spam および Cisco Intelligent Multi-Scan ルールのアップデートを確認できます。

手順

- ステップ 1** [セキュリティ サービス (Security Services)] > [IronPort Anti-Spam] を選択します。
または
- ステップ 2** [セキュリティ サービス (Security Services)] > [IronPort Multi-Scan] を選択します。
- ステップ 3** ルールの [ルールの更新 (Rule Updates)] セクションを表示し、次を行います。

目的	追加情報
各コンポーネントの最新の更新について参照	アップデートが実行されていないか、サーバが設定されていない場合は、「Never Updated」という文字列が表示されます。
アップデートが使用可能かどうかを確認	—
アップグレードが入手可能な場合はルールを更新	[今すぐ更新 (Update Now)] をクリックします。

関連項目

- 「サービスのアップデート」 (P.29-22)
- 「プロキシサーバを経由したアップデート」 (P.29-22)
- 「アップグレードおよびアップデートをダウンロードするためのサーバ設定」 (P.29-22)

スパム対策のテスト

目的	操作内容	追加情報
設定をテストします。	X-advertisement: spam ヘッダーを使用して、設定をテストします。 テストを目的として、Cisco Anti-Spam では、X-Advertisement: spam という形式の X-Header を含むすべてのメッセージをスパムであると見なします。	このヘッダーを付けて送信したテストメッセージには、Cisco Anti-Spam によってフラグが設定され、メールポリシーに対して設定したアクション（「 スパム対策ポリシーの定義 」 (P.13-8)）が実行されることを確認できません。 次のいずれかをこのヘッダーに使用します。 <ul style="list-style-type: none"> • このヘッダーを含むテストメッセージを送信する SMTP コマンドを使用します。「Cisco スпам対策をテストするためのアプライアンスへのメールの送信」 (P.13-24) を参照してください。 • trace コマンドを使用してこのヘッダーを含めます。「テストメッセージを使用したメールフローのデバッグ：トレース」 (P.36-1) を参照してください。
スパム対策エンジンの有効性を評価します。	インターネットから直接本物のメールストリームを使用して製品を評価します。	回避すべき非効率的な評価のアプローチの一覧については、「 スパム対策の性能をテストしない方法 」 (P.13-25) を参照してください。

Cisco スпам対策をテストするためのアプライアンスへのメールの送信

はじめる前に

- アプライアンスにおける Telnet の使用方法を理解します。付録 A 「[アプライアンスへのアクセス](#)」を参照してください。
- 「[スパム対策設定のテスト：SMTP の使用例](#)」 (P.13-25) の例を確認してください。

手順

-
- ステップ 1** メールポリシーの Cisco Anti-Spam をイネーブルにします。
- ステップ 2** 次のヘッダーを含むテスト電子メールをそのメールポリシーに含まれているユーザに送信します。
X-Advertisement: spam

アクセスできるアドレスに Telnet の SMTP コマンドを使用してこのメッセージを送信します。
- ステップ 3** 次に、テストアカウントのメールボックスを調べて、メールポリシーに設定したアクションに基づいてテストメッセージが正しく配信されたことを確認します。

次に例を示します。
- 件名行が変更されている。

- 追加のカスタム ヘッダーが追加されている。
- メッセージが代替アドレスに配信された。
- メッセージがドロップされた。

スパム対策設定のテスト : SMTP の使用例

たとえば、メール ポリシーはテスト アドレスのメッセージを受信するように設定されている必要があります。HAT はテスト接続を許可する必要があります。

```
# telnet IP_address_of_IronPort_Appliance_with_IronPort_Anti-Spam port
220 hostname ESMTP
helo example.com
250 hostname
mail from: <test@example.com>
250 sender <test@example.com> ok
rcpt to: <test@address>
250 recipient <test@address> ok
data
354 go ahead
Subject: Spam Message Test
X-Advertisement: spam

spam test
.
250 Message MID accepted
221 hostname
quit
```

スパム対策の性能をテストしない方法

IronPort Anti-Spam と Cisco Intelligent Multi-Scan のルールは、活発なスパム攻撃を防ぐためにすぐに追加され、攻撃が終了するとすぐに期限切れになるため、次の方法のいずれかを使用して有効性をテストしないでください。

- 再送信されたか、転送されたメールまたはカット アンド ペーストされたスパム メッセージによる評価。
適切なヘッダー、接続 IP、シグニチャなどを持たないメールを使用すると、評点が不正確になります。
- 「難易度の高いスパム」だけをテストする。
SBRS、ブラックリスト、メッセージフィルタなどを使用して「難易度の低いスパム」を取り除くと、全体の検出率が低くなります。
- 別のスパム対策ベンダーによって検出されたスパムの再送信
- 以前のメッセージのテスト
スキャン エンジン は現在の脅威に基づき、迅速にルールを追加し、排除します。したがって、古いメッセージを使用してテストすると、テスト結果が不正確になります。



CHAPTER 14

アウトブレイク フィルタ

- 「アウトブレイク フィルタの概要」 (P.14-1)
- 「アウトブレイク フィルタの動作」 (P.14-2)
- 「アウトブレイク フィルタの機能概要」 (P.14-8)
- 「アウトブレイク フィルタの管理 (GUI)」 (P.14-11)
- 「アウトブレイク フィルタのモニタリング」 (P.14-21)
- 「アウトブレイク フィルタ機能のトラブルシューティング」 (P.14-22)

アウトブレイク フィルタの概要

アウトブレイク フィルタは大規模なウイルスの拡散、および小規模のフィッシング詐欺およびマルウェア配布といった、非ウイルス性の攻撃が発生した際にネットワークを保護します。データが収集され、ソフトウェアの更新が公開されるまで新たな拡散を検知できない通常のアンチマルウェア セキュリティ ソフトウェアとは異なり、シスコは感染が拡散したときにデータを収集し、ユーザにこれらのメッセージが到達することを防ぐためにリアルタイムで電子メール セキュリティ アプライアンスに更新情報を送信します。

シスコは着信メッセージは、着信メッセージが安全またはアウトブレイクの一部であることを判断するルールを開発するためにグローバル トラフィック パターンを使用します。アウトブレイクの一部となる可能性があるメッセージは、シスコからアップデートされたアウトブレイクの情報または Sophos および McAfee によって発行される新しいアンチウイルス定義に基づいて安全と判断されるまで隔離されます。

小規模な非ウイルス性の攻撃で使用されるメッセージは、正当に見える外見、受信者情報、そして短期間だけオンラインに存在し Web セキュリティ サービスが知らないフィッシングおよびマルウェア Web サイトを参照するカスタム URL を使用します。アウトブレイク フィルタはメッセージの内容を分析し、この種の非ウイルス性の攻撃を検出するために URL リンクを検索します。アウトブレイク フィルタは Web セキュリティ プロキシによって潜在的に危険な Web サイトへのトラフィックをリダイレクトするために URL を書き換え、ユーザがアクセスしようとしている Web サイトが悪意があるかもしれないことを警告するかまたは Web サイトを完全にブロックします。

アウトブレイク フィルタの動作

メッセージの遅延、リダイレクトおよび修正

アウトブレイク フィルタ機能は、ウイルス感染からユーザを保護するために 3 つの戦略を使用します。

- **遅延。**アウトブレイク フィルタは、ウイルス感染の一部または非ウイルス性の攻撃である可能性のあるメッセージを隔離します。隔離の間、アプライアンスはアップデートされたアウトブレイク 情報を受信し、攻撃の一部であるかどうか確認するためにメッセージを再スキャンします。
- **リダイレクト。**リンクされた Web サイトのいずれかにアクセスしようとする時、Cisco Web セキュリティ プロキシによって受信者をリダイレクトするように非ウイルス性の攻撃のメッセージ 内の URL を書き換えます。プロキシは、Web サイトがまだ動作中である場合は、その Web サイトにマルウェアが含まれる可能性があることをユーザに警告するスプラッシュ画面を表示し、Web サイトがオフラインになっている場合は、エラー メッセージを表示します。URL のリダイレクトの詳細については、「[URL のリダイレクト](#)」(P.14-4) を参照してください。
- **変更。**非ウイルス性の脅威メッセージの URL 書き換えに加えて、アウトブレイク フィルタはユーザにメッセージの内容についてユーザに警告するためにメッセージの件名を変更して、メッセージ本文の上に免責事項を追加できます。詳細については、「[メッセージの変更](#)」(P.14-5) を参照してください。

脅威カテゴリ

アウトブレイク フィルタ機能は、メッセージに基づくアウトブレイクの次の 2 つのカテゴリからの保護を提供します。ウイルス アウトブレイクは、添付ファイルに見たことのないウイルスが含まれるメッセージで、非ウイルス性の脅威には、外部 Web サイトへのリンクを経由するフィッシング試行、詐欺、およびマルウェア配布が含まれます。

デフォルトでアウトブレイク フィルタ機能は、アウトブレイク中の可能性があるウイルスがあるかどうか送受信メッセージをスキャンします。アプライアンスでアンチスパム スキャンをイネーブルにする場合は、ウイルス アウトブレイクに加えて、非ウイルス性の脅威のスキャンをイネーブルにできます。



(注)

アウトブレイク フィルタが非ウイルス性の脅威をスキャンするために、Cisco Anti-Spam または Cisco Intelligent Multi-Scan スキャンのライセンス キーが必要です。

ウイルス アウトブレイク

アウトブレイク フィルタ機能を使用することで、ウイルス アウトブレイクとの格闘において優位なスタートを切ることができます。アウトブレイクは、見たことのないウイルスまたは既存のウイルスの変異型を含む添付ファイルを持つメッセージがプライベート ネットワークおよびインターネットを経由してすばやく拡散するときに発生します。これらの新しいウイルスまたはウイルスの変異型がインターネットを攻撃した場合、最も危機的な期間はウイルスがリリースされてからアンチウイルス ベンダーがアップデートしたウイルス定義をリリースするまでの期間です。たとえ数時間でも、事前に通知を受けることは、マルウェアまたはウイルスの拡散を抑えるうえで非常に重要です。ウイルス定義がリリースされるまでの間に、新しく発見されたウイルスはグローバルに伝播し、電子メール インフラストラクチャを停止に追い込むことが可能です。

フィッシング、マルウェア配布、およびその他の非ウイルス性の脅威

非ウイルス性の脅威を含んでいるメッセージは、正規の送信元からのメッセージのように設計されていて、多くの場合、少数の受信者に送信されます。これらのメッセージには、信頼できると見せるために次の 1 つまたは複数の特徴がある場合があります。

- 受信者の連絡先情報。
- HTML コンテンツは、ソーシャル ネットワークおよびオンライン販売などの正規の送信元からの電子メールを模倣するように設計されています。
- 新しい IP アドレスを持ち、短期間だけオンラインである Web サイトを指している URL。これは電子メールおよび Web セキュリティ サービスに、その Web サイトが不正かどうか判断するための十分な情報がないことを意味します。
- URL 短縮サービスを指している URL。

これらの特徴すべてによって、これらのメッセージをスパムとして検出するのがさらに難しくなります。アウトブレイク フィルタ機能によって、これらの非ウイルス性の脅威に対するマルチレイヤの防衛が提供され、ユーザがマルウェアをダウンロードしたり、個人情報を新しい不審な Web サイトに提供したりすることを防ぎます。

CASE はメッセージ内に URL を発見すると、そのメッセージを既存のアウトブレイク ルールと比較して、そのメッセージが小規模の非ウイルス性のアウトブレイクの一部かどうか判断し、次に脅威レベルを割り当てます。脅威レベルに応じて、電子メール セキュリティ アプライアンスは、より多くの脅威のデータを集められるまで受信者への配信を遅らせ、Web サイトにアクセスしようとする Cisco Web セキュリティ プロキシへ受信者をリダイレクトするようにメッセージ内の URL を書き換えます。プロキシは、その Web サイトにマルウェアが含まれる可能性があることをユーザに警告するスプラッシュ ページを表示します。

Cisco Security Intelligence Operations

Cisco Security Intelligence Operations (SIO) は、グローバルな脅威情報、レピュテーションに基づくサービス、および高度な分析を Cisco セキュリティ アプライアンスに結び付け、より強力な保護をより迅速な応答時間で提供するセキュリティ エコシステムです。

SIO は次の 3 種類のコンポーネントからなります。

- **SenderBase**。世界有数の規模を誇る脅威モニタリング ネットワークおよび脆弱性データベース。
- **Threat Operations Center (TOC)**。セキュリティ専門家のグローバル チームおよび SenderBase によって収集された実行可能な情報を抽出する自動システム。
- **動的アップデート**。アウトブレイク発生時に、Cisco に自動的に配信されるリアルタイム アップデート。

SIO は、グローバル SenderBase ネットワークからのリアルタイム データを、共通のトラフィック パターンと比較して、アウトブレイクの確かな前兆である異常を識別します。TOC は、データをレビューしてアウトブレイクの可能性の脅威レベルを発行します。Cisco 電子メール セキュリティ アプライアンスは、アップデートされた脅威レベルとアウトブレイク ルールをダウンロードし、それらを使用してすでにアウトブレイク隔離エリアにあるメッセージと同様に送受信メッセージをスキャンします。

現在のウイルス アウトブレイクに関する情報は、次の SenderBase の Web サイトで入手できます。

<http://www.senderbase.org/>

次の SIO Web サイトに、スパム、フィッシング、およびマルウェア配布の試行を含む現在の非ウイルス性の脅威のリストが記載されています。

<http://tools.cisco.com/security/center/home.x>

Context Adaptive Scanning Engine

アウトブレイク フィルタには、Cisco 独自の Context Adaptive Scanning Engine (CASE) が使用されています。CASE は、メッセージング脅威に対するリアルタイムの分析に基づいて自動的かつ定期的に調整されている、100,000 を超える適応メッセージ属性を活用しています。

ウイルス アウトブレイクの場合、CASE はメッセージの内容、コンテキスト、および構造を分析してアダプティブ ルールのトリガーである可能性のあるものを、正確に識別します。CASE は、アダプティブ ルールと SIO から発行されるリアルタイムのアウトブレイク ルールを組み合わせ、各メッセージを評価し、独自の脅威レベルを割り当てます。

非ウイルス性の脅威を検出するために、CASE は URL に対してメッセージをスキャンし、1 つまたは複数の URL が発見されると SIO が提供するアウトブレイク ルールを使用してメッセージの脅威レベルを評価します。

メッセージの脅威レベルに基づいて、CASE は、アウトブレイクを防ぐためにメッセージを一定期間隔離することを推奨します。SIO が提供するアップデートされたアウトブレイク ルールに基づいてメッセージを再評価できるように、CASE は再スキャンの間隔も決定します。脅威レベルが高くなるほど、隔離中のメッセージの再スキャンの頻度が高くなります。

メッセージが隔離解除されるたびに、CASE はメッセージの再スキャンも行います。再スキャン時に、CASE によりメッセージがスパムであるか、ウイルスを含むと判断された場合、メッセージを再度隔離できます。

CASE の詳細については、「[Cisco Anti-Spam : 概要](#)」(P.13-4) を参照してください。

メッセージの遅延

アウトブレイクまたは電子メール攻撃の発生と、ソフトウェア ベンダーによるアップデートしたルールのリリースの間の期間は、ネットワークとユーザが最も脆弱なときです。この期間に、現代のウイルスはグローバルに伝播でき、また不正な Web サイトはマルウェアを配信したり、ユーザの機密情報を収集したりすることができます。限られた期間に疑わしいメッセージを隔離することによって、アウトブレイク フィルタは、ユーザおよびネットワークを保護し、シスコおよびその他のベンダーに新しいアウトブレイクを調査する時間を与えます。

ウイルス アウトブレイクが発生すると、アップデートされたアウトブレイク ルールおよび新しいアンチウイルス シグニチャにより、その電子メールの添付ファイルがクリーン、またはウイルスであることが証明されるまで添付ファイルを含む疑わしいメッセージは隔離されます。

小規模の非ウイルス性の脅威には、Web セキュリティ サービスによる検出を回避するために短期間オンラインになる可能性のある不正な Web サイトへの URL、または Web セキュリティを回避するため、信頼できる Web サイトを途中で置いて URL 短縮サービスを經由する URL が含まれます。脅威レベルのしきい値を満たす URL を含んでいるメッセージの隔離によって、CASE は SIO が提供するアップデートされたアウトブレイク ルールに基づいてメッセージの内容を再評価できるだけでなく、リンクされた Web サイトがオフラインになるか、Web セキュリティ ソリューションによってブロックできるほど長く、メッセージを隔離のままにしておくことができます。

疑いのあるメッセージに対するアウトブレイク フィルタの隔離方法の詳細については、「[動的隔離](#)」(P.14-9) を参照してください。

URL のリダイレクト

CASE がアウトブレイク フィルタの段階でメッセージをスキャンする場合、他の疑わしい内容に加えてメッセージ本文に URL があるかどうか検索します。CASE は、発行されたアウトブレイク ルールを使用して、そのメッセージが脅威であるかどうかを評価して、次に適切な脅威レベルでメッセージをス

コアリングします。脅威レベルに応じて、アウトブレイク フィルタは、受信者が Cisco Web セキュリティ プロキシにリダイレクトされるように、バイパスされたドメインを指している URL を除くすべての URL を書き換えることによって受信者を保護します。メッセージがより大きなアウトブレイクの一部であると思われる場合は、TOC が Web サイトについてさらに詳しく調べるためにメッセージの配信を遅らせます。信頼ドメインへの URL のバイパスの詳細については、「[URL 書き換えおよびドメインのバイパス](#)」(P.14-17) を参照してください。

電子メール セキュリティ アプライアンスがメッセージをリリースおよび配信した後で、受信者による Web サイトへのアクセスの試行があれば、Cisco Web セキュリティ プロキシによってリダイレクトされます。これは、シスコによってホストされている外部プロキシで、Web サイトが引き続き使用可能な場合、その Web サイトが危険である可能性があることをユーザに警告するスプラッシュ画面を表示します。Web サイトがオフラインになった場合は、スプラッシュ画面にエラー メッセージが表示されます。

受信者がメッセージの URL をクリックすることにした場合、Cisco Web セキュリティ プロキシは、ユーザの Web ブラウザにスプラッシュ画面を表示して、メッセージの内容について警告します。[図 14-1](#) に、スプラッシュ画面の警告の例を示します。受信者は、[この警告を無視する (Ignore this warning)] をクリックして Web サイトへ進み続けるか、[終了 (Exit)] をクリックして退出し、ブラウザ ウィンドウを安全に閉じることができます。

図 14-1 シスコのセキュリティによるスプラッシュ画面の警告



Cisco Web セキュリティ プロキシにアクセスする唯一の方法は、メッセージ内の URL を書き換えることです。Web ブラウザで URL を入力しても、プロキシにはアクセスできません。

メッセージの変更

アウトブレイク フィルタ機能は、非ウイルス性の脅威であるメッセージのメッセージ本文を変更して、URL を書き換えるだけでなく、メッセージが疑わしい脅威であるというアラートをユーザに出します。アウトブレイク フィルタ機能は、件名ヘッダーを変更したり、メッセージ本文上部にメッセージの内容について免責事項を追加したりできます。詳細については、「[メッセージ変更](#)」(P.14-17) を参照してください。

脅威の免責事項は、[メール ポリシー (Mail Policies)] > [テキストリソース (Text Resources)] ページから免責事項テンプレートを使用して作成されます。詳細については、「[テキストリソース管理の概要](#)」(P.18-9) を参照してください。

ルールのタイプ：アダプティブ ルールおよびアウトブレイク ルール

アウトブレイク フィルタでは、アダプティブ ルールおよびアウトブレイク ルールの 2 つのタイプのルールを使用して、潜在的なアウトブレイクを検出します。アウトブレイク フィルタ機能は、これらの 2 つのルールセットを使用して、高い有効性を持ち、綿密に的を絞った、一連の脅威検出基準を提供することで、フィルタが確実に特定のアウトブレイクに正確に照準を合わせることができるようにしています。アウトブレイク フィルタのルールおよびアクションは、水面下に隠されているものではなく、管理者の目に見えるようになっており、隔離されたメッセージにただちにアクセスしたり、隔離された理由を確認したりできるようになっています。

アウトブレイク ルール

アウトブレイク ルールは、Cisco Security Intelligence Operations の一部である、Cisco Threat Operations Center (TOC) で作成されるもので、添付ファイルのタイプだけでなく、メッセージ全体に焦点を当てています。アウトブレイク ルールは、SenderBase データ（リアルタイムおよび履歴のトラフィック データ）およびその他のあらゆるメッセージ パラメータの組み合わせ（添付ファイル タイプ、ファイル名のキーワード、またはアンチウイルス エンジンのアップデート）を使用して、リアルタイムでアウトブレイクを認識し、防止します。アウトブレイク ルールには一意の ID が付けられ、GUI のさまざまな場所（たとえばアウトブレイク 隔離など）でルールを参照するために使用されます。

グローバル SenderBase ネットワークからのリアルタイム データは、このベースラインと比較され、アウトブレイクの確かな前兆である異常を識別します。TOC は、データをレビューして脅威のインジケータまたは脅威レベルを発行します。脅威レベルは 0（脅威なし）から 5（非常に危険）の範囲の数値で表し、メッセージが Cisco のお客様による他のゲートウェイの防御が広く導入されていない脅威の可能性を判断します（詳細については、「[脅威レベル](#)」(P.14-7) を参照してください)。脅威レベルは、TOC によりアウトブレイク ルールとして発行されます。

アウトブレイク ルール内で組み合わせることができる特性には、たとえば次のようなものがあります。

- ファイル タイプ、ファイル タイプとサイズ、ファイル タイプとファイル名キーワードなど
- ファイル名キーワードとファイル サイズ
- ファイル名キーワード
- メッセージ URL
- ファイル名と Sophos IDE

アダプティブ ルール

アダプティブ ルールは、CASE 内の一連のルールであり、メッセージの属性を既知のウイルス アウトブレイク メッセージの属性と正確に比較します。これらのルールは、Cisco の広範なウイルス コーパスの中で、既知の脅威のメッセージおよび既知の良好なメッセージを研究し、作成されたものです。アダプティブ ルールは、コーパスの評価に合わせて、頻繁にアップデートされます。アダプティブ ルールは、既存のアウトブレイク ルールを補完して、常にアウトブレイク メッセージを検出します。アウトブレイク ルールは、アウトブレイクの可能性がある状態が発生したときに有効になりますが、アダプティブ ルールは（いったんイネーブルにされると）「常時オン」となり、グローバルな規模で本格的な異常が起きる前にローカルでアウトブレイク メッセージを捕捉します。さらに、アダプティブ ルールは、電子メール トラフィックおよび構造の小規模および微小な変化にも継続的に対応し、お客様にアップデートした保護を提供します。

アウトブレイク

アウトブレイク フィルタ ルールは、基本的に、電子メールのメッセージおよび添付ファイルの一連の特性（ファイル サイズ、ファイル タイプ、ファイル名、メッセージの内容など）に関連付けられた脅威レベル（例：4）です。たとえば、ファイル名に特定のキーワード（たとえば「hello」）が含まれた .exe 形式のファイル（サイズは 143 KB）が添付された、疑わしい電子メール メッセージの発生が増加していることを、Cisco SIO が通知したと想定します。この基準に一致するメッセージに対する脅威レベルを上げたアウトブレイク ルールが発行されます。デフォルトでは、Cisco アプライアンスは、新しく発行されたアウトブレイク ルールおよびアダプティブ ルールを 5 分ごとにチェックし、ダウンロードします（「[アウトブレイク フィルタ ルールのアップデート](#)」（P.14-14）を参照）。アダプティブ ルールは、アウトブレイク ルールほど頻繁にはアップデートされません。Cisco アプライアンスで、疑わしいメッセージの隔離についてしきい値を設定します。メッセージの脅威レベルが隔離のしきい値以上の場合、メッセージはアウトブレイク 隔離エリアに送信されます。非ウイルス性の脅威のメッセージの変更についてしきい値を設定して、疑わしいメッセージで発見された URL すべてを書き換えたり、メッセージ本文の上部に通知を追加したりできます。

脅威レベル

表 14-1 (P.14-7) に、各レベルの基本的なガイドラインまたは定義のセットを示します。

表 14-1 脅威レベルの定義

レベル	リスク	意味
0	なし	メッセージが脅威であるリスクはありません。
1	低	メッセージが脅威であるリスクは低です。
2	低または中	メッセージが脅威であるリスクは低から中です。これは「疑わしい」脅威です。
3	中	メッセージが確認されているアウトブレイクの一部であるか、メッセージの内容が脅威である中から高のリスクがあります。
4	高	メッセージが大規模アウトブレイクの一部であることが確認されているか、メッセージの内容が非常に危険です。
5	きわめて高	メッセージの内容が、非常に大規模または大規模な、かつ非常に危険なアウトブレイクの一部であることが確認されています。

脅威レベルおよびアウトブレイク ルールの詳細については、「[アウトブレイク フィルタ ルール](#)」（P.14-14）を参照してください。

隔離脅威レベルのしきい値設定ガイドライン

隔離脅威レベルのしきい値を使用することで、管理者は疑いのあるメッセージをより積極的または消極的に隔離できるようになります。低い値（1 または 2）は、より積極的な設定値で、多くのメッセージが隔離されます。反対に、高いスコア（4 または 5）は消極的な設定値で、不正である可能性がきわめて高いメッセージのみが隔離されます。

ウイルス アウトブレイクおよび非ウイルス性の脅威の両方に同じしきい値が適用されますが、ウイルス攻撃およびその他の脅威に対して、異なる隔離の保持期間を指定できます。詳細については、「[動的隔離](#)」（P.14-9）を参照してください。

シスコは、デフォルト値の 3 を推奨します。

コンテナ：特定ルールおよび常時ルール

コンテナ ファイルとは、他のファイルを含むジップ (.zip) アーカイブなどのファイルです。TOC は、アーカイブ ファイル内の特定のファイル进行处理するルールを発行できます。

たとえば、TOC により、あるウイルス アウトブレイクが、1 つの .exe を含む 1 つの .zip ファイルで構成されていると判別された場合は、.zip ファイル内の .exe ファイル (.zip(exe)) に脅威レベルを設定する特定のアウトブレイク ルールが発行されます。ただし .zip ファイル内に含まれるその他のファイルタイプ (たとえば .txt ファイル) には特定の脅威レベルを設定しません。2 番目のルール (.zip(*)) は、コンテナ ファイルタイプ内のその他すべてのファイルタイプをカバーします。コンテナに対する常時ルールは、コンテナ内にあるファイルのタイプに関係なく、メッセージの脅威レベル計算に常に使用されます。そのようなコンテナタイプが危険であると判明した場合は、常時ルールが SIO により発行されます。

表 14-2 フォールバック ルールおよび脅威レベル スコア

アウトブレイク ルール	脅威レベル	説明
.zip(exe)	4	このルールは、.zip ファイル内の .exe ファイルの脅威レベルを 4 に設定します。
.zip(doc)	0	このルールは、.zip ファイル内の .doc ファイルの脅威レベルを 0 に設定します。
zip(*)	2	このルールは、含まれているファイルのタイプに関係なく、すべての .zip ファイルの脅威レベルを 2 に設定します。

アウトブレイク フィルタの機能概要

電子メール メッセージは、Cisco アプライアンスで処理される際に、「電子メール パイプライン」と呼ばれる一連の手順を通過します (電子メール パイプラインの詳細については、「[電子メール パイプラインの理解](#)」(P.4-1) を参照してください)。メッセージは電子メール パイプラインを通過するので、これらのエンジンがメール ポリシーをイネーブルにしている場合、アンチスパムおよびアンチウイルス スキャンを実行します。言い換えると、認識されているウイルスが含まれる既知のスパムまたはメッセージは、アウトブレイク フィルタ機能でスキャンされる前に、アンチスパムおよびアンチウイルス 設定に基づいてメール ストリームから除去 (削除、隔離など) されているため、アウトブレイク フィルタ機能ではスキャンされません。このため、アウトブレイク フィルタ機能に到達するメッセージは、スパムおよびウイルスを含まないとマークされています。アウトブレイク フィルタによって隔離されたメッセージは、CASE によって隔離解除されて、再スキャンされる際、アップデートされたスパム ルールおよびウイルス定義に基づいて、スパムまたはウイルスを含んでいるとしてマークされる可能性があることに注意してください。



(注)

フィルタおよびエンジンがディセーブルになっていることでアンチスパムおよびアンチウイルス スキャンをスキップするメッセージでも、アウトブレイク フィルタによってスキャンされます。

メッセージ スコアリング

新しいウイルス攻撃または非ウイルス性の脅威がコンピュータ ネットワークに放たれた時点では、脅威を認識できるアンチウイルスやアンチスパム ソフトウェアはまだありません。アウトブレイク フィルタ機能が非常に重要となるのは、このときです。着信メッセージは、発行されているアウトブレイク およびアダプティブ ルールを使用して、CASE によりスキャンおよびスコアリングされます (「[ルール のタイプ：アダプティブ ルールおよびアウトブレイク ルール](#)」(P.14-6) を参照)。メッセージ スコア

はメッセージの脅威レベルに対応しています。メッセージに該当するルールがあった場合は、どのルールに一致したかによって、CASE は対応する脅威レベルを割り当てます。関連する脅威レベルが存在しない（メッセージに一致するルールが存在しない）場合は、メッセージには脅威レベル 0 が割り当てられます。

その計算が完了すると、電子メール セキュリティ アプライアンスは、メッセージの脅威レベルが隔離またはメッセージ変更のしきい値以上であるかどうかをチェックし、メッセージを隔離するかメッセージの URL を書き換えます。脅威レベルがしきい値を下回る場合、パイプラインの後続の処理が継続されます。

さらに、CASE は既存の隔離されているメッセージを最新のルールに照らして再評価し、メッセージの最新の脅威レベルを決定します。これにより、アウトブレイク メッセージに整合する脅威レベルを持つメッセージのみが隔離され続け、脅威と見なされなくなったメッセージは自動再評価の後に隔離エリアから解放されます。

1 つのアウトブレイク メッセージで複数のスコアが存在する場合（1 つのスコアが、あるアダプティブルールに基づいたもの（または該当するアダプティブルールが複数ある場合はそのうちの最も高いスコア）で、別のスコアはあるアウトブレイク ルールに基づいたもの（または該当するアウトブレイク ルールが複数ある場合はそのうちの最も高いスコア）である場合）は、インテリジェント アルゴリズムを使用して最終的な脅威レベルが決定されます。



(注)

アウトブレイク フィルタ機能は、Cisco アプライアンスでアンチウイルス スキャンをイネーブルにしなくても使用できます。この 2 つのセキュリティ サービスは、お互いを補完するように設計されていますが、別々に動作しています。ただし、Cisco アプライアンスでアンチウイルス スキャンをイネーブルにしていない場合は、アンチウイルス ベンダーのアップデートをモニタリングして、アウトブレイク 隔離エリアにあるメッセージの一部を手動で隔離解除したり、再評価したりする必要があります。アンチウイルス スキャンをイネーブルにしないでアウトブレイク フィルタを使用する場合は、次の点に注意してください。

- アダプティブ ルールはディセーブルにする必要があります。
- メッセージはアウトブレイク ルールに従って隔離されます。
- 脅威レベルが引き下げられたり、隔離時間の期限が過ぎたりした場合は、メッセージは隔離解除されます。

ダウンストリームのアンチウイルス ベンダー（デスクトップおよびグループウェア）は、隔離解除されたメッセージを捕捉する場合があります。



(注)

アウトブレイク フィルタ機能が非ウイルス性の脅威をスキャンするために、アンチスパム スキャンをアプライアンスでグローバルにイネーブルにする必要があります。

動的隔離

アウトブレイク フィルタ機能のアウトブレイク 隔離エリアは、メッセージが脅威であると確認されるか、ユーザに配信しても安全であることが確認されるまで、一時的にメッセージを保管しておくための保持領域です。（詳細については、「[アウトブレイク ライフサイクルおよびルール発行](#)」(P.14-10) を参照してください)。隔離されたメッセージは、複数の方法でアウトブレイク 隔離エリアから解放できます。新しいルールがダウンロードされると、アウトブレイク 隔離エリアにあるメッセージは、CASE によって計算された推奨再スキャン間隔に基づいて再評価されます。更新されたメッセージの脅威レベルが隔離保持のしきい値よりも低くなった場合、メッセージは自動的に（アウトブレイク 隔離の設定に関係なく）隔離解除されるため、メッセージが隔離されている時間を最小限に抑えることができます。メッセージの再評価中に新しいルールが発行された場合は、再スキャンが開始されます。

ウイルス攻撃として隔離されるメッセージは、新しいアンチウイルス シグニチャが使用可能な場合は、自動的にアウトブレイク隔離エリアから解放されることはないため、注意してください。新しいルールは、新しいアンチウイルス シグニチャを参照している場合と、参照していない場合があります。ただし、アウトブレイク ルールによりメッセージの脅威レベルが設定されている脅威レベルのしきい値よりも低いスコアに変更されない限り、アンチウイルス エンジンがアップデートされたことによって、メッセージが隔離解除されることはありません。

CASE の推奨保持期間が経過した場合も、メッセージはアウトブレイク隔離エリアから解放されます。CASE は、メッセージの脅威レベルに基づいて保持期間を計算します。ウイルス アウトブレイクおよび非ウイルス性の脅威に対して別々の最大保持期間を定義できます。CASE の推奨保持期間がその脅威タイプの最大保持期間を超える場合、電子メール セキュリティ アプライアンスは、最大保持期間が経過した時点でメッセージを解放します。ウイルス性のメッセージのデフォルトの最大隔離期間は 1 日です。非ウイルス性の脅威を隔離するデフォルト期間は 4 時間です。メッセージを、手動で隔離解除できます。

また、隔離エリアがいっぱいであるときに、追加のメッセージが挿入されると電子メール セキュリティ アプライアンスもメッセージを解放します（これはオーバーフローと呼ばれます）。オーバーフローは、アウトブレイク隔離エリアが容量の 100 % まで使用されているときに、新しいメッセージが隔離エリアに追加された場合のみ発生します。このとき、メッセージが隔離解除される優先順位は次のとおりです。

- アダプティブルールにより隔離されたメッセージ（最も早く隔離解除されるようにスケジュール設定されているものから）
- アウトブレイク ルールにより隔離されたメッセージ（最も早く隔離解除されるようにスケジュール設定されているものから）

アウトブレイク隔離エリアの使用量が容量の 100 % を下回った時点で、オーバーフローは停止します。隔離エリアのオーバーフローの処理方法に関する詳細については、「[隔離エリアのメッセージ保存期間](#)」(P.27-4) および「[自動的に処理された隔離メッセージのデフォルトアクション](#)」(P.27-5) を参照してください。

アウトブレイク隔離エリアから解放されたメッセージは、アンチウイルスおよびアンチスパム エンジンがメール ポリシーでイネーブルとなっている場合、アンチウイルスおよびアンチスパム エンジンによって再度スキャンされます。このときに既知のウイルスまたはスパムとしてマークされた場合は、このメッセージはメール ポリシー設定に従って処理されます（Virus 隔離エリアまたは Cisco Spam 隔離エリアに隔離される場合もあります）。詳細については、「[アウトブレイク フィルタ機能とアウトブレイク隔離](#)」(P.14-19) を参照してください。

このため、メッセージのライフタイムの間に、メッセージは 2 回隔離される場合がある（1 回はアウトブレイク フィルタ機能により、もう 1 回はアウトブレイク隔離エリアから解放されたとき）と注意しておくことが重要です。各スキャン（アウトブレイク フィルタの前およびアウトブレイク隔離エリアから解放されたとき）照合の結果、何らかの判断がなされたメッセージは、2 回隔離されることはありません。また、アウトブレイク フィルタ機能により、メッセージに対して最終的なアクションが実行されることはないことにも注意してください。アウトブレイク フィルタ機能は、（後続の処理のために）メッセージを隔離するか、またはメッセージをパイプラインの次の手順に移動します。

アウトブレイク ライフサイクルおよびルール発行

ウイルスのアウトブレイク ライフサイクルの非常に初期の段階では、メッセージを隔離するために広範なルールが多く使用されます。より詳しい情報が判明していくと、よりの絞ったルールが発行され、隔離する対象の定義が絞り込まれていきます。新しいルールが発行されると、その時点でウイルスメッセージの可能性があると見なされなくなったメッセージは、隔離解除されます（アウトブレイク隔離エリアにあるメッセージは、新しいルールが発行されると再スキャンされます）。

表 14-3 アウトブレイク ライフサイクルのルールの例

時間	ルールの種類	ルールの説明	アクション
T=0	アダプティブ ルール (過去の アウトブレイク に基づく)	10 万を超えるメッセージ属性 に基づく、統合されたルール セットで、メッセージの内容、 コンテキスト、および構造を分 析します。	アダプティブ ルールに一致したメッ セージは、自動的に隔離されます。
T=5 分	アウトブレイク ルール	.zip (exe) ファイルが含まれ るメッセージを隔離します。	.exe が含まれる .zip 形式の添付ファイ ルはすべて隔離されます。
T=10 分	アウトブレイク ルール	50 KB を超える .zip (exe) ファイルが含まれるメッセージ を隔離します。	50 KB 未満の .zip (exe) ファイルが含 まれたメッセージはすべて隔離解除さ れます。
T=20 分	アウトブレイク ルール	ファイル名に「Price」が含ま れる 50 ~ 55 KB の .zip (exe) ファイルが含まれるメッセージ を隔離します。	この基準に一致しないメッセージはす べて隔離解除されます。
T=12 時 間	アウトブレイク ルール	新しいシグニチャを使用してス キャンします。	残っているすべてのメッセージを、最 新のアンチウイルス シグニチャを使用 してスキャンします。

アウトブレイク フィルタの管理 (GUI)

グラフィカル ユーザ インターフェイス (GUI) にログインし、メニューの [セキュリティ サービス (Security Services)] を選択して、[アウトブレイク フィルタ (Outbreak Filters)] をクリックします。

図 14-2 [アウトブレイク フィルタ (Outbreak Filters)] メインページ
Outbreak Filters

Outbreak Filters Overview		
Global Status:	Enabled	
Adaptive Rules:	Enabled	
Maximum Message Size to Scan:	512K	
Receive Emailed Alerts:	No	
Edit Global Settings...		

Outbreak Filter Rules		
Rule Updates		
Rule Type	Last Update	Current Version
CASE Core Files	Never Updated	3.1.0-012
CASE Utilities	Never Updated	3.1.0-012
Virus Outbreak Rules	Never Updated	20050710_000000
Outbreak Filter Rules (higher number indicates greater risk. 1= lowest threat, 5= highest threat)		
3	OUTBREAK_0003427	We are seeing unusual volume for file extension(s) pif. We are raising the Threat Level to 3. We wil...
3	OUTBREAK_0003420	We are seeing unusual volume for file extension(s) exe. We are raising the Threat Level to 3. We wil...
3	OUTBREAK_0003429	We are seeing unusual volume for file extension(s) zip(exe), zipr(exe). We are raising the Threat L...
3	OUTBREAK_0003430	We are seeing suspicious url(s) propagating through multiple sources. We are raising the Threat Leve...
3	OUTBREAK_0003431	We are seeing suspicious url(s) propagating through multiple sources. We are raising the Threat Leve...
Rules last updated: Wed May 25 22:36:12 2011		
Update Rules Now Clear Current Rules		

[アウトブレイク フィルタ (Outbreak Filters)] ページには、[アウトブレイク フィルタの概要 (Outbreak Filters Overview)] と現在の [アウトブレイク フィルタのルール (Outbreak Filter Rules)] (存在する場合) のリストの 2 つのセクションが表示されます。

図 14-2 で、アウトブレイク フィルタはイネーブル、Adaptive Scanning はイネーブル、また最大メッセージサイズは 512 K に設定されています。これらの設定を変更するには、[グローバル設定を編集 (Edit Global Settings)] をクリックします。グローバル設定の編集に関する詳細については、「アウトブレイク フィルタのグローバル設定の構成」(P.14-12) を参照してください。

[アウトブレイク フィルタのルール (Outbreak Filter Rules)] セクションには、各種コンポーネント (ルール自体だけでなくルール エンジンも含む) の最新アップデートの時刻、日付、およびバージョンのリストと、脅威レベルとともにアウトブレイク フィルタ ルールのリストが示されます。

アウトブレイク ルールの詳細については、「アウトブレイク フィルタルール」(P.14-14) を参照してください。

アウトブレイク フィルタのグローバル設定の構成

ウイルス アウトブレイク フィルタのグローバル設定を設定するには、[グローバル設定を編集 (Edit Global Settings)] をクリックします。

図 14-3 [アウトブレイク フィルタのグローバル設定 (Outbreak Filters Global Settings)] ページ
Edit Outbreak Filters Settings

Outbreak Filters Global Settings	
<input checked="" type="checkbox"/> Enable Outbreak Filters	
Adaptive Rules:	<input checked="" type="checkbox"/> Enable Adaptive Rules
Maximum Message Size to Scan:	512k Maximum <small>Add a trailing K or M to indicate units.</small>
Emailed Alerts: ?	<input type="checkbox"/> Receive Emailed Alerts

Cancel Submit

このページを使用して、次のことを行います。

- アウトブレイク フィルタをグローバルにイネーブルにします。
- アダプティブ ルールのスキャンをイネーブルにします。
- スキャンするファイルの最大サイズを設定します (サイズをバイトで入力することに注意してください)
- アウトブレイク フィルタのアラートをイネーブルにするかどうかを選択します。

アラートおよびアダプティブ ルールはデフォルトではイネーブルになっていないため、注意してください。この機能は、outbreakconfig CLI コマンドから也可以使用できます (『Cisco AsyncOS CLI Reference Guide』を参照)。変更を加えたら、送信して確定します。

アウトブレイク フィルタ機能のイネーブル化

アウトブレイク フィルタ機能をグローバルにイネーブルにするには、[アウトブレイク フィルタのグローバル設定 (Outbreak Filters Global Settings)] ページの [アウトブレイク フィルタを有効にする (Enable Outbreak Filters)] の横にあるボックスをオンにして、[送信 (Submit)] をクリックします。事前にアウトブレイク フィルタのライセンス契約書に同意しておく必要があります。

いったんグローバルにイネーブルにした後は、アウトブレイク フィルタ機能は、各送受信メール ポリシー (デフォルト ポリシーも含む) に対して個別にイネーブルまたはディセーブルにできます。詳細については、「[アウトブレイク フィルタ機能とメール ポリシー](#)」(P.14-14) を参照してください。

アウトブレイク フィルタ機能は、アンチスパム スキャンがイネーブルになっているかどうかに関係なく、Context Adaptive Scanning Engine (CASE) を使用してウイルス性の脅威を検出します。ただし、非ウイルス性の脅威をスキャンするために、アプライアンスで Cisco Anti-Spam または Intelligent Multi-Scan をグローバルにイネーブルにする必要があります。



(注) システムのセットアップ中にライセンスに同意しなかった場合 (『手順 4 : セキュリティ』(P.3-20) を参照) は、[セキュリティ サービス (Security Services)] > [アウトブレイク フィルタ (Outbreak Filters)] ページで [有効 (Enable)] をクリックして、ライセンス契約を読み、同意する必要があります。

アダプティブ ルールのイネーブル化

Adaptive Scanning は、アウトブレイク フィルタのアダプティブ ルールをイネーブルにします。メッセージの内容に関するウイルス シグニチャまたはスパム基準が使用できない場合は、一連の係数または特性 (ファイル サイズなど) が使用されて、メッセージがアウトブレイクの一部である可能性が決定されます。Adaptive Scanning をイネーブルにするには、[アウトブレイク フィルタのグローバル設定 (Outbreak Filters Global Settings)] ページの [適応ルールを有効にする (Enable Adaptive Rules)] の横にあるボックスをオンにして、[送信 (Submit)] をクリックします。

アウトブレイク フィルタのアラートのイネーブル化

[アラート メール (Emailed Alerts)] というラベルの付いたボックスをオンにして、アウトブレイク フィルタ機能のアラートをイネーブルにします。アウトブレイク フィルタの電子メール アラートのイネーブル化は、単にアラート エンジン をイネーブルにして、アウトブレイク フィルタに関するアラートが送信されるようにするためのものです。送信されるアラートおよび送信先の電子メール アドレスの指定は、[アラート (Alerts)] ページの [システム管理 (System Administration)] タブで設定します。アウトブレイク フィルタのアラートの設定に関する詳細については、「アラート、SNMP トラップ、およびアウトブレイク フィルタ」(P.14-22) を参照してください。

アウトブレイク フィルタ ルール

アウトブレイク ルールは、Cisco Security Intelligence Operations から発行されます。Cisco アプライアンスは新しいアウトブレイク ルールを 5 分ごとにチェックおよびダウンロードします。このアップデート間隔を変更できます。詳細については、「アップグレードおよびアップデートをダウンロードするためのサーバ設定」(P.29-22) を参照してください。

アウトブレイク フィルタ ルールの管理

アウトブレイク フィルタ ルールは自動的にダウンロードされるため、ユーザによる管理は一切必要ありません。

ただし、何らかの理由で Cisco アプライアンスが一定期間 Cisco のアップデート サーバの新しいルールにアクセスできない場合は、ローカルでキャッシュされているスコアが有効でなくなっている（つまり、既知のウイルス性の添付ファイル タイプが現在ではアンチウイルス ソフトウェアのアップデートに含まれている、またはすでに脅威ではなくなっている、またはその両方の場合）可能性があります。この場合は、これらの特性を持つメッセージを隔離しておく必要はありません。

[ルールを今すぐアップデート (Update Rules Now)] をクリックすることによって、シスコのアップデートサーバから、アップデートされたアウトブレイク ルールを手動でダウンロードできます。



(注) [ルールを今すぐアップデート (Update Rules Now)] ボタンは、アプライアンスの既存のアウトブレイク ルールを「フラッシュ」しません。アップデートされたアウトブレイク ルールを置き換えるだけです。シスコのアップデートサーバに利用可能なアップデートがない場合、アプライアンスはこのボタンをクリックするまでアウトブレイク ルールをダウンロードしません。

アウトブレイク フィルタ ルールのアップデート

デフォルトでは、Cisco アプライアンスは 5 分ごとに新しいアウトブレイク フィルタ ルールのダウンロードを試行します。この間隔は、[セキュリティ サービス (Security Services)] > [サービスのアップデート (Service Updates)] ページで変更できます。詳細については、「サービスのアップデート」(P.29-22) を参照してください。

アウトブレイク フィルタ機能とメール ポリシー

アウトブレイク フィルタ機能の設定には、メール ポリシーごとに設定できるものがあります。アウトブレイク フィルタ機能は、アプライアンスでメール ポリシーごとにイネーブルまたはディセーブルにできます。メール ポリシーごとに、特定のファイル拡張子およびドメインをアウトブレイク フィルタ機能の処理から除外できます。この機能は、policyconfig CLI コマンドから使用できます（『Cisco AsyncOS CLI Reference Guide』を参照）。



(注)

アウトブレイク フィルタ機能が非ウイルス性の脅威をスキャンするために、Cisco Anti-Spam または Intelligent Multi-Scan スキャンをアプライアンスでグローバルにイネーブルにする必要があります。

図 14-4 メール ポリシーのリスト
Incoming Mail Policies

Find Policies						
Email Address:				<input type="radio"/> Recipient <input checked="" type="radio"/> Sender	Find Policies	
Policies						
Add Policy...						
Order	Policy Name	Anti-Spam	Anti-Virus	Content Filters	Outbreak Filters	Delete
1	Sales_Team	IronPort Anti-Spam Positive: Drop Suspected: Quarantine Marketing Messages: Quarantine	(use default)	(use default)	(use default)	
2	Engineering	(use default)	(use default)	scan_for_confidential ex_employee	Retention Time: Virus: 1 day Other: 4 hours	
	Default Policy	IronPort Anti-Spam Positive: Drop Suspected: Deliver Marketing Messages: Disabled	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	scan_for_confidential no_mps ex_employee	Retention Time: Virus: 1 day	

Key: Default Custom ReadOnly

特定のメール ポリシーに対するアウトブレイク フィルタ機能の設定を変更するには、変更するポリシーの [アウトブレイク フィルタ (Outbreak Filters)] 列のリンクをクリックします。

図 14-5 アウトブレイク フィルタ設定とメール ポリシー
Mail Policies: Outbreak Filters

Outbreak Filtering for Policy: Sales_Team

Enable Outbreak Filtering (Customize settings)

Outbreak Filter Settings

Quarantine Threat Level: 3

Maximum Quarantine Retention: Viral Attachments: 1 Days, Other Threats: 4 Hours

Bypass Attachment Scanning: None configured

Message Modification

Enable Message Modification

Message Modification Threat Level: 3

Message Subject: Prepend [MODIFIED FOR PROTECTION]

URL Rewriting: Cisco Security proxy scans and rewrites all URLs contained in malicious outbreak emails.
 Enable only for unsigned messages (recommended)
 Enable for all messages
 Disable

Bypass Domain Scanning:

(examples: example.com, crm.example.com, 10.0.0.1, 10.0.0.0/24)

Threat Disclaimer: None
Disclaimer text will be applied to the top of the message body for Suspicious and Quarantined messages. To create custom disclaimers go to Mail Policies > Text Resources

Cancel Submit

特定のメール ポリシーに対してアウトブレイク フィルタ機能をイネーブルにし、カスタマイズするには、[アウトブレイク フィルタを有効にする (設定をカスタマイズ) (Enable Outbreak Filtering (Customize Settings))] を選択します。

メール ポリシーに対して次のアウトブレイク フィルタ設定を構成できます。

- 隔離脅威レベル。
- 最大隔離保持期間。
- バイパスするファイル拡張子のタイプ。
- メッセージ変更のしきい値。
- メッセージの件名。
- URL 書き換え。
- 脅威の免責事項。

[アウトブレイク フィルタを有効にする (デフォルトのメール ポリシー設定を継承) (Enable Outbreak Filtering (Inherit Default mail policy settings))] を選択して、デフォルトのメール ポリシーについて定義されているアウトブレイク フィルタ設定を使用します。デフォルト メール ポリシーでアウトブレイク フィルタ機能をイネーブルにしている場合は、その他すべてのメール ポリシーはカスタマイズしない限り同じアウトブレイク フィルタ設定を使用します。

設定を変更したら、変更を確定します。

隔離レベルのしきい値の設定

リストからアウトブレイクの脅威に対する [隔離する脅威レベル (Quarantine Threat Level)] のしきい値を選択します。数字が小さいほど隔離されるメッセージは多くなり、数字が大きいくほど隔離されるメッセージは少なくなります。シスコは、デフォルト値の 3 を推奨します。

詳細については、「[隔離脅威レベルのしきい値設定ガイドライン](#)」(P.14-7) を参照してください。

最大隔離保持

メッセージがアウトブレイク隔離エリアにとどまる最大時間を時間単位または日単位で指定します。ウイルス性の添付ファイルを含む可能性のあるメッセージ、およびフィッシングやマルウェア リンクなどその他の脅威を含む可能性のあるメッセージに対して異なる保持期間を指定できます。ポリシーで [メッセージの変更 (Message Modification)] をイネーブルにしない限り、非ウイルス性の脅威を隔離できません。

CASE は、メッセージに脅威レベルを割り当てるときに隔離保持期間を推奨しています。電子メールセキュリティ アプライアンスは、脅威タイプに対する最大隔離保持期間を超えない限り、CASE が推奨する時間の長さの間、隔離されるメッセージを保持します。

ファイル拡張子タイプのバイパス

特定のファイルタイプをバイパスするようにポリシーを変更できます。バイパスされたファイル拡張子は、CASE によるメッセージの脅威レベルの計算から除外されます。ただし、添付ファイルに対する残りの電子メールセキュリティパイプラインの処理は行われます。

ファイル拡張子をバイパスするには、[添付ファイルのスキャンのバイパス (Bypass Attachment Scanning)] をクリックし、ファイル拡張子を選択または入力してから、[拡張子を追加 (Add Extension)] をクリックします。AsyncOS は、[バイパスするファイル拡張子 (File Extensions to Bypass)] リストに拡張子タイプを表示します。

バイパスされる拡張子のリストから拡張子を削除するには、[バイパスするファイル拡張子 (File Extensions to Bypass)] リストの拡張子の横のゴミ箱アイコンをクリックします。

ファイル拡張子のバイパス : コンテナ ファイルのタイプ

ファイル拡張子をバイパスする場合、コンテナ ファイル内のファイル (たとえば .zip 内の .doc ファイル) もバイパスする拡張子のリストに含まれていれば、バイパスされます。たとえば、バイパスする拡張子のリストに .doc を追加した場合は、コンテナ ファイルに含まれているものも含めて、すべての .doc ファイルがバイパスされます。

メッセージ変更

アプライアンスがフィッシングの試行またはマルウェア Web サイトへのリンクなど非ウイルス性の脅威のメッセージをスキャンする場合は、[メッセージの変更 (Message Modification)] をイネーブルにします。

メッセージの脅威レベルに基づいて、AsyncOS はメッセージを変更し、すべての URL を書き換えて、メッセージから Web サイトを開こうとすると Cisco Web セキュリティ プロキシを経由して受信者をリダイレクトすることができます。アプライアンスはメッセージに免責事項を追加して、ユーザにメッセージの内容が疑わしい、または不正であることを警告することもできます。

非ウイルス性の脅威メッセージを隔離するために、メッセージ変更をイネーブルにする必要があります。

メッセージ変更の脅威レベル

リストから [メッセージの変更 - 脅威レベル (Message Modification Threat Level)] のしきい値を選択します。この設定は、CASE によって返される脅威レベルに基づいて、メッセージを変更するかどうかを決定します。数字が小さいほど変更されるメッセージは多くなり、数字が大きいくほど変更されるメッセージは少なくなります。シスコは、デフォルト値の 3 を推奨します。

メッセージの件名

特定のテキスト文字列を前後に追加することで、変更されたリンクを含む非ウイルス性の脅威メッセージで件名ヘッダーのテキストを変更すると、ユーザにメッセージが保護のために変更されたことを通知します。



(注) [メッセージの件名 (Message Subject)] フィールドでは、空白は無視されません。このフィールドに入力したテキストの後ろまたは前にスペース追加することで、オリジナルのメッセージ件名と、追加テキストを分けることができます (追加テキストをオリジナルの件名の前に追加する場合は追加テキストの前、オリジナルの件名の後ろに追加する場合は追加テキストの後ろにスペースを追加します)。たとえば、[MODIFIED: FOR PROTECTION] というテキストをオリジナルの件名の前に追加する場合は、この後ろに数個のスペースを追加します。



(注) [メッセージの件名 (Message Subject)] フィールドでは、US-ASCII 文字だけを使用できます。

URL 書き換えおよびドメインのバイパス

メッセージの脅威レベルがメッセージ変更のしきい値を超える場合、アウトブレイク フィルタ機能はメッセージ内のすべての URL を書き換え、これらの URL をクリックするとユーザを Cisco Web セキュリティ プロキシのスプラッシュ ページにリダイレクトします。(詳細については、「URL のリダイレクト」(P.14-4) を参照してください)。メッセージの脅威レベルが隔離のしきい値を超える場合、ア

プライアンスがメッセージの隔離も行います。小規模の非ウイルス性のアウトブレイクが進行中の場合、メッセージの隔離は TOC に、アウトブレイクの可能性があるメッセージからリンクされるすべての疑わしい Web サイトを分析し、その Web サイトが不正であるかどうか判断する時間を与えます。CASE は、SIO が提供するアップデートされたアウトブレイク ルールを使用してメッセージを再スキャンし、メッセージがアウトブレイクの一部であるかを判断します。保持期間が過ぎると、アプライアンスはメッセージを隔離エリアから解放します。

AsyncOS は、バイパスされるドメインを指している URL を除き、メッセージ内のすべての URL を書き換えます。

[URL の書き換え (URL Rewriting)] では次のオプションを使用できます。

- [未署名のメッセージでのみ有効 (Enable only for unsigned messages)]: このオプションによって、AsyncOS は、メッセージ変更のしきい値を満たすか超える未署名のメッセージ内の URL を書き換えられるようになります。ただし、署名されたメッセージは含まれません。URL 書き換えについて、シスコはこの設定の使用を推奨します。



(注) 電子メールセキュリティアプライアンス以外のネットワーク上のサーバまたはアプライアンスが DomainKeys/DKIM 署名の検証を担当する場合、電子メールセキュリティアプライアンスは、DomainKeys/DKIM-signed メッセージ内の URL を書き換えたり、メッセージの署名を無効にしたりすることができます。

- [すべてのメッセージで有効 (Enable for all messages)]: このオプションによって、AsyncOS は、メッセージ変更のしきい値を満たすか超えるすべてのメッセージ内の URL を書き換えられるようになります。署名されたメッセージも含まれます。AsyncOS が署名されたメッセージを変更すると、署名は無効になります。
- [無効 (Disable)]: このオプションはアウトブレイク フィルタに対して URL 書き換えをディセーブルにします。

ポリシーを変更して、特定のドメインへの URL を変更から除外できます。ドメインをバイパスするには、IPv4 アドレス、IPv6 アドレス、CIDR 範囲、ホスト名、部分ホスト名、またはドメインを [ドメインのスキャンをバイパス (Bypass Domain Scanning)] フィールドに入力します。複数のエントリを指定する場合は、カンマで区切ります。

脅威の免責事項

電子メールセキュリティアプライアンスは、疑わしいメッセージのヘッダーの上部に免責事項メッセージを追加して、ユーザにメッセージの内容を警告することができます。この免責事項には、メッセージのタイプに応じて HTML またはプレーンテキストが使用できます。

[脅威に関する免責事項 (Threat Disclaimer)] リストから使用する免責事項のテキストを選択するか、[メールポリシー (Mail Policies)] > [テキストリソース (Text Resources)] リンクをクリックし、[免責事項テンプレート (Disclaimer Template)] を使用して新しい免責事項を作成します。[免責事項テンプレート (Disclaimer Template)] には、アウトブレイク脅威情報に関する変数が含まれます。[免責事項のプレビュー (Preview Disclaimer)] をクリックすると、脅威免責事項のプレビューを表示できます。カスタム免責事項メッセージでは、変数を使用してメッセージの脅威レベル、脅威のタイプ、および脅威の説明を表示できます。免責事項メッセージの作成については、「[テキストリソース管理の概要](#)」(P.18-9) を参照してください。

アウトブレイク フィルタ機能とアウトブレイク隔離

アウトブレイク フィルタ機能により隔離されたメッセージは、アウトブレイク隔離エリアに送信されます。この隔離エリアは、メッセージを隔離するために使用されるルール（アウトブレイク ルールの場合はアウトブレイク ID、アダプティブ ルールの場合は一般名称が表示されます）に基づいて、隔離エリアからすべてのメッセージを削除または解放する際に役立つ「サマリー」ビューがあることを除けば、その他のあらゆる隔離と同様に機能します（隔離の操作方法の詳細については、第 27 章「隔離」を参照してください）。サマリー ビューの詳細については、「[アウトブレイク隔離 (Outbreak Quarantine)] および [ルール サマリーによる管理 (Manage by Rule Summary)] ビュー」(P.14-20)を参照してください。

図 14-6 アウトブレイク隔離
Edit Outbreak Quarantine

Settings	
Quarantine Name:	Outbreak
Space Allocation:	2048 MB (Maximum Size 4096 MB)
Default Action:	Release
When Allocated Space is Exceeded Send Messages and:	Modify Subject: Prepend [POSSIBLE VIRUS]
	Add X-Header: Name: <input type="text"/>
	Value: <input type="text"/>
	Strip Attachments: <input checked="" type="radio"/> No <input type="radio"/> Yes
Local Users:	No users selected
Externally Authenticated Users:	External authentication is disabled. Go to System Administration > Users to enable external authentication.
Custom User Roles:	Quarantine Manager

アウトブレイク隔離のモニタリング

適切に設定された隔離エリアはほとんどモニタリングを必要としませんが、特にウイルス アウトブレイクの発生中または発生後の、正規のメッセージが遅延する可能性がある間は、アウトブレイク隔離エリアに注意を払うことを推奨します。

正規のメッセージが隔離された場合、アウトブレイク隔離の設定によっては、次のいずれかが発生します。

- 隔離のデフォルト アクションが [リリース (Release)] に設定されている場合は、保持期間の期限が切れたとき、または隔離エリアがオーバーフローしたときにメッセージが解放されます。オーバーフローのためにメッセージが解放される前に、添付ファイルの削除、件名の変更、X-Header の追加といったアクションがメッセージに対して実行されるように、アウトブレイク隔離を設定できます。これらのアクションの詳細については、「自動的に処理された隔離メッセージのデフォルト アクション」(P.27-5)を参照してください。
- 隔離のデフォルト アクションが [削除 (Delete)] に設定されている場合は、保持期間の期限が切れたとき、または隔離エリアがオーバーフローしたときにメッセージが削除されます。
- オーバーフローは、隔離エリアがいっぱいのときにさらにメッセージが追加された場合に発生します。この場合は、有効期限日に近いメッセージから（必ずしも最も古いメッセージからとは限りません）、新しいメッセージに十分な領域が空くまで、メッセージが解放されていきます。オーバーフローのためにメッセージが解放される前に、添付ファイルの削除、件名の変更、X-Header の追加といったアクションがメッセージに対して実行されるように、アウトブレイク隔離を設定できます。

隔離されているメッセージは、新しいルールが発行されるたびに再スキャンされるため、アウトブレイク隔離エリアにあるメッセージは有効期限が切れる前に解放されることがほとんどです。

それでも、デフォルト アクションが [削除 (Delete)] に設定されている場合は、アウトブレイク 隔離をモニタすることが重要です。シスコは、ほとんどのユーザに対して、デフォルト アクションを [削除 (Delete)] に設定しないことを推奨します。アウトブレイク 隔離エリアからのメッセージの解放、またはアウトブレイク 隔離のデフォルト アクションの変更に関する詳細については、「[自動的に処理された隔離メッセージのデフォルト アクション](#)」(P.27-5) を参照してください。

反対に、新しいルールの上アップデートを待つ間、アウトブレイク 隔離エリアに長時間留めておきたいメッセージがある場合は、たとえばそのメッセージの有効期限を遅らせることもできます。メッセージの保持期間を増やすことにより、隔離エリアのサイズが大きくなる場合があるため、注意してください。



(注)

メッセージがアウトブレイク 隔離エリアに留まっている間にアンチウイルス スキャンが (メール ポリシーごとではなく) グローバルにディセーブルにされた場合は、たとえメッセージが解放される前にもう一度アンチウイルス スキャンを再度イネーブルにしたとしても、そのメッセージが解放されたときのアンチウイルス スキャンは実行されません。



(注)

アウトブレイク フィルタ機能は、Cisco アプライアンスでアンチウイルス スキャンをイネーブルにしなくても使用できます。ただし、アプライアンスでアンチスパム スキャンがイネーブルでない場合は、アウトブレイク フィルタは非ウイルス性の脅威をスキャンできません。

[アウトブレイク 隔離 (Outbreak Quarantine)] および [ルール サマリーによる管理 (Manage by Rule Summary)] ビュー

GUI の [モニタ (Monitor)] メニューにあるリスト内の隔離名をクリックすることで、アウトブレイク 隔離エリアの内容を表示できます。アウトブレイク 隔離には、追加のビューである、アウトブレイク 隔離の [ルール サマリーによる管理 (Manage by Rule Summary)] リンクもあります。

図 14-7 アウトブレイク 隔離の [ルール サマリーによる管理 (Manage by Rule Summary)] リンク Quarantines

Quarantine	Messages	Default Action	Status	Settings
Spam Quarantine	2565	Retain 14 days then Delete		Edit
Outbreak Manage by Rule Summary	0	Retention Varies Action: Release		Edit
Policy	0	Retain 10 days then Delete		Edit
Virus	0	Retain 30 days then Delete		Edit

サマリー ビューの使用によるアウトブレイク 隔離エリア内のメッセージに対するルール ID に基づいたメッセージ アクションの実行

[ルール サマリーによる管理 (Manage by Rule Summary)] リンクをクリックして、ルール ID ごとにグループ化されたアウトブレイク 隔離の内容のリストを表示します。

図 14-8 アウトブレイク隔離の [ルール サマリーによる管理 (Manage by Rule Summary)] ビュー
Outbreak Quarantine Summary

Manage by Rule Summary					
All Select	Rule ID	Number of messages	Average message size	Total size	Capacity
<input type="checkbox"/>	EXE_BAGL	4	16 KB	0.1 MB	0.0%
Totals		4	16 KB		

Select Action... Submit

個別にメッセージを選択しなくても、このビューから特定のアウトブレイクまたはアダプティブ ルールに関するすべてのメッセージに対して、解放、削除、または保持期間延長を実行するように選択できます。また、検索またはリストのソートも実行できます。

この機能は、`quarantineconfig -> outbreakmanage` CLI コマンドからも使用できます。詳細については、『*Cisco AsyncOS CLI Reference Guide*』を参照してください。

アウトブレイク フィルタのモニタリング

Cisco アプライアンスには、アウトブレイク フィルタ機能のパフォーマンスおよび活動をモニタする複数のツールが含まれています。

アウトブレイク フィルタ レポート

お使いの Cisco アプライアンスのアウトブレイク フィルタの現在のステータスおよび設定に加えて、最近のアウトブレイクやアウトブレイク フィルタによって隔離されたメッセージに関する情報が表示されるアウトブレイク フィルタ レポートです。この情報は、[モニタ (Monitor)] > [アウトブレイク フィルタ (Outbreak Filters)] ページで表示します。詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Email Security Monitor」の章を参照してください。

アウトブレイク フィルタの概要とルール リスト

概要およびルール リストは、アウトブレイク フィルタ機能の現在の状態に関して役立つ情報を提供します。この情報は、[セキュリティ サービス (Security Services)] > [アウトブレイク フィルタ (Outbreak Filters)] ページで表示します。

アウトブレイク隔離

アウトブレイク隔離を使用して、アウトブレイク フィルタの脅威レベルのしきい値により、フラグ付けされているメッセージの数をモニタします。また、ルールごとの隔離メッセージのリストも使用できます。この情報は、[モニタ (Monitor)] > [内部隔離 (Local Quarantines)] > [アウトブレイク (Outbreak)] リンクおよび [モニタ (Monitor)] > [内部隔離 (Local Quarantines)] ページの [管理ルール サマリー (Manage Rule by Summary)] リンクで表示します。詳細については、[第 27 章「隔離」](#)を参照してください。

アラート、SNMP トラップ、およびアウトブレイク フィルタ

アウトブレイク フィルタ機能は、定期的な AsyncOS アラートと SNMP トラップという 2 つの異なるタイプの通知をサポートしています。

SNMP トラップは、ルールのアップデートが失敗したときに作成されます。AsyncOS の SNMP トラップの詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Managing and Monitoring via the CLI」の章を参照してください。

AsyncOS のアウトブレイク フィルタ機能には、2 つのタイプのアラート（サイズおよびルール）が用意されています。

AsyncOS アラートは、アウトブレイク 隔離エリアのサイズが最大サイズの 5、50、75、および 95 を超えるたびに生成されます。95 % のしきい値を超えたときに生成されるアラートの重大度は CRITICAL、その他のアラートしきい値の場合は WARNING です。アラートは、隔離エリアのサイズが大きくなり、しきい値を超えたときに生成されます。隔離エリアのサイズが小さくなり、しきい値を下回ったときは生成されません。アラートの詳細については、「アラート」(P.29-30) を参照してください。

また、AsyncOS はルールが発行されたとき、しきい値が変更されたとき、またはルールまたは CASE エンジンのアップデート中に問題が発生したときにもアラートを生成します。

アウトブレイク フィルタ機能のトラブルシューティング

この項では、アウトブレイク フィルタ機能の基本的なトラブルシューティングに関するヒントをいくつか紹介します。

[隔離の管理 (Manage Quarantine)] ページのチェックボックスを使用すると、アウトブレイク 隔離がシスコに対して誤分類を通知するようになります。

複数の添付ファイルおよびバイパスされるファイルタイプ

バイパスされるファイルタイプは、メッセージに 1 つだけ添付されているファイルのタイプが指定したタイプであった場合、または、メッセージに複数のファイルが添付されている場合は、その他の添付ファイルに対して既存のルールが存在しない場合のみ、除外されます。これ以外の場合は、メッセージはスキャンされます。

メッセージ フィルタ、コンテンツ フィルタ、および電子メール パイプライン

メッセージ フィルタおよびコンテンツ フィルタは、アウトブレイク フィルタによるスキャンが実行される前にメッセージに適用されます。フィルタを適用することにより、メッセージがアウトブレイク フィルタ スキャンをスキップしたり、バイパスしたりする場合があります。



CHAPTER 15

データ消失防止

- 「データ消失防止の概要」 (P.15-1)
- 「DLP 配置オプション」 (P.15-3)
- 「データ消失防止のシステム要件」 (P.15-4)
- 「RSA メール DLP」 (P.15-4)
- 「RSA Email DLP の DLP ポリシー」 (P.15-6)
- 「RSA Enterprise Manager」 (P.15-23)
- 「メッセージアクション」 (P.15-33)
- 「メッセージ トラッキングの機密 DLP データの表示または非表示」 (P.15-38)
- 「DLP エンジンおよびコンテンツ照合分類子の更新について」 (P.15-39)
- 「DLP インシデントのメッセージとデータの使用」 (P.15-42)
- 「トラブルシューティング データ消失防止」 (P.15-43)

データ消失防止の概要

データ消失防止 (DLP) 機能により、ユーザーが悪意を持ってまたは過失によって機密データを電子メールで送付しないように防止することで、組織の情報と知的財産を保護し、規制と組織のコンプライアンスを実施します。法または会社のポリシーに違反するデータがないか送信メッセージをスキャンするのに使われる DLP ポリシーを作成して、従業員が電子メールで送付できないデータの種類を定義します。

DLP スキャン プロセスの概要

	アクション	追加情報
1.	組織のユーザは組織外部の受信者に電子メールでメッセージを送信します。	電子メール セキュリティ アプライアンス は、ネットワークに出たり入ったりするメッセージを処理する「ゲートウェイ」アプライアンスです。 ネットワーク内の他のユーザに送信されるメッセージはスキャンされません。
2.	電子メール セキュリティ アプライアンス は DLP スキャン段階に到達する前に電子メールの「ワーク キュー」の段階でメッセージを処理します。	DLP スキャン前プロセスは、たとえばメッセージにスパムやマルウェアが含まれていないことを確認します。 DLP 処理がワークキューのどこで発生するかを確認するには、「 電子メール パイプラインのフロー 」(P.4-1) のワークキュー フロー図を参照してください。
3.	アプライアンスは、DLP ポリシーで特定した重要なコンテンツのメッセージ本文、ヘッダー、添付ファイルをスキャンします。	「 データ消失防止の動作 」(P.15-2) を参照してください。
4.	重要なコンテンツが見つかった場合、アプライアンスはメッセージを隔離するか、廃棄または制限をかけて提供するなどのデータを保護するための処理を行います。 それ以外は、メッセージはアプライアンスのワーク キューを通じて継続され、問題がない場合は、電子メール セキュリティ アプライアンスで受信者に配信されます。	実行されるアクションを定義します。「 メッセージ アクション 」(P.15-33) を参照してください。

データ消失防止の動作

組織内の誰かが組織外部の受信者にメッセージを送信する場合、アプライアンスは、定義したルールに基づいてどの発信メール ポリシーをメッセージの送信者または受信者に適用するかを決定します。アプライアンスは、その発信メール ポリシーに指定された DLP ポリシーを使用してメッセージの内容を評価します。

具体的には、アプライアンスは、単語、語句、社会保障番号などの定義済みのパターン、または適用される DLP ポリシーで機密内容として特定される正規表現と一致するテキストがないかメッセージ内容（ヘッダーと添付ファイルを含む）をスキャンします。

また、アプライアンスは、誤検出の一致を最小限に抑えるため拒否されたコンテキストを評価します。たとえば、クレジットカード番号のパターンに一致する番号は、有効期限、クレジットカード会社名（VISA、AMEX など）、または個人の名前や住所が伴っている場合のみ違反になります。

メッセージ内容が複数の DLP ポリシーに一致したら、指定された順序に基づいてリストの最初に一致した DLP ポリシーが適用されます。内容が違反であるかどうかを判断するために同じ基準を使用する複数の DLP ポリシーが発信メール ポリシーにある場合でも、すべてのポリシーは、1 つの内容スキャンの結果を使用します。

機密である可能性のある内容がメッセージに表示されると、アプライアンスは 0 ～ 100 間のリスク要因スコアを潜在的違反に割り当てます。このスコアは、メッセージに DLP 違反が含まれる確率を示します。

アプライアンスは、そのリスク要因スコアに定義した重大度レベル（クリティカルまたは低いなど）を割り当て、適切な DLP ポリシーでその重大度に指定したメッセージアクションを実行します。

DLP 配置オプション

RSA Email DLP	RSA Enterprise Manager
すべての DLP アクティビティは 電子メール セキュリティ アプライアンス によって処理されます。	サーバ上で実行され、電子メール セキュリティ アプライアンス のパートナー デバイスとして使用する RSA のサードパーティ DLP 管理ソフトウェア。 (注) RSA Enterprise Manager はシスコから購入することはできません。
クラスタ導入以外の単一 電子メール セキュリティ アプライアンス の DLP ポリシーを管理します。	一元化されたインターフェイスからの複数の 電子メール セキュリティ アプライアンス を含む、同じネットワーク上の複数のデバイスの DLP ポリシーを管理します。
電子メール セキュリティ アプライアンス の DLP ポリシーを設定します。	ポリシーは、Enterprise Manager で設定し、組織全体で一貫した DLP ポリシーのネットワーク上の 電子メール セキュリティ アプライアンス に、プッシュされます。
RSA によって設計された 100 個の DLP ポリシー テンプレートが含まれており、ユーザが電子メールを使用して送信できない機密データの定義に使用できます。	RSA の DLP ポリシー テンプレートが含まれ、RSA の DLP データセンターと統合し、フィンガープリント検出方法を使って特定の DLP ポリシーのソース コードとドキュメントをスキャンします。 フィンガープリントについては、「 フィンガープリント 」(P.15-25) で説明します。
電子メール セキュリティ アプライアンス または Cisco コンテンツ セキュリティ管理アプライアンス で隔離されたメッセージを表示および管理します。	隔離されたメッセージは、電子メール セキュリティ アプライアンス または Cisco コンテンツ セキュリティ管理アプライアンス に保存されます。 Enterprise Manager、または 電子メール セキュリティ アプライアンス か Cisco コンテンツ セキュリティ管理アプライアンス に隔離されたメッセージを表示できます Enterprise Manager を使用して、隔離されたメッセージ（たとえば、削除または解放）を管理します。
電子メール セキュリティ アプライアンス または Cisco コンテンツ セキュリティ管理アプライアンス に、レポートおよび管理データを表示し、検索します	Enterprise Manager、または 電子メール セキュリティ アプライアンス か Cisco コンテンツ セキュリティ管理アプライアンス にレポートおよび管理データを表示し、検索します
—	お使いの 電子メール セキュリティ アプライアンス Enterprise Manager に既存の DLP 設定を移行します。
詳細については、「 RSA メール DLP 」(P.15-4) を参照してください。	詳細については、「 RSA Enterprise Manager 」(P.15-23) を参照してください。



(注) 次のアクションは、電子メールセキュリティ アプライアンス にだけ発生します。

- 発信メール ポリシー定義
- メッセージアクション定義
- DLP スキャン

データ消失防止のシステム要件

データ損失の防止は、D-Mode ライセンスを使用するアプライアンスを除き、サポートされるすべての C シリーズおよび X-Series アプライアンスでサポートされています。

RSA Enterprise Manager 機能は、Enterprise Manager 9.0 が必要です。

RSA メール DLP

- 「RSA メール DLP を使用した導入の場合のデータ消失防止をセットアップする方法」(P.15-4)
- 「データ消失防止のイネーブル化 (RSA Email DLP)」(P.15-5)

RSA メール DLP を使用した導入の場合のデータ消失防止をセットアップする方法

次の手順を順番に実行します。

	操作内容	追加情報
ステップ1	DLP 機能をイネーブルにし、導入オプションとして [RSA メール DLP (RSA Email DLP)] を選択します。	「データ消失防止のイネーブル化 (RSA Email DLP)」(P.15-5)
ステップ2	違反が見つかったか疑いがあるメッセージに対して実行できるアクションを定義します。たとえば、そのようなメッセージを隔離できます。	「メッセージアクション」(P.15-33)
ステップ3	DLP ポリシーの作成について次を行います。 <ul style="list-style-type: none"> • 組織から電子メールで送信しないコンテンツを識別します。 • 各違反について実行するアクションを指定します。 	方法を選択します。 <ul style="list-style-type: none"> • 「ウィザードを使用して RSA メール DLP を設定する方法」(P.15-7) • 「事前定義されたテンプレートを使用した DLP ポリシーの作成」(P.15-8) • 「カスタム DLP ポリシーの作成 (詳細)」(P.15-9)
ステップ4	コンテンツが 1 つ以上の DLP ポリシーに一致する可能性がある場合に、DLP 違反のメッセージの評価に使用する DLP ポリシーを指定する場合は、DLP ポリシーの順序を設定します。	「違反との一致に対する Email DLP ポリシーの順序の調整」(P.15-21)

	操作内容	追加情報
ステップ5	DLP 違反をスキャンするメッセージの送信者と受信者グループごとに発信メール ポリシーを作成したことを確認します。	第 10 章「メール ポリシー」を参照してください。 さらに個々の DLP ポリシーの許可および制限されたメッセージ送信者と受信者を改善するには、「DLP ポリシーのメッセージのフィルタリング」(P.15-19)を参照してください。
ステップ6	DLP ポリシーを発信メール ポリシーに割り付けることによって、どの DLP ポリシーをどの送信者と受信者に適用するかを指定します。	「発信メール ポリシーとの DLP ポリシーの関連付け」(P.15-21)
ステップ7	ストレージの設定を構成し、機密 DLP 情報にアクセスします。	<ul style="list-style-type: none"> 「メッセージ トラッキングの機密 DLP データの表示または非表示」(P.15-38) 「メッセージ トラッキングでの機密情報へのアクセスの制御」(P.28-5)

データ消失防止のイネーブル化 (RSA Email DLP)

手順

- ステップ 1** [セキュリティ サービス (Security Services)] > [RSA メール DLP (RSA Email DLP)] を選択します。
- ステップ 2** [有効 (Enable)] をクリックします。
- ステップ 3** ライセンス契約書ページの下部にスクロールし、[承認 (Accept)] をクリックしてライセンス契約に合意します。



(注) ライセンス契約に合意しない場合、RSA Email DLP はアプライアンス上でイネーブルになりません。

- ステップ 4** [データ消失防止 (Data Loss Prevention)] で、[RSA メール DLP (RSA Email DLP)] を選択します。
- ステップ 5** [RSA メール データ消失防止を有効にする (Enable RSA Email Data Loss Prevention)] チェックボックスを選択します。
- ステップ 6** (推奨) 現段階では、このページの他のオプションの選択を解除します。
これらの設定は、後でこの章で説明する手順に従って変更できます。
- ステップ 7** 変更内容を送信し、確定します。

次の作業

「RSA メール DLP を使用した導入の場合のデータ消失防止をセットアップする方法」(P.15-4)を参照してください。

関連項目

- 「メッセージ トラッキングの機密 DLP データの表示または非表示」(P.15-38)
- 「ウィザードを使用して RSA メール DLP を設定する方法」(P.15-7)
- 「DLP エンジンおよびコンテンツ照合分類子の更新について」(P.15-39)

RSA Email DLP の DLP ポリシー

- 「DLP ポリシーの説明」 (P.15-6)
- 「定義済み DLP ポリシー テンプレート」 (P.15-6)
- 「ウィザードを使用して RSA メール DLP を設定する方法」 (P.15-7)
- 「事前定義されたテンプレートを使用した DLP ポリシーの作成」 (P.15-8)
- 「カスタム DLP ポリシーの作成 (詳細)」 (P.15-9)
- 「コンテンツ照合分類子を使用した拒否されたコンテンツの定義について」 (P.15-10)
- 「DLP ポリシーのメッセージのフィルタリング」 (P.15-19)
- 「違反の重大度の評価について」 (P.15-20)
- 「違反との一致に対する Email DLP ポリシーの順序の調整」 (P.15-21)
- 「発信メール ポリシーとの DLP ポリシーの関連付け」 (P.15-21)
- 「DLP ポリシーの編集または削除に関する重要な情報」 (P.15-23)

DLP ポリシーの説明

DLP ポリシーは次が含まれます。

- 発信メッセージが機密データを含んでいるかどうかを判断する一連の条件
- メッセージがそのようなデータを含んでいる場合に実行するアクション。

メッセージ コンテンツの評価方法を以下から指定します。

- 拒否された特定のコンテンツまたは情報のパターン。ポリシーによっては、識別番号を検索する正規表現の作成が必須場合があります。「[コンテンツ照合分類子を使用した拒否されたコンテンツの定義について](#)」 (P.15-10) を参照してください。
- メッセージ フィルタリング用の特定の送信者および受信者のリスト。「[送信者および受信者のフィルタリング](#)」 (P.15-20) を参照してください。
- メッセージ フィルタリング用の添付ファイルのタイプ一覧。「[添付ファイルの種類に基づいたフィルタリング](#)」 (P.15-20) を参照してください。
- 発生するさまざまなアクションを許可する設定は違反の重大度に基づいています。「[違反の重大度の評価について](#)」 (P.15-20) を参照してください。

発信メール ポリシーの DLP ポリシーをイネーブルにする場合に、各ポリシーを適用するメッセージ送信者と受信者を決定します。

定義済み DLP ポリシー テンプレート

DLP ポリシーの作成を簡素化するために、アプライアンスには、RSA が開発した定義済みのポリシー テンプレートの大規模なコレクションが含まれます。

テンプレートのカテゴリには次が含まれます。

- **[規制コンプライアンス (Regulatory Compliance)]**。これらのテンプレートは、個人識別情報、クレジット情報、その他の保護または非公開情報を含む添付ファイル、メッセージを識別します。

- **[許可された使用 (Acceptable Use)]**。これらのテンプレートは、組織の機密情報が含まれる制限された受信者または競合他社に送信されたメッセージを指定します。
- **[プライバシー保護 (Privacy Protection)]**。金融口座、税金記録、国民 ID の識別番号を含むメッセージおよび添付ファイルを識別します。
- **[知的財産保護 (Intellectual Property Protection)]**。これらのテンプレートは、よく使われるパブリッシングおよびデザイン ドキュメント ファイル タイプで、組織が保護する知的財産を含む可能性があるものを識別します。
- **[企業機密情報 (Company Confidential)]**。これらのテンプレートは、会社の財務情報や近い将来の合併および買収に関する情報を含むドキュメントとメッセージを識別します。
- **[カスタム ポリシー (Custom Policy)]**。この「テンプレート」を使用すると、構成によって指定された RSA が開発したコンテンツ照合分類子、または組織が指定した違反識別基準を使用して、独自のポリシーを最初から作成できます。このオプションは高度であり、事前定義されたポリシーテンプレートではユーザのネットワーク環境の独自の要件を満たせない、まれな場合にのみ使用されることを想定しています。

これらのテンプレートの中にはカスタマイズが必要なものもあります。

ウィザードを使用して RSA メール DLP を設定する方法

DLP 評価ウィザードでは一般的な DLP ポリシーを設定し、アプライアンスのデフォルトの発信メールポリシーでイネーブルにします。



(注)

DLP Assessment Wizard を使って追加された DLP ポリシーでは、検出された DLP 違反の重大度にかかわらず、メッセージはすべて配信されます。ウィザードを使用して作成されたポリシーを編集する必要があります。

はじめる前に

- アプライアンスから既存の DLP ポリシーを削除します。DLP ポリシーがアプライアンスに存在しない場合は、DLP Assessment Wizard のみ使用することができます。
- クレジット カード番号、米国社会保障番号、および米国運転免許証番号以外の生徒識別番号またはアカウント番号を含むメッセージを検出する必要がある場合、それらの番号を特定する正規表現を作成します。詳細については、「[識別番号を識別する正規表現](#)」(P.15-14) を参照してください。

手順

- ステップ 1** [セキュリティ サービス (Security Services)] > [RSA メール DLP (RSA Email DLP)] を選択します。
- ステップ 2** [設定を編集 (Edit Settings)] をクリックします。
- ステップ 3** [有効 (Enable)] を選択し、[DLP 評価ウィザードを使用して DLP を設定します。 (DLP using the DLP Assessment Wizard)] チェックボックスをオンにします。
- ステップ 4** [送信 (Submit)] をクリックします。
- ステップ 5** ウィザードを完了します。
次の点を考慮してください。

- カルフォルニアでビジネスを営み、カルフォルニア州民のコンピュータ化した個人情報 (PII) データを保有またはライセンスしている企業は、物理的な所在地にかかわらず、**カルフォルニア SB-1386** に準拠することが必須となっています。この法律は、ウィザードのポリシーの選択肢の 1 つです。
- 自動生成されたスケジュール済み DLP インシデント サマリー レポートを受信する電子メールアドレスを入力しない場合、レポートは生成されません。
- 設定を確認し、変更を加える手順まで戻った場合は、再度このレビュー ページに至るまで、残りの手順を進める必要があります。以前に入力した設定は、すべて残っています。
- ウィザードを完了すると、デフォルトの送信メール ポリシーで DLP ポリシーがイネーブルな [送信メール ポリシー (Outgoing Mail Policies)] ページが表示されます。DLP ポリシー設定の要約が、ページの上部に表示されます。

ステップ 6 変更内容を確定します。

次の作業


- (任意) これらの DLP ポリシーを編集し、追加ポリシーを作成し、メッセージの全体的な処理を変更するか、または重大度レベルの設定を変更するには、[メール ポリシー (Mail Policies)] > [DLP ポリシー マネージャ (DLP Policy Manager)] を選択します。詳細については、「事前定義されたテンプレートを使用した DLP ポリシーの作成」(P.15-8)、「カスタム DLP ポリシーの作成 (詳細)」(P.15-9)、および「重大度スケールの調整」(P.15-21) を参照してください。
- (任意) 他の発信メール ポリシーのある既存の DLP ポリシーをイネーブルにするには、「発信メール ポリシーを使用した送信者および受信者への DLP ポリシーの割り当て」(P.15-22) を参照してください。

関連項目

- 「事前定義されたテンプレートを使用した DLP ポリシーの作成」(P.15-8)
- 「カスタム DLP ポリシーの作成 (詳細)」(P.15-9)

事前定義されたテンプレートを使用した DLP ポリシーの作成

手順

- ステップ 1** [メール ポリシー (Mail Policies)] > [DLP ポリシー マネージャ (DLP Policy Manager)] を選択します。
- ステップ 2** [DLP ポリシーの追加 (Add DLP Policy)] をクリックします。
- ステップ 3** カテゴリ名をクリックし、使用可能な RSA Email DLP ポリシー テンプレートの一覧を表示します。
-  **(注)** 各テンプレートの説明を表示するには、[ポリシーの説明を表示 (Display Policy Descriptions)] をクリックします。
- ステップ 4** 使用する RSA Email DLP ポリシー テンプレートの [追加 (Add)] をクリックします。
- ステップ 5** (任意) テンプレートの定義済みの名前と説明を変更します。
- ステップ 6** ポリシーで、1 つ以上のコンテンツ照合分類子のカスタマイズが要求または推奨される場合は、組織の識別番号付けシステムのパターンを定義するための正規表現と、使用される識別番号に関連する、または通常は関連付けられている単語や語句のリストを入力します。

詳細については、次を参照してください。

- 「コンテンツ照合分類子を使用した拒否されたコンテンツの定義について」 (P.15-10) および
- 「識別番号を識別する正規表現」 (P.15-14) .



(注) 定義済みのテンプレートに基づいたポリシーのコンテンツの分類子は追加または削除できません。

ステップ 7 (任意) 特定の受信者、送信者、添付ファイルの種類、または以前に追加されたメッセージタグを持つメッセージにのみ DLP ポリシーを適用します。

詳細については、「DLP ポリシーのメッセージのフィルタリング」 (P.15-19) を参照してください。

改行やカンマで、複数のエントリを分離できます。

ステップ 8 [重大度設定 (Severity Settings)] の項で、以下を行います。

- 違反の重大度レベルごとに実行するアクションを選択します。

詳細については、「違反の重大度の評価について」 (P.15-20) を参照してください。

- (任意) ポリシーに対して違反の重大度基準を調整する場合は、[スケールの編集 (Edit Scale)] をクリックします。

詳細については、「重大度スケールの調整」 (P.15-21) を参照してください。

ステップ 9 変更内容を送信し、確定します。

関連項目

- 「ウィザードを使用して RSA メール DLP を設定する方法」 (P.15-7)
- 「カスタム DLP ポリシーの作成 (詳細)」 (P.15-9)

カスタム DLP ポリシーの作成 (詳細)



(注) カスタム ポリシーの作成は非常に複雑です。定義済み DLP ポリシー テンプレートが組織のニーズを満たさない場合のみ、カスタム ポリシーを作成します。

Custom Policy テンプレートを使用して、カスタム DLP ポリシーを最初から作成し、定義された RSA コンテンツ照合分類子またはカスタム分類子をポリシーに追加できます。

ポリシーの定義によって、コンテンツが 1 つの分類子またはすべての分類子に一致した場合に、カスタム ポリシーは DLP 違反を返すことができます。

はじめる前に

推奨：コンテンツ違反を識別する基準を定義します。「カスタム DLP ポリシーに対するコンテンツ照合分類子の作成」 (P.15-13) を参照してください。次の手順の中で、これらの基準を定義することもできます。

手順

ステップ 1 [メール ポリシー (Mail Policies)] > [DLP ポリシー マネージャ (DLP Policy Manager)] を選択します。

- ステップ 2** [DLP ポリシーの追加 (Add DLP Policy)] をクリックします。
- ステップ 3** Custom Policy カテゴリの名前をクリックします。
- ステップ 4** Custom Policy テンプレートの [追加 (Add)] をクリックします。
- ステップ 5** ポリシーの名前と説明を入力します。
- ステップ 6** DLP 違反を構成するコンテンツとコンテキストを特定します。
- コンテンツ照合分類子を選択します。
 - [追加 (Add)] をクリックします。
 - [分類子を作成 (Create a Classifier)] を選択した場合、「[カスタム DLP ポリシーに対するコンテンツ照合分類子の作成](#)」(P.15-13) を参照してください。
 - それ以外の場合は、選択された分類子がテーブルに追加されます。
 - (任意) ポリシーに追加分類子を追加します。

たとえば、別の分類子を追加し、[NOT] を選択して、既知の誤検出である可能性の高い一致を削除できます。
 - 複数の分類子を追加した場合、テーブル見出しのオプションを選択し、インスタンスを違反としてカウントするために分類子の一部またはすべてを一致させるかどうかを指定します。
- ステップ 7** (任意) 特定の受信者、送信者、添付ファイルの種類、または以前に追加されたメッセージタグを持つメッセージにのみ DLP ポリシーを適用します。
- 詳細については、「[DLP ポリシーのメッセージのフィルタリング](#)」(P.15-19) を参照してください。
- 改行やカンマで、複数のエントリを分離できます。
- ステップ 8** [重大度設定 (Severity Settings)] の項で、以下を行います。
- 違反の重大度レベルごとに実行するアクションを選択します。

詳細については、「[違反の重大度の評価について](#)」(P.15-20) を参照してください。
 - (任意) ポリシーに対して違反の重大度基準を調整する場合は、[スケールの編集 (Edit Scale)] をクリックします。

詳細については、「[重大度スケールの調整](#)」(P.15-21) を参照してください。
- ステップ 9** 変更内容を送信し、確定します。

関連項目

- 「[ウィザードを使用して RSA メール DLP を設定する方法](#)」(P.15-7)
- 「[事前定義されたテンプレートを使用した DLP ポリシーの作成](#)」(P.15-8)

コンテンツ照合分類子を使用した拒否されたコンテンツの定義について

コンテンツ一致分類子は、電子メールで送信できないコンテンツと、任意選択でそのコンテンツがデータ消失防止違反と見なされるために発生する必要があるコンテキストを定義します。

患者識別番号が組織から電子メールで送信されることを回避する必要があるとします。

これらの番号をアプライアンスに認識させるために、1 つ以上の正規表現を使用して組織の記録番号付けシステムのパターンを指定する必要があります。補足情報として記録番号を伴うかもしれない単語およびフレーズのリストを追加できます。分類子が発信メッセージ内に番号パターンを検出すると、補足情報を検索し、そのパターンが識別番号か、また、ランダムな番号の文字列でないかを確認します。コンテキストと一致する情報を含むことにより、誤検出の一致が減少します。

この例では、HIPAA および HITECH テンプレートを使用する DLP ポリシーを作成します。このテンプレートには、患者識別番号コンテンツ照合分類子という患者識別番号を検出するようにカスタマイズ可能な分類子が含まれます。パターン 123-CL456789 の番号を検出するには、分類子の正規表現 `[0-9]{3}\-[A-Z]{2}[0-9]{6}` を入力します。関連フレーズとして「Patient ID」を入力します。ポリシーの作成を完了し、発信メール ポリシーでイネーブルにします。変更内容を送信し、確定します。フレーズ「患者 ID」が番号パターンの近くに設定された発信メッセージからポリシーが番号パターンを検出した場合、DLP ポリシーは DLP 違反を返します。

DLP ポリシーでのコンテンツ照合分類子の使用方法について

定義済み DLP ポリシー テンプレートの多くは、RSA のコンテンツ照合分類子が含まれます。これらの分類子の一部は、組織のデータに使用されるパターンを識別するためにカスタマイズする必要があります。

カスタム DLP ポリシーを作成すると、事前定義された分類子を選択するか、独自の分類子を作成できます。

コンテンツ照合分類子の例

次の例は、分類子がメッセージの内容を照合する方法を示します。

クレジットカード番号

DLP ポリシー テンプレートのいくつかは、クレジットカード番号分類子を含みます。クレジットカード番号はそれ自体、数と句読点のパターン、発行者固有のプレフィックス、最後のチェック デジットなどさまざまな制約があります。この分類子で一致するには、別のクレジットカード番号、有効期限、発行者の名前など、追加の補足情報が必要です。これで誤検出の数が減ります。

例を示します。

- 4999-9999-9999-9996 (補足情報がないため一致せず)
- 4999-9999-9999-9996 01/09 (一致)
- Visa 4999-9999-9999-9996 (一致)
- 4999-9999-9999-9996 4899 9999 9999 9997 (複数のクレジットカード番号があるため一致)

米国社会保障番号

米国社会保障番号分類子では、正しい形式の番号と誕生日や名前および「SSN」という文字列などの補足データが必要です。

例を示します。

- 321-02-3456 (補足情報がないため一致せず)
- 321-02-3456 July 4 (一致)
- 321-02-3456 7/4/1980 (一致)
- 321-02-3456 7/4 (一致せず)
- 321-02-3456 321-02-7654 (複数の SSN があるため一致)
- SSN: 321-02-3456 (一致)
- Joe Smith 321-02-3456 (一致)
- 321-02-3456 CA 94066 (一致)

ABA 送金番号

ABA 送金番号分類子は、クレジットカード番号分類子とほぼ同じです。

例を示します。

- 119999992 (補足情報がないため一致せず)
- routing 119999992 account 1234567 (一致)

米国運転免許証

米国運転免許証分類子を使用するポリシーは多数あります。デフォルトでは、この分類子は米国 50 州すべておよびコロンビア特別区の運転免許を検索します。カルフォルニア州の AB-1298 およびモンタナ州の HB-732 など米国の州固有のポリシーでは、51 タイプのすべての米国運転免許を検索します。California SB 1386 など特定の州用の事前定義された DLP ポリシー テンプレートは、すべての州向けの検出ルールを使用し、カルフォルニア州以外の運転免許のデータに対して DLP 違反を返します。これは、プライバシー違反と考えられるからです。

誤検出またはアプライアンスのパフォーマンスに懸念がある場合は、[メール ポリシー (Mail Policies)] > [DLP ポリシー マネージャ (DLP Policy Manager)] に移動し、[詳細設定 (Advanced Settings)] セクションで [米国運転免許証 (US Drivers Licenses)] リンクをクリックすることにより、検索を特定の米国の州に限定する、またはどの州も検索しないようにできます。

各州の分類子はその州のパターンと照合し、対応する州の名前または略称および追加の補足データを定めています。

例を示します。

- CA DL: C3452362 (番号と補足データのパターンが正しいため一致)
- California DL: C3452362 (一致)
- DL: C3452362 (補足データ不足のため一致せず)
- California C3452362 (補足データ不足のため一致せず)
- OR DL: C3452362 (オレゴン州の正しいパターンではないため一致せず)
- OR DL: 3452362 (オレゴン州の正しいパターンのため一致)
- WV DL: D654321 (ウェストバージニア州の正しいパターンのため一致)
- WV DL: G6543 (ウェストバージニア州の正しいパターンでないため一致せず)

米国の国内のプロバイダー ID

米国の国内のプロバイダー ID の分類子は、チェック デジットを含む 10 桁の数字である国家プロバイダー認証 (NPI) をスキャンします。

例を示します。

- NPI: 3459872347 (NPI があるため一致)
- 3459872347 (補足情報がないため一致せず)
- NPI: 3459872342 (誤ったチェック デジットのため一致せず)

生徒記録

事前定義された Family Educational Rights and Privacy Act (FERPA; 家族教育権とプライバシー法) DLP ポリシー テンプレートは、生徒記録分類子を使用します。より正確に検出するため、この分類子とカスタマイズされた生徒識別番号分類子を組み合わせ、特定の生徒 ID パターンを検出します。

例を示します。

- Joe Smith, Class Rank: 234, Major: Chemistry Transcript (一致)

企業財務情報

事前定義された Sarbanes-Oxley (SOX) ポリシー テンプレートは、企業財務情報分類子を使用し、非公開の企業の財務情報を検索します。

例を示します。

2009 Cisco net sales, net income, depreciation (一致)

FORM 10-Q 2009 I.R.S.Employer Identification No. (一致)

カスタム DLP ポリシーに対するコンテンツ照合分類子の作成

作成したカスタム分類子は、カスタム DLP ポリシーの作成時に使用できる分類子のリストに追加されます。

手順	操作内容	情報
ステップ1	潜在的な DLP 違反を特定するためにコンテンツ照合分類子がどのように使用されているかを理解します。	参照先： <ul style="list-style-type: none"> • 「コンテンツ照合分類子を使用した拒否されたコンテンツの定義について」(P.15-10) • 「コンテンツ照合分類子の例」(P.15-11)
ステップ2	[メール ポリシー (Mail Policies)] > [DLP ポリシーのカスタマイズ (DLP Policy Customizations)] を選択し、[カスタム分類子の追加 (Add Custom Classifier)] をクリックします。 分類子の名前と説明を入力します。	—
ステップ3	近接性および最小合計スコアを入力します。	「疑わしい違反のリスク要因の判別子」(P.15-18) を参照してください。
ステップ4	次の検出規則タイプから 1 つを選択し、関連するコンテンツの一致基準を定義します。 <ul style="list-style-type: none"> • 単語またはフレーズ • ディクショナリのテキスト • 正規表現、または • 既存のデータ消失防止エンティティ 	参照先： <ul style="list-style-type: none"> • 「機密情報を特定する分類子検出ルール (カスタム DLP ポリシーのみ)」(P.15-14) • 「機密 DLP 用語 (カスタム DLP ポリシーのみ) のカスタム ディクショナリの使用」(P.15-16)
ステップ5	(任意) [ルールの追加 (Add Rule)] をクリックして、追加ルールを追加します。	<ul style="list-style-type: none"> • 「識別番号を識別する正規表現」(P.15-14) 重み付けや最大スコアの詳細については、「疑わしい違反のリスク要因の判別子」(P.15-18) を参照してください。

手順	操作内容	情報
ステップ6	複数のルールを含める場合は、ルールの すべて一致 と いずれか一致 を指定します。	この設定は、[ルール (Rules)] セクションの上部にあります。
ステップ7	変更内容を送信し、確定します。	—

次の作業

カスタム DLP ポリシーでカスタム コンテンツ分類子を使用します。「[カスタム DLP ポリシーの作成 \(詳細\)](#)」(P.15-9) を参照してください。

関連項目

- 「[カスタム コンテンツ分類子が使用されるポリシーの表示](#)」(P.15-19)

機密情報を特定する分類子検出ルール (カスタム DLP ポリシーのみ)

コンテンツ照合分類子では、メッセージやドキュメント内の DLP 違反を検出するルールが必要となります。分類子では、次の検出ルールの 1 つ以上のルールを使用できます。

- **単語またはフレーズ (Words or Phrases)**。分類子が探す単語およびフレーズの一覧。複数のエントリは、カンマまたは改行で区切ります。
- **正規表現 (Regular Expression)**。メッセージや添付ファイルの検索パターンを定義する正規表現。誤検出を防止するため、照合から除外するパターンも定義できます。詳細については、「[識別番号を識別する正規表現](#)」(P.15-14) と「[識別番号を識別する正規表現の例](#)」(P.15-15) を参照してください。
- **ディクショナリ (Dictionary)**。単語とフレーズに関連するディクショナリ。アプライアンスには RSA が作成したディクショナリがあります。または独自に作成できます。「[機密 DLP 用語 \(カスタム DLP ポリシーのみ\) のカスタム ディクショナリの使用](#)」(P.15-16) を参照してください。
- **エンティティ (Entity)**。定義済みのパターンは、クレジットカード番号、アドレス、社会保障番号、または ABA 送金番号などの機密データの一般的なタイプを識別します。エンティティの説明については、[メールポリシー (Mail Policies)] > [DLP ポリシー マネージャ (DLP Policy Manager)] に移動し、[DLP ポリシーの追加 (Add DLP Policy)] をクリックし、[プライバシー保護 (Privacy Protection)] をクリックして、[ポリシーの説明を表示 (Display Policy Descriptions)] をクリックします。

識別番号を識別する正規表現

ポリシー テンプレートによっては、1 つ以上のコンテンツ照合分類子をカスタマイズする必要であり、カスタマイズには、カスタム アカウント番号、患者識別番号または生徒識別番号などの極秘情報に結び付く可能性がある識別番号を検索するための正規表現の作成があります。コンテンツ照合分類子に使用される正規表現の形式は、**POSIX 基本正規表現形式**の正規表現です。



(注)

正規表現では大文字と小文字は区別されるため、[a-zA-Z] のように大文字と小文字を含める必要があります。特定の文字のみ使用する場合は、その文字に合わせて正規表現を定義します。

8 桁の数字など、あまり特殊ではないパターンほど、ランダムな 8 桁の数字を実際の顧客番号と区別するため、追加の単語とフレーズを検索するポリシーが必要になります。

次の表を、分類子用の正規表現の作成ガイドとして使用してください。

要素	説明
正規表現 (abc)	正規表現の一連の命令が文字列の一部に一致すると、分類子用の正規表現はその文字列に一致するということとなります。 たとえば、正規表現 ACC は、文字列 ACCOUNT と ACCT に一致します。
[]	大カッコは文字のセットを示すために使用します。文字は個々または範囲で定義できます。 たとえば、[a-z] は、a から z までのすべての小文字に一致し、[a-zA-Z] は、A から Z までのすべての大文字と小文字に一致します。[xyz] は、x、y または z の文字のみに一致します。
円記号 (\)	円記号は特殊文字のエスケープに使用します。したがって、\ と続けると、ピリオドそのものだけに一致し、\\$ はドル記号のみに一致し、^ はキャレット記号のみに一致します。 円記号は、\d などトークンの始まりともなります。 重要： 円記号はパーサーでも特殊なエスケープ文字として使用します。そのため、正規表現で円記号を使用する場合、2 つの円記号が必要です。解析後には「実際に」使用される円記号 1 つのみが残り、正規表現システムに渡されます。
\d	数字 (0 ~ 9) に一致するトークン。複数の数字に一致させるには、整数を {} に入れ数の長さを規定します。 たとえば、\d は、5 などの 1 桁の数字のみに一致しますが、55 には一致しません。\\d{2} を使うと、55 などの 2 桁の数に一致しますが、5 には一致しません。
繰り返し回数 {min,max}	1 つ前のトークンの繰り返し回数を指定する正規表現表記がサポートされています。 たとえば、「\\d{8}」という表現は、12345678 および 11223344 には一致しますが、8 には一致しません。
論理和 ()	代替、つまり「or」演算子に相当します。A と B を正規表現とすると、「A B」という表現は「A」と「B」のいずれかに一致するすべての文字列に一致します。1 つの正規表現で数パターンを組み合わせるために使用できます。 たとえば、「foo bar」という表現は foo や bar とは一致しますが、foobar とは一致しません。

識別番号を識別する正規表現の例

識別または口座番号に数字と文字のパターンを記述する単純な正規表現には、次のように表示される可能性があります。

- 8 桁の数：\\d{8}
- 数字のセットの間にハイフンがある識別コード：\\d{3}-\\d{4}-\\d
- 大文字または小文字の英字 1 つで始まる識別コード：[a-zA-Z]\\d{7}
- 3 桁の数字で始まり、大文字が 9 つ続く識別コード：\\d{3}[A-Z]{9}

- | を使い、検索する 2 つの異なる数字パターンを定義：\d{3}[A-Z]{9}|\d{2}[A-Z]{9}-\d

機密 DLP 用語（カスタム DLP ポリシーのみ）のカスタム ディクショナリの使用

AsyncOS には、RSA Security Inc. による事前定義された一連のディクショナリが提供されますが、DLP スキャン機能に一致する用語を指定するカスタム DLP ディクショナリを作成することもできます。

複数の方法でカスタム DLP ディクショナリを作成できます。

- [カスタム DLP ディクショナリの直接追加](#)
- [テキスト ファイルとして DLP ディクショナリを作成し、DLP ディクショナリのインポート。](#)
- [別の電子メール セキュリティ アプライアンスから DLP ディクショナリのエクスポートし、DLP ディクショナリのインポート。](#)

カスタム DLP ディクショナリの直接追加

手順

-
- ステップ 1** [メール ポリシー (Mail Policies)] > [DLP ポリシー マネージャ (DLP Policy Manager)] を選択します。
 - ステップ 2** [詳細設定 (Advanced Settings)] セクションで、[カスタム DLP 辞書 (Custom DLP Dictionaries)] の側のリンクをクリックします。
 - ステップ 3** [辞書を追加 (Add Dictionary)] をクリックします。
 - ステップ 4** カスタム ディクショナリの名前を入力します。
 - ステップ 5** 用語のリストに新規ディクショナリのエン트리 (単語とフレーズ) を入力します。
ディクショナリの単語は大文字と小文字が区別され、非 ASCII 文字を含めることができます。
複数のエントリを入力する場合は、改行でエントリを区切ります。
 - ステップ 6** [追加 (Add)] をクリックします。
 - ステップ 7** 変更内容を送信し、確定します。
-

テキスト ファイルとして DLP ディクショナリを作成

ユーザ独自のディクショナリをテキスト ファイルとしてローカル マシンに作成し、アプライアンスにインポートすることもできます。ディクショナリのテキスト ファイルにおける各単語には、強制改行を使用します。ディクショナリの単語は大文字と小文字が区別され、非 ASCII 文字を含めることができます。

DLP ディクショナリのエクスポート



(注) 事前定義された DLP ディクショナリはエクスポートできません。

手順

- ステップ 1 [メール ポリシー (Mail Policies)] > [DLP ポリシー マネージャ (DLP Policy Manager)] を選択します。
- ステップ 2 [詳細設定 (Advanced Settings)] の [カスタム DLP 辞書 (Custom DLP Dictionaries)] セクションのリンクをクリックします。
- ステップ 3 [辞書をエクスポート (Export Dictionary)] をクリックします。
- ステップ 4 エクスポートするディクショナリを選択します。
- ステップ 5 ディクショナリのファイル名を入力します。
- ステップ 6 エクスポートされたディクショナリを保存する場所 (ローカル コンピュータまたはアプライアンスの configuration ディレクトリのいずれか) を選択します。
- ステップ 7 ファイルのエンコード方式を選択します。
- ステップ 8 [送信 (Submit)] をクリックし、ファイルを保存します。

DLP ディクショナリのインポート

はじめる前に

電子メール セキュリティ アプライアンス に非 DLP ディクショナリからエクスポートしたファイルをインポートする場合は、最初にテキスト ファイルから重み値を削除し、正規表現を単語または語句に変換する必要があります。

手順

- ステップ 1 [メール ポリシー (Mail Policies)] > [DLP ポリシー マネージャ (DLP Policy Manager)] を選択します。
- ステップ 2 [詳細設定 (Advanced Settings)] セクションで、[カスタム DLP 辞書 (Custom DLP Dictionaries)] の側のリンクをクリックします。
- ステップ 3 [辞書をインポート (Import Dictionary)] をクリックします。
- ステップ 4 ファイルをローカル マシンからインポートするか、アプライアンスの configuration ディレクトリからインポートするかを選択します。
- ステップ 5 エンコード方式を選択します。
- ステップ 6 [次へ (Next)] をクリックします。
「Success」メッセージが表示され、インポートしたディクショナリは、[辞書を追加 (Add Dictionary)] ページに表示されます。ただし、このプロセスはまだ完全ではありません。
- ステップ 7 ディクショナリの名前を指定し、編集します。
- ステップ 8 [送信 (Submit)] をクリックします。

疑わしい違反のリスク要因の判別子

アプライアンスは DLP 違反に対してメッセージをスキャンすると、メッセージにリスク要因スコアを割り当てます。このスコアは、メッセージに DLP 違反が含まれる確率を示します。スコアが 0 であれば、メッセージにはほぼ確実に違反が含まれないことを意味します。スコアが 100 であれば、ほぼ確実に違反が含まれます。

定義済みのテンプレートに基づいた DLP ポリシーについて

定義済みのテンプレートから作成された DLP ポリシーに対するリスク要因のスコアリングパラメータを表示または変更することはできません。ただし、特定 DLP ポリシーに大量の誤検出の一致がある場合、そのポリシーに対して重大度スケールを調整できます。「違反の重大度の評価について」(P.15-20)を参照してください。SOX (Sarbanes-Oxley) テンプレートなどのコンテンツ照合分類子のないテンプレートに基づくポリシーでは、メッセージがポリシーに違反した場合はスキャンエンジンは常に「75」というリスク要素の値を返します。

カスタム DLP ポリシーについて

カスタム DLP ポリシーに対するコンテンツ照合分類子を作成すると、リスク要因スコアを決定するために使用される値を指定します。

- **近接性。**違反と見なすには、メッセージや添付ファイルの中でルールと一致する箇所がどのくらい近くで発生する必要があるかを定義します。たとえば、社会保障番号に似た数値のパターンが長いメッセージの上部に表示され、アドレスが末尾に送信者の署名で表示されている場合、それらは無関係であると推定され、データは一致としてカウントされません。
- **最小総合スコア。**機密情報が DLP 違反として分類されるために必要な最小限のリスク要因スコア。メッセージの一致のスコアが最小総合スコアに達しなかった場合、そのデータは機密であるとは見なされません。
- **重み。**作成する各カスタムルールで、ルールの重要度を示す「重み」を指定します。スコアは検出ルールに一致した数にルールの重みを乗算することで取得できます。重みが 10 のルールで違反が 2 つある場合は、スコアは 20 となります。あるルールが分類子にとって他より重要であれば、より大きい重みをアサインすることになります。
- **最大スコア。**ルールの最大スコアは、重みが低いルールに一致するものが大量に発生しても、スキャンの最終スコアがゆがめられないようにするものです。

リスク要因を計算するため、分類子は検出ルールに一致する数にルールの重みを乗算します。この値が検出ルールの最大スコアを超過した場合、分類子は最大スコアを使用します。分類子が複数の検出ルールを持つ場合、すべての検出ルールのスコアを合計して 1 つの値にします。分類子は次の表にあるように、検出ルールのスコア (10 ~ 10000) を 10 ~ 100 の対数目盛りにマッピングし、リスク要因を算出します。

表 15-1 検出ルール スコアからのリスク要因スコアの計算方法

ルールのスコア	リスク要因
10	10
20	20
30	30
50	40
100	50
150	60
300	70
500	80

表 15-1 検出ルール スコアからのリスク要因スコアの計算方法

ルールのスコア	リスク要因
1000	90
10000	100

カスタム コンテンツ分類子が使用されるポリシーの表示

手順

- ステップ 1** [メール ポリシー (Mail Policies)] > [DLP ポリシーのカスタマイズ (DLP Policy Customizations)] を選択します。
- ステップ 2** [カスタム分類子 (Custom Classifiers)] セクションで、[カスタム分類子 (Custom Classifiers)] テーブルの見出しにある [ポリシー (Policies)] をクリックします。

関連項目

- 「[カスタム DLP ポリシーに対するコンテンツ照合分類子の作成](#)」 (P.15-13)

DLP ポリシーのメッセージのフィルタリング

パフォーマンスや精度を向上させるために、次の基準に基づいて特定のメッセージだけに適用されるように DLP ポリシーを制限できます。

オプション	説明
送信者および受信者のフィルタリング	<p>DLP ポリシーを制限し、次のいずれかを使用して指定する送信者または受信者を含むまたは含まないメッセージに適用する。</p> <ul style="list-style-type: none"> • 完全な電子メールアドレス：user@example.com • 電子メールアドレスの一部：user@ • ドメインのすべてのユーザ：@example.com • 部分ドメインのすべてのユーザ：@.example.com <p>改行やカンマで、複数のエントリを分離できます。</p> <p>AsyncOS は最初に発信メッセージの受信者または送信者が発信メールポリシーと一致するか照合し、次に送信者または受信者がそのメールポリシーでイネーブルとなっている DLP ポリシーで指定した送信者および受信者フィルタと一致するか照合します。</p> <p>たとえば、パートナードメインの受信者を除いて、すべての送信者に対し特定のタイプの情報を送信することを拒否する場合があります。パートナードメイン内のすべてのユーザを除外するフィルタを含め、その情報に対し DLP ポリシーを作成し、すべての送信元に適用される発信メールポリシーにこの DLP ポリシーを含めます。</p>
添付ファイルの種類に基づいたフィルタリング	<p>特定の種類の添付ファイルを含むまたは含まないメッセージのみをスキャンするよう DLP ポリシーを限定できます。添付ファイルのカテゴリを選択し、次に定義済みのファイルタイプを選択するか、リストされていないファイルタイプを指定します。事前定義されていないファイルタイプを指定すると、AsyncOS は、添付ファイルの拡張子をもとにファイルタイプを検索します。</p> <p>DLP のスキャンを、最小ファイルサイズの添付ファイルに限定することができます。</p>
メッセージタグによるフィルタリング	<p>DLP ポリシーを特定のフレーズを含むメッセージのスキャンに限定する場合は、メッセージまたはコンテンツフィルタを使って発信メッセージにそのフレーズがないか検索し、カスタムメッセージタグを当該メッセージに挿入することができます。詳細については、「コンテンツフィルタのアクション」(P.11-10) および第 9 章「メッセージフィルタを使用した電子メールポリシーの適用」を参照してください。</p>

違反の重大度の評価について

DLP スキャンエンジンが潜在的な DLP 違反を検出すると、そのインスタンスが実際に DLP 違反である確率を表すリスク要因スコアを計算します。ポリシーはリスク要因スコアを、ポリシーで定義された重大度基準と比較して、重大度レベルを特定します（[低 (Low)]、[クリティカル (Critical)] など）。各重大度で、違反に対して実行するアクションを指定します（ただし、[Ignore (無視)] を指定すると、アクションは実行されません）。各重大度レベルに達するために必要なリスク要因スコアは、調整できます。

関連項目

- 「[疑わしい違反のリスク要因の判別子](#)」(P.15-18)。
- 「[重大度スケールの調整](#)」(P.15-21)

重大度スケールの調整

すべてのポリシーにはデフォルトの重大度スケールがあります。各ポリシーに対してこのスケールを調整できます。

たとえば、リスク要因スコアが 90 から 100 の場合、デフォルトで違反の重大度レベルはクリティカルになります。ただし、特定のポリシーに一致する違反についてはデータ消失の可能性があります、機密度を上げることが必要になることがあります。この DLP ポリシーには、クリティカルな重大度レベルを 75 ~ 100 のリスク要因スコアを持つ違反に変更できます。

手順

- ステップ 1** [メール ポリシー (Mail Policies)] > [DLP ポリシー マネージャ (DLP Policy Manager)] を選択します。
- ステップ 2** 編集するポリシーの名前をクリックします。
- ステップ 3** 重大度の [重大度設定 (Severity Settings)] セクションで、[スケールの編集... (Edit Scale...)] をクリックします。
- ステップ 4** 基準の矢印を使って、重大度レベルに対するスコアを調整します。
- ステップ 5** [完了 (Done)] をクリックします。
- ステップ 6** [重大度スケール (Severity Scale)] のテーブルで、必要なときにスコアがあることを確認します。
- ステップ 7** [送信 (Submit)] をクリックします。

関連項目

- 「違反の重大度の評価について」 (P.15-20)

違反との一致に対する Email DLP ポリシーの順序の調整

DLP 違反が、発信メール ポリシーでイネーブルな DLP ポリシーに 1 つ以上一致する場合、リストで最初に一致した DLP ポリシーのみが使用されます。

手順

- ステップ 1** [DLP ポリシー マネージャ (DLP Policy Manager)] ページで、[ポリシーの順番の編集 (Edit Policy Order)] をクリックします。
- ステップ 2** 移動するポリシーの行をクリックし、新しい順序の場所にドラッグします。
- ステップ 3** ポリシーの順序の変更を完了したら、変更内容を送信し、確定します。

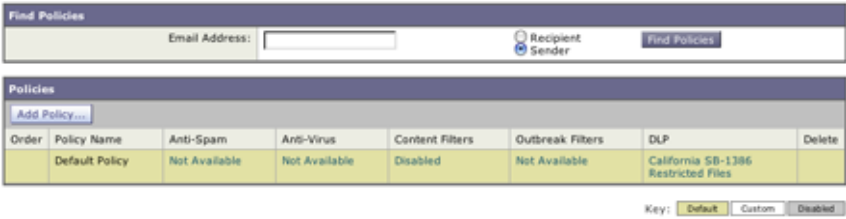
発信メール ポリシーとの DLP ポリシーの関連付け

- 「デフォルトの発信メール ポリシーとの DLP ポリシーの関連付け」 (P.15-22)
- 「発信メール ポリシーを使用した送信者および受信者への DLP ポリシーの割り当て」 (P.15-22)

デフォルトの発信メール ポリシーとの DLP ポリシーの関連付け

デフォルトの発信メール ポリシーは、他の発信メール ポリシーが送信者または受信者に一致しない場合に使用されます。

図 15-1 イネーブルになっている DLP ポリシーを伴うデフォルトの発信メール ポリシー
Outgoing Mail Policies



Order	Policy Name	Anti-Spam	Anti-Virus	Content Filters	Outbreak Filters	DLP	Delete
	Default Policy	Not Available	Not Available	Disabled	Not Available	California SB-1386 Restricted Files	

Key: Default Custom Disabled

はじめる前に

「RSA メール DLP を使用した導入の場合のデータ消失防止をセットアップする方法」(P.15-4) のテーブルの、ここまでのすべてのアクティビティを実行します。たとえば、デフォルトの発信メール ポリシーに含める DLP ポリシーを作成したことを確認します。

手順

- ステップ 1 [メール ポリシー (Mail Policies)] > [メール ポリシー (Mail Policies)] を選択します。
- ステップ 2 テーブルの [デフォルト ポリシー (Default Policy)] の行で、[DLP] の列の [ディセーブル (Disabled)] リンクをクリックします。
- ステップ 3 [DLP を有効にする (設定をカスタマイズ) (Enable DLP (Customize Settings))] を選択します。
- ステップ 4 デフォルトの発信メール ポリシーでイネーブルにする DLP ポリシーを選択します。
- ステップ 5 変更内容を送信し、確定します。

次の作業

追加の発信メール ポリシーの DLP ポリシーを選択します。「発信メール ポリシーを使用した送信者および受信者への DLP ポリシーの割り当て」(P.15-22) を参照してください。

発信メール ポリシーを使用した送信者および受信者への DLP ポリシーの割り当て

発信メール ポリシーでイネーブルにすることによって、どの送信者と受信者にどの DLP ポリシーを適用するかを指定します。発信メール ポリシー内で DLP ポリシーだけを使用することができます。

はじめる前に

デフォルトの発信メール ポリシーの DLP ポリシーを設定します。「デフォルトの発信メール ポリシーとの DLP ポリシーの関連付け」(P.15-22) を参照してください。

手順

- ステップ 1 [メール ポリシー (Mail Policies)] > [メール ポリシー (Mail Policies)] を選択します。
- ステップ 2 テーブルの任意の行の DLP 列のリンクをクリックします。

- ステップ 3** この発信メール ポリシーに関連付ける DLP ポリシーを選択します。
- ステップ 4** 変更を送信します。
- ステップ 5** 他の発信メール ポリシーに対して、必要に応じて繰り返します。
- ステップ 6** 変更内容を確定します。

次の作業

「RSA メール DLP を使用した導入の場合のデータ消失防止をセットアップする方法」(P.15-4) を参照してください。

DLP ポリシーの編集または削除に関する重要な情報

アクション	情報
DLP ポリシーの編集	ポリシーの名前を変更すると、発信メール ポリシーで再度イネーブルにする必要があります。
DLP ポリシーの削除	ポリシーを削除すると、DLP ポリシーが 1 つ以上の発信メール ポリシーで使用された場合に、通知を受信します。DLP ポリシーの削除により、このようなメール ポリシーからポリシーが削除されます。

RSA Enterprise Manager

- 「Enterprise Manager と電子メール セキュリティ アプライアンスの連携方法」(P.15-23)
- 「Enterprise Manager のマニュアル」(P.15-24)
- 「RSA Enterprise Manager の導入における展開データ消失防止のセットアップ方法」(P.15-24)
- 「RSA メール DLP から RSA Enterprise Manager への移行」(P.15-30)
- 「Enterprise Manager の DLP ポリシー更新の確認」(P.15-31)
- 「RSA Enterprise Manager と言語サポート」(P.15-32)
- 「クラスタ化されたアプライアンスでの Enterprise Manager の使用」(P.15-32)
- 「Enterprise Manager 導入におけるポリシーの削除とディセーブル化について」(P.15-32)
- 「電子メール セキュリティ アプライアンスと Enterprise Manager 間の接続の切断」(P.15-33)
- 「Enterprise Manager から RSA メール DLP への切り替え」(P.15-33)

Enterprise Manager と電子メール セキュリティ アプライアンスの連携方法

RSA Enterprise Manager DLP を電子メール セキュリティ アプライアンス でイネーブルにすると、アプライアンスは電子メール セキュリティ アプライアンス をパートナー デバイスとして自動的に追加する Enterprise Manager に設定を送信します。次に Enterprise Manager を開くときは、電子メール セキュリティ アプライアンス に設定した発信メール ポリシーの名前とメタデータ、およびメッセージア

クシオンが Enterprise Manager に表示され、DLP ポリシーを設定するときに使用できるようになります。(代わりに、既存の DLP ポリシーを電子メールセキュリティアプライアンスから Enterprise Manager にエクスポートできます)。

Enterprise Manager の DLP ポリシーを設定すると、Enterprise Manager は電子メールセキュリティアプライアンスに DLP ポリシーを送信します。デフォルトでは、Enterprise Manager にプッシュされたすべての DLP ポリシーは、電子メールセキュリティアプライアンスも含めたプッシュ先となるすべてのデバイスでイネーブルになります。

電子メールセキュリティアプライアンスは、Enterprise Manager から受信した DLP ポリシーを保存し、違反に対する発信メッセージのスキャンに使用し、検出された違反に対しアクションを実行します。電子メールセキュリティアプライアンスは、該当する場合はメッセージの暗号化を含めた、配信にリリースされるメッセージの処理をします。電子メールセキュリティアプライアンスは、表示と管理のために違反に関する情報を送信します。

関連項目

- 「データ消失防止の動作」(P.15-2)
- 「DLP 配置オプション」(P.15-3)

Enterprise Manager のマニュアル

この導入では、RSA Inc. の次のマニュアルが必要になります。

- 『*Managing Partner Device DLP with Enterprise Manager*』(テクニカルノート)。Enterprise Manager のセットアップと、それを使用した Cisco Email Security アプライアンスを含むパートナーデバイスの DLP 機能の管理方法を説明します。
- 『*RSA DLP Network 9.0 Deployment Guide*』。ネットワークで RSA DLP ソフトウェアを展開する方法を説明します。
- 『*RSA DLP Network 9.0 User Guide*』。Enterprise Manager を使った Cisco Email Security アプライアンスなどのパートナー DLP デバイスの管理方法や、RSA DLP Network ソフトウェアの使用手順を説明します。

RSA Enterprise Manager の導入における展開データ消失防止のセットアップ方法

次の手順を順番に実行します。

	操作内容	追加情報
ステップ1	ネットワークに Enterprise Manager を設定し、電子メールセキュリティアプライアンスとの提携の準備をします。	DLP Datacenter については、オンラインヘルプおよび『 <i>Managing Partner Device DLP with Enterprise Manager</i> 』のテクニカルノートを含む、RSA のマニュアルを確認します。
ステップ2	電子メールセキュリティアプライアンスで、どのメッセージに対して DLP 違反をスキャンするかを決定する発信メールポリシーを作成します。 異なるポリシーは、ユーザのユーザまたはグループに割り当てることができます。	第 10 章「メールポリシー」を参照してください。 注： 発信メールポリシーには受信者を指定するオプションがあります。ただし、Enterprise Manager を使用した導入の場合、この情報は LDAP からは入手できません。

	操作内容	追加情報
ステップ3	電子メールセキュリティ アプライアンス で、DLP 違反が検出された、または疑われたメッセージに対して実行できるアクションを定義します。 たとえば、そのようなメッセージを隔離できます。	「メッセージアクション」(P.15-33)
ステップ4	電子メールセキュリティ アプライアンス と Enterprise Manager 間のセキュアな通信に証明書を取得およびアップロードします。	「電子メールセキュリティ アプライアンスと Enterprise Manager 間の SSL 接続用の証明書の取得とアップロード(推奨)」(P.15-26) を参照してください。
ステップ5	電子メールセキュリティ アプライアンス で、ESA の DLP モード用の RSA Enterprise Manager を選択し、電子メールセキュリティ アプライアンスと Enterprise Manager 間の接続を設定します。	「Enterprise Manager DLP の有効化と電子メールセキュリティ アプライアンスとの接続の設定」(P.15-28) を参照してください。
ステップ6	Enterprise Manager にメッセージ送信者の LDAP 識別名を提供します。	「Enterprise Manager へのメッセージ送信者を識別する LDAP の使用」(P.15-29)
ステップ7	電子メールセキュリティ アプライアンス から DLP ポリシーをエクスポートして、Enterprise Manager にインポートする場合は、ここで指定します。	電子メールセキュリティ アプライアンス から RSA メール DLP ポリシーをエクスポートするには、「電子メールセキュリティ アプライアンスからの DLP ポリシーのエクスポート」(P.15-31) を参照してください。 ポリシーをインポートするには、RSA Enterprise Manager のマニュアルを参照してください。
ステップ8	Enterprise Manager で、DLP ポリシーを作成します。 <ul style="list-style-type: none"> 違反と見なすコンテンツのタイプを識別します。 各違反について実行するアクションを指定します。 	オンライン ヘルプおよびテクニカル ノート『 <i>Managing Partner Device DLP with Enterprise Manager</i> 』を含め、DLP データセンター向け RSA のドキュメントで DLP ポリシーを作成するための手順に従います。
ステップ9	Enterprise Manager で、発信メール ポリシーに DLP ポリシーを関連付けることにより、どの送信者と受信者にどの DLP ポリシーを適用するかを指定します。	「Enterprise Manager 導入の DLP ポリシーに発信メール ポリシーを関連付ける方法について」(P.15-30) を参照してください。
ステップ10	Enterprise Manager で、DLP ポリシーの順序を指定します。 アプライアンスが DLP 違反のメッセージを評価するときは、リストの最初に一致したポリシーにのみ適用します。	Enterprise Manager で DLP ポリシーを配置します。 RSA Enterprise Manager のマニュアルを参照してください。
ステップ11	電子メールセキュリティ アプライアンス で、メッセージトラッキングでのストレージの設定と機密 DLP 情報へのアクセスを構成します。	<ul style="list-style-type: none"> 「メッセージトラッキングの機密 DLP データの表示または非表示」(P.15-38) 「メッセージトラッキングでの機密情報へのアクセスの制御」(P.28-5)

フィンガープリント

Enterprise Manager の導入に、RSA の DLP データセンターが含まれている場合、フィンガープリントをイネーブルにできます。

フィンガープリントによって、ソース コードおよび機密文書の検出が向上します。

- データベース
- ドキュメントのテキストの完全または部分一致するテキスト
- ファイルのビット単位の完全一致である、完全バイナリー一致

フィンガープリントをイネーブルにした場合、Enterprise Manager は電子メール セキュリティ アプライアンスにフィンガープリントの検出情報を送信し、電子メール セキュリティ アプライアンスは、データ消失防止でこのメッセージをスキャンするときにこの情報を使用します。

フィンガープリントの詳細については、Enterprise Manager のマニュアルを参照してください。

関連項目

- 「Enterprise Manager DLP の有効化と電子メール セキュリティ アプライアンスとの接続の設定」 (P.15-28)

電子メール セキュリティ アプライアンスと Enterprise Manager 間の SSL 接続用の証明書の取得とアップロード (推奨)

電子メール セキュリティ アプライアンスと Enterprise Manager との SSL 接続を使用する場合は、公認の認証局から 1 つ以上の証明書および 2 台のマシンの相互認証に使用する署名キーが必要です。

SSL 接続を設定する場合、Enterprise Manager サーバがサーバで、電子メール セキュリティ アプライアンスはクライアントになります。

次の手順をすべて実行します。

- 「RSA の証明書のツールを使用したクライアントおよびサーバの証明書の生成」 (P.15-26)
- 「電子メール セキュリティ アプライアンスへの証明書のアップロード」 (P.15-27)
- 「電子メール セキュリティ アプライアンスへのカスタム認証局ファイルのアップロード」 (P.15-28)
- 「Enterprise Manager の電子メール セキュリティ アプライアンスからの証明書の生成」 (P.15-28)
- 「SSL 設定の完了」 (P.15-28)

RSA の証明書のツールを使用したクライアントおよびサーバの証明書の生成

RSA では、接続のサーバ認証とクライアント認証の両方に使用できる単一 .p12 ファイルの生成に使用できる証明書の生成ツールを提供します。アプライアンスおよび Enterprise Manager サーバに異なる証明書を使用する場合は、別のソースから取得する必要があります。

このツールは、Enterprise Manager サーバに p12 証明書ファイルと .pem 証明書ファイルの 2 つのファイルを作成して保存します。p12 ファイルを使用する場合は、認証局のリストとして電子メール セキュリティ アプライアンスに .pem ファイルをインポートする必要があります。

詳細については、RSA のマニュアルを参照してください。

手順

ステップ 1 Enterprise Manager サーバ上でコマンドプロンプトを開きます。

ステップ 2 C:\Program Files\RSA\Enterprise Manager\ などに変更します。

ステップ 3 次のコマンドを実行します。

```
「%JAVA_HOME%/bin/java」 -cp ./emcerttool.jar
com.rsa.dlp.tem.X509CertGenerator -clientservercasigned -cacn <NAME OF CAPROVIDED DURING
INSTALL> -cakeystore catem-keystore -castorepass <PASSWORD FOR CA PROVIDED DURING
INSTALL> -cn <DEVICE_CN> -storepass <DEVICE STORE PASSWORD> -keystore <NAME OF DEVICE
STORE>
```



(注) 証明書的一般名は、の 電子メール セキュリティ アプライアンス ホスト名である必要があります。

Enterprise Manager が、グループまたはクラスター レベルで接続された電子メール セキュリティ アプライアンスを管理する場合は、各アプライアンスには、そのアプライアンスのホスト名に一致する共通名を使用した証明書が必要です。

コマンドの例は、次のように表示されます。

```
[%JAVA_HOME%/bin/java] -cp ./emcerttool.jar
com.rsa.dlp.tem.X509CertGenerator -clientservercasigned -cacn emc-cisco
-cakeystore catem-keystore -castorepass esaem -cn ironport -storepass esaem
-keystore device-store
```

また、次のコマンドライン スイッチを使用できます。

```
-org <value in double quotes if it contains space>
-orgunit <value in double quotes if it contains space>
-title <value in double quotes if it contains space>
-validity <number of days>
```

この手順は、同じフォルダに < device-store>.p12 ファイルを出力します。

この .p12 ファイルが、電子メール セキュリティ アプライアンス にアップロードする証明書です。

また次も必要になります。

- このフォルダからの .pem ファイルは、電子メール セキュリティ アプライアンス のカスタム認証局リストにインポートするために必要です。
- 入力した Device Store のパスワード。

電子メール セキュリティ アプライアンスへの証明書のアップロード

はじめる前に

.p12 証明書ファイルを作成します。「RSA の証明書のツールを使用したクライアントおよびサーバの証明書の生成」(P.15-26) でこの手順を使用できます。

手順

- ステップ 1** [ネットワーク (Network)] > [証明書 (Certificates)] を選択します。
- ステップ 2** [証明書の追加 (Add Certificate)] をクリックします。
- ステップ 3** [証明書のインポート (Import Certificate)] オプションを選択します。
- ステップ 4** ネットワーク上またはローカル マシンの証明書ファイルへのパスを入力します。
- ステップ 5** ファイルのパスワードを入力します。
- ステップ 6** [次へ (Next)] をクリックして証明書の情報を表示します。

- ステップ 7** 証明書の名前を入力します。電子メール セキュリティ アプライアンスは共通名をデフォルトで割り当てます。
- Enterprise Manager が、グループまたはクラスター レベルで接続された電子メール セキュリティ アプライアンスを管理する場合、すべての証明書は、それぞれの証明書の共通名がクラスターの各マシンに固有であっても、同じ証明書名でなければなりません。
- ステップ 8** 変更内容を送信し、確定します。

電子メール セキュリティ アプライアンスへのカスタム認証局ファイルのアップロード

はじめる前に

認証局のファイルを取得します。「[RSA の証明書のツールを使用したクライアントおよびサーバの証明書の生成](#)」(P.15-26) の手順を使用して証明書を生成した場合、これは .p12 証明書ファイルと同じフォルダにある .pem ファイルです。

手順

- ステップ 1** [ネットワーク (Network)] > [証明書 (Certificates)] を選択します。
- ステップ 2** [認証局 (Certificate Authorities)] セクションで、[設定を編集 (Edit Settings)] をクリックします。
- ステップ 3** [カスタム リスト (Custom List)] の [有効 (Enable)] をクリックします。
- ステップ 4** ローカル マシンまたはネットワーク マシンのカスタム リスト (.pem ファイル) のフルパスを入力します。
- ステップ 5** 変更内容を送信し、確定します。

Enterprise Manager の電子メール セキュリティ アプライアンスからの証明書の生成

クライアントとサーバの両方で同じ証明書を使用しない場合は、電子メール セキュリティ アプライアンスからの自己署名証明書を生成し、Enterprise Manager にアップロードできます。「[GUI を使用した自己署名証明書の作成](#)」(P.20-3) を参照してください。

SSL 設定の完了


「[Enterprise Manager DLP の有効化と電子メール セキュリティ アプライアンスとの接続の設定](#)」(P.15-28) で SSL 設定を完了します。

Enterprise Manager DLP の有効化と電子メール セキュリティ アプライアンスとの接続の設定

はじめる前に

- テーブル「[RSA Enterprise Manager の導入における展開データ消失防止のセットアップ方法](#)」(P.15-24) のこのステップの前にすべての手順を完了します。
- お使いの環境に RSA の DLP データセンターが含まれている場合、フィンガープリントをイネーブルにできます。詳細については、「[フィンガープリント](#)」(P.15-25) を参照してください。

手順

- ステップ 1** 電子メール セキュリティ アプライアンスで [セキュリティ サービス (Security Services)] > [RSA メール DLP (RSA Email DLP)] を選択します。
- ステップ 2** 以前、データ消失防止をイネーブルした場合は、[設定を編集 (Edit Settings)] をクリックし、[ステップ 5](#) に移動します。
- ステップ 3** [有効 (Enable)] をクリックします。
- ステップ 4** ライセンス契約書ページの下部にスクロールし、[承認 (Accept)] をクリックしてライセンス契約に合意します。
-  **(注)** ライセンス契約に合意しない場合、データ消失防止はアプライアンスでイネーブルになりません。
- ステップ 5** [データ消失防止 (Data Loss Prevention)] から、[RSA Enterprise Manager] を選択します。
- ステップ 6** DLP ポリシーおよびポート番号 20000 の管理に、使用するネットワークの Enterprise Manager サーバのホスト名を入力します。コロンを使用してホスト名とポート番号を区切ります (:)。
- ステップ 7** 電子メール セキュリティ アプライアンスと Enterprise Manager との SSL 接続を使用するには、次の手順を実行します。
- [SSL 通信を有効にする (Enable SSL Communication)] のチェックボックスを選択します。
 - サーバ証明書を選択します。サーバは、Enterprise Manager です。
 - クライアント証明書を選択します。クライアントは電子メール セキュリティ アプライアンスです。クライアントとサーバの両方で同じ証明書を使用できます。
- ステップ 8** (任意) お使いの環境に RSA の DLP データセンターが含まれている場合、フィンガー プリントを有効にしてソース コード、データベースやその他の文書の検出を改善するかどうかを選択します。
- ステップ 9** (任意) メッセージ トラッキングがアプライアンス上ですでにイネーブルになっている場合は、一致したコンテンツのログギングをイネーブルにするかしないかを選択します。
- これを選択すると、電子メール セキュリティ アプライアンスは DLP 違反をログに記録し、AsyncOS は DLP 違反および周辺コンテンツをメッセージ トラッキングに表示します。その中には、クレジットカード番号や社会保障番号などの機密データが含まれます。
- ステップ 10** 自動的に DLP エンジンに更新をダウンロードするようにアプライアンスを有効にしないでください。
- ステップ 11** 変更内容を送信し、確定します。
- 電子メール セキュリティ アプライアンスはパートナー デバイスとして自動的にアプライアンスを追加する Enterprise Manager に設定を送信します。

Enterprise Manager へのメッセージ送信者を識別する LDAP の使用

電子メール セキュリティ アプライアンス が DLP インシデント データを Enterprise Manager に送信する場合、メッセージ送信者を特定するために、アプライアンスは完全な LDAP 識別名を含める必要があります。アプライアンスが LDAP サーバからこの情報を取得します。

はじめる前に

- 「RSA Enterprise Manager の導入における展開データ消失防止のセットアップ方法」(P.15-24) のテーブルの、ここまでのすべてのステップを実行します。[ユーザ識別名クエリ (User Distinguished Name Query)] オプションは、これらの手順に従わない場合は利用できません。
- 電子メールセキュリティ アプライアンスの LDAP サーバ プロファイルを作成します。詳細については、第 22 章「LDAP クエリ」を参照してください。
- デフォルトのクエリを使用しない場合は、完全な識別名を取得するためにアプライアンスが使用するクエリ文字列を作成します。Active Directory サーバに対して、デフォルトのクエリ文字列は (proxyAddresses=smtp: {a}) です。OpenLDAP サーバの場合は、デフォルトのクエリ文字列は (mail= {a}) です。独自のクエリとメール属性を定義することもできます。属性が複数の場合は、カンマで区切ります。

手順

-
- ステップ 1** 電子メールセキュリティ アプライアンスの [システム管理 (System Administration)] > [LDAP] を選択します。
- ステップ 2** ユーザが使用する LDAP サーバのプロファイルを編集します。
- ステップ 3** [ユーザ識別名 (User Distinguished Name Query)] のチェックボックスを選択します。
このオプションは、DLP 導入オプションとして RSA Enterprise Manager を選択した場合にだけ使用できます。
- ステップ 4** クエリの名前を入力します。
- ステップ 5** ユーザの識別名を取得するためのクエリ文字列を入力します。
- ステップ 6** クエリをテストするには、このボタンをクリックします。
- ステップ 7** 変更内容を送信し、確定します。
-

Enterprise Manager 導入の DLP ポリシーに発信メール ポリシーを関連付ける方法について

どの送信者および受信者に、どの DLP ポリシーを適用するかを指定するには、Enterprise Manager を使用して DLP ポリシーに発信メール ポリシーを関連付けます。詳細については、RSA Enterprise Manager のマニュアルを参照してください。Enterprise Manager はメッセージのスキャンに使用するために電子メールセキュリティ アプライアンスにメッセージを送信します。

RSA メール DLP とは異なり、発信メール ポリシーは、Enterprise Manager がイネーブルの場合、デフォルトのメール ポリシーの DLP 設定を使用できません。メール ポリシーが Enterprise Manager で DLP ポリシーに指定されていない場合は、DLP スキャンは、メール ポリシーでイネーブルになりません。

RSA メール DLP から RSA Enterprise Manager への移行

既存の RSA メール DLP 設定を RSA Enterprise Manager に移行する場合、RSA メール DLP モードから RSA Enterprise Manager モードにアプライアンスを切替える前に Enterprise Manager にアップロードできる DLP 設定を .zip ファイルにエクスポートできます。

電子メールセキュリティ アプライアンスは、Enterprise Manager から DLP ポリシーの最初パッケージを受信するまで既存のローカル RSA メール DLP ポリシーを使用します。

電子メール セキュリティ アプライアンスは、後で RSA メール DLP モードに戻す場合のために、既存の RSA メール DLP ポリシーを保存します。

関連項目

- 「電子メール セキュリティ アプライアンスからの DLP ポリシーのエクスポート」 (P.15-31)
- 「RSA Enterprise Manager の導入における展開データ消失防止のセットアップ方法」 (P.15-24)

電子メール セキュリティ アプライアンスからの DLP ポリシーのエクスポート

DLP ポリシー設定を .zip ファイルとして 電子メール セキュリティ アプライアンス からエクスポートし、Enterprise Manager にインポートできます。

DLP 導入モードとして選択されているのが RSA メール DLP または RSA Enterprise Manager であるかにかかわらず DLP ポリシーをエクスポートできます。

手順

ステップ 1 [セキュリティ サービス (Security Services)] > [RSA メール DLP (RSA Email DLP)] を選択します。

ステップ 2 [DLP 設定のエクスポート (Export DLP Configuration)] をクリックします。

ステップ 3 .zip ファイルの名前を入力し、[エクスポート (Export)] をクリックします。

無効化された DLP ポリシーと発信メール ポリシーに割り当てられていない DLP ポリシーは含まれていません。



(注) 電子メール セキュリティ アプライアンスがクラスタの一部の場合、アプライアンスはクラスタの低レベルからのみポリシーをエクスポートします。たとえば、DLP ポリシーがクラスタとマシン レベルにある場合、アプライアンスはマシン レベルからのみ DLP ポリシーをエクスポートします。

次の作業

Enterprise Manager に DLP ポリシーをインポートし、管理対象アプライアンスへ配布することについては、Enterprise Manager のマニュアルを参照してください。

Enterprise Manager の DLP ポリシー更新の確認

Enterprise Manager は定期的に 電子メール セキュリティ アプライアンス の DLP ポリシーを更新します。

Enterprise Manager から最新の DLP ポリシー更新を表示するには、[セキュリティ サービス (Security Services)] > [RSA メール DLP (RSA Email DLP)] に移動します。

関連項目

- 「電子メール セキュリティ アプライアンスと Enterprise Manager 間の接続の切断」 (P.15-33)

RSA Enterprise Manager と言語サポート

電子メール セキュリティ アプライアンスは、Enterprise Manager で使用していた言語で RSA Enterprise Manager から受信したデータを表示します。アプライアンスは、アプライアンスのインターフェイスに選択した言語ではこの情報を表示できません。これは、アプライアンスがデータ パッケージで受信した Enterprise Manager で作成された DLP ポリシー、コンテンツ照合分類子、辞書およびその他すべてに適用されます。たとえば、Enterprise Manager の DLP ポリシーと分類子が英語で記述されていた場合は、電子メール セキュリティ アプライアンスのインターフェイスがフランス語で表示される場合でも、電子メール セキュリティ アプライアンスは Enterprise Manager からの DLP ポリシーと分類子の名前と説明を英語で表示します。他のインターフェイスはフランス語で表示されます。

クラスタ化されたアプライアンスでの Enterprise Manager の使用

クラスタ化された電子メール セキュリティ アプライアンスの DLP ポリシーの管理に Enterprise Manager を使用する場合、次に注意してください。

- 電子メール セキュリティ アプライアンスは Enterprise Manager に発信メール ポリシーとメッセージアクションをこれらの設定が構成されている最小クラスタ レベルから送信します。これらの設定がクラスタとマシン レベルで個別に設定されている場合、電子メール セキュリティ アプライアンスはマシン レベルから Enterprise Manager に設定を送信します。より高いクラスタ レベルで発信メール ポリシーおよびメッセージアクションを使用する場合は、使用しない低レベルで定義したポリシーとアクションを削除します。
- 電子メール セキュリティ アプライアンスは、この設定が構成されている最小クラスタ レベルで指定されたデータ消失防止モードを使用します。たとえば、クラスタ化されたアプライアンスが、ローカル RSA メール DLP モードをマシン レベルで使用し、RSA Enterprise Manager をクラスタ レベルで使用するよう設定されている場合、アプライアンスはデータ消失防止に RSA メール DLP を使用し、Enterprise Manager とは通信しません。

Enterprise Manager 導入におけるポリシーの削除とディセーブル化について

DLP ポリシーの削除とディセーブル化

- DLP ポリシーを削除するには、Enterprise Manager を使用します。
- DLP ポリシーをディセーブルまたはイネーブルにするには、電子メール セキュリティ アプライアンスを使用します。[メール ポリシー (Mail Policies)] > [DLP ポリシーマネージャ (DLP Policy Manager)] に移動します。

無効 DLP ポリシーに関連付けられた発信メール ポリシーは、DLP 違反のメッセージの評価時にこのポリシーをとばします。

発信メール ポリシーの削除

DLP ポリシーにリンクされている発信メール ポリシーを削除しようとする、電子メール セキュリティ アプライアンスにメール ポリシーが使用中であることを警告するメッセージが表示されます。ポリシーをいったん削除すると、Enterprise Manager は自動的にそれを使用した DLP ポリシーから削除された発信メール ポリシーのリンクを解除します。削除されたメール ポリシーの設定に基づいたメッセージをスキャンしないこと以外は、DLP スキャンは以前と同様に動作します。Enterprise Manager によって電子メール セキュリティ アプライアンスに送信された次の DLP ポリシー パッケージには、削除されたメール ポリシーに関連しているものは何も含まれません。

電子メールセキュリティ アプライアンスと Enterprise Manager 間の接続の切断

電子メールセキュリティ アプライアンスと企業マネージャ間の接続が失われると、アプライアンスおよび Enterprise Manager が送信できないデータは、接続が復元されるまで配信のためにキューに入れます。電子メールセキュリティ アプライアンス の場合は、DLP 違反を含んでいる可能性のあるメッセージ データがキューに格納されていることを意味します。Enterprise Manager の場合は、新しい DLP ポリシー情報を持つデータのパッケージがキューに格納されていることを意味します。Enterprise Manager から更新された DLP ポリシー データを 電子メールセキュリティ アプライアンス が受信しない場合、アプライアンスは、Enterprise Manager から前に受信した DLP ポリシーを使用し続けます。

関連項目

- 「Enterprise Manager は電子メールセキュリティ アプライアンスとの接続を解除します。」(P.15-43)

Enterprise Manager から RSA メール DLP への切り替え

RSA Enterprise Manager を使用してからデータ消失防止に RSA メール DLP の使用に戻す場合、「データ消失防止のイネーブル化 (RSA Email DLP)」(P.15-5) を参照してください。

電子メールセキュリティ アプライアンスは、RSA Enterprise Manager モードを使用するように設定する前に使用していた RSA メール DLP ポリシーに自動的に戻します。RSA メール DLP モードだったときにアプライアンスがローカル DLP ポリシーを使用しなかった場合、アプライアンスはローカル DLP ポリシーを作成するまで Enterprise Manager の DLP ポリシーを使用し続けます。

Enterprise Manager と類似したローカル DLP ポリシーを使用する場合は、DLP Policy Manager を使用してそれらを再作成できます。電子メールセキュリティ アプライアンスは自動的に Enterprise Manager が使用するものに基づいて新しいポリシーを作成せず、Enterprise Manager からインポートすることはできません。

DLP Policy Manager を使用した DLP ポリシーの作成の詳細については、「RSA Email DLP の DLP ポリシー」(P.15-6) を参照してください。

Enterprise Manager のパートナー デバイスとして電子メールセキュリティ アプライアンスを除外する手順については、RSA Enterprise Manager のマニュアルを参照してください。

メッセージアクション

発信メッセージから DLP 違反の可能性が検出されると、電子メールセキュリティ アプライアンス が実行するプライマリおよびセカンダリ アクションを指定します。さまざまなアクションに対して、異なる違反タイプおよび重大度を割り当てることができます。

プライマリ アクションは次のとおりです。

- 配信 (Deliver)
- ドロップ (Drop)
- 隔離 (Quarantine)

セカンダリ アクションは次のとおりです。

- メッセージを配信する場合は、コピーをポリシー隔離に送信します。このコピーは、メッセージ ID を含む元のメッセージの完全なクローンです。コピーの隔離は、DLP 違反を監視する別の方法を提供する他、導入前に RSA メール DLP システムをテストすることができます。隔離からコピーをリリースすると、アプライアンスはすでに元のメッセージを受信した受信者にコピーを配信します。
- メッセージの暗号化 このアプライアンスは、メッセージ本文だけを暗号化します。メッセージヘッダーは暗号化されません。
- DLP 違反があるメッセージの件名ヘッダーの変更
- メッセージへの免責事項の追加。
- 代替宛先メールホストへのメッセージの送信。
- 他の受信者にメッセージのコピー (bcc) の送信。(たとえば、重大な DLP 違反を含むメッセージのコピーを、検査のためにコンプライアンス責任者のメールボックスに送信します)。
- DLP 違反の通知メッセージを、送信者や、マネージャまたは DLP コンプライアンス責任者といった他の連絡先に送信します。「DLP 通知のドラフト」(P.15-36) を参照してください。



(注)

これらのアクションは相互排他的ではなく、各ユーザグループのさまざまな要求を処理するために、異なる DLP ポリシー内でアクションをいくつか組み合わせることができます。また、同じポリシーの異なる重大度レベルに基づいて別の処理を設定できます。たとえば、重大な DLP 違反を含むメッセージを隔離し、コンプライアンス担当者に通知を送信しますが、重大度レベルの低いメッセージを配信することもできます。

DLP 違反アクション (メッセージアクション) に対して実行するアクションの定義

はじめる前に

- DLP ポリシーに違反したメッセージ (またはメッセージのコピー) を保持する専用隔離を少なくとも 1 つ作成します。

これは、電子メールセキュリティアプライアンスの内部隔離またはセキュリティ管理アプライアンスの集中型隔離に指定できます。

Enterprise Manager を使用した導入の場合

- Enterprise Manager がタスクを完了するために十分なタイムアウトを設定します。
- 自動処理については慎重に考慮してください。隔離されたメッセージは Enterprise Manager で管理する必要がありますが、電子メールセキュリティアプライアンスは隔離スペースが割り当てられたスペースを超えると、隔離メッセージをリリースまたは削除します。

詳細については、第 27 章「隔離」を参照してください。

- 配信前にメッセージを暗号化する場合は、暗号化プロファイルを設定してください。第 16 章「Cisco Email Encryption」を参照してください。
- DLP 違反またはその疑いがあるメッセージを配信する場合、免責事項を含めるには、[メールポリシー (Mail Policies)] > [テキストリソース (Text Resources)] で、免責事項のテキストを指定します。詳細については、「免責事項テンプレート」(P.18-12) を参照してください。
- DLP 違反の送信者またはコンプライアンス責任者などの他の人に通知を送信するには、まず DLP 通知テンプレートを作成します。「DLP 通知のドラフト」(P.15-36) を参照してください。

手順

-
- ステップ 1** [メール ポリシー (Mail Policies)] > [DLP ポリシーのカスタマイズ (DLP Policy Customizations)] を選択します。
- ステップ 2** [メッセージアクション (Message Actions)] セクションで [メッセージアクションの追加 (Add Message Action)] をクリックします。
- ステップ 3** メッセージアクションの名前を入力します。
- ステップ 4** メッセージアクションの説明を入力します。
- ステップ 5** DLP 違反を含むメッセージをドロップ、配信、または隔離するか選択します。



(注) [配信 (Deliver)] を選択すると、ポリシー隔離に送信されたメッセージのコピーを取ることを選択できます。メッセージのコピーはメッセージ ID を含む完全なクローンです

- ステップ 6** 配信にメッセージの隔離からリリースを暗号化する場合は、[暗号化を有効にする (Enable Encryption)] チェックボックスを選択して、次のオプションを選択します。
- [暗号化ルール (Encryption Rule)]。メッセージを常に暗号化するか、TLS 接続を介した送信試行が最初に失敗した場合だけ暗号化します。
 - [暗号化プロファイル (Encryption Profile)]。Cisco IronPort 暗号化アプライアンスまたはまたはホステッドキーサービスを使用する場合、指定した暗号化プロファイルを使用してメッセージを暗号化し、配信します。
 - [暗号化されたメッセージの件名 (Encrypted Message Subject)]。暗号化されたメッセージの件名です。既存のメッセージ件名を保持するには、\$Subject の値を使用します。
- ステップ 7** アクションとして隔離を選択した場合は、DLP 違反を含むメッセージに使用するポリシー隔離を選択します。
- ステップ 8** 次のオプションのいずれかを使用してメッセージを変更する場合は、[詳細 (Advanced)] をクリックします。
- カスタム ヘッダーを追加します。
 - メッセージの件名を変更します。
 - 代替ホストに配信します。
 - 他の受信者にコピー (bcc) を送信します
 - DLP 通知メッセージを送信します。
- ステップ 9** 変更内容を送信し、確定します。
-

メッセージアクションの表示および編集

手順

-
- ステップ 1** [メール ポリシー (Mail Policies)] > [DLP ポリシーのカスタマイズ (DLP Policy Customizations)] を選択します。
- ステップ 2** [メッセージアクション (Message Actions)] セクションでアクションを選択します。

目的	操作内容
各アクションが割り当てられているメールポリシーを表示します。	メッセージアクション表の見出しで [ポリシー (Policies)] のリンクをクリックします。
アクションごとに入力した説明を表示します。	メッセージアクション表の見出しで [説明 (Description)] のリンクをクリックします。
メッセージアクションの詳細を表示または編集します。	メッセージアクションの名前をクリックします。
メッセージアクションを削除します。	削除対象のメッセージアクションの横にあるゴミ箱のアイコンをクリックします。 確認メッセージは、1つ以上の DLP ポリシーでメッセージアクションが使用されているかどうかを通知します。
メッセージアクションを複製します。 この機能は、メッセージアクションを変更する前にバックアップコピーを作成するか、または新たな、または類似のメッセージアクションの出発点として使用するために使用できます。	複製するメッセージアクションの横にある [重複 (Duplicate)] アイコンをクリックします。

ステップ 3 変更を送信し、確定します。

DLP 通知のドラフト

組織のデータ消失防止ポリシーに違反する情報が電子メールメッセージに含まれている場合に送信される通知のテンプレートを作成するには、この手順を使用します。この通知は、DLP ポリシーに違反しているメッセージの送信者、または別のアドレス（マネージャまたは DLP コンプライアンス責任者）に送信できます。

はじめる前に

- RSA Enterprise Manager を使用した導入の場合、電子メールセキュリティ アプライアンス ([メッセージアクション (Message Actions)] ページ) または Enterprise Manager (DLP ポリシー) を DLP 違反の通知をユーザに送信するように設定できます。重複する通知を回避するには、両方ではなくどちらか一方を使用して通知を設定します。
- 「[DLP 通知テンプレートの変数の定義](#)」(P.15-37) の内容についてよく理解しておきます。各違反についての詳細を含む通知をカスタマイズするためにこれらの変数を使用できます。

手順

ステップ 1 [メールポリシー (Mail Policies)] > [テキストリソース (Text Resources)] を選択します。

ステップ 2 [テキストリソースを追加 (Add Text Resource)] をクリックします。

ステップ 3 [タイプ (Type)] に、[DLP 通知テンプレート (DLP Notification Template)] を選択します。

DLP 変数は通常の通知テンプレートでは利用可能ではありません。

ステップ 4 通知テキストおよび変数を入力します。

通知は、発信メッセージに組織のデータ消失防止ポリシーに違反する機密データが含まれるかもしれないことを受信者に通知する必要があります。

次の作業

DLP Policy Manager の DLP ポリシーで [メッセージアクション (Message Action)] にこの DLP 通知テンプレートを指定します。

DLP 通知テンプレートの変数の定義

通知に、各 DLP 違反に関する特定の情報を含めるには、次の変数を使用します。

変数	置き換える値
\$DLPPolicy	違反があった Email DLP ポリシーの名前に置き換えられます。
\$DLPSeverity	違反の重大度に置き換えられます。「Low」、「Medium」、「High」または「Critical」のいずれかです。
\$DLPRiskFactor	メッセージに含まれる機密性の高い情報のリスク係数 (0 ~ 100 のスコア) に置き換えられます。
\$To	メッセージの To: ヘッダーに置き換えられます (エンベロープ受信者には置き換えられません)。
\$From	メッセージの From: ヘッダーに置き換えられます (エンベロープ送信者には置き換えられません)。
\$Subject	元のメッセージの件名に置き換えられます。
\$Date	現在の日付 (MM/DD/YYYY 形式) に置き換えられます。
\$Time	現在の時刻 (ローカル時間帯) に置き換えられます。
\$GMTimestamp	現在の時刻および日付 (GMT) に置き換えられます。電子メールメッセージの Received: 行で見られる形式と同様です。
\$MID	メッセージを識別するために内部的に使用されるメッセージ ID または「MID」に置き換えられます。RFC822「Message-Id」の値とは異なるため注意してください (「Message-Id」を取得するには \$Header を使用します)。
\$Group	メッセージのインジェクト時に、送信者が一致する送信者グループの名前に置き換えられます。送信者グループに名前がない場合は、文字列「>Unknown<」が挿入されます。
\$Reputation	送信者の SenderBase レピュテーション スコアに置き換えられます。レピュテーション スコアがない場合は「None」に置き換えられます。
\$filenames	メッセージの添付ファイルのファイル名を示すカンマ区切りリストに置き換えられます。
\$filetypes	メッセージの添付ファイルのファイル タイプを示すカンマ区切りリストに置き換えられます。
\$filesizes	メッセージの添付ファイルのファイル サイズを示すカンマ区切りリストに置き換えられます。
\$remotehost	メッセージを Cisco アプライアンスに送信したシステムのホスト名に置き換えられます。
\$AllHeaders	メッセージヘッダーに置き換えられます。

変数	置き換える値
<code>\$EnvelopeFrom</code>	メッセージのエンベロープ送信者 (Envelope From、<MAIL FROM>) に置き換えられます。
<code>\$Hostname</code>	Cisco アプライアンスのホスト名に置き換えられます。
<code>\$bodysize</code>	メッセージのサイズ (バイト単位) に置き換えられます。
<code>\$header['string']</code>	元のメッセージに一致するヘッダーが含まれる場合、引用符付きヘッダーの値に置き換えられます。二重引用符が使用される場合もあります。
<code>\$remoteip</code>	メッセージを Cisco アプライアンスに送信したシステム IP アドレスに置き換えられます。
<code>\$recvlistener</code>	メッセージを受信したリスナーのニックネームに置き換えられます。
<code>\$dropped_filenames</code>	<code>\$filenames</code> と同様に、ドロップされたファイルのリストを表示します。
<code>\$dropped_filename</code>	直近にドロップされたファイル名のみを返します。
<code>\$recvint</code>	メッセージを受信したインターフェイスのニックネームに置き換えられます。
<code>\$timestamp</code>	現在の時刻および日付 (ローカル時間帯) に置き換えられます。電子メール メッセージの Received: 行で見られる形式と同様です。
<code>\$Time</code>	現在の時刻 (ローカル時間帯) に置き換えられます。
<code>\$orgid</code>	SenderBase 組織 ID (整数値) で置き換えられます。
<code>\$envelope recipients</code>	メッセージのエンベロープ受信者すべて (Envelope To、<RCPT TO>) に置き換えられます。
<code>\$dropped_filetypes</code>	<code>\$filetypes</code> と同様に、ドロップされたファイル タイプのリストを表示します。
<code>\$dropped_filetype</code>	直近にドロップされたファイルのファイル タイプのみを返します。

メッセージ トラッキングの機密 DLP データの表示または非表示

RSA Email DLP および RSA Enterprise Manager の両方の導入によって、メッセージ トラッキングに表示できる周辺コンテンツとともに、DLP ポリシーに違反した内容を記録するオプションが提供されます。この内容は、クレジットカード番号や社会保障番号などの機密データを含む場合があります。この内容を記録しないことを選択できます。

はじめる前に

メッセージ トラッキングをイネーブルにします。第 25 章「メッセージ トラッキング」を参照してください。

手順

- ステップ 1** [セキュリティ サービス (Security Services)] > [RSA メール DLP (RSA Email DLP)] を選択します。

ステップ 2 [設定を編集 (Edit Settings)] をクリックします。

目的	操作内容
メッセージトラッキングに重要なコンテンツを含めます。	[一致したコンテンツのログへの記録 (Enable Matched Content Logging)] チェックボックスを選択します。
メッセージトラッキングから機密情報を非表示にします	[一致したコンテンツのログへの記録 (Enable Matched Content Logging)] チェックボックスをオフにします。

ステップ 3 変更内容を送信し、確定します。

次の作業

一致したコンテンツのロギングをイネーブルにした場合は、この情報を表示する管理ユーザを指定します。「[メッセージトラッキングでの機密情報へのアクセスの制御](#)」(P.28-5) を参照してください。

DLP エンジンおよびコンテンツ照合分類子の更新について

RSA DLP エンジンとアプライアンスの定義済みコンテンツ照合分類子の更新は別のセキュリティ サービスの更新に依存しません。

- 「[RSA DLP エンジンの現在のバージョンの決定](#)」(P.15-39)
- 「[DLP 更新に関する警告](#)」(P.15-40)
- 「[DLP エンジンとコンテンツ照合分類子の手動による更新](#)」(P.15-40)
- 「[自動アップデートの有効化 \(推奨されません\)](#)」(P.15-40)
- 「[一元化された \(クラスタ化された\) アプライアンスの DLP 更新](#)」(P.15-41)
- 「[DLP 更新のロールバック](#)」(P.15-41)

RSA DLP エンジンの現在のバージョンの決定

手順

- ステップ 1** [セキュリティ サービス (Security Services)] > [RSA メール DLP (RSA Email DLP)] を選択します。
- ステップ 2** [最新 DLP バージョン ファイル (Current DLP Version Files)] のセクションを参照してください。

DLP 更新に関する警告

導入モード	警告
すべて (All)	シスコは自動更新を有効にすることを推奨しません。「 自動アップデートの有効化 (推奨されません) 」(P.15-40) を参照してください。
RSA メール DLP (RSA Email DLP)	DLP 更新は既存のローカル DLP ポリシーで使用されるコンテンツ照合分類子を変更する場合があります。シスコは、実稼働環境で使用されるアプライアンスを更新する前に、手動で DLP 更新をラボ環境のアプライアンスにダウンロードし、DLP ポリシーをテストすることを推奨します。
RSA Enterprise Manager DLP	ローカル アプライアンスに DLP 更新をダウンロードしても、Enterprise Manager を使用して設定される DLP ポリシーで使うコンテンツ照合分類子は変更されません。しかし、後でアプライアンスを RSA メール DLP を使用するように切り替えると、既存のローカル DLP ポリシーは更新された分類子を使用します。

DLP エンジンとコンテンツ照合分類子の手動による更新

はじめる前に

その場合は、次のトピックを参照してください。

- 「[DLP 更新に関する警告](#)」(P.15-40)
- (該当する場合) 「[一元化された \(クラスタ化された\) アプライアンスの DLP 更新](#)」(P.15-41)

手順

- ステップ 1** [セキュリティ サービス (Security Services)] > [RSA メール DLP (RSA Email DLP)] を選択します。
- ステップ 2** [最新 DLP バージョンファイル (Current DLP Version Files)] セクションで [今すぐ更新 (Update Now)] をクリックします。
- このボタンは、ダウンロード可能な新規アップデートがある場合にだけ使用できます。

自動アップデートの有効化 (推奨されません)

アプライアンスが定期的に更新をチェックし、ダウンロードすることを有効にするには、この手順を使用します。



(注)

シスコは、自動更新を使用しないことを推奨します。これらの更新は、DLP ポリシーで使用されるコンテンツ照合分類子を変更する場合があります。代わりに、手動で DLP 更新をダウンロードし、実稼働環境で使われるアプライアンスを更新する前に、ラボ環境でテストします。

はじめる前に

- [セキュリティ サービス (Security Services)] > [サービスのアップデート (Service Updates)] ページで、自動アップデートをイネーブルにし、すべてのサービス契約更新に更新間隔を指定してください。
- 「一元化された (クラスタ化された) アプライアンスの DLP 更新」 (P.15-41) を参照してください。

手順

-
- ステップ 1** [セキュリティ サービス (Security Services)] > [RSA メール DLP (RSA Email DLP)] を選択します。
 - ステップ 2** [設定を編集 (Edit Settings)] をクリックします。
 - ステップ 3** [自動アップデートを有効にする (Enable automatic updates)] チェックボックスを選択します。
 - ステップ 4** 変更内容を送信し、確定します。
-

一元化された (クラスタ化された) アプライアンスの DLP 更新

次の点に注意してください。

- クラスタ化された導入でのアプライアンスでは、自動 DLP 更新を有効にできません。
- DLP が設定されたレベルで DLP 更新は実行されます。たとえば、DLP がクラスタ レベルで設定されている場合は、DLP 更新もそのレベルで実行する必要があります。
- マシン レベルで `diprollback` CLI コマンドを使用したときのみ、アプライアンスの更新をロールバックできます。
- マシン レベルで `dipstatus` CLI コマンドを使用したときのみ、アプライアンスの DLP エンジンの状態をチェックできます。

DLP 更新のロールバック

この手順は、システムを以前の DLP エンジンとコンテンツ照合分類子を使用する状態に戻します。



(注) DLP 更新のロールバックは、メール ポリシーで使用する DLP ポリシーを無効にします。

はじめる前に

「一元化された (クラスタ化された) アプライアンスの DLP 更新」 (P.15-41) も参照してください。

手順

-
- ステップ 1** CLI では、`diprollback` コマンドを使用します。
 - ステップ 2** メール ポリシーで使用されている DLP ポリシーを再度有効にします。
-

DLP インシデントのメッセージとデータの使用



(注)

Enterprise Manager のマニュアルや、Cisco コンテンツ セキュリティ管理アプライアンス も、環境に応じて参照してください。

目的	操作内容
DLP ポリシー名、違反の重大度、行われるアクションなどの基準を使って DLP 違反が含まれるメッセージを検索し、検出されたメッセージの詳細情報を表示します。	<p>第 25 章「メッセージトラッキング」を参照してください。</p> <p>Enterprise Manager を導入している場合、メッセージは Enterprise Manager にも表示できます。Enterprise Manager のマニュアルを参照してください。</p>
疑わしい DLP 違反として隔離されたメッセージを表示または管理できます。	<p>「ポリシー、ウイルス、またはアウトブレイク隔離のメッセージの操作」(P.27-11)を参照してください。</p> <p>Enterprise Manager を導入している場合、隔離されたメッセージは Enterprise Manager または電子メールセキュリティアプライアンスに表示できますが、隔離されたメッセージを解放または削除するためには Enterprise Manager を使用する必要があります。</p>
DLP インシデントのサマリーを表示します。	DLP インシデント サマリーのレポートについては、第 26 章「電子メールセキュリティ モニタの使用法」を参照してください。
発信メールで検出された DLP 違反に関する情報を表示します。	<p>DLP インシデント レポートについては、第 26 章「電子メールセキュリティ モニタの使用法」を参照してください。</p> <p>Enterprise Manager を導入している場合、Enterprise Manager のマニュアルを参照してください。</p>
疑わしい違反を含む DLP インシデント データとメッセージを表示するには Enterprise Manager を使用します。	Enterprise Manager のマニュアルを参照してください。

関連項目

- 「メッセージトラッキングの機密 DLP データの表示または非表示」(P.15-38)
- 「メッセージトラッキングでの機密情報へのアクセスの制御」(P.28-5)

トラブルシューティング データ消失防止

Enterprise Manager は電子メール セキュリティ アプライアンスとの接続を解除します。

問題 Enterprise Manager は 電子メール セキュリティ アプライアンス との接続を解除します。

ソリューション 正しい証明書が電子メール セキュリティ アプライアンスに正常にインストールされていません。「[電子メール セキュリティ アプライアンスと Enterprise Manager 間の SSL 接続用の証明書の取得とアップロード \(推奨\)](#)」(P.15-26) を参照してください。

クラスタまたはグループ配置がある場合は、アプライアンスの [ネットワーク (Network)] > [証明書 (Certificates)] ページを参照し、証明書がすべてについて同じであることを確認してください。

関連項目

- 「[電子メール セキュリティ アプライアンスと Enterprise Manager 間の接続の切断](#)」(P.15-33)



CHAPTER 16

Cisco Email Encryption

- 「Cisco Email Encryption の概要」 (P.16-1)
- 「電子メールセキュリティ アプライアンスを使用したメッセージの暗号化」 (P.16-3)
- 「暗号化するメッセージの決定」 (P.16-7)
- 「メッセージへの暗号化ヘッダーの追加」 (P.16-11)

Cisco Email Encryption の概要

Cisco AsyncOS は暗号化を使用して着信と発信メールをサポートします。この機能を使用するには、暗号化されたメッセージの特性およびキー（鍵）サーバの接続性の情報を指定する暗号化プロファイルを作成します。キー サーバは、次のいずれかであると考えられます。

- Cisco Registered Envelope Service (マネージド サービス)、または
- Cisco 暗号化アプライアンス (ローカルの管理対象サーバ)

次に、暗号化するメッセージを作成するために、コンテンツ フィルタ、メッセージ フィルタ、データ消失防止ポリシーを作成します。

1. フィルタ条件に合致する発信メッセージは、電子メールセキュリティ アプライアンスの暗号化処理のキューに入れられます。
2. メッセージが暗号化されると、暗号化に使われたキーが暗号化プロファイルで指定されたキーサーバに保存され、暗号化されたメッセージが配信のキューに入れられます。
3. キューの中の電子メールの暗号化を妨げるような条件（つまり、一時的な C-Series のビジー状態や CRES が使用できない状態）が一時的に存在すると、メッセージはキューに入れられ、しばらくしてから再度暗号化が試行されます。



(注)

また、メッセージを暗号化する前に、まず TLS 接続経由で送信を試みるようにアプライアンスを設定することもできます。詳細については、「TLS 接続を暗号化の代わりに使用」 (P.16-8) を参照してください。

サポート対象の Web ブラウザ

- Microsoft® Internet Explorer 7 (Windows XP および Vista)
- Microsoft® Internet Explorer 8 (Windows XP および Vista)

ローカル キー サーバで暗号化する方法

- Firefox 3.0 および 3.5
- Safari 4.0 (Mac OS X)

ローカル キー サーバで暗号化する方法

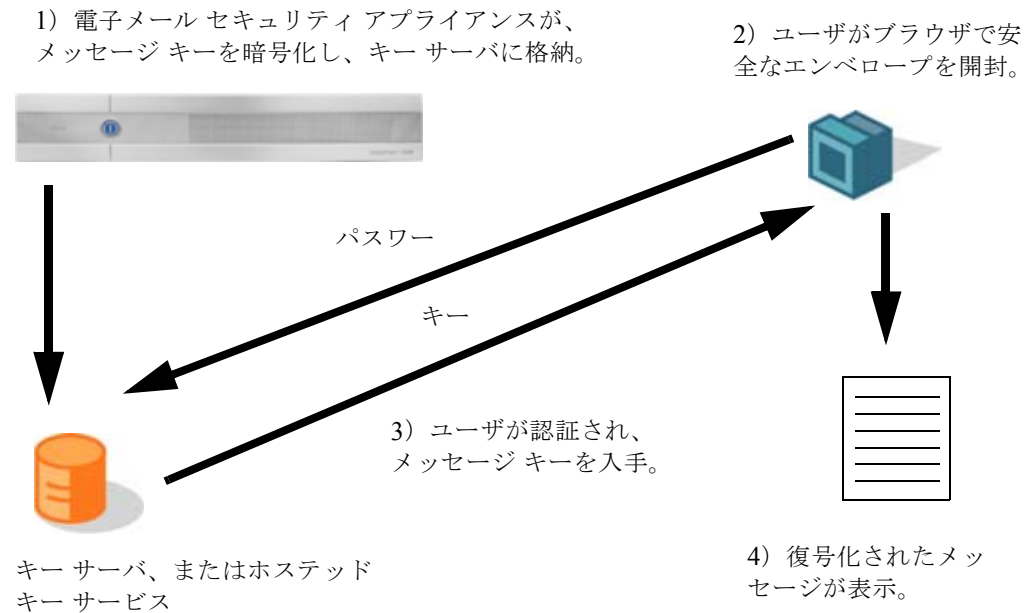
表 16-1 ローカル キー サーバで暗号化する方法

手順	操作内容	詳細
ステップ 1	ネットワークの Cisco IronPort 暗号化アプライアンスを設定します。	第 3 章「セットアップおよび設置」を参照してください。
ステップ 2	メッセージ暗号化をイネーブルにします。	「電子メールセキュリティ アプライアンスでのメッセージの暗号化のイネーブル化」(P.16-4)。
ステップ 3	暗号化プロファイルを作成して、暗号化されたメッセージにセキュリティ設定を使用するための暗号キー サーバを指定します。	「キー サービスによる暗号化メッセージの処理方法の設定」(P.16-4)。
ステップ 4	アプライアンスが暗号化できるように、メッセージが満たす必要のある条件を定義します。	「暗号化するメッセージの決定」(P.16-7)。
ステップ 5	電子メールのワークフローにおいてメッセージを暗号化するタイミングを決定します。	<ul style="list-style-type: none"> • 「コンテンツ フィルタを使用したメッセージの暗号化と即時配信」(P.16-8)。 または <ul style="list-style-type: none"> • 「コンテンツ フィルタを使用した配信時のメッセージの暗号化」(P.16-9)。
ステップ 6	(任意) メッセージに追加セキュリティのフラグを付けます。	「メッセージへの暗号化ヘッダーの追加」(P.16-11)。
ステップ 7	メッセージを暗号化するユーザ グループを定義します。	メール ポリシーを作成します。 第 10 章「メール ポリシー」を参照してください。
ステップ 8	定義したユーザ グループに定義済みの暗号化アクションを関連付けます。	メール ポリシーにコンテンツ フィルタを関連付けます。 第 10 章「メール ポリシー」を参照してください。

暗号化ワークフロー

電子メール暗号化を使用する場合、Cisco 電子メール セキュリティ アプライアンスはメッセージを暗号化し、ローカル キー サーバまたはホステッド キー サービスにメッセージ キーを格納します。受信者が暗号化されたメッセージを開封すると、キー サービスによって受信者が認証され、復号化されたメッセージが表示されます。

図 16-1 暗号化ワークフロー



暗号化されたメッセージを開封する基本的なワークフローは次のとおりです。

1. 暗号化プロファイルを設定するときは、メッセージ暗号化のパラメータを指定します。暗号化されたメッセージでは、メッセージ キーが電子メール セキュリティ アプライアンスによりローカル キー サーバ、またはホステッド キー サービス (Cisco Registered Envelope Service) に作成および格納されます。
2. 受信者はブラウザで安全なエンベロープを開封します。
3. ブラウザで暗号化されたメッセージを開封するとき、受信者の本人確認のためパスワードが必要となります。キー サーバはメッセージに関連付けられた暗号化キーを返します。



(注) 暗号化された電子メール メッセージの初回開封時に、受信者は安全なエンベロープを開封するためのキー サービスに登録する必要があります。登録後、暗号化プロファイルの設定によっては、受信者が暗号化されたメッセージを認証なしで開封することも可能です。暗号化プロファイルでは、パスワード不要と指定できますが、特定の機能が使用できなくなります。

4. 復号化したメッセージが表示されます。

電子メール セキュリティ アプライアンスを使用したメッセージの暗号化

電子メール セキュリティ アプライアンスによる暗号化を使用するには、暗号化プロファイルを設定する必要があります。encryptionconfig CLI コマンド、または GUI の [セキュリティ サービス (Security Services)] > [IronPort メール暗号化 (IronPort Email Encryption)] で、暗号化プロファイルをイネーブルにして設定することができます。

電子メール セキュリティ アプライアンスでのメッセージの暗号化のイネーブル化

手順

-
- ステップ 1** [セキュリティ サービス (Security Services)] > [IronPort 電子メール暗号化 (IronPort Email Encryption)] をクリックします。
- ステップ 2** [有効 (Enable)] をクリックします。
- ステップ 3** (任意) 次のオプションを設定するには、[設定の編集 (Edit Settings)] をクリックしてください:
- 暗号化する最大メッセージ サイズ。シスコが推奨するメッセージ サイズは 10 MB です。アプライアンスが暗号化するメッセージの最大サイズは 25 MB です。
-
-  **(注)** 推奨される 10 MB の制限を超えてメッセージを暗号化すると、アプライアンスのパフォーマンスが遅くなる可能性があります。
- Cisco Registered Envelope サービスを使用する場合、メッセージ受信者は 10 MB より大きい添付ファイルのある暗号化メッセージへは返信できません。
-
- プロキシ サーバを設定します。
-

キー サービスによる暗号化メッセージの処理方法の設定

キー サービスを使用する場合、1 つ以上の暗号化プロファイルを作成できます。さまざまな電子メールグループに異なるセキュリティ レベルを使用する場合、それぞれ別の暗号化プロファイルを作成することもできます。たとえば、機密資料を含んだメッセージを高レベルのセキュリティで送信し、他のメッセージを中レベルのセキュリティで送信するという場合です。この場合、特定のキーワード（「confidential」など）を含むメッセージには高レベルのセキュリティ暗号化プロファイルを作成し、他の発信メッセージには別の暗号化プロファイルを作成します。

暗号化プロファイルをカスタム ユーザ ロールに割り当て、そのロールに割り当てられた委任管理者が DLP ポリシーとコンテンツ フィルタで暗号化プロファイルを使用できるようにします。DLP ポリシーとコンテンツ フィルタを設定する場合は、管理者、オペレータ、および委任ユーザだけが暗号化プロファイルを使用できます。カスタム ロールに割り当てられない暗号化プロファイルは、メールまたは DLP ポリシー権限を持つすべての委任管理者が使用できます。詳細については、「[管理タスクの分散](#)」を参照してください。



(注)

1 つのホステッド キー サービスに複数の暗号化プロファイルを設定できます。組織に複数のブランドがある場合、PXE エンベロープ用にキー サーバに格納された異なるロゴを参照することができます。

暗号化プロファイルは次の設定を保存します。

- [キー サーバ設定 (Key server settings)]。キー サーバとそのキー サーバに接続するための情報を指定します。
- [エンベロープ設定 (Envelope settings)]。セキュリティ レベル、開封確認を返すか、暗号化キューにあるメッセージがタイムアウトするまでの時間、使用する暗号化アルゴリズムのタイプ、および復号化アプレットをブラウザで動作可能にするかなど、メッセージ エンベロープの詳細を指定します。

- [メッセージ設定 (Message settings)]。安全なメッセージ転送や安全な「全員に返信」をイネーブルにするかなど、メッセージに関する詳細を指定します。
- [通知設定 (Notification settings)]。暗号化失敗通知と同様、テキスト形式および HTML 形式の通知を使う通知テンプレートを指定します。暗号化プロファイル作成時に、テキストリソース内のテンプレートを作成し、テンプレートを選択します。暗号化失敗通知のメッセージの件名も指定できます。通知の詳細については、「暗号化通知テンプレート」(P.18-23) および「バウンス通知および暗号化失敗通知テンプレート」(P.18-22) を参照してください。

手順

- ステップ 1** [メール暗号化プロファイル (Email Encryption Profiles)] のセクションで [暗号化プロファイルの追加 (Add Encryption Profile)] をクリックします。
- ステップ 2** 暗号化プロファイルの名前を入力します。
- ステップ 3** [使用者 (ロール) (Used By (Roles))] リンクをクリックし、暗号化プロファイルへのアクセス権を設定するカスタム ユーザ ロールを選択して、[OK] をクリックします。
- このカスタム ロールに割り当てられた委任管理者は、責任があるすべての DLP ポリシーとコンテンツ フィルタに対して暗号化プロファイルを使用できます。
- ステップ 4** [キー サーバ設定 (Key Server Settings)] セクションで次のキー サーバから選択します。
- Cisco Encryption アプライアンス (ネットワーク内)
 - Cisco Registered Envelope Service (ホステッド キー サービス)
- ステップ 5** Cisco 暗号化アプライアンス (ローカル キー サービス) を選択した場合は、次の設定を入力します。
- [内部 URL (Internal URL)]。Cisco 電子メール セキュリティ アプライアンスは、この URL を使用してネットワーク内の Cisco 暗号化アプライアンスと通信します。
 - [外部 URL (External URL)]。受信者のメッセージは、この URL を使用して Cisco 暗号化アプライアンスのキーおよび他のサービスにアクセスします。受信者は、受信 HTTP または HTTPS 要求をするためにこの URL を使用します。
- ステップ 6** Cisco Registered Envelope サービスを選択した場合は、ホステッド キー サービスの URL を入力します。キー サービスの URL は、`https://res.cisco.com` です。
- ステップ 7** [キー サーバ設定 (Key Server Settings)] で [詳細 (Advanced)] をクリックし、受信者がエンベロープを開封した場合、エンベロープの暗号化ペイロードの転送に HTTP または HTTPS を使用するかどうかを指定します。次のいずれかを選択してください。
- **キー サービスを HTTP で使用する (Use the Key Service with HTTP)** 受信者がエンベロープを開封した場合、HTTP を使用してキー サービスから暗号化ペイロードを転送します。Cisco Registered Envelope サービスを使用する場合は、**ステップ 6** で指定した URL です。暗号化 Cisco アプライアンスを使用する場合は、**ステップ 5** で指定した外部 URL です。
- ペイロードがすでに暗号化されているため、HTTP に転送しても安全であり、HTTPS に送信するよりも迅速です。これは、HTTPS 経由でイメージ要求を送信するよりも、パフォーマンスがさらに向上します。
- **HTTPS でキー サービスを使用する (Use the Key Service with HTTPS)** 受信者がエンベロープを開封すると、HTTPS を使用してキー サービスから暗号化ペイロードを転送します。Cisco Registered Envelope サービスを使用する場合は、**ステップ 6** で指定した URL です。暗号化 Cisco アプライアンスを使用する場合は、**ステップ 5** で指定した外部 URL です。
 - **ペイロード トランスポートの個別の URL を指定します。** (Specify a separate URL for payload transport.) 暗号化ペイロードにキー サーバを使用しない場合は、ペイロード転送には HTTP または HTTPS を使用するかどうかを別の URL を使用して指定できます。

- ステップ 8** [エンベロープ設定 (Envelope Settings)] のセクションで、メッセージのセキュリティ レベルを選択します。
- [高レベルセキュリティ (High Security)]。受信者は、暗号化されたメッセージを開封するには、パスワードを必ず入力する必要があります。
 - [中レベルセキュリティ (Medium Security)]。受信者の資格情報がキャッシュされていれば、受信者は暗号化されたメッセージを開封するために資格情報を入力する必要はありません。
 - [パスワードは不要です (No Password Required)]。暗号化されたメッセージの最も低いセキュリティ レベルです。暗号化されたメッセージを開封するために受信者がパスワードを入力する必要はありません。それでも、パスワード保護されないエンベロープの [開封確認 (Read Receipts)]、[全員への安全な返信 (Secure Reply All)]、および [メッセージの安全な転送 (Secure Message Forwarding)] 機能をイネーブルにできます。
- ステップ 9** ユーザが組織のロゴをクリックするとその組織の URL が開くようにするよう、ロゴのリンクを追加できます。次のオプションから選択します。
- [リンクなし (No link)]。実際のリンクは、メッセージ エンベロープに追加されません。
 - [カスタム リンク URL (Custom link URL)]。URL を入力し、メッセージ エンベロープへの実際のリンクを追加します。
- ステップ 10** 任意で、開封確認をイネーブルにします。このオプションをイネーブルにすると、受信者が安全なエンベロープを開くと、送信者は開封確認を受信します。
- ステップ 11** 次の設定を行うために、任意で [エンベロープ設定 (Envelope Settings)] の [詳細設定 (Advanced)] をクリックしてください。
- 暗号化キューにあるメッセージがタイムアウトするまでの時間 (秒単位) を入力します。メッセージがタイムアウトになると、アプライアンスはメッセージをバウンスし、送信者に通知を送信します。
 - 暗号化アルゴリズムを選択します。
 - [ARC4]。ARC4 は最もよく選択されるアルゴリズムで、メッセージ受信者に対する復号化遅延を最小限にとどめながら強力な暗号化を実現します。
 - [AES]。AES は、より強力な暗号化を実現しますが、復号化により長い時間がかかるため、受信者には遅延が発生します。AES は、通常、政府や銀行業務のアプリケーションで使用されます。
 - 復号化アプレットをイネーブルまたはディセーブルにします。このオプションをイネーブルにすると、メッセージの添付ファイルがブラウザ環境で開かれるようになります。このオプションをディセーブルにすると、メッセージの添付ファイルがキー サーバで復号化されるようになります。ディセーブルの場合、メッセージの開封により時間がかかるようになりますが、ブラウザ環境に依存しなくなります。
- ステップ 12** [メッセージ設定 (Message Settings)] セクションで、[全員にセキュアな返信 (Secure Reply All)] をイネーブルまたはディセーブルにします。
- ステップ 13** [セキュアなメッセージ転送 (Secure Message Forwarding)] をイネーブルまたはディセーブルにします。
- ステップ 14** HTML 形式の通知テンプレートを選択します。テキスト リソースで設定した HTML 形式の通知から選択します。テンプレートが設定されていなかった場合、システムはデフォルトのテンプレートを使用します。



(注) キー サーバは、受信者の電子メール アプリケーションによって、HTML またはテキスト形式の通知を使います。両方の通知を設定する必要があります。

- ステップ 15** テキスト形式の通知テンプレートを選択します。テキスト リソースで設定したテキスト形式の通知から選択します。テンプレートが設定されていなかった場合、システムはデフォルトのテンプレートを使用します。
- ステップ 16** 暗号化失敗通知用の件名ヘッダーを入力します。暗号化プロセスがタイムアウトした場合、アプライアンスは通知を送信します。
- ステップ 17** メッセージ本文の暗号化失敗通知テンプレートを選択します。テキスト リソースで設定した暗号化失敗通知テンプレートから選択します。テンプレートが設定されていなかった場合、システムはデフォルトのテンプレートを使用します。
- ステップ 18** 変更内容を送信し、確定します。
- ステップ 19** Cisco Registered Envelope Service を使用する場合、アプライアンスをプロビジョニングする手順を追加で実行する必要があります。アプライアンスをプロビジョニングすると、暗号化プロファイルがホステッドキー サービスとともに登録されます。アプライアンスをプロビジョニングするには、登録する暗号化プロファイルの [登録 (Provision)] ボタンをクリックします。

PXE エンジンの最新バージョンへの更新

[シスコ電子メール暗号化設定 (Cisco Email Encryption Settings)] ページには、PXE エンジンの現在のバージョンおよびアプライアンスで使用するドメイン マッピング ファイルが表示されます。[セキュリティ サービス (Security Services)] > [サービス アップデート (Service Updates)] ページ (または CLI の `updateconfig` コマンド) を使って、自動的に PXE エンジンを更新するように Cisco アプライアンスを設定できます。詳細については、「サービスのアップデート」(P.29-22) を参照してください。

また、[IronPort メール暗号化設定 (IronPort Email Encryption Settings)] ページの [PXE エンジンの更新 (PXE Engine Updates)] セクションの [今すぐ更新 (Update Now)] ボタン (または CLI の `encryptionupdate` コマンド) を使って、手動でエンジンを更新することもできます。

暗号化するメッセージの決定

暗号化プロファイルの作成後、どの電子メール メッセージを暗号化すべきかを定める発信コンテンツ フィルタを作成する必要があります。コンテンツ フィルタは、発信電子メールをスキャンしてメッセージが指定された条件に一致するか判断します。コンテンツ フィルタによりメッセージが条件に一致すると判断されたら、Cisco 電子メール セキュリティ アプライアンスはメッセージを暗号化し、生成されたキーをキー サーバに送信します。このアプライアンスは、使用するキー サーバを決定するための、暗号化プロファイルで指定された設定と、他の暗号化設定を使用します。

データ消失防止スキャン後に解放された後でも、メッセージを暗号化できます。詳細については、「DLP 違反アクション (メッセージ アクション) に対して実行するアクションの定義」(P.15-34) を参照してください。

TLS 接続を暗号化の代わりに使用

ドメイン用に指定された送信先コントロールに基づき、Cisco アプライアンスは、メッセージを暗号化する代わりに TLS 接続を介してメッセージをセキュアに中継できます (TLS 接続が使用可能な場合)。アプライアンスは、送信先コントロール (Required、Preferred、または None) の TLS 設定と暗号化コンテンツ フィルタで定義されたアクションに基づいて、メッセージを暗号化するか TLS 接続で送信するか決定します。

コンテンツ フィルタ作成時に、必ずメッセージを暗号化するか、まず TLS 接続で送信を試みて、TLS 接続が使用不可であればメッセージを暗号化するかを指定できます。表 16-2 では、暗号化制御フィルタが TLS 接続でのメッセージの送信を試みる場合、電子メールセキュリティ アプライアンスが、ドメインの送信先コントロールの TLS 設定に基づいてどのようにメッセージを送信するかを示しています。

表 16-2 ESA アプライアンスの TLS サポート

送信先コントロール TLS 設定	TLS 接続が使用可能である場合のアクション	TLS 接続が使用不可である場合のアクション
なし (None)	エンベロープを暗号化して送信します。	エンベロープを暗号化して送信します。
TLS 推奨 (TLS Preferred)	TLS を通して送信します。	エンベロープを暗号化して送信します。
TLS 必須 (TLS Required)	TLS を通して送信します。	リトライまたはメッセージのバウンス

送信先コントロールで TLS をイネーブルにする方法については、「[電子メールを受信するためのゲートウェイの設定](#)」を参照してください。

コンテンツ フィルタを使用したメッセージの暗号化と即時配信

はじめる前に

- コンテンツ フィルタを構築するための条件の概念を理解するには、「[コンテンツ フィルタの概要](#)」(P.11-1) を参照してください。
- (任意) 「[メッセージへの暗号化ヘッダーの追加](#)」(P.16-11) を参照してください。

手順

- ステップ 1** [メール ポリシー (Mail Policies)] > [発信コンテンツ フィルタ (Outgoing Content Filters)] に移動します。
- ステップ 2** [フィルタ (Filters)] セクションで、[フィルタを追加 (Add Filter)] をクリックします。
- ステップ 3** [条件 (Conditions)] セクションで、[条件を追加 (Add Condition)] をクリックします。
- ステップ 4** 暗号化するメッセージをフィルタリングする条件を追加します。たとえば、機密資料を暗号化するために、件名または本文に特定の単語またはフレーズ («Confidential» など) を含むメッセージを識別する条件を追加できます。
- ステップ 5** [OK] をクリックします。
- ステップ 6** 任意で、[アクションを追加 (Add Action)] をクリックし、[ヘッダーの追加 (Add Header)] を選択し、追加の暗号化設定を指定する暗号化ヘッダーをメッセージに挿入します。
- ステップ 7** [アクション (Actions)] セクションで、[アクションを追加 (Add Action)] をクリックします。

- ステップ 8** [アクションを追加 (Add Action)] リストから [すぐに暗号化して配信 (最終アクション) (Encrypt and Deliver Now (Final Action))] を選択します。
- ステップ 9** 条件に合致するメッセージを常に暗号化するか、TLS 接続を介した送信の試行が失敗したときのみメッセージを暗号化するかを選択します。
- ステップ 10** コンテンツ フィルタに関連付ける暗号化プロファイルを選択します。
- 暗号化プロファイルは、使用するキー サーバ、セキュリティ レベル、およびメッセージ エンベロープのフォーマット化に関する設定、および他のメッセージ設定を指定します。暗号化プロファイルをコンテンツ フィルタに関連付けた場合、コンテンツ フィルタはこれらの格納された設定を暗号化メッセージに使用します。
- ステップ 11** メッセージの件名を入力します。
- ステップ 12** [OK] をクリックします。

図 16-2 のコンテンツ フィルタは、メッセージ本文で ABA コンテンツを検索するコンテンツ フィルタを示します。コンテンツ フィルタで定義されているアクションは、電子メールを暗号化して配信すると指定しています。

図 16-2 暗号化コンテンツ フィルタ

Content Filter Settings			
Name:	sensitive_content		
Currently Used by Policies:	No policies currently use this rule.		
Description:	encrypt messages that contain sensitive material		
Order:	2 (of 2)		

Conditions			
Order	Condition	Rule	Delete
1	Message Body	only-body-contains(*aba*, 1)	

Actions			
Order	Action	Rule	Delete
1	Encrypt and Deliver (Final Action)	encrypt ("encrypt_sensitive", "\${Subject}")	

- ステップ 13** 暗号化アクションを追加した後、[送信 (Submit)] をクリックします。
- ステップ 14** 変更内容を確定します。

次の作業

コンテンツ フィルタを追加したら、フィルタを発信メール ポリシーに追加する必要があります。組織のニーズに応じて、デフォルト ポリシーでコンテンツ フィルタをイネーブルにする、またはフィルタを特定のメール ポリシーに適用することを選択します。メール ポリシーの操作については、「[メールポリシーの概要](#)」(P.10-1) を参照してください。

コンテンツ フィルタを使用した配信時のメッセージの暗号化

配信時にメッセージを暗号化するコンテンツ フィルタを作成するには、次の手順に従ってください。配信時の暗号化とは、メッセージが次の処理の段階に進み、すべての処理が完了した時点で、メッセージが暗号化され、配信されることを意味します。

はじめる前に

- コンテンツ フィルタを構築するための条件の概念を理解するには、「[コンテンツ フィルタの概要](#)」(P.11-1) を参照してください。
- (任意) 「[メッセージへの暗号化ヘッダーの追加](#)」(P.16-11) を参照してください。

手順

-
- ステップ 1** [メール ポリシー (Mail Policies)] > [発信コンテンツ フィルタ (Outgoing Content Filters)] に移動します。
 - ステップ 2** [フィルタ (Filters)] セクションで、[フィルタを追加 (Add Filter)] をクリックします。
 - ステップ 3** [条件 (Conditions)] セクションで、[条件を追加 (Add Condition)] をクリックします。
 - ステップ 4** 暗号化するメッセージをフィルタリングする条件を追加します。たとえば、機密資料を暗号化するために、件名または本文に特定の単語またはフレーズ (「Confidential」など) を含むメッセージを識別する条件を追加できます。
 - ステップ 5** [OK] をクリックします。
 - ステップ 6** 任意で、[アクションを追加 (Add Action)] をクリックし、[ヘッダーの追加 (Add Header)] を選択し、追加の暗号化設定を指定する暗号化ヘッダーをメッセージに挿入します。
 - ステップ 7** [アクション (Actions)] セクションで、[アクションを追加 (Add Action)] をクリックします。
 - ステップ 8** [アクションを追加 (Add Action)] リストから [配信時の暗号化 (Encrypt on Delivery)] を選択します。
 - ステップ 9** 条件に合致するメッセージを常に暗号化するか、TLS 接続を介した送信の試行が失敗したときのみメッセージを暗号化するかを選択します。
 - ステップ 10** コンテンツ フィルタに関連付ける暗号化プロファイルを選択します。
暗号化プロファイルは、使用するキー サーバ、セキュリティ レベル、およびメッセージ エンベロープのフォーマット化に関する設定、および他のメッセージ設定を指定します。暗号化プロファイルをコンテンツ フィルタに関連付けた場合、コンテンツ フィルタはこれらの格納された設定を暗号化メッセージに使用します。
 - ステップ 11** メッセージの件名を入力します。
 - ステップ 12** [OK] をクリックします。
 - ステップ 13** 暗号化アクションを追加した後、[送信 (Submit)] をクリックします。
 - ステップ 14** 変更内容を確定します。
-

次の作業

コンテンツ フィルタを追加したら、フィルタを発信メール ポリシーに追加する必要があります。組織のニーズに応じて、デフォルト ポリシーでコンテンツ フィルタをイネーブルにする、またはフィルタを特定のメール ポリシーに適用することを選択します。メール ポリシーの操作については、「[メール ポリシーの概要](#)」(P.10-1) を参照してください。

メッセージへの暗号化ヘッダーの追加

AsyncOS では、コンテンツ フィルタまたはメッセージ フィルタを使って SMTP ヘッダーをメッセージに挿入することで、暗号化設定をメッセージに追加できます。暗号化ヘッダーは、関連付けられた暗号化プロファイルで定義されている暗号化設定を上書きすることが可能で、指定された暗号化機能をメッセージに適用できます。



(注) Cisco 暗号化アプライアンスはフラグ付きのメッセージを処理するように設定する必要があります。

手順

- ステップ 1** [メール ポリシー (Mail Policies)] > [発信コンテンツ フィルタ (Outgoing Content Filters)] または [受信コンテンツ フィルタ (Incoming Content Filters)] フィルタに進みます。
- ステップ 2** [フィルタ (Filters)] セクションで、[フィルタを追加 (Add Filter)] をクリックします。
- ステップ 3** [アクション (Actions)] セクションで、[アクションを追加 (Add Action)] をクリックして [追加/編集 (Add/Edit)] ヘッダーを選択し、追加の暗号化設定を指定するためにメッセージに暗号化ヘッダーを挿入します。

たとえば、Registered Envelope を送信後 24 時間で期限切れにする場合は、ヘッダー名として X-PostX-ExpirationDate、ヘッダーの値として +24:00:00 を入力します。

関連項目

- 暗号化コンテンツ フィルタの作成の詳細については、「[コンテンツ フィルタを使用したメッセージの暗号化と即時配信](#)」(P.16-8) を参照してください。
- メッセージ フィルタを使用したヘッダー挿入については、「[メッセージ フィルタを使用した電子メール ポリシーの適用](#)」を参照してください。

暗号化ヘッダー

表 16-3 に、メッセージに追加可能な暗号化ヘッダーを示します。

表 16-3 電子メール暗号化ヘッダー

MIME ヘッダー	説明	値
X-PostX-Reply-Enabled	メッセージで安全な返信をイネーブルにするかを示し、メッセージ バーに [返信 (Reply)] ボタンを表示します。このヘッダーは、メッセージに暗号化設定を追加します。	[返信 (Reply)] ボタンを表示または非表示にするかを示すブール値。true に設定するとボタンを表示します。デフォルト値は false です。
X-PostX-Reply-All-Enabled	メッセージで安全な「全員に返信」をイネーブルにするかを示し、メッセージ バーに [全員に返信 (Reply All)] ボタンを表示します。このヘッダーは、デフォルトのプロファイル設定を上書きします。	[全員に返信 (Reply All)] ボタンを表示または非表示にするかを示すブール値。true に設定するとボタンを表示します。デフォルト値は false です。

表 16-3 電子メール暗号化ヘッダー（続き）

MIME ヘッダー	説明	値
X-PostX-Forward-Enabled	メッセージの安全な転送をイネーブルにするかを示し、メッセージバーに [転送 (Forward)] ボタンを表示します。このヘッダーは、デフォルトのプロファイル設定を上書きします。	[転送 (Forward)] ボタンを表示または非表示にするかを示すブール値。true に設定するとボタンを表示します。デフォルト値は false です。
X-PostX-Send-Return-Receipt	開封確認をイネーブルにするかを示します。受信者が安全なエンベロープを開くと、送信者は開封確認を受信します。このヘッダーは、デフォルトのプロファイル設定を上書きします。	開封確認を送信するかを示すブール値。true に設定するとボタンを表示します。デフォルト値は false です。
X-PostX-ExpirationDate	送信前に Registered Envelope の有効期限の日付を設定します。有効期限後は、キー サーバにより Registered Envelope へのアクセスが制限されます。 Registered Envelope は、メッセージの期限が切れたというメッセージを表示します。このヘッダーは、メッセージに暗号化設定を追加します。 Cisco Registered Envelope Service を使用している場合、メッセージ送信後に http://res.cisco.com の Web サイトにログインして、メッセージ管理機能でメッセージの有効期限を設定、調整、削除できます。	相対的な日付や時間を含む文字列値。相対的な時間、分、秒には +HH:MM:SS 形式、相対的な日付には +D 形式を使います。デフォルトでは、有効期限はありません。
X-PostX-ReadNotificationDate	送信前に Registered Envelope の「開封期限」の日付を設定します。Registered Envelope がこの期限までに読まれなかった場合、ローカル キー サーバは通知を生成します。このヘッダーを持つ Registered Envelope は、Cisco Registered Envelope Service では機能せず、ローカル キー サーバでのみ機能します。このヘッダーは、メッセージに暗号化設定を追加します。	相対的な日付や時間を含む文字列値。相対的な時間、分、秒には +HH:MM:SS 形式、相対的な日付には +D 形式を使います。デフォルトでは、有効期限はありません。
X-PostX-Suppress-Applet-For-Open	復号化アプレットをディセーブルにするかを示します。復号化アプレットにより、ブラウザ環境でメッセージの添付ファイルが開かれます。アプレットをディセーブルにすると、メッセージの添付ファイルはキー サーバで復号化されます。このオプションをディセーブルにすると、メッセージの開封により時間がかかるようになりますが、ブラウザ環境に依存しなくなります。このヘッダーは、デフォルトのプロファイル設定を上書きします。	復号化アプレットをディセーブルにするかを示すブール値。アプレットをディセーブルにするには true に設定します。デフォルト値は false です。

表 16-3 電子メール暗号化ヘッダー (続き)

MIME ヘッダー	説明	値
X-PostX-Use-Script	JavaScript を含まないエンベロープを送信するかしないかを示します。JavaScript を含まないエンベロープとは、受信者のコンピュータ上でエンベロープをローカルに開封するために使われる JavaScript を含まない Registered Envelope のことです。受信者は、メッセージを見るには Open Online メソッド、または Open by Forwarding メソッドのいずれかを使用する必要があります。受信者のドメインのゲートウェイにより JavaScript が削除され、暗号化されたメッセージを開封できない場合、このヘッダーを使います。このヘッダーはメッセージに暗号化設定を追加します。	JavaScript アプレットを含めるか含めないかのブール値。JavaScript を含まないエンベロープを送信するには、false に設定します。デフォルト値は true です。
X-PostX-Remember-Envelope-Key-Checkbox	オフラインでエンベロープを開封するため、エンベロープ固有のキーのキャッシングを許可するかしないかを示します。エンベロープ キーのキャッシングでは、受信者が正しいパスワードを入力し、[このエンベロープのパスワードを記憶する (Remember the password for this envelope)] チェックボックスをオンにした場合、個別のエンベロープの復号化キーが受信者のコンピュータでキャッシングされます。これ以降、受信者はそのコンピュータでエンベロープを再開封するためにパスワードをもう一度入力する必要はありません。このヘッダーは、メッセージに暗号化設定を追加します。	エンベロープ キーのキャッシングをイネーブルにするか、[このエンベロープのパスワードを記憶する (Remember the password for this envelope)] チェックボックスを表示するかしないかのブール値。デフォルト値は false です。

暗号化ヘッダーの例

この項では、暗号化ヘッダーの例を示します。

オフラインでの開封のためエンベロープ キーをイネーブルにする

エンベロープ キーのキャッシングをイネーブルにして Registered Envelope を送信するには、次のヘッダーをメッセージに挿入します。

```
X-PostX-Remember-Envelope-Key-Checkbox: true
```

[このエンベロープのパスワードを記憶する (Remember the password for this envelope)] チェックボックスが Registered Envelope に表示されます。

JavaScript を含まないエンベロープをイネーブルにする

JavaScript を含めずに Registered Envelope を送信するには、次のヘッダーをメッセージに挿入します。

```
X-PostX-Use-Script: false
```

受信者が `securedoc.html` 添付ファイルを開くと、Registered Envelope が [オンラインを開く (Open Online)] リンクとともに表示され、[開く (Open)] ボタンがディセーブルになります。

メッセージ有効期限をイネーブルにする

送信後、24 時間で有効期限が切れるようにメッセージを設定するには、次のヘッダーをメッセージに挿入します。

```
X-PostX-ExpirationDate: +24:00:00
```

送信後 24 時間は、受信者はその暗号化されたメッセージを開封して内容を見ることができます。それ以降、Registered Envelope では、エンベロープの有効期限が切れたことを示すメッセージが表示されます。

復号化アプレットをディセーブルにする

復号化アプレットをディセーブルにし、メッセージの添付ファイルをキー サーバで復号するには、次のヘッダーをメッセージに挿入します。

```
X-PostX-Suppress-Applet-For-Open: true
```



(注)

復号化アプレットをディセーブルにしている場合、メッセージの開封には時間がかかりますが、ブラウザ環境には依存しなくなります。



CHAPTER 17

電子メール認証

- 「電子メール認証の概要」 (P.17-1)
- 「DomainKeys と DKIM 認証」 (P.17-1)
- 「DomainKeys および DKIM 署名の設定」 (P.17-3)
- 「DKIM 署名を使用した受信メッセージの確認方法」 (P.17-15)
- 「SPF および SDF 検証の概要」 (P.17-20)
- 「SPF/SDIF を使用して受信メッセージの確認方法」 (P.17-22)
- 「SPF と SDF のイネーブル化」 (P.17-22)
- 「SPF/SDIF 検証済みメールに対して実行するアクションの決定」 (P.17-29)
- 「SPF/SDIF 結果のテスト」 (P.17-32)

電子メール認証の概要

Cisco AsyncOS では、電子メールの偽造を防止するために、電子メール検証と署名をサポートします。着信メールを検証するために、AsyncOS は SPF (Sender Policy Framework)、SDIF (Sender ID Framework)、DKIM (DomainKeys Identified Mail) をサポートしています。送信メールを認証するために、AsyncOS は DomainKeys および DKIM 署名をサポートしています。

関連項目

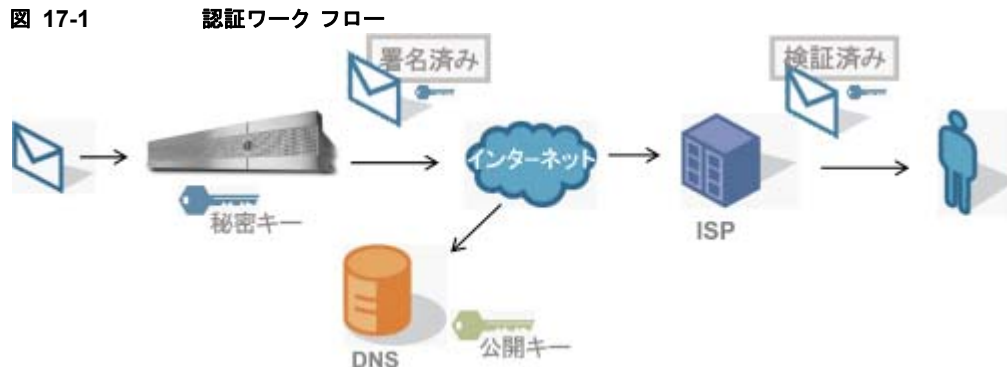
- 「DomainKeys と DKIM 認証」 (P.17-1) .
- 「SPF および SDF 検証の概要」 (P.17-20) .

DomainKeys と DKIM 認証

DomainKeys または DKIM 電子メール認証では、送信側が公開キー暗号化を使用して電子メールに署名します。これにより、検証済みのドメインを使用して、電子メールの From: (または Sender:) ヘッダーのドメインと比較して、偽造を検出できます。

DomainKeys と DKIM は、署名と検証の 2 つの主要部分から構成されます。AsyncOS では、DomainKeys の「署名」部分のプロセスをサポートし、DKIM の署名と検証の両方をサポートします。バウンスおよび遅延メッセージで DomainKeys および DKIM 署名を使用することもできます。

DomainKeys と DKIM 認証ワークフロー



1. 管理者（ドメイン所有者）が公開キーを DNS 名前空間にパブリッシュします。
2. 管理者は発信メール転送エージェント（MTA）に秘密キーをロードします。
3. そのドメインの権限のあるユーザによって送信される電子メールが、各秘密キーによってデジタル署名されます。署名は DomainKey または DKIM 署名ヘッダーとして電子メールに挿入され、電子メールが送信されます。
4. 受信側 MTA は、電子メールのヘッダーから DomainKeys または DKIM 署名と、要求された送信側ドメイン（Sender: または From: ヘッダーによって）を抽出します。DomainKeys または DKIM 署名ヘッダー フィールドから抽出された要求された署名ドメインから、公開キーが取得されます。
5. 公開キーは、DomainKeys または DKIM 署名が適切な秘密キーによって生成されているかどうかを確認するために使われます。

発信 DomainKeys 署名をテストするには、Yahoo! または Gmail アドレスを使用できます。これらのサービスは無料で提供され、DomainKeys 署名されている着信メッセージを検証します。

AsyncOS の DomainKeys および DKIM 署名

AsyncOS の DomainKeys および DKIM 署名は、ドメイン プロファイルによって実装され、メールフロー ポリシー（一般に、発信「リレー」ポリシー）によってイネーブルにされます。詳細については、『Cisco IronPort AsyncOS for Email Configuration Guide』の「Configuring the Gateway to Receive Mail」の章を参照してください。メッセージの署名は、メッセージ送信前にアプライアンスによって実行される最後の操作です。

ドメイン プロファイルはドメインとドメイン キー情報（署名キーと関連情報）を関連付けます。電子メールは、Cisco アプライアンスで、メールフロー ポリシーによって送信され、いずれかのドメイン プロファイルに一致する送信側電子メールアドレスが、ドメイン プロファイルに指定されている署名キーを使用して DomainKeys 署名されます。DKIM と DomainKeys の両方の署名をイネーブルにすると、DKIM 署名が使われます。DomainKeys および DKIM プロファイルは、domainkeysconfig CLI コマンドまたは GUI の [メール ポリシー (Mail Policies)] > [ドメイン プロファイルとメール ポリシー (Domain Profiles and the Mail Policies)] > [署名キー (Signing Keys)] ページから実装します。

DomainKeys および DKIM 署名は次のように機能します。ドメイン所有者はパブリック DNS（そのドメインに関連付けられた DNS TXT レコード）に格納される公開キーと、アプライアンスに格納され、そのドメインから送信されるメール（発信されるメール）の署名に使われる秘密キーの 2 つのキーを生成します。

メッセージがメッセージの送信（発信）に使われるリスナーで受信されると、Cisco アプライアンスは、ドメイン プロファイルが存在するかどうかを調べます。アプライアンスに作成された（およびメールフロー ポリシー用に実装された）ドメイン プロファイルが存在する場合、メッセージの有効な

Sender: または From: アドレスがスキャンされます。どちらも存在する場合、DomainKeys には Sender: が使われます。DKIM 署名には、From: アドレスが常に使われます。それ以外の場合は、最初の From: アドレスが使われます。有効なアドレスが見つからない場合、メッセージは署名されず、イベントが mail_logs に記録されます。



(注)

DomainKey および DKIM プロファイルの両方を作成した（およびメール フロー ポリシーで署名をイネーブルにしている）場合、AsyncOS は DomainKeys と DKIM の両方の署名で送信メッセージを署名します。

有効な送信側アドレスが見つかった場合、送信側アドレスが既存のドメイン プロファイルに対して照合されます。一致しているものが見つかった場合、メッセージは署名されます。見つからない場合、メッセージは署名なしで送信されます。メッセージに既存の DomainKeys（「DomainKey-Signature:」ヘッダー）がある場合、メッセージは、元の署名の後に新しい送信側アドレスが追加されている場合にのみ、署名されます。メッセージに既存の DKIM 署名がある場合、新しい DKIM 署名がメッセージに追加されます。

AsyncOS はドメインに基づいて電子メールに署名するメカニズムに加えて、署名キーを管理する（新しいキーの作成または既存のキーの入力）方法を提供します。

このマニュアルのコンフィギュレーションの説明は、署名と検証の最も一般的な使用方法を示しています。着信メールのメール フロー ポリシーで DomainKeys および DKIM 署名をイネーブルにすることも、発信メールのメール フロー ポリシーで DKIM 検証をイネーブルにすることもできます。



(注)

クラスタ環境にドメイン プロファイルと署名キーを設定する場合、[ドメイン キー プロファイル (Domain Key Profile)] 設定と [署名キー (Signing Key)] 設定がリンクしていることに注意します。そのため、署名キーをコピー、移動、または削除した場合、同じ操作が関連プロファイルに対して行われます。

DomainKeys および DKIM 署名の設定

署名キー

署名キーは Cisco アプライアンスに格納されている秘密キーです。署名キーの作成時に、キー サイズを指定します。キー サイズが大きいほどセキュリティが向上しますが、パフォーマンスに影響する可能性もあります。Cisco アプライアンスでは 512 ~ 2048 ビットのキーをサポートしています。768 ~ 1024 ビットのキー サイズは安全であると見なされ、現在ほとんどの送信側で使われています。大きなキー サイズに基づいたキーはパフォーマンスに影響する可能性があるため、2048 ビットを超えるキーはサポートされていません。署名キーの作成方法については、「[新しい署名キーの作成](#)」(P.17-10) を参照してください。

既存のキーを入力する場合、それをフォームに貼り付けるだけです。既存の署名キーの別の使用方法は、キーをテキスト ファイルとしてインポートすることです。既存の署名キーの追加の詳細については、「[既存の署名キーのインポートまたは入力](#)」(P.17-10) を参照してください。

キーを入力すると、ドメイン プロファイルで使用できるようになり、ドメイン プロファイルの [署名キー (Signing Key)] ドロップダウン リストに表示されます。

署名キーのエクスポートとインポート

署名キーを Cisco アプライアンス上のテキスト ファイルにエクスポートできます。キーをエクスポートすると、アプライアンスに現在存在するすべてのキーがテキスト ファイルに挿入されます。キーのエクスポートの詳細については、「[署名キーのエクスポート](#)」(P.17-10) を参照してください。

エクスポートされたキーをインポートすることもできます。



(注)

キーをインポートすると、アプライアンス上のすべての現在のキーが置き換えられます。

詳細については、「[既存の署名キーのインポートまたは入力](#)」(P.17-10) を参照してください。

公開キー

署名キーをドメイン プロファイルに関連付けると、公開キーが含まれる DNS テキスト レコードを作成できます。これは、ドメイン プロファイルのリストの [DNS テキスト レコード (DNS Text Record)] カラムの [生成 (Generate)] リンクから(または CLI の `domainkeysconfig -> profiles -> dnstxt` から) 実行します。

図 17-2 [ドメイン プロファイル (Domain Profiles)] ページの DNS テキスト レコードの生成リンク

Profile Name	Domain	Selector	Users	Signing Key	DNS Text Record	Test Profile	Delete
ExampleProfile	example.com	test	.example.com	myTestKey	Generate	Test	All Delete

DNS テキスト レコードの生成の詳細については、「[DNS テキスト レコードの生成](#)」(P.17-12) を参照してください。

[署名キー (Signing Keys)] ページの [ビュー (View)] リンクから、公開キーを表示することもできます。

図 17-3 [署名キー (Signing Keys)] ページの公開キーの表示リンク

Name	Key Size (Bits)	Public Key	Domain Profiles	Delete
TestKey	768	View	ExampleProfile	All Delete

ドメイン プロファイル

ドメイン プロファイルは送信側ドメインを署名に必要なその他の情報と共に署名キーに関連付けます。

- ドメイン プロファイルの名前。
- ドメイン名 (「d=」ヘッダーに含まれるドメイン)。
- セレクトタ (セレクトタは公開キーのクエリーを形成するために使用されます。DNS クエリー タイプでは、この値が送信側ドメインの「_domainkey」名前空間の前に付けられます)。

- 正規化方法（署名アルゴリズムに提示するためにヘッダーと内容が準備される方法）。AsyncOS は DomainKeys に対して「simple」と「nofws」、DKIM に対して「relaxed」と「simple」をサポートしています。
- 署名キー（詳細については、「署名キー」(P.17-3) を参照してください）。
- 署名するヘッダーのリストと本文の長さ（DKIM のみ）。
- 署名のヘッダー（DKIM のみ）に含めるタグのリスト。これらのタグは次の情報を保持します。
 - 署名されたメッセージが代理したユーザまたはエージェントの ID（たとえば、メーリング リスト マネージャ）。
 - 公開キーを取得するために使用されるクエリー方法のカンマ区切りリスト。
 - 署名が作成されたときのタイムスタンプ。
 - 秒による署名の有効期限。
 - 垂直バーによって隔離されている（つまり、|）ヘッダー フィールドの一覧は、メッセージの署名時を示します。
- 署名（DKIM のみ）に含めるタグ。
- プロファイル ユーザのリスト（署名用にドメイン プロファイルの使用を許可されたアドレス）。



(注)

プロファイル ユーザに指定されたアドレスのドメインは [ドメイン (Domain)] フィールドに指定されたドメインに一致している必要があります。

既存のすべてのドメイン プロファイルで、特定の用語を検索できます。詳細については、「ドメイン プロファイルの検索」(P.17-14) を参照してください。

DKIM 署名を持つシステムで生成されたメッセージに署名するかどうかを選択できます。詳細については、「システムで生成されたメッセージへの署名」(P.17-14) を参照してください。

ドメイン プロファイルのエクスポートとインポート

既存のドメイン プロファイルを Cisco アプライアンス上のテキスト ファイルにエクスポートできます。ドメイン プロファイルをエクスポートすると、アプライアンスに存在するすべてのプロファイルが 1 つのテキスト ファイルに挿入されます。「ドメイン プロファイルのエクスポート」(P.17-13) を参照してください。

以前にエクスポートしたドメイン プロファイルをインポートできます。ドメイン プロファイルをインポートすると、マシン上のすべての現在のドメイン プロファイルが置き換えられます。「ドメイン プロファイルのインポート」(P.17-13) を参照してください。

送信メールの署名のイネーブル化

DomainKeys および DKIM 署名は発信メールのメール フロー ポリシーでイネーブルにします。詳細については、『Cisco IronPort AsyncOS for Email Configuration Guide』の「Configuring the Gateway to Receive Mail」の章を参照してください。

手順

- ステップ 1** [メール フロー ポリシー (Mail Flow Policies)] ページ ([メール ポリシー (Mail Policies)] メニューから) で、[リレー (RELAYED)] メール フロー ポリシー (送信) をクリックします。

- ステップ 2** [セキュリティ サービス (Security Features)] セクションから、[オン (On)] を選択して、[DomainKeys/DKIM 署名 (DomainKeys/DKIM Signing)] をイネーブルにします。
- ステップ 3** 変更内容を送信し、確定します。

バウンスおよび遅延メッセージの署名のイネーブル化

発信メッセージに署名するだけでなく、バウンスおよび遅延メッセージに署名したい場合があります。これにより、会社から受信するバウンスおよび遅延メッセージが正当なものであることを受信者に警告したい場合があります。バウンスおよび遅延メッセージの DomainKeys および DKIM 署名をイネーブルにするには、公開リスナーに関連付けられたバウンス プロファイルの DomainKeys/DKIM 署名をイネーブルにします。

手順

- ステップ 1** 署名された発信メッセージを送信する公開リスナーに関連付けられているバウンス プロファイルで、[ハードバウンスと遅延警告メッセージ (Hard Bounce and Delay Warning Messages)] に移動します。
- ステップ 2** [バウンスおよび遅延メッセージに対してドメインキー署名を使用 (Use Domain Key Signing for Bounce and Delay Messages)] をイネーブルにします。



(注) バウンスおよび遅延メッセージに署名するには、「[DomainKeys/DKIM 署名の設定 \(GUI\)](#)」(P.17-6) に示されたすべての手順を完了している必要があります。



(注) ドメイン プロファイルの [差出人 : (From:)] アドレスは、バウンス返信アドレスに使用されているアドレスと一致している必要があります。これらのアドレスを一致させるには、バウンス プロファイルの返信アドレスを設定し ([システム管理 (System Administration)] > [返信先アドレス (Return Addresses)])、ドメイン プロファイルの [ユーザのプロファイリング (Profile Users)] リストで同じ名前を使用します。たとえば、バウンス返信アドレスに MAILER-DAEMON@example.com の返信アドレスを設定し、ドメイン プロファイルにプロファイル ユーザとして MAILER-DAEMON@example.com を追加します。

DomainKeys/DKIM 署名の設定 (GUI)

手順

- ステップ 1** 新規の秘密キーを作成するか、既存の秘密キーをインポートします。署名キーの作成またはインポートについては、「[署名キー](#)」(P.17-3) を参照してください。
- ステップ 2** ドメイン プロファイルを作成し、キーをドメイン プロファイルに関連付けます。ドメイン プロファイルの作成については、「[ドメイン プロファイル](#)」(P.17-4) を参照してください。
- ステップ 3** DNS テキスト レコードを作成します。DNS テキスト レコードの作成については、「[DNS テキスト レコードの生成](#)」(P.17-12) を参照してください。

- ステップ 4** 発信メールのメール フロー ポリシーで、DomainKeys/DKIM 署名をまだイネーブルにしていない場合は、イネーブルにします（「送信メールの署名のイネーブル化」(P.17-5) を参照してください）。
- ステップ 5** 任意で、バウンスおよび遅延メッセージの DomainKeys/DKIM 署名をイネーブルにします。バウンスおよび遅延メッセージの署名のイネーブル化については、「バウンスおよび遅延メッセージの署名のイネーブル化」(P.17-6) を参照してください。
- ステップ 6** 電子メールを送信します。ドメイン プロファイルに一致するドメインから送信されたメールは DomainKeys/DKIM 署名されます。さらに、バウンスおよび遅延メッセージの署名を設定した場合は、バウンスまたは遅延メッセージに署名されます。



(注) DomainKey および DKIM プロファイルの両方を作成した（およびメール フロー ポリシーで署名をイネーブルにしている）場合、AsyncOS は DomainKeys と DKIM の両方の署名で送信メッセージを署名します。

DomainKeys 署名のドメイン プロファイルの作成

手順

- ステップ 1** [メール ポリシー (Mail Policies)] > [署名プロファイル (Signing Profiles)] を選択します。
- ステップ 2** [ドメイン署名プロファイル (Domain Signing Profile)] セクションで、[プロファイルを追加 (Add Profile)] をクリックします。
- ステップ 3** プロファイル名を入力します
- ステップ 4** [ドメイン キー タイプ (Domain Key Type)] については、[ドメイン キー (Domain Keys)] を選択します。
新しいオプションがページに表示されます。
- ステップ 5** ドメイン名を入力します。
- ステップ 6** セレクタを入力します。セレクタは、「_domainkey」名前空間の前に付けられる任意の名前で、送信側ドメインあたり複数の同時公開キーをサポートするために使われます。セレクタ値と長さは、DNS 名前空間と電子メール ヘッダーで有効である必要があります、それらにセミコロンを含めることができないという規定が追加されます。
- ステップ 7** 正規化 ([no forwarding whitespaces] または [simple]) を選択します。
- ステップ 8** すでに署名キーを作成している場合、署名キーを選択します。それ以外の場合は、次のステップに進みます。署名キーをリストから選択させるために、少なくとも 1 つの署名キーを作成する（またはインポートする）必要があります。「新しい署名キーの作成」(P.17-10) を参照してください。
- ステップ 9** 署名のドメイン プロファイルを使用するユーザ（電子メール アドレス、ホストなど）を入力します。
- ステップ 10** 変更内容を送信し、確定します。
- ステップ 11** この時点で、送信メール フロー ポリシーで DomainKeys/DKIM 署名をイネーブルにしていない場合はイネーブルにする必要があります（「送信メールの署名のイネーブル化」(P.17-5) を参照してください）。



(注) DomainKeys と DKIM の両方のプロファイルを作成している場合、AsyncOS は送信メールに DomainKeys と DKIM の両方の署名を実行します。

DKIM 署名の新しいドメイン プロファイルの作成

手順

- ステップ 1** [メール ポリシー (Mail Policies)] > [署名プロファイル (Signing Profiles)] を選択します。
- ステップ 2** [ドメイン署名プロファイル (Domain Signing Profile)] セクションで、[プロファイルを追加 (Add Profile)] をクリックします。
- ステップ 3** プロファイル名を入力します
- ステップ 4** [ドメイン キー タイプ (Domain Key Type)] に対して、[DKIM] を選択します。
新しいオプションがページに表示されます。
- ステップ 5** ドメイン名を入力します。
- ステップ 6** セレクタを入力します。セレクタは、「_domainkey」名前空間の前に付けられる任意の名前で、送信側ドメインあたり複数の同時公開キーをサポートするために使われます。セレクタ値と長さは、DNS 名前空間と電子メール ヘッダーで有効である必要があり、それらにセミコロンを含めることができないという規定が追加されます。
- ステップ 7** ヘッダーの正規化を選択します。次のオプションから選択します。
- [Relaxed]。「relaxed」ヘッダー正規化アルゴリズムは、次を実行します。ヘッダー名を小文字に変更し、ヘッダーを展開して、連続した空白を 1 つの空白に短縮し、先頭と末尾の空白を取り除きます。
 - [Simple]。ヘッダーは変更されません。
- ステップ 8** 本文の正規化を選択します。次のオプションから選択します。
- [Relaxed]。「relaxed」ヘッダー正規化アルゴリズムは、次を実行します。本文末尾の空の行を取り除き、行中の空白を 1 つの空白に短縮し、行の末尾の空白を取り除きます。
 - [Simple]。本文末尾の空の行を取り除きます。
- ステップ 9** すでに署名キーを作成している場合、署名キーを選択します。それ以外の場合は、次のステップに進みます。署名キーをリストから選択させるために、少なくとも 1 つの署名キーを作成する（またはインポートする）必要があります。「[新しい署名キーの作成](#)」(P.17-10) を参照してください。
- ステップ 10** 署名するヘッダーのリストを選択します。次のヘッダーから選択できます。
- [すべて (All)]。AsyncOS は署名時に存在するすべてのヘッダーに署名します。送信中にヘッダーの追加や削除が予想されない場合は、すべてのヘッダーに署名することが考えられます。
 - [標準 (Standard)]。送信中にヘッダーの追加や削除が予想される場合は、標準ヘッダーを選択することが考えられます。AsyncOS は次の標準ヘッダーにのみ署名します（メッセージにそのヘッダーが存在しない場合、DKIM 署名は、そのヘッダーにヌル値を示します）。
 - From
 - Sender、Reply To-
 - Subject
 - Date、Message-ID

- To、Cc
- MIME-Version
- Content-Type、Content-Transfer-Encoding、Content-ID、Content-Description
- Resent-Date、Resent-From、Resent-Sender、Resent-To、Resent-cc、Resent-Message-ID
- In-Reply-To、References
- List-Id、List-Help、List-Unsubscribe、List-Subscribe、List-Post、List-Owner、List-Archive



(注) [標準 (Standard)] を選択した場合、署名するヘッダーを追加できます。

ステップ 11 メッセージ本文に署名する方法を指定します。メッセージ本文に署名するか、署名するバイト数を選択できます。次のオプションのいずれかを選択します。

- [本文全体を含む (Whole Body Implied)]。本文の長さを判断するために「=」タグを使用しないでください。メッセージ全体に署名し、変更を許可しません。
- [本文全体を自動判断 (Whole Body Auto-determined)]。メッセージ本文全体に署名し、送信中に本文の末尾へのデータの追加を許可します。
- [最初に署名 _ バイト (Sign first _ bytes)]。指定したバイト数まで、メッセージ本文に署名します。

ステップ 12 メッセージ署名のヘッダー フィールドに含めるタグを選択します。これらのタグに格納されている情報はメッセージ署名の検証に使用されます。次のオプションから 1 つ以上を選択します。

- 「**I**」のタグ。署名されたメッセージが代理したユーザまたはエージェントの ID (たとえば、メール リングリスト マネージャ)。ドメイン @example.com など、@記号が付加されたドメイン名を入力します。
- 「**q**」タグ。公開キーを取得するために使用されるクエリー方法のコロン区切りリスト。現在、唯一有効な値は dns/txt です。
- 「**t**」タグ。署名が作成されたときのタイムスタンプを表示します。
- 「**X**」タグ。署名が終了する絶対的な日時。署名の有効期限 (秒単位) を指定します。デフォルト値は 31536000 秒です。
- 「**z**」タグ。垂直バーによって隔離されている (つまり、|) ヘッダー フィールドの一覧は、メッセージの署名時を示します。これには、ヘッダー フィールドの名前と値が含まれます。次に例を示します。

```
z=From:admin@example.com|To:joe@example.com|
Subject:test%20message|Date:Date:August%2026,%202011%205:30:02%20PM%20-0700
```

ステップ 13 署名のドメイン プロファイルを使用するユーザ (電子メール アドレス、ホストなど) を入力します。



(注) ドメイン プロファイルを作成する場合、特定のユーザに関連付けるプロファイルの決定において、階層を使用することに注意してください。たとえば、example.com のプロファイルと joe@example.com の別のプロファイルを作成するとします。joe@example.com からメールが送信される場合、joe@example.com のプロファイルが使われます。しかし、メールが adam@example.com から送信される場合は、example.com のプロファイルが使われます。

ステップ 14 変更内容を送信し、確定します。

ステップ 15 この時点で、送信メール フロー ポリシーで DomainKeys/DKIM 署名をイネーブルにしていない場合はイネーブルにする必要があります (「送信メールの署名のイネーブル化」(P.17-5) を参照してください)。



(注) DomainKeys と DKIM の両方のプロファイルを作成している場合、AsyncOS は送信メールに DomainKeys と DKIM の両方の署名を実行します。

新しい署名キーの作成

署名キーは DomainKeys および DKIM 署名のドメイン プロファイルに必要です。

手順

ステップ 1 [メール ポリシー (Mail Policies)] > [署名キー (Signing Keys)] を選択します。

ステップ 2 [キーを追加 (Add Key)] をクリックします。

ステップ 3 キーの名前を入力します。

ステップ 4 [生成 (Generate)] をクリックし、キー サイズを選択します。

キー サイズが大きいくほどセキュリティが向上しますが、パフォーマンスに影響する可能性があります。シスコでは、セキュリティとパフォーマンスのバランスが良い 768 ビットのキー サイズが推奨されます。

ステップ 5 変更内容を送信し、確定します。



(注) キーを割り当てるドメイン プロファイルを編集していない場合は、編集する必要がある場合があります。

署名キーのエクスポート

アプライアンスのすべてのキーは、1 つのテキスト ファイルとしてエクスポートされます。

手順

ステップ 1 [メール ポリシー (Mail Policies)] > [署名キー (Signing Keys)] を選択します。

ステップ 2 [キーをエクスポート (Export Keys)] をクリックします。

ステップ 3 ファイルの名前を入力し、[送信 (Submit)] をクリックします。

既存の署名キーのインポートまたは入力

キーの貼り付け

手順

ステップ 1 [メール ポリシー (Mail Policies)] > [署名キー (Signing Keys)] を選択します。

- ステップ 2 [キーを追加 (Add Key)] をクリックします。
- ステップ 3 [貼り付けキー (Paste Key)] フィールドにキーを貼り付けます (PEM フォーマットされ、RSA キーのみである必要があります)。
- ステップ 4 変更内容を送信し、確定します。

既存のエクスポート ファイルからのキーのインポート



(注) キー ファイルを取得するには、「署名キーのエクスポート」(P.17-10) を参照してください。

手順

- ステップ 1 [メール ポリシー (Mail Policies)] > [署名キー (Signing Keys)] を選択します。
- ステップ 2 [キーをインポート (Import Keys)] をクリックします。
- ステップ 3 エクスポートされた署名キーを含むファイルを選択します。
- ステップ 4 [送信 (Submit)] をクリックします。インポートによってすべての既存の署名キーが置き換えられることが警告されます。テキスト ファイルのすべてのキーがインポートされます。
- ステップ 5 [インポート (Import)] をクリックします。

署名キーの削除

選択した [署名キー (Signing Keys)] の除外

手順

- ステップ 1 [メール ポリシー (Mail Policies)] > [署名キー (Signing Keys)] を選択します。
- ステップ 2 削除する各署名キーの右のチェックボックスをオンにします。
- ステップ 3 [削除 (Delete)] をクリックします。
- ステップ 4 削除を確認します。

すべての署名キーの削除

手順

- ステップ 1 [メール ポリシー (Mail Policies)] > [署名キー (Signing Keys)] を選択します。
- ステップ 2 [署名キー (Signing Keys)] ページの [すべてのキーを消去 (Clear All Keys)] をクリックします。
- ステップ 3 削除を確認します。

DNS テキスト レコードの生成

手順

-
- ステップ 1** [メール ポリシー (Mail Policies)] > [署名プロファイル (Signing Profiles)] を選択します。
- ステップ 2** [ドメイン署名プロファイル (Domain Signing Profiles)] セクションの [DNS テキストレコード (DNS Text Record)] カラムで、対応するドメイン プロファイルに対して [生成 (Generate)] リンクをクリックします。
- ステップ 3** DNS テキスト レコードに含める属性のチェックボックスをオンにします。
- ステップ 4** [再生成 (Generate Again)] をクリックして、変更を含めてキーを再生成します。
- ステップ 5** DNS テキスト レコードがウィンドウの下部のテキスト フィールド (コピーできます) に表示されます。場合によっては、複数の文字列の DNS テキスト レコードが生成されます。「[複数の文字列の DNS テキスト レコード](#)」(P.17-12) を参照してください。
- ステップ 6** [完了 (Done)] をクリックします。
-

複数の文字列の DNS テキスト レコード

DNS テキスト レコードの生成に使用される署名キーのサイズが 1024 ビットより大きい場合は、複数の文字列の DNS テキスト レコードが生成されることがあります。これは、DNS テキスト レコードの単一の文字列に含めることができるのは、255 文字以下であるためです。一部の DNS サーバでは複数の文字列の DNS テキスト レコードが受け入れられないか、実行されないため、DKIM 認証は失敗する可能性があります。

このシナリオを回避するために、二重引用符を使用して、複数の文字列の DNS テキスト レコードを、255 バイト未満の文字列に分割することを推奨します。次に、例を示します。

```
s._domainkey.domain.com. IN TXT "v=DKIM1;"
"p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQE"
"A4Vbhjq2n/3DbEk6EHdeVX1IXFT7OE181amoZLbvwmX+bej"
"CdxcsFV3uS7G8oOJSWBP0z++nTQmy9ZDWfaiopU6k7tzoI"
"+oRDlKkhCQrM4oP2B2F5sTDkYwPY3Pen2jgC2OgbPnbo3o"
"m3c1wMWgSoZxoZUE4ly5kPuK9fTtpeJHNiZAqkFICiev4yrkL"
"R+SmFsJn9MYH5+lchyZ74Bvm+16Xq2mptWXEwpwOxWI"
"YHXsZo2zRjedrQ45vmgb8xUx5ioYY9/yBLHudGc+GUKTjli4"
"mQg48yCD/HVnfsSRXaPinliEkypH9cSngvWuIYUQz0dHU;"
```

このようにして分割された DNS テキスト レコードが、DKIM 実装により、処理前に元の単一の文字列に再構築されます。

ドメイン プロファイルのテスト

署名キーを作成し、それをドメイン プロファイルに関連付け、DNS テキストを生成して、権限のある DNS に挿入したら、ドメイン プロファイルをテストできます。

手順

-
- ステップ 1** [メール ポリシー (Mail Policies)] > [署名プロファイル (Signing Profiles)] を選択します。
- ステップ 2** [ドメイン署名プロファイル (Domain Signing Profiles)] セクションの [テストプロファイル (Test Profile)] カラムで、ドメイン プロファイルの [テスト (Test)] リンクをクリックします。

- ステップ 3** 成功または失敗を示すメッセージがページの上部に表示されます。テストが失敗した場合、エラー テキストを含む警告メッセージが表示されます。
-

ドメイン プロファイルのエクスポート

アプライアンスのすべてのドメイン プロファイルは、単一のテキスト ファイルにエクスポートされます。

手順

- ステップ 1** [メール ポリシー (Mail Policies)] > [署名プロファイル (Signing Profiles)] を選択します。
- ステップ 2** [ドメイン プロファイルのエクスポート (Export Domain Profiles)] をクリックします。
- ステップ 3** ファイルの名前を入力し、[送信 (Submit)] をクリックします。
-

ドメイン プロファイルのインポート

手順

- ステップ 1** [メール ポリシー (Mail Policies)] > [署名プロファイル (Signing Profiles)] を選択します。
- ステップ 2** [ドメイン プロファイルのインポート (Import Domain Profiles)] をクリックします。
- ステップ 3** エクスポートされたドメイン プロファイルを含むファイルを選択します。
- ステップ 4** [送信 (Submit)] をクリックします。インポートによってすべての既存のドメイン プロファイルが置き換えられることが警告されます。テキスト ファイルのすべてのドメイン プロファイルがインポートされます。
- ステップ 5** [インポート (Import)] をクリックします。
-

ドメイン プロファイルの削除

ドメイン プロファイルの削除

手順

- ステップ 1** [メール ポリシー (Mail Policies)] > [署名プロファイル (Signing Profiles)] を選択します。
- ステップ 2** 削除する各ドメイン プロファイルの右のチェックボックスをオンにします。
- ステップ 3** [削除 (Delete)] をクリックします。
- ステップ 4** 削除を確認します。
-

すべてのドメイン プロファイルの削除

手順

-
- ステップ 1** [メール ポリシー (Mail Policies)] > [署名プロファイル (Signing Profiles)] を選択します。
- ステップ 2** [すべて消去 (Clear All)] をクリックします。
- ステップ 3** 削除を確認します。
-

ドメイン プロファイルの検索

手順

-
- ステップ 1** [メール ポリシー (Mail Policies)] > [署名プロファイル (Signing Profiles)] を選択します。
- ステップ 2** [ドメイン プロファイルの検索 (Find Domain Profiles)] で、検索条件を指定します。
- ステップ 3** [プロファイルの検索 (Find Profiles)] をクリックします。
- ステップ 4** 検索では、各ドメイン プロファイルの email、domain、selector、signing key name のフィールドがスキャンされます。
-



(注) 検索語を入力しない場合、検索エンジンはすべてのドメイン プロファイルを返します。

システムで生成されたメッセージへの署名

DKIM 署名を持つシステムで生成されたメッセージに署名するかどうか選択できます。アプライアンスは次のメッセージに署名します。

- Cisco IronPort スпам隔離通知
- コンテンツ フィルタで生成された通知
- 設定メッセージ
- サポート リクエスト

手順

-
- ステップ 1** [メール ポリシー (Mail Policies)] > [署名プロファイル (Signing Profiles)] を選択します。
- ステップ 2** [システム生成メッセージの DKIM 署名 (DKIM Signing of System Generated Messages)] のセクションの [設定を編集 (Edit Settings)] をクリックします。
- ステップ 3** [オン (On)] を選択します。
- ステップ 4** 変更内容を送信し、確定します。
-

ドメインキーとロギング

DomainKeys 署名時には、次のような行がメール ログに追加されます。

```
Tue Aug 28 15:29:30 2007 Info: MID 371 DomainKeys: signing with dk-profile - matches
user123@example.com
Tue Aug 28 15:34:15 2007 Info: MID 373 DomainKeys: cannot sign - no profile matches
user12@example.com
```

DKIM 署名時には、次のような行がメール ログに追加されます。

```
Tue Aug 28 15:29:54 2007 Info: MID 372 DKIM: signing with dkim-profile - matches
user@example.com
Tue Aug 28 15:34:15 2007 Info: MID 373 DKIM: cannot sign - no profile matches
user2@example.com
```

DKIM 署名を使用した受信メッセージの確認方法

表 17-1 DKIM 署名を使用した受信メッセージの確認方法

	操作内容	詳細
ステップ1	DKIM 署名を使用してメッセージを確認するプロファイルを作成します。	「DKIM 検証プロファイルの作成」(P.17-17)
ステップ2	(任意) DKIM 署名を使用して受信メッセージの確認に使用されるカスタムのメールフローポリシーを作成します。	「メールフローポリシーを使用した着信メッセージのルール定義」(P.7-15)
ステップ3	DKIM 署名を使用した受信メッセージの確認にメールフローポリシーを設定します。	「メールフローポリシーでの DKIM 検証の設定」(P.17-19)
ステップ4	電子メールセキュリティアプライアンスが確認されたメッセージで実行するアクションを定義します。	「DKIM 検証済みメールのアクションの設定」(P.17-19)
ステップ5	特定の送信者または受信者のグループにアクションを関連付けます。	「メールポリシーの設定」(P.10-6)

AsyncOS による DKIM 検証チェック

DKIM 検証用に AsyncOS アプライアンスを設定すると、次のチェックが実行されます。

手順

- ステップ 1 AsyncOS は受信メールの [DKIM シグネチャ (DKIM-Signature)] フィールド、署名ヘッダーの構文、有効なタグ値、必須タグを調べます。署名がこれらのいずれかのチェックで失敗すると、AsyncOS は *permfail* を返します。
- ステップ 2 署名チェックの実行後、公開 DNS レコードから公開キーが取得され、TXT レコードが検証されます。このプロセス中にエラーが検出されると、AsyncOS は *permfail* を返します。公開キーの DNS クエリーで応答を取得できない場合、*tempfail* が発生します。

ステップ 3 公開キーの取得後、AsyncOS はハッシュ値をチェックし、署名を検証します。この手順中にエラーが発生すると、AsyncOS は *permfail* を返します。

ステップ 4 チェックにすべて合格すると、AsyncOS は *pass* を返します。



(注) メッセージ本文が指定された長さより長い場合、AsyncOS は次の判定を返します。

```
dkim = pass (partially verified [x bytes])
```

ここで *X* は検証されたバイト数を表します。

最終検証結果は、*Authentication-Results* ヘッダーとして入力されます。たとえば、次のいずれかのようなヘッダーを受け取ることがあります。

```
Authentication-Results: example1.com
```

```
header.from=From:user123@example.com; dkim=pass (signature verified)
```

```
Authentication-Results: example1.com
```

```
header.from=From:user123@example.com; dkim=pass (partially verified [1000 bytes])
```

```
Authentication-Results: example1.com
```

```
header.from=From:user123@example.com; dkim=permfail (body hash did not verify)
```



(注) 現在の DKIM 検証は最初の有効な署名で停止します。最後に検出された署名を使用して、検証できません。この機能は、後のリリースで使用できるようになる可能性があります。

DKIM の検証プロファイルの管理

DKIM の検証プロファイルは電子メールセキュリティ アプライアンスのメールフロー ポリシーが DKIM 署名を保証するために使用されるパラメータのリストです。たとえば、クエリーがタイムアウトする前に 30 秒取る検証プロファイルと、クエリーがタイムアウトする前に 3 秒だけ取る検証プロファイルの、2 つの検証プロファイルを作成できます。THROTTLED メールフロー ポリシーに 2 つめの検証プロファイルを割り当てて、DDoS の場合の接続スタベーションを防止できます。検証プロファイルは次の情報で構成されます。

- 検証プロファイルの名前。
- 許容できる公開キーの最小、最大サイズ。デフォルトのキーのサイズは 512 および 2048 です。
- メッセージの中で検証できる署名の最大数。メッセージに定義した署名の最大数よりも多くの署名がある場合、アプライアンスは残りの署名をスキップし、メッセージの処理を続行します。デフォルトは、5 つの署名です。
- 送信者のシステム時刻と検証者側のシステム時刻との間の時間の最大許容差（秒単位）。たとえば、メッセージ署名が 05:00:00 に期限切れとなる場合に検証者のシステム時刻が 05:00:30 だと、時間の許容差が 60 秒の場合はメッセージ署名は有効なままですが、許容差が 10 秒だと無効になります。デフォルトは 60 秒です。
- 本文の長さのパラメータを使用するかどうかを指定するオプション。
- 一時的な障害の場合に実行する SMTP アクション。
- 永続的な障害の場合に実行する SMTP アクション。

プロファイル名ですべての既存の検証プロファイルを検索できます。

アプライアンス Cisco のコンフィギュレーションディレクトリに DKIM 検証プロファイルテキストファイルとしてエクスポートできます。検証プロファイルのエクスポートすると、アプライアンスに存在するすべてのプロファイルが 1 つのテキストファイルに挿入されます。詳細については、「[DKIM 検証プロファイルのエクスポート](#)」(P.17-17) を参照してください。

以前エクスポートした DKIM 検証プロファイルをインポートできます。DKIM 検証プロファイルをインポートすると、マシンの現在のすべての DKIM 検証プロファイルを置き換えることになります。詳細については、「[DKIM 検証プロファイルのインポート](#)」(P.17-18) を参照してください。

DKIM 検証プロファイルの作成

手順

- ステップ 1** [メール ポリシー (Mail Policies)] > [検証プロファイル (Verification Profiles)] をクリックします。
- ステップ 2** [プロファイルを追加 (Add Profile)] をクリックします。
- ステップ 3** プロファイル名を入力します。
- ステップ 4** アプライアンスが許可する署名キーの最小キー サイズを選択します。
- ステップ 5** アプライアンスが許可する署名キーの最大キー サイズを選択します。
- ステップ 6** 1 つのメッセージで検証する署名の最大数を選択します。デフォルトは 5 つの署名です。
- ステップ 7** キー クエリーがタイムアウトするまでの時間 (秒) を選択します。デフォルトは 10 秒です。
- ステップ 8** 送信者のシステム時刻と検証者側のシステム時刻との間の時間の最大許容差 (秒単位) を選択します。デフォルトは 60 秒です。
- ステップ 9** メッセージの確認に、署名の本文の長さのパラメータを使用するかどうかを選択します。
- ステップ 10** 署名を確認するときに一時的な障害がある場合、電子メールセキュリティ アプライアンスがメッセージを受け入れるか、拒否するかを選択します。アプライアンスがメッセージを拒否する場合、デフォルトの 451 SMTP 応答コードまたは別の SMTP 応答コードとテキストを送信するよう選択できます。
- ステップ 11** 署名を確認するときに永続的な障害がある場合は、電子メールセキュリティ アプライアンスがメッセージを受け入れるか、拒否するかを選択します。アプライアンスがメッセージを拒否する場合、デフォルトの 451 SMTP 応答コードまたは別の SMTP 応答コードとテキストを送信するよう選択できます。
- ステップ 12** 変更を送信します。
新しいプロファイルが DKIM 検証プロファイルのテーブルに表示されます。
- ステップ 13** 変更内容を確定します。
- ステップ 14** この時点で着信メール フロー ポリシーで DKIM 検証をイネーブルにし、使用する検証プロファイルを選択する必要があります。

DKIM 検証プロファイルのエクスポート

アプライアンスのすべての DKIM 検証プロファイルは単一のテキストファイルとしてエクスポートされ、アプライアンスの configuration ディレクトリに保存されます。

手順

- ステップ 1** [メール ポリシー (Mail Policies)] > [検証プロファイル (Verification Profiles)] を選択します。

- ステップ 2 [プロファイルをエクスポート (Export Profiles)] をクリックします。
 - ステップ 3 ファイルの名前を入力し、[送信 (Submit)] をクリックします。
-

DKIM 検証プロファイルのインポート

手順

- ステップ 1 [メール ポリシー (Mail Policies)] > [検証プロファイル (Verification Profiles)] を選択します。
 - ステップ 2 [プロファイルをインポート (Import Profiles)] をクリックします。
 - ステップ 3 DKIM 検証プロファイルを含むファイルを選択します。
 - ステップ 4 [送信 (Submit)] をクリックします。インポートによってすべての既存の DKIM 検証プロファイルが置き換えられることが警告されます。
 - ステップ 5 [インポート (Import)] をクリックします。
-

DKIM 検証プロファイルの削除

選択した DKIM 検証プロファイルの削除

手順

- ステップ 1 [メール ポリシー (Mail Policies)] > [検証プロファイル (Verification Profiles)] を選択します。
 - ステップ 2 削除する各 DKIM 検証プロファイルの右のチェックボックスをオンにします。
 - ステップ 3 [削除 (Delete)] をクリックします。
 - ステップ 4 削除を確認します。
-

すべての DKIM 検証プロファイルの削除

手順

- ステップ 1 [メール ポリシー (Mail Policies)] > [検証プロファイル (Verification Profiles)] を選択します。
 - ステップ 2 [すべて消去 (Clear All)] をクリックします。
 - ステップ 3 削除を確認します。
-

DKIM 検証プロファイルの検索

すべての DKIM 検証プロファイルについてプロファイル名から特定の用語を検索します。

手順

- ステップ 1 [メール ポリシー (Mail Policies)] > [検証プロファイル (Verification Profiles)] を選択します。
- ステップ 2 [次の DKIM 検証プロファイルを検索 (Search DKIM Verification Profiles)] では、検索条件を指定します。
- ステップ 3 [プロファイルの検索 (Find Profiles)] をクリックします。
検索では、各 DKIM 検証プロファイル名をスキャンします。
検索語を入力しない場合、検索エンジンはすべての DKIM 検証プロファイルを返します。

メール フロー ポリシーでの DKIM 検証の設定

DKIM 検証は、受信メールのメール フロー ポリシーでイネーブルにします。

手順

- ステップ 1 [メール ポリシー (Mail Policies)] > [メール フロー ポリシー (Mail Flow Policies)] を選択します。
- ステップ 2 検証を実行するリスナーの着信メール ポリシーをクリックします。
- ステップ 3 メール フロー ポリシーの [セキュリティ サービス (Security Features)] セクションで、[オン (On)] を選択して、[DKIM 検証 (DKIM Verification)] をイネーブルにします。
- ステップ 4 ポリシーで使用する DKIM 検証プロファイルを選択します。
- ステップ 5 変更内容を確定します。

DKIM 検証とロギング

DKIM 検証時には、次のような行がメール ログに追加されます。

```
mail.current:Mon Aug 6 13:35:38 2007 Info: MID 17 DKIM: no signature
```

```
mail.current:Mon Aug 6 15:00:37 2007 Info: MID 18 DKIM: verified pass
```

DKIM 検証済みメールのアクションの設定

DKIM メールを検証すると、メールに *Authentication-Results* ヘッダーが追加されますが、認証結果に関係なく、メールは受け入れられます。これらの認証結果に基づいてアクションを設定するには、コンテンツ フィルタを作成して、DKIM 検証済みメールに対するアクションを実行します。たとえば、DKIM 検証が失敗した場合、メールを配信、バウンス、ドロップ、または隔離エリアに送るように設定することができます。これを実行するには、コンテンツ フィルタを使用して、アクションを設定する必要があります。

手順

-
- ステップ 1** [着信フィルタ (Incoming Filters)] > [メール ポリシー (Mail Policies)] を選択します。
- ステップ 2** [フィルタを追加 (Add Filter)] をクリックします。
- ステップ 3** [条件 (Conditions)] セクションで、[条件を追加 (Add Condition)] をクリックします。
- ステップ 4** 条件のリストから [DKIM 認証 (DKIM Authentication)] を選択します。
- ステップ 5** DKIM 条件を選択します。次のオプションのいずれかを選択します。
- [Pass]。メッセージは認証テストに合格しました。
 - [Neutral]。認証が実行されませんでした。
 - [Temperror]。修復可能なエラーが発生しました。
 - [Permerror]。修復不可能なエラーが発生しました。
 - [Hardfail]。認証テストが失敗しました。
 - [None]。メッセージは署名されていません。
- ステップ 6** 条件に関連付けるアクションを選択します。たとえば、DKIM 検証が失敗した場合、受信者に通知し、メッセージをバウンスさせることができます。または DKIM 検証に合格した場合、それ以上処理せずに、メッセージをすぐに配信することができます。
- ステップ 7** 新しいコンテンツ フィルタを送信します。
- ステップ 8** 適切な受信メール ポリシーでコンテンツ フィルタをイネーブルにします。
- ステップ 9** 変更内容を確定します。
-

SPF および SIDF 検証の概要

Cisco AsyncOS は、SPF (Sender Policy Framework) および SIDF (Sender ID Framework) 検証をサポートしています。SPF と SIDF は DNS レコードに基づいて電子メールの信頼性を検証する方法です。SPF と SIDF により、インターネット ドメインの所有者は、特別な形式の DNS TXT レコードを使用して、そのドメインに電子メールを送信する権限のあるマシンを指定することができます。準拠したメール受信側は、パブリッシュされた SPF レコードを使用して、メール トランザクション中に、送信側のメール転送エージェントの ID の権限をテストします。

SPF/SIDF 認証を使用すると、送信側はそれらの名前の使用が許可されるホストを指定する SPF レコードをパブリッシュし、準拠するメール受信側はパブリッシュされた SPF レコードを使用して、メール トランザクション中に送信側のメール転送エージェントの ID の権限をテストします。



- (注)** SPF チェックでは、解析と評価が必要であるため、AsyncOS のパフォーマンスに影響する場合があります。さらに、SPF チェックによって、DNS インフラストラクチャの負荷が増えることに注意してください。

SPF と SIDF を操作する場合、SIDF は SPF に似ていますが、いくつかの違いがあります。SIDF と SPF のすべての違いの説明については、RFC 4406 を参照してください。このマニュアルの目的のため、この 2 つの用語は、1 つのタイプの検証のみを適用する場合を除いて、まとめて説明しています。



- (注)** AsyncOS は着信リレーに対して SPF をサポートしていません。

有効な SPF レコードに関する注意

Cisco アプライアンスで SPF および SIDF を使用するには、RFC 4406 および 4408 に従って、SPF レコードをパブリッシュします。PRA ID の決定方法の定義については、RFC 4407 を確認してください。さらに、SPF レコードと SIDF レコードを作成する場合に犯しやすい誤りについては、次の Web サイトを参照してください。

http://www.openspf.org/FAQ/Common_mistakes

有効な SPF レコード

SPF HELO チェックに合格するには、各送信側 MTA に（ドメインとは別に）「v=spf1 a -all」 SPF レコードを含めます。このレコードを含めないと、HELO チェックは HELO ID に None 判定を下す可能性があります。ドメインへの SPF 送信側が大量の None 判定を返した場合、これらの送信側は各送信側 MTA に「v=spf1 a -all」 SPF レコードを含めていない可能性があります。

有効な SIDF レコード

SIDF フレームワークをサポートするには、「v=spf1」レコードと「spf2.0」レコードの両方をパブリッシュする必要があります。たとえば、DNS レコードは次の例のようになります。

```
example.com. TXT "v=spf1 +mx a:colo.example.com/28 -all"
```

```
smtp-out.example.com TXT "v=spf1 a -all"
```

```
example.com. TXT "spf2.0/mfrom,pra +mx a:colo.example.com/28 -all"
```

SIDF は HELO ID を検証しないため、この場合、各送信側 MTA に SPF v2.0 レコードをパブリッシュする必要はありません。



(注) SIDF をサポートしない場合は、「spf2.0/pra ~all」レコードをパブリッシュします。

SPF レコードのテスト

RFC の確認に加えて、Cisco アプライアンスに SPF 検証を実装する前に、SPF レコードをテストすることを推奨します。openspf.org Web サイトでは、いくつかのテスト ツールが提供されています。

<http://www.openspf.org/Tools>

次のツールを使用して、電子メールが SPF レコード チェックに失敗した理由を判断できます。

<http://www.openspf.org/Why>

さらに、テストリスナーで SPF をイネーブルにし、シスコの trace CLI コマンドを使用して（または GUI からトレースを実行して）、SPF 結果を表示できます。トレースを使用すると、さまざまな送信側 IP を簡単にテストできます。

SPF/SIDF を使用して受信メッセージの確認方法

表 17-2 SPF/SIDF を使用して受信メッセージの確認方法

	操作内容	詳細
ステップ 1	(任意) SPF/SIDF を使用して受信メッセージの確認に使用されるカスタムのメールフローポリシーを作成します。	「メールフローポリシーを使用した着信メッセージのルールの定義」(P.7-15)
ステップ 2	SPF/SIDF を使用して受信メッセージの確認にメールフローポリシーを設定します。	「SPF と SIDF のイネーブル化」(P.17-22)
ステップ 3	電子メールセキュリティアプライアンスが確認されたメッセージで実行するアクションを定義します。	「SPF/SIDF 検証済みメールに対して実行するアクションの決定」(P.17-29)
ステップ 4	特定の送信者または受信者のグループにアクションを関連付けます。	「メールポリシーの設定」(P.10-6)
ステップ 5	(任意) メッセージの検証の結果をテストします。	「SPF/SIDF 結果のテスト」(P.17-32)



警告

シスコでは、グローバルな電子メール認証を強く奨励していますが、業界での採用途上にある現時点では、SPF/SIDF 認証の失敗に対して慎重な処理を行うよう提案しています。さらに多くの組織で社内公認のメール送信インフラストラクチャの制御能力が向上するまでは、シスコは電子メールのパウンスを回避し、代わりに SPF/SIDF 検証に失敗した電子メールを隔離できます。



(注)

AysncOS コマンドライン インターフェイス (CLI) では、Web インターフェイスよりも詳細な SPF レベルの制御設定を提供しています。SPF 判定に基づいて、アプライアンスは、リスナー単位で SMTP 会話においてメッセージを許可または拒否できます。listenerconfig コマンドを使用して、リスナーのホスト アクセス テーブルのデフォルトの設定を編集する場合、SPF 設定を変更できます。設定の詳細については、「CLI を使用した SPF および SIDF のイネーブル化」(P.17-23) を参照してください。

SPF と SIDF のイネーブル化

SPF/SIDF を使用するには、受信リスナーでメールフローポリシーの SPF/SIDF をイネーブルにする必要があります。デフォルトのメールフローポリシーから、リスナーで SPF/SIDF をイネーブルにするか、特定の受信メールポリシーについて SPF/SIDF をイネーブルにすることができます。

手順

- ステップ 1 [メールポリシー (Mail Policies)] > [メールフローポリシー (Mail Flow Policy)] を選択します。
- ステップ 2 [デフォルトポリシーパラメータ (Default Policy Parameters)] をクリックします。
- ステップ 3 デフォルトのポリシーパラメータで、[セキュリティサービス (Security Features)] セクションを表示します。
- ステップ 4 [SPF/SIDF 検証 (SPF/SIDF Verification)] セクションで、[オン (On)] をクリックします。

- ステップ 5** 準拠のレベルを設定します（デフォルトは SIDF 互換）。このオプションを使用して、使用する SPF または SIDF 検証の規格を判断できます。SIDF 準拠に加えて、SPF と SIDF を組み合わせた SIDF 互換を選択できます。

表 17-3 SPF/SIDF 準拠レベル

準拠レベル	説明
SPF	SPF/SIDF 検証は RFC4408 に従って動作します。 - PRA (Purported Responsible Address) ID 検証は行われません。 注 ：HELO ID に対してテストするには、この準拠オプションを選択します。
SIDF	SPF/SIDF 検証は RFC4406 に従って動作します。 - PRA ID は規格への完全準拠によって判断されます。 - SPF v1.0 レコードは spf2.0/mfrom,pra として扱われます。 - 存在しないドメインや形式が誤った ID については、Fail の判定が返されます。
SIDF 互換 (SIDF Compatible)	SPF/SIDF 検証は、次の違いを除き、RFC4406 に従って動作します。 - SPF v1.0 レコードは spf2.0/mfrom として扱われます。 - 存在しないドメインや形式が誤った ID については、None の判定が返されます。 注 ：この準拠オプションは、OpenSPF コミュニティ (www.openspf.org) の要求に応じて導入されました。



(注) CLI からはさらに多くの設定を使用できます。詳細については、「[CLI を使用した SPF および SIDF のイネーブル化](#)」(P.17-23) を参照してください。

- ステップ 6** SIDF 互換の準拠レベルを選択した場合、メッセージに Resent-Sender: または Resent-From: ヘッダーが存在する場合に、検証で PRA ID の Pass 結果を None にダウングレードするかどうかを設定します。このオプションをセキュリティ目的で選択できます。
- ステップ 7** SPF の準拠レベルを選択した場合、HELO ID に対してテストを実行するかどうかを設定します。このオプションを使用して、HELO チェックをディセーブルにすることによって、パフォーマンスが向上することがあります。これは、spf-passed フィルタ ルールで、PRA または MAIL FROM ID が最初にチェックされるため、便利な場合があります。アプライアンスは SPF 準拠レベルに対してのみ HELO チェックを実行します。

CLI を使用した SPF および SIDF のイネーブル化

AsyncOS CLI では各 SPF/SIDF 準拠レベルのより詳細な制御設定をサポートしています。リスナーのホスト アクセス テーブルのデフォルトの設定をする場合、リスナーの SPF/SIDF 準拠レベルと、アプライアンスが SPF/SIDF 検証結果に基づいて実行する SMTP アクション (ACCEPT または REJECT) を選択できます。アプライアンスがメッセージを拒否する場合に送信する SMTP 応答を定義することもできます。

準拠レベルに応じて、アプライアンスは HELO ID、MAIL FROM ID、または PRA ID に対してチェックを実行します。アプライアンスが、次の各 ID チェックの各 SPF/SIDF 検証結果に対し、セッションを続行する (ACCEPT) か、セッションを終了する (REJECT) かを指定できます。

- **[None]**。情報の不足のため、検証を実行できません。
- **[Neutral]**。ドメイン所有者は、クライアントに指定された ID を使用する権限があるかどうかをアサートしません。
- **[SoftFail]**。ドメイン所有者は、ホストが指定された ID を使用する権限がないと思うが、断言を避けたいと考えています。
- **[Fail]**。クライアントは、指定された ID でメールを送信する権限がありません。
- **[TempError]**。検証中に一時的なエラーが発生しました。
- **[Permerror]**。検証中に永続的なエラーが発生しました。

アプライアンスは、メッセージに **Resent-Sender:** または **Resent-From:** ヘッダーが存在する場合に、PRA ID の **Pass** 結果を **None** にダウングレードするように **SIDF** 互換準拠レベルを設定していない限り、**Pass** 結果のメッセージを受け入れます。アプライアンスは **PRA** チェックで **None** が返された場合に指定された **SMTP** アクションを実行します。

ID チェックに対して **SMTP** アクションを定義していない場合、アプライアンスは **Fail** を含むすべての検証結果を自動的に受け入れます。

イネーブルにされたいずれかの ID チェックの ID 検証結果が **REJECT** アクションに一致する場合、アプライアンスはセッションを終了します。たとえば、管理者は、すべての **HELO ID** チェック結果に基づいてメッセージを受け入れるようにリスナーを設定しますが、**MAIL FROM ID** チェックからの **Fail** 結果に対してはメッセージを拒否するようにリスナーを設定するとします。メッセージが **HELO ID** チェックに失敗しても、アプライアンスはその結果を受け入れるため、セッションが続行します。次に、メッセージが **MAIL FROM ID** チェックで失敗した場合、リスナーはセッションを終了し、**REJECT** アクションの **SMTP** 応答を返します。

SMTP 応答は、アプライアンスが **SPF/SIDF** 検証結果に基づいてメッセージを拒否する場合に返すコード番号とメッセージです。**TempError** 結果は、他の検証結果と異なる **SMTP** 応答を返します。

TempError の場合、デフォルトの応答コードは 451 で、デフォルトのメッセージテキストは「#4.4.3 Temporary error occurred during SPF verification」です。他のすべての検証結果の場合のデフォルトの応答コードは 550 で、デフォルトのメッセージテキストは「#5.7.1 SPF unauthorized mail is prohibited」です。**TempError** や他の検証結果に独自の応答コードとメッセージテキストを指定できます。

任意で、**Neutral**、**SoftFail**、または **Fail** 検証結果に対して **REJECT** アクションが実行された場合に、**SPF** パブリッシュドメインから、サードパーティの応答を返すように、アプライアンスを設定することができます。デフォルトで、アプライアンスは次の応答を返します。

```
550-#5.7.1 SPF unauthorized mail is prohibited.
```

```
550-The domain example.com explains:
```

```
550 <Response text from SPF domain publisher>
```

これらの **SPF/SIDF** 設定をイネーブルにするには、`listenerconfig -> edit` サブコマンドを使用し、リスナーを選択します。次に、`hostaccess -> default` サブコマンドを使用して、ホストアクセステーブルのデフォルトの設定を編集します。次のプロンプトに **yes** と答えて、**SPF** 制御を設定します。

```
Would you like to change SPF/SIDF settings? [N]> yes
```

```
Would you like to perform SPF/SIDF Verification? [Y]> yes
```

ホスト アクセス テーブルでは、次の SPF 制御設定を使用できます。

表 17-4 CLI を使用した SPF 制御設定

準拠レベル	使用可能な SPF 制御設定
SPF のみ (SPF Only)	<ul style="list-style-type: none"> • HELO ID チェックを実行するかどうか • 次の ID チェックの結果に基づいて実行される SMTP アクション <ul style="list-style-type: none"> – HELO ID (イネーブルの場合) – MAIL FROM ID • REJECT アクションに対して返される SMTP 応答コードとテキスト • 秒単位の検証タイムアウト
SIDF 互換 (SIDF Compatible)	<ul style="list-style-type: none"> • HELO ID チェックを実行するかどうか • メッセージに Resent-Sender: または Resent-From: ヘッダーが存在する場合に、検証で PRA ID の Pass 結果を None にダウングレードするかどうか • 次の ID チェックの結果に基づいて実行される SMTP アクション <ul style="list-style-type: none"> – HELO ID (イネーブルの場合) – MAIL FROM ID – PRA Identity • REJECT アクションに対して返される SMTP 応答コードとテキスト • 秒単位の検証タイムアウト
SIDF 厳格 (SIDF Strict)	<ul style="list-style-type: none"> • 次の ID チェックの結果に基づいて実行される SMTP アクション <ul style="list-style-type: none"> – MAIL FROM ID – PRA Identity • SPF REJECT アクションの場合に返される SMTP 応答コードとテキスト • 秒単位の検証タイムアウト

次に、ユーザが SPF Only 準拠レベルを使用して、SPF/SIDF 検証を設定する例を示します。アプライアンスは HELO ID チェックを実行し、None および Neutral 検証結果を受け入れ、その他の結果を拒否します。SMTP アクションの CLI プロンプトはすべての ID タイプで同じです。ユーザは MAIL FROM ID の SMTP アクションを定義しません。アプライアンスは、その ID のすべての検証結果を自動的に受け入れます。アプライアンスはすべての REJECT 結果に対して、デフォルトの拒否コードとテキストを使用します。

```
Would you like to change SPF/SIDF settings? [N]> yes
```

```
Would you like to perform SPF/SIDF Verification? [N]> yes
```

What Conformance Level would you like to use?

1. SPF only
2. SIDF compatible
3. SIDF strict

[2]> **1**

Would you like to have the HELO check performed? [Y]> **y**

Would you like to change SMTP actions taken as result of the SPF verification? [N]> **y**

Would you like to change SMTP actions taken for the HELO identity? [N]> **y**

What SMTP action should be taken if HELO check returns None?

1. Accept
2. Reject

[1]> **1**

What SMTP action should be taken if HELO check returns Neutral?

1. Accept
2. Reject

[1]> **1**

What SMTP action should be taken if HELO check returns SoftFail?

1. Accept
2. Reject

[1]> **2**

What SMTP action should be taken if HELO check returns Fail?

1. Accept

2. Reject

[1]> 2

What SMTP action should be taken if HELO check returns TempError?

1. Accept

2. Reject

[1]> 2

What SMTP action should be taken if HELO check returns PermError?

1. Accept

2. Reject

[1]> 2

Would you like to change SMTP actions taken for the MAIL FROM identity? [N]> n

Would you like to change SMTP response settings for the REJECT action? [N]> n

Verification timeout (seconds)

[40]>

次に、リスナーのデフォルトのポリシー パラメータに SPF/SIDF 設定がどのように表示されるかを示します。

SPF/SIDF Verification Enabled: Yes

Conformance Level: SPF only

Do HELO test: Yes

SMTP actions:

For HELO Identity:

None, Neutral: Accept

```

SoftFail, Fail, TempError, PermError: Reject

For MAIL FROM Identity: Accept

SMTP Response Settings:

Reject code: 550

Reject text: #5.7.1 SPF unauthorized mail is prohibited.

Get reject response text from publisher: Yes

Defer code: 451

Defer text: #4.4.3 Temporary error occurred during SPF verification.

Verification timeout: 40

```

listenerconfig コマンドの詳細については、『Cisco AsyncOS CLI Reference Guide』を参照してください。

Received-SPF ヘッダー

AsyncOS で SPF/SIDF 検証を設定すると、電子メールに SPF/SIDF 検証ヘッダー (Received-SPF) が配置されます。さらに、Received-SPF ヘッダーには、次の情報が含まれます。

- **検証結果** : SPF 検証結果 (「[検証結果](#)」(P.17-29) を参照してください)。
- **ID** : SPF 検証でチェックされた ID : HELO、MAIL FROM、PRA。
- **レシーバ** : 検証するホスト名 (チェックを実行する)。
- **クライアント IP アドレス** : SMTP クライアントの IP アドレス。
- **ENVELOPE FROM** : エンベロープ送信者メールボックス。(MAIL FROM ID は空にすることができないため、これは、MAIL FROM ID と異なることがあります)。
- **x-sender** : HELO、MAIL FROM、または PRA ID の値。
- **x-conformance** : 準拠のレベル (「[表 17-3SPF/SIDF 準拠レベル](#)」(P.17-23) を参照) と PRA チェックのダウングレードが実行されたかどうか。

次の例に、SPF/SIDF チェックに合格したメッセージに追加されるヘッダーを示します。

```

Received-SPF: Pass identity=pra; receiver=box.example.com;

client-ip=1.2.3.4; envelope-from="alice@foo.com";

x-sender="alice@company.com"; x-conformance=sidf_compatible

```



(注)

spf-status および spf-passed フィルタ ルールでは、received-SPF ヘッダーを使用して、SPF/SIDF 検証の状態が判断されます。

SPF/SIDF 検証済みメールに対して実行するアクションの決定

SPF/SIDF 検証されたメールを受信する場合、SPF/SIDF 検証の結果によって異なるアクションを実行することが必要になる場合があります。次のメッセージおよびコンテンツ フィルタ ルールを使用して、SPF/SIDF 検証済みメールの状態を判断し、検証結果に基づいてメッセージへのアクションを実行できます。

- `spf-status`。このフィルタ ルールは SPF/SIDF 状態に基づいてアクションを決定します。有効な SPF/SIDF 戻り値ごとに異なるアクションを入力できます。
- `spf-passed`。このフィルタ ルールは SPF/SIDF 結果をブール値として一般化します。



(注) `spf-passed` フィルタ ルールはメッセージ フィルタでのみ使用できます。

より詳細な結果に対処する必要がある場合は、`spf-status` ルールを使用し、簡単なブール値を作成する必要がある場合は `spf-passed` ルールを使用できます。

検証結果

`spf-status` フィルタ ルールを使用する場合、次の構文を使用して、SPF/SIDF 検証結果に対してチェックできます。

```
if (spf-status == "Pass")
```

1 つの条件で複数の状態判定に対してチェックする場合、次の構文を使用できます。

```
if (spf-status == "PermError, TempError")
```

さらに、次の構文を使用して、HELO、MAIL FROM、PRA ID に対して検証結果をチェックすることもできます。

```
if (spf-status("pra") == "Fail")
```



(注) `spf-status` メッセージ フィルタ ルールは、HELO、MAIL FROM、PRA ID に対して結果をチェックする場合にのみ使用できます。`spf-status` コンテンツ フィルタ ルールは、ID に対してチェックする場合に使用できません。

次のいずれかの検証結果を受け取る可能性があります。

- **None** : 情報の不足のため、検証を実行できません。
- **Pass** : クライアントは、指定された ID でメールを送信する権限がありません。
- **Neutral** : ドメイン所有者は、クライアントに指定された ID を使用する権限があるかどうかをアサートしません。
- **SoftFail** : ドメイン所有者は、指定された ID を使用する権限がホストにないと思うが、断言を避けたいと考えています。

- Fail : クライアントは、指定された ID でメールを送信する権限がありません。
- TempError : 検証中に一時的なエラーが発生しました。
- PermError : 検証中に永続的なエラーが発生しました。

CLI での spf-status フィルタ ルールの使用

次の例に、spf-status メッセージ フィルタ の使用例を示します。

```
skip-spam-check-for-verified-senders:

    if (sendergroup == "TRUSTED" and spf-status == "Pass"){

        skip-spamcheck();

    }

quarantine-spf-failed-mail:

    if (spf-status("pra") == "Fail") {

        if (spf-status("mailfrom") == "Fail"){

            # completely malicious mail

            quarantine("Policy");

        } else {

            if(spf-status("mailfrom") == "SoftFail") {

                # malicious mail, but tempting

                quarantine("Policy");

            }

        }

    } else {

        if(spf-status("pra") == "SoftFail"){

            if (spf-status("mailfrom") == "Fail"

                or spf-status("mailfrom") == "SoftFail"){

                # malicious mail, but tempting

                quarantine("Policy");

            }

        }

    }

}
```

```
    }  
  }  
  
stamp-mail-with-spf-verification-error:  
  
  if (spf-status("pra") == "PermError, TempError"  
      or spf-status("mailfrom") == "PermError, TempError"  
      or spf-status("helo") == "PermError, TempError"){  
    # permanent error - stamp message subject  
  
    strip-header("Subject");  
  
    insert-header("Subject", "[POTENTIAL PHISHING] $Subject"); }  
.
```

GUI での spf-status コンテンツ フィルタ ルール

GUI でコンテンツ フィルタから spf-status ルールをイネーブルにすることもできます。ただし、spf-status コンテンツ フィルタ ルールを使用した場合、HELO、MAIL FROM、PRA ID に対して結果をチェックできません。

GUI から spf-status コンテンツ フィルタ ルールを追加するには、[メール ポリシー (Mail Policies)] > [受信コンテンツ フィルタ (Incoming Content Filters)] をクリックします。次に [条件を追加 (Add Condition)] ダイアログボックスから、[SPF 検証 (SPF Verification)] フィルタ ルールを追加します。条件に、1 つ以上の検証結果を指定します。

SPF 検証条件を追加したら、SPF 状態に基づいて実行するアクションを指定します。たとえば、SPF 状態が SoftFail の場合、メッセージを隔離します。

spf-passed フィルタ ルールの使用

spf-passed ルールは SPF 検証の結果をブール値として表示します。次の例に、spf-passed とマークされていない電子メールを隔離するために使用する spf-passed ルールを示します。

```
quarantine-spf-unauthorized-mail:  
  
  if (not spf-passed) {  
  
    quarantine("Policy");  
  
  }
```



(注)

spf-status ルールと異なり spf-passed ルールは SPF/SIDF 検証値を簡単なブール値に単純化します。次の検証結果は、spf-passed ルールに合格していないものとして扱われます。None、Neutral、Softfail、TempError、PermError、Fail。より詳細な結果に基づいて、メッセージへのアクションを実行するには、spf-status ルールを使用します。

SPF/SIDF 結果のテスト

組織によって SPF/SIDF の実装方法が異なるため、SPF/SIDF 検証の結果をテストし、これらの結果を使用して、SPF/SIDF の失敗の処理方法を決定します。コンテンツ フィルタ、メッセージ フィルタ、Email Security Monitor - Content Filters レポートを組み合わせて使用し、SPF/SIDF 検証の結果をテストします。

SPF/SIDF 検証の依存度によって、SPF/SIDF 結果をテストする詳細レベルが決まります。

SPF/SIDF 結果の基本の詳細度のテスト

受信メールの SPF/SIDF 検証結果の基本評価基準を取得するため、コンテンツ フィルタと [メール セキュリティ モニタ - コンテンツ フィルタ (Email Security Monitor - Content Filters)] ページを使用できます。このテストでは、SPF/SIDF 検証結果のタイプごとに受信されたメッセージ数が表示されます。

手順

- ステップ 1** 受信リスナーで、メール フロー ポリシーの SPF/SIDF 検証をイネーブルにし、コンテンツ フィルタを使用して、実行するアクションを設定します。SPF/SIDF をイネーブルにする方法については、「[SPF と SIDF のイネーブル化](#)」(P.17-22) を参照してください。
- ステップ 2** SPF/SIDF 検証のタイプごとに spf-status コンテンツ フィルタを作成します。命名規則を使用して、検証のタイプを示します。たとえば、SPF/SIDF 検証に合格したメッセージには「SPF-Passed」を使用し、検証中の一時的エラーのために合格しなかったメッセージには、「SPF-TempErr」を使用します。spf-status コンテンツ フィルタの作成については、「[GUI での spf-status コンテンツ フィルタ ルール](#)」(P.17-31) を参照してください。
- ステップ 3** 多数の SPF/SIDF 検証済みメッセージの処理後、[モニタ (Monitor)] > [コンテンツ フィルタ (Content Filters)] をクリックして、各 SPF/SIDF 検証済みコンテンツ フィルタをトリガーしたメッセージ数を確認します。

SPF/SIDF 結果の高い詳細度のテスト

SPF/SIDF 検証結果のより包括的な情報を得るには、送信者の特定のグループの SPF/SIDF 検証をイネーブルにし、それらの特定の送信者の結果を確認するだけです。次に、その特定のグループのメールポリシーを作成し、メールポリシーで SPF/SIDF 検証をイネーブルにします。「[SPF/SIDF 結果の基本の詳細度のテスト](#)」(P.17-32) で説明するように、コンテンツ フィルタを作成し、Content Filters レポートを確認します。検証が有効であることがわかったら、この指定した送信者のグループの電子メールをドロップするかバウンスするかの決断の基準として、SPF/SIDF 検証を使用できます。

手順

- ステップ 1** SPF/SIDF 検証のメールフローポリシーを作成します。受信リスナーで、メールフローポリシーの SPF/SIDF 検証をイネーブルにします。SPF/SIDF をイネーブルにする方法については、「[SPF と SIDF のイネーブル化](#)」(P.17-22) を参照してください。
- ステップ 2** SPF/SIDF 検証の送信者グループを作成し、命名規則を使用して、SPF/SIDF 検証を示します。送信者グループの作成については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「[Configuring the Gateway to Receive Mail](#)」の章を参照してください。
- ステップ 3** SPF/SIDF 検証のタイプごとに `spf-status` コンテンツ フィルタを作成します。命名規則を使用して、検証のタイプを示します。たとえば、SPF/SIDF 検証に合格したメッセージには「SPF-Passed」を使用し、検証中の一時的エラーのために合格しなかったメッセージには、「SPF-TempErr」を使用します。`spf-status` コンテンツ フィルタの作成については、「[GUI での spf-status コンテンツ フィルタ ルール](#)」(P.17-31) を参照してください。
- ステップ 4** 多数の SPF/SIDF 検証済みメッセージの処理後、[モニタ (Monitor)] > [コンテンツ フィルタ (Content Filters)] をクリックして、各 SPF/SIDF 検証済みコンテンツ フィルタをトリガーしたメッセージ数を確認します。
-



CHAPTER 18

テキスト リソース

- 「テキスト リソースの概要」 (P.18-1)
- 「コンテンツ ディクショナリ」 (P.18-2)
- 「ディクショナリの追加」 (P.18-4)
- 「コンテンツ ディクショナリ フィルタ ルールの使用方法およびテスト方法」 (P.18-6)
- 「テキスト リソースについて」 (P.18-8)
- 「テキスト リソース管理の概要」 (P.18-9)
- 「テキスト リソースの使用」 (P.18-12)

テキスト リソースの概要

この章では、コンテンツ ディクショナリ、免責事項、およびテンプレートなどのさまざまなテキスト リソースの作成および管理について説明します。

関連項目

- 「機密 DLP 用語 (カスタム DLP ポリシーのみ) のカスタム ディクショナリの使用」 (P.15-16)

コンテンツ ディクショナリ

コンテンツ ディクショナリを使用して、企業のポリシーに沿った適切なアクションを実行できるようにメッセージまたはコンテンツ フィルタに対してメッセージをスキャンできます。ディクショナリの作成、削除、および表示、ディクショナリからのエントリの追加または削除、およびディクショナリ全体のインポートまたはエクスポートができます。ディクショナリごとに、大文字と小文字の区別および単語の区切りの検出方法を決定することもできます。たとえば、機密性の高い単語や野卑な単語のリストを作成し、フィルタ ルールを使用してリスト内の単語に対してメッセージをスキャンし、一致する単語を含むメッセージをドロップまたはアーカイブできます。また、単語によってフィルタ アクションをより簡単にトリガーできるように、ディクショナリに「重み」の条件を追加できます。

ディクショナリには、非 ASCII 文字を含めることができます。

テキストリソース

テキストリソースは、免責事項、通知テンプレート、アンチウイルステンプレートなどのテキストオブジェクトです。AsyncOS のさまざまなコンポーネントで使用できる新規オブジェクトを作成できます。テキストリソースをインポートおよびエクスポートできます。

メッセージの免責事項スタンプ

メッセージの免責事項スタンプを使用すると、免責事項のテキストリソースをメッセージに追加できます。たとえば、企業内から送信される各メッセージに著作権宣言文、宣伝メッセージ、または免責事項を付加できます。

コンテンツディクショナリ

コンテンツディクショナリは、アプライアンスの本文スキャン機能と連携して動作する単語またはエントリのグループであり、コンテンツフィルタおよびメッセージフィルタの両方に利用できます。定義したディクショナリを使用し、ディクショナリに含まれる単語に対してメッセージ、メッセージヘッダー、およびメッセージの添付ファイルをスキャンすることで、企業のポリシーに沿った適切なアクションを実行できます。たとえば、機密性の高い単語や野卑な単語のリストを作成し、フィルタルールを使用してリスト内の単語を含むメッセージをスキャンし、メッセージをドロップ、アーカイブ、または隔離できます。

AsyncOS オペレーティングシステムには、GUI ([メールポリシー (Mail Policies)] > [辞書 (Dictionaries)]) または CLI の `dictionaryconfig` コマンドを使用して、合計 100 個のコンテンツディクショナリを定義する能力があります。ディクショナリの作成、削除、および表示、ディクショナリからのエントリの追加または削除、およびディクショナリ全体のインポートまたはエクスポートができます。

ディクショナリの内容

ディクショナリの単語は 1 行につき 1 つのテキスト文字列で作成し、エントリはプレーンテキストまたは正規表現の形式で記載できます。ディクショナリには、非 ASCII 文字を含めることもできます。正規表現のディクショナリを定義すると、より柔軟に単語を照合させることができます。ただし、このためには適切に単語を区切る方法を理解する必要があります。Python スタイルの正規表現の詳細については、次の URL からアクセスできる「Python Regular Expression HOWTO」を参考にしてください。

<http://www.python.org/doc/howto/>



(注)

ディクショナリのエントリの最初に特殊文字 # を使用すると、文字クラス [#] をコメントとして扱われることなく使用できます。

単語によってフィルタ条件をより簡単にトリガーできるように、各単語に「重み」を指定できます。AsyncOS では、コンテンツディクショナリの単語に対してメッセージをスキャンし、単語インスタンスの数に単語の重みを掛けることでメッセージのスコアを付けます。2 つの単語インスタンスに 3 の重みが付いている場合、スコアは 6 になります。AsyncOS は、このスコアをコンテンツフィルタまたはメッセージフィルタに関連するしきい値と比較し、メッセージがフィルタアクションをトリガーするかどうかを決定します。

コンテンツ デictionary にスマート ID を追加することもできます。スマート ID は、社会保障番号や ABA ルーティング番号など共通の数字パターンに一致するパターンをデータ内から検索するアルゴリズムです。これらの ID はポリシーの拡張に便利です。正規表現の詳細については、『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「Using Message Filters to Enforce Email Policies」の章にある「Regular Expressions in Rules」を参照してください。スマート ID の詳細については、『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「Using Message Filters to Enforce Email Policies」の章にある「Smart Identifiers」を参照してください。



(注)

端末の CLI に非 ASCII 文字を含む dictionary が正しく表示される場合とされない場合があります。非 ASCII 文字を含む dictionary を表示および変更する最適な方法は、dictionary をテキストファイルにエクスポートし、テキスト ファイルを編集して、新しいファイルを再びアプライアンスにインポートする方法です。詳細については、「[テキスト ファイルとして dictionary をインポートおよびエクスポートする方法](#)」(P.18-3) を参照してください。

単語境界と 2 バイト文字セット

一部の言語 (2 バイト文字セット) では、単語または単語の区切りに関する概念や、大文字/小文字がありません。単語を構成する文字 (正規表現で「\w」と表される文字) の識別などが必要になる複雑な正規表現では、ロケールが不明な場合、またはエンコードが不明な場合、問題が発生します。この理由から、単語境界の拡張をディセーブルにできます。

テキスト ファイルとして dictionary をインポートおよびエクスポートする方法

コンテンツ デictionary 機能には、デフォルトでアプライアンスの configuration ディレクトリに配置されている次のテキスト ファイルが含まれます。

- config.dtd
- profanity.txt
- proprietary_content.txt
- sexual_content.txt

これらのテキスト ファイルは、コンテンツ デictionary 機能と組み合わせて使用することで、新規 dictionary の作成をサポートすることを目的としています。これらのコンテンツ デictionary は重み付けされており、スマート ID を使用することでデータ内のパターンを高い精度で検出し、コンプライアンスの問題となるパターンの場合にはフィルタをトリガーします。



(注)

dictionary をインポートおよびエクスポートする場合は、完全に一致する単語の設定と大文字と小文字を区別する設定が保持されません。この設定は、設定ファイルにのみ保持されます。

configuration ディレクトリへのアクセスの詳細については、[付録 A 「アプライアンスへのアクセス」](#)を参照してください。

ユーザ独自の dictionary ファイルを作成して、アプライアンスにインポートすることもできます。非 ASCII 文字を dictionary に追加する最適な方法は、アプライアンス以外の場所でテキストファイルの dictionary に単語を追加し、アプライアンス上にファイルを移動してから新しい dictionary としてファイルをインポートする方法です。dictionary のインポートの詳細については、「[dictionary のインポート](#)」(P.18-5) を参照してください。dictionary のエクスポートについては、「[dictionary のエクスポート](#)」(P.18-6) を参照してください。



警告

これらのテキスト ファイルには、一部の人の間では卑猥、下品または不快に感じられる単語が含まれています。これらのファイルからコンテンツ ディクショナリに単語をインポートした場合、アプライアンスに設定したコンテンツ ディクショナリを後で閲覧する際にこれらの単語が表示されます。

ディクショナリの追加

手順

ステップ 1 [メール ポリシー (Mail Policies)] > [辞書 (Dictionaries)] ページに移動します。

ステップ 2 [辞書を追加 (Add Dictionary)] をクリックします。

ステップ 3 ディクショナリの名前を入力します。

ステップ 4 (任意) 高度なマッチングを設定します。



(注) AsyncOS は、設定ファイルに保存する際に、[単語全体的一致 (Match Whole Words)] と [大文字小文字を区別 (Case Sensitive)] の設定を保持します。ディクショナリをインポートおよびエクスポートするときは、AsyncOS はこれらの設定は保持しません。

ステップ 5 (任意) ディクショナリにスマート ID を追加します。

スマート ID は、社会保障番号や ABA ルーティング番号など共通の数字パターンに一致するパターンをデータ内から検索するアルゴリズムです。スマート ID の詳細については、『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「Using Message Filters to Enforce Email Policies」の章を参照してください。

ステップ 6 新規ディクショナリのエントリを単語のリストに入力します。

追加する複数の新しいエントリがあり、フィルタ アクションを同じ様にトリガーにする場合は、1 行につき 1 つずつ新しい語を入力します。



(注) 正規表現「.*」をエントリの最初または最後に使用したコンテンツ ディクショナリのエントリがあると、その「単語」に一致する MIME パートが見つかった場合にシステムがロックされます。ディクショナリのエントリの最初または最後に「.*」を使用しないことを推奨します。

ステップ 7 単語に対する重みを指定します。

フィルタ アクションを他の単語よりトリガーしやすくなるように、ディクショナリの単語に「重み」を付けられます。この重みがフィルタ アクションの決定に使用される仕組みの詳細については、『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「Using Message Filters to Enforce Email Policies」の章にある「Threshold Scoring for Content Dictionaries」を参照してください。

ステップ 8 [追加 (Add)] をクリックします。

ステップ 9 変更内容を送信し、確定します。

関連項目

- 「ディクショナリの内容」(P.18-2)

デクショナリの削除

はじめる前に

AsyncOS は、削除されたデクショナリを参照しているすべてのメッセージ フィルタを無効としてマークすることに注意してください。AsyncOS は削除されたデクショナリを参照しているすべてのコンテンツ フィルタをイネーブルのままにしますが、今後無効と判断します。

手順

-
- ステップ 1** [メール ポリシー (Mail Policies)] > [辞書 (Dictionaries)] ページに移動します。
 - ステップ 2** デクショナリの横にあるゴミ箱アイコンをクリックして、デクショナリのリストから削除します。確認メッセージには、デクショナリを現在参照しているフィルタがすべて表示されます。
 - ステップ 3** 確認メッセージで [削除 (Delete)] をクリックします。
 - ステップ 4** 変更内容を確定します。
-

デクショナリのインポート

はじめる前に

インポートするファイルが、アプライアンスの `configuration` ディレクトリに存在することを確認します。

手順

-
- ステップ 1** [メール ポリシー (Mail Policies)] > [辞書 (Dictionaries)] ページに移動します。
 - ステップ 2** [辞書をインポート (Import Dictionary)] をクリックします。
 - ステップ 3** インポート元の場所を選択します。
 - ステップ 4** インポートするファイルを選択します。
 - ステップ 5** デクショナリの単語に使用するデフォルトの重みを選択します。
AsyncOS では、重みが指定されていない単語に対してデフォルトの重みを割り当てます。ファイルのインポート後に重みを編集できます。
 - ステップ 6** エンコード方式を選択します。
 - ステップ 7** [次へ (Next)] をクリックします。
 - ステップ 8** デクショナリの名前を指定し、編集します。
 - ステップ 9** 変更内容を送信し、確定します。
-

Dictionary のエクスポート

手順

-
- ステップ 1** [メール ポリシー (Mail Policies)] > [辞書 (Dictionaries)] ページに移動します。
- ステップ 2** [辞書をエクスポート (Export Dictionary)] をクリックします。
- ステップ 3** エクスポートする Dictionary を選択します。
- ステップ 4** エクスポートされた Dictionary のファイル名を入力します。
これは、アプライアンスの設定ディレクトリに作成されるファイルの名前になります。
- ステップ 5** エクスポート先の場所を選択します。
- ステップ 6** テキスト ファイルのエンコード方式を選択します。
- ステップ 7** 変更内容を送信し、確定します。
-

コンテンツ Dictionary フィルタ ルールの使用方法およびテスト方法

Dictionary は、さまざまな `dictionary-match()` メッセージ フィルタ ルールおよびコンテンツ フィルタ に使用できます。

Dictionary の照合 フィルタ ルール

メッセージ フィルタ ルール (`dictionary-match(<dictionary_name>)`) (および同様のルール) は、メッセージの本文にコンテンツ Dictionary (`dictionary_name`) に存在するいずれかの正規表現が含まれる場合に有効と判断されます。該当の Dictionary が存在しない場合は、ルールは無効と判断されます。

`dictionary-match()` ルールは、`body-contains()` 本文スキャン ルールと同様にメッセージ本文と添付ファイルのみをスキャンし、ヘッダーをスキャンしないことに注意してください。

ヘッダーのスキャンには、適切な `*-dictionary-match()` タイプのルールを使用できます (`subject-dictionary-match()` や、より一般的なルールでカスタム ヘッダーを含むすべてのヘッダーを指定できる `header-dictionary-match()` など、特定のヘッダーに対するルールが存在します)。Dictionary の照合の詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Using Message Filters to Enforce Email Policies」の章にある「Dictionary Rules」を参照してください。

表 18-1 コンテンツ Dictionary のメッセージ フィルタ ルール

ルール	構文	説明
Dictionary 照合	<code>dictionary-match(<dictionary_name>)</code>	指定した Dictionary に存在するすべての正規表現に一致した単語がメッセージに含まれているか。

次の例では `dictionary-match()` ルールを使用して、Cisco アプライアンスが（前回の例で作成した）「`secret_words`」という名前のディクショナリ内の単語を含むメッセージをスキャンした際に、管理者にメッセージをブラインドカーボンコピーで送信する新規メッセージフィルタが作成されます。設定値によっては、大文字/小文字も含めて「`codename`」と完全に一致する単語を含むメッセージのみが、このフィルタで有効と判断されることに注意してください。

```
bcc_codenames:

    if (dictionary-match ('secret_words'))

        {

            bcc('administrator@example.com');

        }
```

この例では、Policy 隔離にメッセージを送信します。

```
quarantine_codenames:

    if (dictionary-match ('secret_words'))

        {

            quarantine('Policy');

        }
```

ディクショナリ エントリの例

表 18-2 ディクショナリ エントリの例

説明	例 :
ワイルドカード	*
アンカー	最後で使用する場合 : <code>foo\$</code> 先頭で使用する場合 : <code>^foo</code>
電子メール アドレス (ピリオドをエスケープしないこと)	<code>foo@example.com</code> , <code>@example.com</code> <code>example.com\$</code> (最後で使用する場合) <code>@example.*</code>
件名	An email subject (電子メールの件名に ^ アンカーを使用する際は、件名の先頭に「RE:」や「FW:」などが多く付いていることを覚えておいてください)

コンテンツ ディクショナリのテスト方法

`trace` 機能を使用すると、`dictionary-match()` ルールを使用しているメッセージフィルタに対して迅速なフィードバックが得られます。詳細については、「[テストメッセージを使用したメールフローのデバッグ : トレース](#)」(P.36-1)を参照してください。上記の `quarantine_codenames` フィルタの例のように、`quarantine()` アクションを使用してフィルタをテストすることもできます。

テキスト リソースについて

テキスト リソースは、メッセージへの添付や、メッセージとしての送信が可能なテキスト テンプレートです。テキスト リソースは、次のいずれかの種類になります。

- **メッセージ免責事項**：メッセージに追加されるテキスト。詳細については、「[免責事項テンプレート](#)」(P.18-12) を参照してください。
- **通知テンプレート**：通知として送信されるメッセージ (`notify()` および `notify-bcc()` アクションで使用されます)。詳細については、「[通知テンプレート](#)」(P.18-19) を参照してください。
- **アンチウイルス通知テンプレート**：メッセージにウイルスが見つかったときに、通知として送信されるメッセージ。コンテナ用のテンプレート (元のメッセージに付加)、またはメッセージに付加せず通知として送信されるテンプレートを作成できます。詳細については、「[アンチウイルス通知テンプレート](#)」(P.18-20) を参照してください。
- **バウンスおよび暗号化失敗通知テンプレート**：メッセージがバウンスされたときやメッセージの暗号化に失敗したときに通知として送信されるメッセージ。詳細については、「[バウンス通知および暗号化失敗通知テンプレート](#)」(P.18-22) を参照してください。
- **暗号化通知テンプレート**：発信電子メールを暗号化するように Cisco アプライアンスを設定した場合に送信されるメッセージ。このメッセージは、受信者が暗号化されたメッセージを受信したことを受信者に通知し、メッセージを読む手順を示します。詳細については、「[暗号化通知テンプレート](#)」(P.18-23) を参照してください。

CLI (`textconfig`) または GUI を使用して、テキスト リソースの追加、削除、編集、インポート、およびエクスポートを含むテキスト リソースの管理ができます。GUI を使用したテキスト リソースの管理については、「[テキスト リソース管理の概要](#)」(P.18-9) を参照してください。

テキスト リソースには、非 ASCII 文字を含めることができます。



(注)

非 ASCII 文字を含むテキスト リソースは端末の CLI に正しく表示される場合とされない場合があります。非 ASCII 文字を含むテキスト リソースを表示および変更するには、テキスト リソースをテキスト ファイルにエクスポートし、テキスト ファイルを編集して、新しいファイルを再びアプライアンスにインポートします。詳細については、「[テキスト ファイルとしてテキスト リソースをインポートおよびエクスポートする](#)」(P.18-8) を参照してください。

テキスト ファイルとしてテキスト リソースをインポートおよびエクスポートする

アプライアンスの `configuration` ディレクトリに対するアクセス権を持っている必要があります。インポートするテキスト ファイルは、アプライアンス上の `configuration` ディレクトリに存在する必要があります。エクスポートされたテキスト ファイルは、`configuration` ディレクトリに配置されます。

`configuration` ディレクトリへのアクセスの詳細については、[付録 A 「アプライアンスへのアクセス」](#) を参照してください。

非 ASCII 文字をテキスト リソースに追加するには、アプライアンス以外の場所でテキスト ファイルのテキスト リソースに単語を追加し、アプライアンス上にファイルを移動し、新しいテキスト リソースとしてファイルをインポートします。テキスト リソースのインポートの詳細については、「[テキスト リソースのインポート](#)」(P.18-10) を参照してください。テキスト リソースのエクスポートについては、「[テキスト リソースのエクスポート](#)」(P.18-10) を参照してください。

テキスト リソース管理の概要

GUI または CLI を使用してテキスト リソースを管理できます。この項では、GUI について説明します。

`textconfig` コマンドを使用して CLI からテキスト リソースを管理します。

テキスト リソース管理には、次のタスクが含まれます。

- 追加
- 編集および削除
- エクスポートおよびインポート
- すべてのテキスト リソース タイプのプレーン テキスト メッセージの定義
- 一部のテキスト リソース タイプの HTML ベースのメッセージの定義

関連項目

- [「HTML ベースのテキスト リソースの概要」 \(P.18-11\)](#) .

テキスト リソースの追加

手順

-
- ステップ 1** [メール ポリシー (Mail Policies)] > [テキスト リソース (Text Resources)] に移動します。
 - ステップ 2** [テキスト リソースを追加 (Add Text Resource)] をクリックします。
 - ステップ 3** [名前 (Name)] フィールドにテキスト リソースの名前を入力します。
 - ステップ 4** [タイプ (Type)] フィールドからテキスト リソースのタイプを選択します。
 - ステップ 5** [テキスト (Text)] または [HTML およびプレーン テキスト (HTML and Plain Text)] のどちらかのフィールドに、メッセージ テキストを入力します。

テキスト リソースがプレーン テキスト メッセージのみを許可する場合は、[テキスト (Text)] フィールドを使用します。テキスト リソースが HTML およびプレーン テキスト メッセージの両方を許可する場合は、[HTML およびプレーン テキスト (HTML and Plain Text)] フィールドを使用します。
 - ステップ 6** 変更内容を送信し、確定します。
-

関連項目

- [「HTML ベースのテキスト リソースの概要」 \(P.18-11\)](#) .

テキスト リソースの削除

はじめる前に

テキスト リソースの削除の影響に注意してください。

- 削除されたテキスト リソースを参照しているすべてのメッセージ フィルタは、無効としてマークされます。

- 削除されたテキスト リソースを参照しているすべてのコンテンツ フィルタはイネーブルのままになりますが、今後無効と判断されます。

手順

-
- ステップ 1** [メール ポリシー (Mail Policies)] > [テキスト リソース (Text Resources)] ページに移動し、削除するテキスト リソースの [削除 (Delete)] 列にあるゴミ箱アイコンをクリックします。確認メッセージが表示されます。
- ステップ 2** [削除 (Delete)] をクリックして、テキスト リソースを削除します。
- ステップ 3** 変更内容を確定します。
-

テキスト リソースのインポート

はじめる前に

インポートするファイルが、アプライアンスの configuration ディレクトリに存在することを確認します。

手順

-
- ステップ 1** [メール ポリシー (Mail Policies)] > [テキスト リソース (Text Resources)] ページに移動し、[テキスト リソースのインポート (Import Text Resource)] をクリックします。
- ステップ 2** インポートするファイルを選択します。
- ステップ 3** エンコード方式を指定します。
- ステップ 4** [次へ (Next)] をクリックします。
- ステップ 5** 名前を選択し、テキスト リソース タイプを編集および選択します。
- ステップ 6** 変更内容を送信し、確定します。
-

テキスト リソースのエクスポート

はじめる前に

テキスト リソースをエクスポートする場合は、テキスト ファイルがアプライアンスの configuration ディレクトリに作成されることに注意してください。

手順

-
- ステップ 1** [メール ポリシー (Mail Policies)] > [テキスト リソース (Text Resources)] ページに移動し、[テキスト リソースのエクスポート (Export Text Resource)] をクリックします。
- ステップ 2** エクスポートするテキスト リソースを選択します。
- ステップ 3** テキスト リソースのファイル名を入力します。
- ステップ 4** テキスト ファイルのエンコード方式を選択します。
-

- ステップ 5** [送信 (Submit)] をクリックしてテキスト リソースを含むテキスト ファイルを configuration ディレクトリに作成します。

HTML ベースのテキスト リソースの概要

免責事項などの一部のテキスト リソースは、HTML ベースのメッセージおよびプレーン テキスト メッセージの両方を使用して作成できます。HTML ベースのメッセージとプレーン テキスト メッセージの両方を含むテキスト リソースが電子メール メッセージに適用された場合、HTML ベースのテキスト リソース メッセージは電子メール メッセージのテキストまたは HTML 部分に適用され、プレーン テキスト メッセージは電子メール メッセージのテキストまたはプレーン部分に適用されます。

HTML ベースのテキスト リソースを追加または編集する場合、GUI には、HTML コードを手動で記述せずにリッチ テキストの入力を可能にするリッチ テキスト編集が含まれます。

HTML ベースのテキスト リソースを追加および編集する場合は、次の点に留意してください。

- HTML バージョンに基づいて、メッセージのプレーン テキスト バージョンを自動的に生成するよう選択できます。または、プレーン テキスト バージョンを個別に定義できます。
- [コード ビュー (Code View)] ボタンをクリックすることにより、リッチ テキスト エディタと HTML コード間を切り替えることができます。
- リッチ テキスト エディタでサポートされない HTML コードを GUI で入力するには、コード ビューに切り替え、HTML コードを手動で入力します。たとえば、これは、 HTML タグを使用して外部サーバにあるイメージ ファイルへの参照を挿入する場合があります。

HTML ベースのテキスト リソースのインポートおよびエクスポート

HTML ベースのテキスト リソースをテキスト ファイルにエクスポートしたり、テキスト ファイルから HTML ベースのテキスト リソースをインポートしたりできます。HTML ベースのテキスト リソースをファイルにエクスポートする場合、ファイルにはテキスト リソースの各バージョンに対する次のセクションが含まれます。

- [html_version]
- [text_version]

これらのセクションの順序は重要ではありません。

たとえば、エクスポートされたファイルには、次のテキストが含まれることがあります。

```
[html_version]
<p>Sample <i>message.</i></p>
[text_version]
Sample message.
```

HTML ベースのテキスト リソースをエクスポートおよびインポートする場合は、次のルールとガイドラインに留意してください。

- プレーン テキスト メッセージが HTML バージョンから自動的に生成される HTML ベースのテキスト リソースをエクスポートする場合、エクスポートされたファイルには [text_version] セクションが含まれません。
- テキスト ファイルからインポートするとき、[html_version] セクション下のすべての HTML コードは作成されたテキスト リソースの HTML メッセージに変換されます (テキスト リソース タイプが HTML メッセージをサポートする場合)。同様に、[text_version] セクション下のすべてのテキストは、作成されたテキスト リソースのプレーン テキスト メッセージに変換されます。

- HTML ベースのテキスト リソースを作成するために、空の、または存在しない [html_version] セクションを含むファイルからインポートする場合、Cisco アプライアンスは [text_version] セクションのテキストを使用して HTML およびプレーンテキスト メッセージの両方を作成します。

テキスト リソースの使用

すべてのタイプのテキスト リソースは、[テキスト リソース (Text Resources)] ページまたは CLI の `textconfig` コマンドを使用して、同じ方法で作成されます。一度作成されると、各タイプで異なる使われ方をします。免責事項テンプレートおよび通知テンプレートは、フィルタおよびリスナーで使用されます。一方、アンチウイルス通知テンプレートは、メール ポリシーおよびアンチウイルス設定値で使用されます。

免責事項テンプレート

Cisco アプライアンスは、リスナーが受信した一部またはすべてのメッセージのテキストの上または下 (ヘッダーまたはフッター) にデフォルトの免責事項を追加できます。次の方法を使用して、Cisco アプライアンスでメッセージに免責事項を追加できます。

- リスナーから、GUI または `listenerconfig` コマンドを使用する方法 ([「リスナーからの免責事項テキストの追加」 \(P.18-12\)](#) を参照)。
- コンテンツ フィルタ アクション `Add Disclaimer Text` を使用する方法 ([「コンテンツ フィルタのアクション」 \(P.11-10\)](#) を参照)。
- メッセージ フィルタ アクション `add-footer()` を使用する方法 ([『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「Using Message Filters to Enforce Email Policies」の章](#) を参照)。
- データ消失防止プロファイルを使用する方法 ([「データ消失防止」 \(P.15-1\)](#) を参照)。
- メッセージの目的がフィッシングまたはマルウェアの配布である可能性があることをユーザに通知するようアウトブレイク フィルタに対してメッセージの修正を使用する方法 ([「メッセージの変更」 \(P.14-5\)](#) を参照)。このタイプの通知に追加される免責事項は、テキストの上に追加されます。

たとえば、企業内から送信される各メッセージに著作権宣言文、宣伝メッセージ、または免責事項を付加できます。

免責事項テキストを使用する前に、免責事項テンプレートを作成する必要があります。GUI の [テキスト リソース (Text Resources)] ページ ([「テキスト リソースの追加」 \(P.18-9\)](#) を参照) または `textconfig` コマンド ([『Cisco AsyncOS CLI Reference Guide』](#) を参照) を使用して、使用するテキスト文字列のセットを作成および管理します。

リスナーからの免責事項テキストの追加

免責事項テキスト リソースを作成したら、リスナーで受信するメッセージに付加するテキスト文字列を選択します。免責事項テキストをメッセージの上部または下部に追加できます。この機能は、パブリック (インバウンド) リスナーとプライベート (アウトバウンド) リスナーの両方に使用できます。

テキストおよび HTML から構成されるメッセージ (Microsoft Outlook では、このタイプのメッセージを「`multipart alternative`」と呼びます) を送信する場合、Cisco アプライアンスは、メッセージの両方の部分に免責事項をスタンプします。ただし、メッセージが署名済みのコンテンツである場合、署名が無効になるためコンテンツは変更されません。代わりに、免責事項スタンプによって「`Content-Disposition inline attachment`」と呼ばれる新規パートが作成されます。マルチパート

メッセージの詳細については、『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「Using Message Filters to Enforce Email Policies」の章にある「Message Bodies vs. Message Attachments」を参照してください。

次に、GUI からリスナーのメッセージに適用する免責事項を選択する例を示します。

図 18-1 リスナーに免責事項を含める編集
Add Listener

Listener Settings	
Name:	<input type="text"/>
Type of Listener:	<input checked="" type="radio"/> Public <input type="radio"/> Private
Interface:	Management TCP Port: 25
Bounce Profile:	Default
Disclaimer Above:	None <small>Disclaimer text will be applied above the message body.</small>
Disclaimer Below:	None <small>Disclaimer text will be applied below the message body.</small>
SMTP Authentication Profile:	None
Certificate:	System Default
▶ SMTP Address Parsing Options: Optional settings for controlling parsing in SMTP "MAIL FROM" and "RCPT TO"	
▶ Advanced: Optional settings for customizing the behavior of the Listener	
▶ LDAP Queries: No LDAP Server Profiles have been created. Profiles can be defined at System Administration ▶ LDAP	
SMTP Call-Ahead Profile:	None

フィルタからの免責事項の追加

フィルタアクション `add-footer()` またはコンテンツ フィルタ アクション「Add Disclaimer Text」を使用して、メッセージの免責事項に特定の事前定義されたテキスト文字列を付加することもできます。たとえば、次のメッセージ フィルタ ルールは、LDAP グループ「Legal」のユーザから送信されるすべてのメッセージに、`legal.disclaimer` という名前のテキスト文字列を付加します。

```
Add-Disclaimer-For-Legal-Team:

if (mail-from-group == 'Legal')
{
    add-footer('legal.disclaimer');
}
```

免責事項およびフィルタ アクション変数

メッセージ フィルタ アクション変数を使用することもできます（詳細については、『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「Using Message Filters to Enforce Email Policies」の章にある「Action Variables」を参照してください）。

免責事項テンプレートには、次の変数を使用できます。

表 18-3 アンチウイルス通知変数

変数	置き換える値
\$To	メッセージの To: ヘッダーに置き換えられます (エンベロープ受信者には置き換えられません)。
\$From	メッセージの From: ヘッダーに置き換えられます (エンベロープ送信者には置き換えられません)。
\$Subject	元のメッセージの件名に置き換えられます。
\$Date	現在の日付 (MM/DD/YYYY 形式) に置き換えられます。
\$Time	現在の時刻 (ローカル時間帯) に置き換えられます。
\$GMTimestamp	現在の時刻および日付 (GMT) に置き換えられます。電子メールメッセージの Received: 行で見られる形式と同様です。
\$MID	メッセージを識別するために内部的に使用されるメッセージ ID または「MID」に置き換えられます。RFC822「Message-Id」の値とは異なるため注意してください (「Message-Id」を取得するには \$Header を使用します)。
\$Group	メッセージのインジェクト時に、送信者が一致する送信者グループの名前に置き換えられます。送信者グループに名前がない場合は、文字列「>Unknown<」が挿入されます。
\$Policy	メッセージのインジェクト時に、送信者に適用した HAT ポリシーの名前に置き換えられます。事前に定義されているポリシー名が使用されていない場合、文字列「>Unknown<」が挿入されます。
\$Reputation	送信者の SenderBase レピュテーション スコアに置き換えられます。レピュテーション スコアがない場合は「None」に置き換えられます。
\$filenames	メッセージの添付ファイルのファイル名を示すカンマ区切りリストに置き換えられます。
\$filetypes	メッセージの添付ファイルのファイルタイプを示すカンマ区切りリストに置き換えられます。
\$filesizes	メッセージの添付ファイルのファイルサイズを示すカンマ区切りリストに置き換えられます。
\$remotehost	メッセージを Cisco アプライアンスに送信したシステムのホスト名に置き換えられます。
\$AllHeaders	メッセージヘッダーに置き換えられます。
\$EnvelopeFrom	メッセージのエンベロープ送信者 (Envelope From、<MAIL FROM>) に置き換えられます。
\$Hostname	Cisco アプライアンスのホスト名に置き換えられます。
\$header['string']	元のメッセージに一致するヘッダーが含まれる場合、引用符付きヘッダーの値に置き換えられます。二重引用符が使用される場合もあります。
\$enveloperecipients	メッセージのエンベロープ受信者すべて (Envelope To、<RCPT TO>) に置き換えられます。
\$bodysize	メッセージのサイズ (バイト単位) に置き換えられます。
\$FilterName	処理中のフィルタの名前を返します。

表 18-3 アンチウイルス通知変数 (続き)

変数	置き換える値
\$MatchedContent	スキャン フィルタ ルール (body-contains などのフィルタ ルールやコンテンツ ディクショナリを含む) をトリガーした内容を返します。
\$DLPPolicy	違反があった Email DLP ポリシーの名前に置き換えられます。
\$DLPSeverity	違反の重大度に置き換えられます。「Low」、「Medium」、「High」または「Critical」のいずれかです。
\$DLPRiskFactor	メッセージに含まれる機密性の高い情報のリスク係数 (0 ~ 100 のスコア) に置き換えられます。
\$threat_category	フィッシング、ウイルス、詐欺、マルウェアなどのアウトブレイク フィルタ脅威のタイプに置き換えられます。
\$threat_type	アウトブレイク フィルタ脅威カテゴリのサブカテゴリに置き換えられます。たとえば、チャリティ詐欺、金銭目的のフィッシング、偽の取引などがあります。
\$threat_description	アウトブレイク フィルタ脅威の説明に置き換えられます。
\$threat_level	メッセージの脅威レベル (スコア 0 ~ 5) に置き換えられます。

メッセージ フィルタ アクション変数を免責事項で使用するには、(GUI の [テキストリソース (Text Resource)] ページまたは `textconfig` コマンドから) メッセージの免責事項を作成し、変数を参照します。

```
(running textconfig command)
```

```
Enter or paste the message disclaimer here. Enter '.' on a blank line to end.
```

```
This message processed at: $Timestamp
```

```
.
```

```
Message disclaimer "legal.disclaimervar" created.
```

```
Current Text Resources:
```

1. legal.disclaimer (Message Disclaimer)
2. legal.disclaimervar (Message Disclaimer)

```
Choose the operation you want to perform:
```

- NEW - Create a new text resource.
- IMPORT - Import a text resource from a file.

```

- EXPORT - Export text resource to a file.
- PRINT - Display the content of a resource.
- EDIT - Modify a resource.
- DELETE - Remove a resource from the system.

[]>

```

```
mail3.example.com>commit
```

次に、新しい免責事項をフィルタに使用します。

```

Add-Timestamp:

if (mail-from-group == 'Legal')
{
    add-footer('legal.disclaimervar');
}

```

`add-footer()` アクションでは、フッターを **inline attachment**、**UTF-8 coded attachment**、**quoted printable attachment** として追加することで、非 ASCII テキストをサポートします。

免責事項スタンプと複数エンコード方式

AsyncOS には、異なる文字エンコード方式を含む免責事項スタンプの動作を変更するために使用される設定値が存在します。デフォルトでは、AsyncOS は電子メール メッセージの本文パート内に添付されるように、免責事項を配置します。`localeconfig` コマンド内で設定した設定値を使用して、本文パートと免責事項のエンコード方式が異なる場合の動作を設定できます。数個のパートから構成される電子メール メッセージを確認することで、この設定が理解しやすくなります。

To: joe@example.com	
From: mary@example.com	ヘッダー
Subject: Hi!	
<空自行>	
Hello!	本文パート
This message has been scanned...	最初の添付パート
Example.zip	2 番目の添付パート

最初の空白行に続くメッセージの本文には、多くの MIME パートが含まれている場合があります。多くの場合、最初のパートは「本文」または「テキスト」と呼ばれ、2 番目以降のパートは「アタッチメント」と呼ばれます。

免責事項は「アタッチメント」（上記の例）または本文の一部として、電子メールに含めることができます。

To: joe@example.com From: mary@example.com Subject: Hi!	ヘッダー
<空白行>	
Hello!	本文パート
This message has been scanned...	本文に含められた免責事項
Example.zip	最初の添付パート

一般的に、メッセージの本文と免責事項の間でエンコード方式の不一致が起こると、免責事項が本文に含まれ（インライン）個別のアタッチメントとして含まれないように、AsyncOS はメッセージ全体をメッセージの本文と同じエンコード方式でエンコードしようとします。つまり、免責事項と本文のエンコード方式が一致する場合、または免責事項のテキストに（本文の）インラインに表示できる文字が含まれている場合は、免責事項はインラインに含められます。たとえば、US-ASCII 文字のみを含む ISO-8859-1 エンコードされた免責事項が生成される可能性があります。結果的に、この免責事項は問題なく「インライン」に表示されます。

ただし、免責事項が本文と組み合わせられない場合、`localeconfig` コマンドを使用し、本文テキストを昇格または変換して免責事項のエンコード方式と一致させるように AsyncOS を設定することで、免責事項をメッセージの本文に含めることができます。

```
example.com> localeconfig
```

```
Behavior when modifying headers: Use encoding of message body
```

```
Behavior for untagged non-ASCII headers: Impose encoding of message body
```

```
Behavior for mismatched footer or heading encoding: Only try encoding from  
message body
```

```
Choose the operation you want to perform:
```

```
- SETUP - Configure multi-lingual settings.
```

```
[ ]> setup
```

```
If a header is modified, encode the new header in the same encoding as
```

```
the message body? (Some MUAs incorrectly handle headers encoded in a
```

different encoding than the body. However, encoding a modified header in the same encoding as the message body may cause certain characters in the modified header to be lost.) [Y]>

If a non-ASCII header is not properly tagged with a character set and is being used or modified, impose the encoding of the body on the header during processing and final representation of the message? (Many MUAs create non-RFC-compliant headers that are then handled in an undefined way. Some MUAs handle headers encoded in character sets that differ from that of the main body in an incorrect way. Imposing the encoding of the body on the header may encode the header more precisely. This will be used to interpret the content of headers for processing, it will not modify or rewrite the header unless that is done explicitly as part of the processing.) [Y]>

Footers or headings are added in-line with the message body whenever possible. However, if the footer or heading is encoded differently than the message body, and if imposing a single encoding will cause loss of characters, it will be added as an attachment. The system will always try to use the message body's encoding for the footer or heading. If that fails, and if the message body's encoding is US-ASCII, the system can try to edit the message body to use the footer's or heading's encoding. Should the system try to impose the footer's or headings's encoding on the message body? [N]> **y**

Behavior when modifying headers: Use encoding of message body
Behavior for untagged non-ASCII headers: Impose encoding of message body.
Behavior for mismatched footer or heading encoding: Try both body and footer or heading encodings

Choose the operation you want to perform:

- SETUP - Configure multi-lingual settings.

localeconfig コマンドの詳細については、『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「Customizing Listeners」の章を参照してください。

通知テンプレート

通知テンプレートは、`notify()` および `notify-copy()` フィルタ アクションで使用されます。通知テンプレートには、アンチウイルス通知により使用されるアンチウイルス関連の変数を含む非 ASCII テキストおよびアクション変数を含めることができます（『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「Using Message Filters to Enforce Email Policies」の章にある「Action Variables」を参照）。たとえば、`$Allheaders` アクション変数を使用して、元のメッセージのヘッダーを含めることができます。通知用の From: アドレスを設定できます。[「アプライアンスに生成されるメッセージの返信アドレスの設定」\(P.29-29\)](#) を参照してください。

通知テンプレートを作成したら、コンテンツ フィルタおよびメッセージ フィルタから参照させることができます。図 18-2 は、「`grapewatchers@example.com`」に「`grape_text`」通知が送信されるように `notify-copy()` フィルタ アクションを設定したコンテンツ フィルタを示しています。

図 18-2 コンテンツ フィルタによる通知の例
Edit Content Filter

Edit Filter	
Name:	grapecheck
Currently used by policies:	DEFAULT
Description:	Looking for grapes.
Order:	1
Apply filter:	<input checked="" type="radio"/> If one or more conditions match <input type="radio"/> Only if ALL conditions match
Conditions	
<input type="button" value="Select New Condition..."/> <input type="button" value="Add Condition"/>	
Condition	Delete
body-contains("grape")	
Actions	
<input type="button" value="Select New Action..."/> <input type="button" value="Add Action"/>	
Action	Delete
notify-copy ("grapewatchers@example.com", "Found one!", "", "grape_text")	
<input type="button" value="Cancel"/> <input type="button" value="Submit"/>	

アンチウイルス通知テンプレート

アンチウイルス通知テンプレートには、次の 2 つのタイプがあります。

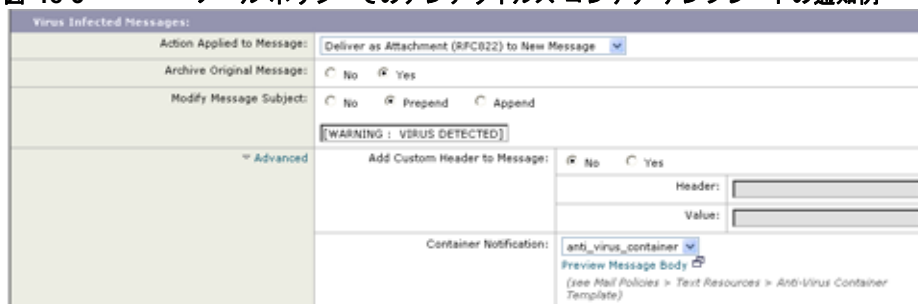
- **アンチウイルス通知テンプレート。**アンチウイルス通知テンプレートは、元のメッセージがウイルス通知に添付されていない場合に使用されます。
- **アンチウイルス コンテナ テンプレート。**コンテナ テンプレートは、元のメッセージが添付ファイルとして送信される際に使用されます。

アンチウイルス通知テンプレートは、フィルタの代わりにアンチウイルス エンジンで使用される以外は、基本的に通知テンプレートと同様に使用されます。メール ポリシーの編集集中に送信するカスタム通知を指定できます。アンチウイルス通知用の From: アドレスを設定できます。詳細については、「[アプライアンスに生成されるメッセージの返信アドレスの設定](#)」(P.29-29) を参照してください。

カスタム アンチウイルス通知テンプレート

図 18-3 は、カスタム アンチウイルス通知が指定されたメール ポリシーを示しています。

図 18-3 メール ポリシーでのアンチウイルス コンテナ テンプレートの通知例



アンチウイルス通知変数

アンチウイルス通知を作成する際に、表 18-4 に記載されている通知変数を使用できます。

表 18-4 アンチウイルス通知変数

変数	置き換える値
\$To	メッセージの To: ヘッダーに置き換えられます (エンベロープ受信者には置き換えられません)。
\$From	メッセージの From: ヘッダーに置き換えられます (エンベロープ送信者には置き換えられません)。
\$Subject	元のメッセージの件名に置き換えられます。
\$AV_VIRUSES	メッセージで発見されたすべてのウイルスのリストに置き換えられます。 "Unix/Apache.Trojan", "W32/Bagel-F"
\$AV_VIRUS_TABLE	パートごとに MIME-Part/Attachment 名とウイルスを示すテーブルに置き換えられます。 "HELLO.SCR" : "W32/Bagel-F" <unnamed part of the message> : "Unix/Apache.Trojan"
\$AV_VERDICT	アンチウイルスの判定に置き換えられます。

表 18-4 アンチウイルス通知変数 (続き)

変数	置き換える値
\$AV_DROPPED_TABLE	ドロップされた添付ファイルのテーブルに置き換えられます。各行は、パートまたはファイル名とパートに付随するウイルスのリストにより構成されます。 "HELLO.SCR" : "W32/Bagel-f", "W32/Bagel-d" "Love.SCR" : "Netsky-c", "W32/Bagel-d"
\$AV_REPAIRED_VIRUSES	発見および修復されたすべてのウイルスのリストに置き換えられます。
\$AV_REPAIRED_TABLE	発見および修復されたすべてのパーツとウイルスのテーブルに置き換えられます。"HELLO.SCR" : "W32/Bagel-F"
\$AV_DROPPED_PARTS	ドロップされたファイル名のリストに置き換えられます。 "HELLO.SCR", "CheckThisOut.exe"
\$AV_REPAIRED_PARTS	修復されたファイル名またはパーツのリストに置き換えられます。
\$AV_ENCRYPTED_PARTS	暗号化されたファイル名またはパーツのリストに置き換えられます。
\$AV_INFECTED_PARTS	ウイルスを含むファイルのファイル名のカンマ区切りリストに置き換えられます。
\$AV_UNSCANNABLE_PARTS	スキャンできなかったファイル名またはパーツのリストに置き換えられます。
\$Date	現在の日付 (MM/DD/YYYY 形式) に置き換えられます。
\$Time	現在の時刻 (ローカル時間帯) に置き換えられます。
\$GMTimestamp	現在の時刻および日付 (GMT) に置き換えられます。電子メール メッセージの Received: 行で見られる形式と同様です。
\$MID	メッセージを識別するために内部的に使用されるメッセージ ID または「MID」に置き換えられます。RFC822「Message-Id」の値とは異なるため注意してください (「Message-Id」を取得するには \$Header を使用します)。
\$Group	メッセージのインジェクト時に、送信者が一致する送信者グループの名前に置き換えられます。送信者グループに名前がない場合は、文字列「>Unknown<」が挿入されます。
\$Policy	メッセージのインジェクト時に、送信者に適用した HAT ポリシーの名前に置き換えられます。事前に定義されているポリシー名が使用されていない場合、文字列「>Unknown<」が挿入されます。
\$Reputation	送信者の SenderBase レピュテーション スコアに置き換えられます。レピュテーション スコアがない場合は「None」に置き換えられます。
\$filenames	メッセージの添付ファイルのファイル名を示すカンマ区切りリストに置き換えられます。
\$filetypes	メッセージの添付ファイルのファイル タイプを示すカンマ区切りリストに置き換えられます。
\$filesizes	メッセージの添付ファイルのファイル サイズを示すカンマ区切りリストに置き換えられます。

表 18-4 アンチウイルス通知変数 (続き)

変数	置き換える値
\$remotehost	メッセージを Cisco アプライアンスに送信したシステムのホスト名に置き換えられます。
\$AllHeaders	メッセージ ヘッダーに置き換えられます。
\$EnvelopeFrom	メッセージのエンベロープ送信者 (Envelope From、<MAIL FROM>) に置き換えられます。
\$Hostname	Cisco アプライアンスのホスト名に置き換えられます。



(注)

変数名は大文字/小文字を区別しません。たとえば、テキストリソースで「\$to」と「\$To」は同等です。元のメッセージで「AV_」変数が空の場合、文字列 <None> で置き換えられます。

テキストリソースを定義した後、[メールポリシー (Mail Policies)] > [受信/送信メールポリシー (Incoming/Outgoing Mail Policies)] > [ウイルス対策設定の編集 (Edit Anti-Virus Settings)] ページまたは `policyconfig -> edit -> antivirus` コマンドを使用して、修復されたメッセージ、スキャンできなかったメッセージ、暗号化されたメッセージ、またはウイルスが陽性のメッセージに対して、元のメッセージが RFC 822 のアタッチメントとして含まれるように指定します。詳細については、「[カスタムのアラート通知の送信 \(受信者宛でのみ\)](#)」(P.12-12) を参照してください。

バウンス通知および暗号化失敗通知テンプレート

バウンス通知および暗号化失敗通知テンプレートは、バウンス通知およびメッセージ暗号化失敗通知で使用される以外は、基本的に通知テンプレートと同様に使用されます。暗号化プロファイルを編集時に、バウンス プロファイルおよびカスタム メッセージ暗号化失敗通知を編集していた場合に送信するカスタム バウンス通知を指定できます。

図 18-4 は、バウンス プロファイルで指定されたバウンス通知テンプレートを示しています。

図 18-4 バウンス プロファイルのバウンス通知の例



(注)

カスタム テンプレートを使用する場合は、RFC-1891 の DSN を使用してください。

図 18-5 は、暗号化プロファイルで指定された暗号化失敗テンプレートを示しています。

図 18-5 暗号化プロファイルの暗号化失敗通知の例



バウンス通知および暗号化失敗通知変数

バウンス通知または暗号化失敗通知を作成する際に、表 18-5 に記載されている通知変数を使用できません。

表 18-5 バウンス通知変数

変数	置き換える値
\$Subject	元のメッセージの件名。
\$Date	現在の日付（MM/DD/YYYY 形式）に置き換えられます。
\$Time	現在の時刻（ローカル時間帯）に置き換えられます。
\$GMTTimeStamp	現在の時刻および日付（GMT）に置き換えられます。電子メールメッセージの Received: 行で見られる形式と同様です。
\$MID	メッセージを識別するために内部的に使用されるメッセージ ID または「MID」に置き換えられます。RFC822「Message-Id」の値とは異なるため注意してください（「Message-Id」を取得するには \$Header を使用します）。
\$BouncedRecipient	バウンスされた受信者のアドレス。
\$BounceReason	通知理由。
\$remotehost	メッセージを Cisco アプライアンスに送信したシステムのホスト名に置き換えられます。

暗号化通知テンプレート

暗号化通知テンプレートは、アウトバウンド電子メールを暗号化するように Cisco 電子メール暗号化を設定した際に使用されます。この通知では、受信者が暗号化されたメッセージを受信したことを通知し、メッセージを読む手順を説明しています。暗号化メッセージと一緒に送信するカスタム暗号化通知を指定できます。暗号化プロファイルを作成する際は、HTML 形式およびテキスト形式の両方の暗号化通知を指定します。このため、カスタムプロファイルを作成する場合は、テキスト形式および HTML 形式の両方の通知を作成する必要があります。

図 18-6 は、暗号化プロファイルで指定された暗号化通知を示しています。

図 18-6 暗号化プロファイルでイネーブルになっている暗号化通知テンプレート





CHAPTER 19

SMTP サーバを使用した受信者の検証

- 「SMTP Call-Ahead 受信者検証の概要」 (P.19-1)
- 「SMTP Call-Ahead 受信者検証のワークフロー」 (P.19-1)
- 「外部 SMTP サーバを使用した受信者の検証方法」 (P.19-3)
- 「リスナーでの SMTP サーバ経由の着信メールの検証のイネーブル化」 (P.19-6)
- 「LDAP ルーティング クエリーの設定」 (P.19-6)
- 「SMTP Call-Ahead クエリーのルーティング」 (P.19-7)
- 「特定のユーザまたはグループの SMTP Call-Ahead 検証のバイパス」 (P.19-8)

SMTP Call-Ahead 受信者検証の概要

SMTP Call-Ahead 受信者検証機能では、受信者宛ての着信メールを受け入れる前に、外部 SMTP サーバにクエリーを実行します。LDAP 承認または Recipient Access Table (RAT; 受信者アクセス テーブル) を使用できない場合、受信者を検証するためにこの機能を使用します。たとえば、それぞれ別のドメインを使用する多数のメール ボックスのメールをホストしていて、LDAP インフラストラクチャが各受信者を検証するために LDAP サーバにクエリーすることを許可していないとします。この場合、電子メール セキュリティ アプライアンスが SMTP サーバにクエリーを実行して、SMTP 通信を続ける前に受信者を検証できます。

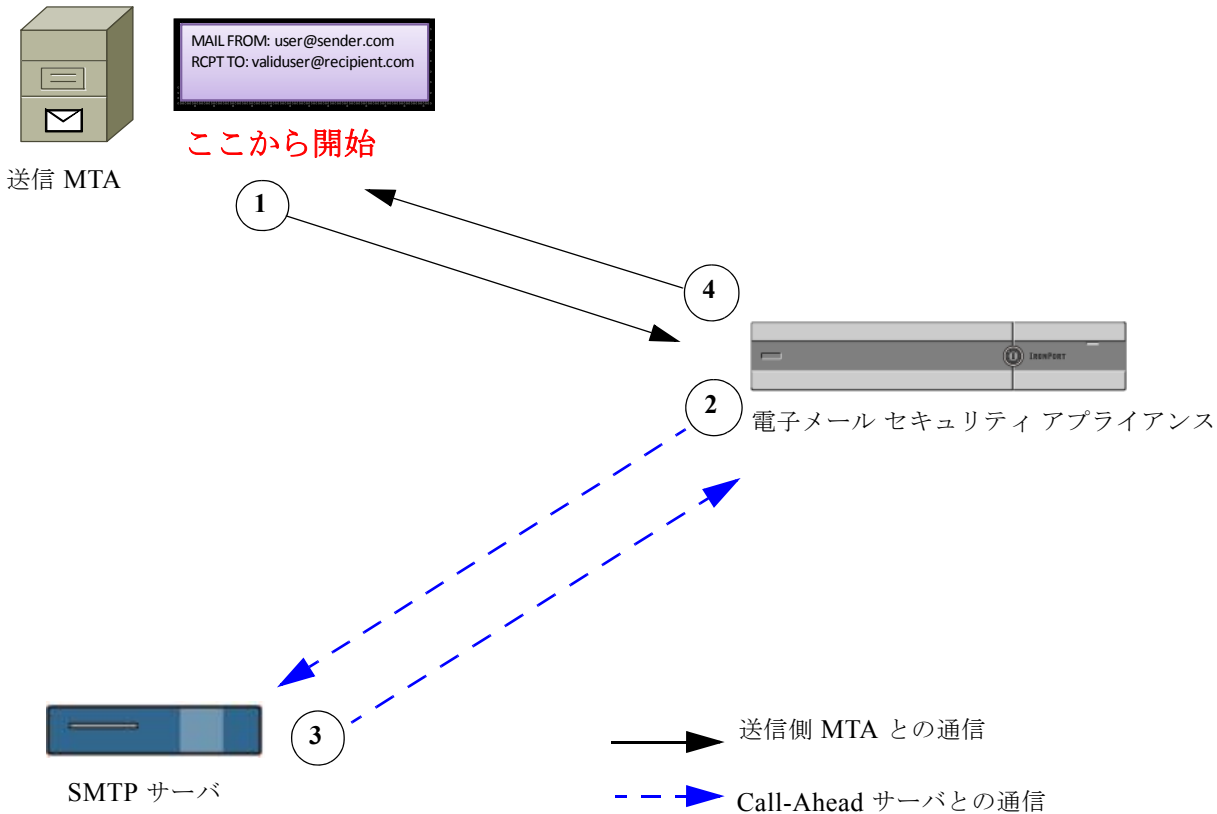
SMTP Call-Ahead 受信者検証を使用して、無効な受信者宛てのメッセージの処理を減らします。通常、無効な受信者宛てのメッセージは、ドロップする前にワーク キューを通して処理します。代わりに、電子メール パイプラインの着信および受信部分で追加処理を行わずに無効なメッセージをドロップまたはバウンスできます。

SMTP Call-Ahead 受信者検証のワークフロー

電子メール セキュリティ アプライアンスで SMTP Call-Ahead 受信者検証を設定すると、電子メール セキュリティ アプライアンスは、SMTP サーバに「事前に電話して」受信者を検証する間、送信側の MTA との SMTP 通信を中断します。Cisco アプライアンスは、SMTP サーバにクエリーを実行するとき、SMTP サーバの応答を電子メール セキュリティ アプライアンスに返し、ユーザの設定に基づいて、メールを受け入れるか、コードとカスタム応答で接続をドロップすることができます。

図 19-1 に、SMTP Call-Ahead 検証通信の基本的なワークフローを示します。

図 19-1 SMTP Call Ahead サーバ通信のワークフロー



1. 送信側の MTA が SMTP 通信を開始します。
2. 電子メールセキュリティアプライアンスは、SMTP サーバにクエリーを送信して受信者 `validuser@recipient.com` を検証する間、SMTP 通信を中断します。



(注) SMTP ルートまたは LDAP ルーティング クエリーが設定されている場合、SMTP サーバへのクエリーにはこれらのルートが使用されます。

3. SMTP サーバは、電子メールセキュリティアプライアンスにクエリーの応答を返します。
4. 電子メールセキュリティアプライアンスは SMTP 通信を再開し、送信側の MTA に応答を送信し、SMTP サーバの応答（および SMTP Call-Ahead プロファイルの設定）に基づいて接続を続行するかドロップします。

電子メールパイプラインでの処理の順序が決まっているため、特定の受信者宛てのメッセージが RAT によって拒否された場合、SMTP Call-Ahead 受信者検証は発生しません。たとえば、RAT で `example.com` 宛てのメールのみを受け入れるように指定した場合、SMTP Call-Ahead 受信者検証が発生する前に、`recipient@domain2.com` 宛てのメールは拒否されます。



(注) HAT でディレクトリハーベスト攻撃防止 (DHAP) を設定した場合、SMTP Call-Ahead サーバの拒否は、指定した 1 時間あたりの最大無効受信者数の中の拒否数に含まれるので注意してください。SMTP サーバによって拒否が増える場合を考慮してこの数を調整する必要があります。DHAP の詳細については、『Cisco IronPort AsyncOS for Email Configuration Guide』の「Configuring the Gateway to Receive Mail」を参照してください。

外部 SMTP サーバを使用した受信者の検証方法

表 19-1 外部 SMTP サーバを使用した受信者の検証方法

	操作内容	追加情報
ステップ 1	アプライアンスの SMTP サーバへの接続およびサーバの応答の解釈方法を決定します。	「Call-Ahead サーバ プロファイルの設定」(P.19-3)
ステップ 2	SMTP サーバが受信者を検証するようにパブリック リスナーを設定します。	「リスナーでの SMTP サーバ経由の着信メールの検証のイネーブル化」(P.19-6)
ステップ 3	(任意) メール別の別のホストにルーティングする際に使用する SMTP サーバを決定するには、LDAP ルーティング クエリーを更新します。	「LDAP ルーティング クエリーの設定」(P.19-6)
ステップ 4	(任意) 特定の受信者に対して Call-Ahead 検証をバイパスするようにアプライアンスを設定します。	「特定のユーザまたはグループの SMTP Call-Ahead 検証のバイパス」(P.19-8)

Call-Ahead サーバ プロファイルの設定

SMTP Call-Ahead サーバ プロファイルの設定では、電子メール セキュリティ アプライアンスと SMTP サーバの接続方法と SMTP サーバから返される応答の解釈方法を設定します。

手順

- ステップ 1 [ネットワーク (Network)] > [SMTP Call-Ahead] をクリックします。
- ステップ 2 [プロファイルを追加 (Add Profile)] をクリックします。
- ステップ 3 プロファイルの設定値を入力します。詳細については、「表 19-2SMTP Call-Ahead サーバ プロファイルの設定」(P.19-4) を参照してください。
- ステップ 4 プロファイルの高度な設定を指定します。詳細については、「表 19-3SMTP Call-Ahead サーバ プロファイルの高度な設定」(P.19-5) を参照してください。
- ステップ 5 変更内容を送信し、確定します。

SMTP Call-Ahead サーバ プロファイルの設定

SMTP Call-Ahead サーバ プロファイルの設定時に、電子メール セキュリティ アプライアンスと SMTP サーバの接続方法を設定する必要があります。

表 19-2 SMTP Call-Ahead サーバ プロファイルの設定


設定	説明
プロファイル名 (Profile Name)	Call-Ahead サーバ プロファイルの名前。
コールアヘッド サーバ タイプ (Call-Ahead Server Type)	<p>コールアヘッド サーバへの接続方法を次から 1 つ選択します。</p> <ul style="list-style-type: none"> [配信ホストを使用 (Use Delivery Host)]。SMTP Call-Ahead クエリーに配信電子メール アドレスのホストを使用するように指定する場合は、このオプションを選択します。たとえば、メールの受信アドレスが <i>recipient@example.com</i> の場合、SMTP クエリーは <i>example.com</i> に関連付けられた SMTP サーバに対して実行されます。SMTP ルートまたは LDAP ルーティング クエリーを設定した場合、クエリー先の SMTP サーバの決定には、これらのルートが使用されます。LDAP ルーティング クエリーの設定についての詳細は、「LDAP ルーティング クエリーの設定」(P.19-6) を参照してください。 [スタティック Call-Ahead サーバ (Static Call-Ahead Server)]。クエリー先の Call-Ahead サーバのスタティック リストを作成する場合は、このオプションを使用します。Call-Ahead サーバの名前や場所が頻繁に変わらないと思われる場合は、このオプションを使用できます。このオプションを使用すると、電子メール セキュリティ アプライアンスは、リストの最初のスタティック Call-Ahead サーバからラウンドロビン方式でホストにクエリーを送信します。 <p> (注) スタティック Call-Ahead サーバタイプを選択すると、クエリーに SMTP ルートは適用されないので注意してください。その代わりに MX ルックアップが実行され、その後、ホストでスタティック サーバの Call-Ahead IP アドレスを取得するためのルックアップが実行されます。</p>
スタティック コールアヘッド サーバ (Static Call-Ahead Servers)	<p>スタティック コールアヘッド サーバタイプを使用する場合は、このフィールドにホストとポートの組み合わせのリストを入力します。次の構文を使用して、サーバとポートのリストを作成します。</p> <pre>ironport.com:25</pre> <p>複数のエントリがある場合は、カンマで区切ります。</p>

表 19-3 に、SMTP Call-Ahead サーバ プロファイルの高度な設定を説明します。

表 19-3 SMTP Call-Ahead サーバ プロファイルの高度な設定

設定	説明
インターフェイス (Interface)	SMTP サーバと SMTP 通信を開始するときに使用されるインターフェイス。 [管理インターフェイス (Management interface)] または [自動 (Auto)] のどちらを使用するかを選択します。[自動 (Auto)] を選択すると、電子メールセキュリティアプライアンスは、使用するインターフェイスを自動的に検出しようとします。Cisco IronPort インターフェイスは、次の方法で SMTP サーバとの接続を試みます。 <ul style="list-style-type: none"> Call-Ahead サーバが設定済みインターフェイスの 1 つと同じサブネット上にある場合、接続は一致するインターフェイスによって開始されます。 設定済みの任意の SMTP ルートが、クエリーのルートに使用されません。 それ以外の場合、デフォルト ゲートウェイと同じサブネット上にあるインターフェイスが使用されます。
MAIL FROM アドレス (MAIL FROM Address)	SMTP サーバとの SMTP 通信に使用される MAIL FROM: アドレス。
検証要求タイムアウト (Validation Request Timeout)	SMTP サーバからの結果を待機する秒数。このタイムアウト値は、複数の Call-Ahead サーバにアクセスする可能性のある 1 つの受信者検証要求に対する値です。「 Call Ahead Server Responses 」(P.19-5) を参照してください。
検証エラーのアクション (Validation Failure Action)	受信者検証要求が失敗した場合 (タイムアウト、サーバの障害、ネットワークの問題、または不明な応答により) に実行するアクション。電子メールセキュリティアプライアンスでのさまざまな応答の処理方法を設定できます。「 Call Ahead Server Responses 」(P.19-5) を参照してください。
一時的なエラーのアクション (Temporary Failure Action)	受信者検証要求が一時的に失敗した場合 (リモート SMTP サーバから 4xx 応答が返された) に実行するアクション。メールボックスが一杯の場合、メールボックスを利用できない場合、またはサービスを利用できない場合に発生することがあります。 「 Call Ahead Server Responses 」(P.19-5) を参照してください。
セッションあたりの最大受信者数 (Max. Recipients per Session)	1 つの SMTP セッションで検証する最大受信者数。 1 ~ 25,000 セッションの間で指定します。
サーバあたりの最大接続数 (Max. Connections per Server)	1 台の Call-ahead SMTP サーバへの最大接続数。 1 ~ 100 接続の間で指定します。
キャッシュ (Cache)	SMTP 応答のキャッシュのサイズ。100 ~ 1,000,000 エントリの間で指定します。
キャッシュ TTL (Cache TTL)	キャッシュ内でのエントリの存続可能時間値。このフィールドのデフォルト値は 900 秒です。60 ~ 86400 秒の間で指定します。

Call Ahead Server Responses

SMTP サーバからは、次の応答が返されます。

- **2xx** : Call Ahead サーバから 2 で始まる SMTP コードを受け取った場合、受信者は受け入れられます。たとえば、応答が 250 の場合、メーリングアクションを続行できます。
- **4xx** : 4 で始まる SMTP コードは、SMTP 要求の処理中に一時的な障害が発生したことを示します。後で再試行すると正常に処理されることがあります。たとえば、応答 451 は、要求されたアクションが中止されたか、処理中にローカルエラーが発生したことを示します。
- **5xx** : 5 で始まる SMTP コードは、SMTP 要求の処理中に永続的な障害が発生したことを示します。たとえば、応答 550 は、要求されたアクションが実行されなかったか、メールボックスを使用できなかったことを示します。
- **Timeout**. Call-Ahead サーバから応答が戻されない場合、タイムアウトが発生する前に再試行する時間を設定できます。
- **Connection error**. Call-Ahead サーバへの接続に失敗した場合、受信者アドレスへの接続を受け入れるか拒否するかを設定できます。

リスナーでの SMTP サーバ経由の着信メールの検証のイネーブル化

SMTP Call-Ahead サーバ プロファイルを作成したら、そのプロファイルをリスナーでイネーブルにして、リスナーが SMTP サーバ経由の着信メールを検証できるようにする必要があります。プライベートリスナーでは受信者の検証は必要ないので、SMTP Call-Ahead 機能はパブリックリスナーでのみ使用できます。

手順

-
- ステップ 1** [ネットワーク (Network)] > [リスナー (Listeners)] に移動します。
 - ステップ 2** SMTP Call-Ahead 機能をイネーブルにするリスナーの名前をクリックします。
 - ステップ 3** [SMTP Call Ahead プロファイル (SMTP Call Ahead Profile)] フィールドで、イネーブルにする SMTP Call-Ahead プロファイルを選択します。
 - ステップ 4** 変更内容を送信し、確定します。
-

LDAP ルーティング クエリーの設定

LDAP ルーティング クエリーを使用して、メールを異なるメール ホストにルーティングする場合、AsyncOS は、代替メールホスト属性を使用して、クエリー先の SMTP サーバを決定します。ただし、この処理が不適切な場合があります。たとえば、次のスキーマでは、メール ホスト属性 (mailHost) には、Call-Ahead SMTP サーバの属性 (callAhead) で指定されているサーバとは異なる SMTP アドレスがあります。

```
dn: mail=cisco.com, ou=domains
mail: cisco.com
mailHost: smtp.mydomain.com
policy: ASAV
callAhead: smtp2.mydomain.com,smtp3.mydomain.com:9025
```

この場合、[SMTP Call-Ahead] フィールドを使用して、SMTP Call-Ahead クエリーを callAhead 属性で指定されているサーバに転送するルーティング クエリーを作成できます。たとえば、次の属性でルーティング クエリーを作成できます。

図 19-2 SMTP Call-Ahead 用に設定された LDAP ルーティング クエリー :

Routing Query	
Name:	LDAP1.routing
Query String:	{mail={d}}
Recipient Email to Rewrite the Envelope Recipient:	
Alternative Mailhost Attribute:	mailHost
SMTP Call-Ahead Server Attribute (optional):	callAhead
<small>This attribute is used only if an SMTP Call-Ahead server is configured. Go to Network > SMTP Call-Ahead.</small>	

このクエリーでは、{d} は受信者アドレスのドメイン部分を表し、SMTP Call-Ahead サーバ属性は、クエリーに使用する Call-Ahead サーバとポートの値として、ポート 9025 の smtp2.mydomain.com、smtp3.mydomain.com を返します。



(注)

この例は、LDAP ルーティング クエリーを使用して SMTP Call-Ahead クエリーを正しい SMTP サーバに転送できるクエリーの設定例の 1 つです。この例で説明したクエリー文字列や特定の LDAP 属性を使用する必要はありません。

SMTP Call-Ahead クエリーのルーティング

SMTP Call-Ahead クエリーのルーティング時、AsyncOS は次の順序で情報をチェックします。

図 19-3 SMTP Call-Ahead クエリー ルーティングのワークフロー

ドメイン名をチェックします。



LDAP ルーティング クエリーを
チェックします。



SMTP ルートをチェックします。



DNS ルックアップを実行します (MX ルックアップ、A ルックアップの順に実行)。

ドメインに LDAP ルーティング クエリーまたは SMTP ルートが設定されていない場合、前の状態の結果は次のステージに渡されます。SMTP ルートが存在しない場合は、DNS ルックアップが実行されません。

SMTP Call-Ahead クエリーの代わりに LDAP ルーティング クエリーを使用するときに、SMTP ルートも設定されている場合、ルーティング動作は、ルーティング クエリーから返される値によって異なります。

- LDAP ルーティング クエリーからポートなしで 1 つのホスト名が返された場合、SMTP Call-Ahead クエリーは SMTP ルートを適用します。SMTP ルートがホスト名として宛先ホストだけ指定した場合、SMTP サーバの IP アドレスを取得するように、DNS ルックアップが実行されません。
- LDAP ルーティング クエリーからポートとともに 1 つのホスト名が返された場合、その SMTP ルートが使用されますが、SMTP ルートでポートが指定されていても、LDAP クエリーによって返されたポートが使用されます。SMTP ルートがホスト名として宛先ホストだけ指定した場合、SMTP サーバの IP アドレスを取得するように、DNS ルックアップが実行されます。
- LDAP ルーティング クエリーからポートとともに、またはポートなしで複数のホストが返された場合、SMTP ルートが適用されますが、SMTP ルートでポートが指定されていても、LDAP ルーティング クエリーによって返されたポートが使用されます。SMTP ルートがホスト名として宛先ホストだけ指定した場合、SMTP サーバの IP アドレスを取得するように、DNS ルックアップが実行されます。

特定のユーザまたはグループの SMTP Call-Ahead 検証のバイパス

リスナーで SMTP Call-Ahead 検証をイネーブルにしたまま、特定のユーザまたはユーザグループに対して SMTP Call-Ahead 検証を省略する必要がある場合があります。

SMTP Call-Ahead クエリー中にメールを遅延させてはならない受信者に対する SMTP Call-Ahead 検証を省略する場合があります。たとえば、有効であることが明確であり、迅速な対応を必要とするカスタマーサービスのエイリアスに RAT エントリを追加できます。

GUI から SMTP Call-Ahead 検証をバイパスするように設定するには、RAT エントリの追加または編集時に、[SMTP Call-Ahead をバイパス (Bypass SMTP Call-Ahead)] を選択します。



CHAPTER 20

他の MTA との暗号化通信

- 「他の MTA との暗号化通信の概要」 (P.20-1)
- 「証明書の取得」 (P.20-2)
- 「リスナー HAT の TLS のイネーブル化」 (P.20-6)
- 「配信時の TLS および証明書検証のイネーブル化」 (P.20-9)
- 「認証局のリストの管理」 (P.20-15)
- 「HTTPS の証明書のイネーブル化」 (P.20-17)

他の MTA との暗号化通信の概要

エンタープライズ ゲートウェイ (またはメッセージ転送エージェント、つまり MTA) は、通常インターネット上で「クリアに」通信します。つまり、通信は暗号化されません。場合によっては、悪意のあるエージェントが、送信者または受信者に知られることなく、この通信を傍受する可能性があります。通信は第三者によってモニタされる可能性や、変更される可能性さえあります。

Transport Layer Security (TLS; トランスポート レイヤ セキュリティ) は Secure Socket Layer (SSL; セキュア ソケット レイヤ) テクノロジーを改良したバージョンです。これは、インターネット上での SMTP カンパセーションの暗号化に広く使用されているメカニズムです。AsyncOS では SMTP への STARTTLS 拡張 (セキュア SMTP over TLS) がサポートされます。詳細については、RFC 3207 を参照してください (これは、廃止になった RFC 2487 に代わるバージョンです)。

AsyncOS の TLS 実装では、暗号化によってプライバシーが確保されます。これによって、X.509 証明書および証明書認証サービスからの秘密キーのインポートや、アプライアンス上で使用する自己署名証明書を作成できます。AsyncOS では、パブリック リスナーおよびプライベート リスナーに対する個々の TLS 証明書、インターフェイス上のセキュア HTTP (HTTPS) 管理アクセス、LDAP インターフェイス、およびすべての発信 TLS 接続がサポートされます。

TLS を使用した SMTP カンバセーションの暗号化方法

表 20-1 TLS を使用した SMTP カンバセーションの暗号化方法

	操作内容	詳細
ステップ 1	公認の認証局からの X.509 証明書と秘密キーを取得します。	「証明書の取得」(P.20-2)
ステップ 2	電子メール セキュリティ アプライアンスに証明書をインストールします。	次のいずれかで証明書をインストールします。 <ul style="list-style-type: none"> 「GUI を使用した自己署名証明書の作成」(P.20-3) 「GUI を使用した証明書のインポート」(P.20-5)
ステップ 3	メッセージ受信用、またはメッセージ配信用、またはその両方の TLS をイネーブルにします。	<ul style="list-style-type: none"> 「リスナー HAT の TLS のイネーブル化」(P.20-6) 「配信時の TLS および証明書検証のイネーブル化」(P.20-9)
ステップ 4	(任意) リモート ドメインからの証明書を検証し、ドメインのクレデンシャルを確立するためにアプライアンスが使用する信頼できる認証局のリストをカスタマイズします。	「認証局のリストの管理」(P.20-15)
ステップ 5	(任意) TLS 接続が必要なドメインにメッセージを送信できない場合に警告を送信するよう電子メール セキュリティ アプライアンスを設定します。	「要求された TLS 接続が失敗した場合のアラートの送信」(P.20-11)

証明書の取得

TLS を使用するには、Cisco アプライアンスに対する受信および配信のための X.509 証明書および一致する秘密キーが必要です。SMTP での受信および配信の両方には同じ証明書を使用し、インターフェイス (LDAP インターフェイス) 上での HTTPS サービスや宛先ドメインへのすべての発信 TLS 接続には別の証明書を使用することも、それらのすべてに対して 1 つの証明書を使用することもできます。

既知の認証局サービスから認証および秘密キーを購入できます。認証局は、ID の検証および公開キーの配布に使用されるデジタル証明書を発行する第三者機関または企業です。これによって、有効で信頼できる身元によって証明書が発行されたことがさらに保証されます。Cisco では、サービスの重複を推奨しません。

Cisco アプライアンスでは、独自の自己署名証明書を作成して、公開証明書を取得するために認証局に送信する証明書署名要求 (CSR) を生成できます。認証局は、秘密キーによって署名された信頼できる公開証明書を返送します。GUI の [ネットワーク (Network)] > [証明書 (Certificates)] ページまたは CLI の `certconfig` コマンドを使用して自己署名証明書を作成し、CSR を生成して、信頼できる公開証明書をインストールします。

最初に証明書を取得または作成する場合、インターネットで「certificate authority services SSL Server Certificates (SSL サーバ証明書を提供している認証局)」を検索して、お客様の環境のニーズに最適なサービスを選択してください。サービスの手順に従って、証明書を取得します。

`certconfig` を使用して証明書を設定した後で、GUI の [ネットワーク (Network)] > [証明書 (Certificates)] ページおよび CLI の `print` コマンドを使用して証明書のリスト全体を表示できます。`print` コマンドでは中間証明書が表示されないことに注意してください。



警告

Cisco アプライアンスには TLS および HTTPS 機能がテスト済みであることを示すデモ証明書が同梱されますが、デモ証明書付きのサービスのいずれかをイネーブルにすることはセキュアではないため、通常の使用には推奨できません。デフォルトのデモ証明書が付属しているいずれかのサービスをイネーブルにすると、CLI に警告メッセージが表示されます。

中間証明書

ルート証明書の検証に加えて、AsyncOS では、中間証明書の検証の使用もサポートされます。中間証明書とは信頼できるルート認証局によって発行された証明書であり、信頼の連鎖を効率的に作成することによって、追加の証明書を作成するために使用されます。たとえば、信頼できるルート認証局によって証明書を発行する権利が与えられた `godaddy.com` によって証明書が発行されたとします。`godaddy.com` によって発行された証明書では、信頼できるルート認証局の秘密キーと同様に `godaddy.com` の秘密キーが検証される必要があります。

証明書と集中管理

証明書は通常、証明書の共通名にローカル マシンのホスト名を使用します。電子メール セキュリティ アプライアンスがクラスタの一部である場合は、クラスタ レベルでインストールできるワイルドカードの証明書を除いてマシン レベルとして各クラスタ メンバの証明書をインポートする必要があります。メンバーのリスナーが別のマシンと通信するときにクラスタが参照できるように、各クラスタ メンバの証明書は、同じ証明書の名前を使用する必要があります。

GUI を使用した自己署名証明書の作成

次のいずれかの理由によりアプライアンスの証明書を作成またはインポートする可能性があります。

- 他の MTA との SMTP カンバセーションを TLS（着信と発信カンバセーションの両方）を使用し、暗号化するため。
- HTTPS を使用して GUI にアクセスするためのアプライアンスの HTTPS サービスをイネーブルにするため。
- LDAP サーバがクライアント認証を要求した場合に LDAPS のクライアント証明書として使用するため。
- アプライアンスと DLP 用の RSA Enterprise Manager 間のセキュアな通信を許可するため。

手順

ステップ 1 [ネットワーク (Network)] > [証明書 (Certificates)] ページに移動します。

ステップ 2 [証明書の追加 (Add Certificate)] をクリックします。

ステップ 3 [自己署名証明書の作成 (Create Self-Signed Certificate)] を選択します。

図 20-1 に、[自己署名証明書の作成 (Create Self-Signed Certificate)] オプションが選択された [証明書の追加 (Add Certificate)] ページが表示されます。

図 20-1 [証明書 (Certificate)] ページ

Add Certificate

Add Certificate:

Common Name:

Organization:

Organizational Unit:

City (Locality):

State (Province):

Country:

Duration before expiration: days

Private Key Size: 2048 1024

ステップ 4 自己署名証明書に、次の情報を入力します。

共通名 (Common Name)	完全修飾ドメイン名。
組織 (Organization)	組織の正確な正式名称。
組織単位 (Organizational Unit)	組織の部署名。
市区町村 (City (Locality))	組織の本拠地がある都市。
都道府県 (State (Province))	組織の本拠地がある州、郡、または地方。
国 (Country)	組織の本拠地がある 2 文字の ISO 国名コード。
失効までの期間 (Duration before expiration)	証明書が期限切れになるまでの日数。
秘密キーのサイズ (Private Key Size)	CSR 用に生成する秘密キーのサイズ。2048 ビットおよび 1024 ビットだけがサポートされます。

ステップ 5 [次へ (Next)] をクリックして、証明書および署名情報を確認します。

図 20-2 に、自己署名証明書の例を示します。

図 20-2 [証明書 (Certificate)] ページの表示

View Certificate example.com

Add Certificate

Certificate Name:

Common Name:

Organization:

Organizational Unit:

City (Locality):

State (Province):

Country:

Signature Issued By: Common Name (CN): example.com
Organization (O): Example
Organizational Unit (OU): Org
Issued On: Feb 17 21:45:33 2020 GMT
Expires On: Feb 15 21:45:33 2020 GMT

If you would like a signed certificate, Download the certificate request. Submit this to a certificate authority. Once you receive the signed certificate, Upload it below.

Upload Signed Certificate:

Uploading a new certificate will overwrite the existing certificate.

Upload intermediate certificates if applicable.

ステップ 6 証明書の名前を入力します。AsyncOS のデフォルトでは、直前に入力した共通の名前が割り当てられます。

ステップ 7 自己署名証明書の CSR を認証局に送信する場合、[証明書署名要求をダウンロード (Download Certificate Signing Request)] をクリックしてローカルまたはネットワーク マシンに PEM 形式で CSR を保存します。

ステップ 8 変更内容を送信し、確定します。

秘密キーによって署名された信頼できる公開証明書を認証局が戻すと、[証明書 (Certificates)] ページの証明書の名前をクリックしてローカル マシンまたはネットワーク上のファイルへのパスを入力することで、信頼できる公開証明書をアップロードします。受信した信頼できる公開証明書が PEM 形式であるか、またはアプライアンスにアップロードする前に PEM を使用するように変換できる形式であることを確認します。(変換ツールは <http://www.openssl.org> の無料のソフトウェア OpenSSL に含まれています)。

認証局から証明書をアップロードすると、既存の証明書が上書きされます。自己署名証明書に関連する中間証明書をアップロードすることもできます。パブリック リスナーまたはプライベート リスナー、IP インターフェイスの HTTPS サービス、LDAP インターフェイス、または宛先ドメインへのすべての発信 TLS 接続に証明書を使用できます。

GUI を使用した証明書のインポート

AsyncOS では PKCS #12 形式で保存された証明書をインポートしてアプライアンスで使用することもできます。

手順

ステップ 1 [ネットワーク (Network)] > [証明書 (Certificates)] ページに移動します。

ステップ 2 [証明書の追加 (Add Certificate)] をクリックします。

ステップ 3 [証明書のインポート (Import Certificate)] オプションを選択します。

ステップ 4 ネットワーク上またはローカル マシンの証明書ファイルへのパスを入力します。

ステップ 5 ファイルのパスワードを入力します。

ステップ 6 [次へ (Next)] をクリックして証明書の情報を表示します。

ステップ 7 証明書の名前を入力します。

AsyncOS のデフォルトでは、共通の名前が割り当てられます。

ステップ 8 変更内容を送信し、確定します。

自己署名証明書の作成または CLI を使用した証明書のインポート

自己署名証明書を作成するか、または CLI を使用して証明書をインポートする場合、`certconfig` コマンドを使用します。

GUI を使用した証明書のエクスポート

AsyncOS では、証明書をエクスポートし、PKCS #12 形式で保存することも可能です。

手順

- ステップ 1 [ネットワーク (Network)] > [証明書 (Certificates)] ページに移動します。
- ステップ 2 [証明書のエクスポート (Export Certificate)] をクリックします。
- ステップ 3 エクスポートする証明書を選択します。
- ステップ 4 証明書のファイル名を入力します。
- ステップ 5 証明書ファイルのパスワードを入力します。
- ステップ 6 [エクスポート (Export)] をクリックします。
- ステップ 7 ファイルをローカル マシンまたはネットワーク マシンに保存します。
- ステップ 8 さらに証明書をエクスポートするか、または [キャンセル (Cancel)] をクリックして [ネットワーク (Network)] > [証明書 (Certificates)] ページに戻ります。

リスナー HAT の TLS のイネーブル化

暗号化が必要なリスナーに対して TLS をイネーブルにする必要があります。インターネットに対するリスナー（つまり、パブリック リスナー）には TLS をイネーブルにしますが、内部システムのリスナー（つまり、プライベートリスナー）には必要ありません。また、すべてのリスナーに対して暗号化をイネーブルにすることもできます。

リスナーの TLS に次の設定を指定できます。

表 20-2 リスナーの TLS 設定

TLS 設定	意味
1. No	TLS では着信接続を行えません。リスナーに対する接続では、暗号化された SMTP キャンパセーションは必要ありません。これは、アプライアンス上で設定されるすべてのリスナーに対するデフォルト設定です。
2. 推奨 (Preferred)	TLS で MTA からのリスナーへの着信接続が可能です。
3. 必須 (Required)	TLS で MTA からリスナーへの着信接続が可能です。また、STARTTLS コマンドを受信するまで Cisco アプライアンスは NOOP、EHLO または QUIT 以外のすべてのコマンドに対してエラー メッセージで応答します。この動作は RFC 3207 によって指定されています。RFC 3207 では、Secure SMTP over Transport Layer Security の SMTP サービス拡張が規定されています。TLS が「必要」であることは、送信側で TLS の暗号化を行わない電子メールが、送信前に Cisco アプライアンスによって拒否されることを意味し、このため、暗号化されずにクリア テキストで転送されることが回避されます。

デフォルトでは、プライベートリスナーとパブリックリスナーのどちらも TLS 接続を許可しません。電子メールの着信（受信）または発信（送信）の TLS をイネーブルにするには、リスナーの HAT の TLS をイネーブルにする必要があります。また、プライベートリスナーおよびパブリックリスナーのすべてのデフォルト メール フロー ポリシー設定で `tls` 設定が「off」になっています。

リスナーの作成時に、個々のパブリックリスナーに TLS 接続の専用の証明書を割り当てることができます。詳細については、「GUI からのリスナーの作成による接続要求のリスン」(P.5-8) を参照してください。

GUI を使用したパブリックまたはプライベートのリスナーへの TLS 接続のための証明書の割り当て

手順

- ステップ 1 [ネットワーク (Network)] > [リスナー (Listeners)] ページに移動します。
- ステップ 2 編集するリスナーの名前をクリックします。
- ステップ 3 [証明書 (Certificate)] フィールドから、証明書を選択します。
- ステップ 4 変更内容を送信し、確定します。

CLI を使用したパブリックまたはプライベートのリスナーへの TLS 接続のための証明書の割り当て

手順

- ステップ 1 `listenerconfig -> edit` コマンドを使用して、設定するリスナーを選択します。
- ステップ 2 `certificate` コマンドを使用して、使用できる証明書を表示します。
- ステップ 3 プロンプトが表示されたら、リスナーを割り当てる証明書を選択します。
- ステップ 4 リスナーの設定が完了したら、`commit` コマンドを発行して、変更をイネーブルにします。

ロギング

TLS が必要であるにもかかわらず、リスナーで使用できない場合、Cisco アプライアンスによってメール ログ インスタンスで通知されます。次の条件のいずれかを満たす場合、メール ログが更新されません。

- リスナーに対して TLS が「必須 (required)」と設定されている。
- Cisco アプライアンスは、「STARTTLS コマンドを最初に発行 (Must issue a STARTTLS command first)」コマンドを送信した。
- 正常な受信者が受信せずに接続が終了した。

TLS 接続が失敗した理由に関する情報がメール ログに記録されます。

GUI の例：リスナーの HAT の TLS 設定の変更

手順

- ステップ 1 [メール ポリシー (Mail Policies)] > [メール フロー ポリシー (Mail Flow Policies)] ページに移動します。

■ リスナー HAT の TLS のイネーブル化

- ステップ 2** 変更するポリシーを持つリスナーを選択し、編集するポリシーの名前へのリンクをクリックします。(デフォルトポリシーパラメータも編集可能)。
- ステップ 3** [暗号化と認証 (Encryption and Authentication)] セクションの [TLS:] フィールドで、リスナーの TLS のレベルを選択します。

図 20-3 リスナーのメールフローポリシーパラメータで要求される TLS

Encryption and Authentication:	TLS:	<input checked="" type="radio"/> Off <input type="radio"/> Preferred <input type="radio"/> Required
	SMTP Authentication:	<input checked="" type="radio"/> Off <input type="radio"/> Preferred <input type="radio"/> Required
	If Both TLS and SMTP Authentication are enabled:	<input type="checkbox"/> Require TLS To Offer SMTP Authentication

- ステップ 4** 変更内容を送信し、確定します。
選択した TLS 設定が反映されてリスナーのメールフローポリシーが更新されます。

CLI 例：リスナーの HAT の TLS 設定の変更

手順

- ステップ 1** `listenerconfig -> edit` コマンドを使用して、設定するリスナーを選択します。
- ステップ 2** リスナーのデフォルトの HAT 設定を編集するには、`hostaccess -> default` コマンドを使用します。
- ステップ 3** 次の質問が表示されたら、次の選択肢のいずれかを入力して TLS 設定を変更します。

```
Do you want to allow encrypted TLS connections?
```

1. No
2. Preferred
3. Required

```
[1]> 3
```

```
You have chosen to enable TLS. Please use the 'certconfig' command to ensure that there is a valid certificate configured.
```

この例では、リスナーで使用できる有効な証明書があるかどうかを確認するために `certconfig` コマンドを使用するかどうかを質問しています。証明書を作成していない場合、リスナーではアプライアンスにあらかじめインストールされているデモ証明書を使用します。テスト目的でデモ証明書で TLS をイネーブルにすることはできますが、セキュアではないため、通常の使用には推奨できません。リスナーに証明書を割り当てるには、`listenerconfig -> edit -> certificate` コマンドを使用します。

TLS を設定すると、CLI でリスナーの概要に設定が反映されます。

```
Name: Inboundmail
```

```
Type: Public
```



```
Interface: PublicNet (192.168.2.1/24) TCP Port 25

Protocol: SMTP

Default Domain:

Max Concurrency: 1000 (TCP Queue: 50)

Domain map: disabled

TLS: Required
```

ステップ 4 変更をイネーブルにするには、`commit` コマンドを発行します。

配信時の TLS および証明書検証のイネーブル化

[送信先コントロール (Destination Controls)] ページまたは `destconfig` コマンドを使用すると、TLS をイネーブルにして、特定のドメインに電子メールを配信するように要求できます。

TLS だけでなく、ドメインのサーバ証明書の検証も要求できます。このドメイン証明書は、ドメインのクレデンシャルを確立するために使用されるデジタル証明書に基づいています。証明プロセスには次の 2 つの要件が含まれます。

- 信頼できる Certificate Authority (CA; 認証局) によって発行された証明書で終わる SMTP セッションの証明書発行者のチェーン。
- 受信マシンの DNS 名またはメッセージの宛先ドメインのいずれかと一致する証明書に表示された Common Name (CN)。

または

メッセージの宛先ドメインが、証明書のサブジェクト代替名 (subjectAltName) の拡張の DNS 名のいずれかと一致している (RFC 2459 を参照)。この一致では、RFC 2818 のセクション 3.1 で説明されているワイルドカードがサポートされます。

信頼できる CA は、ID の検証および公開キーの配布に使用されるデジタル証明書を発行する、第三者機関または企業です。これによって、有効で信頼できる身元によって証明書が発行されたことがさらに保証されます。

エンベロープ暗号化の代わりに TLS 接続を介してドメインにメッセージを送信するように Cisco アプリアンスを設定できます。詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Cisco Email Encryption」の章を参照してください。

すべての発信 TLS 接続に対してアプリアンスで使用する証明書を指定できます。証明書を指定するには、[送信先コントロール (Destination Controls)] ページの [Edit Global Settings] をクリックするか、または CLI の `destconfig -> setup` を使用します。証明書はドメインごとの設定ではなく、グローバル設定です。

[送信先コントロール (Destination Controls)] ページまたは `destconfig` コマンドを使用してドメインを含める場合、指定されたドメインの TLS に 5 つの異なる設定を指定できます。TLS のエンコードにドメインとの交換が必須であるか、または推奨されるかの指定に加えて、ドメインの検証が必要かどうかも指定できます。設定の説明については、表 20-3 を参照してください。

表 20-3 配信の TLS 設定

TLS 設定	意味
デフォルト	<p>デフォルトの TLS 設定では、リスナーからドメインの MTA への発信接続に [送信先コントロール (Destination Controls)] ページまたは <code>destconfig -> default</code> サブコマンドを使用するように設定されています。</p> <p>質問「このドメインに特定の TLS 設定を適用しますか? (Do you wish to apply a specific TLS setting for this domain?)」に「いいえ (no)」と回答すると、「デフォルト」値が設定されます。</p>
1. いいえ (No)	インターフェイスからドメインの MTA への発信接続には、TLS がネゴシエートされません。
2. 推奨 (Preferred)	Cisco アプライアンス インターフェイスからドメインの MTA への TLS がネゴシエートされます。ただし、(220 応答を受信する前に) TLS ネゴシエーションに失敗すると、SMTP トランザクションは「クリアな」(暗号化されない)ままです。証明書が信頼できる認証局によって発行された場合、検証は行われません。220 応答を受信した後にエラーが発生した場合、SMTP トランザクションはクリア テキストにフォールバックされません。
3. 必須 (Required)	Cisco アプライアンス インターフェイスからドメインの MTA への TLS がネゴシエートされます。ドメインの証明書の検証は行われません。ネゴシエーションに失敗すると、電子メールはその接続を介して送信されません。ネゴシエーションに成功すると、暗号化されたセッションを経由して電子メールが配信されます。
4. 推奨 (検証) (Preferred (Verify))	<p>Cisco アプライアンスからドメインの MTA への TLS がネゴシエートされます。アプライアンスはドメインの証明書の検証を試行します。</p> <p>次の 3 つの結果が考えられます。</p> <ul style="list-style-type: none"> • TLS がネゴシエートされ、証明書が検証される。暗号化されたセッションによってメールが配信される。 • TLS がネゴシエートされるものの、証明書は検証されない。暗号化されたセッションによってメールが配信される。 • TLS 接続が確立されず、証明書は検証されない。電子メール メッセージがプレーン テキストで配信される。
5. 必須 (検証) (Required (Verify))	<p>Cisco アプライアンスからドメインの MTA への TLS がネゴシエートされます。ドメインの証明書の検証が必要です。</p> <p>次の 3 つの結果が考えられます。</p> <ul style="list-style-type: none"> • TLS 接続がネゴシエートされ、証明書が検証される。暗号化されたセッションによって電子メール メッセージが配信される。 • TLS 接続がネゴシエートされるものの、信頼できる CA によって証明書が検証されない。メールは配信されない。 • TLS 接続がネゴシエートされない。メールは配信されない。

グッド ネイバー テーブルに指定された受信者ドメインの指定されたエントリがない場合、または指定されたエントリが存在するものの、そのエントリに対して指定された TLS 設定が存在しない場合、[送信先コントロール (Destination Controls)] ページまたは `destconfig -> default` サブコマンド (「いいえ (No)」、「推奨 (Preferred)」、「必須 (Required)」、「推奨 (検証) Preferred (Verify)」、「必須 (検証) Required (Verify)」) を使用して動作を設定する必要があります。

要求された TLS 接続が失敗した場合のアラートの送信

TLS 接続が必要なドメインにメッセージを配信する際に TLS ネゴシエーションが失敗した場合、Cisco アプライアンスがアラートを送信するかどうかを指定できます。アラート メッセージには失敗した TLS ネゴシエーションの宛先ドメイン名が含まれます。Cisco アプライアンスは、システム アラートのタイプの警告重大度レベル アラートを受信するよう設定されたすべての受信者にアラートメッセージを送信します。GUI の [システム管理 (System Administration)] > [アラート (Alerts)] ページ (または CLI の `alertconfig` コマンド) を使用してアラートの受信者を管理できます。

GUI を使用した TLS 接続アラートのイネーブル化

手順

- ステップ 1** メール ポリシーの [送信先コントロール (Destination Controls)] ページに移動します。
- ステップ 2** [グローバル設定を編集 (Edit Global Settings)] をクリックします。
- ステップ 3** [必要な TLS 接続に失敗した場合にアラートを送信: (Send an alert when a required TLS connection fails:)] の [有効 (Enable)] をクリックします。
これは、ドメイン単位ではなく、グローバルな設定です。アプライアンスが配信を試行したメッセージの情報については、[モニタ (Monitor)] > [メッセージトラッキング (Message Tracking)] ページまたはメール ログを使用します。
- ステップ 4** 変更内容を送信し、確定します。

CLI を使用した TLS 接続アラートのイネーブル化

CLI を使用して TLS 接続アラートをイネーブルにするには、`destconfig -> setup` コマンドを使用します。

ロギング

ドメインに TLS が必要であるにもかかわらず、使用できない場合、Cisco アプライアンスによってメール ログ インスタンスで通知されます。TLS 接続を使用できなかった理由も記載されています。次の条件のいずれかを満たす場合、メール ログが更新されます。

- リモート MTA で ESMTP がサポートされない (たとえば、Cisco アプライアンスからの EHLO コマンドが理解できない)。
- リモート MTA で ESMTP がサポートされるものの、「STARTTLS」が EHLO 応答でアドバタイズされる拡張のリストにない。
- リモート MTA で「STARTTLS」拡張がアドバタイズされたものの、Cisco アプライアンスで STARTTLS コマンドを送信した際にエラーが返される。

CLI の例

この例では、`destconfig` コマンドを使用して、TLS 接続の要求および「`partner.com`」ドメインの暗号化されたカンパセーションを実行します。リストが表示されます。

`example.com` の証明書は、あらかじめインストールされているデモ証明書の代わりに発信 TLS 接続で使用されます。テスト目的でデモ証明書で TLS をイネーブルにすることはできますが、セキュアではないため、通常の使用には推奨できません。

```
mail3.example.com> destconfig
```

```
There is currently 1 entry configured.
```

```
Choose the operation you want to perform:
```

- SETUP - Change global settings.
- NEW - Create a new entry.
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- IMPORT - Import tables from a file.
- EXPORT - Export tables to a file.

```
[ ]> setup
```

```
The "Demo" certificate is currently configured. You may use "Demo", but this will not be secure.
```

```
1. example.com
```

```
2. Demo
```

```
Please choose the certificate to apply:
```

```
[1]> 1
```

```
Do you want to send an alert when a required TLS connection fails? [N]>
```

```
There is currently 1 entry configured.
```

```
Choose the operation you want to perform:
```

- SETUP - Change global settings.
- NEW - Create a new entry.
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- IMPORT - Import tables from a file.
- EXPORT - Export tables to a file.

```
[> new
```

```
Enter the domain you wish to limit.
```

```
[> partner.com
```

```
Do you wish to configure a concurrency limit for partner.com? [Y]> n
```

```
Do you wish to apply a messages-per-connection limit to this domain? [N]> n
```

```
Do you wish to apply a recipient limit to this domain? [N]> n
```

```
Do you wish to apply a specific bounce profile to this domain? [N]> n
```

```
Do you wish to apply a specific TLS setting for this domain? [N]> y
```

```
Do you want to use TLS support?
```

1. No
2. Preferred

- 3. Required
- 4. Preferred (Verify)
- 5. Required (Verify)

[1]> **3**

You have chosen to enable TLS. Please use the 'certconfig' command to ensure that there is a valid certificate configured.

Do you wish to apply a specific bounce verification address tagging setting for this domain? [N]> **n**

Do you wish to apply a specific bounce profile to this domain? [N]> **n**

There are currently 2 entries configured.

Choose the operation you want to perform:

- SETUP - Change global settings.
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- CLEAR - Remove all entries.
- IMPORT - Import tables from a file.
- EXPORT - Export tables to a file.

[>] **list**

	Rate		Bounce	Bounce
Domain	Limiting	TLS	Verification	Profile
=====	=====	=====	=====	=====

```
partner.com  Default  Req      Default  Default
(Default)   On           Off      Off       (Default)
```

There are currently 2 entries configured.

Choose the operation you want to perform:

```
- SETUP - Change global settings.
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- CLEAR - Remove all entries.
- IMPORT - Import tables from a file.
- EXPORT - Export tables to a file.

[]>
```

認証局のリストの管理

アプライアンスは、リモート ドメインからの証明書の検証にはドメインのクレデンシャルを確立するために使用する保存された信頼できる認証局を使用します。次の信頼できる認証局を使用するようにアプライアンスを設定できます。

- **プレインストールされたリスト。**アプライアンスには信頼できる認証局のリストがあらかじめインストールされています。これは、システム リストと呼ばれます。
- **ユーザ定義のリスト。**信頼できる認証局のリストをカスタマイズし、アプライアンスにリストをインポートできます。

システム リストまたはカスタマイズされたリストのいずれか、または両方のリストを使って、リモート ドメインからの証明書を検証できます。

GUI の [ネットワーク (Network)] > [証明書 (Certificates)] > [認証局の編集 (Edit Certificate Authorities)] ページまたは CLI の `certconfig > certauthority` コマンドを使用してリストします。

[ネットワーク (Network)] > [証明書 (Certificates)] > [認証局の編集 (Edit Certificate Authorities)] ページで、次のタスクを実行できます。

- **認証局のシステム リスト (インストール済み) を参照します。**詳細については、「[プレインストールされたの認証局リストの参照](#)」(P.20-16) を参照してください。

- システム リストを使用するかどうかを選択します。システム リストはイネーブルまたはディセーブルにできます。詳細については、「システム認証局リストのディセーブル化」(P.20-16) を参照してください。
- カスタム認証局リストを使用するかどうかを選択します。カスタム リストを使用して、テキスト ファイルからリストをインポートするようにアプライアンスをイネーブルにできます。詳細については、「カスタム認証局リストのインポート」(P.20-16) を参照してください。
- ファイルに、認証局のリストをエクスポートします。テキスト ファイルに、認証局のシステム リストまたはカスタム リストをエクスポートできます。詳細については、「認証局リストのエクスポート」(P.20-17) を参照してください。

プレインストールされたの認証局リストの参照

手順

-
- ステップ 1** [ネットワーク (Network)] > [証明書 (Certificates)] ページに移動します。
 - ステップ 2** [認証局 (Certificate Authorities)] セクションで、[設定を編集 (Edit Settings)] をクリックします。
 - ステップ 3** [システム認証局を表示 (View System Certificate Authorities)] をクリックします。
-

システム認証局リストのディセーブル化

プレインストールされたシステム認証局リストはアプライアンスから削除できませんが、イネーブルまたはディセーブルにできます。アプライアンスがリモート ホストからの証明書を確認するためにカスタム リストのみを使用することをディセーブルにすることがあります。

手順

-
- ステップ 1** [ネットワーク (Network)] > [証明書 (Certificates)] ページに移動します。
 - ステップ 2** [認証局 (Certificate Authorities)] セクションで、[設定を編集 (Edit Settings)] をクリックします。
 - ステップ 3** [システム リスト (System List)] で [ディセーブル (Disable)] をクリックします。
 - ステップ 4** 変更内容を送信し、確定します。
-

カスタム認証局リストのインポート

信頼できる認証局のカスタム リストを作成して、アプライアンスにインポートできます。ファイルは PEM 形式にして、アプライアンスで信頼する認証局の証明書が含まれている必要があります。

手順

-
- ステップ 1** [ネットワーク (Network)] > [証明書 (Certificates)] ページに移動します。
 - ステップ 2** [認証局 (Certificate Authorities)] セクションで、[設定を編集 (Edit Settings)] をクリックします。
 - ステップ 3** [カスタム リスト (Custom List)] の [有効 (Enable)] をクリックします。

- ステップ 4** ローカル マシンまたはネットワーク マシンのカスタム リストへのフル パスを入力します。
- ステップ 5** 変更内容を送信し、確定します。

認証局リストのエクスポート

システム内の信頼できる認証局のサブセットのみを使用するか、既存のカスタム リストの編集を行う場合、リストを .txt ファイルにエクスポートして、認証局を追加または削除するように編集できます。リストの編集が完了したら、ファイルをカスタム リストとしてアプライアンスにインポートします。

手順

- ステップ 1** [ネットワーク (Network)] > [証明書 (Certificates)] ページに移動します。
- ステップ 2** [認証局 (Certificate Authorities)] セクションで、[設定を編集 (Edit Settings)] をクリックします。
- ステップ 3** [リストのエクスポート (Export List)] をクリックします。
[認証局リストのエクスポート (Export Certificate Authority List)] ページが表示されます。
- ステップ 4** 自分がエクスポートするリストを選択します。
- ステップ 5** リストのファイル名を入力します。
- ステップ 6** [エクスポート (Export)] をクリックします。

AsyncOS では、.txt ファイルとしてリストを開くか、または保存するかを確認するダイアログボックスが表示されます。

HTTPS の証明書のイネーブル化

GUI の [ネットワーク (Network)] > [IP インターフェイス (IP Interfaces)] ページまたは CLI の `interfaceconfig` コマンドのいずれかを使用して、IP インターフェイスで HTTPS サービスの証明書をイネーブルにできます。GUI を使用して IP インターフェイスを追加する場合、HTTPS サービスに使用する証明書を選択し、[HTTPS] チェックボックスをオンにして、ポート番号を入力します。

次の例では、`interfaceconfig` コマンドを使用して、ポート 443 (デフォルト ポート) 上で HTTPS サービスをイネーブルにするように IP インターフェイス `PublicNet` を編集します。インターフェイスのその他のすべてのデフォルトが受け入れられます。(プロンプトで `Enter` と入力すると、角カッコで囲まれて表示されるデフォルト値が受け入れられる)。

この例では、アプライアンスにあらかじめインストールされているデモ証明書を使用します。テスト目的でデモ証明書で HTTPS サービスをイネーブルにすることはできますが、セキュアではないため、通常の使用には推奨できません。



- (注) GUI のシステム設定ウィザードを使用して HTTPS サービスをイネーブルにできます。『Cisco IronPort AsyncOS for Email Configuration Guide』の「Setup and Installation」の章の「Define the Default Router (Gateway), Configure the DNS Settings, and Enabling Secure Web Access」を参照してください。

このコマンドからの変更が確定されると、ユーザがセキュア HTTPS の URL (`https://192.168.2.1`) を使用してグラフィカル ユーザ インターフェイス (GUI) にアクセスできるようになります。

```
mail3.example.com> interfaceconfig
```

```
Currently configured interfaces:
```

1. Management (192.168.42.42/24: mail3.example.com)
2. PrivateNet (192.168.1.1/24: mail3.example.com)
3. PublicNet (192.168.2.1/24: mail3.example.com)

```
Choose the operation you want to perform:
```

- NEW - Create a new interface.
- EDIT - Modify an interface.
- GROUPS - Define interface groups.
- DELETE - Remove an interface.

```
[>] edit
```

```
Enter the number of the interface you wish to edit.
```

```
[>] 3
```

```
IP interface name (Ex: "InternalNet"):
```

```
[PublicNet]>
```

```
Would you like to configure an IPv4 address for this interface (y/n)? [Y]> y
```

```
IPv4 Address (Ex: 192.168.1.2):
```

```
[192.168.2.1]>
```

```
Netmask (Ex: "255.255.255.0" or "0xffffffff00"):
```

```
[24]>
```

```
Would you like to configure an IPv6 address for this interface (y/n)? [N]>
```

```
Ethernet interface:
```

```
1. Data 1
```

```
2. Data 2
```

```
3. Management
```

```
[2]>
```

```
Hostname:
```

```
[mail3.example.com]>
```

```
Do you want to enable Telnet on this interface? [N]>
```

```
Do you want to enable SSH on this interface? [N]>
```

```
Do you want to enable FTP on this interface? [N]>
```

```
Do you want to enable HTTP on this interface? [Y]>
```

```
Which port do you want to use for HTTP?
```

```
[80]>
```

```
Do you want to enable HTTPS on this interface? [N]> y
```

```
Which port do you want to use for HTTPS?
```

```
[443]> 443
```

```
Do you want to enable Spam Quarantine HTTP on this interface? [N]>
```

```
Do you want to enable Spam Quarantine HTTPS on this interface? [N]>
```

```
The "Demo" certificate is currently configured. You may use "Demo", but this will not be secure. To assure privacy, run "certconfig" first.
```

```
Both HTTP and HTTPS are enabled for this interface, should HTTP requests redirect to the secure service? [Y]>
```

```
Currently configured interfaces:
```

1. Management (192.168.42.42/24: mail3.example.com)
2. PrivateNet (192.168.1.1/24: mail3.example.com)
3. PublicNet (192.168.2.1/24: mail3.example.com)

```
Choose the operation you want to perform:
```

- NEW - Create a new interface.
- EDIT - Modify an interface.
- GROUPS - Define interface groups.
- DELETE - Remove an interface.

```
[ ]>
```



CHAPTER 21

ルーティングおよび配信機能の設定

- 「ローカル ドメインの電子メールのルーティング」 (P.21-1)
- 「アドレスの書き換え」 (P.21-6)
- 「エイリアス テーブルの作成」 (P.21-7)
- 「マスカレードの設定」 (P.21-16)
- 「ドメイン マップ機能」 (P.21-28)
- 「バウンスした電子メールの処理」 (P.21-36)
- 「送信先コントロールによる電子メール配信の管理」 (P.21-43)
- 「Cisco バウンス検証」 (P.21-51)
- 「電子メール配信パラメータの設定」 (P.21-56)
- 「Virtual Gateway™ テクノロジーを使用してすべてのホストされたドメインでの構成のメールゲートウェイ」 (P.21-59)
- 「[グローバル配信停止 (Global Unsubscribe)] 機能の使用」 (P.21-68)

ローカル ドメインの電子メールのルーティング

第 5 章「電子メールを受信するためのゲートウェイの設定」では、エンタープライズゲートウェイ設定に対して SMTP 接続を提供するようにプライベートリスナーとパブリックリスナーをカスタマイズしました。これらのリスナーは、特定の接続を処理したり (HAT 変更経由)、特定ドメインのメールを受信したり (パブリックリスナーの RAT 変更経由) するようにカスタマイズされています。

Cisco アプライアンスでは、メールをローカルドメイン経由で、[ネットワーク (Network)] > [SMTP ルート (SMTP Routes)] ページ (または `smtproutes` コマンド) を使用して指定されたホストにルーティングします。この機能は、`sendmail` の `mailertable` 機能に似ています。



(注)

GUI でシステムセットアップウィザード (またはコマンドラインインターフェイスで `systemsetup` コマンド) を実行し (『Cisco IronPort AsyncOS for Email Configuration Guide』の「Setup and Installation」の章を参照)、変更内容を確定した場合、そのときに入力した RAT エントリごとに、アプライアンスで最初の SMTP ルート エントリが定義されています。

SMTP ルートの概要

SMTP ルートでは、異なる Mail Exchange (MX) ホストへ特定のドメインのすべての電子メールをリダイレクトできます。たとえば、example.com から groupware.example.com へのマッピングを行うことができます。このマッピングによって、[エンベロープ受信者 (Envelope Recipients)] アドレスに @example.com を持つすべての電子メールが、代わりに groupware.example.com に送られます。システムは、通常の電子メール配信のように、groupware.example.com で「MX」ルックアップを実行し、次にホストで「A」ルックアップを実行します。この代替 MX ホストは、DNS MX レコードにリストされている必要はなく、また、電子メールがリダイレクトされているドメインのメンバーになっている必要もありません。Cisco AsyncOS オペレーティングシステムでは、Cisco アプライアンスで最大 4 万の SMTP ルート マッピングを設定できます。(「SMTP ルートの制限」(P.21-3) を参照)。

この機能を使用すると、ホストを「ひとかたまりにする」ことができます。.example.com のようにドメインの一部を指定した場合は、example.com で終わるすべてのドメインがこのエントリに一致します。たとえば、fred@foo.example.com と wilma@bar.example.com は、両方ともマッピングに一致します。

SMTP ルート テーブルにホストがない場合は、DNS を使用して MX ルックアップが実行されます。結果は、SMTP ルート テーブルに対して再チェックされません。foo.domain の DNS MX エントリが bar.domain の場合、foo.domain に送信されるすべての電子メールが bar.domain に配信されます。bar.domain から他のホストへのマッピングを作成した場合、foo.domain へ送信される電子メールは影響を受けません。

つまり、再帰的なエントリは続きません。a.domain から b.domain にリダイレクトされるエントリがあり、b.domain から a.domain にリダイレクトされるエントリがある場合、メールのループは作成されません。この場合、a.domain に送信される電子メールは、b.domain で指定された MX ホストに配信されます。反対に、b.domain に送信される電子メールは、a.domain で指定された MX ホストに配信されます。

すべての電子メール配信で、SMTP ルート テーブルは、上から順に読み取られます。マッピングと一致する最も具体的なエントリが選択されます。たとえば、SMTP ルート テーブルで host1.example.com と .example.com の両方についてマッピングがある場合は、host1.example.com のエントリが使用されます。これは、具体的ではない .example.com エントリの後に出現した場合であっても、このエントリのほうが具体的なエントリであるためです。そうでない場合は、エンベロープ受信者のドメインで通常の MX ルックアップが実行されます。

デフォルトの SMTP ルート

特殊なキーワード ALL を使用して、デフォルトの SMTP ルートも定義できます。ドメインが SMTP ルート リストの以前のマッピングと一致しない場合、デフォルトでは、それが ALL エントリで指定される MX ホストにリダイレクトされます。

SMTP ルート エントリを印刷する場合、デフォルトの SMTP ルートは ALL: として一覧表示されます。デフォルトの SMTP ルートは削除できません。入力した値をクリアすることのみ可能です。

デフォルトの SMTP ルートを設定するには、[ネットワーク (Network)] > [SMTP ルート (SMTP Routes)] ページまたは smtproutes コマンドを使用します。

SMTP ルートの定義

ルートを構築するには、[ネットワーク (Network)] > [SMTP ルート (SMTP Routes)] ページ (または smtproutes コマンド) を使用します。新しいルートを作成するには、まず、永続的なルートを作成するドメインまたはドメインの一部を指定する必要があります。次に、宛先ホストを指定します。宛先

ホストは、完全修飾ホスト名として入力することも、IP アドレスとして入力することもできます。IP アドレスは、インターネット プロトコル バージョン 4 (IPv4) またはバージョン 6 (IPv6) を指定できます。

IPv6 アドレスの場合、AsyncOS は次の形式をサポートします。

- 2620:101:2004:4202::0-2620:101:2004:4202::ff
- 2620:101:2004:4202::
- 2620:101:2004:4202::23
- 2620:101:2004:4202::/64

エントリと一致するメッセージをドロップするために、特殊な宛先ホスト `/dev/null` を指定することもできます。(実際に `/dev/null` をデフォルト ルートに指定すると、アプライアンスが受信したメールは配信されなくなります)。

受信側のドメインに複数の宛先ホストを設定できます。MX レコードと同様に、それぞれの宛先ホストにプライオリティ番号を割り当てます。最低番号が割り当てられた宛先ホストは、受信側ドメインのプライマリ宛先ホストであることを示します。一覧にある他の宛先ホストは、バックアップとして使用されます。

プライオリティが同じ宛先は、「ラウンドロビン」方式で使用されます。ラウンドロビン処理は、SMTP 接続に基づいていて、必ずしもメッセージに基づくものではありません。また、1 つ以上の宛先ホストが応答しない場合は、到達可能ないずれかのホストにメッセージが配信されます。設定されているすべての宛先ホストが応答しない場合、メールは受信側ドメインのキューに入れられ、宛先ホストへの配信が後で試みられます。(MX レコードの使用へのフェールオーバーは行われません)。

CLI で `smtproutes` コマンドを使用してルートを構築するときは、ホスト名または IP アドレスに続けて `/pri=` とその後にプライオリティを割り当てるための整数 `0 ~ 65535` (`0` は最高のプライオリティ) を使用して、各宛先ホストにプライオリティを設定できます。たとえば、`host1.example.com/pri=0` のプライオリティは、`host2.example.com/pri=10` よりも高くなります。複数のエントリを指定する場合は、カンマで区切ります。

SMTP ルートの制限

最大 40,000 ルートまで定義できます。最後のデフォルト ルート `ALL` は、この制限内のルートとしてカウントされます。そのため、定義できるのは最大 39,999 個のカスタム ルートと、特殊なキーワード `ALL` を使用する 1 つのルートです。

SMTP ルートと DNS

MX ルックアップを実行して、特定のドメインに対するネクスト ホップを決定するようアプライアンスに指示するには、特殊キーワード `USEDNS` を使用します。これは、サブドメインのメールを特定のホストにルーティングする必要がある場合に役立ちます。たとえば、`example.com` へのメールが企業の Exchange サーバに送信されることになっている場合、次のような SMTP ルートになっていることがあります。

```
example.com exchange.example.com
```

ただし、さまざまなサブドメイン (`foo.example.com`) 宛のメールの場合は、次のような SMTP ルートを追加します。

```
.example.com USEDNS
```

SMTP ルートおよびアラート

[システム管理 (System Administration)] > [アラート (Alerts)] ページ (または `alertconfig` コマンド) で指定されたアドレスにアプライアンスから送信されたアラートは、これらの宛先に対して定義された SMTP ルートに従います。

SMTP ルート、メール配信、およびメッセージ分裂

着信: 1 つのメッセージに 10 人の受信者がいて、全員が同じ Exchange サーバに属する場合、AsyncOS では TCP 接続を 1 つ開き、メールストアには 10 の別々のメッセージではなく、メッセージを 1 つのみ配置します。

発信: 同様に機能しますが、1 つのメッセージが 10 の異なるドメインの 10 人の受信者に送られる場合、AsyncOS では 10 の MTA に対する 10 の接続を開き、それぞれに 1 つずつ電子メール配信を行います。

分裂: 1 つの着信メッセージに 10 人の受信者がいて、それぞれが別々の Incoming Policy グループ (10 グループ) に属する場合、10 人全員の受信者が同じ Exchange サーバを使用している場合、メッセージは分裂します。つまり、10 の別々の電子メールが 1 つの TCP 接続で配信されます。

SMTP ルートと発信 SMTP 認証

発信 SMTP 認証プロファイルが作成されたら、SMTP ルートに適用できます。これによって、ネットワークエッジにあるメールリレーサーバの背後に Cisco アプライアンスが配置されている場合に、発信メールを認証できます。発信 SMTP 認証の詳細については、「[発信 SMTP 認証](#)」(P.22-39) を参照してください。

GUI を使用した発信電子メール送信の SMTP ルート管理

Cisco アプライアンスの SMTP ルートを管理するには、[ネットワーク (Network)] > [SMTP ルート (SMTP Routes)] ページを使用します。テーブルでマッピングの追加、変更、および削除ができます。SMTP ルート エントリをエクスポートまたはインポートすることができます。

SMTP ルートの追加

手順

- ステップ 1** [ネットワーク (Network)] > [SMTP ルート (SMTP Routes)] ページの [ルートを追加 (Add Route)] をクリックします。
- ステップ 2** 受信ドメインを入力します。ここでは、ホスト名、ドメイン、IPv4 アドレス、または IPv6 アドレスを指定できます。
- ステップ 3** 宛先ホストを入力します。ここでは、ホスト名、IPv4 アドレス、または IPv6 アドレスを指定できます。複数の宛先ホストを追加するには、[行を追加 (Add Row)] をクリックし、新しい行に次の宛先ホストを入力します。



(注) ポート番号を指定するには、宛先ホストに「:<ポート番号>」を追加します (例: `example.com:25`)。

- ステップ 4** 複数の宛先ホストを追加する場合は、0 ~ 65535 の整数を入力してホストのプライオリティを割り当てます。0 が最上位の優先レベルです。詳細については、「SMTP ルートの定義」(P.21-2) を参照してください。
- ステップ 5** 変更内容を送信し、確定します。
-

SMTP ルートのエクスポート

ホスト アクセス テーブル (HAT) および受信者アクセス テーブル (RAT) の場合と同様に、ファイルをエクスポートおよびインポートして SMTP ルート マッピングを変更することもできます。SMTP ルートをエクスポートするには、次の手順に従います。

手順

- ステップ 1** [SMTP ルート (SMTP Routes)] ページの [SMTP ルートをエクスポート (Export SMTP Routes)] をクリックします。
- ステップ 2** ファイルの名前を入力し、[送信 (Submit)] をクリックします。
-

SMTP ルートのインポート

ホスト アクセス テーブル (HAT) および受信者アクセス テーブル (RAT) の場合と同様に、ファイルをエクスポートおよびインポートして SMTP ルート マッピングを変更することもできます。SMTP ルートをインポートするには、次の手順に従います。

手順

- ステップ 1** [SMTP ルート (SMTP Routes)] ページの [SMTP ルートをインポート (Import SMTP Routes)] をクリックします。
- ステップ 2** エクスポートされた SMTP ルートが含まれているファイルを選択します。
- ステップ 3** [送信 (Submit)] をクリックします。インポートにより、既存の SMTP ルートがすべて置き換えられることが警告されます。テキスト ファイルにあるすべての SMTP ルートがインポートされます。
- ステップ 4** [インポート (Import)] をクリックします。

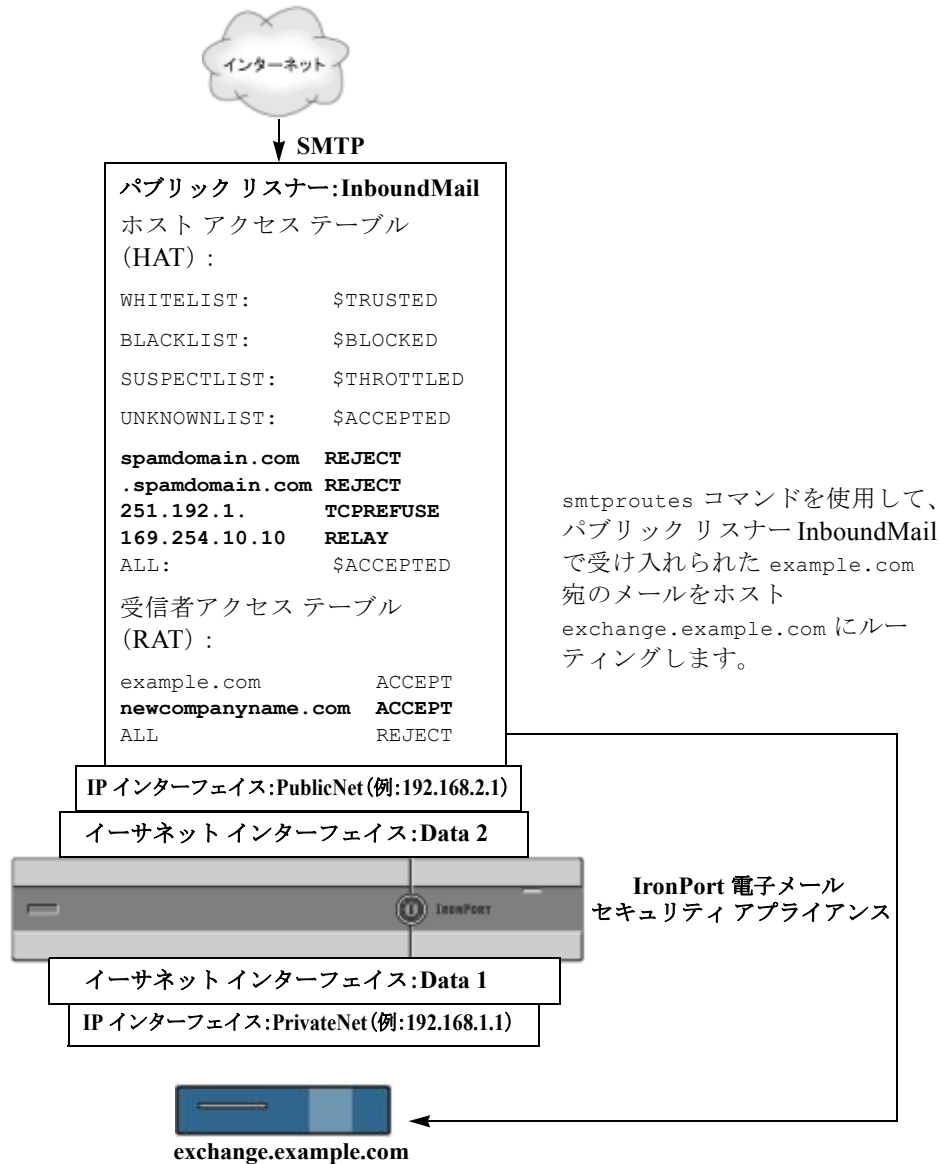
ファイルには「コメント」を格納できます。文字「#」で始まる行はコメントと見なされ、AsyncOS によって無視されます。次に例を示します。

```
# this is a comment, but the next line is not
```

```
ALL:
```

この時点で、電子メール ゲートウェイの設定は次のようになります。

図 21-1 パブリック リスナー用に定義された SMTP ルート



アドレスの書き換え

AsyncOS では、電子メール パイプラインでエンベロープ送信者および受信者のアドレスを書き換える方法が複数あります。アドレスの書き換えは、たとえばパートナー ドメインに送信されたメールをリダイレクトする場合や、社内インフラストラクチャを隠す（マスクする）場合に使用できます。

表 21-1 に、送信者および受信者の電子メール アドレスを書き換えるために使用される各種機能の概要を示します。

表 21-1 アドレスの書き換え方法

元のアドレス	変更後	機能	作業対象
*@anydomain	user@domain	エイリアス テーブル (「エイリアス テーブルの作成」(P.21-7) を参照)	<ul style="list-style-type: none"> エンベロープ受信者のみ グローバルに適用 エイリアスを電子メール アドレスまたは他のエイリアスにマッピング
*@olddomain	*@newdomain	ドメイン マッピング (「ドメイン マップ機能」(P.21-28) を参照)	<ul style="list-style-type: none"> エンベロープ受信者のみ リスナーごとに適用
*@olddomain	*@newdomain	マスカレード (「マスカレードの設定」(P.21-16) を参照)	<ul style="list-style-type: none"> エンベロープ送信者、および To:、From:、または CC: ヘッダー リスナーごとに適用

エイリアス テーブルの作成

エイリアス テーブルを使用すると、1 人または複数の受信者にメッセージをリダイレクトできます。エイリアスからユーザ名や他のエイリアスへのマッピング テーブルは、一部の UNIX システムで `sendmail` コンフィギュレーションの `/etc/mail/aliases` 機能と同様の方法で作成できます。

リスナーが受信した電子メールのエンベロープ受信者 (Envelope To または RCPT TO と呼ばれます) がエイリアス テーブルで定義されているエイリアスと一致すると、電子メールのエンベロープ受信者 アドレスが書き換えられます。



(注) RAT チェックの後からメッセージフィルタの前までに、リスナーはエイリアス テーブルをチェックし、受信者を変更します。『Cisco IronPort AsyncOS for Email Configuration Guide』の「Understanding the Email Pipeline」を参照してください。



(注) エイリアス テーブル機能により、電子メールのエンベロープ受信者が実際に書き換えられます。これは、電子メールのエンベロープ受信者を書き換えず、電子メールを指定されたドメインに再ルーティングするだけの `smtproutes` コマンド (「バウンスした電子メールの処理」(P.21-36) を参照) とは異なります。

コマンドラインによるエイリアス テーブルの設定

エイリアス テーブルはセクションで定義します。各セクションの先頭にはドメイン コンテキスト (そのセクションに関連するドメインのリスト) があり、その後にマップのリストが続きます。

ドメイン コンテキストは、1 つ以上のドメインまたは部分ドメインのリストです。カンマで区切り、角カッコ (「[」および「]」) で囲みます。ドメインは、文字、数字、ハイフン、およびピリオドで構成される文字列です (RFC 1035、セクション 2.3.1. の「Preferred name syntax」を参照)。部分ドメイン (.example.com など) は、ピリオドで始まるドメインです。部分ドメインに一致するサブ文字列で終わるようなすべてのドメインは、一致であると見なされます。たとえば、ドメイン コンテキスト

.example.com は、mars.example.com および venus.example.com と一致します。ドメイン コンテキストの後には、マップ（エイリアスと受信者リスト）のリストがあります。マップは、次のように構成されます。

表 21-2 エイリアス テーブルの構文

左辺 (LHS)	区切り文字	右辺 (RHS)
一致する 1 つ以上のエイリアスのリスト	コロン文字 (':')	1 つ以上の受信者アドレスまたはエイリアスのリスト

左辺のエイリアスでは、次の形式を使用できます。

username	一致するエイリアスを指定します。先行する「ドメイン」属性がテーブルで指定されている必要があります。このパラメータがないと、エラーになります。
user@domain	一致する正確な電子メールアドレスを指定します。

左辺 1 行あたり複数のエイリアスをカンマで区切って入力できます。

右辺の各受信者は、user@domain 形式の完全な電子メールアドレス、または別のエイリアスを指定できます。

エイリアス ファイルには、暗黙的なドメインのない「グローバルな」エイリアス（特定ドメインではなく、グローバルに適用されるエイリアス）、エイリアスに 1 つ以上の暗黙的なドメインのあるドメイン コンテキスト、またはその両方を指定できます。

エイリアスの「チェーン」（再帰的なエントリ）を作成することはできますが、完全な電子メールアドレスで終わる必要があります。

sendmail コンフィギュレーションのコンテキストと互換性を持たせるために、メッセージをドロップするための特殊な宛先である /dev/null がサポートされています。エイリアス テーブルによってメッセージが /dev/null にマッピングされると、ドロップ済みカウンタが増分します。（『Cisco IronPort AsyncOS for Email Daily Management Guide』の「Managing and Monitoring via the CLI」を参照）。受信者は受け入れられますが、キューには入りません。

エイリアス テーブルのエクスポートおよびインポート

エイリアス テーブルをインポートするには、先に付録 A 「アプライアンスへのアクセス」を確認し、アプライアンスにアクセスできるようにします。

既存のエイリアス テーブルを保存するには、aliasconfig コマンドの export サブコマンドを使用します。ファイル（ファイル名は自分で指定）は、リスナーの /configuration ディレクトリに書き込まれます。このファイルを CLI の外部で変更し、インポートし直すことができます。（ファイルに不正な形式のエントリがある場合は、ファイルのインポート時にエラーが出力されます）。

エイリアス テーブル ファイルを /configuration ディレクトリに配置し、aliasconfig コマンドの import サブコマンドを使用してファイルをアップロードします。

テーブルの行の先頭でナンバー記号 (#) を使用すると、その行がコメントアウトされます。

コンフィギュレーションの変更が反映されるように、必ずエイリアス テーブル ファイルをインポートした後で commit コマンドを発行してください。

エイリアス テーブルのエントリの削除

コマンドライン インターフェイス (CLI) を使用してエイリアス テーブルからエントリを削除する場合は、先にドメイングループを選択するように求められます。「ALL (any domain)」エントリを選択すると、すべてのドメインに適用されるエイリアスの番号付きリストが表示されます。その後、削除するエイリアスの番号を選択します。

エイリアス テーブルの例



(注)

このテーブル例のすべてのエントリは、コメントアウトされています。

```
# sample Alias Table file

# copyright (c) 2001-2005, IronPort Systems, Inc.

#

# Incoming Envelope To addresses are evaluated against each
# entry in this file from top to bottom. The first entry that
# matches will be used, and the Envelope To will be rewritten.

#

# Separate multiple entries with commas.

#

# Global aliases should appear before the first domain
# context. For example:

#

#   admin@example.com: administrator@example.com

#   postmaster@example.net: administrator@example.net

#

# This alias has no implied domain because it appears
# before a domain context:

#

#   someaddr@somewhere.dom: specificperson@here.dom

#

# The following aliases apply to recipients @ironport.com and
```

```
# any subdomain within .example.com because the domain context
# is specified.
#
# Email to joe@ironport.com or joe@foo.example.com will
# be delivered to joseph@example.com.
#
# Similarly, email to fred@mx.example.com will be
# delivered to joseph@example.com
#
# [ironport.com, .example.com]
#
# joe, fred: joseph@example.com
#
#
# In this example, email to partygoers will be sent to
# three addresses:
#
# partygoers: wilma@example.com, fred@example.com, barney@example.com
#
# In this example, mail to help@example.com will be delivered to
# customercare@otherhost.dom. Note that mail to help@ironport.com will
# NOT be processed by the alias table because the domain context
# overrides the previous domain context.
#
# [example.com]
#
# help: customercare@otherhost.dom
#
# In this example, mail to nobody@example.com is dropped.
```

```
#
# nobody@example.com: /dev/null
#
# "Chains" may be created, but they must end in an email address.
# For example, email to "all" will be sent to 9 addresses:
#
# [example.com]
#
# all: sales, marketing, engineering
# sales: joe@example.com, fred@example.com, mary@example.com
# marketing:bob@example.com, advertising
# engineering:betty@example.com, miles@example.com, chris@example.com
# advertising:richard@example.com, karen@advertising.com
```

aliasconfig コマンドの例

この例では、`aliasconfig` コマンドを使用してエイリアス テーブルを作成します。まず、`example.com` のドメイン コンテキストを指定します。次に、`customercare` のエイリアスを作成し、`customercare@example.com` に送信されたすべての電子メールが `bob@example.com`、`frank@example.com`、および `sally@example.com` にリダイレクトされるようにします。さらに、`admin` のグローバル エイリアスを作成し、`admin` に送信された電子メールが `administrator@example.com` にリダイレクトされるようにします。最後に、確認用にエイリアス テーブルが出力されます。

テーブルの出力時に、`admin` のグローバル エイリアスは、`example.com` の最初のドメイン コンテキストの *前* に出力されます。

```
mail3.example.com> aliasconfig

No aliases in table.

Choose the operation you want to perform:

- NEW - Create a new entry.
- IMPORT - Import aliases from a file.

[ ]> new
```

How do you want your aliases to apply?

1. Globally
2. Add a new domain context

[1]> **2**

Enter new domain context.

Separate multiple domains with commas.

Partial domains such as .example.com are allowed.

[> **example.com**

Enter the alias(es) to match on.

Separate multiple aliases with commas.

Allowed aliases:

- "user" - This user in this domain context.
- "user@domain" - This email address.

[> **customercare**

Enter address(es) for "customercare".

Separate multiple addresses with commas.

[> **bob@example.com, frank@example.com, sally@example.com**

Adding alias customercare: bob@example.com,frank@example.com,sally@example.com

Do you want to add another alias? [N]> **n**

There are currently 1 mappings defined.

Choose the operation you want to perform:

- NEW - Create a new entry.
- EDIT - Modify an entry.

- DELETE - Remove an entry.
- PRINT - Display the table.
- IMPORT - Import aliases from a file.
- EXPORT - Export table to a file.
- CLEAR - Clear the table.

[> **new**

How do you want your aliases to apply?

1. Globally
2. Add a new domain context
3. example.com

[1]> **1**

Enter the alias(es) to match on.

Separate multiple aliases with commas.

Allowed aliases:

- "user@domain" - This email address.
- "user" - This user for any domain
- "@domain" - All users in this domain.
- "@.partialdomain" - All users in this domain, or any of its sub domains.

[> **admin**

Enter address(es) for "admin".

Separate multiple addresses with commas.

[> **administrator@example.com**

Adding alias admin: administrator@example.com

Do you want to add another alias? [N]> **n**

```
There are currently 2 mappings defined.
```

```
Choose the operation you want to perform:
```

- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- PRINT - Display the table.
- IMPORT - Import aliases from a file.
- EXPORT - Export table to a file.
- CLEAR - Clear the table.

```
[ ]> print
```

```
admin: administrator@example.com
```

```
[ example.com ]
```

```
customer: bob@example.com, frank@example.com, sally@example.com
```

```
There are currently 2 mappings defined.
```

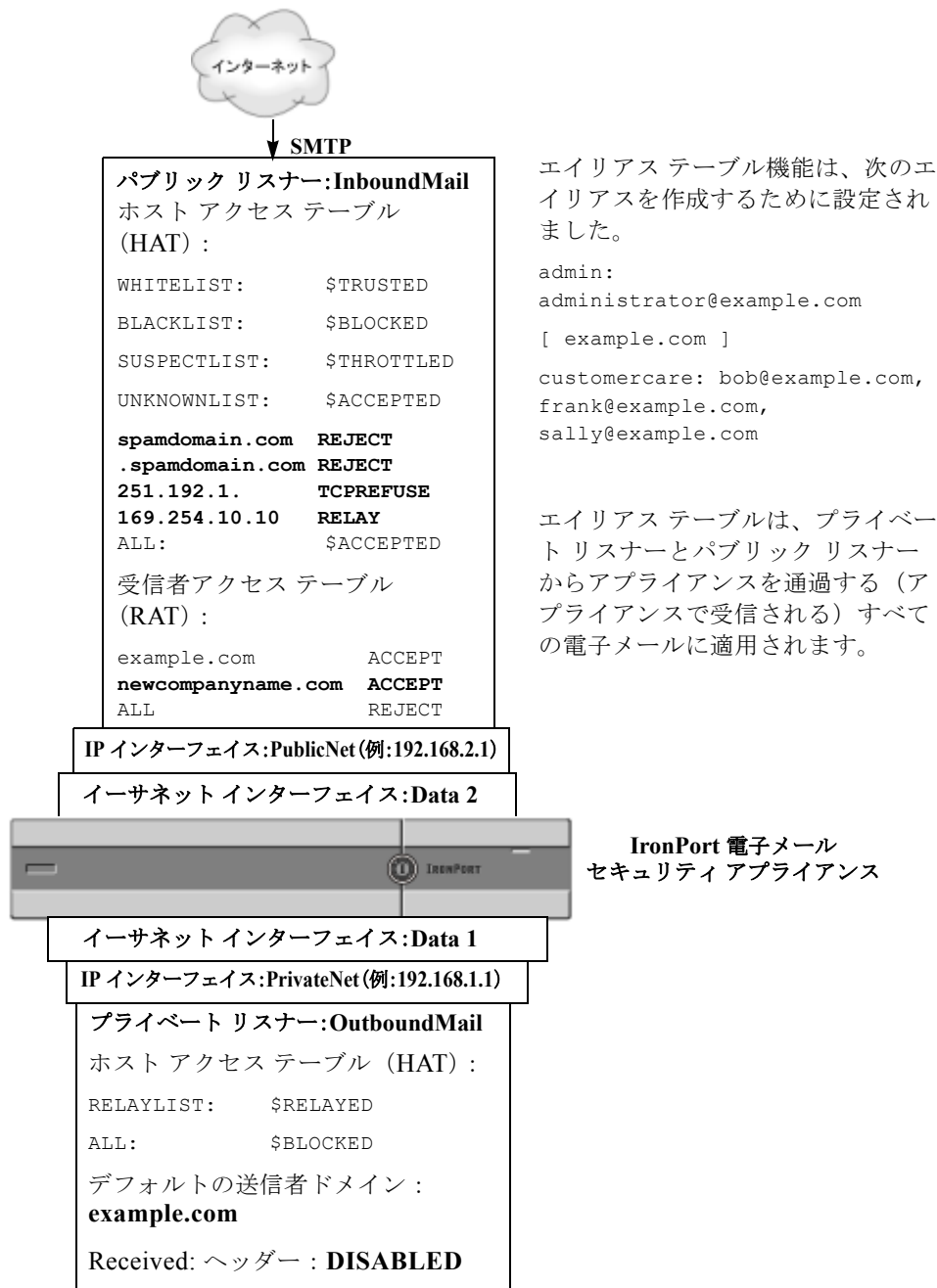
```
Choose the operation you want to perform:
```

- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- PRINT - Display the table.
- IMPORT - Import aliases from a file.
- EXPORT - Export table to a file.
- CLEAR - Clear the table.

```
[ ]>
```

この時点で、電子メール ゲートウェイの設定は次のようになります。

図 21-2 アプライアンスに定義されたエイリアス テーブル



マスカレードの設定

マスカレードは、作成したテーブルに従って、エンベロープ送信者（送信者または MAIL FROM と呼ばれます）、およびリスナーで処理される電子メールの To:、From:、CC: ヘッダーを書き換える機能です。この機能の典型的な実装例は、「仮想ドメイン」です。単一のサイトから複数のドメインをホストできます。もう一つの典型的な実装は、電子メールヘッダー内の文字列からサブドメインを「取り除く」ことで、ネットワークインフラストラクチャを「隠す」ことです。マスカレード機能は、プライベートリスナーとパブリックリスナーの両方で利用できます。



(注) マスカレード機能は、システム全体に対して設定するエイリアステーブル機能とは異なり、リスナー単位で設定します。



(注) リスナーは、LDAP 受信者受け入れクエリーの直後で LDAP ルーティングクエリーの前、メッセージがワークキュー内にある間に、マスカレードテーブルで一致を探して受信者を変更します。『Cisco IronPort AsyncOS for Email Configuration Guide』の「Understanding the Email Pipeline」を参照してください。

マスカレード機能により、エンベロープ送信者および受信した電子メールの To:、From:、CC: フィールドのアドレスが実際に書き換えられます。作成するリスナーごとに別々のマスカレードパラメータを指定できます。2 つある方法のいずれかを使用します。

- 作成したマッピングのスタティックテーブルを使用
- LDAP クエリーを使用

この項では、スタティックテーブルを使用する方法について説明します。テーブルの形式は、一部の UNIX システムで sendmail コンフィギュレーションの /etc/mail/genericstable 機能と上位互換性があります。LDAP マスカレードクエリーの詳細については、第 22 章「LDAP クエリー」を参照してください。

マスカレードと altsrchoost

一般に、マスカレード機能ではエンベロープ送信者が書き換えられ、メッセージで実行されるそれ以降のアクションは、マスカレードされたアドレスから「トリガー」されます。ただし、CLI から altsrchoost コマンドを実行した場合、altsrchoost マッピングは元のアドレスからトリガーされます（つまり変更後のマスカレードされたアドレスではない）。

詳細については、「Virtual Gateway™ テクノロジーを使用してすべてのホストされたドメインでの構成のメールゲートウェイ」(P.21-59) および「確認：電子メールパイプライン」(P.21-73) を参照してください。

スタティック マスカレード テーブルの設定

マッピングのスタティック マスカレード テーブルを設定するには、listenerconfig コマンドの edit -> masquerade サブコマンドを使用します。また、マッピングが含まれるファイルをインポートできます。「マスカレード テーブルのインポート」(P.21-18) を参照してください。このサブコマンドにより、入力アドレス、ユーザ名、およびドメインを新しいアドレスおよびドメインにマッピングするテーブルを作成および維持します。LDAP マスカレードクエリーの詳細については、第 22 章「LDAP クエリー」を参照してください。

メッセージがシステムに挿入されるときは、テーブルが参照され、ヘッダーに一致が見つかったらメッセージが書き換えられます。

ドメインのマスカレードテーブルは、次のように構成されます。

表 21-3 マスカレード テーブルの構文

左辺 (LHS)	区切り文字	右辺 (RHS)
一致する 1 つ以上のユーザ名やドメインのリスト	空白文字 (スペースまたはタブ文字)	書き換え後のユーザ名やドメイン

次の表に、マスカレードテーブルで有効なエントリを示します。

左辺 (LHS)	右辺 (RHS)
username	username@domain
このエントリは、一致するユーザ名を指定します。左辺のユーザ名に一致する着信電子メールメッセージは、一致となり、右辺のアドレスで書き換えられます。右辺は、完全なアドレスである必要があります。	
user@domain	username@domain
このエントリは、一致する正確なアドレスを指定します。左辺の完全なアドレスに一致する着信メッセージは、右辺のアドレスで書き換えられます。右辺は、完全なアドレスである必要があります。	
@domain	@domain
このエントリは、特定のドメインの任意のアドレスを指定します。左辺の元のドメインは、右辺のドメインで置き換えられますが、ユーザ名は変更ありません。	
@.partialdomain	@domain
このエントリは、特定のドメインの任意のアドレスを指定します。左辺の元のドメインは、右辺のドメインで置き換えられますが、ユーザ名は変更ありません。	
All	@domain
ALL エントリは、そのままのアドレスに一致し、右辺のアドレスで書き換えます。右辺は、ドメインの先頭に「@」を付ける必要があります。このエントリは、テーブル内の位置に関係なく、常に優先度最低になります。	
(注) ALL エントリは、プライベートリスナーのみに使用できます。	

- ルールは、マスカレードテーブルでの出現順序に従って一致します。
- デフォルトでは受信時にヘッダーの From:、To:、および CC: フィールド内のアドレスが一致し、書き換えられます。エンベロープ送信者に一致して書き換えるようにオプションを設定することもできます。エンベロープ送信者および書き換え対象ヘッダーは、config サブコマンドを使用して有効と無効を切り替えます。
- テーブルの行の先頭でナンバー記号 (#) を使用すると、その行がコメントアウトされます。# から行の末尾まで、すべてコメントであると見なされて無視されます。
- マスカレードテーブルは、最大で 400,000 エントリです。これは、new サブコマンドを使ってエントリ作成した場合も、ファイルからインポートした場合も同じです。

プライベート リスナー用マスカレード テーブルの例

```
# sample Masquerading file

@example.com @example.com # Hides local subdomains in the header

sales sales_team@success.com

@techsupport tech_support@biggie.com

user@localdomain user@company.com

ALL @bigsender.com
```

マスカレード テーブルのインポート

従来の `sendmail` の `/etc/mail/genericstable` ファイルをインポートできます。`genericstable` ファイルをインポートするには、先に付録 A 「アプライアンスへのアクセス」を確認し、アプライアンスにアクセスできるようにします。

`genericstable` ファイルを `configuration` ディレクトリに配置し、`masquerade` サブコマンドの `import` サブコマンドを使用してファイルをアップロードします。コマンドは、次の順序で使用します。

```
listenerconfig -> edit -> injector_number -> masquerade -> import
```

または、`export` サブコマンドを使用して既存のコンフィギュレーションをダウンロードできます。ファイル（ファイル名は自分で指定）は、`configuration` ディレクトリに書き込まれます。このファイルを CLI の外部で変更し、インポートし直すことができます。

`import` サブコマンドを使用するときは、ファイルに有効なエントリのみが含まれているようにしてください。無効なエントリ（左辺があって右辺がない場合など）があると、ファイルのインポート時に CLI で構文エラーが発生します。インポート中に構文エラーが発生すると、ファイル全体でマッピングがインポートされません。

リスナーのコンフィギュレーションの変更内容が反映されるように、`genericstable` ファイルをインポートした後で必ず `commit` コマンドを発行してください。

マスカレードの例

この例では、`listenerconfig` の `masquerade` サブコマンドを使用して、PrivateNet インターフェイス上にある「OutboundMail」という名前のプライベート リスナー用に、ドメイン マスカレード テーブルを作成します。

まず、マスカレードに LDAP を使用するオプションを宣言します。（LDAP マスカレード クエリーの詳細については、第 22 章 「LDAP クエリー」を参照してください）。

次に、`@example.com` の部分ドメイン表記が `@example.com` にマッピングされます。これにより、サブドメイン `.example.com` 内にある任意のマシンから送信されるすべての電子メールが `example.com` にマッピングされます。さらに、ユーザ名 `joe` がドメイン `joe@example.com` にマッピングされます。両方のエントリを確認するためにドメイン マスカレード テーブルが出力されて、`masquerade.txt` という名前のファイルにエクスポートされます。`config` サブコマンドを使用して、CC: フィールドのアドレスの書き換えが無効になり、最後に変更が確定されます。

```
mail3.example.com> listenerconfig
```

Currently configured listeners:

1. InboundMail (on PublicNet, 192.168.2.1) SMTP TCP Port 25 Public
2. OutboundMail (on PrivateNet, 192.168.1.1) SMTP TCP Port 25 Private

Choose the operation you want to perform:

- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.

[> **edit**

Enter the name or number of the listener you wish to edit.

[> **2**

Name: OutboundMail

Type: Private

Interface: PrivateNet (192.168.1.1/24) TCP Port 25

Protocol: SMTP

Default Domain:

Max Concurrency: 600 (TCP Queue: 50)

Domain Map: Disabled

TLS: No

SMTP Authentication: Disabled

Bounce Profile: Default

Footer: None

LDAP: Off

Choose the operation you want to perform:

- NAME - Change the name of the listener.

- INTERFACE - Change the interface.
- LIMITS - Change the injection limits.
- SETUP - Configure general options.
- HOSTACCESS - Modify the Host Access Table.
- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this listener.
- MASQUERADE - Configure the Domain Masquerading Table.
- DOMAINMAP - Configure domain mappings.
- LDAPACCEPT - Configure an LDAP query to determine whether a recipient address should be accepted or bounced/dropped.
- LDAPROUTING - Configure an LDAP query to reroute messages.
- LDAPGROUP - Configure an LDAP query to determine whether a sender or recipient is in a specified group.
- SMTPAUTH - Configure an SMTP authentication.

```
[ ]> masquerade
```

```
Do you want to use LDAP for masquerading? [N]> n
```

```
Domain Masquerading Table
```

```
There are currently 0 entries.
```

```
Masqueraded headers: To, From, Cc
```

```
Choose the operation you want to perform:
```

- NEW - Create a new entry.
- DELETE - Remove an entry.
- PRINT - Display all entries.
- IMPORT - Import all entries from a file.
- EXPORT - Export all entries to a file.
- CONFIG - Configure masqueraded headers.

- CLEAR - Remove all entries.

[> **new**

Enter the source address or domain to masquerade.

Username like "joe" are allowed.

Full addresses like "user@example.com" are allowed.

Full addresses with subdomain wildcards such as "username@.company.com" are allowed.

Domains like @example.com and @.example.com are allowed.

Hosts like @training and @.sales are allowed.

[> **@.example.com**

Enter the masqueraded address or domain.

Domains like @example.com are allowed.

Full addresses such as user@example.com are allowed.

[> **@example.com**

Entry mapping @.example.com to @example.com created.

Domain Masquerading Table

There are currently 1 entries.

Masqueraded headers: To, From, Cc

Choose the operation you want to perform:

- NEW - Create a new entry.

- DELETE - Remove an entry.

- PRINT - Display all entries.

- IMPORT - Import all entries from a file.

- EXPORT - Export all entries to a file.

- CONFIG - Configure masqueraded headers.

- CLEAR - Remove all entries.

[> **new**

Enter the source address or domain to masquerade.

Username like "joe" are allowed.

Full addresses like "user@example.com" are allowed.

Full addresses with subdomain wildcards such as "username@.company.com" are allowed.

Domains like @example.com and @.example.com are allowed.

Hosts like @training and @.sales are allowed.

[> **joe**

Enter the masqueraded address.

Only full addresses such as user@example.com are allowed.

[> **joe@example.com**

Entry mapping joe to joe@example.com created.

Domain Masquerading Table

There are currently 2 entries.

Masqueraded headers: To, From, Cc

Choose the operation you want to perform:

- NEW - Create a new entry.

- DELETE - Remove an entry.

- PRINT - Display all entries.

- IMPORT - Import all entries from a file.

- EXPORT - Export all entries to a file.

- CONFIG - Configure masqueraded headers.

- CLEAR - Remove all entries.

```
[> print

@.example.com    @example.com
joe      joe@example.com

Domain Masquerading Table

There are currently 2 entries.

Masqueraded headers: To, From, Cc

Choose the operation you want to perform:
- NEW - Create a new entry.
- DELETE - Remove an entry.
- PRINT - Display all entries.
- IMPORT - Import all entries from a file.
- EXPORT - Export all entries to a file.
- CONFIG - Configure masqueraded headers.
- CLEAR - Remove all entries.

[> export

Enter a name for the exported file:

[> masquerade.txt

Export completed.

Domain Masquerading Table

There are currently 2 entries.

Masqueraded headers: To, From, Cc
```

Choose the operation you want to perform:

- NEW - Create a new entry.
- DELETE - Remove an entry.
- PRINT - Display all entries.
- IMPORT - Import all entries from a file.
- EXPORT - Export all entries to a file.
- CONFIG - Configure masqueraded headers.
- CLEAR - Remove all entries.

[>] **config**

Do you wish to masquerade Envelope Sender?

[N]> **y**

Do you wish to masquerade From headers?

[Y]> **y**

Do you wish to masquerade To headers?

[Y]> **y**

Do you wish to masquerade CC headers?

[Y]> **n**

Do you wish to masquerade Reply-To headers?

[Y]> **n**

Domain Masquerading Table

There are currently 2 entries.

- NEW - Create a new entry.
- DELETE - Remove an entry.
- PRINT - Display all entries.
- IMPORT - Import all entries from a file.
- EXPORT - Export all entries to a file.
- CONFIG - Configure masqueraded headers.
- CLEAR - Remove all entries.

[]>

Name: OutboundMail

Type: Private

Interface: PrivateNet (192.168.1.1/24) TCP Port 25

Protocol: SMTP

Default Domain:

Max Concurrency: 600 (TCP Queue: 50)

Domain Map: Disabled

TLS: No

SMTP Authentication: Disabled

Bounce Profile: Default

Footer: None

LDAP: Off

Choose the operation you want to perform:

- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- LIMITS - Change the injection limits.
- SETUP - Configure general options.
- HOSTACCESS - Modify the Host Access Table.

```
- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this listener.

- MASQUERADE - Configure the Domain Masquerading Table.

- DOMAINMAP - Configure domain mappings.

- LDAPACCEPT - Configure an LDAP query to determine whether a recipient address should be accepted or bounced/dropped.

- LDAPROUTING - Configure an LDAP query to reroute messages.

- LDAPGROUP - Configure an LDAP query to determine whether a sender or recipient is in a specified group.

- SMTPAUTH - Configure an SMTP authentication.

[]>
```

Currently configured listeners:

1. InboundMail (on PublicNet, 192.168.2.1) SMTP TCP Port 25 Public
2. OutboundMail (on PrivateNet, 192.168.1.1) SMTP TCP Port 25 Private

Choose the operation you want to perform:

```
- NEW - Create a new listener.

- EDIT - Modify a listener.

- DELETE - Remove a listener.

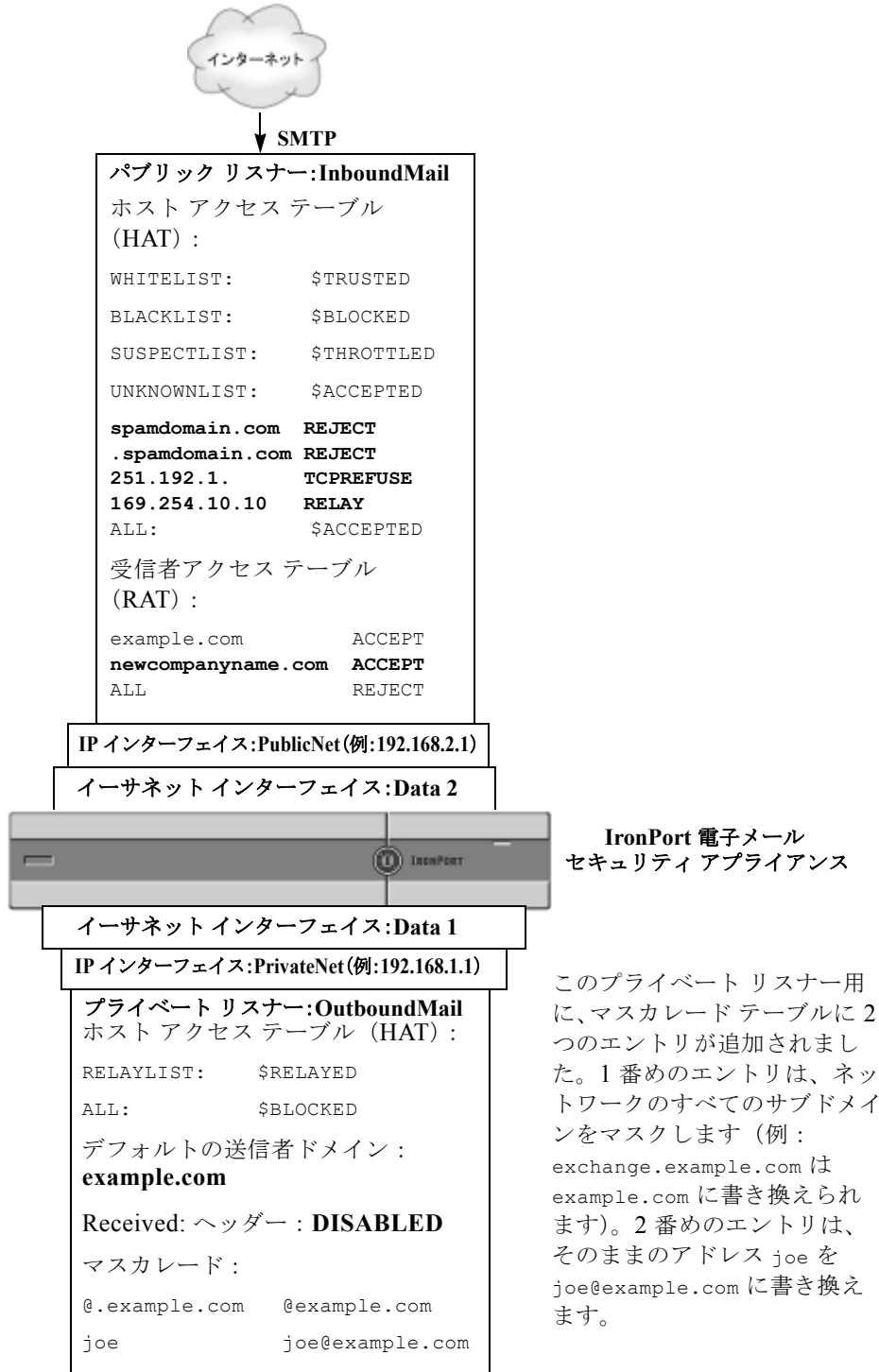
- SETUP - Change global settings.

[]>
```

```
mail3.example.com> commit
```

これでエンタープライズ ゲートウェイの設定は次のようになります。

図 21-3 プライベート リスナー用に定義されたマスカレード



ドメイン マップ機能

リスナー用に「ドメイン マップ」を設定できます。設定するリスナーごとにドメイン マップ テーブルを作成できます。ドメイン マップ テーブルに含まれているドメインと一致するメッセージでは、各受信者のエンベロープ受信者が書き換えられます。この機能は、sendmail の「ドメイン テーブル」機能または Postfix の「仮想テーブル」機能に似ています。この機能では、エンベロープ受信者のみが影響を受け、「To:」ヘッダーは書き換えられません。



(注)

ドメイン マップ機能の処理は、RAT の直前でデフォルト ドメインの評価直後に発生します。『Cisco IronPort AsyncOS for Email Configuration Guide』の「Understanding the Email Pipeline」を参照してください。

ドメイン マップ機能でよくある実装では、複数のレガシー ドメインの着信メールを受け入れます。たとえば、会社が他の会社を買収した場合に、Cisco アプライアンスにドメイン マップを作成して買収したドメインのメッセージを受け入れ、エンベロープ受信者を会社の現在のドメインに書き換えることができます。



(注)

一意のドメイン マッピングを最大で 20,000 個設定できます。

表 21-4 ドメイン マップ テーブルの構文の例

左側	右側	コメント
username@example.com	username2@example.net	右側は完全なアドレスのみ
user@.example.com	user2@example.net	
@example.com	user@example.net または @example.net	完全なアドレス、または完全修飾ドメイン名。
@.example.com	user@example.net または @example.net	

次の例では、listenerconfig コマンドの domainmap サブコマンドを使用して、パブリック リスナー「InboundMail」用のドメイン マップが作成されます。このドメイン、および oldcompanyname.com のサブドメインのメールは、ドメイン example.com にマッピングされます。マッピングは、確認のために出力されます。この例は、両方のドメインをリスナーの RAT に配置するコンフィギュレーションとは異なります。ドメイン マップ機能により、実際にエンベロープ受信者 joe@oldcompanyname.com が joe@example.com に書き換えられます。一方、リスナーの RAT 内にドメイン oldcompanyname.com を置くと、joe@oldcompanyname.com のメールが受け入れられて、エンベロープ受信者を書き換えずにルーティングされます。また、エイリアス テーブル機能とも異なります。エイリアス テーブルでは、明示的なアドレスに解決されることが必要です。「任意のユーザ名@domain」を「同じユーザ名@newdomain」にマッピングするようには作成できません。

```
mail3.example.com> listenerconfig
```

```
Currently configured listeners:
```


1. Inboundmail (on PublicNet, 192.168.2.1) SMTP TCP Port 25 Public
2. Outboundmail (on PrivateNet, 192.168.1.1) SMTP TCP Port 25 Private

Choose the operation you want to perform:

- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.

[> **edit**

Enter the name or number of the listener you wish to edit.

[> **1**

Name: InboundMail

Type: Public

Interface: PublicNet (192.168.2.1/24) TCP Port 25

Protocol: SMTP

Default Domain:

Max Concurrency: 1000 (TCP Queue: 50)

Domain Map: Disabled

TLS: No

SMTP Authentication: Disabled

Bounce Profile: Default

Use SenderBase For Reputation Filters and IP Profiling: Yes

Footer: None

LDAP: Off

Choose the operation you want to perform:

- NAME - Change the name of the listener.

1. Inboundmail (on PublicNet, 192.168.2.1) SMTP TCP Port 25 Public
2. Outboundmail (on PrivateNet, 192.168.1.1) SMTP TCP Port 25 Private

Choose the operation you want to perform:

- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.

[]> **edit**

Enter the name or number of the listener you wish to edit.

[]> **1**

Name: InboundMail

Type: Public

Interface: PublicNet (192.168.2.1/24) TCP Port 25

Protocol: SMTP

Default Domain:

Max Concurrency: 1000 (TCP Queue: 50)

Domain Map: Disabled

TLS: No

SMTP Authentication: Disabled

Bounce Profile: Default

Use SenderBase For Reputation Filters and IP Profiling: Yes

Footer: None

LDAP: Off

Choose the operation you want to perform:

- NAME - Change the name of the listener.

- INTERFACE - Change the interface.
- LIMITS - Change the injection limits.
- SETUP - Configure general options.
- HOSTACCESS - Modify the Host Access Table.
- RCPTACCESS - Modify the Recipient Access Table.
- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this listener.
- MASQUERADE - Configure the Domain Masquerading Table.
- DOMAINMAP - Configure domain mappings.

```
[> domainmap
```

```
Domain Map Table
```

```
There are currently 0 Domain Mappings.
```

```
Domain Mapping is: disabled
```

```
Choose the operation you want to perform:
```

- NEW - Create a new entry.
- IMPORT - Import domain mappings from a file.

```
[> new
```

```
Enter the original domain for this entry.
```

```
Domains such as "@example.com" are allowed.
```

```
Partial hostnames such as "@.example.com" are allowed.
```

```
Email addresses such as "test@example.com" and "test@.example.com"
are also allowed.
```

```
[> @.oldcompanyname.com
```

```
Enter the new domain for this entry.
```

The new domain may be a fully qualified
such as "@example.domain.com" or a complete
email address such as "test@example.com"

```
[ ]> @example.com
```

Domain Map Table

There are currently 1 Domain Mappings.

Domain Mapping is: enabled

Choose the operation you want to perform:

- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- PRINT - Display all domain mappings.
- IMPORT - Import domain mappings from a file.
- EXPORT - Export domain mappings to a file.
- CLEAR - Clear all domain mappings.

```
[ ]> print
```

```
@.oldcompanyname.com --> @example.com
```

Domain Map Table

There are currently 1 Domain Mappings.

Domain Mapping is: enabled

Choose the operation you want to perform:

- NEW - Create a new entry.

- EDIT - Modify an entry.
- DELETE - Remove an entry.
- PRINT - Display all domain mappings.
- IMPORT - Import domain mappings from a file.
- EXPORT - Export domain mappings to a file.
- CLEAR - Clear all domain mappings.

[]>

Name: InboundMail

Type: Public

Interface: PublicNet (192.168.2.1/24) TCP Port 25

Protocol: SMTP

Default Domain:

Max Concurrency: 1000 (TCP Queue: 50)

Domain Map: Enabled

TLS: No

SMTP Authentication: Disabled

Bounce Profile: Default

Use SenderBase For Reputation Filters and IP Profiling: Yes

Footer: None

LDAP: Off

Choose the operation you want to perform:

- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- LIMITS - Change the injection limits.
- SETUP - Configure general options.
- HOSTACCESS - Modify the Host Access Table.
- RCPTACCESS - Modify the Recipient Access Table.

- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this listener.
 - MASQUERADE - Configure the Domain Masquerading Table.
 - DOMAINMAP - Configure domain mappings.
- []>

ドメイン マップ テーブルのインポートおよびエクスポート

ドメイン マップ テーブルをインポートまたはエクスポートするには、先に[付録 A 「アプライアンスへのアクセス」](#)を確認し、アプライアンスにアクセスできるようにします。

マッピングするドメインのエントリが含まれるテキスト ファイルを作成します。エントリは空白文字 (タブ文字またはスペース) で区切ります。テーブルの行の先頭でナンバー記号 (#) を使用すると、その行がコメントアウトされます。

ファイルを **configuration** ディレクトリに配置し、**domain** サブコマンドの **import** サブコマンドを使用してファイルをアップロードします。コマンドは、次の順序で使用します。

```
listenerconfig -> edit -> injector_number -> domainmap -> import
```

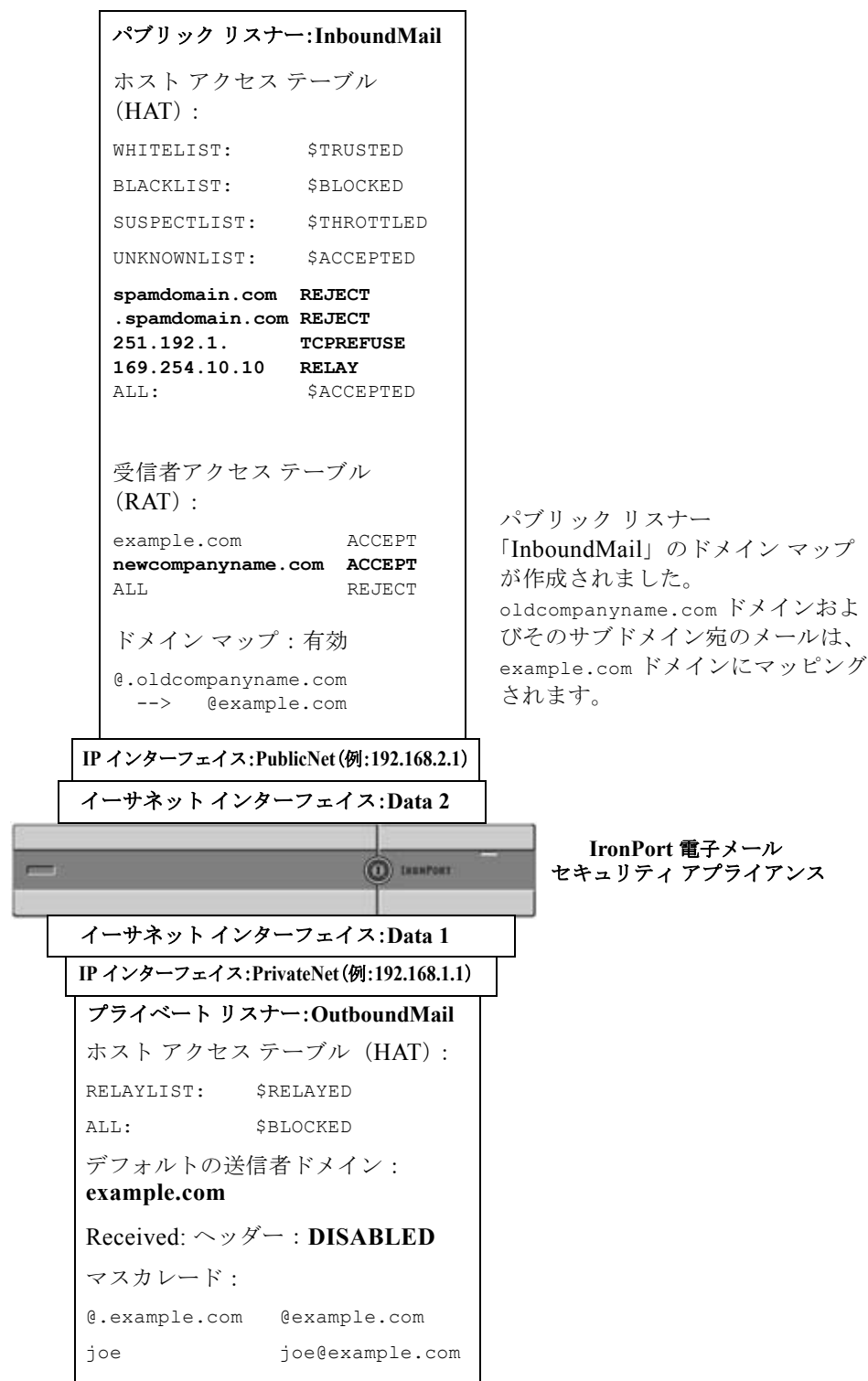
または、**export** サブコマンドを使用して既存のコンフィギュレーションをダウンロードできます。ファイル (ファイル名は自分で指定) は、**configuration** ディレクトリに書き込まれます。このファイルを CLI の外部で変更し、インポートし直すことができます。

import サブコマンドを使用するときは、ファイルに有効なエントリのみが含まれているようにしてください。無効なエントリ (左辺があって右辺がない場合など) があると、ファイルのインポート時に CLI で構文エラーが発生します。インポート中に構文エラーが発生すると、ファイル全体でマッピングがインポートされません。

リスナーのコンフィギュレーションの変更が反映されるように、ドメイン マップ テーブル ファイルをインポートした後で **commit** コマンドを発行してください。

これでエンタープライズ ゲートウェイの設定は次のようになります。

図 21-4 パブリック リスナー用に定義されたドメイン マップ



パブリック リスナー「InboundMail」のドメイン マップが作成されました。oldcompanyname.com ドメインおよびそのサブドメイン宛のメールは、example.com ドメインにマッピングされます。

IronPort 電子メール
セキュリティ アプライアンス

バウンスした電子メールの処理

バウンスした電子メールは、あらゆる電子メール配信においてやむを得ないものです。Cisco アプライアンスでは、詳細に設定できるさまざまな方法で、バウンスした電子メールを処理できます。

この項では、Cisco アプライアンスで着信メールに基づいて発信バウンスを生成する方法の制御について説明していることに注意してください。Cisco アプライアンスが発信メールに基づいて着信バウンスを制御する方法について管理するには、Cisco バウンス検証を使用します（「Cisco バウンス検証」(P.21-51) を参照）。

配信不可能な電子メールの処理

Cisco AsyncOS オペレーティング システムでは、配信不可能な電子メール（「バウンスしたメッセージ」）は、次のカテゴリに分類されます。

「カンパセーションの」バウンス：

最初の SMTP カンパセーションで、リモート ドメインがメッセージをバウンスします。

ソフト バウンス	一時的に配信不可能なメッセージ。たとえば、ユーザのメールボックスがいっぱい です。これらのメッセージは、後で再試行できます。（例：SMTP 4XX エラー コー ド）。
ハード バウンス	永続的に配信できないメッセージ。たとえば、そのユーザはそのドメインにはもう 存在しません。これらのメッセージは、再試行されません。（例：SMTP 5XX エ ラー コード）。

「遅延」（または「カンパセーションでない」）バウンス：

リモート ドメインは、メッセージを配信するために受け入れて、後でのみバウンスします。

ソフト バウンス	一時的に配信不可能なメッセージ。たとえば、ユーザのメールボックスがいっぱい です。これらのメッセージは、後で再試行できます。（例：SMTP 4XX エラー コー ド）。
ハード バウンス	永続的に配信できないメッセージ。たとえば、そのユーザはそのドメインにはもう 存在しません。これらのメッセージは、再試行されません。（例：SMTP 5XX エ ラー コード）。

GUI の [ネットワーク (Network)] メニューの [バウンス プロファイル (Bounce Profiles)] ページ（または `bounceconfig` コマンド）を使用して、作成するリスナーごとにハードおよびソフトのカンパセーション バウンスの Cisco AsyncOS の処理方法を設定します。バウンス プロファイルを作成したら、[ネットワーク (Network)] > [リスナー (Listeners)] ページ（または `listenerconfig` コマンド）を使用して、プロファイルを各リスナーに適用します。メッセージフィルタを使用して、特定のメッセージにバウンス プロファイルを割り当てることもできます。（詳細については、第 9 章「メッセージフィルタを使用した電子メール ポリシーの適用」を参照してください）。

ソフト バウンスおよびハード バウンスに関する注意

- カンパセーション ソフト バウンスの場合、ソフト バウンス イベントは、受信者への配信が一時的に失敗するたびに定義されます。単一の受信者が複数のソフト バウンス イベントを繰り返し発生させることがあります。[バウンス プロファイル (Bounce Profiles)] ページまたは `bounceconfig` コマンドを使用して、各ソフト バウンス イベントのパラメータを設定します。（「バウンス プロファイルのパラメータ」(P.21-37) を参照）。

- デフォルトでは、ハードバウンスした受信者ごとにバウンスメッセージが生成され、元の送信者に送信されます。(メッセージは、メッセージエンベロープのエンベロープ送信者アドレスで定義されたアドレスに送信されます。Envelope From も通常エンベロープ送信者を意味します)。この機能をディセーブルにし、代わりにハードバウンスに関する情報をログファイルに頼ることもできます (『Cisco IronPort AsyncOS for Email Daily Management Guide』の「Logging」を参照)。
- キュー内での最大時間または再試行の最大回数のどちらかに達すると、ソフトバウンスはハードバウンスになります。

バウンス プロファイルのパラメータ

バウンス プロファイルを設定するときは、次のパラメータを使用して、メッセージごとにカンバセーションバウンスを処理する方法を制御します。

表 21-5 バウンス プロファイルのパラメータ

最大再試行回数 (Maximum number of retries)	ソフトバウンスしたメッセージを配信し直すために、ハードバウンスメッセージとして扱われるようになる前に、受信者のホストに再接続が試みられる回数。デフォルトの再試行回数は 100 回です。
キューの最大時間 (秒) (Maximum number of seconds in queue)	ソフトバウンスしたメッセージを配信し直すために、ハードバウンスしたメッセージとして扱われるようになる前に、受信者のホストに再接続が試みられるのに費やされる時間。デフォルトは 259,200 秒 (72 時間) です。
メッセージを再試行するまでの初回待機時間 (秒) (Initial number of seconds to wait before retrying a message)	ソフトバウンスしたメッセージを最初に配信し直すまでの待機時間。デフォルトは 60 秒です。初回再試行時間を大きい値に設定すると、ソフトバウンスの試行頻度が低下します。逆に頻度を上げるには、小さい値にします。
メッセージを再試行するまでの最大待機時間 (秒) (Maximum number of seconds to wait before retrying a message)	ソフトバウンスしたメッセージを配信し直すまでに待機する最大時間。デフォルトは 3,600 秒 (1 時間) です。これは、次の試行までの間隔ではなく、再試行回数を制御するために使用できるもう 1 つのパラメータです。初回再試行間隔の上限は、最大再試行間隔に制限されます。計算された再試行間隔が最大再試行間隔を超える場合は、最大再試行間隔が使用されます。
ハードバウンスメッセージの生成形式 (Hard bounce message generation format)	ハードバウンスメッセージの生成がイネーブルかディセーブルかを指定します。イネーブルの場合は、メッセージの形式を選択できます。デフォルトでは、生成されるバウンスメッセージで DNS 形式 (RFC 1894) が使用されます。バウンスメッセージに使用するカスタム通知テンプレートを選択できます。詳細については、『Cisco IronPort AsyncOS for Email Configuration Guide』の「Text Resources」を参照してください。 バウンス応答から DSN の status フィールドを解析するかどうかを選択することもできます。「はい」の場合、AsyncOS は DSN ステータスコード (RFC 3436) を検索し、そのコードを配信ステータス通知の Status フィールドで使用します。
遅延警告メッセージの送信 (Send delay warning messages)	遅延の警告を送信するかどうかを指定します。イネーブルにした場合は、メッセージ間の最小間隔、および送信する最大再試行回数を指定します。 警告メッセージに使用するカスタム通知テンプレートを選択できます。詳細については、『Cisco IronPort AsyncOS for Email Configuration Guide』の「Text Resources」を参照してください。

表 21-5 バウンス プロファイルのパラメータ (続き)

バウンス先の受信者の指定 (Specify Recipient for Bounces)	メッセージのバウンス先としてデフォルトのエンベロープ送信者アドレスではなく、別のアドレスにすることができます。
バウンスおよび遅延メッセージへの DomainKeys 署名の使用 (Use DomainKeys signing for bounce and delay messages)	バウンス メッセージおよび遅延メッセージの署名に使用する DomainKeys プロファイルを選択できます。DomainKeys の詳細については、「 DomainKeys と DKIM 認証 」(P.17-1) を参照してください。
グローバル設定	
これらの設定を行うには、[バウンス プロファイル (Bounce Profiles)] ページの [グローバル設定を編集 (Edit Global Settings)] リンクを使用するか、または CLI で <code>bounceconfig</code> コマンドでデフォルトのバウンス プロファイルを編集します。	
到達不能ホストをリトライするまでの最初の待機時間 (秒) (Initial number of seconds to wait before retrying an unreachable host)	システムが到達不可能なホストへの再試行を待機する時間。デフォルトは 60 秒です。
到達不能ホストの最大許容再試行間隔 (Max interval allowed between retries to an unreachable host)	システムが到達不可能なホストへの再試行を待機する最大時間。デフォルトは 3,600 秒 (1 時間) です。ホストがダウンしているために配信が最初に失敗すると、再試行値の最小秒数で開始し、ダウンしたホストに対するその後の再試行では、間隔を徐々に延ばしていきます。最大で、この最大秒数になります。

ハードバウンスと status コマンド

ハードバウンス メッセージの生成がイネーブルの場合、アプライアンスで配信用のハードバウンスメッセージが生成されるたびに、`status` および `status detail` コマンドの次のカウンタが増えています。

Counters:	Reset	Uptime	Lifetime
Receiving			
Messages Received	0	0	0
Recipients Received	0	0	0
Gen. Bounce Recipients	0	0	0

詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Monitoring and Managing via the CLI」を参照してください。ハードバウンスメッセージの生成がディセーブルの場合、受信者でハードバウンスが発生しても、これらのカウンタはどれも増えません。



(注)

メッセージ エンベロープのエンベロープ送信者アドレスは、メッセージ ヘッダーの「From:」とは異なります。Cisco AsyncOS では、ハード バウンス メッセージをエンベロープ送信者アドレスとは異なる電子メール アドレスに送信するように設定できます。

カンバセーション バウンスおよび SMTP ルートのメッセージ フィルタ アクション

SMTP ルート マッピングおよびメッセージ フィルタ アクションは、カンバセーション バウンスの結果としてアプライアンスで生成された SMTP バウンス メッセージのルーティングには適用されません。Cisco アプライアンスでカンバセーション バウンス メッセージが受信されると、元のメッセージのエンベロープ送信者に返送する SMTP バウンス メッセージが生成されます。この場合、アプライアンスでは実際にメッセージが生成されるため、リレー用に挿入されたメッセージに適用されるすべての SMTP ルートは適用されません。

バウンス プロファイルの例

これら 2 つの例では、異なるバウンス プロファイル パラメータが使用されます。

表 21-6 例 1: バウンス プロファイル パラメータ

パラメータ	値
最大再試行回数 (Max number of retries)	2
キューの最大時間 (秒) (Maximum number of seconds in queue)	259,200 秒 (72 時間)
再試行するまでの初回最大時間 (秒) (Initial number of seconds before retrying)	60 秒
再試行するまでの最大待機時間 (秒) (Max number of seconds to wait before retrying)	60 秒

例 1 では、受信者への最初の配信は、 $t = 0$ で実行されます。これは、メッセージが Cisco アプライアンスに挿入された直後です。デフォルトの初回再試行時間は 60 秒であるため、最初の再試行は約 1 分後の $t = 60$ で実行されます。再試行間隔が計算されます。再試行間隔は、最大再試行間隔である 60 秒を使用して決定されます。そのため、2 回目の再試行は、 $t =$ 約 120 で実行されます。最大再試行回数は 2 であるため、この再試行の直後にその受信者のハード バウンス メッセージが生成されます。

表 21-7 例 2: バウンス プロファイル パラメータ

パラメータ	値
最大再試行回数 (Max number of retries)	100
キューの最大時間 (秒) (Maximum number of seconds in queue)	100 秒
再試行するまでの初回最大時間 (秒) (Initial number of seconds before retrying)	60 秒
再試行するまでの最大待機時間 (秒) (Max number of seconds to wait before retrying)	120 秒

例 2 では、最初の配信は $t = 0$ 、最初の再試行は $t = 60$ で実行されます。2 回目の配信 ($t = 120$ で発生するようにスケジュール) の直前にメッセージがハード バウンスされます。なぜなら、この時点でキュー内での最大時間である 100 秒を超過しているためです。

配信ステータス通知形式

システムによって生成されるバウンス メッセージは、デフォルトではハードとソフトの両方のバウンスで **Delivery Status Notification (DSN; 配信ステータス通知)** 形式を使用します。DSN は、RFC 1894 (<http://www.faqs.org/rfcs/rfc1894.html> を参照) で規定されている形式であり、「メッセージを 1 人以上の受信者に配信したときの結果をレポートするために、Message Transfer Agent (MTA; メッセージ転送エージェント) または電子的なメール ゲートウェイで使用できる MIME コンテンツ タイプを定義」します。デフォルトでは、配信ステータス通知には配信ステータスの説明、およびメッセージのサイズが 10 k よりも小さい場合は元のメッセージが含まれます。メッセージ サイズが 10 k よりも大きい場合、配信ステータス通知には、メッセージ ヘッダーのみが含まれます。メッセージ ヘッダーが 10 k を超える場合は、配信ステータス通知ではヘッダーが切り捨てられます。DSN に 10 k よりも大きいメッセージ (またはメッセージ ヘッダー) を含める場合は、`bounceconfig` コマンドの `max_bounce_copy` パラメータを使用できます (このパラメータは CLI からのみ利用できます)。

遅延警告メッセージ

システムで生成される [遅延通知メッセージ (Time in Queue Message)] でも、DSN 形式が使用されます。デフォルト パラメータを変更するには、[ネットワーク (Network)] メニューの [バウンス プロファイル (Bounce Profiles)] ページ (または `bounceconfig` コマンド) を使用して、既存のバウンス プロファイルを編集するか新規に作成し、以下のパラメータのデフォルト値を変更します。

- 遅延警告メッセージが送信される最小間隔。(The minimum interval between sending delay warning messages.)
- 遅延警告メッセージが送信される受信者あたりの最大数。(The maximum number of delay warning messages to send per recipient.)

遅延警告メッセージとハード バウンス (Delay Warning Messages and Hard Bounces)

[キューでの最大保持時間 (Maximum Time in Queue)] 設定と [遅延警告メッセージの送信 (Send Delay Warning Messages)] の最小間隔設定の両方を非常に小さい時間に設定した場合は、同じメッセージに対して遅延警告とハード バウンスの両方を同時に受信することが可能です。Cisco システムでは遅延警告メッセージの送信をイネーブルにする場合は、これらの設定のデフォルト値を最小設定として使用することを推奨します。

さらに、アプライアンスによって生成される遅延警告メッセージおよびバウンス メッセージは、処理中に最大で 15 分遅延することがあります。

新しいバウンス プロファイルの作成

次の例では、[バウンス プロファイル (Bounce Profiles)] ページを使用して、`bouncepr1` という名前のバウンス プロファイルが作成されます。このプロファイルでは、ハード バウンスされたすべてのメッセージが代替アドレスである `bounce-mailbox@example.com` に送信されます。遅延警告メッセージはイネーブルです。受信者あたり警告メッセージが 1 つ送信されます。警告メッセージ間のデフォルト値は 4 時間 (14400 秒) です。

デフォルトのバウンス プロファイルの編集

バウンス プロファイルを編集するには、バウンス プロファイルのリストで名前をクリックします。デフォルトのバウンス プロファイルを編集することもできます。この例では、デフォルト プロファイルを編集して、到達不可能なホストへの再試行を待機する最大秒数を 3600 (1 時間) から 10800 (3 時間) に増やします。

minimalist バウンス プロファイルの例

次の例では、minimalist という名前のバウンス プロファイルが作成されます。このプロファイルでは、メッセージがバウンスされるときに再試行されず（最大再試行回数が 0）、再試行を待機する最大時間が指定されます。ハード バウンス メッセージはディセーブルであり、ソフト バウンス 警告は送信されません。

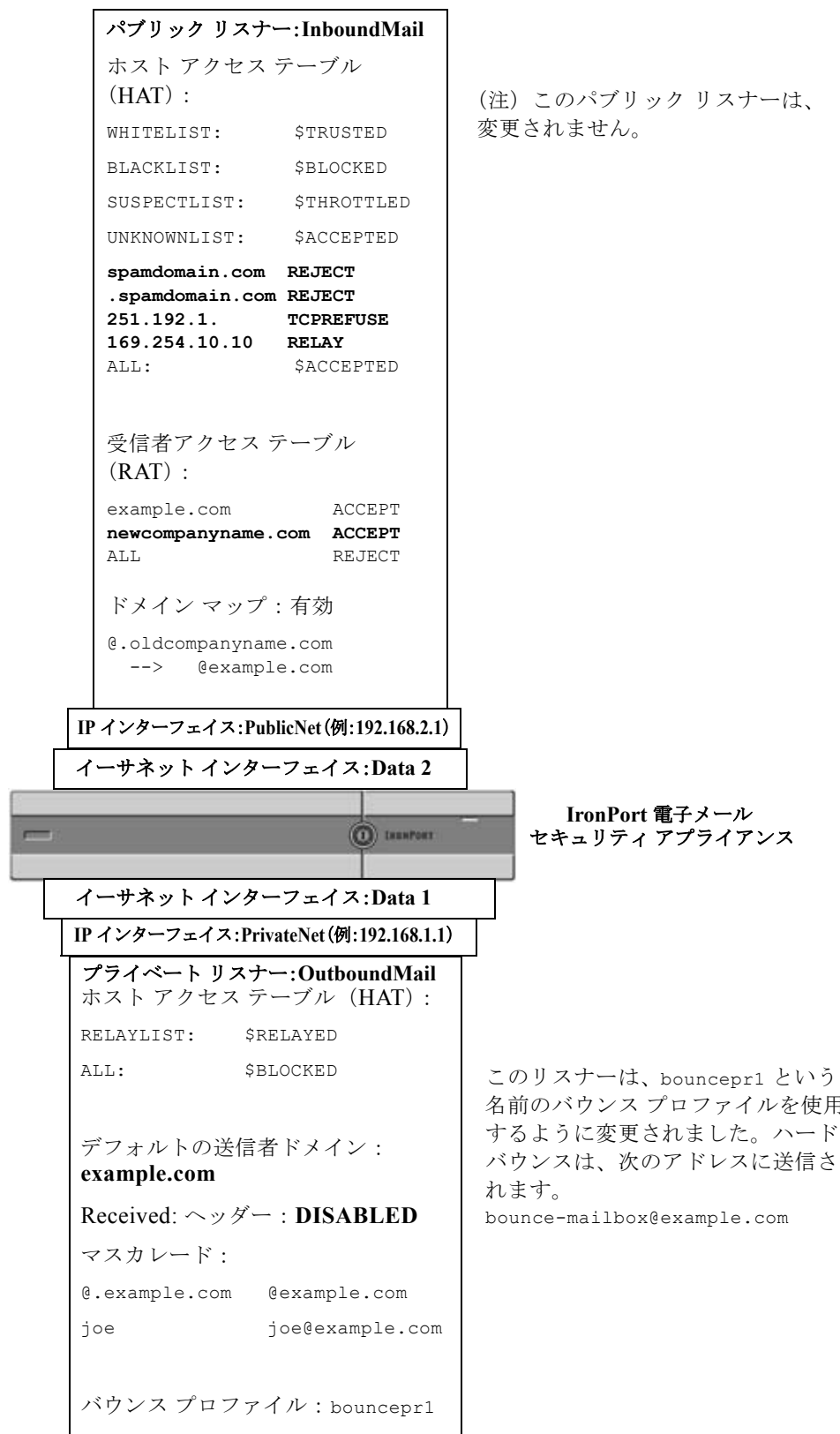
リスナーへのバウンス プロファイルの適用

バウンス プロファイルを作成したら、[ネットワーク (Network)] > [リスナー (Listeners)] ページまたは listenerconfig コマンドを使用して、そのプロファイルをリスナーに適用できます。

次の例では、bouncepr1 プロファイルが **OutgoingMail** リスナーに適用されます。

この時点で、電子メール ゲートウェイの設定は次のようになります。

図 21-5 プライベート リスナーへのバウンス プロファイルの適用



送信先コントロールによる電子メール配信の管理

大量の電子メールが未管理で配信されると、受信者ドメインで混乱が生じることがあります。AsyncOS では、アプライアンスで開く接続数やアプライアンスで各宛先ドメイン宛に送信されるメッセージ数を定義することにより、メッセージ配信を詳細に管理できます。

送信先コントロール機能（GUI では [メール ポリシー (Mail Policies)] > [送信先コントロール (Destination Controls)]、CLI では `destconfig` コマンド) を使用すると、次の項目を制御できます。

レート制限 (Rate Limiting)

- [同時接続 (Concurrent Connections)] : リモート ホストに対してアプライアンスが開こうとする同時接続数。
- [接続あたりの最大メッセージ数 (Maximum Messages Per Connection)] : アプライアンスが新しい接続を開始する前に、宛先ドメインに送信するメッセージ数。
- [受信者 (Recipients)] : アプライアンスが特定の期間に特定のリモート ホストに対して送信する受信者数。
- [制限 (Limits)] : 宛先ごと、および MGA ホスト名ごとに、制限を適用する方法。

TLS

- リモート ホストに対する TLS 接続を受入、可能、必須のいずれにするか ([「TLS の管理」\(P.21-46\)](#) を参照)。
- TLS 接続が必要なリモート ホストに対してメッセージが配信されるときに、TLS ネゴシエーションが失敗した場合にアラートを送信するかどうか。これは、ドメイン単位ではなく、グローバルな設定です。
- リモート ホストに対するすべての発信 TLS 接続で使用する TLS 証明書の割り当て。

バウンス検証 (Bounce Verification)

- Cisco バウンス検証を使用して、アドレス タギングを実行するかどうか ([「Cisco バウンス検証」\(P.21-51\)](#) を参照)。

バウンス プロファイル (Bounce Profile)

- 特定のリモート ホストに対してアプライアンスで使われるバウンス プロファイル (デフォルトのバウンス プロファイルは、[ネットワーク (Network)] > [バウンス プロファイル (Bounce Profiles)] ページで設定します)。

未指定のドメインに対するデフォルト設定を制御することもできます。

メール配信に使用するインターフェイスの決定

出力インターフェイスを `deliveryconfig` コマンド、メッセージフィルタ (`alt-src-host`)、または仮想ゲートウェイを使用して指定しない場合は、出力インターフェイスは AsyncOS ルーティングテーブルによって選択されます。基本的には、「自動」を選択すると AsyncOS によって選択されます。

詳細は次のとおりです。ローカル アドレスは、インターフェイスのネットマスクをインターフェイスの IP アドレスに適用することで識別されます。どちらも、[ネットワーク (Network)] > [インターフェイス (Interfaces)] ページまたは `interfaceconfig` コマンドを使用して（あるいはシステムのセットアップ時に）設定されます。アドレス空間が重なる場合は、より具体的なネットマスクが使用されます。宛先がローカルの場合、パケットは適切なローカル インターフェイス経由で送信されます。

宛先がローカルではない場合、パケットはデフォルトのルータ ([ネットワーク (Network)] > [ルーティング (Routing)] ページまたは `setgateway` コマンドを使用して設定) に対して送信されます。デフォルト ルータの IP アドレスはローカルです。出力インターフェイスは、ローカル アドレスの出力インターフェイスの選択ルールに従って決まります。たとえば、AsyncOS では、デフォルト ルータの IP アドレスが含まれていて最も具体的な IP アドレスおよびネットマスクが選択されます。

ルーティング テーブルは、[ネットワーク (Network)] > [ルーティング (Routing)] ページ（または `routeconfig` コマンド）を使用して設定されます。ルーティング テーブルで一致するエントリが、デフォルト ルートよりも優先されます。ルートが具体的になるほど、優先度が高くなります。

デフォルトの配信制限

発信宛先ドメインごとに、専用の発信キューがあります。そのため、ドメインごとに別々の同時接続制限 ([送信先コントロール (Destination Controls)] テーブルで指定) があります。さらに、[送信先コントロール (Destination Controls)] テーブルで具体的に示されていない一意的ドメインごとに、テーブルで設定した別の「デフォルト (Default)」制限を使用します。

[送信先コントロール (Destination Controls)] の使用

GUI で [メール ポリシー (Mail Policies)] > [送信先コントロール (Destination Controls)] ページ、または CLI で `destconfig` コマンドを使用して、送信先コントロール エントリを作成、編集、および削除します。

IP アドレス バージョンの制御

ドメイン接続に使用する IP アドレスのバージョンを設定できます。電子メール セキュリティ アプライアンスは両方のインターネット プロトコル バージョン 4 (IPv4) およびインターネット プロトコル バージョン (IPv6) を使用します。アプライアンスのリスナーをプロトコルの両方または 1 つのバージョンを使用するように設定できます。

IPv4 または IPv6 に対して [必須 (Required)] 設定を指定した場合、Cisco アプライアンスは指定されたバージョンのアドレスを使用してドメインへの接続をネゴシエーションします。ドメインが IP アドレスのバージョンを使わない場合、電子メールは送信されません。IPv4 または IPv6 の [推奨 (Preferred)] 設定を指定した場合、Cisco アプライアンスは最初に指定されたバージョンのアドレスを使用してドメインへの接続をネゴシエーションし、最初の試みが到達可能でない場合は他にフォールバックします。

ドメインに対する接続、メッセージ、受信者の数の管理

アプライアンスで電子メールを配信する方法を制限することにより、アプライアンスからの電子メールを扱うリモート ホストや独自の社内グループウェア サーバに負荷がかかり過ぎないようにできます。

ドメインごとに、特定の期間にシステムで超過しないようにする接続、発信メッセージ、受信者の最大数を割り当てることができます。この「グッドネイバー」テーブルは、送信先コントロール機能（[メールポリシー（Mail Policies）]>[送信先コントロール（Destination Controls）]）、または `destconfig` コマンド（以前の `setgoodtable` コマンド）を使用して定義します。ドメイン名を指定するには、次の構文を使用します。

`domain.com`

または

`.domain.com`

この構文を使用すると、AsyncOS で `sample.server.domain.com` のようなサブドメインの送信先コントロールを指定できるようになります。詳細なサブドメインアドレスを個別に入力する必要はありません。

接続、メッセージ、受信者については、定義する制限が各 Virtual Gateway アドレスとシステム全体のどちらに対して適用されるのかを設定します。（Virtual Gateway アドレス制限では、IP インターフェイスごとの同時接続数を管理します。システム全体の制限では、Cisco アプライアンスで許可される接続の合計数を管理します）。

また、定義する制限が指定されたドメインの各 MX レコードとドメイン全体のどちらに対して適用されるのかを設定することもできます。（多くのドメインには、電子メールの受け入れに関して複数の MX レコードがあります）。



(注)

現在のシステム デフォルトは、ドメインあたり 500 接続、接続あたり 50 メッセージです。

これらの値については、表 21-8 を参照してください。

表 21-8 [送信先コントロール（Destination Controls）] テーブルの値

フィールド	説明
同時接続 (Concurrent Connections)	Cisco アプライアンスによって特定のホストに対して行われる発信接続の最大数。（ドメインには、社内グループウェアのホストを含めることができます）。
接続あたりの最大メッセージ数 (Maximum Messages Per Connection)	新しい接続が開始されるまでに、Cisco アプライアンスから特定のホストに対する単一発信接続に対して許可されるメッセージの最大数。
受信者 (Recipients)	<p>特定の期間内に許可される受信者の最大数。[なし (None)] は、当該ドメインに対して、受信者の制限がないことを示します。</p> <p>Cisco アプライアンスが受信者の数を数える最小期間（1 ～ 60 分）。期間に「0」を指定すると、この機能がディセーブルになります。</p> <p>(注) 受信者制限を変更すると、すでにキュー内にあるすべてのメッセージのカウンタがリセットされます。アプライアンスは、新しい受信者制限に基づいてメッセージを配信します。</p>

表 21-8 【送信先コントロール (Destination Controls)】テーブルの値 (続き)

フィールド	説明
制限の適用 (Apply Limits)	<p>制限がドメイン全体とそのドメインに指定された各メール交換 IP アドレスのどちらに適用されるのかを指定します。(多くのドメインで複数の MX レコードがあります)。</p> <p>この設定は、接続、メッセージ、受信者の制限に適用されます。</p> <p>制限がシステム全体と各 Virtual Gateway アドレスのどちらに適用されるのかを指定します。</p> <p>(注) IP アドレスのグループを設定しても、仮想ゲートウェイを設定していない場合は、仮想ゲートウェイごとに適用制限を設定しないでください。この設定は、仮想ゲートウェイを使用するように設定されたシステムのみを対象にしています。仮想ゲートウェイの設定方法については、「Virtual Gateway™ テクノロジーを使用してすべてのホストされたドメインでの構成のメールゲートウェイ」(P.21-59) を参照してください。</p>



(注)

制限が Virtual Gateway アドレスごとに適用される場合でも、システム全体の制限を仮想ゲートウェイの数で除算した値を Virtual Gateway の制限に設定することによって、システム全体の制限を効果的に実装できます。たとえば、4 つの Virtual Gateway アドレスが設定されていて、ドメイン yahoo.com に対して 100 より多くの同時接続を開かないようにするには、Virtual Gateway の制限を同時接続数 25 に設定します。



(注)

delivernow コマンドをすべてのドメインに対して実行すると、destconfig コマンドで追跡されているすべてのカウンタがリセットされます。

TLS の管理

ドメイン単位で Transport Layer Security (TLS; トランスポート層セキュリティ) を設定することもできます。「Required」設定が指定された場合、Cisco アプライアンスのリスナーからドメインの MTA に対して TLS 接続がネゴシエートされます。ネゴシエーションに失敗すると、電子メールはその接続を介して送信されません。詳細については、「[配信時の TLS および証明書検証のイネーブル化](#)」(P.20-9) を参照してください。

TLS 接続が必要なドメインにメッセージを配信する際に TLS ネゴシエーションが失敗した場合、Cisco アプライアンスがアラートを送信するかどうかを指定できます。アラートメッセージには失敗した TLS ネゴシエーションの宛先ドメイン名が含まれます。Cisco アプライアンスは、システムアラートのタイプの警告重大度レベルアラートを受信するよう設定されたすべての受信者にアラートメッセージを送信します。GUI の [システム管理 (System Administration)] > [アラート (Alerts)] ページ (または CLI の alertconfig コマンド) を使用してアラートの受信者を管理できます。

TLS 接続アラートをイネーブルにするには、[送信先コントロール (Destination Controls)] ページの [グローバル設定を編集 (Edit Global Settings)] をクリックまたは destconfig -> setup サブコマンドを使用します。これは、ドメイン単位ではなく、グローバルな設定です。アプライアンスが配信を試行したメッセージの情報については、[モニタ (Monitor)] > [メッセージトラッキング (Message Tracking)] ページまたはメールログを使用します。

すべての発信 TLS 接続に使用する証明書を指定する必要があります。[送信先コントロール (Destination Controls)] ページの [グローバル設定を編集 (Edit Global Settings)] または `destconfig` -> `setup` サブコマンドを使用して、証明書を指定します。証明書の取得方法については、「[証明書の取得](#)」(P.20-2) を参照してください。

アラートの詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「System Administration」を参照してください。

Cisco バウンス検証タギングの管理

送信されるメールにバウンス検証のタギングが行われるかどうかを指定できます。デフォルトに対して指定することも、特定の宛先に対して指定することもできます。Cisco では、デフォルトに対してバウンス検証をイネーブルにした後で、具体的な除外対象として新しい宛先を作成することを推奨します。詳細については、「[Cisco バウンス検証](#)」(P.21-51) を参照してください。

バウンスの管理

リモート ホストに配信する接続や受信者の数を制御できるだけでなく、そのドメインで使用されるバウンス プロファイルを指定することもできます。指定すると、バウンス プロファイルは `destconfig` コマンドの 5 番目のカラムに表示されます。バウンス プロファイルを指定しない場合は、デフォルトのバウンス プロファイルが使用されます。詳細については、「[新しいバウンス プロファイルの作成](#)」(P.21-40) を参照してください。

新しい送信先コントロール エントリの追加

手順

- ステップ 1 [送信先の追加 (Add Destination)] をクリックします。
- ステップ 2 エントリを設定します。
- ステップ 3 変更内容を送信し、確定します。

送信先コントロール エントリ コンフィギュレーションのインポートおよびエクスポート

複数のドメインを管理している場合は、すべてのドメインの送信先コントロール エントリを定義する単一の設定ファイルを作成して、アプライアンスにインポートできます。設定ファイルの形式は、Windows INI 設定ファイルと似ています。ドメインのパラメータはセクションにまとめられ、セクション名としてドメイン名が使用されます。たとえば、セクション名 `[example.com]` を使用して、ドメイン `example.com` のパラメータをグループにします。定義されないすべてのパラメータは、デフォルトの送信先コントロール エントリから継承されます。デフォルトの送信先コントロール エントリのパラメータを定義するには、設定ファイルに [デフォルト (DEFAULT)] セクションを含めます。

設定ファイルをインポートすると、アプライアンスの送信先コントロール エントリがすべて上書きされます。ただし、設定ファイルに [デフォルト (DEFAULT)] セクションが含まれていない場合、デフォルト エントリは上書きされません。その他すべての既存の送信先コントロール エントリは削除されません。

設定ファイルでは、ドメインに対して次のパラメータを定義できます。[デフォルト (DEFAULT)] セクションには bounce_profile パラメータを除くすべてのパラメータが必要です。

表 21-9 送信先コントロール設定ファイルのパラメータ

パラメータ名	説明
ip_sort_pref	ドメインに対してインターネット プロトコル バージョンを指定します。 次のいずれかの値を入力します。 <ul style="list-style-type: none"> IPv6 「Preferred」 の場合の PREFER_V6 IPv6 「Required」 の場合の REQUIRE_V6 IPv4 「Preferred」 の場合の PREFER_V4 IPv4 「Required」 の場合の REQUIRE_V4
max_host_concurrency	Cisco アプライアンスによって特定のホストに対して行われる発信接続の最大数。 ドメインに対してこのパラメータを定義する場合は、limit_type および limit_apply パラメータも定義する必要があります。
max_messages_per_connection	新しい接続が開始されるまでに、Cisco アプライアンスから特定のホストに対する単一発信接続に対して許可されるメッセージの最大数。
recipient_minutes	Cisco アプライアンスが受信者の数を数える期間 (1 ~ 60 分)。受信者制限を適用しないようにする場合は、未定義のままにします。
recipient_limit	特定の期間内に許可される受信者の最大数。受信者制限を適用しないようにする場合は、未定義のままにします。 ドメインに対してこのパラメータを定義する場合は、recipient_minutes、limit_type、および limit_apply パラメータも定義する必要があります。
limit_type	制限がドメイン全体とそのドメインに指定された各メール交換 IP アドレスのどちらに適用されるのかを指定します。 次のいずれかの値を入力します。 <ul style="list-style-type: none"> 0 (または host) : ドメインの場合 1 (または MXIP) : メール交換 IP アドレスの場合
limit_apply	制限がシステム全体と各 Virtual Gateway アドレスのどちらに適用されるのかを指定します。 次のいずれかの値を入力します。 <ul style="list-style-type: none"> 0 (または system) : システム全体の場合 1 (または VG) : Virtual Gateway の場合
bounce_validation	バウンス検証アドレス タギングをオンにするかどうかを指定します。 次のいずれかの値を入力します。 <ul style="list-style-type: none"> 0 (または off) 1 (または on)

表 21-9 送信先コントロール設定ファイルのパラメータ (続き)

パラメータ名	説明
table_tls	<p>ドメインの TLS 設定を指定します。詳細については、「配信時の TLS および証明書検証のイネーブル化」(P.20-9) を参照してください。</p> <p>次のいずれかの値を入力します。</p> <ul style="list-style-type: none"> 0 (または off) 1 (または on) : 「推奨 (Preferred)」の場合 2 (または required) : 「必須 (Required)」の場合 3 (または on_verify) 「推奨 (検証) (Preferred (Verify))」の場合 4 (または require_verify) : 「必須 (検証) (Required (Verify))」の場合 <p>文字列には、大文字と小文字の区別はありません。</p>
bounce_profile	<p>使用するバウンス プロファイルの名前。[デフォルト (DEFAULT)] 送信先コントロール エントリでは使用できません。</p>
send_tls_req_alert	<p>必須の TLS 接続が失敗した場合にアラートを送信するかどうか。</p> <p>次のいずれかの値を入力します。</p> <ul style="list-style-type: none"> 0 (または off) 1 (または on) <p>これはグローバル設定であり、[デフォルト (DEFAULT)] 送信先コントロール エントリでのみ使用できます。</p>
certificate	<p>発信 TLS 接続で使用される証明書。これはグローバル設定であり、[デフォルト (DEFAULT)] 送信先コントロール エントリでのみ使用できます。</p> <p>(注) 証明書を指定しない場合は、デモの証明書が割り当てられますが、デモの証明書を使用することはセキュアではないため、通常の使用には推奨できません。</p>

ドメイン example1.com、example2.com、およびデフォルトの宛先制御エントリの例を次に示します。

```
[DEFAULT]
ip_sort_pref = PREFER_V6
max_host_concurrency = 500
max_messages_per_connection = 50
recipient_minutes = 60
recipient_limit = 300
```

```
limit_type = host

limit_apply = VG

table_tls = off

bounce_validation = 0

send_tls_req_alert = 0

certificate = example.com

[example1.com]

ip_sort_pref = PREFER_V6

recipient_minutes = 60

recipient_limit = 100

table_tls = require_verify

limit_apply = VG

bounce_profile = tls_failed

limit_type = host

[example2.com]

table_tls = on

bounce_profile = tls_failed
```

上記の例では、**example1.com** および **example2.com** について次の宛先制御エントリが生成されます。

```
example1.com

  IP Address Preference: IPv6 Preferred

  Maximum messages per connection: 50

  Rate Limiting:

    500 concurrent connections

    100 recipients per 60 minutes

  Limits applied to entire domain, across all virtual gateways
```

```
TLS: Required (Verify)

Bounce Profile: tls_failed

example2.com

IP Address Preference: IPv6 Preferred

Maximum messages per connection: Default

Rate Limiting: Default

TLS: Preferred

Bounce Profile: tls_failed
```

[送信先コントロール (Destination Controls)] ページの [テーブルのインポート (Import Table)] ボタン、または `destconfig -> import` コマンドを使用して、設定ファイルをインポートします。[送信先コントロール (Destination Controls)] ページの [テーブルのエクスポート (Export Table)] ボタン、または `destconfig -> export` コマンドを使用して、送信先コントロール エントリを INI ファイルにエクスポートすることもできます。エクスポートされた INI ファイルには [デフォルト (Default)] ドメイン管理エントリも含まれています。

送信先コントロールと CLI

CLI で `destconfig` コマンドを使用して、送信先コントロール エントリを設定できます。このコマンドについては、『*Cisco AsyncOS CLI Reference Guide*』で説明します。

Cisco バウンス検証

「バウンス」メッセージは、受信側の MTA によって送信される新しいメッセージで、元の電子メールのエンベロープ送信者が新しいエンベロープ受信者として使用されます。このバウンスは、元のメッセージが配信不可能なときに（通常は、受信者アドレスが存在しないため）、通常は空のエンベロープ送信者 (MAIL FROM: <>) でエンベロープ受信者に送り返されます。

スパム送信者は、誤った宛先を指定したバウンス攻撃による電子メール インフラストラクチャへの攻撃をますます増やしています。このような攻撃は、未知の正当なメール サーバによって送信される、膨大なバウンス メッセージによって行われます。基本的に、スパム送信者が使用するプロセスでは、オープン リレーおよび「ゾンビ」ネットワークを経由してさまざまなドメインで無効な可能性のあるアドレス (エンベロープ受信者) に電子メールを送信します。このようなメッセージでは、エンベロープ送信者が偽装されるため、スパムは正当なドメインから送信されたように見えます (これは「Joe job (ジョー ジョブ)」とも呼ばれます)。

次に、無効なエンベロープ受信者による着信電子メールごとに、受信側のメール サーバによって新しい電子メール (バウンス メッセージ) が生成され、一緒に無実なドメイン (エンベロープ送信者アドレスが偽装されたドメイン) の電子メール送信者宛に送信されます。その結果、このターゲット ドメインは、「誤った宛先が指定された」膨大なバウンスを受信します。このバウンス メッセージは、数百万にもおよびることがあります。このような分散 DoS 攻撃により、電子メール インフラストラクチャがダウンして、ターゲットが正当な電子メールの送受信を行えなくなります。

誤った宛先を指定したバウンス攻撃に対処するため、AsyncOS には Cisco [バウンス検証 (Bounce Verification)] が用意されています。イネーブルにすると、Cisco バウンス検証によって、その Cisco アプライアンスから送信されたメッセージのエンベロープ送信者アドレスにタグが付けられます。次に、Cisco アプライアンスで受信したバウンス メッセージで、エンベロープ受信者にこのタグが付いているかどうかチェックされます。正当なバウンス (このタグが付いている) であれば、タグが外されて配信されます。タグが付いていないバウンス メッセージは、別の処理を行えます。

Cisco バウンス検証を使用して、発信メールに基づいて着信バウンス メッセージを管理できます。Cisco アプライアンスで着信メールに基づいて発信バウンスを生成する方法の制御については、「[バウンスした電子メールの処理](#)」(P.21-36) を参照してください。

概要 : タギングと Cisco バウンス検証

バウンス検証をイネーブルにして電子メールを送信すると、Cisco アプライアンスにより、メッセージのエンベロープ送信者アドレスが書き換えられます。たとえば、MAIL FROM: joe@example.com が MAIL FROM: prvs=joe=123ABCDEF@example.com になるとします。この例の 123... という文字列は、「バウンス検証タグ」であり、Cisco アプライアンスによって送信されるたびに、エンベロープ送信者に追加されました。このタグは、バウンス検証設定で定義されたキーを使用して生成されます (キーの指定については、「[Cisco バウンス検証アドレスのタグ付けキー](#)」(P.21-53) を参照してください)。このメッセージがバウンスすると、バウンス内のエンベロープ受信者アドレスに通常はこのバウンス検証タグが含まれます。

デフォルトではシステム全体でバウンス検証タギングをイネーブルまたはディセーブルにできます。特定のドメインに対してバウンス検証タギングをイネーブルまたはディセーブルにすることもできます。ほとんどの場合、デフォルトでイネーブルにしておき、除外する具体的なドメインを [送信先コントロール (Destination Controls)] テーブルに列挙します («[送信先コントロール \(Destination Controls\)](#)」の使用」(P.21-44) を参照)。

メッセージにタグ付きのアドレスがすでに含まれている場合は、別のタグが追加されません (Cisco アプライアンスがバウンス メッセージを DMZ 内の Cisco アプライアンスに配信する場合)。

着信バウンス メッセージの処理

有効なタグが含まれているバウンスは配信されます。タグが削除され、エンベロープ受信者が復元されます。これは、電子メールパイプラインのドメイン マップ処理の直後に発生します。Cisco アプライアンスでタグの付いていないバウンスやタグが無効に付いたバウンスの処理方法として、拒否するか、それともカスタム ヘッダーを追加するのかを定義できます。詳細については、「[Cisco バウンス検証設定の設定](#)」(P.21-55) を参照してください。

バウンス検証タグが存在しない場合、タグの生成に使用されたキーが変更された場合、またはメッセージが 7 日より古い場合、そのメッセージは Cisco バウンス検証で定義された設定に従って扱われます。たとえば、次のメール ログには、Cisco アプライアンスで拒否されたバウンス メッセージが示されています。

```
Fri Jul 21 16:02:19 2006 Info: Start MID 26603 ICID 125192
```

```
Fri Jul 21 16:02:19 2006 Info: MID 26603 ICID 125192 From: <>
```

```
Fri Jul 21 16:02:40 2006 Info: MID 26603 ICID 125192 invalid bounce, rcpt address <bob@example.com> rejected by bounce verification.
```



```
Fri Jul 21 16:03:51 2006 Info: Message aborted MID 26603 Receiving aborted by sender
```

```
Fri Jul 21 16:03:51 2006 Info: Message finished MID 26603 aborted
```



(注) 非バウンス メールを独自の社内メール サーバ (Exchange など) に配信する場合は、その社内ドメインに対して Cisco バウンス検証タギングをディセーブルにしてください。

AsyncOS では、バウンスがヌルの MAIL FROM アドレス (<>) が設定されたメールであると見なされます。タグ付きのエンベロープ受信者が含まれる可能性のある非バウンス メッセージの場合は、より緩やかなポリシーが適用されます。そのような場合、7 日でのキー失効は無視され、古いキーとの一致も調べられません。

Cisco バウンス検証アドレスのタグ付けキー

タギング キーは、バウンス検証タグを生成するときに Cisco アプライアンスで使用されるテキスト文字列です。ドメインから発信されるすべてのメールには一貫してタグが付けられるため、すべての Cisco アプライアンスで同じキーを使用することが理想的です。そのようにして、ある Cisco アプライアンスで発信メッセージのエンベロープ送信者にタグが付けられる場合、別の Cisco アプライアンスからバウンスを受信しても、その着信バウンスが検証および配信されます。

タグには 7 日間の猶予期間があります。たとえば、7 日間のうちにタギング キーを複数回変更できます。その場合、Cisco アプライアンスは 7 日より新しいこれまでのすべてのキーを使用して、タグの付いたメッセージを検証しようとしています。

タグなしのバウンスされたメッセージの合法的受け入れ

AsyncOS には、Cisco バウンス検証に関連して、タグの付いていないバウンスを有効とするかどうかを検討する HAT 設定もあります。デフォルト設定は「いいえ」であり、タグの付いていないバウンスは無効であると見なされます。さらに、[メール ポリシー (Mail Policies)] > [バウンス検証 (Bounce Verification)] ページで選択されたアクションに従って、メッセージが拒否されるか、またはカスタムヘッダーが付加されます。「はい」を選択した場合、タグの付いていないバウンスは有効であると見なされ、受け入れられます。これは、次のようなシナリオで使用できます。

電子メールをメーリング リストに送信することを検討しているユーザがいるとします。しかし、メーリング リストでは、エンベロープ送信者の固定セットからのメッセージのみを受け入れています。そのような場合、ユーザからのタグ付きメッセージは受け入れられません (タグは定期的に変更されるため)。

手順

- ステップ 1** ユーザがメールを送信しようとするドメインを [送信先コントロール (Destination Controls)] テーブルに追加し、そのドメインに対するタギングをディセーブルにします。この時点で、ユーザは問題なくメールを送信できます。
- ステップ 2** しかし、そのドメインからのバウンスにはタグが付いていないため、バウンス受信を適切にサポートするには、そのドメインの送信者グループを作成し、[承認 (Accept)] メール フロー ポリシーの [タグなしバウンスを有効と見なす (Consider Untagged Bounces to be Valid)] パラメータをイネーブルにします。

図 21-6 [タグなしバウンスを有効と見なす (Consider Untagged Bounces to be Valid)] HAT パラメータ

Security Features	
Spam Detection:	<input checked="" type="radio"/> Use Default (On) <input type="radio"/> On <input type="radio"/> Off
Virus Protection:	<input checked="" type="radio"/> Use Default (On) <input type="radio"/> On <input type="radio"/> Off
Encryption and Authentication:	TLS: <input checked="" type="radio"/> Use Default (Off) <input type="radio"/> Off <input type="radio"/> Preferred <input type="radio"/> Required
	SMTP Authentication: <input checked="" type="radio"/> Use Default (Off) <input type="radio"/> Off <input type="radio"/> Preferred <input type="radio"/> Required
	If Both TLS and SMTP Authentication are enabled: <input type="checkbox"/> Require TLS To Offer SMTP Authentication
Domain Key/DKIM Signing:	<input checked="" type="radio"/> Use Default (Off) <input type="radio"/> On <input type="radio"/> Off
DKIM Verification:	<input checked="" type="radio"/> Use Default (Off) <input type="radio"/> On <input type="radio"/> Off
SPF/SIDF Verification:	<input checked="" type="radio"/> Use Default (Off) <input type="radio"/> On <input type="radio"/> Off
Bounce Verification:	Conformance Level: <input type="text" value="SPF Compatible"/>
	Downgrade PRA verification result if "Resent-Sender:" or "Resent-From:" were used: <input type="radio"/> Use Default (No) <input type="radio"/> No <input type="radio"/> Yes
	HELO Test: <input type="radio"/> Use Default (On) <input type="radio"/> Off <input type="radio"/> On
Consider Untagged Bounces to be Valid: <input checked="" type="radio"/> Use Default (No) <input type="radio"/> Yes <input type="radio"/> No	
<small>(Applies only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.)</small>	

バウンス Cisco 検証を使用してバウンス メッセージ ストームを防止

手順

- ステップ 1 タギング キーを入力します。詳細については、「[バウンス検証アドレスのタグ付けキー (Bounce Verification Address Tagging Keys)] の設定」(P.21-54) を参照してください。
- ステップ 2 バウンス検証設定を編集します。詳細については、「Cisco バウンス検証設定の設定」(P.21-55) を参照してください。
- ステップ 3 [送信先コントロール (Destination Controls)]を使用したバウンス検証。詳細については、「[送信先コントロール (Destination Controls)] の使用」(P.21-44) を参照してください。

図 21-7 IronPort の [バウンス検証 (Bounce Verification)] ページ

Bounce Verification Settings	
Action when invalid bounce received:	Reject
Smart exceptions to tagging:	Enabled
Edit Settings	
Bounce Verification Address Tagging Keys	
New Key... Clear All Keys	
Address Tagging Keys	Status
example.com's bounce key	Current <small>(see Mail Policies > Destination Controls to set or view destinations which have Bounce Verification Address Tagging enabled)</small>
Purge Keys <input type="text" value="Not used in one month"/>	
Key: <input type="text" value="Current"/> <input type="text" value="Previously used"/>	

[バウンス検証アドレスのタグ付けキー (Bounce Verification Address Tagging Keys)] の設定

[バウンス検証アドレスのタグ付けキー (Bounce Verification Address Tagging Keys)] のリストには、現在のキー、および過去に使用してまだ削除されていないキーが示されます。新規のキーを追加するには、次の手順を実行します。

手順

- ステップ 1 [メール ポリシー (Mail Policies)] > [バウンス検証 (Bounce Verification)] ページで、[キーを追加 (New Key)] をクリックします。
- ステップ 2 テキスト文字列を入力し、[送信 (Submit)] をクリックします。
- ステップ 3 変更内容を確定します。

キーの削除

古いアドレス タギング キーを削除するには、プルダウン メニューから削除するルールを選択し、[除去 (Purge)] をクリックします。

Cisco バウンス検証設定の設定

バウンス検証設定では、無効なバウンスを受信したときに実行するアクションを指定します。

手順

- ステップ 1 [メール ポリシー (Mail Policies)] > [バウンス検証 (Bounce Verification)] を選択します。
- ステップ 2 [設定を編集 (Edit Settings)] をクリックします。
- ステップ 3 無効なバウンスを拒否するのか、カスタム ヘッダーをメッセージに追加するのかを選択します。ヘッダーを追加する場合は、ヘッダーの名前と値を入力します。
- ステップ 4 必要に応じて、スマート例外機能をイネーブルにします。この設定を使用すると、(着信メールと発信メールの両方で 1 つのリスナーを使用している場合であっても) 着信メール メッセージ、および社内メール サーバで生成されるバウンス メッセージをバウンス検証処理から自動的に除外できるようにします。
- ステップ 5 変更内容を送信し、確定します。

CLI を使用した Cisco バウンス検証の設定

CLI で `bvconfig` コマンドおよび `destconfig` コマンドを使用して、バウンス検証を設定できます。これらのコマンドについては、『*Cisco AsyncOS CLI Reference Guide*』で説明します。

Cisco バウンス検証とクラスタ設定

バウンス検証は、両方の Cisco アプライアンスで同じ「バウンス キー」を使用している限り、クラスタ設定で動作します。同じキーを使用する場合は、どちらのシステムでも正当なバウンスを受け入れられる必要があります。変更後のヘッダー タグ/キーは、各 Cisco アプライアンスに固有ではありません。

電子メール配信パラメータの設定

`deliveryconfig` コマンドは、Cisco アプライアンスから電子メールを配信するときに使用されるパラメータを設定します。

Cisco アプライアンスは、SMTP と QMQP という複数のメール プロトコルを使用してメールを受信します。ただし、すべての発信電子メールは、SMTP を使用して配信されます。このため、`deliveryconfig` コマンドではプロトコルの指定が不要です。



(注)

このセクションに記載されている機能またはコマンドには、ルーティングの優先順位に影響を与えるものや、影響を受けるものが含まれています。詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の付録 B、「Assigning Network and IP Addresses」を参照してください。

デフォルトの配信 IP インターフェイス

デフォルトで、電子メール配信には IP インターフェイスまたは IP インターフェイス グループが使用されます。現在設定されているどの IP インターフェイスまたは IP インターフェイス グループでも設定できます。特定のインターフェイスが指定されない場合は、受信者ホストと通信するときに SMTP HELO コマンドでデフォルトの配信インターフェイスと関連付けられたホスト名が使用されます。IP インターフェイスを設定するには、`interfaceconfig` コマンドを使用します。

電子メール配信インターフェイスの自動選択を使用するときのルールは次のとおりです。

- リモートの電子メール サーバが設定済みインターフェイスのいずれかと同じサブネット上にある場合、トラフィックは一致するインターフェイス上を流れます。
- `auto-select` に設定した場合、`routeconfig` を使用して設定したスタティック ルートが有効になります。
- そうでない場合、デフォルト ゲートウェイと同じサブネット上にあるインターフェイスが使用されます。すべての IP アドレスで宛先に対するルートが同等の場合、使用可能なうち最も効率的なインターフェイスが使用されます。

[配信可能性あり (Possible Delivery)] 機能

[配信可能性あり (Possible Delivery)] 機能がイネーブルになると、AsyncOS では、メッセージ本文が配信されてから受信者ホストがメッセージの受信を確認するまでの間にタイムアウトするすべてのメッセージを「配信可能性あり」と見なして扱います。この機能を使用すると、受信者ホストで連続するエラーにより受信の確認が妨げられる場合に、メッセージのコピーを複数受信しなくて済みます。AsyncOS では、この受信を配信可能性ありとしてメール ログに記録し、そのメッセージを完了したものと見なします。[配信可能性あり (Possible Delivery)] 機能は、イネーブルのままにしておくことを推奨します。

デフォルトの最大同時接続数

アプライアンスが発信メッセージの配信で確立するデフォルトの最大同時接続数も指定できます。(システム全体のデフォルトはドメインごとに 10,000 接続です)。この制限は、リスナーあたりの最大同時発信メッセージ配信数 (リスナーあたりのデフォルトは、プライベート リスナーで 600 接続、パブリック リスナーで 1000 接続です)。デフォルトよりも小さい値を設定すると、Cisco ゲートウェイが弱いネットワークを支配しないようにすることができます。たとえば、特定のファイアウォールが大量の接続をサポートしない場合、そのような環境では Cisco で Denial of Service (DoS; サービス拒否) 警告が引き起こされることがあります。

deliveryconfig の例

次の例では、`deliveryconfig` コマンドを使用し、[配信可能性あり (Possible Delivery)] をイネーブルにして、デフォルトのインターフェイスを [自動 (Auto)] に設定します。システム全体の最大発信メッセージ配信は、9000 接続です。

```
mail3.example.com> deliveryconfig

Choose the operation you want to perform:

- SETUP - Configure mail delivery.

[ ]> setup

Choose the default interface to deliver mail.

1. Auto
2. PublicNet2 (192.168.3.1/24: mail4.example.com)
3. Management (192.168.42.42/24: mail3.example.com)
4. PrivateNet (192.168.1.1/24: mail3.example.com)
5. PublicNet (192.168.2.1/24: mail3.example.com)

[1]> 1

Enable "Possible Delivery" (recommended)? [Y]> y

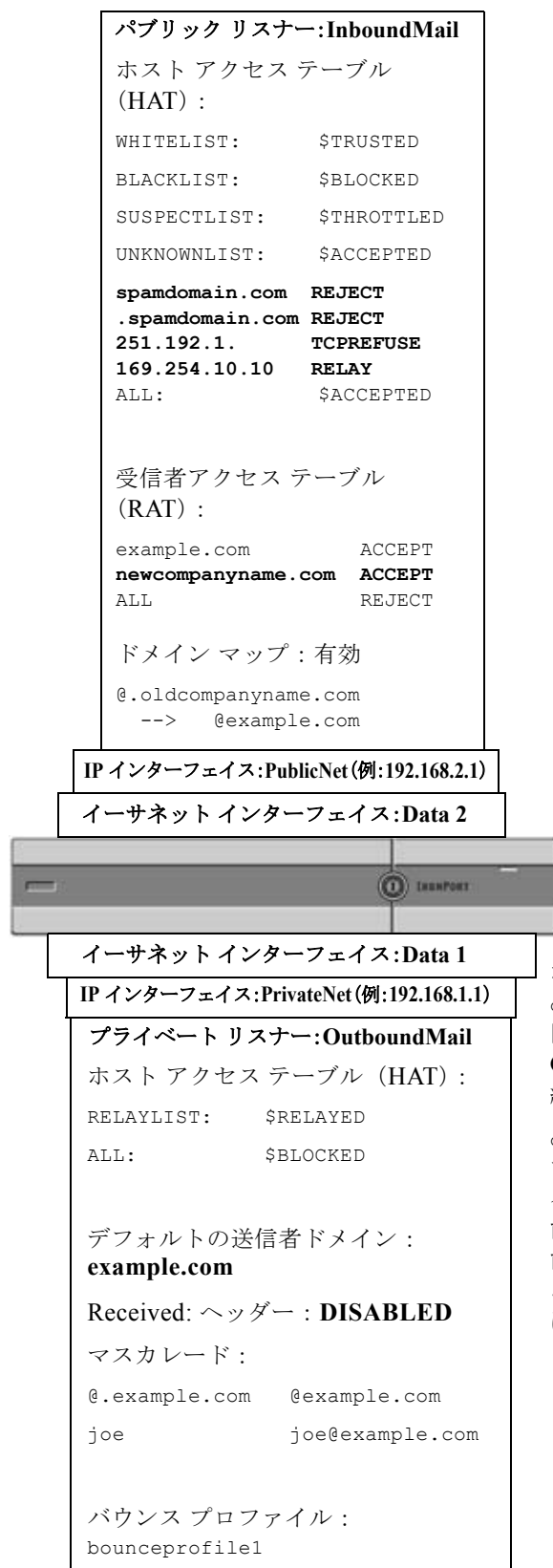
Please enter the default system wide maximum outbound message delivery
concurrency

[10000]> 9000

mail3.example.com>
```

これで電子メール ゲートウェイのコンフィギュレーションは次のようになります。

図 21-8 宛先および配信パラメータの設定



**IronPort 電子メール
セキュリティ アプライアンス**

ホスト small-isp.net の destconfig エントリを使用して、同時接続数 100、または Virtual Gateway アドレスを使用して同時接続数 10 に制限されます。

deliveryconfig コマンドを使用して、電子メール配信用インターフェイスの自動選択を使用し、[配信可能性あり (Possible Delivery)] 機能をイネーブルにしました。システム全体の最大発信メッセージ配信は、合計で 9000 同時接続です。

Virtual Gateway™ テクノロジーを使用してすべてのホストされたドメインでの構成のメール ゲートウェイ

この項では、Cisco Virtual Gateway™ テクノロジーとその利点、Virtual Gateway アドレスの設定方法、および Virtual Gateway アドレスのモニタおよび管理方法について説明します。

Cisco Virtual Gateway テクノロジーでは、ホストするすべてのドメインに対して異なる IP アドレス、ホスト名、およびドメインを使用してエンタープライズメール ゲートウェイを設定し、同じ物理アプライアンス内にホストしている場合でも、それらのドメインに対して別々に企業の電子メール ポリシー強制およびスパム対策方針を作成できます。



(注)

利用できる Virtual Gateway アドレスの数は、使用する Cisco アプライアンスのモデルによって異なります。一部のアプライアンス モデルでは、ライセンス キーを使用して多くの Virtual Gateway アドレスをサポートするようにアップグレードできます。使用するアプライアンスでの Virtual Gateway アドレスの数をアップグレードする詳細については、Cisco 販売代理店にお問い合わせください。

概要

企業がカスタマーと電子メールで信頼性の高いコミュニケーションを実現できるように、シスコは独自の Virtual Gateway テクノロジーを開発しました。Virtual Gateway テクノロジーを使用すると、Cisco アプライアンスを複数の Virtual Gateway アドレスに分割し、そのアドレスを使用して電子メールを送受信できます。各 Virtual Gateway アドレスには、別々の IP アドレス、ホスト名、ドメイン、および電子メール キューが与えられます。

別々の IP アドレスとホスト名を各 Virtual Gateway アドレスに割り当てることにより、ゲートウェイ経由で配信される電子メールが受信者ホストで正しく識別され、重要な電子メールがスパムと見なされてブロックされるのを防ぐことができます。Cisco アプライアンスには、Virtual Gateway アドレスごとに SMTP HELO コマンドで正しいホスト名を付与できる高度な機能があります。そのため、受信側の Internet Service Provider (ISP; インターネット サービス プロバイダー) が逆 DNS ルックアップを実行すると、Cisco アプライアンスでは、その Virtual Gateway アドレス経由で送信された電子メールの IP アドレスと一致させることができます。多くの ISP では迷惑電子メールを検出するために逆 DNS ルックアップを使用しているため、この機能は非常に有用です。逆 DNS ルックアップでの IP アドレスが送信側ホストの IP アドレスと一致しない場合、ISP では、送信者が不正であると見なして、電子メールを破棄する頻度が高くなります。Cisco Virtual Gateway テクノロジーでは、逆 DNS ルックアップが送信側の IP アドレスと常に一致するため、メッセージが意図せずブロックされてしまうのを防げます。

各 Virtual Gateway アドレスでのメッセージも、別々のメッセージ キューに割り当てられます。受信者ホストで特定の Virtual Gateway アドレスからの電子メールをブロックしている場合、そのホスト宛のメッセージはキューに残され、最終的にはタイムアウトします。しかしブロックされていない別の Virtual Gateway キュー内にある同じドメイン宛のメッセージは、正常に配信されます。これらのキューは、配信では別のもので扱われますが、システム管理、ロギング、レポートの機能では、全体的な観点からすべての Virtual Gateway キューが一体のものとして扱われます。

Virtual Gateway アドレスの設定

Cisco Virtual Gateway アドレスを設定する前に、電子メールの送信元として使用される IP アドレスのセットを割り当てる必要があります。(詳細については、『Cisco IronPort AsyncOS for Email Configuration Guide』の「Assigning Network and IP Addresses」を参照してください)。また、IP ア

ドレスが有効なホスト名に解決されるように DNS サーバが正しく設定されている必要があります。DNS サーバが正しく設定されていれば、受信者ホストで逆 DNS ルックアップが実行されると、有効な IP/ホスト名のペアに解決されます。

仮想ゲートウェイで使用する新しい IP インターフェイスの作成

IP アドレスとホスト名が確立したら、Virtual Gateway アドレスを設定するために、まずはその IP/ホスト名のペアで新しい IP インターフェイスを作成します。それには、GUI の [ネットワーク (Network)] > [IP インターフェイス (IP Interfaces)] ページ、または CLI の `interfaceconfig` コマンドを使用します。

IP インターフェイスを設定したら、複数の IP インターフェイスをインターフェイス グループへと結合できます。これらのグループは、電子メールの配信時に「ラウンドロビン」方式で順番に使用される Virtual Gateway アドレスに割り当てることができます。

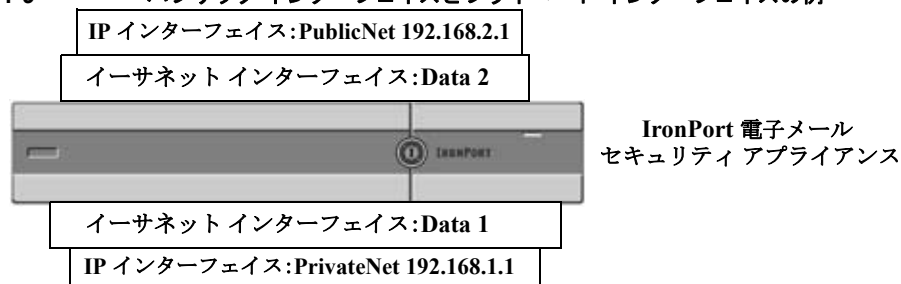
必要な IP インターフェイスを作成したら、2 つの方法で Virtual Gateway アドレスを設定し、各 IP インターフェイスまたはインターフェイス グループから送信される電子メール キャンペーンを定義します。

- `altsrchoost` コマンドを使用すると、特定の送信者 IP アドレスまたはエンベロープ送信者アドレスの情報からホストの IP インターフェイス (Virtual Gateway アドレス) またはインターフェイス グループに電子メールをマッピングして配信できます。
- メッセージフィルタを使用して、特定ホストの IP インターフェイス (Virtual Gateway アドレス) またはインターフェイス グループを使用してフラグ付きのメッセージを配信するためのフィルタを設定できます。「送信元ホスト (Virtual Gateway アドレス) 変更アクション」(P.9-60) を参照してください。(この方法は前述の方法よりも柔軟性があり、強力です)。

IP インターフェイスを作成する詳細については、『Cisco IronPort AsyncOS for Email Configuration Guide』の付録「Accessing the Appliance」を参照してください。

ここまで、図 21-9 に示すように定義された次のインターフェイスを用いて、電子メール ゲートウェイの設定を使用してきました。

図 21-9 パブリック インターフェイスとプライベート インターフェイスの例



次の例では、[IP インターフェイス (IP Interfaces)] ページで管理インターフェイスの他に 2 つのインターフェイス (PrivateNet および PublicNet) が設定されていることを確認できます。

図 21-10 [IP インターフェイス (IP Interfaces)] ページ
IP Interfaces

Network Interfaces and IP Addresses			
Add IP Interface...			
Name	IP Address	Hostname	Delete
Management	192.168.42.42/24	mail3.example.com	
PrivateNet	192.168.1.1/24	mail3.example.com	
PublicNet	192.168.2.1/24	mail3.example.com	

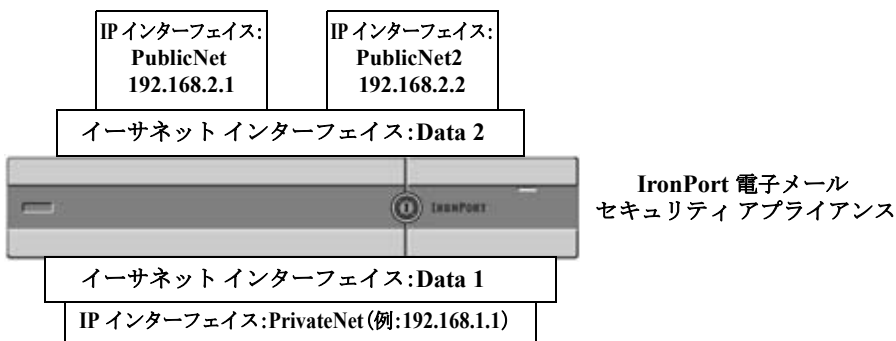
次に、[IP インターフェイスの追加 (Add IP Interface)] ページを使用して、Data2 イーサネット インターフェイス上に PublicNet2 という名前の新しいインターフェイスを作成します。IP アドレス 192.168.2.2 が使用され、ホスト名 mail4.example.com が指定されています。さらに、FTP (ポート 21)、Telnet (ポート 23)、および SSH (ポート 22) がイネーブルになります。

図 21-11 [IP インターフェイスの追加 (Add IP Interface)] ページ
Add IP Interface

IP Interface Settings									
Name:	PublicNet2								
Ethernet Port:	Data 2								
IP Address:	192.168.2.2 *								
Netmask:	255.255.255.0 *								
Hostname:	mail4.example.com								
Services:	<table border="1"> <thead> <tr> <th>Service</th> <th>Port</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/> FTP</td> <td>21</td> </tr> <tr> <td><input checked="" type="checkbox"/> Telnet</td> <td>23</td> </tr> <tr> <td><input checked="" type="checkbox"/> SSH</td> <td>22 *</td> </tr> </tbody> </table>	Service	Port	<input checked="" type="checkbox"/> FTP	21	<input checked="" type="checkbox"/> Telnet	23	<input checked="" type="checkbox"/> SSH	22 *
Service	Port								
<input checked="" type="checkbox"/> FTP	21								
<input checked="" type="checkbox"/> Telnet	23								
<input checked="" type="checkbox"/> SSH	22 *								
Appliance Management									
<input type="checkbox"/> HTTP	80 *								
<input type="checkbox"/> HTTPS	443 *								
<input type="checkbox"/> Redirect HTTP requests to HTTPS (HTTP and HTTPS Services will be turned on)									
IronPort Spam Quarantine									
<input type="checkbox"/> IronPort Spam Quarantine HTTP	80								
<input type="checkbox"/> IronPort Spam Quarantine HTTPS	443								
<input type="checkbox"/> Redirect HTTP requests to HTTPS (HTTP and HTTPS Services will be turned on)									
<input type="checkbox"/> This is the default interface for IronPort Spam Quarantine Quarantine login and notifications will originate on this interface. URL Displayed in Notifications: <input type="radio"/> Hostname <input type="radio"/> (examples: http://xpmq.url/, http://10.1.1.1:82/)									
Warnings - * Please exercise care when disabling or changing these items, as this could disrupt active connections to this appliance when changes to these items are committed. ** Hyperlinks and URLs affected by these changes will not be usable until the changes are committed.									
<input type="button" value="Cancel"/>	<input type="button" value="Submit"/>								

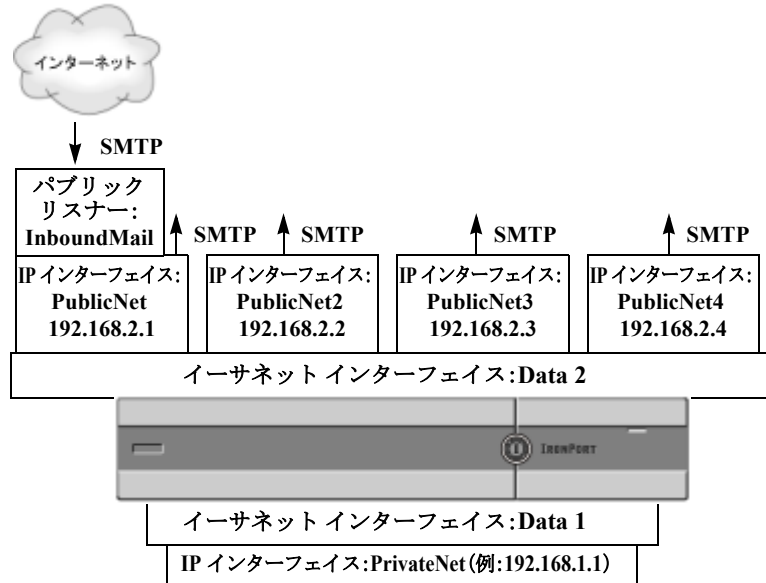
これで電子メール ゲートウェイのコンフィギュレーションは次のようになります。

図 21-12 別のパブリック インターフェイスの追加



Virtual Gateway アドレスを使用すると、図 21-13 に示すようなコンフィギュレーションも可能です。

図 21-13 1 つのイーサネット インターフェイス上にある 4 つの Virtual Gateway アドレス



4 つの IP インターフェイスはそれぞれメール配信に使用できますが、インターネットからのメールを受け入れるように設定されるのはパブリック リスナー 1 つだけです。

メッセージから配信用 IP インターフェイスへのマッピング

altsrchost コマンドを使用すると、各 Cisco アプライアンスを、電子メールの配信元となる複数の IP インターフェイス (Virtual Gateway アドレス) にセグメント化することが最も単純で単刀直入な方法です。ただし、メッセージを特定の Virtual Gateway にマッピングする際にさらに強力な柔軟な方法が必要であれば、メッセージフィルタの使用を検討してください。詳細については、第 9 章「メッセージフィルタを使用した電子メールポリシーの適用」を参照してください。

altsrchost コマンドを使用すると、次のいずれかに基づいて、電子メールの配送中に使用する IP インターフェイスまたはインターフェイス グループを管理できます。

- 送信者の IP アドレス
- エンベロープ送信者アドレス

電子メールの配信元にする IP インターフェイスまたはインターフェイス グループを指定するには、送信者の IP アドレスまたはエンベロープ送信者アドレスを IP インターフェイスまたはインターフェイス グループ (インターフェイス名またはグループ名で指定) とペアにするマッピング キーを作成します。

Cisco AsyncOS では、IP アドレスとエンベロープ送信者アドレスの両方をマッピング キーと比較します。IP アドレスまたはエンベロープ送信者アドレスがいずれかのキーと一致する場合、対応する IP インターフェイスが発信配信に使用されます。一致しない場合は、デフォルトの発信インターフェイスが使用されます。

一致する可能性のあるキーを優先順に示します。

送信者の IP アドレス	送信者の IP アドレスは完全一致する必要があります。 例: 192.168.1.5
完全形式のエンベロープ送信者	エンベロープ送信者は、アドレス全体が完全一致する必要があります。 例: username@example.com

ユーザ名	エンベロープ送信者アドレスの @ 記号までの部分に対してユーザ名構文と一致させます。@ 記号を含める必要があります。例：username@
ドメイン	エンベロープ送信者アドレスの @ 記号で始まる部分に対してドメイン名構文と一致させます。@ 記号を含める必要があります。例：@example.com



(注) リスナーは `altsrchoost` テーブルで情報をチェックし、マスカレード情報をチェックした後からメッセージフィルタがチェックされる前までに、電子メールを特定のインターフェイスに転送します。

`altsrchoost` コマンド内のサブコマンドを使用して、CLI で Virtual Gateway にマッピングを作成します。

構文	説明
<code>new</code>	新しいマッピングを手動で作成します。
<code>print</code>	マッピングの現在のリストを表示します。
<code>delete</code>	テーブルからマッピングを 1 つ削除します。

altsrchoost ファイルのインポート

HAT、RAT、`smtproutes`、マスカレード テーブル、エイリアス テーブルと同様に、`altsrchoost` エントリはファイルをエクスポートおよびインポートして変更できます。

手順

- ステップ 1** `altsrchoost` コマンドの `export` サブコマンドを使用して、既存のエントリをファイル（ファイル名は自分で指定）にエクスポートします。
- ステップ 2** CLI の外部で、ファイルを取得します。（詳細については、[付録 A 「アプライアンスへのアクセス」](#) を参照してください）。
- ステップ 3** テキスト エディタを使用して、ファイルに新しいエントリを作成します。ルールが `altsrchoost` テーブルに出現する順序が重要です。
- ステップ 4** ファイルを保存してインターフェイスの「`altsrchoost`」ディレクトリに配置し、インポートできるようにします。（詳細については、[付録 A 「アプライアンスへのアクセス」](#) を参照してください）。
- ステップ 5** `altsrchoost` の `import` サブコマンドを使用して、編集したファイルをインポートします。

altsrchoost の制限

最大 1,000 個の `altsrchoost` エントリを追加できます。

altsrchoost コマンド用に有効なマッピングが記載されたテキスト ファイルの例

```
# Comments to describe the file

@example.com DemoInterface

paul@ PublicInterface

joe@ PublicInterface

192.168.1.5, DemoInterface

steve@example.com PublicNet
```

import および export サブコマンドは、1 行単位で実行され、送信者 IP アドレスまたはエンベロープ送信者アドレスの行をインターフェイス名にマッピングします。スペース以外の文字からなる 1 番目のブロックがキー、スペース以外の文字からなる 2 番目のブロックがインターフェイス名となり、カンマ (,) またはスペース () で区切ります。コメント行はナンバー記号 (#) で始まり、無視されます。

CLI を使用した altsrchoost マッピングの追加

次の例では、altsrchoost テーブルが出力されて、既存のマッピングがないことが示されます。その後、2 つのエントリが作成されます。

- グループウェア サーバ ホスト @exchange.example.com からのメールは、PublicNet インターフェイスにマッピングされます。
- 送信者 IP アドレス 192.168.35.35 (たとえば、マーケティング キャンペーン メッセージング システム) からのメールは、PublicNet2 インターフェイスにマッピングされます。

最後に、確認のために altsrchoost マッピングが出力されて、変更が確定されます。

```
mail3.example.com> altsrchoost
```

```
There are currently no mappings configured.
```

```
Choose the operation you want to perform:
```

- NEW - Create a new mapping.
- IMPORT - Load new mappings from a file.

```
[> new
```

```
Enter the Envelope From address or client IP address for which you want to set up a
Virtual Gateway mapping. Partial addresses such as "@example.com" or "user@" are
allowed.
```

```
[> @exchange.example.com
```

Which interface do you want to send messages for @exchange.example.com from?

1. PublicNet2 (192.168.2.2/24: mail4.example.com)
2. Management (192.168.42.42/24: mail3.example.com)
3. PrivateNet (192.168.1.1/24: mail3.example.com)
4. PublicNet (192.168.2.1/24: mail4.example.com)

[1]> 4

Mapping for @exchange.example.com on interface PublicNet created.

Choose the operation you want to perform:

- NEW - Create a new mapping.
- EDIT - Modify a mapping.
- DELETE - Remove a mapping.
- IMPORT - Load new mappings from a file.
- EXPORT - Export all mappings to a file.
- PRINT - Display all mappings.
- CLEAR - Remove all mappings.

[]> new

Enter the Envelope From address or client IP address for which you want to set up a Virtual Gateway mapping. Partial addresses such as "@example.com" or "user@" are allowed.

[]> 192.168.35.35

Which interface do you want to send messages for 192.168.35.35 from?

1. PublicNet2 (192.168.2.2/24: mail4.example.com)
2. Management (192.168.42.42/24: mail3.example.com)
3. PrivateNet (192.168.1.1/24: mail3.example.com)
4. PublicNet (192.168.2.1/24: mail4.example.com)

```
[1]> 1
```

```
Mapping for 192.168.35.35 on interface PublicNet2 created.
```

```
Choose the operation you want to perform:
```

- NEW - Create a new mapping.
- EDIT - Modify a mapping.
- DELETE - Remove a mapping.
- IMPORT - Load new mappings from a file.
- EXPORT - Export all mappings to a file.
- PRINT - Display all mappings.
- CLEAR - Remove all mappings.

```
[> print
```

1. 192.168.35.35 -> PublicNet2
2. @exchange.example.com -> PublicNet

```
Choose the operation you want to perform:
```

- NEW - Create a new mapping.
- EDIT - Modify a mapping.
- DELETE - Remove a mapping.
- IMPORT - Load new mappings from a file.
- EXPORT - Export all mappings to a file.
- PRINT - Display all mappings.
- CLEAR - Remove all mappings.

```
[>
```

```
mail3.example.com> commit
```

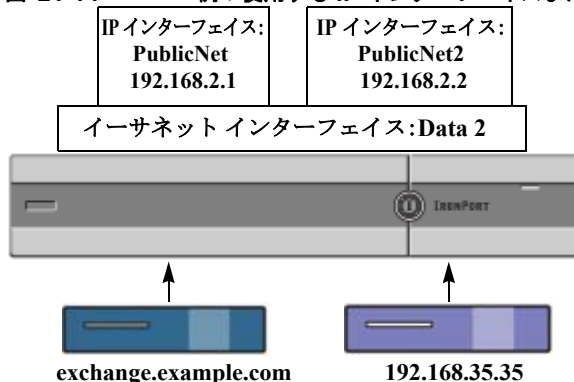
```
Please enter some comments describing your changes:
```

```
[> Added 2 altsrchoost mappings
```

```
Changes committed: Thu Mar 27 14:57:56 2003
```

この例におけるコンフィギュレーションの変更を図 21-14 に示します。

図 21-14 例：使用する IP インターフェイスまたはインターフェイス グループの選択



これらのマッピングを作成するように altsrchoost テーブルが変更されました。

@exchange.example.com からのメッセージはインターフェイス PublicNet を使用し、192.168.35.35 からのメッセージはインターフェイス PublicNet2 を使用します。

Virtual Gateway アドレスのモニタリング

Virtual Gateway アドレスごとに独自の配信用電子メール キューがありますが、システム管理、ログイン、レポートの機能では、全体的な観点からすべての Virtual Gateway キューが一体のものとして扱われます。Virtual Gateway キューごとに受信者ホストのステータスをモニタするには、hoststatus および hostrate コマンドを使用します。『Cisco IronPort AsyncOS for Email Daily Management Guide』の「Reading the Available Components of Monitoring」を参照してください。

hoststatus コマンドは、特定の受信者ホストに関する電子メール動作のモニタリング情報を返します。

Virtual Gateway テクノロジーを使用している場合は、各 Virtual Gateway アドレスに関する情報も表示されます。このコマンドは、返されるホスト情報のドメインを入力する必要があります。AsyncOS キャッシュに格納されている DNS 情報と、受信者ホストから最後に返されたエラーも表示されます。返されるデータは、最後に実行した resetcounters コマンドからの累積です。

返される統計情報は、カウンタとゲージの 2 つのカテゴリにグループ化されます。さらに、返される他のデータには、最後のアクティビティ、MX レコード、最後の 5XX エラーがあります。

Virtual Gateway アドレスごとの配信接続の管理

一部のシステム パラメータには、システム レベルと Virtual Gateway アドレス レベルで設定が必要です。

たとえば、一部の受信者 ISP では、各クライアント ホストに許可されている接続数を制限しています。そのため、特に電子メールが複数の Virtual Gateway アドレスで配信されているときに、ISP との関係を管理することが必要です。

destconfig コマンド、および Virtual Gateway アドレスに対する影響については、「送信先コントロールによる電子メール配信の管理」(P.21-43) を参照してください。

Virtual Gateway アドレスの「グループ」を作成すると、グループが 254 個の IP アドレスで構成されている場合であっても、Virtual Gateway のグッド ネイバー テーブル設定がグループに適用されます。

たとえば、254 個の発信 IP アドレスのグループを作成して、「ラウンドロビン」方式で順番に使用するようにセットアップされているとします。また、small-isp.com のグッド ネイバー テーブルで、同時接続数がシステムの場合は 100、Virtual Gateway アドレスの場合は 10 であるとします。このコンフィギュレーションでは、そのグループ内の 254 個の IP アドレスすべてに対して、合計で 10 よりも多くの接続が開くことはありません。グループは、単一の Virtual Gateway アドレスとして扱われます。

[グローバル配信停止 (Global Unsubscribe)] 機能の使用

特定の受信者、受信者ドメイン、または IP アドレスが Cisco アプライアンスからメッセージを受信しないようにするには、Cisco AsyncOS の [グローバル配信停止 (Global Unsubscribe)] 機能を使用します。unsubscribe コマンドを使用すると、[グローバル配信停止 (Global Unsubscribe)] リストにアドレスを追加/削除したり、この機能をイネーブル/ディセーブルにすることができます。「グローバルに配信停止された」ユーザ、ドメイン、電子メールアドレス、および IP アドレスのリストで、すべての受信者アドレスがチェックされます。受信者がリスト内のアドレスと一致する場合、受信者はドロップされるかハードバウンズされ、Global Unsubscribe (GUS; グローバル配信停止) カウンタが増分されます。(ログファイルには、一致する受信者がドロップされたのかハードバウンズされたのかが記録されます)。GUS のチェックは、電子メールを受信者に送信する直前に行われるため、システムで送信されるすべてのメッセージが検査されます。



(注)

[グローバル配信停止 (Global Unsubscribe)] 機能は、メーリングリストからの名前の削除やメーリングリストの全般的な保守に代わるものではありません。この機能は、不適切なエンティティに電子メールが配信されないようにするフェールセーフメカニズムとして動作することを目的としています。

[グローバル配信停止 (Global Unsubscribe)] 機能は、プライベートリスナーおよびパブリックリスナーに適用されます。

[グローバル配信停止 (Global Unsubscribe)] 停止に含めることのできる最大アドレス数は 10,000 件です。この制限を増やすには、Cisco 販売代理店にお問い合わせください。[グローバル配信停止 (Global Unsubscribe)] に追加されたアドレスは、次の 4 つのうちいずれかの形式をとります。

表 21-10 グローバル配信停止の構文

username@example.com	完全形式の電子メールアドレス この構文は、特定ドメインの特定受信者をブロックするために使用されます。
username@	ユーザ名 ユーザ名構文は、すべてのドメインで特定ユーザ名を持つすべての受信者をブロックします。構文は、ユーザ名の後にアットマーク (@) を付けます。
@example.com	ドメイン ドメイン構文は、特定ドメイン宛のすべての受信者をブロックするために使用されます。構文は、具体的なドメインの前にアットマーク (@) を付けます。

表 21-10 グローバル配信停止の構文 (続き)

@.example.com	部分ドメイン 部分ドメイン構文は、特定ドメイン宛およびそのすべてのサブドメイン宛のすべての受信者をブロックするために使用されます。
10.1.28.12	IP アドレス IP アドレス構文は、特定 IP アドレス宛のすべての受信者をブロックするために使用されます。単一 IP アドレスで複数ドメインをホストしている場合に、この構文が便利です。構文は、一般的なドット区切りのオクテット IP アドレスです。

CLI を使用したグローバル配信停止へのアドレスの追加

この例では、アドレス `user@example.net` がグローバル配信停止リストに追加され、メッセージをハードバウンスするように機能が設定されます。このアドレスに送信されるメッセージはバウンスされず、配信の直前にメッセージがバウンスされます。

```
mail3.example.com> unsubscribe
```

```
Global Unsubscribe is enabled. Action: drop.
```

```
Choose the operation you want to perform:
```

- NEW - Create a new entry.
- IMPORT - Import entries from a file.
- SETUP - Configure general settings.

```
[ ]> new
```

```
Enter the unsubscribe key to add. Partial addresses such as
```

```
"@example.com" or "user@" are allowed, as are IP addresses. Partial hostnames such as "@.example.com" are allowed.
```

```
[ ]> user@example.net
```

```
Email Address 'user@example.net' added.
```

```
Global Unsubscribe is enabled.
```

```
Choose the operation you want to perform:
```

■ [グローバル配信停止 (Global Unsubscribe)] 機能の使用

```
- NEW - Create a new entry.
- DELETE - Remove an entry.
- PRINT - Display all entries.
- IMPORT - Import entries from a file.
- EXPORT - Export all entries to a file.
- SETUP - Configure general settings.
- CLEAR - Remove all entries.

[ ]> setup

Do you want to enable the Global Unsubscribe feature? [Y]> y

Would you like matching messages to be dropped or bounced?

1. Drop
2. Bounce

[1]> 2

Global Unsubscribe is enabled. Action: bounce.

Choose the operation you want to perform:

- NEW - Create a new entry.
- DELETE - Remove an entry.
- PRINT - Display all entries.
- IMPORT - Import entries from a file.
- EXPORT - Export all entries to a file.
- SETUP - Configure general settings.
- CLEAR - Remove all entries.

[ ]>

mail3.example.com> commit
```

```
Please enter some comments describing your changes:
```

```
[ ]> Added username "user@example.net" to global unsubscribe
```

```
Changes committed: Thu Mar 27 14:57:56 2003
```

グローバル配信停止ファイルのエクスポートおよびインポート

HAT、RAT、smtproutes、スタティック マスカレード テーブル、エイリアス テーブル、ドメイン マップ テーブル、altsrchost エントリと同様に、グローバル配信停止エントリはファイルのエクスポートおよびインポートして変更できます。

手順

ステップ 1 unsubscribe コマンドの export サブコマンドを使用して、既存のエントリをファイル（ファイル名は自分で指定）にエクスポートします。

ステップ 2 CLI の外部で、ファイルを取得します。（詳細については、[付録 A「アプライアンスへのアクセス」](#)を参照してください）。

ステップ 3 テキスト エディタを使用して、ファイルに新しいエントリを作成します。

ファイル内でエントリを区切るには、改行します。あらゆるオペレーティング システムの改行表現を使用できます（<CR>、<LF>、または <CR><LF>）。コメント行はナンバー記号（#）で始まり、無視されます。たとえば、次のファイルでは、単一の受信者電子メール アドレス（test@example.com）、特定ドメインのすべての受信者（@testdomain.com）、複数ドメインで同じ名前を持つすべてのユーザ（testuser@）、および特定 IP アドレスの任意の受信者（11.12.13.14）が除外されます。

```
# this is an example of the global_unsubscribe.txt file
```

```
test@example.com
```

```
@testdomain.com
```

```
testuser@
```

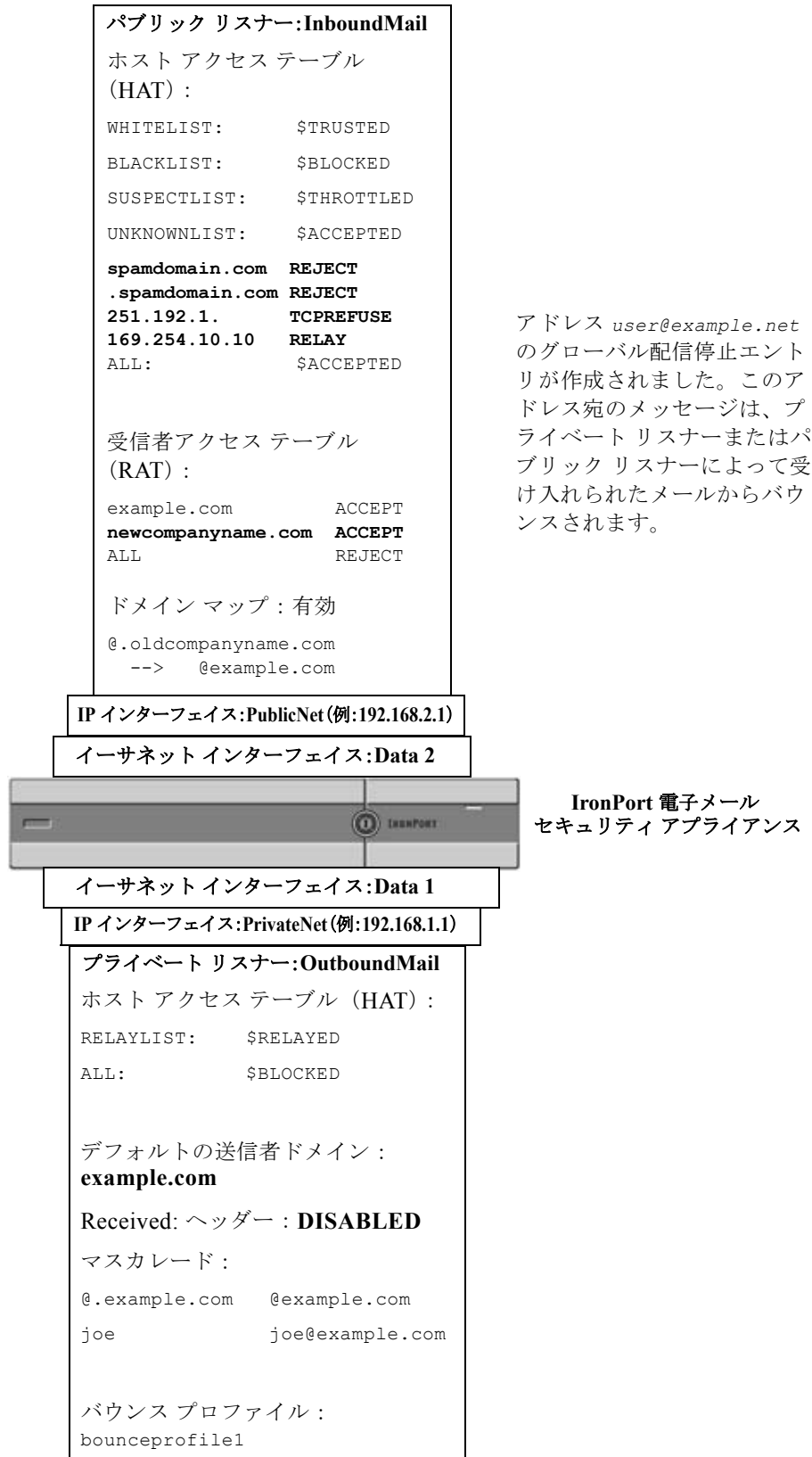
```
11.12.13.14
```

ステップ 4 ファイルを保存してインターフェイスの configuration ディレクトリに配置し、インポートできるようにします。（詳細については、[付録 A「アプライアンスへのアクセス」](#)を参照してください）。

ステップ 5 unsubscribe の import サブコマンドを使用して、編集したファイルをインポートします。

これで電子メール ゲートウェイのコンフィギュレーションは次のようになります。

図 21-15 グローバル配信停止の例



確認：電子メールパイプライン

表 21-11 および表 21-12 に、受信から配信へのルーティングまで、電子メールがシステムでルーティングされる様子の概要を示します。各機能は上から順に実行されます。ここでは簡単に説明します。

図 21-15 の共有領域は、ワーク キュー内で発生する処理を表します。

このパイプラインに含まれる機能の設定の大部分は、`trace` コマンドを使用してテストできます。詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Debugging Mail Flow Using Test Messages: Trace」を参照してください。



(注) 発信メールの場合は、ウイルス アウトブレイク フィルタ ステージの後に RSA 電子メール データ損失防止スキャンが実行されます。

表 21-11 Cisco アプライアンスの電子メールパイプライン：電子メール受信機能

機能	説明
ホスト アクセス テーブル (HAT)	接続の ACCEPT、REJECT、RELAY、または TCPREFUSE。
ホスト DNS 送信者検証	最大アウトバウンド接続数。
送信者グループ	IP アドレスあたりの最大同時インバウンド接続数。
エンベロープ送信者検証	接続あたりの最大メッセージ サイズおよびメッセージ数。
送信者検証例外テーブル	メッセージあたりおよび時間あたりの最大受信者数。
メール フロー ポリシー	TCP リッスン キュー サイズ。 TLS : no/preferred/required SMTP AUTH : no/preferred/required 不正な形式の FROM ヘッダーを持つ電子メールのドロップ 送信者検証例外テーブル内のエントリからのメールを常に受け入れるか拒否します。 SenderBase オン/オフ (IP プロファイリング/フロー制御)
Received ヘッダー	受け入れた電子メールに対する Received ヘッダーの追加：オン/オフ。
デフォルト ドメイン	「素」ユーザ アドレスにデフォルト ドメインを追加します。
バウンス検証	着信バウンス メッセージを正規メッセージとして検証します。
ドメイン マップ	ドメイン マップ テーブル内のドメインと一致するメッセージに含まれている各受信者のエンベロープ受信者の書き換え。
受信者アクセス テーブル (RAT)	(パブリック リスナーのみ) RCPT TO およびカスタム SMTP 応答内の受信者の ACCEPT または REJECT 特別な受信者にスロットリングのバイパスを許可します。
エイリアス テーブル	エンベロープ受信者を書き換えます。(システム全体を対象に設定されます。aliasconfig は、listenerconfig のサブコマンドではありません)。
LDAP 受信者の受け入れ	受信者受け入れの LDAP 検証は、SMTP カンバセーションで行われます。受信者が LDAP ディレクトリで見つからない場合、メッセージはドロップされるかバウンスされます。代わりにワーク キュー内で LDAP 検証を行うように設定することもできます。

表 21-12 Cisco アプライアンスの電子メールパイプライン：ルーティングおよび配信機能

ワークキュー	LDAP 受信者の受け入れ	受信者受け入れの LDAP 検証はワーク キュー内で行われます。受信者が LDAP ディレクトリで見つからない場合、メッセージはドロップされるかバウンスされます。代わりに SMTP キャンパセーション LDAP 検証を行うよう設定することもできます。	
	マスカレード または LDAP マスカレード	マスカレードは、ワーク キューで行われます。マスカレードでは、スタティック テーブルを使用するか LDAP クエリーを使用して、エンベロープ送信者、To:、From:、CC: ヘッダーを書き換えます。	
	LDAP ルーティング	LDAP クエリーは、メッセージルーティングまたはアドレス書き換えのために実行されます。グループ LDAP クエリーは、メッセージ フィルタ ルール mail-from-group および rcpt-to-group と連携して動作します。	
	メッセージ フィルタ *	メッセージ フィルタは、メッセージが「分裂」される前に適用されます。* メッセージを隔離エリアに送信できます。	
	アンチスパム **	受信者単位のスキャン	アンチスパム スキャン エンジンでは、メッセージを調査して、さらに処理できるようにその分析結果を返します。
	アンチウイルス *		アンチウイルス スキャンでは、ウイルスを検出するためにメッセージを検査します。メッセージはスキャンされ、可能であれば、任意で修復されます。 * メッセージを隔離エリアに送信できます。
	コンテンツ フィルタ *		コンテンツ フィルタが適用されます。* メッセージを隔離エリアに送信できます。
	アウトブレイク フィルタ *	アウトブレイク フィルタ機能を使用すると、ウイルス感染から保護できます。* メッセージを隔離エリアに送信できます。	
	仮想ゲートウェイ	特定の IP インターフェイスまたは IP インターフェイスのグループを介してメールを送信します。	
	配信制限	1. デフォルト配信インターフェイスを設定します。 2. アウトバウンド接続の合計最大数を設定します。	
ドメインベースの制限値	ドメイン単位で、各仮想ゲートウェイおよびシステム全体の最大アウトバウンド接続数、使用するバウンス プロファイル、配信用の TLS プレファレンス：no/preferred/required を定義します。		
ドメインベースのルーティング	エンベロープ受信者を書き換えず、ドメインに基づいてメールをルーティングします。		
グローバル配信停止	特定のリストに従って受信者をドロップします（システム全体を対象に設定）。		
バウンス プロファイル	配信不能メッセージの処理です。リスナー単位、送信先コントロール エントリ単位、およびメッセージ フィルタ 経由で設定可能です。		

* これらの機能では、Quarantines という特別なキューにメッセージを送信できます。



CHAPTER 22

LDAP クエリー

- 「LDAP クエリーの概要」 (P.22-1)
- 「LDAP サーバに関する情報を保存する LDAP サーバ プロファイルの作成」 (P.22-5)
- 「LDAP クエリーに関する作業」 (P.22-12)
- 「受信者検証で受け入れクエリーを使用する」 (P.22-19)
- 「複数ターゲット アドレスへのメール送信にルーティング クエリーを使用する」 (P.22-20)
- 「エンベロープ送信者を書き換えるためのマスカレード クエリーの使用」 (P.22-21)
- 「受信者がグループ メンバーであるかどうかを指定するグループ LDAP クエリーの使用」 (P.22-23)
- 「特定のドメインヘルディングするためのドメイン ベース クエリーの使用」 (P.22-26)
- 「一連の LDAP クエリーを実行するためのチェーン クエリーの使用」 (P.22-28)
- 「LDAP によるディレクトリ ハーベスト攻撃防止」 (P.22-29)
- 「SMTP 認証を行うための AsyncOS の設定」 (P.22-32)
- 「ユーザの外部 LDAP 認証の設定」 (P.22-40)
- 「Cisco IronPort スпам隔離内のエンド ユーザ認証」 (P.22-43)
- 「スパム隔離のエイリアス統合のクエリー」 (P.22-44)
- 「RSA Enterprise Manager の送信者のユーザ識別名の特定」 (P.22-45)
- 「AsyncOS を複数の LDAP サーバと連携させるための設定」 (P.22-46)

LDAP クエリーの概要

ユーザ情報がネットワーク インフラストラクチャ内の LDAP ディレクトリ (Microsoft Active Directory、SunONE Directory Server、OpenLDAP などのディレクトリ) に格納されている場合は、メッセージの受け入れ、ルーティング、および認証のために LDAP サーバに対してクエリーを実行するように Cisco を設定できます。Cisco アプライアンスは、1 つまたは複数の LDAP サーバと連携させるように設定できます。

ここでは、実行できる LDAP クエリーのタイプ、LDAP と Cisco アプライアンスとが連携してメッセージの認証、受け入れ、ルーティングを行うしくみ、および LDAP と連携するように Cisco アプライアンスを設定する方法の概要を示します。

LDAP クエリーの概要

ユーザ情報がネットワーク インフラストラクチャ内の LDAP ディレクトリに格納されている場合は、次の目的で LDAP サーバに対してクエリーを実行するように Cisco アプライアンスを設定できます。

- **受け入れクエリー**。既存の LDAP インフラストラクチャを使用して、着信メッセージ（パブリック リスナーでの）の受信者メールアドレスの扱い方を定義できます。詳細については、「[受信者検証で受け入れクエリーを使用する](#)」(P.22-19) を参照してください。
- **ルーティング (エイリアシング)**。ネットワーク内の LDAP ディレクトリに格納されている情報に基づいてメッセージを適切なアドレスやメール ホストへルーティングするように、アプライアンスを設定できます。詳細については、「[複数ターゲット アドレスへのメール送信にルーティングクエリーを使用する](#)」(P.22-20) を参照してください。
- **証明書認証** ユーザのメール クライアントと電子メール セキュリティ アプライアンス間の SMTP セッションを認証するためのクライアント証明書の有効性を確認するクエリーを作成できます。詳細については、「[クライアント証明書の有効性の確認](#)」(P.23-51) を参照してください。
- **マスカレード**。発信メールの場合はエンベロープ送信者、着信メールの場合はメッセージ ヘッダー (To:、Reply To:、From:、CC: など) をマスカレードできます。マスカレードの詳細については、「[エンベロープ送信者を書き換えるためのマスカレードクエリーの使用](#)」(P.22-21) を参照してください。
- **グループクエリー**。LDAP ディレクトリ内のグループに基づいてメッセージに対するアクションを実行するように、Cisco アプライアンスを設定できます。このように設定するには、グループクエリーとメッセージフィルタとを関連付けます。定義済みの LDAP グループに一致するメッセージに対しては、メッセージフィルタに使用できる任意のメッセージアクションを実行できます。詳細については、「[受信者がグループメンバーであるかどうかを指定するグループ LDAP クエリーの使用](#)」(P.22-23) を参照してください。
- **ドメインベースクエリー**。ドメインベースクエリーを作成すると、Cisco アプライアンスは同じリスナー上でドメインごとに異なるクエリーを実行できます。電子メールセキュリティアプライアンスがドメインベースクエリーを実行するときは、どのクエリーを使用するかをドメインに基づいて決定し、そのドメインに関連付けられている LDAP サーバに対してクエリーを実行します。
- **チェーンクエリー**。チェーンクエリーを作成すると、Cisco アプライアンスに一連のクエリーを順番に実行させることができます。チェーンクエリーが設定済みのときは、Cisco アプライアンスはシーケンス内のクエリーを 1 つずつ実行し、LDAP アプライアンスから肯定的な結果が返されると実行を停止します。
- **ディレクトリハーベスト防止**。LDAP ディレクトリを使用したディレクトリハーベスト攻撃を防ぐように Cisco アプライアンスを設定できます。ディレクトリハーベスト防止は、SMTP コンバセッション中に行うことも、ワークキューの中で行うこともできます。受信者が LDAP ディレクトリ内で見つからない場合に、遅延バウンスを実行するか、そのメッセージ全体をドロップするかを設定できます。その結果、スパム送信者はメールアドレスが有効なものかどうかを区別できなくなります。「[LDAP によるディレクトリハーベスト攻撃防止](#)」(P.22-29) を参照してください。
- **SMTP 認証**。AsyncOS では、SMTP 認証がサポートされています。SMTP Auth は、SMTP サーバに接続するクライアントを認証するメカニズムです。この機能を利用すると、ユーザはリモート接続するとき（たとえば自宅や出張先にいる場合）でも、メールサーバを使用してメールを送信できるようになります。詳細については、「[SMTP 認証を行うための AsyncOS の設定](#)」(P.22-32) を参照してください。
- **外部認証**。Cisco アプライアンスにログインするユーザの認証を LDAP ディレクトリを使用して行うように、Cisco アプライアンスを設定できます。詳細については、「[ユーザの外部 LDAP 認証の設定](#)」(P.22-40) を参照してください。

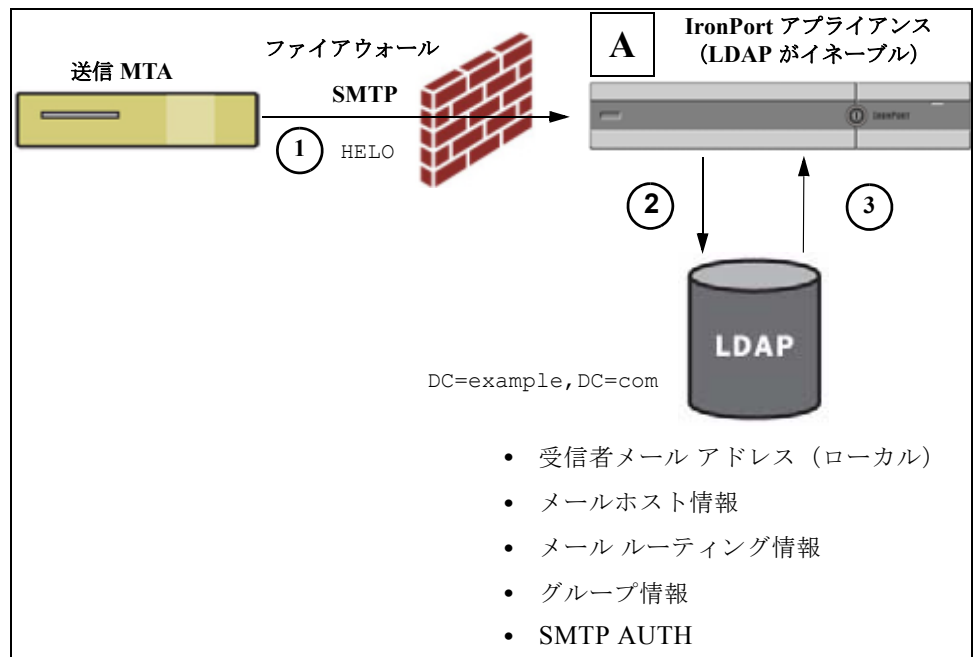
- **スパム隔離へのエンドユーザ認証。** エンドユーザ隔離画面にログインするユーザを検証するように、アプライアンスを設定できます。詳細については、「[Cisco IronPort スパム隔離内のエンドユーザ認証](#)」(P.22-43) を参照してください。
- **スパム隔離のエイリアス統合。** スпамに関する電子メール通知を使用する場合、このクエリーを使用してエンドユーザのエイリアスを統合すると、エンドユーザがエイリアスのメールアドレスごとに隔離通知を受け取ることはなくなります。詳細については、「[スパム隔離のエイリアス統合のクエリー](#)」(P.22-44) を参照してください。
- **ユーザ識別名。** データ消失防止 (DLP) のために RSA Enterprise Manager を使用する場合、このクエリーは DLP 違反を含む可能性があるメッセージ送信者の識別名を取得します。電子メールセキュリティ アプライアンスは、Enterprise Manager に DLP インシデント データを送信する際に識別名を含めます。詳細については、「[RSA Enterprise Manager の送信者のユーザ識別名の特定](#)」(P.22-45) を参照してください。

LDAP と AsyncOS との連携の仕組み

LDAP ディレクトリと Cisco アプライアンスとを連携させると、受信者受け入れ、メッセージルーティング、およびヘッダーマスカレードに LDAP ディレクトリ サーバを使用できます。LDAP グループクエリーをメッセージフィルタとともに使用すると、メッセージが Cisco アプライアンスで受信されたときの取り扱いのルールを作成できます。

図 22-1 に、Cisco アプライアンスと LDAP がどのように連携するかを示します。

図 22-1 LDAP の設定



1. 送信 MTA からパブリック リスナー「A」にメッセージが SMTP 経由で送信されます。
2. Cisco アプライアンスは、LDAP サーバに対してクエリーを実行します。この LDAP サーバは [システム管理 (System Administration)] > [LDAP] ページ (またはグローバル ldapconfig コマンド) で定義されます。
3. データが LDAP ディレクトリから受信されます。リスナーで使用するように [システム管理 (System Administration)] > [LDAP] ページ (または ldapconfig コマンド) で定義されたクエリーに応じて、次の処理が実行されます。

- メッセージを新しい受信者アドレスにルーティングするか、ドロップまたはバウンスする
- メッセージを新しい受信者のメールホストにルーティングする
- メッセージヘッダー From:、To:、CC: をクエリーに基づいて書き換える
- メッセージフィルタ ルール rcpt-to-group または mail-from-group で定義された、それ以降のアクション（グループクエリーと組み合わせて使用）。



(注) Cisco アプライアンスからは、複数の LDAP サーバに接続できます。複数の LDAP サーバを使用して、ロード バランシングやフェールオーバーを行うように LDAP プロファイルを設定できます。複数の LDAP サーバと連携させる方法の詳細については、「[AsyncOS を複数の LDAP サーバと連携させるための設定](#)」(P.22-46) を参照してください。

Cisco IronPort アプライアンスを LDAP サーバと連携させるための設定

受け入れ、ルーティング、エイリアシング、およびマスカレードのために Cisco アプライアンスを LDAP ディレクトリと連携させるには、以下の手順に従って AsyncOS アプライアンスを設定する必要があります。

手順

ステップ 1 LDAP サーバ プロファイルを設定します。 サーバ プロファイルの内容は、AsyncOS から LDAP サーバに接続するための、次のような情報です。

- クエリー送信先となるサーバの名前とポート
- ベース DN
- サーバへのバインドのための認証に必要な情報

サーバ プロファイルの設定方法の詳細については、「[LDAP サーバに関する情報を保存する LDAP サーバ プロファイルの作成](#)」(P.22-5) を参照してください。

LDAP サーバ プロファイルを設定するときに、AsyncOS からの接続先となる LDAP サーバを 1 つまたは複数設定できます。

AsyncOS から複数のサーバに接続するように設定する方法については、「[AsyncOS を複数の LDAP サーバと連携させるための設定](#)」(P.22-46) を参照してください。

ステップ 2 LDAP クエリーを設定します。 LDAP クエリーは、LDAP サーバ プロファイルで設定します。ここで設定するクエリーは、実際に使用する LDAP の実装とスキーマに合わせて調整してください。

作成できる LDAP クエリーのタイプについては、「[LDAP クエリーの概要](#)」(P.22-2) を参照してください。

クエリーの記述方法については、「[LDAP クエリーに関する作業](#)」(P.22-12) を参照してください。

ステップ 3 LDAP サーバ プロファイルをパブリック リスナーまたはプライベート リスナーに対してイネーブルにします。 LDAP サーバ プロファイルをリスナーに対してイネーブルにすると、そのリスナーによって、メッセージの受け入れ、ルーティング、または送信のときに LDAP クエリーが実行されるようになります。

詳細については、「[特定のリスナーで実行するための LDAP クエリーのイネーブル化](#)」(P.22-7) を参照してください。



(注)

グループ クエリーを設定するときは、AsyncOS と LDAP サーバとを連携させるためにさらに設定作業が必要です。グループ クエリーの設定方法については、「受信者がグループ メンバーであるかどうかを指定するグループ LDAP クエリーの使用」(P.22-23) を参照してください。エンドユーザ認証またはスパム通知統合のクエリーを設定するときは、Cisco スпам隔離機能への LDAP エンドユーザアクセスをイネーブルにする必要があります。Cisco スпам隔離の詳細については、『Cisco IronPort AsyncOS for Email Daily Management Guide』の「Configuring the Cisco Spam Quarantines Feature」を参照してください。

LDAP サーバに関する情報を保存する LDAP サーバ プロファイルの作成

LDAP ディレクトリを使用するように AsyncOS を設定するには、LDAP サーバ プロファイルを作成します。この中に、LDAP サーバに関する情報が格納されます。

手順

- ステップ 1** [システム管理 (System Administration)] > [LDAP] ページの [LDAP サーバプロファイルを追加 (Add LDAP Server Profile)] をクリックします。
- ステップ 2** サーバ プロファイルの名前を入力します。
- ステップ 3** LDAP サーバのホスト名を入力します。

複数のホスト名を入力すると、LDAP サーバのフェールオーバーやロード バランシングができるようになります。複数のエントリを指定する場合は、カンマで区切ります。詳細については、「AsyncOS を複数の LDAP サーバと連携させるための設定」(P.22-46) を参照してください。
- ステップ 4** 認証方法を選択します。匿名認証を使用することも、ユーザ名とパスワードを指定することもできます。
- ステップ 5** LDAP サーバのタイプを、[Active Directory]、[OpenLDAP]、[不明またはそれ以外 (Unknown or Other)] から選択します。
- ステップ 6** ポート番号を入力します。

デフォルト ポートは 3268 です。これは Active Directory のデフォルト ポートであり、複数サーバ環境のグローバル カタログへのアクセスが可能になります。
- ステップ 7** LDAP サーバのベース DN (識別名) を入力します。

ユーザ名とパスワードを使用して認証する場合は、パスワードが格納されているエントリへの完全 DN がユーザ名に含まれている必要があります。たとえば、マーケティング グループに属しているユーザの電子メール アドレスが joe@example.com であるとします。このユーザのエントリは、次のようになります。

```
uid=joe, ou=marketing, dc=example dc=com
```
- ステップ 8** LDAP サーバとの通信に SSL を使用するかどうかを選択します。
- ステップ 9** [詳細 (Advanced)] で、キャッシュの存続可能時間を入力します。この値は、キャッシュを保持する時間の長さです。
- ステップ 10** 保持するキャッシュ エントリの最大数を入力します。
- ステップ 11** 同時接続の最大数を入力します。

ロード バランシングを行うように LDAP サーバ プロファイルを設定した場合は、指定された LDAP サーバにこれらの接続が振り分けられます。たとえば、同時接続数を 10 と設定し、3 台のサーバを使用して接続のロード バランシングを行う場合は、AsyncOS によってサーバへの接続が 10 ずつ作成され、接続の総数は 30 となります。



(注) 同時接続の最大数には、LDAP クエリーに使用される LDAP 接続も含まれます。ただし、Cisco スпам隔離機能に対して LDAP 認証を使用する場合は、これよりも多くの接続が開かれることがあります。

ステップ 12 サーバへの接続をテストするために、[テスト サーバ (Test Server(s))] ボタンをクリックします。複数の LDAP サーバを指定した場合は、すべてのサーバのテストが実行されます。テストの結果が [接続ステータス (Connection Status)] フィールドに表示されます。詳細については、「LDAP サーバのテスト」(P.22-7) を参照してください。

ステップ 13 クエリーを作成します。該当するチェックボックスをオンにして、フィールドに入力します。選択できるのは、[承認 (Accept)]、[ルーティング (Routing)]、[マスカレード (Masquerade)]、[グループ (Group)]、[SMTP 認証 (SMTP Authentication)]、[外部認証 (External Authentication)]、[スパム隔離エンドユーザ認証 (Spam Quarantine End-User Authentication)]、[スパム隔離エイリアス統合 (Spam Quarantine Alias Consolidation)] です。



(注) メッセージを受信または送信するときに Cisco アプライアンスが LDAP クエリーを実行できるようにするには、該当するリスナーに対して LDAP クエリーをイネーブルにする必要があります。詳細については、「特定のリスナーで実行するための LDAP クエリーのイネーブル化」(P.22-7) を参照してください。

ステップ 14 クエリーをテストするために、[クエリのテスト (Test Query)] ボタンをクリックします。

テスト パラメータを入力して [テストの実行 (Run Test)] をクリックします。テストの結果が [接続ステータス (Connection Status)] フィールドに表示されます。クエリーの定義や属性に変更を加えた場合は、[更新 (Update)] をクリックします。詳細については、「LDAP クエリーのテスト」(P.22-17) を参照してください。



(注) 空パスワードでのバインドを許可するように LDAP サーバが設定されている場合は、パスワード フィールドが空でもクエリーのテストは合格となります。

ステップ 15 変更内容を送信し、確定します。



(注) サーバ設定の数に制限はありませんが、設定できるクエリーは、サーバ 1 台につき受信者受け入れ 1 つ、ルーティング 1 つ、マスカレード 1 つ、グループ クエリー 1 つのみです。

LDAP サーバのテスト

[LDAP サーバ プロファイルを追加/編集 (Add/Edit LDAP Server Profile)] ページの [テスト サーバ (Test Server(s))] ボタン (または CLI の `ldapconfig` コマンドの `test` サブコマンド) を使用して、LDAP サーバへの接続をテストします。サーバ ポートへの接続に成功したか失敗したかを示すメッセージが表示されます。複数の LDAP サーバが設定されている場合は、各サーバのテストが実行されて、結果が個別に表示されます。

特定のリスナーで実行するための LDAP クエリーのイネーブル化

メッセージを受信または送信するときに Cisco アプライアンスが LDAP クエリーを実行できるようにするには、該当するリスナーに対して LDAP クエリーをイネーブルにする必要があります。

LDAP クエリーのグローバル設定

LDAP グローバル設定では、すべての LDAP トラフィックをアプライアンスがどのように扱うかを定義します。

手順

- ステップ 1** [システム管理 (System Administration)] > [LDAP] ページの [設定を編集 (Edit Settings)] をクリックします。
- ステップ 2** LDAP トラフィックに使用する IP インターフェイスを選択します。インターフェイスの 1 つが自動的にデフォルトとして選択されます。
- ステップ 3** LDAP インターフェイスに使用する TLS 証明書を選択します ([ネットワーク (Network)] > [証明書 (Certificates)] ページまたは CLI の `certconfig` コマンドを使用して追加された TLS 証明書。「他の MTA との暗号化通信の概要」(P.20-1) を参照してください)。
- ステップ 4** 変更内容を送信し、確定します。

LDAP サーバ プロファイル作成の例

次に示す例では、[システム管理 (System Administration)] > [LDAP] ページを使用してアプライアンスのバインド先となる LDAP サーバを定義し、受信者受け入れ、ルーティング、およびマスカレードのクエリーを設定します。



(注)

LDAP 接続試行のタイムアウトは 60 秒です。この時間には、DNS ルックアップと接続そのものに加えて、アプライアンス自体の認証バインド (該当する場合) も含まれます。初回の失敗後は、同じサーバ内の別のホストに対する試行がただちに行われます (2 つ以上のホストをカンマ区切りリストで指定した場合)。サーバ内にホストが 1 つしかない場合は、そのホストへの接続が繰り返し試行されます。

図 22-2 LDAP サーバプロファイルの設定 (1/2)

The screenshot shows the 'LDAP Server Settings' configuration page. The 'Server Attributes' section is expanded, showing the following fields and values:

- LDAP Server Profile Name: PublicLDAP
- Host Name(s): myldapserver.example.com
- Authentication Method: Use Password (selected)
- Username: cn=anonymous
- Password: *****
- Server Type: Active Directory
- Port: 3268
- Base DN: dc=example, dc=com
- Connection Protocol: Use SSL (unchecked)
- Advanced section:
 - Cache TTL (time-to-live): 900 Seconds
 - Maximum Retained Cache Entries: 10000
 - Maximum number of simultaneous connections for each host: 10
 - Multiple host options: Load-balance connections among all hosts listed (selected)

最初に、「PublicLDAP」というニックネームを myldapserver.example.com LDAP サーバに与えます。接続数は 10 (デフォルト値) に設定されており、複数 LDAP サーバ (ホスト) のロード バランス オプションはデフォルトのままとなっています。ここで複数のホストの名前を、カンマ区切りのリストとして指定できます。クエリーの送信先は、ポート 3268 (デフォルト値) です。SSL は、このホストの接続プロトコルとしてはイネーブルになっていません。example.com のベース DN が定義されています (dc=example, dc=com)。キャッシュの存続可能時間は 900 秒、キャッシュ エントリの最大数は 10000 に設定されています。認証方法は、「パスワードを使用」に設定されています。

受信者受け入れ、メール ルーティング、およびマスカレードのクエリーが定義されています。クエリー名では、大文字と小文字が区別されます。正しい結果が返されるようにするには、正確に一致している必要があります。

図 22-3 LDAP サーバプロファイルの設定 (2/2)

The screenshot shows the 'LDAP Server Settings' configuration page, focusing on the query sections:

- Accept Query:** Name: PublicLDAP.accept, Query String: {proxyAddresses=sntp:(a)}
- Routing Query:** Name: PublicLDAP.routing, Query String: {mailLocalAddress=(a)}
- Masquerade Query:** Name: PublicLDAP.masquerade, Query String: {mailRoutingAddress=(a)}

パブリック リスナー上の LDAP クエリーのイネーブル化

この例では、パブリック リスナー「InboundMail」で受信者受け入れに対して LDAP クエリーを使用するように更新します。さらに、受信者受け入れの判定を SMTP カンバセーション中に行うように設定します (詳細については、「[受信者検証で受け入れクエリーを使用する](#)」(P.22-19) を参照してください)。

図 22-4 リスナーでの受け入れとルーティングのクエリーのイネーブル化

LDAP Queries: Accept

Accept Query: exampleTest.accept

Work Queue

Non-Matching Recipients: Bounce

SMTP Conversation

If the LDAP server is unreachable:

Allow Mail in

Drop Connection, return error code:

Code: 451

Text: Temporary recipient validation er

When the Directory Harvest Attack Prevention threshold (maximum invalid recipients per hour) is reached:

Code: 550

Text: Too many invalid recipients

Drop Connection if the Directory Harvest Attack Prevention threshold (maximum invalid recipients per hour) is reached within an SMTP conversation.

Routing

Masquerade

Group

プライベート リスナーでの LDAP クエリーのイネーブル化

この例では、プライベートリスナー「OutboundMail」で LDAP クエリーを使用してマスカレードを行うように更新します。マスカレード対象のフィールドは、From、To、CC、Reply-To などがあります。

図 22-5 リスナーでのマスカレード クエリーのイネーブル化

LDAP Queries: Masquerade

Masquerade Query: exampleTest.masquerade

Addresses to Masquerade:

Envelope Sender

From (Header)

To (Header)

CC (Header)

Reply-To (Header)

Group

Microsoft Exchange 5.5 に対する拡張サポート

AsyncOS には、Microsoft Exchange 5.5 をサポートするための設定オプションがあります。これよりも新しいバージョンの Microsoft Exchange を使用する場合は、このオプションをイネーブルにする必要はありません。LDAP サーバを設定するときに、Microsoft Exchange 5.5 サポートをイネーブルにするかどうかを選択できます。選択するには、CLI を使用する必要があります。次に示すように、`ldapconfig -> edit -> server -> compatibility` サブコマンドを実行して、質問に「y」と答えます。

```
mail3.example.com> ldapconfig
```

Current LDAP server configurations:

1. PublicLDAP: (ldapexample.com:389)

Choose the operation you want to perform:

- NEW - Create a new server configuration.
- EDIT - Modify a server configuration.
- DELETE - Remove a server configuration.

[> **edit**

Enter the name or number of the server configuration you wish to edit.

[> **1**

Name: PublicLDAP

Hostname: ldapexample.com Port 389

Authentication Type: anonymous

Base: dc=ldapexample,dc=com

Choose the operation you want to perform:

- SERVER - Change the server for the query.
- LDAPACCEPT - Configure whether a recipient address should be accepted or bounced/dropped.
- LDAPROUTING - Configure message routing.
- MASQUERADE - Configure domain masquerading.
- LDAPGROUP - Configure whether a sender or recipient is in a specified group.
- SMTPAUTH - Configure SMTP authentication.

[> **server**

Name: PublicLDAP

Hostname: ldapexample.com Port 389


```
Authentication Type: anonymous
```

```
Base: dc=ldapexample,dc=com
```

```
Microsoft Exchange 5.5 Compatibility Mode: Disabled
```

```
Choose the operation you want to perform:
```

- NAME - Change the name of this configuration.
- HOSTNAME - Change the hostname used for this query.
- PORT - Configure the port.
- AUTHTYPE - Choose the authentication type.
- BASE - Configure the query base.
- COMPATIBILITY - Set LDAP protocol compatibility options.

```
[> compatibility
```

```
Would you like to enable Microsoft Exchange 5.5 LDAP compatibility mode? (This is not recommended for versions of Microsoft Exchange later than 5.5, or other LDAP servers.)  
[N]> y
```

```
Do you want to configure advanced LDAP compatibility settings? (Typically not required)  
[N]>
```

```
Name: PublicLDAP
```

```
Hostname: ldapexample.com Port 389
```

```
Authentication Type: anonymous
```

```
Base: dc=ldapexample,dc=com
```

```
Microsoft Exchange 5.5 Compatibility Mode: Enabled (attribute "objectClass")
```

```
Choose the operation you want to perform:
```

- NAME - Change the name of this configuration.
- HOSTNAME - Change the hostname used for this query.
- PORT - Configure the port.

- AUTHTYPE - Choose the authentication type.
 - BASE - Configure the query base.
 - COMPATIBILITY - Set LDAP protocol compatibility options.
- []>

LDAP クエリーに関する作業

LDAP サーバプロファイル内に、実行したい LDAP クエリーのタイプごとに 1 つのエントリを作成します。LDAP クエリーを作成するときは、実際に使用する LDAP サーバのクエリー構文で入力する必要があります。作成するクエリーは、実際に使用する LDAP ディレクトリ サービスの実装に合わせて調整が必要であることに注意してください。特に、組織固有のニーズを満たすように新しいオブジェクトクラスや属性がディレクトリに追加されている場合です。

LDAP クエリーのタイプ

- **受け入れクエリー**。詳細については、「[受信者検証で受け入れクエリーを使用する](#)」(P.22-19) を参照してください。
- **ルーティングクエリー**。詳細については、「[複数ターゲットアドレスへのメール送信にルーティングクエリーを使用する](#)」(P.22-20) を参照してください。
- **証明書認証クエリー**。詳細については、「[クライアント証明書の有効性の確認](#)」(P.23-51) を参照してください。
- **マスカレードクエリー**。詳細については、「[エンベロープ送信者を書き換えるためのマスカレードクエリーの使用](#)」(P.22-21) を参照してください。
- **グループクエリー**。詳細については、「[受信者がグループメンバーであるかどうかを指定するグループ LDAP クエリーの使用](#)」(P.22-23) を参照してください。
- **ドメインベースクエリー**。詳細については、「[特定のドメインヘルディングするためのドメインベースクエリーの使用](#)」(P.22-26) を参照してください。
- **チェーンクエリー**。詳細については、「[一連の LDAP クエリーを実行するためのチェーンクエリーの使用](#)」(P.22-28) を参照してください。

次の目的のためにクエリーを設定することもできます。

- **ディレクトリ ハーベスト防止**。詳細については、「[LDAP クエリーの概要](#)」(P.22-2) を参照してください。
- **SMTP 認証**。詳細については、「[SMTP 認証を行うための AsyncOS の設定](#)」(P.22-32) を参照してください。
- **外部認証**。詳細については、「[ユーザの外部 LDAP 認証の設定](#)」(P.22-40) を参照してください。
- **スパム隔離へのエンドユーザ認証のクエリー**。詳細については、「[Cisco IronPort スпам隔離内のエンドユーザ認証](#)」(P.22-43) を参照してください。
- **スパム隔離のエイリアス統合のクエリー**。詳細については、「[スパム隔離のエイリアス統合のクエリー](#)」(P.22-44) を参照してください。

指定した検索クエリーは、システム上で設定済みのすべてのリスナーに使用できます。

ベース識別名 (DN)

ディレクトリのルート レベルを「ベース」と呼びます。ベースの名前は DN (distinguishing name) です。Active Directory (および RFC 2247 に基づく標準) のベース DN のフォーマットでは、DNS ドメインがドメイン コンポーネント (dc=) に変換されます。たとえば、example.com のベース DN は「dc=example, dc=com」です。DNS 名の各部分が順番に表現されることに注意してください。これには、実際の LDAP 設定が反映されることも、されないこともあります。

実際に使用するディレクトリに複数のドメインが含まれている場合は、クエリーの対象のベースを 1 つだけ入力するのは不都合であることもあります。そのような場合は、LDAP サーバ設定を指定するときに、ベースを「NONE」に設定します。ただし、このように設定すると検索の効率が低下します。

LDAP クエリーの構文

LDAP パス内でスペースを使用できます。引用符で囲む必要はありません。CN と DC の構文では、大文字と小文字は区別されません。

```
Cn=First Last,oU=user,dc=domain,DC=COM
```

クエリーに入力する変数名では大文字と小文字が区別されるので、正しく動作させるには、使用する LDAP 実装に一致させる必要があります。たとえば、プロンプトで `mailLocalAddress` と入力したときに実行されるクエリーは、`maillocaladdress` と入力したときとは異なります。

トークン

次のトークンを LDAP クエリー内で使用できます。

- {a} ユーザ名 @ ドメイン名
- {d} ドメイン名
- {dn} 識別名
- {g} グループ名
- {u} ユーザ名
- {f} MAIL FROM: アドレス



(注) {f} トークンを使用できるのは、受け入れクエリーのみです。

たとえば、メールを受け入れるための Active Directory LDAP サーバに対するクエリーは、次のようになります。

```
((mail={a})(proxyAddresses=smtp:{a}))
```



(注) 作成したクエリーは、[LDAP] ページの [テスト (Test)] 機能 (または `ldapconfig` コマンドの `test` サブコマンド) を使用してテストすることを強く推奨します。期待したとおりの結果が返されることを確認してから、リスナーに対して LDAP 機能をイネーブルにしてください。詳細については、「LDAP クエリーのテスト」(P.22-17) を参照してください。

セキュア LDAP (SSL)

AsyncOS と LDAP サーバとの通信に SSL を使用するように設定できます。SSL を使用するように LDAP サーバ プロファイルを設定した場合の動作は次のようになります。

- AsyncOS は、CLI の `certconfig` で設定された LDAPS 証明書を使用します（「GUI を使用した自己署名証明書の作成」(P.20-3) を参照）。

LDAP サーバによっては、LDAPS 証明書の使用をサポートするように設定する作業が必要になります。

- 設定済みの LDAPS 証明書がない場合は、デモ証明書が使用されます。

ルーティング クエリー

LDAP ルーティング クエリーの再帰の制限はありません。ルーティングは完全にデータ ドリブンで行われます。ただし、AsyncOS には、ルーティングの永久ループを防止するために循環参照の有無を調べる機能があります。

LDAP サーバへの匿名のバインドをクライアントに許可する

組織によっては、匿名クエリーを許可するように LDAP ディレクトリ サーバを設定することが必要になります。（匿名クエリーを許可すると、クライアントが匿名でサーバにバインドしてクエリーを実行できるようになります）。匿名クエリーを許可するように Active Directory を設定する具体的な手順については、Microsoft サポート技術情報 320528 を参照してください。URL は次のとおりです。

<http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B320528>

または、認証とクエリー実行専用のユーザを 1 つ用意します。このようにすれば、任意のクライアントから匿名クエリーを受け付けるように LDAP ディレクトリ サーバを開放する必要はありません。

ここでは、次の手順について説明します。

- 「匿名」認証を許可するように Microsoft Exchange 2000 サーバをセットアップする方法。
- 「匿名バインド」を許可するように Microsoft Exchange 2000 サーバをセットアップする方法。
- Cisco AsyncOS が LDAP データを Microsoft Exchange 2000 サーバから「匿名バインド」と「匿名」認証の両方を使用して取得するようにセットアップする方法。

ユーザ電子メール アドレスを問い合わせるという目的で「匿名」または「匿名バインド」認証を許可するには、Microsoft Exchange 2000 サーバに対して特定のアクセス許可を設定する必要があります。このような設定が非常に役立つのは、SMTP ゲートウェイに対する着信メール メッセージの有効性を検証するために LDAP クエリーを使用する場合です。

匿名認証のセットアップ

ここで説明するセットアップ手順を実行すると、Microsoft Windows Active Directory 内の Active Directory サーバおよび Exchange 2000 サーバに対する未認証のクエリーで特定のデータを使用できるようになります。Active Directory への「匿名バインド」を許可する手順については、「Active Directory の匿名バインドのセットアップ」(P.22-15) を参照してください。

手順

ステップ 1 どのような Active Directory アクセス許可が必要であることを確認する。

ADSI Edit スナップインまたは LDP ユーティリティを使用して、以下の Active Directory オブジェクトの属性に対するアクセス許可を修正する必要があります。

- クエリーの対象であるドメインの、ドメイン名前付けコンテキストのルート。

- 電子メール情報クエリーの対象であるユーザが属している OU および CN オブジェクトすべて。

次の表に、必要なコンテナすべてに適用されている必要のあるアクセス許可を示します。

ユーザオブジェクト	権限	継承	アクセス許可のタイプ
全員 (Everyone)	内容の一覧表示	コンテナ オブジェクト	オブジェクト
全員 (Everyone)	内容の一覧表示	組織単位オブジェクト	オブジェクト
全員 (Everyone)	パブリック インフォメーション読み取り	ユーザ オブジェクト	プロパティ
全員 (Everyone)	電話とメールのオプションの読み取り	ユーザ オブジェクト	プロパティ

ステップ 2 Active Directory のアクセス許可を設定する。

- Windows 2000 Support Tools から ADSIEdit を開きます。
- [ドメイン ネーミング コンテキスト (Domain Naming Context)] フォルダを見つけます。このフォルダに、ドメインの LDAP パスがあります。
- [ドメイン ネーミング コンテキスト (Domain Naming Context)] フォルダを右クリックして [プロパティ (Properties)] をクリックします。
- [セキュリティ (Security)] をクリックします。
- [詳細 (Advanced)] をクリックします。
- [追加 (Add)] をクリックします。
- ユーザ オブジェクト [全員 (Everyone)] をクリックして [OK] をクリックします。
- [権限の種類 (Permission Type)] タブをクリックします。
- [適用 (Apply onto)] ボックスの [継承 (Inheritance)] をクリックします。
- [権限 (Permission)] アクセス許可の [許可 (Allow)] チェックボックスをオンにします。

ステップ 3 Cisco メッセージング ゲートウェイを設定する

Command Line Interface (CLI; コマンドライン インターフェイス) の `ldapconfig` を使用して、LDAP サーバエントリを作成します。次の情報を指定してください。

- Active Directory または Exchange サーバのホスト名
- ポート 3268
- ドメインのルート名前付けコンテキストに一致するベース DN
- 認証タイプ: 匿名

Active Directory の匿名バインドのセットアップ

ここで説明するセットアップ手順を実行すると、Microsoft Windows Active Directory 内の Active Directory サーバおよび Exchange 2000 サーバに対する匿名バインドクエリーで特定のデータを使用できるようになります。Active Directory サーバの匿名バインドを使用するときは、ユーザ名 `anonymous` とブランクのパスワードが送信されます。



(注) 匿名バインドを試行するときに何らかのパスワードが Active Directory サーバに送信されると、認証に失敗することがあります。

手順

ステップ 1 どのような Active Directory アクセス許可が必要であることを確認する。

ADSI Edit スナップインまたは LDP ユーティリティを使用して、以下の Active Directory オブジェクトの属性に対するアクセス許可を修正する必要があります。

- クエリーの対象であるドメインの、ドメイン名前付けコンテキストのルート。
- 電子メール情報クエリーの対象であるユーザが属している OU および CN オブジェクトすべて。

次の表に、必要なコンテナすべてに適用されている必要のあるアクセス許可を示します。

ユーザ オブジェクト	権限	継承	アクセス許可のタイプ
ANONYMOUS LOGON	内容の一覧表示	コンテナ オブジェクト	オブジェクト
ANONYMOUS LOGON	内容の一覧表示	組織単位オブジェクト	オブジェクト
ANONYMOUS LOGON	パブリック インフォメーション読み取り	ユーザ オブジェクト	プロパティ
ANONYMOUS LOGON	電話とメールのオプションの読み取り	ユーザ オブジェクト	プロパティ

ステップ 2 Active Directory のアクセス許可を設定する。

- Windows 2000 Support Tools から ADSIEdit を開きます。
- [ドメイン ネーミング コンテキスト (Domain Naming Context)] フォルダを見つけます。このフォルダに、ドメインの LDAP パスがあります。
- [ドメイン ネーミング コンテキスト (Domain Naming Context)] フォルダを右クリックして [プロパティ (Properties)] をクリックします。
- [セキュリティ (Security)] をクリックします。
- [詳細 (Advanced)] をクリックします。
- [追加 (Add)] をクリックします。
- ユーザ オブジェクト [匿名ログオン (ANONYMOUS LOGON)] をクリックして [OK] をクリックします。
- [権限の種類 (Permission Type)] タブをクリックします。
- [適用 (Apply onto)] ボックスの [継承 (Inheritance)] をクリックします。
- [権限 (Permission)] アクセス許可の [許可 (Allow)] チェックボックスをオンにします。

ステップ 3 Cisco メッセージング ゲートウェイを設定する。

[システム管理 (System Administration)] > [LDAP] ページ (または CLI の ldapconfig) を使用して LDAP サーバエントリを作成します。次の情報を指定してください。

- Active Directory または Exchange サーバのホスト名
- ポート 3268
- ドメインのルート名前付けコンテキストに一致するベース DN
- 認証タイプ: パスワード ベース (cn=anonymous をユーザとして使用し、パスワードは空白)

Active Directory の実装に関する注意

- Active Directory サーバが LDAP 接続を受け付けるポートは、3268 と 389 です。グローバル カタログへのアクセス用のデフォルト ポートは 3268 です。
- Active Directory サーバが LDAPS 接続を受け付けるポートは、636 と 3269 です。Microsoft 製品で LDAPS がサポートされるのは、Windows Server 2003 以上です。
- Cisco アプライアンスは、グローバル カタログでもあるドメイン コントローラに接続してください。これは、複数のベースに対するクエリーを同じサーバを使用して実行できるようにするためです。
- クエリーを正常に実行するには、Active Directory の中で、ディレクトリ オブジェクトに対する読み取り許可をグループ Everyone に付与する必要があります。これには、ドメイン名前付けコンテキストのルートも含まれます。
- 一般的に、多くの Active Directory 実装では、mail 属性エントリに一致する値の「ProxyAddresses」属性エントリが存在します。
- Microsoft Exchange 環境が同じインフラストラクチャ内に複数あり、互いを認識している場合は、Exchange 環境の間でメールをルーティングするときに、送信元 MTA に戻る方向のルートは通常は必要ありません。

LDAP クエリーのテスト

[LDAP サーバ プロファイルを追加/編集 (Add/Edit LDAP Server Profile)] ページの [クエリーのテスト (Test Query)] ボタン (または CLI の test サブコマンド) を使用して、クエリー タイプごとに、設定した LDAP サーバに対するクエリーをテストします。結果が表示されるだけでなく、クエリー接続テストの各ステージの詳細も表示されます。テストは、クエリー タイプのそれぞれに対して行うことができます。

ldaptest コマンドを、次の例のようにバッチ コマンドとして使用できます。

```
ldaptest LDAP.ldapaccept foo@ironport.com
```

LDAP サーバ属性の Host Name フィールドに複数のホストを入力した場合は、Cisco アプライアンスは各 LDAP サーバに対してクエリーのテストを行います。

表 22-1 LDAP クエリーのテスト

クエリーのタイプ	受信者が一致する場合 (PASS)	受信者が一致しない場合 (FAIL)
受信者受け入れ ([承認 (Accept)]、 <code>ldapaccept</code>)	メッセージを受け入れます。	受信者が無効：カンパセーションまたは遅延バウンスまたはメッセージをドロップ (リスナー設定による)。DHAP：ドロップ。
ルーティング ([ルーティング (Routing)]、 <code>ldaprouting</code>)	クエリーの設定に基づいてルーティングします。	このメッセージの処理を続行します。
マスカレード ([マスカレード (Masquerade)]、 <code>masquerade</code>)	クエリー内で定義された変数マッピングに従ってヘッダーを変更します。	このメッセージの処理を続行します。
グループメンバーシップ ([グループ (Group)]、 <code>ldapgroup</code>)	メッセージフィルタ ルールに対して「true」を返します。	メッセージフィルタ ルールに対して「false」を返します。
SMTP Auth ([SMTP 認証 (SMTP Authentication)]、 <code>smtppauth</code>)	LDAP サーバから返されたパスワードを使用して認証を行います。つまり、SMTP 認証が行われます。	一致するパスワードを見つけることはできません。SMTP 認証の試行は失敗します。
外部認証 (<code>externalauth</code>)	バインド、ユーザ レコード、およびユーザのグループメンバーシップに対して個別に「match positive」が返されます。	バインド、ユーザ レコード、およびユーザのグループメンバーシップに対して個別に「match negative」が返されます。
スパム隔離へのエンドユーザ認証 (<code>isqauth</code>)	エンドユーザ アカウントに対して「match positive」が返されます。	一致するパスワードを見つけることはできません。エンドユーザ認証の試行は失敗します。
スパム隔離のエイリアス統合 (<code>isqalias</code>)	統合されたスパム通知の送信先である電子メール アドレスが返されます。	スパム通知の統合はできません。



(注)

クエリーに入力する変数名では大文字と小文字が区別されるので、正しく動作させるには、使用する LDAP 実装に一致させる必要があります。たとえば、プロンプトで `mailLocalAddress` と入力したときに実行されるクエリーは、`maillocaladdress` と入力したときとは異なります。作成したすべてのクエリーについて、`ldapconfig` コマンドの `test` サブコマンドを使用してテストし、正しい結果が返されることを確認することを強く推奨します。

LDAP サーバへの接続のトラブルシューティング

LDAP サーバがアプライアンスから到達不能である場合は、次のエラーのいずれかが表示されます。

- Error: LDAP authentication failed: <LDAP Error "invalidCredentials" [0x31]>
- Error: Server unreachable: unable to connect
- Error: Server unreachable: DNS lookup failure

サーバが到達不能になる原因としては、サーバ設定で入力されたポートの誤りや、ファイアウォールでポートが開いていないことが考えられます。LDAP サーバの通信には一般に、ポート 3268 または 389 が使用されます。Active Directory では、複数サーバ環境でのグローバル カタログへのアクセスにはポート 3268 が使用されます（詳細については『Cisco IronPort AsyncOS for Email Configuration Guide』の「Firewall Information」を参照してください）。AsyncOS 4.0 で、LDAP サーバと SSL 経由で通信する（通常はポート 636 を使用）機能が追加されました。詳細については、「セキュア LDAP (SSL)」(P.22-13) を参照してください。

サーバが到達不能になる原因としてはその他に、入力されたホスト名が解決不可能であることが考えられます。

[LDAP サーバ プロファイルを追加/編集 (Add/Edit LDAP Server Profile)] ページの [テスト サーバ (Test Server(s))] (または CLI の ldapconfig コマンドの test サブコマンド) を使用すると、LDAP サーバへの接続をテストできます。詳細については、「LDAP サーバのテスト」(P.22-7) を参照してください。

LDAP サーバが到達不能である場合：

- LDAP 受け入れまたはマスカレードまたはルーティングがワーク キューに対してイネーブルになっている場合は、メールはワーク キュー内に留まります。
- LDAP 受け入れはイネーブルになっておらず、他のクエリー（グローバル ポリシー チェックなど）がフィルタ内で使用されている場合は、そのフィルタの評価結果が false になります。

受信者検証で受け入れクエリーを使用する

既存の LDAP インフラストラクチャを使用して、着信メッセージ（パブリック リスナーでの）の受信者メールアドレスの扱い方を定義できます。ディレクトリ内のユーザ データに対する変更は、次回 Cisco アプライアンスがディレクトリ サーバに対してクエリーを実行したときに更新されます。キャッシュのサイズと、Cisco が取得したデータを保持する時間の長さは設定可能です。



(注) 特別な受信者（たとえば administrator@example.com）に対して LDAP 受け入れクエリーをバイパスすることもできます。このように設定するには、受信者アクセス テーブル (RAT) を使用します。この設定の方法については、『Cisco IronPort AsyncOS for Email Configuration Guide』の「Configuring the Gateway to Receive Email」を参照してください。

受け入れクエリーの例

表 22-2 に、受け入れクエリーの例を示します。

表 22-2 一般的な LDAP 実装での LDAP クエリー文字列の例：受け入れ

クエリーの対象	受信者検証
OpenLDAP	(mailLocalAddress={a}) (mail={a}) (mailAlternateAddress={a})
Microsoft Active Directory アドレス帳 Microsoft Exchange	((mail={a})(proxyAddresses=smtp:{a}))

表 22-2 一般的な LDAP 実装での LDAP クエリー文字列の例：受け入れ（続き）

クエリーの対象	受信者検証
Sun ONE Directory Server	(mail={a}) (mailAlternateAddress={a}) (mailEquivalentAddress={a}) (mailForwardingAddress={a}) (mailRoutingAddress={a})
Lotus Notes Lotus Domino	(((mail={a})(uid={u}))(cn={u})) ((ShortName={u})(InternetAddress={a})(FullName={u}))

ユーザ名（左側）の検証を行うこともできます。このことが役に立つのは、ディレクトリに格納されていないドメインのメールも受け入れるようにしたい場合です。受け入れクエリーを (uid={u}) に設定してください。

Lotus Notes の場合の受け入れクエリーの設定

LDAPACCEPT と Lotus Notes とを組み合わせる場合は、注意が必要です。Notes LDAP に格納されているユーザの属性が次のように設定されているとします。

```
mail=juser@example.com
```

```
cn=Joe User
```

```
uid=juser
```

```
cn=123456
```

```
location=New Jersey
```

Lotus はこのユーザへの電子メールを、指定されたアドレス以外の形式（たとえば Joe_User@example.com）であっても、LDAP ディレクトリに存在しないにもかかわらず受け入れます。したがって、AsyncOS は、このユーザの有効なユーザ メール アドレスをすべて見つけることはできません。

この解決策の 1 つは、他の形式のアドレスのパブリッシュを試みるというものです。詳細については、Lotus Notes 管理者に問い合わせてください。

複数ターゲットアドレスへのメール送信にルーティングクエリーを使用する

AsyncOS では、エイリアス拡張（複数ターゲットアドレスへの LDAP ルーティング）がサポートされます。AsyncOS によって、元のメールメッセージはエイリアス ターゲットごとに別の新しいメッセージで置き換えられます（たとえば、recipient@yoursite.com へのメッセージは、newrecipient1@hotmail.com や recipient2@internal.yourcompany.com などへの、それぞれ独立したメッセージで置き換えられます）。ルーティングクエリーは、他の電子メール処理システムではエイリアシングクエリーと呼ばれることもあります。

ルーティング クエリーの例

表 22-3 一般的な LDAP 実装での LDAP クエリー文字列の例：ルーティング

クエリーの対象	別のメールホストへのルーティング
OpenLDAP	(mailLocalAddress={a})
Microsoft Active Directory アドレス帳 Microsoft Exchange	該当しない可能性あり ^a
Sun ONE Directory Server	(mail={a}) (mailForwardingAddress={a}) (mailEquivalentAddress={a}) (mailRoutingAddress={a}) (otherMailbox={a}) (rfc822Mailbox={a})

a.Active Directory の実装によっては、proxyAddresses 属性のエントリが複数存在することがありますが、この属性の値は Active Directory によって smtp:user@domain.com という形式で格納されるため、このデータは LDAP ルーティング/エイリアス拡張には使用できません。ターゲット アドレスはそれぞれ別の attribute:value ペアに存在する必要があります。Microsoft Exchange 環境が同じインフラストラクチャ内に複数あり、互いを認識している場合は、Exchange 環境の間でメールをルーティングするときに、送信元 MTA に戻る方向のルートは通常は必要ありません。

ルーティング : MAILHOST と MAILROUTINGADDRESS

ルーティング クエリーの場合は、MAILHOST の値は IP アドレスではなく、解決可能なホスト名であることが必要です。これには、内部的な DNSconfig が必要になるのが一般的です。

MAILHOST は、ルーティング クエリーでは省略可能です。MAILROUTINGADDRESS は、MAILHOST が設定されていない場合は必須です。

エンベロープ送信者を書き換えるためのマスカレード クエリーの使用

マスカレードとは、電子メールのエンベロープ送信者（「送信者」または「MAIL FROM」と呼ばれることもあります）および To:、From:、CC: の各ヘッダーを、定義済みのクエリーに基づいて書き換える機能です。この機能の一般的な実装例の 1 つが「仮想ドメイン」であり、これによって複数のドメインを 1 つのサイトからホスティングできるようになります。他の一般的な実装としては、ネットワークインフラストラクチャを「隠す」ために、電子メール ヘッダーの文字列からサブドメインを取り除く（「ストリップング」）というものがあります。

マスカレード クエリーの例

表 22-4 一般的な LDAP 実装での LDAP クエリー文字列の例：マスカレード

クエリーの対象	マスカレード
OpenLDAP	(mailRoutingAddress={a})
Microsoft Active Directory アドレス帳	(proxyaddresses=smtptp:{a})
Sun ONE Directory Server	(mail={a}) (mailAlternateAddress={a}) (mailEquivalentAddress={a}) (mailForwardingAddress={a}) (mailRoutingAddress={a})

「フレンドリ名」のマスカレード

ユーザ環境によっては、LDAP ディレクトリ サーバスキーマの中に、メール ルーティング アドレスやローカル メール アドレス以外に「フレンドリ名」が含まれていることがあります。AsyncOS では、エンベロープ送信者（発信メールの場合）やメッセージ ヘッダー（受信メールの場合、To:、Reply To:、From:、CC: など）を、この「フレンドリ名」でマスカレードできます。フレンドリ アドレスには、有効な電子メール アドレスでは通常は許可されない特殊文字（引用符、スペース、カンマなど）が含まれていてもかまいません。

LDAP クエリー経由でヘッダーをマスカレードするときに、フレンドリ メール文字列全体を LDAP サーバからの結果で置き換えるかどうかを設定時に選択できます。この動作がイネーブルになっている場合、エンベロープ送信者には user@domain 部分のみが使用されることに注意してください（フレンドリ名はルールに反するため）。

標準的な LDAP マスカレードのときと同様に、LDAP クエリーの結果が空（長さが 0 またはすべてホワイトスペース）の場合は、マスカレードは行われません。

この機能をイネーブルにするには、LDAP ベースのマスカレード クエリーをリスナーに対して設定するときに ([LDAP] ページまたは ldapconfig コマンド)、次の質問に対して「y」と回答します。

```
Do you want the results of the returned attribute to replace the entire
friendly portion of the original recipient? [N]
```

たとえば、次のような LDAP エントリがあるとします。

属性	値
mailRoutingAddress	admin\@example.com
mailLocalAddress	joe.smith\@example.com
mailFriendlyAddress	"Administrator for example.com," <joe.smith\@example.com>

この機能がイネーブルになっている場合に、LDAP クエリーが (mailRoutingAddress={a}) で、マスカレード属性が (mailLocalAddress) ならば、次のように置き換えられます。

元のアドレス (From、To、CC、Reply-to)	マスカレードされたヘッダー	マスカレードされたエンベロープ送信者
admin@example.com	From: "Administrator for example.com," <joe.smith@example.com>	MAIL FROM: <joe.smith@example.com>

受信者がグループメンバーであるかどうかを指定するグループ LDAP クエリーの使用

LDAP ディレクトリ内で定義されたグループに受信者が属しているかどうかを、LDAP サーバに対するクエリーを使用して判定できます。

手順

- ステップ 1** メッセージフィルタを作成します。この中で、メッセージに作用するルールとして、`rcpt-to-group` または `mail-from-group` を使用します。
- ステップ 2** 次に、[システム管理 (System Administration)] > [LDAP] ページ (または `ldapconfig` コマンド) を使用して、アプライアンスのバインド先となる LDAP サーバを定義し、グループメンバーシップを調べるクエリーを設定します。
- ステップ 3** [ネットワーク (Network)] > [リスナー (Listeners)] ページ (または `listenerconfig -> edit -> ldapgroup` サブコマンド) を使用して、このグループクエリーをリスナーに対してイネーブルにします。

グループクエリーの例

表 22-5 一般的な LDAP 実装での LDAP クエリー文字列の例：グループ

クエリーの対象	グループ
OpenLDAP	OpenLDAP では、 <code>memberOf</code> 属性はデフォルトではサポートされません。LDAP 管理者によって、この属性または類似の属性がスキーマに追加されていることがあります。
Microsoft Active Directory	<code>(&(memberOf={g})(proxyAddresses=smtp:{a}))</code>
Sun ONE Directory Server	<code>(&(memberOf={g})(mailLocalAddress={a}))</code>

たとえば、LDAP ディレクトリで「マーケティング」グループのメンバーが `ou=Marketing` と分類されているとします。この分類を使用して、このグループが送受信するメールを特別な方法で取り扱うことができます。ステップ 1 で、メッセージに作用するメッセージフィルタを作成し、ステップ 2 と 3 で LDAP ルックアップメカニズムをイネーブルにします。

グループクエリーの設定

次に示す例では、マーケティンググループ (LDAP グループ「Marketing」として定義) のメンバーからのメールを代替メール配信ホスト `marketingfolks.example.com` に配信します。

手順

- ステップ 1** 初めに、グループメンバーシップに関して肯定的に一致するメッセージに作用する、メッセージフィルタを作成します。この例では、作成するフィルタの中で `mail-from-group` ルールを使用します。メッセージのうち、エンベロープ送信者が LDAP グループ「marketing-group1」に属していることが判明したものはすべて、代替配信ホストに送信されます (フィルタの `alt-mailhost` アクション)。

グループメンバーシップフィールド変数 (groupName) は、ステップ 2 で定義します。グループ属性「groupName」の値は、marketing-group1 と定義されます。

```
mail3.example.com> filters

Choose the operation you want to perform:

- NEW - Create a new filter.
- IMPORT - Import a filter script from a file.

[]> new

Enter filter script. Enter '.' on its own line to end.

MarketingGroupfilter:

  if (mail-from-group == "marketing-group1") {

    alt-mailhost ('marketingfolks.example.com');}

.

1 filters added.

Choose the operation you want to perform:

- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.

[]>
```

メッセージフィルタ ルール mail-from-group と rcpt-to-group の詳細については、「メッセージフィルタ ルール」(P.9-2) を参照してください。

ステップ 2 次に、[LDAP サーバ プロファイルを追加 (Add LDAP Server Profile)] ページを使用して、アプライアンスのバインド先となる LDAP サーバを定義し、グループ メンバーシップを調べる最初のクエリーを定義します。

ステップ 3 次に、パブリック リスナー「InboundMail」で LDAP クエリーを使用してグループ ルーティングを行うように更新します。[リスナーを編集 (Edit Listener)] ページを使用して、前のステップで指定した LDAP クエリーをイネーブルにします。

このクエリーが実行されると、リスナーが受け入れたメッセージによって LDAP サーバに対するクエリーがトリガーされて、グループ メンバーシップが特定されます。PublicLDAP2.group クエリーはすでに、[システム管理 (System Administration)] > [LDAP] ページで定義されています。

図 22-6 リスナーでのグループ クエリーの指定
Edit Listener

Listener Settings	
Name:	IncomingMail
Type of Listener:	Public
Interface:	Data 1 TCP Port: 25
Bounce Profile:	Default
Disclaimer Above:	None <small>Disclaimer text will be applied above the message body.</small>
Disclaimer Below:	None <small>Disclaimer text will be applied below the message body.</small>
SMTP Authentication Profile:	None
Certificate:	test
▶ SMTP Address Parsing Options:	Optional settings for controlling parsing in SMTP "MAIL FROM" and "RCPT TO" fields.
▶ Advanced:	Optional settings for customizing the behavior of the Listener
▼ LDAP Queries:	<ul style="list-style-type: none"> ▶ Accept ▶ Routing ▶ Masquerade ▼ Group

この例では、変更を有効にするには **commit** が必要であることに注意してください。

例：グループ クエリーを使用してスパムとウイルスのチェックをスキップする

メッセージフィルタはパイプラインの初めの方で実行されるので、グループ クエリーを使用すると、特定のグループについてウイルスとスパムのチェックをスキップできます。たとえば、社内の IT グループへのメッセージについては、スパムとウイルスのチェックをスキップしてすべて受信したいという要望があるとします。LDAP レコードの中に、DN をグループ名として使用するグループ エントリを作成します。このグループ名は、次の DN エントリで構成されます。

```
cn=IT, ou=groups, o=sample.com
```

LDAP サーバ プロファイルを作成し、次のグループ クエリーを指定します。

```
(&(memberOf={g})(proxyAddresses=smtp:{a}))
```

次に、このクエリーをリスナーに対してイネーブルにします。これで、メッセージがそのリスナーで受信されたときに、このグループ クエリーがトリガーされます。

IT グループのメンバーについてはウイルスとスパムのチェックをスキップするために、次のメッセージフィルタを作成して、着信メッセージを LDAP グループと比較して検査します。

```
[ ]> - NEW - Create a new filter.

- IMPORT - Import a filter script from a file.

[ ]> new

Enter filter script. Enter '.' on its own line to end.

IT_Group_Filter:

if (rcpt-to-group == "cn=IT, ou=groups, o=sample.com"){

skip-spamcheck();

skip-viruscheck();

deliver();

}

.

1 filters added.
```



(注)

このメッセージフィルタ内の `rcpt-to-group` には、グループ名として入力された DN (`cn=IT, ou=groups, o=sample.com`) が反映されています。メッセージフィルタ内で使用しているグループ名が正しいことを確認してください。フィルタの実行時に、LDAP ディレクトリ内でその名前との比較が確実に行われるようにするためです。

リスナーが受け入れたメッセージによって LDAP サーバに対するクエリーがトリガーされて、グループメンバーシップが特定されます。メッセージ受信者が IT グループのメンバーの場合は、メッセージフィルタの定義に従ってウイルスとスパムのチェックがいずれもスキップされて、メッセージが受信者に配信されます。フィルタで LDAP クエリーの結果をチェックするには、LDAP サーバに対する LDAP クエリーを作成し、その LDAP クエリーをリスナーに対してイネーブルにする必要があります。

特定のドメインヘルパーティングするためのドメイン ベース クエリーの使用

ドメインベース クエリーとは、LDAP クエリーをタイプ別にグループ化し、特定のドメインに関連付けたい場合、特定のリスナーに割り当てたものです。ドメインベース クエリーが使用されるのは、複数の LDAP サーバがそれぞれ異なるドメインに関連付けられているが、すべての LDAP サーバに対するクエリーを同じリスナー上で実行する場合です。たとえば、「MyCompany」という会社が「HisCompany」と「HerCompany」の 2 社を買収するとします。MyCompany は自社のドメイン `MyCompany.example.com` に加えて `HisCompany.example.com` および `HerCompany.example.com` のドメインを運用するとともに、ドメインごとに別の LDAP サーバを運用して、各ドメインに関連付けら

れた従業員の情報を格納しています。この 3 つのドメインのメールをすべて受け入れるために、MyCompany はドメインベース クエリーを作成します。これで、MyCompany.example.com は Mycompany.example.com、HisCompany.example.com、および HerCompany.example.com のメールを同じリスナー上で受け入れることができます。

手順

- ステップ 1** ドメインベース クエリーで使用するドメインごとに 1 つずつ、サーバ プロファイルを作成します。このサーバ プロファイルのそれぞれに対して、ドメインベース クエリーに使用するクエリーを設定します（受け入れ、ルーティングなど）。詳細については、「[LDAP サーバに関する情報を保存する LDAP サーバ プロファイルの作成](#)」(P.22-5) を参照してください。
- ステップ 2** ドメインベース クエリーを作成します。ドメインベース クエリーを作成するときは、各サーバ プロファイルからクエリーを選択します。また、どのクエリーを実行するかを **Envelope To** フィールドに基づいて決定するように、**Cisco** アプライアンスを設定します。クエリーの作成方法の詳細については、「[ドメインベース クエリーの作成](#)」(P.22-27) を参照してください。
- ステップ 3** ドメインベース クエリーをパブリックまたはプライベートのリスナーに対してイネーブルにします。リスナーの設定方法の詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「[Configuring the Gateway to Receive Mail](#)」を参照してください。



(注) ドメインベース クエリーは他にも、**Cisco** スпам隔離機能の LDAP エンドユーザ アクセスやスパム通知のために使用できます。詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「[Configuring the Cisco Spam Quarantines Feature](#)」を参照してください。

ドメインベース クエリーの作成

ドメインベース クエリーは、[システム管理 (System Administration)] > [LDAP] > [LDAP サーバ プロファイル (LDAP Server Profiles)] ページで作成します。

手順

- ステップ 1** [LDAP サーバ プロファイル (LDAP Server Profiles)] ページの [詳細 (Advanced)] をクリックします。
- ステップ 2** [ドメイン割り当ての追加 (Add Domain Assignments)] をクリックします。
- ステップ 3** ドメインベース クエリーの名前を入力します。
- ステップ 4** クエリーのタイプを選択します。



(注) ドメインベース クエリーを作成するときに、選択するクエリーのタイプはすべて同じでなければなりません。クエリー タイプを選択すると、**Cisco** アプライアンスはそのタイプのクエリーを利用可能なサーバ プロファイルから取得し、クエリー フィールドを生成します。

- ステップ 5** [ドメイン割り当て (Domain Assignments)] フィールドに、ドメインを入力します。
- ステップ 6** このドメインに関連付けるクエリーを選択します。
- ステップ 7** クエリーのドメインがすべて追加されるまで、行を追加します。

一連の LDAP クエリーを実行するためのチェーンクエリーの使用

- ステップ 8** どのクエリーにも一致しないときに実行する、デフォルトのクエリーを入力できます。デフォルトのクエリーを入力しない場合は、[None] を選択します。
- ステップ 9** クエリーをテストします。[クエリーのテスト (Test Query)] ボタンをクリックし、テストするユーザログインとパスワードまたはメールアドレスを [テストパラメータ (Test Parameters)] のフィールドに入力します。結果が [接続ステータス (Connection Status)] フィールドに表示されます。
- ステップ 10** (省略可能) {f} トークンを受け入れクエリー内で使用する場合は、エンベロープ送信者アドレスをテストクエリーに追加できます。



(注) ドメインベースクエリーの作成が終了したら、このクエリーをパブリックまたはプライベートのリスナーに関連付ける必要があります。

- ステップ 11** 変更内容を送信し、確定します。

一連の LDAP クエリーを実行するためのチェーンクエリーの使用

チェーンクエリーは、Cisco アプライアンスによって順番に実行が試行される一連の LDAP クエリーで構成されます。Cisco アプライアンスは、この「チェーン」の中の各クエリーの実行を試行し、LDAP サーバから肯定的なレスポンスが返されると（または「チェーン」の最後のクエリーで否定的なレスポンスが返されるか失敗すると）実行を停止します。チェーンクエリーが役立つのは、LDAP ディレクトリ内のエントリにおいて、さまざまな属性に類似の（または同一の）値が格納されている場合です。たとえば、属性 maillocaladdress と mail がユーザ電子メールアドレスの格納に使用されているとします。この両方の属性に対して確実にクエリーを実行するには、チェーンクエリーを使用します。

手順

- ステップ 1** チェーンクエリー内で使用するクエリーごとに、サーバプロファイルを作成します。このサーバプロファイルのそれぞれについて、チェーンクエリーに使用するクエリーを設定します。詳細については、「LDAP サーバに関する情報を保存する LDAP サーバプロファイルの作成」(P.22-5) を参照してください。
- ステップ 2** チェーンクエリーを作成します。詳細については、「チェーンクエリーの作成」(P.22-29) を参照してください。
- ステップ 3** チェーンクエリーをパブリックまたはプライベートのリスナーに対してイネーブルにします。リスナーの設定方法の詳細については、『Cisco IronPort AsyncOS for Email Configuration Guide』の「Configuring the Gateway to Receive Mail」を参照してください。



(注) ドメインベースクエリーは他にも、Cisco スпам隔離機能の LDAP エンドユーザアクセスやスパム通知のために使用できます。詳細については、『Cisco IronPort AsyncOS for Email Daily Management Guide』の「Configuring the Cisco Spam Quarantines Feature」を参照してください。


チェーンクエリーの作成

チェーンクエリーは、[システム管理 (System Administration)] > [LDAP] > [LDAP サーバ プロファイル (LDAP Server Profiles)] ページで作成します。

手順

- ステップ 1** [LDAP サーバ プロファイル (LDAP Server Profiles)] ページの [詳細 (Advanced)] をクリックします。
 - ステップ 2** [チェーンクエリーを追加 (Add Chain Query)] をクリックします。
 - ステップ 3** チェーンクエリーの名前を入力します。
 - ステップ 4** クエリーのタイプを選択します。

チェーンクエリーを作成するときに、選択するクエリーのタイプはすべて同じでなければなりません。クエリータイプを選択すると、Cisco アプライアンスはそのタイプのクエリーを利用可能なサーバプロファイルから取得し、クエリーフィールドを生成します。
 - ステップ 5** チェーンクエリーに追加するクエリーを選択します。

Cisco アプライアンスによって、ここで設定した順にクエリーが実行されます。したがって、複数のクエリーをチェーンクエリーに追加する場合は、より限定的なクエリーの後でより広範なクエリーが実行されるような順序にすることを推奨します。
 - ステップ 6** クエリーをテストします。[クエリーのテスト (Test Query)] ボタンをクリックし、テストするユーザログインとパスワードまたはメールアドレスを [テストパラメータ (Test Parameters)] のフィールドに入力します。結果が [接続ステータス (Connection Status)] フィールドに表示されます。
 - ステップ 7** (省略可能) {f} トークンを受け入れクエリー内で使用する場合は、エンベロープ送信者アドレスをテストクエリーに追加できます。
-  **(注)** チェーンクエリーの作成が終了したら、このクエリーをパブリックまたはプライベートのリスナーに関連付ける必要があります。
- ステップ 8** 変更内容を送信し、確定します。

LDAP によるディレクトリハーベスト攻撃防止

ディレクトリハーベスト攻撃は、悪意のある送信者が、よくある名前を持つ受信者宛にメッセージを送信することによって開始します。電子メールゲートウェイは、受信者がその場所に有効なメールボックスを持っているかどうかを調べて応答を返します。これを大量に実行すると、悪意のある送信者は、どのアドレスにスパムを送信すればよいかを、有効なアドレスの「収穫 (ハーベスト)」によって特定できるようになります。

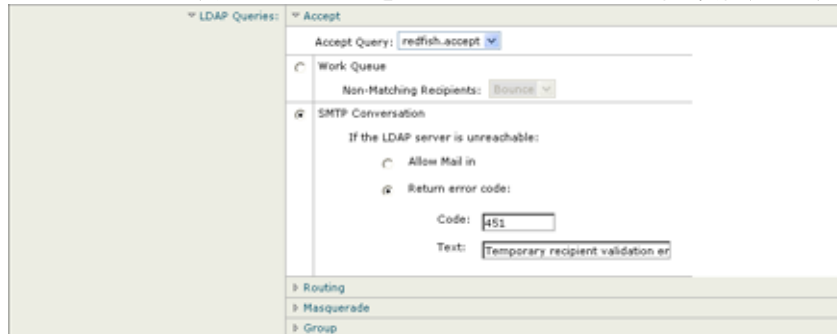
Cisco 電子メールセキュリティアプライアンスでは、LDAP 受け入れ検証クエリーを使用すると、Directory Harvest Attack (DHA; ディレクトリハーベスト攻撃) を検出して防止できます。LDAP 受け入れを設定するときに、ディレクトリハーベスト攻撃防止を SMTP キャンパセーション中に行うか、ワークキューの中で行うかを選択できます。

SMTP カンバセーション中のディレクトリ ハーベスト攻撃防止

DHA を防止するには、ドメインだけを Recipient Access Table (RAT; 受信者アクセス テーブル) に入力しておき、LDAP 受け入れ検証を SMTP カンバセーション内で実行します。

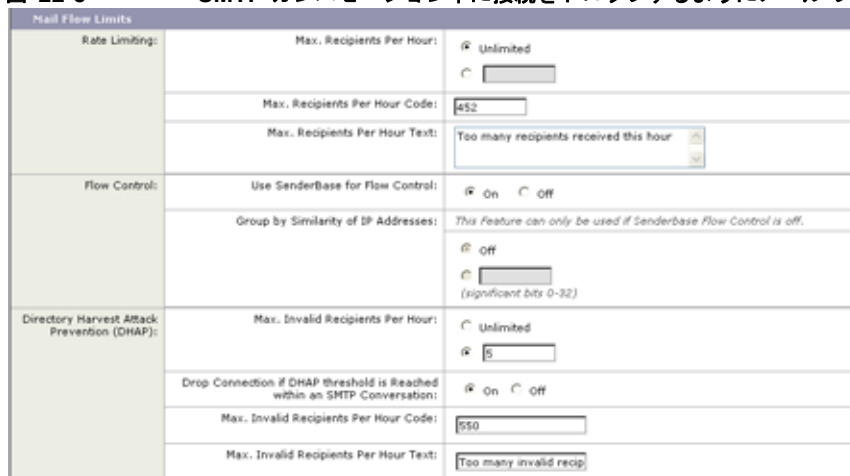
SMTP カンバセーション中にメッセージをドロップするには、LDAP 受け入れのための LDAP サーバ プロファイルを設定します。次に、LDAP 受け入れクエリーを SMTP カンバセーション中に実行するようにリスナーを設定します。

図 22-7 受け入れクエリーを SMTP カンバセーション中に実行するように設定



リスナーで実行する LDAP 受け入れクエリーを設定したら、そのリスナーに関連付けられたメール フロー ポリシーの中の DHAP (ディレクトリ ハーベスト攻撃防止) 設定を指定する必要があります。

図 22-8 SMTP カンバセーション中に接続をドロップするようにメール フロー ポリシーを設定する



リスナーに関連付けられたメール フロー ポリシーの中で、ディレクトリ ハーベスト攻撃防止のための次の項目を設定します。

- [1 時間あたりの無効な受信者の最大数 (Max. Invalid Recipients Per hour)]。このリスナーがリモート ホストから受け取る無効な受信者の 1 時間あたりの最大数です。このしきい値は、RAT 拒否の総数を表します。これは、無効な LDAP 受信者宛てのため SMTP カンバセーション中にドロップされたメッセージの総数と、ワーク キュー内でバウンスされたメッセージの合計です。たとえば、しきい値を 5 と設定した場合に、検出された RAT 拒否が 2 件で、無効な LDAP 受信者宛てのためドロップされたメッセージが 3 件であるとします。この時点で、Cisco アプライアンスはしきい値に到達したと判断して、接続をドロップさせます。デフォルトでは、パブリック リスナーでの 1 時間あたりの受信者の最大数は 25 です。プライベート リスナーの場合は、1 時間あたりの受信者の最大数はデフォルトでは無制限です。この最大数を「Unlimited」に設定すると、そのメール フロー ポリシーに対して DHAP はイネーブルになりません。

- [SMTP 対話内で DHAP しきい値に到達した場合、接続をドロップ (Drop Connection if DHAP Threshold is reached within an SMTP conversation)]。ディレクトリ ハーベスト攻撃防止のしきい値に達したときに Cisco アプライアンスによって接続をドロップさせる設定をします。
- [時間コードあたりの最大受信者数 (Max. Recipients Per Hour Code)]。接続をドロップするときに使用するコードを指定します。デフォルトのコードは 550 です。
- [時間テキストあたりの最大受信者数 (Max. Recipients Per Hour Text)]。ドロップした接続に対して使用するテキストを指定します。デフォルトのテキストは「Too many invalid recipients」です。

しきい値に達した場合は、受信者が無効であってもメッセージのエンベロープ送信者にバウンスメッセージが送信されることはありません。

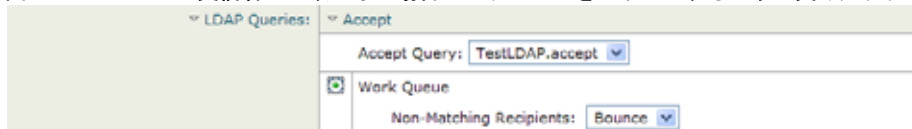
ワーク キュー内でのディレクトリ ハーベスト攻撃防止

ディレクトリ ハーベスト攻撃 (DHA) のほとんどは、ドメインだけを Recipient Access Table (RAT; 受信者アクセス テーブル) に入力しておき、LDAP 受け入れ検証をワーク キュー内で実行することによって防止できます。この方法を使用すると、悪意のある送信者が、受信者が有効かどうかを SMTP カンバセーション中に知ることはできなくなります。(受け入れクエリーが設定されているときは、システムはメッセージを受け入れて、LDAP 受け入れ検証をワーク キュー内で実行します)。ただし、メッセージのエンベロープ送信者には、受信者が無効である場合にバウンスメッセージが送信されます。

ワーク キュー内でディレクトリ ハーベスト攻撃防止するための設定

ディレクトリ ハーベスト攻撃を防止するには、初めに LDAP サーバ プロファイルを設定して LDAP 受け入れをイネーブルにします。LDAP 受け入れクエリーをイネーブルにしたら、次のように、その受け入れクエリーを使用するようにリスナーを設定するとともに、受信者が一致しない場合はメールをバウンスするように指定します。

図 22-9 受信者が一致しない場合はメッセージをバウンスするように受け入れクエリーを設定



次に、メール フロー ポリシーを設定します。このポリシーでは、所定の時間内に送信 IP アドレスあたりどれだけの無効な受信者アドレスをシステムが受け入れるかを定義します。この数を超えると、システムはこの状態が DHA (ディレクトリ ハーベスト攻撃) であると判断してアラート メッセージを送信します。このアラート メッセージに含まれる情報は次のとおりです。

```
LDAP: Potential Directory Harvest Attack from host=('IP-address', 'domain_name'),
dhap_limit=n, sender_group=sender_group,

listener=listener_name, reverse_dns=(reverse_IP_address, 'domain_name', 1),
sender=envelope_sender, rcpt=envelope_recipients
```

メール フロー ポリシーで指定されたしきい値に達するまでは、システムによってメッセージがバウンスされますが、それ以降は応答を返すことなく受け入れられてドロップされます。したがって、正当な送信者にはアドレスの誤りが通知されますが、悪意のある送信者は、どの受信者が受け入れられたかを判断できません。

この無効受信者カウンタの働きは、現在 AsyncOS に実装されているレート制限機能に似ています。つまり、管理者がこの機能をイネーブルにして、上限値をパブリック リスナーの HAT 内のメールフローポリシーの中で設定します (HAT のデフォルトのメールフローポリシーを含む)。

たとえば、パブリック リスナーの HAT 内のメールフローポリシーを CLI で作成または編集するときは、次のような質問が表示されます (`listenerconfig -> edit -> hostaccess -> default | new` コマンドを実行)。

```
Do you want to enable Directory Harvest Attack Prevention per host? [Y]> y
```

```
Enter the maximum number of invalid recipients per hour from a remote host.
```

```
[25]>
```

この機能は、メールフローポリシーを GUI で編集するときにも表示されます (対応するリスナーに対して LDAP クエリーが作成済みの場合)。

図 22-10 GUI の DHAP 機能



1 時間当たりの無効受信者数を入力すると、そのメールフローポリシーに対して DHAP (ディレクトリハーベスト攻撃防止) がイネーブルになります。デフォルトで、パブリックリスナーでは 1 時間あたり最大 25 件の無効受信者が受け入れられます。プライベートリスナーの場合は、1 時間あたりの無効受信者数はデフォルトでは無制限です。この最大数を「Unlimited」に設定すると、そのメールフローポリシーに対して DHAP はイネーブルになりません。

SMTP 認証を行うための AsyncOS の設定

AsyncOS では、SMTP 認証がサポートされています。SMTP Auth は、SMTP サーバに接続するクライアントを認証するメカニズムです。

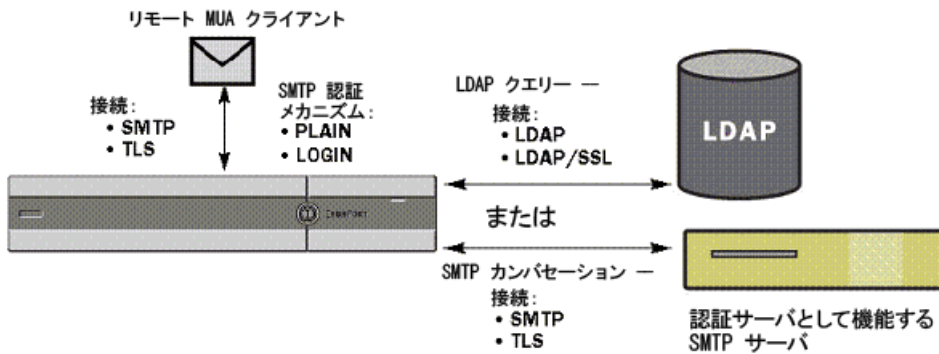
このメカニズムを利用すると、特定の組織に所属するユーザが、その組織のメールサーバにリモートで接続している (自宅や出張先などから) ときもメールサーバを使用してメールを送信できるようになります。Mail User Agent (MUA; メールユーザエージェント) は、メールの送信を試行するときに認証要求 (チャレンジ/レスポンス) を発行できます。

SMTP 認証は、発信メールリレーに対しても使用できます。これを利用すると、Cisco アプライアンスがネットワークのエッジではない場合に、アプライアンスからリレーサーバへのセキュア接続を確立できます。

AsyncOS では、ユーザクレデンシャルの認証方式として次の 2 つがサポートされています。

- LDAP ディレクトリを使用する。
- 別の SMTP サーバを使用する (SMTP Auth 転送と SMTP Auth 発信)。

図 22-11 SMTP Auth のサポート : LDAP ディレクトリストアまたは SMTP サーバ



SMTP 認証方式を設定したら、HAT メールフローポリシー内で使用される SMTP Auth プロファイルを、`smtppauthconfig` コマンドを使用して作成します（「リスナーでの SMTP 認証のイネーブル化」(P.22-36) を参照）。

SMTP 認証の設定

LDAP サーバを使用して認証を行う場合は、[LDAP サーバ プロファイルを追加 (Add LDAP Server Profile)] または [LDAP サーバプロファイルを編集 (Edit LDAP Server Profile)] ページ（または `ldapconfig` コマンド）でクエリータイプとして `SMTPAUTH` を選択して SMTP 認証クエリーを作成します。設定する LDAP サーバのそれぞれについて、SMTP 認証プロファイルとして使用する `SMTPAUTH` クエリーを 1 つ設定できます。

SMTP 認証クエリーには、「LDAP バインド」と「パスワードを属性として取得」の 2 種類があります。「パスワードを属性として取得」を使用するときは、Cisco アプライアンスによって LDAP ディレクトリ内のパスワードフィールドが取り出されます。このパスワードは、プレーンテキストでも、暗号化またはハッシュ化済みで格納されていてもかまいません。LDAP バインドを使用するときは、Cisco アプライアンスはクライアントが指定したクレデンシャルを使用して LDAP サーバへのログインを試行します。

パスワードを属性として指定

OpenLDAP の規定 (RFC 2307 に基づく) では、コーディングのタイプを中カッコで囲み、その後にエンコードされたパスワードを続けることになっています（たとえば「`{SHA}5en6G6MezRroT3XKqkdPOmY/BfQ=`」）。この例では、パスワード部分はプレーンテキストのパスワードに SHA を適用してから base64 エンコーディングしたものです。

Cisco アプライアンスがパスワードを取得する前に、SASL メカニズムのネゴシエートが MUA との間で行われ、アプライアンスと MUA はどの方法を使用するかを決定します（サポートされているメカニズムは LOGIN、PLAIN、MD5、SHA、SSHA、CRYPT SASL です）。その後で、アプライアンスは LDAP データベースに対するクエリーを実行してパスワードを取得します。LDAP 内では、中カッコで囲まれたプレフィックスがパスワードに付いていることがあります。

- プレフィックスが付いていない場合は、LDAP 内に格納されているパスワードがプレーンテキストであると見なされます。
- プレフィックスが付いている場合は、アプライアンスはそのハッシュ化パスワードを取得し、MUA によって指定されたユーザ名とパスワードの両方あるいはどちらかのハッシュを実行して、ハッシュ後のパスワードと比較します。Cisco アプライアンスでサポートされるハッシュタイプは SHA1 と MD5 であり、RFC 2307 の規定に基づいて、パスワードフィールド内ではハッシュ化パスワードの前にハッシュメカニズムのタイプが付加されます。

- LDAP サーバの中には、OpenWave LDAP サーバのように、暗号化されたパスワードの前に暗号化タイプを付加しないものもあり、代わりに暗号化タイプが別の LDAP 属性として格納されています。このような場合は、管理者が指定したデフォルトの SMTP AUTH 暗号化方式であると見なされて、そのパスワードと SMTP カンバセーションで取得されたパスワードとが比較されます。

Cisco アプライアンスは、SMTP Auth 交換から任意ユーザ名を受け取って LDAP クエリーに変換し、このクエリーを使用してクリア テキストまたはハッシュ化されたパスワード フィールドを取得します。次に、SMTP Auth クレデンシャルで指定されたパスワードに対してハッシュが必要な場合は実行し、その結果を LDAP からのパスワードと比較します（ハッシュ タイプのタグがある場合は取り除く）。一致した場合は、SMTP Auth カンバセーションが続行されます。一致しない場合は、エラー コードが返されます。

SMTP 認証クエリーの設定

表 22-6 SMTP Auth LDAP クエリーのフィールド

名前 (Name)	クエリーの名前。
クエリ文字列 (Query String)	<p>認証を LDAP バインド経由で行うか、パスワードを属性として取得して行うかを選択できます。</p> <p>[バインド (Bind)] : LDAP サーバへのログイン試行には、クライアントによって指定されたクレデンシャルを使用します (これを「LDAP バインド」と呼びます)。</p> <p>SMTP Auth クエリーで使用される同時接続の最大数を指定します。この数は、上の LDAP サーバ属性で指定した数を超えてはなりません。バインド認証時に大量のセッションタイムアウトが発生するのを防ぐには、ここで指定する同時接続の最大数を大きくします (一般的には、接続のほぼすべてを SMTP Auth に割り当てることができます)。バインド認証ごとに、新しい接続が 1 つ使用されます。残りの接続は、他のタイプの LDAP クエリーで共有されます。</p> <p>[属性としてのパスワード (Password as Attribute)] : パスワードを取得して認証を行うには、下の [SMTP 認証パスワード属性 (SMTP Auth password attribute)] フィールドでパスワードを指定します。</p> <p>選択した種類の認証に使用する LDAP クエリーを指定します。</p> <p>Active Directory のクエリーの例 :</p> <pre>(&(samaccountname={u})(objectCategory=person) (objectClass=user))</pre>
SMTP 認証パスワード属性 (SMTP Auth Password Attribute)	[属性としてパスワード取得した認証 (Authenticate by fetching the password as an attribute)] を選択した場合は、パスワード属性をここで指定します。

次の例では、[システム管理 (System Administration)] > [LDAP] ページを使用して LDAP 設定「PublicLDAP」を編集し、SMTPAUTH クエリーを追加しています。クエリー文字列 (uid={u}) は、userPassword 属性と比較するように作成されています。

図 22-12 SMTP 認証クエリー

SMTPAUTH プロファイルの設定が完了すると、そのクエリーを SMTP 認証に使用するようリスナーを設定できます。

第 2 の SMTP サーバ経由での SMTP 認証（転送を使用する SMTP Auth）

SMTP 認証カンバセーションのために指定されたユーザ名とパスワードを、別の SMTP サーバを使用して検証するようにアプライアンスを設定できます。

認証を行うサーバは、メールを転送するサーバとは別のものであり、SMTP 認証要求への応答だけを行います。認証に成功したときは、専用メールサーバによるメールの SMTP 転送を続行できます。この機能は、「転送を使用する SMTP Auth」と呼ばれることもあります。クレデンシャルのみが別の SMTP サーバに転送（プロキシ）されて認証が行われるからです。

手順

- ステップ 1** [ネットワーク (Network)] > [SMTP 認証 (SMTP Authentication)] を選択します。
- ステップ 2** [プロファイルを追加 (Add Profile)] をクリックします。
- ステップ 3** SMTP 認証プロファイルの一意の名前を入力します。
- ステップ 4** [プロファイルタイプ (Profile Type)] で [転送 (Forward)] を選択します。
- ステップ 5** [次へ (Next)] をクリックします。
- ステップ 6** 転送サーバのホスト名/IP アドレスとポートを入力します。認証要求の転送に使用する転送インターフェイスを選択します。同時接続の最大数を指定します。次に、アプライアンスから転送サーバへの接続に対して TLS を必須とするかどうかを設定します。使用する SASL メカニズムも、[プレーン (PLAIN)] と [ログイン (LOGIN)] から選択できます (使用できる場合)。この選択は、転送サーバごとに設定されます。
- ステップ 7** 変更内容を送信し、確定します。
- ステップ 8** 認証プロファイルの作成が完了すると、そのプロファイルをリスナーに対してイネーブルにできます。詳細については、「[リスナーでの SMTP 認証のイネーブル化](#)」(P.22-36) を参照してください。

LDAP を使用する SMTP 認証

LDAP ベースの SMTP 認証プロファイルを作成するには、SMTP 認証クエリーを LDAP サーバ プロファイルとともに [システム管理 (System Administration)] > [LDAP] ページであらかじめ作成しておく必要があります。このプロファイルを使用して SMTP 認証プロファイルを作成します。LDAP プロファイルの作成方法の詳細については、「LDAP クエリーの概要」(P.22-2) を参照してください。

手順

-
- ステップ 1 [ネットワーク (Network)] > [SMTP 認証 (SMTP Authentication)] を選択します。
 - ステップ 2 [プロファイルを追加 (Add Profile)] をクリックします。
 - ステップ 3 SMTP 認証プロファイルの一意の名前を入力します。
 - ステップ 4 [プロファイルタイプ (Profile Type)] で [LDAP] を選択します。
 - ステップ 5 [次へ (Next)] をクリックします。
 - ステップ 6 この認証プロファイルに使用する LDAP クエリーを選択します。
 - ステップ 7 デフォルトの暗号化方式をドロップダウンメニューから選択します。選択肢には、[SHA]、[Salted SHA]、[Crypt]、[Plain]、[MD5] があります。LDAP サーバによって暗号化後のパスワードの前に暗号化タイプが付加される場合は、[None] を選択してください。LDAP サーバによって暗号化タイプが別エンティティとして保存される場合は (たとえば OpenWave LDAP サーバ)、暗号化方式をメニューから選択してください。デフォルトの暗号化設定は、LDAP クエリーにバインドが使用される場合は使用されません。
 - ステップ 8 [完了 (Finish)] をクリックします。
 - ステップ 9 変更内容を送信し、確定します。
 - ステップ 10 認証プロファイルの作成が完了すると、そのプロファイルをリスナーに対してイネーブルにできます。詳細については、「リスナーでの SMTP 認証のイネーブル化」(P.22-36) を参照してください。
-

リスナーでの SMTP 認証のイネーブル化

[ネットワーク (Network)] > [SMTP 認証 (SMTP Authentication)] ページで、実行する認証のタイプ (LDAP ベースまたは SMTP 転送ベース) を指定して SMTP 認証「プロファイル」を作成したら、[ネットワーク (Network)] > [リスナー (Listeners)] ページ (または listenerconfig コマンド) を使用して、このプロファイルをリスナーに関連付ける必要があります。



(注) 認証済みのユーザには、ユーザのその時点のメールフローポリシーの中で RELAY 接続動作が許可されます。



(注) 1 つのプロファイル内で複数の転送サーバを指定することもできます。SASL メカニズム CRAM-MD5 と DIGEST-MD5 は、Cisco アプライアンスと転送サーバの間ではサポートされません。

次の例では、リスナー「InboundMail」で SMTPAUTH プロファイルが使用されるように、[リスナーを編集 (Edit Listener)] ページで設定しています。

図 22-13 SMTP 認証プロファイルを [リスナーを編集 (Edit Listener)] ページで選択する Edit Listener

Listener Settings	
Name:	IncomingMail
Type of Listener:	Public
Interface:	Data 1 TCP Port: 25
Bounce Profile:	Default
Disclaimer Above:	None <small>Disclaimer text will be applied above the message body.</small>
Disclaimer Below:	None <small>Disclaimer text will be applied below the message body.</small>
SMTP Authentication Profile:	forwarding_based
Certificate:	test
▶ SMTP Address Parsing Options:	Optional settings for controlling parsing in SMTP "MAIL FROM" and "RCPT TO" commands.
▶ Advanced:	Optional settings for customizing the behavior of the Listener

プロファイルを使用するようにリスナーを設定したら、そのリスナーでの SMTP 認証を許可、禁止、または必須とするようにホスト アクセス テーブルのデフォルト設定を変更できます。

図 22-14 メールフロー ポリシーでの SMTP 認証のイネーブル化

Encryption and Authentication:	①	SMTP Authentication:	<input type="radio"/> Use Default (Off) <input checked="" type="radio"/> Off <input type="radio"/> Preferred <input type="radio"/> Required
	②	If Both TLS and SMTP Authentication are enabled:	<input type="checkbox"/> Require TLS To Offer SMTP Authentication
		TLS:	<input type="radio"/> Use Default (Off) <input checked="" type="radio"/> Off <input type="radio"/> Preferred <input type="radio"/> Required

番号	説明
1.	[SMTP 認証 (SMTP Authentication)] フィールドでは、リスナー レベルで SMTP 認証を制御します。[いいえ (No)] を選択した場合は、SMTP 認証に関する他の設定にかかわらず、このリスナーでは認証はイネーブルになりません。
2.	2 番目のプロンプト ([SMTP 認証 (SMTP Authentication)]) で [必須 (Required)] を選択した場合は、AUTH キーワードが発行されるのは TLS がネゴシエートされた (クライアントが別の EHLO コマンドを発行した) 後となります。

SMTP 認証と HAT ポリシーの設定

送信者は送信者グループとしてまとめられ、その後で SMTP 認証ネゴシエーションが開始するので、ホスト アクセス テーブル (HAT) の設定には影響は及びません。リモート メール ホストが接続するときに、アプライアンスは初めにどの送信者グループが該当するかを特定して、その送信者グループのメール ポリシーを適用します。たとえば、リモート MTA 「suspicious.com」が SUSPECTLIST という送信者グループに属している場合は、「suspicious.com」の SMTPAUTH ネゴシエーションの結果とは無関係に THROTTLE ポリシーが適用されます。

ただし、SMTPAUTH を使用して認証を受ける送信者の扱いは、「通常の」送信者とは異なります。SMTPAUTH セッションに成功した場合の接続動作は「RELAY」に変更されるので、実質的に Recipient Access Table (RAT; 受信者アクセス テーブル) と LDAPACCEPT はバイパスされます。その結果、送信者はメッセージを Cisco アプライアンス経由でリレーできます。したがって、適用されるレート制限やスロットリングがある場合は、引き続き有効になります。

HAT 遅延拒否

HAT 遅延拒否が設定済みのときは、HAT 送信者グループとメールフロー ポリシーの設定に基づいて本来ならばドロップされる接続も、認証に成功し、RELAY メールフロー ポリシーが許可されます。

遅延拒否を設定するには、CLI の `listenerconfig --> setup` コマンドを使用します。この動作は、デフォルトではディセーブルになっています。

次の表に、HAT の遅延拒否を設定する方法を説明します。

```
example.com> listenerconfig
```

```
Currently configured listeners:
```

1. listener1 (on main, 172.22.138.17) QMQP TCP Port 628 Private
2. listener2 (on main, 172.22.138.17) SMTP TCP Port 25 Private

```
Choose the operation you want to perform:
```

- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.

```
[ ]> setup
```

```
Enter the global limit for concurrent connections to be allowed across all listeners.
```

```
[300]>
```

```
[...]
```

```
By default HAT rejected connections will be closed with a banner
```

```
message at the start of the SMTP conversation. Would you like to do the rejection at the message recipient level instead for more detailed logging of rejected mail?
```

```
[N]> y
```

```
Do you want to modify the SMTP RCPT TO reject response in this case?
```

```
[N]> y
```

Enter the SMTP code to use in the response. 550 is the standard code.

[550]> 551

Enter your custom SMTP response. Press Enter on a blank line to finish.

Sender rejected due to local mail policy.

Contact your mail admin for assistance.

クライアント認証を使用した SMTP セッションの認証

電子メールセキュリティ アプライアンスは、電子メールセキュリティ アプライアンスとユーザのメールクライアント間の SMTP セッションを認証するためにクライアント証明書の使用をサポートします。

SMTP 認証プロファイルを作成する場合は、証明書を確認するときに使用する証明書認証 LDAP クエリーを選択します。また、クライアント証明書が使用できなかった場合、電子メールセキュリティ アプライアンスがユーザ認証するための SMTP AUTH コマンドにフォールバックするかどうかを指定できます。

組織でユーザを認証するためにクライアント証明書を使用する場合、クライアント証明書を持たないユーザがユーザのデータが許可するように指定されている限りメールを送信できるかどうか判断するために、SMTP 認証クエリーを使用できます。

詳細については、「[クライアント証明書を使用した SMTP セッションの認証](#)」を参照してください。

発信 SMTP 認証

SMTP 認証は、発信メールリレーをユーザ名とパスワードを使用して検証するときにも使用できます。「発信」SMTP 認証プロファイルを作成してから、このプロファイルを全ドメインの SMTP ルートに関連付けます。メール配信試行のたびに、Cisco アプライアンスは必要なクレデンシャルを使用してアップストリームメールリレーにログインします。PLAIN SASL フォーマットのログインのみがサポートされます。

手順

- ステップ 1 [ネットワーク (Network)] > [SMTP 認証 (SMTP Authentication)] を選択します。
- ステップ 2 [プロファイルを追加 (Add Profile)] をクリックします。
- ステップ 3 SMTP 認証プロファイルの一意の名前を入力します。
- ステップ 4 [プロファイルタイプ (Profile Type)] で [送信 (Outgoing)] を選択します。
- ステップ 5 [次へ (Next)] をクリックします。
- ステップ 6 認証プロファイルの認証用ユーザ名とパスワードを入力します。
- ステップ 7 [完了 (Finish)] をクリックします。
- ステップ 8 [ネットワーク (Network)] > [SMTP ルート (SMTP Routes)] を選択します。

- ステップ 9** テーブルの [受信ドメイン (Receiving Domain)] カラムで、[その他のすべてのドメイン (All Other Domains)] リンクをクリックします。
- ステップ 10** SMTP ルートの宛先ホストの名前を [宛先ホスト (Destination Host)] に入力します。これは、発信メールの配信に使用される外部メールリレーのホスト名です。
- ステップ 11** 発信 SMTP 認証プロファイルをドロップダウンメニューから選択します。
- ステップ 12** 変更内容を送信し、確定します。

ロギングと SMTP 認証

SMTP 認証メカニズム (LDAP ベース、SMTP 転送サーバベース、または SMTP 発信) がアプライアンス上で設定されている場合は、以下のイベントが Cisco メール ログに記録されます。

- (情報) SMTP 認証成功：認証されたユーザと、使用されたメカニズムも記録されます。(プレーンテキストのパスワードが記録されることはありません)。
- (情報) SMTP 認証失敗：認証されたユーザと、使用されたメカニズムも記録されます。
- (警告) 認証サーバに接続不可能：サーバ名とメカニズムも記録されます。
- (警告) タイムアウト イベント：転送サーバ (アップストリームの、インジェクションを行う Cisco アプライアンスと通信) が認証要求を待つ間にタイムアウトしたとき。

ユーザの外部 LDAP 認証の設定

ネットワーク上の LDAP ディレクトリを使用してユーザを認証するように Cisco アプライアンスを設定できます。このように設定すると、ユーザが各自の LDAP ユーザ名とパスワードを使用してログインできるようになります。LDAP サーバに対する認証クエリーを設定したら、アプライアンスによる外部認証の使用をイネーブルにします (GUI の [システム管理 (System Administration)] > [ユーザ (Users)] ページまたは CLI の `userconfig` コマンドを使用します)。

手順

- ステップ 1** ユーザアカウントを見つけるためのクエリーを作成します。LDAP サーバプロファイルで、LDAP ディレクトリ内のユーザアカウントを検索するためのクエリーを作成します。
- ステップ 2** グループメンバーシップクエリーを作成します。ユーザが特定のディレクトリグループのメンバーかどうかを判断するためのクエリーを作成します。
- ステップ 3** LDAP サーバを使用するように外部認証をセットアップします。この LDAP サーバをユーザ認証に使用するようにアプライアンスを設定し、ユーザロールを LDAP ディレクトリ内のグループに割り当てます。詳細については、『Cisco IronPort AsyncOS for Email Daily Management Guide』の「Adding Users」を参照してください。



- (注) [LDAP] ページの [クエリーのテスト (Test Query)] ボタン (または `ldaptest` コマンド) を使用して、クエリーから返される結果が期待したとおりであることを確認します。詳細については、「LDAP クエリーのテスト」(P.22-17) を参照してください。

ユーザ アカウント クエリー

外部ユーザを認証するために、AsyncOS はクエリーを使用してそのユーザのレコードを LDAP ディレクトリ内で検出し、ユーザのフル ネームが格納されている属性を見つけます。管理者が選択したサーバタイプに応じて、AsyncOS によってデフォルトのクエリーとデフォルトの属性が入力されます。アカウントが失効しているユーザは拒否するようにアプライアンスを設定することもできます。それには、RFC 2307 で規定されている属性が LDAP ユーザ レコード内で定義されている必要があります (shadowLastChange、shadowMax、および shadowExpire)。ユーザ レコードが存在するドメインレベルのベース DN が必須です。

表 22-7 に、AsyncOS がユーザ アカウントを Active Directory サーバ上で検索するとき使用されるデフォルトのクエリー文字列とユーザのフル ネーム属性を示します。

表 22-7 デフォルトのユーザ アカウント クエリー文字列と属性 : Active Directory

サーバタイプ	Active Directory
ベース DN	(ブランク) (ユーザ レコードを見つけるには具体的なベース DN を使用する必要があります)
クエリー文字列	(&(objectClass=user)(sAMAccountName={u}))
ユーザのフル ネームが格納されている属性	displayName

表 22-8 に、AsyncOS がユーザ アカウントを OpenLDAP サーバ上で検索するとき使用されるデフォルトのクエリー文字列とユーザのフル ネーム属性を示します。

表 22-8 デフォルトのユーザ アカウント クエリー文字列と属性 : OpenLDAP

サーバタイプ	OpenLDAP
ベース DN	(ブランク) (ユーザ レコードを見つけるには具体的なベース DN を使用する必要があります)
クエリー文字列	(&(objectClass=posixAccount)(uid={u}))
ユーザのフル ネームが格納されている属性	gecos

グループ メンバーシップ クエリー

AsyncOS は、ユーザが特定のディレクトリ グループのメンバーかどうかを判断するという目的でもクエリーを使用します。ディレクトリ グループ メンバーシップ内のメンバーシップによって、そのユーザのシステム内のアクセス許可が決まります。GUI の [システム管理 (System Administration)] > [ユーザ (Users)] ページ (または CLI の userconfig) で外部認証をイネーブルにするときに、ユーザ ロールを LDAP ディレクトリ内のグループに割り当てます。ユーザ ロールによって、そのユーザがシステム内で持つアクセス許可が決まります。外部認証されたユーザの場合は、ロールは個々のユーザではなくディレクトリ グループに割り当てられます。たとえば、IT というディレクトリ グループ内のユーザに「Administrator」というロールを割り当て、「Support」というディレクトリ グループのユーザに「Help Desk User」というロールを割り当てます。

1 人のユーザが複数の LDAP グループに属しており、それぞれユーザ ロールが異なる場合は、最も限定的なロールのアクセス許可が AsyncOS によってそのユーザに付与されます。たとえば、ユーザが Operator 権限を持つグループと Help Desk User 権限を持つグループに属する場合、AsyncOS はユーザに Help Desk User ロールの権限を割り当てます。

グループ メンバーシップを問い合わせるための LDAP プロファイルを設定するときに、グループ レコードが格納されているディレクトリ レベルのベース DN を入力し、グループ メンバーのユーザ名が格納されている属性と、グループ名が格納されている属性を入力します。LDAP サーバ プロファイルに対して選択されたサーバ タイプに基づいて、ユーザ名とグループ名の属性のデフォルト値とデフォルト クエリー文字列が AsyncOS によって入力されます。



(注)

Active Directory サーバの場合は、ユーザが特定のグループのメンバーかどうかを判断するためのデフォルトのクエリー文字列は (&(objectClass=group)(member={u})) です。ただし、使用する LDAP スキーマにおいて、「memberof」のリストでユーザ名ではなく識別名が使用されている場合は、{dn} を {u} の代わりに使用できます。

表 22-9 に、AsyncOS が Active Directory サーバ上でグループ メンバーシップ情報を検索するときに使用されるデフォルトのクエリー文字列と属性を示します。

表 22-9 デフォルトのグループ メンバーシップ クエリー文字列と属性 : Active Directory

サーバ タイプ	Active Directory
ベース DN	(ブランク) (グループ レコードを見つけるには具体的なベース DN を使用する必要があります)
ユーザが特定のグループのメンバーかどうかを判断するためのクエリー文字列	(&(objectClass=group)(member={u})) (注) 使用する LDAP スキーマにおいて memberOf リストの中でユーザ名ではなく識別名が使用されている場合は、{u} の代わりに {dn} を使用できます。
各メンバーのユーザ名 (またはそのユーザのレコードの DN) が格納されている属性	member
グループ名が格納されている属性	cn

表 22-10 に、AsyncOS が OpenLDAP サーバ上でグループ メンバーシップ情報を検索するときに使用されるデフォルトのクエリー文字列と属性を示します。

表 22-10 デフォルトのグループ メンバーシップ クエリー文字列と属性 : OpenLDAP

サーバ タイプ	OpenLDAP
ベース DN	(ブランク) (グループ レコードを見つけるには具体的なベース DN を使用する必要があります)
ユーザが特定のグループのメンバーかどうかを判断するためのクエリー文字列	(&(objectClass=posixGroup)(memberUid={u}))
各メンバーのユーザ名 (またはそのユーザのレコードの DN) が格納されている属性	memberUid
グループ名が格納されている属性	cn

Cisco IronPort スпам隔離内のエンド ユーザ認証

スパム隔離へのエンドユーザ認証のクエリーとは、ユーザが Cisco スпам隔離機能にログインするときにユーザを検証するためのクエリーです。トークン {u} は、ユーザを示します（ユーザのログイン名を表します）。トークン {a} は、ユーザの電子メール アドレスを示します。LDAP クエリーによって「SMTP:」が電子メール アドレスから除去されることはありません。ただし、AsyncOS はこの部分をアドレスから除去します。

Cisco スпам隔離機能のエンドユーザ アクセス検証に LDAP クエリーを使用するには、[有効なクエリとして指定する (Designate as the active query)] チェックボックスをオンにしてください。すでにアクティブなクエリーがある場合、そのクエリーはディセーブルになります。[システム管理 (System Administration)] > [LDAP] ページを開いたときに、アクティブなクエリーの横にアスタリスク (*) が表示されます。

サーバタイプに基づいて、次のデフォルト クエリー文字列がエンドユーザ認証クエリーに使用されます。

- **Active Directory** : (sAMAccountName={u})
- **OpenLDAP** : (uid={u})
- **Unknown or Other** : (ブランク)

デフォルトでは、プライマリ メール属性は **Active Directory** サーバの場合は proxyAddresses、**OpenLDAP** サーバの場合は mail です。独自のクエリーとメール属性を入力できます。クエリーを CLI で作成するには、ldapconfig コマンドの isqauth サブコマンドを使用します。



(注)

ユーザのログイン時に各自のメール アドレス全体を入力させる場合は、(mail=smtp:{a}) というクエリー文字列を使用します。

スパム隔離機能に対するエンドユーザ認証をイネーブルにする方法については、『Cisco IronPort AsyncOS for Email Daily Management Guide』の「Configuring the Cisco Spam Quarantines Feature」を参照してください。

Active Directory エンドユーザ認証の設定の例

ここでは、Active Directory サーバとエンドユーザ認証クエリーの設定の例を示します。この例では、Active Directory サーバに対してパスワード認証を使用し、メール属性は mail と proxyAddresses を使用し、Active Directory サーバに対するエンドユーザ認証にはデフォルトのクエリー文字列を使用します。

表 22-11 LDAP サーバとスパム隔離へのエンドユーザ認証の設定例 : Active Directory

認証方式	パスワードを使用（検索用にバインドするための低特権のユーザを作成するか、匿名検索を設定する必要があります）
サーバタイプ	Active Directory
ポート	3268
ベース DN	(ブランク)
接続プロトコル	(ブランク)
クエリー文字列	(sAMAccountName={u})
メール属性	mail, proxyAddresses

OpenLDAP エンドユーザ認証の設定の例

ここでは、OpenLDAP サーバとエンドユーザ認証クエリーの設定の例を示します。この例では、OpenLDAP サーバに対して匿名認証を使用し、メール属性は mail と mailLocalAddress を使用し、OpenLDAP サーバに対するエンドユーザ認証にはデフォルトのクエリー文字列を使用します。

表 22-12 LDAP サーバとスパム隔離へのエンドユーザ認証の設定例：OpenLDAP

認証方式	匿名
サーバタイプ	OpenLDAP
ポート	389
ベース DN	(ブランク) (古いスキーマでは具体的なベース DN の使用が要求されることがあります)
接続プロトコル	(ブランク)
クエリー文字列	(uid={u})
メール属性	mail,mailLocalAddress

スパム隔離のエイリアス統合のクエリー

スパム通知を使用する場合は、スパム隔離のエイリアス統合クエリーを使用して電子メール エイリアスを 1 つにまとめると、受信者がエイリアスごとに隔離通知を受け取ることはなくなります。たとえば、ある受信者がメールアドレス john@example.com、jsmith@example.com、および john.smith@example.com のメールを受け取るものとします。エイリアス統合を使用すると、受信者が受け取るスパム通知は 1 通だけとなります。送信先は、このユーザのエイリアスすべてに送信されるメッセージのプライマリ メールアドレスとして選択されたアドレスです。

メッセージを統合してプライマリ メールアドレスに送信するには、受信者の代替メールアドレスを検索するためのクエリーを作成してから、受信者のプライマリ メールアドレスを [メール属性 (Email Attribute)] フィールドに入力します。

Cisco スпам隔離機能のスパム通知に LDAP クエリーを使用するには、[有効なクエリとして指定する (Designate as the active query)] チェックボックスをオンにしてください。すでにアクティブなクエリーがある場合、そのクエリーはディセーブルになります。[システム管理 (System Administration)] > [LDAP] ページを開いたときに、アクティブなクエリーの横にアスタリスク (*) が表示されます。

Active Directory サーバの場合は、デフォルトのクエリー文字列は

(!(proxyAddresses={a})(proxyAddresses=smtp:{a})) で、デフォルトのメール属性は mail です。

OpenLDAP サーバの場合は、デフォルトのクエリー文字列は (mail={a}) で、デフォルトのメール属性は mail です。独自のクエリーとメール属性を定義することもできます。属性が複数の場合は、カンマで区切ります。Cisco では、入力するメール属性が複数ある場合は、最初のメール属性として、変動する可能性のある値を複数持つ属性 (たとえば proxyAddresses) ではなく、値を 1 つだけ使用する一意の属性 (たとえば mail) を入力することを推奨します。

クエリーを CLI で作成するには、ldapconfig コマンドの isqalias サブコマンドを使用します。

Active Directory エイリアス統合の設定の例

ここでは、Active Directory サーバとエイリアス統合クエリーの設定の例を示します。この例では、Active Directory サーバに対して匿名認証を使用し、Active Directory サーバに対するエイリアス統合用のクエリー文字列を指定し、メール属性は mail を使用します。

表 22-13 LDAP サーバとスパム隔離のエイリアス統合の設定例 : Active Directory

認証方式	匿名
サーバタイプ	Active Directory
ポート	3268
ベース DN	(ブランク)
接続プロトコル	Use SSL
クエリー文字列	(!(mail={a})(mail=smtp:{a}))
メール属性	mail

OpenLDAP エイリアス統合の設定の例

ここでは、OpenLDAP サーバとエイリアス統合クエリーの設定の例を示します。この例では、OpenLDAP サーバに対して匿名認証を使用し、OpenLDAP サーバに対するエイリアス統合用のクエリー文字列を指定し、メール属性は mail を使用します。

表 22-14 LDAP サーバとスパム隔離のエイリアス統合の設定例 : OpenLDAP

認証方式	匿名
サーバタイプ	OpenLDAP
ポート	389
ベース DN	(ブランク) (古いスキーマでは具体的なベース DN の使用が要求されることがあります)
接続プロトコル	Use SSL
クエリー文字列	(mail={a})
メール属性	mail

RSA Enterprise Manager の送信者のユーザ識別名の特定

電子メールセキュリティ アプライアンスは、Enterprise Manager に DLP インシデント データを送信する際に、メッセージ送信者の完全な識別名を含める必要があります。Enterprise Manager 送信者名を取得するには、LDAP サーバのユーザ識別名のクエリーを作成して、クエリーを電子メールセキュリティ アプライアンスで発信メッセージを送信するリスナーに追加します。電子メールセキュリティ アプライアンスは RSA Enterprise Manager で DLP が有効になっている場合に限り、このクエリーを使用します。それ以外の場合、サーバ プロファイルのオプションとして表示されません。

ユーザの識別名の設定例

ここでは、Active Directory サーバとエンドユーザ識別名クエリーの設定の例を示します。この例では、Active Directory サーバに対して匿名認証を使用し、Active Directory サーバに対するユーザの識別名検索用のクエリー文字列を指定します。

表 22-15 LDAP サーバとスパム隔離のエイリアス統合の設定例 : Active Directory

認証方式	匿名
サーバタイプ	Active Directory
ポート	3268
ベース DN	(ブランク)
接続プロトコル	Use SSL
クエリー文字列	(proxyAddresses=smtp:{a})

AsyncOS を複数の LDAP サーバと連携させるための設定

LDAP プロファイルを設定するときに、Cisco アプライアンスからの接続先となる複数の LDAP サーバをリストとして設定できます。複数の LDAP サーバを使用するには、LDAP サーバに格納されている情報が同一になるように設定する必要があります。また、構造も同一で、使用する認証情報も同一でなければなりません（レコードを統合できる製品がサードパーティから提供されています）。

冗長化した複数の LDAP サーバに接続するように Cisco アプライアンスを設定すると、LDAP のフェールオーバーまたはロード バランシングを設定できます。

複数の LDAP サーバを使用すると、次のことが可能になります。

- **フェールオーバー。**フェールオーバーのための LDAP プロファイルを設定しておくことで、Cisco アプライアンスが最初の LDAP サーバに接続できなくなったときに、リスト内の次の LDAP サーバへのフェールオーバーが行われます。
- **ロード バランシング。**ロード バランシングのための LDAP プロファイルを設定しておくことで、Cisco アプライアンスが LDAP クエリーを実行するときに、アプライアンスからの接続はリスト内の LDAP サーバに分散されます。

冗長 LDAP サーバを設定するには、[システム管理 (System Administration)] > [LDAP] ページまたは CLI の `ldapconfig` コマンドを使用します。

サーバとクエリーのテスト

[LDAP サーバ プロファイルを追加 (または編集) (Add (or Edit) LDAP Server Profile)] ページの [テスト サーバ (Test Server(s))] ボタン (または CLI の `test` サブコマンド) を使用して、LDAP サーバへの接続をテストします。複数の LDAP サーバを使用する場合は、各サーバのテストが実行されて、各サーバの結果が個別に表示されます。各 LDAP サーバでのクエリーのテストも実行されて、結果が個別に表示されます。

フェールオーバー

LDAP クエリーが確実に解決されるようにするには、フェールオーバーのための LDAP プロファイルを設定します。

アプライアンスは、LDAP サーバ リスト内の最初のサーバへの接続を、所定の時間が経過するまで試行します。Cisco アプライアンスがリスト内の最初の LDAP サーバに接続できない場合は、リスト内の次の LDAP サーバへの接続が試行されます。デフォルトでは、アプライアンスは常にリスト内の最初のサーバへの接続を試行し、それ以降の各サーバへの接続を、リスト内で指定されている順に試行します。Cisco アプライアンスが確実にプライマリの LDAP サーバにデフォルトで接続するようにするには、そのサーバが LDAP サーバ リストの先頭に入力されていることを確認してください。

Cisco アプライアンスが 2 番め以降の LDAP サーバに接続した場合は、タイムアウトの時間に達するまで、そのサーバに接続したままになります。タイムアウトの時間に達すると、リスト内の最初のサーバへの再接続が試行されます。

LDAP フェールオーバーのための Cisco アプライアンスの設定

LDAP フェールオーバーを行うように Cisco アプライアンスを設定するには、GUI で以下の手順を実行します。

手順

ステップ 1 [システム管理 (System Administration)] > [LDAP] ページで、編集する LDAP サーバ プロファイルを選択します。

ステップ 2 LDAP サーバ プロファイルから、次の項目を設定します。

The screenshot shows the 'LDAP Server Settings' window with the following fields and options:

- LDAP Server Configuration Name:** example.com
- Host Name(s):** ldapserver1.example.com, ldapserver2.example.com, ldapserver3.example.com (with a circled 1 next to the label)
- Maximum number of simultaneous connections for all hosts:** 10 (with a circled 2 next to the value)
- Multiple host options:**
 - Load-balance connections among all hosts listed
 - Failover connections in the order listed (with a circled 3 next to the label)

番号	説明
1	LDAP サーバのリストです。
2	最大接続数を設定します。
3	フェールオーバー モードを選択します。

ステップ 3 他の LDAP 設定を指定して変更を確定します。

ロード バランシング

LDAP 接続をグループ内の LDAP サーバ間に分散させるには、ロード バランシングのための LDAP プロファイルを設定します。

ロード バランシングのための LDAP プロファイルを設定しておく、Cisco アプライアンスからの接続はリスト内の LDAP サーバに分散されます。接続に失敗したときやタイムアウトしたときは、Cisco アプライアンスは使用可能な LDAP サーバを判断して、使用可能なサーバに再接続します。Cisco アプライアンスは、管理者が設定した最大同時接続数に基づいて、同時に確立する接続の数を決定します。

リストで指定された LDAP サーバの 1 つが応答しなくなった場合は、Cisco アプライアンスからの接続の負荷は残りの LDAP サーバに分散されます。

ロード バランシングのための Cisco アプライアンスの設定

手順

ステップ 1 [システム管理 (System Administration)] > [LDAP] ページで、編集する LDAP サーバ プロファイルを選択します。

ステップ 2 LDAP サーバ プロファイルから、次の項目を設定します。

The screenshot shows the 'Server Attributes' configuration window. It includes the following fields and options:

- LDAP Server Configuration Name: example.com
- Host Name(s): ldapsrv1.example.com, ldapsrv2.example.com, ldapsrv3.example.com (with a note: 'Separate multiple entries with commas.')
- Maximum number of simultaneous connections for all hosts: 10
- Multiple host options:
 - Load-balance connections among all hosts listed
 - Failover connections in the order listed

番号	説明
1	LDAP サーバのリストです。
2	最大接続数を設定します。
3	ロード バランシング モードを選択します。

ステップ 3 他の LDAP 設定を指定して変更を確定します。



CHAPTER 23

クライアント証明書を使用した SMTP セッションの認証

- 「証明書と SMTP 認証の概要」 (P.23-49)
- 「クライアント証明書の有効性の確認」 (P.23-51)
- 「LDAP ディレクトリを使用したユーザの認証」 (P.23-52)
- 「クライアント証明書を使用した TLS 経由の SMTP 接続の認証」 (P.23-52)
- 「アプライアンスからの TLS 接続の確立」 (P.23-53)
- 「無効にされた証明書のリストの更新」 (P.23-54)

証明書と SMTP 認証の概要

電子メールセキュリティ アプライアンスは、電子メールセキュリティ アプライアンスとユーザのメールクライアント間の SMTP セッションを認証するためにクライアント証明書の使用をサポートします。電子メールセキュリティ アプライアンスは、アプリケーションがメッセージを送信するためにアプライアンスに接続しようとするときに、ユーザのメールクライアントからのクライアント証明書を要求することができます。アプライアンスがクライアント証明書を受け取ったとき、証明書が有効である、有効期限が切れていない、無効になっていないことを確認します。証明書が有効であれば、電子メールセキュリティ アプライアンスは TLS 経由でメール アプリケーションからの SMTP 接続を許可します。

ユーザがメールクライアントに Common Access Card (CAC) を使用する必要がある組織では、CAC および ActivClient のミドルウェア アプリケーションがアプライアンスに提供する証明書を要求するために、この機能を使用して電子メールセキュリティ アプライアンスを設定できます。

メールの送信時にユーザに証明書を提供することを要求するように電子メールセキュリティ アプライアンスを設定できますが、ここでは特定のユーザに対する例外を許可します。これらのユーザには、ユーザの認証に SMTP 認証 LDAP クエリーを使用するようにアプライアンスを設定できます。

ユーザはセキュア接続 (TLS) 経由でメッセージを送信するために自分のメールクライアントを設定し、アプライアンスからサーバ証明書を受け入れる必要があります。

クライアント証明書でのユーザの認証方法

表 23-1 クライアント証明書でのユーザの認証方法

	操作内容	追加情報
ステップ 1	LDAP サーバの認証クエリーを定義します。	「クライアント証明書の有効性の確認」(P.23-51)
ステップ 2	証明書ベースの SMTP 認証プロファイルを作成します。	「クライアント証明書を使用した TLS 経由の SMTP 接続の認証」(P.23-52)
ステップ 3	証明書 SMTP 認証プロファイルを使用するようにリスナーを設定します。	「GUI からのリスナーの作成による接続要求のリスン」(P.5-8)
ステップ 4	TLS、クライアント認証および SMTP 認証を要求するように RELAYED メールフローポリシーを変更します。	「アプライアンスからの TLS 接続の確立」(P.23-53)

SMTP 認証 LDAP クエリーでのユーザの認証方法

表 23-2 SMTP 認証 LDAP クエリーでのユーザの認証方法

	操作内容	追加情報
ステップ 1	許可クエリー文字列と認証方式のバインドを使用する、サーバの SMTP 認証クエリーを定義します。	「LDAP ディレクトリを使用したユーザの認証」(P.23-52)
ステップ 2	LDAP ベースの SMTP 認証プロファイルを作成します。	「SMTP 認証を行うための AsyncOS の設定」(P.22-32)
ステップ 3	LDAP の SMTP 認証プロファイルを使用するようにリスナーを設定します。	ユーザが接続で LDAP ベースの SMTP 認証の使用を許可されていない場合は、アプライアンスが接続拒否するか、すべてのアクティビティを記録する間一時的に許可するかを選択します。
ステップ 4	TLS および SMTP 認証を要求するように RELAYED メールフローポリシーを変更します。	「アプライアンスからの TLS 接続の確立」(P.23-53)

クライアント認証が無効な場合の LDAP SMTP 認証クエリーでのユーザの認証方法

表 23-3 クライアント認証または LDAP SMTP 認証クエリーでのユーザの認証方法

	操作内容	追加情報
ステップ 1	許可クエリー文字列と認証方式のバインドを使用する、サーバの SMTP 認証クエリーを定義します。	「LDAP ディレクトリを使用したユーザの認証」(P.23-52)
ステップ 2	LDAP サーバの認証ベースのクエリーを定義します。	「クライアント証明書の有効性の確認」(P.23-51)
ステップ 3	証明書ベースの SMTP 認証プロファイルを作成します。	「クライアント証明書を使用した TLS 経由の SMTP 接続の認証」(P.23-52)

表 23-3 クライアント認証または LDAP SMTP 認証クエリーでのユーザの認証方法

	操作内容	追加情報
ステップ 4	LDAP の SMTP 認証プロファイルを作成します。	「SMTP 認証を行うための AsyncOS の設定」(P.22-32)
ステップ 5	証明書 SMTP 認証プロファイルを使用するようにリスナーを設定します。	「GUI からのリスナーの作成による接続要求のリッスン」(P.5-8)
ステップ 6	<p>1. 次の設定を使用するように RELAYED メールフローポリシーを変更します。</p> <ul style="list-style-type: none"> • TLS 推奨 • SMTP 認証必須 • SMTP 認証のために TLS が必要 	「アプライアンスからの TLS 接続の確立」(P.23-53)

クライアント証明書の有効性の確認

ユーザのメールクライアントと電子メールセキュリティアプライアンス間の SMTP セッションを認証するために、証明書認証 LDAP クエリーはクライアント証明書の有効性をチェックします。このクエリーを作成する際に、認証のための証明書フィールドのリストを選択して、ユーザ ID 属性（デフォルトは uid）を指定して、クエリー文字列を入力します。

たとえば、証明書の共通名とシリアル番号を検索するクエリー文字列は、
(&(objectClass=posixAccount)(cacn={cn})(cacserial={sn})) のようになります。クエリーを作成した後で、証明書 SMTP 認証プロファイルで使用できます。この LDAP クエリーは、OpenLDAP、Active Directory および Oracle Directory をサポートします。

LDAP サーバの設定の詳細については、第 22 章「LDAP クエリー」を参照してください。

手順

-
- ステップ 1** [システム管理 (System Administration)] > [LDAP] を選択します。
- ステップ 2** 新しい LDAP プロファイルを作成します。詳細については、「LDAP サーバに関する情報を保存する LDAP サーバプロファイルの作成」(P.22-5) を参照してください。
- ステップ 3** [認証クエリーを証明 (Certificate Authentication Query)] チェックボックスをオンにします。
- ステップ 4** クエリー名を入力します。
- ステップ 5** ユーザの証明書を認証するためのクエリー文字列を入力します。たとえば、(&(objectClass=user)(cn={cn})) と入力します。
- ステップ 6** sAMAccountName などのユーザ ID 属性を入力します。
- ステップ 7** 変更内容を送信し、確定します。
-

LDAP ディレクトリを使用したユーザの認証

SMTP 認証 LDAP クエリーには、電子メール セキュリティ アプライアンスがユーザのメール クライアントが LDAP ディレクトリのユーザのレコードに基づいてアプライアンスを介してメール送信できるかを判断する、許可クエリー文字列が含まれています。これは、レコードに許可することが指定してされていれば、クライアントの証明書のないユーザがメールを送信することが可能です。

その他の属性に基づいた結果のフィルタリングもできます。たとえば、`(&(uid={u})(!(caccn=*)) (cacexempt=*) (cacemergercy>={t})))` というクエリー文字列は、次の条件のいずれかがユーザに当てはまるかどうかチェックします。

- CAC がユーザに発行されていない (`caccn=*`)
- CAC が免除される (`cacexempt=*`)
- CAC なしで一時的にユーザがメールを送信できる期間が将来切れる (`cacemergercy>={t}`)

SMTP 認証クエリーの使用の詳細については、「SMTP 認証を行うための AsyncOS の設定」(P.22-32) を参照してください。

手順

-
- ステップ 1** [システム管理 (System Administration)] > [LDAP] を選択します。
 - ステップ 2** LDAP プロファイルを定義します。詳細については、「LDAP サーバに関する情報を保存する LDAP サーバプロファイルの作成」(P.22-5) を参照してください。
 - ステップ 3** LDAP プロファイルの SMTP 認証クエリーを定義します。
 - ステップ 4** [SMTP 認証クエリー (SMTP Authentication Query)] チェックボックスをオンにします。
 - ステップ 5** クエリー名を入力します。
 - ステップ 6** ユーザの ID を問い合わせる文字列を入力します。たとえば、`(uid={u})`。
 - ステップ 7** 認証方式に [LDAP BIND] を選択します。
 - ステップ 8** 許可クエリー文字列を入力します。たとえば、`(&(uid={u})(!(caccn=*)) (cacexempt=*) (cacemergercy>={t})))`。
 - ステップ 9** 変更内容を送信し、確定します。
-

クライアント証明書を使用した TLS 経由の SMTP 接続の認証

証明書ベースの SMTP 認証プロファイルでは、電子メール セキュリティ アプライアンスがクライアント証明書を使用して TLS 経由の SMTP 接続を認証できます。プロファイルを作成する場合、証明書を確認するために使用する証明書認証 LDAP クエリーを選択します。また、クライアント証明書が使用できなかった場合、電子メール セキュリティ アプライアンスがユーザ認証のための SMTP AUTH コマンドにフォールバックするかどうかを指定できます。

LDAP を使用した SMTP 接続の認証の詳細については、「SMTP 認証を行うための AsyncOS の設定」(P.22-32) を参照してください。

手順

- ステップ 1 [ネットワーク (Network)] > [SMTP 認証 (SMTP Authentication)] を選択します。
- ステップ 2 [プロファイルを追加 (Add Profile)] をクリックします。
- ステップ 3 SMTP 認証プロファイルの名前を入力します。
- ステップ 4 [プロファイルタイプ (Profile Type)] で [証明書 (Certificate)] を選択します。
- ステップ 5 [次へ (Next)] をクリックします。
- ステップ 6 プロファイル名を入力します。
- ステップ 7 この SMTP 認証プロファイルに使用する証明書 LDAP クエリーを選択します。



(注) クライアント証明書が使用可能でない場合、SMTP AUTH コマンドを許可するオプションを選択しないでください。

- ステップ 8 [完了 (Finish)] をクリックします。
- ステップ 9 変更内容を送信し、確定します。

アプライアンスからの TLS 接続の確立

RELAYED メールフローポリシーの [クライアント証明書の検証 (Verify Client Certificate)] オプションは、クライアント証明書が有効な場合ユーザのメールアプリケーションへの TLS 接続を確立するように、電子メールセキュリティアプライアンスに指示します。TLS 推奨設定にこのオプションを選択した場合、ユーザが証明書を持たない場合にもアプライアンスは非 TLS 接続を許可しますが、ユーザが無効な証明書を持つ場合は、接続を拒否します。TLS 必須設定の場合、このオプションを選択すると、アプライアンスが接続を許可するために有効な証明書が必要になります。

クライアント証明書を持つユーザの SMTP セッションを認証するには、次の設定を選択します。

- TLS 必須 (TLS - Required)
- クライアント証明書の検証 (Verify Client Certificate)
- SMTP 認証が必要 (Require SMTP Authentication)



(注) SMTP 認証は必須ですが、電子メールセキュリティアプライアンスは証明書認証を使用しているため、SMTP 認証 LDAP クエリーを使用しません。

クライアント証明書の代わりに SMTP 認証クエリーを使用して、ユーザの SMTP セッションを認証するには、次の RELAYED メールフローポリシーの設定を選択します。

- TLS 必須 (TLS - Required)
- SMTP 認証が必要 (Require SMTP Authentication)

他のユーザからの LDAP ベースの SMTP 認証を許可する一方で、特定のユーザからのクライアントの認証を要求するように電子メールセキュリティアプライアンスに要求するには、次の RELAYED メールフローポリシーの設定を選択します。

- TLS 推奨 (TLS - Preferred)
- SMTP 認証が必要 (Require SMTP Authentication)

- TLS に SMTP 認証を提供するよう義務付けます。

無効にされた証明書のリストの更新

電子メールセキュリティアプライアンスは、ユーザの証明書が失効していないことを確認するために、証明書検証の一環として（証明書失効リストと呼ばれる）失効した証明書のリストを確認します。サーバ上でこのリストを最新のバージョンに保ち、電子メールセキュリティアプライアンスはユーザが作成したスケジュールでこれをダウンロードします。

手順

-
- ステップ 1** [ネットワーク (Network)] > [CRL ソース (CRL Sources)] に移動します。
 - ステップ 2** SMTP TLS 接続のため CRL チェックをイネーブルにします。
 - a.** [グローバル設定 (Global Settings)] で [設定を編集 (Edit Settings)] をクリックします。
 - b.** [インバウンド SMTP TLS の CRL チェック (CRL check for inbound SMTP TLS)] チェックボックスをオンにします。
 - c.** (任意) [インバウンド SMTP TLS の CRL チェック (CRL check for inbound SMTP TLS)] チェックボックスをオンにします。
 - d.** 変更を送信します。
 - ステップ 3** [CRL ソースの追加 (Add CRL Source)] をクリックします。
 - ステップ 4** CRL ソースの名前を入力します。
 - ステップ 5** ファイルタイプを選択します。ASN.1 または PEM を指定できます。
 - ステップ 6** ファイル名を含むファイルのプライマリソースの URL を入力します。たとえば、`https://crl.example.com/certs.crl`
 - ステップ 7** アプライアンスがプライマリソースに接続できない場合は、必要に応じて 2 番目のソースの URL を入力します。
 - ステップ 8** CRL ソースをダウンロードするスケジュールを指定します。
 - ステップ 9** CRL ソースをイネーブルにします。
 - ステップ 10** 変更内容を送信し、確定します。
-



CHAPTER 24

FIPS 管理

- 「FIPS 管理の概要」 (P.24-1)
- 「FIPS 管理の概要」 (P.24-1)
- 「アプライアンスの FIPS モードへの切り替え」 (P.24-2)
- 「証明書およびキーの管理」 (P.24-2)
- 「DKIM 署名と検証のキーの管理」 (P.24-3)

FIPS 管理の概要

Federal Information Processing Standard (FIPS ; 連邦情報処理標準) 140 は、米国およびカナダ連邦政府が共同で策定して公式に発表した標準規格です。これは、慎重な扱いを要するにもかかわらず機密扱いでない情報を保護するために、政府機関によって使用される暗号化モジュールの要件を規定しています。Cisco IronPort 電子メール セキュリティ アプライアンスは FIPS 140-2 Level 1 コンプライアンスの達成に CiscoSSL の暗号化ツール キットを使用します。

CiscoSSL の暗号化ツール キットは、OpenSSL の FIS サポートの拡張バージョンと、FIPS 準拠のシスコの共通の暗号化モジュールである Cisco SSL を含む GGSG 承認された暗号化スイートです。シスコの共通の暗号化モジュールは、電子メール セキュリティ アプライアンスが SSH などのプロトコルに対する FIPS 検証済み暗号化アルゴリズムに使用するソフトウェア ライブラリです。

FIPS 管理の概要

電子メール セキュリティ アプライアンスは、アプライアンスが FIPS モードの場合 CiscoSSL と FIPS 準拠の証明書を通信に使用します。詳細については、「[アプライアンスの FIPS モードへの切り替え](#)」 (P.24-2) を参照してください。



(注) FIPS 準拠の一部として、AsyncOS for Email は SSH バージョン 1 をサポートしません。

FIPS レベル 1 に準拠するため、電子メール セキュリティ アプライアンスはお使いの設定に次の変更を行いません。

- **SMTP の受信および配信。** 電子メール セキュリティ アプライアンス のパブリック リスナーとリモート ホスト間の TLS での着信および発信 SMTP カンパセーションは TLS バージョン 1 および FIPS 暗号スイートを使用します。FIPS モードのときは、`sslconfig` を使用してこれらの値は変更できません。TLS v1 は FIPS モードでサポートされる TLS の唯一のバージョンです。

- **Web インターフェイス。**電子メール セキュリティ アプライアンスの Web インターフェイスへの HTTPS セッションに TLS バージョン 1 および FIPS の暗号スイートを使用します。これには、IronPort スпам隔離への HTTPS セッションなど、他の IP インターフェイスが含まれます。FIPS モードのときは、`sslconfig` を使用してこれらの値は変更できません。
- **証明書。**FIPS モードは、アプライアンスに使用される証明書のタイプを制限します。証明書は、次のいずれかのシグニチャ アルゴリズムを使用する必要があります：SHA-1、SHA-224、SHA-256、SHA-384、および SHA-512。アプライアンスは、これらのアルゴリズムのいずれも使用しない証明書はインポートしません。アプライアンスは非準拠の証明書を使用中の場合は FIPS モードにスイッチすることはできません。代わりにエラー メッセージ代わりに表示されます。詳細については、「[証明書およびキーの管理](#)」(P.24-2) を参照してください。
- **DKIM 署名および検証。**DKIM 署名および検証に使用される RSA キーの長さは 1024、1536、2048 ビットである必要があります。アプライアンスは非準拠の RSA キーを使用中の場合は FIPS モードにスイッチすることはできません。代わりにエラー メッセージ代わりに表示されます。DKIM 署名を検証する場合に署名が FIPS 準拠のキーを使用しないと、アプライアンスは永続的な障害を返します。第 24 章「[DKIM 署名と検証のキーの管理](#)」を参照してください。
- **LDAPS。**外部認証用の LDAP サーバを使用するなど、電子メール セキュリティ アプライアンスと LDAP サーバ間の TLS トランザクションは TLS バージョン 1 および FIPS の暗号スイートを使用します。LDAP サーバが MD5 ハッシュを使用してパスワードを保存する場合、SMTP 認証クエリーは MD5 が FIPS 準拠でないため、失敗します。
- **ログ。**SSH2 は SCP 経由のログのプッシュに許可された唯一のプロトコルです。FIPS 管理に関するエラー メッセージについては、INFO レベルの FIPS ログを確認してください。
- **CONSOLE シリアル ポート。**シリアル接続を介して電子メール セキュリティ アプライアンスにアクセスすると、シリアル コンソール ポートへの接続が終了した 30 分でタイムアウトします。
- **中央集中型管理。**クラスタ化されたアプライアンスについては、FIPS モードはクラスタ レベルでしか有効にできません。

アプライアンスの FIPS モードへの切り替え

AsyncOS for Email には FIPS モードにアプライアンスを切り替える `fipsconfig` CLI コマンドが含まれています。アプライアンスを非 FIPS モードに戻す場合にも、`fipsconfig` CLI コマンドを使用します。管理者だけがこのコマンドを使用できます。

アプライアンスは、非 FIPS 準拠の証明書または使用中の DKIM キーがある場合、警告を表示します。これらのキーと証明書を削除するまで、FIPS モードにアプライアンスを切り替えることはできません。

アプライアンスを非 FIPS モードから FIPS モード、または FIPS モードから非 FIPS モードに切り替えた後、再起動が必要になります。

AsyncOS はアプライアンスが FIPS モードの場合、この設定の印刷のみに `sslconfig` コマンドを制限します。

証明書およびキーの管理

AsyncOS では、証明書と秘密キーのペアを使用してアプライアンスと外部のマシン間の通信を暗号化することができます。既存の証明書およびキー ペアをアップロードしたり、自己署名証明書を生成したり、または証明書署名要求 (CSR) を生成して認証局に送信し、公開証明書を取得したりできます。認証局は秘密キーによって署名された信頼できる公開証明書を戻し、それをアプライアンスにアップロードできます。

アプライアンスが FIPS モードの場合は、次に進むことができます。

アプライアンス側 FIPS モードは、アプライアンスが FIPS に準拠するためにアプライアンスが使用する証明書に一定の制限を追加します。証明書は、次のいずれかのシングルチャールゴリズムを使用する必要があります：SHA-1、SHA-224、SHA-256、SHA-384、および SHA-512。

アプライアンスは、これらのアルゴリズムのいずれも使用しない証明書はインポートしません。また、リスナーで使用中の非準拠の証明書が存在する場合、FIPS モードにスイッチすることもできません。代わりにエラー メッセージ代わりに表示されます。

証明書の非 FIPS 状態はアプライアンスが FIPS モードであるときに CLI と GUI の両方に表示されません。リスナーまたは送信先コントロールなどの機能に対して使用する証明書を選択するときに、アプライアンスはオプションとして非準拠の証明書を表示しません。

アプライアンスにおける証明書の使用の詳細については、「[証明書の取得](#)」(P.20-2) を参照してください。

次のいずれかのサービスで FIPS 準拠の証明書を使用できます。

- **SMTP の受信および配信。** TLS を使用して暗号化を必要とするすべてのリスナーに証明書を割り当てるには、[ネットワーク (Network)] > [リスナー (Listeners)] ページ (または listenerconfig -> edit -> certificate の CLI コマンド) を使用します。インターネットに対するリスナーの TLS のみをイネーブルにするか (公開リスナー)、または内部システムを含むすべてのリスナーの暗号化をイネーブルにする (プライベートリスナー) ことができます。
- **送信先コントロール。** 電子メール配信のすべての発信 TLS 接続にグローバル設定として証明書を割り当てるには、[メール ポリシー (Mail Policies)] > [送信先コントロール (Destination Controls)] ページ (または destconfig CLI コマンド) を使用します。
- **インターフェイス。** 管理インターフェイスが含まれるインターフェイスで HTTPS サービスの証明書をイネーブルにするには、[ネットワーク (Network)] > [IP インターフェイス (IP Interfaces)] ページ (または CLI の interfaceconfig コマンド) を使用します。
- **LDAP。** TLS 接続が必要なすべての LDAP トラフィックに証明書を割り当てるには、[システム管理 (System Administration)] > [LDAP] ページを使用します。このアプライアンスでは、ユーザの外部認証の LDAP を使用することもできます。

DKIM 署名と検証のキーの管理

電子メールセキュリティ アプライアンスでの DomainKeys および DKIM の動作の概要については、[第 17 章「電子メール認証」](#) を参照してください。

DKIM: 署名

DKIM 署名キーの作成時に、キー サイズを指定します。FIPS モードの 電子メールセキュリティ アプライアンスでは、1024、1536 および 2048 ビットのキー サイズのみがサポートされます。キー サイズが大きいほどセキュリティが向上しますが、パフォーマンスに影響する可能性があります。

アプライアンスは非準拠の RSA キーを使用中の場合は FIPS モードにスイッチすることはできません。代わりにエラー メッセージ代わりに表示されます。

FIPS 準拠の署名キーはドメイン プロファイルで利用可能です。これは [メール ポリシー (Mail Policies)] > [ドメイン プロファイル (Domain Profiles)] ページを使用してドメイン プロファイルを作成または編集するときに、[署名キー (Signing Key)] のリストに表示されます。署名キーをドメイン プロファイルに関連付けると、公開キーが含まれる DNS テキスト レコードを作成できます。これを行うには、ドメイン プロファイルのリストの [DNS テキスト レコード (DNS Text Record)] 列にある [生成 (Generate)] リンク (または CLI の domainkeysconfig -> profiles -> dnstxt コマンド) を使用します。

DKIM の検証

アプライアンスは、メッセージが DKIM 署名を確認する際に FIPS 準拠キーを使用する必要があります。シグニチャが FIPS 準拠のキーを使用しない場合、アプライアンスは永続的な障害を返します。



CHAPTER 25

メッセージ トラッキング

- 「メッセージ トラッキングの概要」 (P.25-1)
- 「メッセージ トラッキングのイネーブル化」 (P.25-1)
- 「メッセージの検索」 (P.25-2)
- 「メッセージ トラッキングの検索結果の使用」 (P.25-4)
- 「有効なメッセージ トラッキング データの検査」 (P.25-6)

メッセージ トラッキングの概要

メッセージ トラッキングにより、メッセージ フローの詳細なビューを表示することでヘルプ デスク コールを解決に役立ちます。たとえば、メッセージが想定どおりに配信されない場合、ウイルス感染が検出されたか、スパム隔離に入れられたか、あるいはメール ストリーム以外の場所にあるのかを判断できます。

ユーザが指定した基準に一致する特定の電子メール メッセージまたはメッセージのグループを検索できます。



(注) メッセージの内容を読み取るためにメッセージ トラッキングは使用できません。

メッセージ トラッキングのイネーブル化



(注) メッセージ トラッキングのデータは、この機能をイネーブルにした後で処理されたメッセージに対してのみ保持されます。

はじめる前に

- メッセージ トラッキングで添付ファイル名を検索して表示したり、ログ ファイル内の添付ファイル名を表示したりするには、メッセージ フィルタやコンテンツ フィルタなどの本文スキャン プロセスを少なくとも 1 つ設定してイネーブルにする必要があります。
- 件名での検索をサポートするには、ログファイルで件名ヘッダーを記録するように設定する必要があります。詳細については、第 34 章「ロギング」を参照してください。

- 中央集中型トラッキングを設定する場合、次を実行します。
この電子メールセキュリティアプライアンスで中央集中型メッセージトラッキングをサポートするように、セキュリティ管理アプライアンスを設定します。『Cisco Content Security Management Appliance User Guide』を参照してください。

手順

- ステップ 1** [サービス (Services)] > [メッセージトラッキング (Message Tracking)] をクリックします。
- ステップ 2** [メッセージトラッキングサービスを有効にする (Enable Message Tracking Service)] をクリックします。
- ステップ 3** システム設定ウィザードを実行してから初めてメッセージトラッキングをイネーブルにする場合は、エンドユーザライセンス契約書を確認し、[承認 (Accept)] をクリックします。
- ステップ 4** メッセージトラッキングサービスを選択します。

オプション	説明
ローカルトラッキング (Local Tracking)	このアプライアンスでメッセージトラッキングを使用します。
中央集中型トラッキング (Centralized Tracking)	これを含め複数の電子メールセキュリティアプライアンスのメッセージをトレースするためにセキュリティ管理アプライアンスを使用します。

- ステップ 5** (任意) 拒否された接続に関する情報を保存するチェックボックスをオンにします。
最適なパフォーマンスを得るために、この設定を無効にしたままにします。
- ステップ 6** 変更内容を送信し、確定します。

次の作業

ローカルトラッキングを選択した場合、次を実行します。
誰が DLP 違反に関連したコンテンツにアクセスできるかを選択します。「[メッセージトラッキングでの機密情報へのアクセスの制御](#)」(P.28-5) を参照してください。

メッセージの検索

手順

- ステップ 1** [モニタ (Monitor)] > [メッセージトラッキング (Message Tracking)] を選択します。
- ステップ 2** 検索条件を入力します。
- すべてのオプションを表示するには、[詳細 (Advanced)] リンクをクリックします。
 - トラッキングでは、ワイルドカード文字や正規表現はサポートされません。
 - トラッキング検索では大文字と小文字は区別されません。

- 特に指定のない限り、クエリーは「AND」検索です。クエリーは、検索フィールドに指定されたすべての条件に一致するメッセージを返します。たとえば、エンベロープ受信者と件名行のパラメータにテキスト スtring を指定すると、クエリーは、指定されたエンベロープ受信者と件名行の両方に一致するメッセージだけを返します。
- 検索条件は、次のとおりです。

オプション	説明
エンベロープ送信者 (Envelope Sender)	[次で始まる (Begins With)]、[次に合致する (Is)]または[次を含む (Contains)]を選択し、そしてメッセージ送信者を検索するための電子メールアドレス、ユーザ名、ドメインを入力します。 文字を入力できます。エントリの検証は実行されません。
エンベロープ受信者 (Envelope Recipient)	[次で始まる (Begins With)]、[次に合致する (Is)]または[次を含む (Contains)]を選択し、そしてメッセージ受信者を検索するための電子メールアドレス、ユーザ名、ドメインを入力します。 文字を入力できます。エントリの検証は実行されません。
件名 (Subject)	[次で始まる (Begins With)]、[次に合致する (Is)]または[次を含む (Contains)]を選択し、そしてメッセージの件名行で検索するテキスト文字列を入力します。 警告： 規制によりそのようなトラッキングが禁止されている環境では、このタイプの検索を使用しないでください。
受信したメッセージ数 (Message Received)	日時の範囲を指定します。 日付を指定しなければ、クエリーは、すべての日付に対するデータを返します。時間範囲だけを指定すると、クエリーは、すべての利用可能な日付にわたってその時間範囲内のデータを返します。 メッセージが電子メール セキュリティ アプライアンスによって受信された現地日時を使用します。
詳細オプション	
送信者 IP アドレス (Sender IP Address)	リモート ホストの IP アドレスを指定します。 拒否された接続のみまたはすべてのメッセージを検索の範囲で検索できます。
添付ファイル名 (Attachment name)	[次で始まる (Begins With)]、[次に合致する (Is)]または[次を含む (Contains)]を選択し、検索する添付ファイル名の ASCII または Unicode テキスト文字列を入力します。 入力したテキストの先頭および末尾のスペースは除去されません。
メッセージ イベント (Message Event)	1 つ以上のメッセージ処理イベントを選択します。たとえば、配信メッセージ、隔離メッセージ、ハード バウンス メッセージを検索できます。 メッセージ イベントは「OR」演算子を使用して追加されます。複数のイベントを選択して、指定した条件の任意のものと一致するメッセージを検索します。
メッセージ ID ヘッダー (Message ID Header)	SMTP メッセージ ID ヘッダーのテキスト文字列を入力します。 この RFC 822 メッセージ ヘッダーは、各電子メール メッセージを識別します。これは最初にメッセージが作成されるときに挿入されます。
IronPort MID	検索するメッセージ番号を入力します。IronPort MID は電子メール セキュリティ アプライアンスの各電子メール メッセージを識別します。
クエリー設定 (Query Settings)	デフォルトのクエリー タイムアウトおよび返ってくる結果の最大数を変更します。

- ステップ 3** [検索 (Search)] をクリックして、クエリーを送信します。
クエリー結果がページの下部に表示されます。

関連項目

- 「メッセージ トラッキングの検索結果の使用」(P.25-4)

メッセージ トラッキングの検索結果の使用

検索結果を使用する場合に実行できる操作：

- 検索条件に戻って、クエリー設定の [詳細 (Advanced)] をクリックし、[クエリ設定 (Query Settings)] までスクロールし、結果の最大数を 1000 に設定すると、250 件以上の検索結果を表示できます。
- 検索結果セクションの右上でオプションを選択すると、各ページに表示される結果を増やすことができます。
- 検索結果セクションの右上から、複数のページの検索結果内を移動できます。
- 条件として追加する検索結果の値の上でカーソルを移動すると、検索結果を限定できます。オレンジ色で強調表示されている場合は、その値をクリックすると、その条件で検索を絞り込むことができます。これで、検索条件が追加されます。たとえば、特定の受信者に送信されたメッセージを検索した場合は、検索結果で送信者の名前をクリックすると、最初に指定した時間範囲内の（および、その他の条件を満たす）、その送信者からその受信者へのすべてのメッセージを見つけることができます。
- 検索条件に 1000 件以上のメッセージが一致する場合、(検索結果セクションの右上にあるリンク) [すべてエクスポート (Export All)] をクリックし、最大 50,000 件の検索結果をカンマ区切り形式ファイルとしてエクスポートし、他のアプリケーションでデータを使用できます。
- メッセージの行の [詳細の表示 (Show Details)] をクリックすると、メッセージの詳細情報を表示できます。メッセージの詳細を表示した新しいブラウザ ウィンドウが開きます。
- 隔離されたメッセージの場合、メッセージが隔離された理由などの詳細情報を表示するにはメッセージ トラッキングの検索結果のリンクをクリックします。



(注)

レポート ページのリンクをクリックして、メッセージ トラッキングのメッセージ詳細を表示したが、その結果が予期したものでない場合があります。これは、確認している期間中に、レポーティングとトラッキングを同時に継続してイネーブルにしていなかった場合に発生する可能性があります。

メッセージの詳細

項目	説明
[エンベロープとヘッダーのサマリー (Envelope and Header Summary)] セクション	
受信時間 (Received Time)	電子メール セキュリティ アプライアンスがメッセージを受信した時間。 日時は電子メール セキュリティ アプライアンスで設定される現地時間を使用して表示されます。
MID	一義的な IronPort メッセージ ID。

項目	説明
メッセージ サイズ (Message Size)	メッセージ サイズ。
件名 (Subject)	メッセージの件名リスト。 トラッキング結果の件名行は、メッセージの件名がないか、ログ ファイルで件名ヘッダーを記録するよう設定されていない場合、[(件名なし) (No Subject)] という値になる場合があります。詳細については、第 34 章「ロギング」を参照してください。
エンベロープ送信者 (Envelope Sender)	SMTP エンベロープ内の送信者のアドレス。
エンベロープ受信者 (Envelope Recipients)	導入でエイリアス拡張のためのエイリアス テーブルを使用する場合、検索では元のエンベロープ アドレスではなく拡張された受信者アドレスを見つけます。エイリアス テーブルの詳細については、「ルーティングおよび配信機能の設定」の章にある「エイリアス テーブルの作成」の章を参照してください。 それ以外のあらゆる場合においては、メッセージ トラッキング クエリーによって本来のエンベロープ受信者アドレスが検索されます。
メッセージ ID ヘッダー (Message ID Header)	RFC 822 のメッセージ ヘッダー。
SMTP 認証ユーザ ID (SMTP Auth User ID)	送信者が SMTP 認証を使用してメッセージを送信した場合は、SMTP で認証された送信者のユーザ名。それ以外の場合、この値は「N/A」となります。
添付ファイル (Attachments)	メッセージに添付されたファイルの名前。 名前に対してクエリーが実行された少なくとも 1 つの添付ファイルを含むメッセージが検索結果に表示されます。 トラッキングできない添付ファイルもあります。パフォーマンス上の理由から、添付ファイル名のスキューン、メッセージまたはコンテンツ フィルタリング、DLP、免責事項スタンプなどの、他のスキューン操作の一部としてのみ実行されます。添付ファイル名は、添付ファイルがまだ添付されている間に本文スキューンを通過するメッセージに対してのみ使用できます。添付ファイルの名前が検索結果に表示されない状況を含みます (ただし限定はされません)。 <ul style="list-style-type: none"> システムがコンテンツ フィルタのみを使用しているときに、メッセージがドロップされるか、またはその添付ファイルがアンチスパムまたはアンチウイルス フィルタによって削除された場合 本文スキューンが実行される前に、メッセージ分裂ポリシーによって一部のメッセージから添付ファイルが削除された場合 パフォーマンス上の理由から、添付ファイル内のファイルの名前 (たとえば、OLE オブジェクトや、.ZIP ファイルなどのアーカイブ) は検索されません。
[ホスト サマリーの送信 (Sending Host Summary)] セクション	
逆引き DNS ホスト名 (Reverse DNS Hostname)	逆引き DNS (PTR) ルックアップによって検証される送信ホストの名前。
IP アドレス (IP Address)	送信元ホストの IP アドレス。

項目	説明
SBRS スコア (SBRS Score)	SenderBase レピュテーション スコア。範囲は、10（最も信頼できる送信者）～-10（明らかなスパム送信者）です。スコアが「None」の場合、そのメッセージが処理された時点において、このホストに関する情報が存在しなかったことを意味します。 SBRS の詳細については、第 6 章「レピュテーション フィルタリング」を参照してください。
[処理詳細 (Processing Details)] セクション	
サマリー情報 (Summary information) ([サマリー (Summary)] タブは、[DLP に一致した内容 (DLP Matched Content)] タブも存在する場合に限り表示されます。常にサマリー情報を表示します)。	[サマリー (Summary)] セクションでは、メッセージ処理中に記録されるステータス イベントを表示します。 エントリーには、メール ポリシーの処理（アンチスパム スキャンやアンチウイルス スキャンなど）とメッセージ分割などの他のイベントに関する情報、およびコンテンツまたはメッセージ フィルタによって追加されるカスタム ログ エントリーが含まれます。 メッセージが配信された場合、配信の詳細がここに表示されます。 記録された最新のイベントは、処理の詳細内で強調表示されます。
[DLP に一致した内容 (DLP Matched Content)] タブ	このタブは、DLP ポリシーによって検出されたメッセージに対してのみ表示されます。 DLP ポリシーの一致をトリガーした機密のコンテンツに加え、一致に関する情報が含まれます。 誰がこの情報へアクセスできるかを制御できます。「 メッセージ トラッキングでの機密情報へのアクセスの制御 」(P.28-5) を参照してください。

関連項目

- 「[メッセージの検索](#)」(P.25-2)

有効なメッセージ トラッキング データの検査

メッセージ トラッキング データに含まれる日付範囲を確認すること、およびそのデータの欠落インターバルを識別することができます。

-
- ステップ 1** [モニタ (Monitor)] > [メッセージ トラッキング (Message Tracking)] を選択します。
- ステップ 2** 右上隅にある [検索 (Search)] ボックスに表示される [時間範囲内のデータ: (Data in time range:)] を確認します。
- ステップ 3** [時間範囲内のデータ: (Data in time range:)] で示される値をクリックします。
-

メッセージ トラッキングおよびアップグレードについて

新しいメッセージ トラッキング機能は、アップグレードの前に処理されたメッセージには適用できない場合があります。これは、これらのメッセージについては、必須データが保持されていない場合があります。メッセージ トラッキング データおよびアップグレードに関連する制限については、ご使用のリリースのリリース ノートを参照してください。



CHAPTER 26

電子メール セキュリティ モニタの使用方法

- 「電子メール セキュリティ モニタの概要」 (P.26-1)
- 「電子メール セキュリティ モニタ ページ」 (P.26-2)
- 「レポートの概要」 (P.26-44)
- 「レポートの管理」 (P.26-45)
- 「電子メール レポートのトラブルシューティング」 (P.26-48)

電子メール セキュリティ モニタの概要

電子メール セキュリティ モニタ機能は、レピュテーション フィルタリング、アンチスパム、アンチウイルス スキャン、アウトブレイク フィルタ、ポリシーの施行（コンテンツ フィルタ、データ損失防止など）、およびメッセージ配信など、電子メール配信プロセスの各ステップからデータを収集します。データベースは、IP アドレスによる各電子メール送信者の識別と記録を行いつつ、SenderBase レピュテーション サービスと連携してリアルタイムの ID 情報を収集します。ユーザは、すべての電子メール送信者のローカル メール フロー履歴をただちに報告し、インターネット上の送信者のグローバル情報を含むプロファイルを表示できます。電子メール セキュリティ モニタ機能では、セキュリティ チームが、ユーザへのメール送信者、ユーザによって送受信されるメールの量、およびセキュリティ ポリシーの有効性の「ループを閉じる」ことができます。

この章では、次の方法について説明します。

- 発着するメッセージフローをモニタするための電子メール セキュリティ モニタ機能へのアクセス。
- 送信者の SenderBase Reputation Score (SBRS; SenderBase レピュテーション スコア) に対するクエリによる、メール フロー ポリシーの決定（ホワイトリスト、ブラックリスト、およびグレーリストの更新）。ネットワーク オーナー、ドメイン、さらには個別の IP アドレスについてもクエリを実行できます。
- メール フロー、メール ステータスおよびシステムに送受信されたメールに関する報告。

電子メール セキュリティ モニタ データベースでは、着信メールの所定の電子メール送信者について、次の重要パラメータを取得します。

- メッセージの量
- 接続履歴
- 受け入れられた接続と 拒否された接続
- 受け入れ率と調整上限値
- レピュテーション フィルタの一致率

- スパムの疑いのある、および明白にスパムと識別されるアンチスパム メッセージの数
- アンチ ウイルス スキャンによって検出されたウイルス陽性メッセージの数

アンチスパム スキャンの詳細については、第 13 章「アンチスパム」を参照してください。アンチウイルス スキャンについては、第 12 章「アンチウイルス」を参照してください。

電子メール セキュリティ モニタ機能は、内部ユーザ（電子メール受信者）またはメッセージの送信者を含む、特定のメッセージによってトリガーされたコンテンツ フィルタに関する情報も取得します。

電子メール セキュリティ モニタ機能は GUI だけで使用でき、電子メール トラフィックおよびアプライアンス（隔離、ワーク キュー、感染など）のステータスへのビューを提供します。アプライアンスは、送信者が標準のトラフィック プロファイルの範囲に該当しない場合に識別します。識別された送信者はインターフェイスで強調表示されるので、送信者を送信者グループに割り当てるか、送信者のアクセス プロファイルを変更することによって是正措置を取ることができます。または、引き続き AsyncOS のセキュリティ サービスに対応させることができます。送信メールにも同様のモニタリング機能があり、メール キューの上位ドメインおよび受信ホストのステータスにビューを提供します（「[送信処理ステータス詳細 (Delivery Status Details)] ページ」(P.26-20) を参照）。



(注)

電子メール セキュリティ モニタ機能では、アプライアンスの再起動時にワーク キューに存在したメッセージの情報は報告されません。

電子メール セキュリティ モニタと集中管理

このバージョンの AsyncOS では、クラスタ化されたアプライアンスの電子メール セキュリティ モニタ レポートを集約できません。すべてのレポートは、マシン レベルに制限されます。つまりレポートは、グループ レベルまたはクラスタ レベルでは実行できません。個別のマシンのみで実行できます。

[アーカイブ レポート (Archived Reports)] ページについても同様です。設定されている各マシンは、独自のアーカイブを備えています。したがって、「レポート生成」機能は、選択したマシンのみで実行されます。

[定期レポート (Scheduled Reports)] ページは、マシン レベルに制限されません。したがって、複数のマシンで設定を共有できます。マシン レベルで実行された、個別のスケジュール設定されたレポートは、インタラクティブ レポートとまったく同様なので、クラスタ レベルでスケジュール設定されたレポートを設定する場合、クラスタ内の各マシンが独自のレポートを送信します。

[このレポートをプレビュー (Preview This Report)] ボタンは、ログインホストに対して常に実行できます。

電子メール セキュリティ モニタ ページ

電子メール セキュリティ モニタ機能は、[モニタ (Monitor)] メニューで使用可能なすべてのページ（ただし [隔離 (Quarantines)] ページは除く）で構成されます。

GUI でこれらのページを使用して、アプライアンスのリスナーに接続しているドメインをモニタできます。お使いのアプライアンスの「メール フロー」のモニタ、ソート、分析、および分類を実行し、正規メールの大量送信者と「スパマー」（未承諾の商業用メールの大量送信者）またはウイルス送信者の疑いのあるユーザとを区別できます。これらのページは、システムへの着信接続のトラブルシューティングにも役立ちます（SBRS スコア、ドメインに対する直近の送信グループの一致など重要情報を含みます）。

これらのページは、アプライアンスに関連するメール、さらにゲートウェイの範囲を超えて存在するサービス（SenderBase レピュテーション サービス、アンチスパム スキャン サービス、アンチウイルス スキャンセキュリティ サービス、コンテンツ フィルタ、およびアウトブレイク フィルタ）に関連するメールの分類に役立ちます。

ページ右上の [印刷用 PDF (Printable PDF)] リンクをクリックすると、すべての電子メール セキュリティ モニタ ページを読みやすい印刷形式の PDF 版で生成できます。英語以外の言語での PDF の生成については、「[レポートに関する注意事項](#)」(P.26-45) を参照してください。

[エクスポート (Export)] リンクでは、グラフおよび他のデータを Comma Separated Value (CSV; カンマ区切り値) 形式にエクスポートできます。

エクスポートされた CSV データは、電子メール セキュリティ アプライアンスでの設定にかかわらず、すべてのメッセージ トラッキングおよびレポート データを GMT で示します。GMT 時間への変換の目的は、アプライアンスに依存せずにデータを使用したり、複数の時間帯にあるアプライアンスからのデータを参照する際にデータを使用したりできるようにするためです。



(注)

ローカライズされた CSV データをエクスポートする場合、一部のブラウザでは見出しが正しく表示されないことがあります。これは、ローカライズされたテキストに対して、一部のブラウザが適切な文字セットを使用していないためです。この問題を回避するには、ファイルをディスクに保存し、[ファイル (File)] > [開く (Open)] を使用してファイルを開きます。ファイルを開いたら、ローカライズされたテキストを表示するための文字セットを選択します。

レポート データのエクスポートの自動化の詳細については、「[CSV データの取得](#)」(P.26-42) を参照してください。

検索と電子メール セキュリティ モニタ

電子メール セキュリティ モニタ ページの多くには、検索フォームが含まれています。次の 4 種類の項目を検索できます。

- IP アドレス (IPv4 および IPv6)
- ドメイン
- ネットワーク オーナー
- 内部ユーザ
- 宛先ドメイン
- 内部送信者のドメイン
- 内部送信者の IP アドレス
- 発信ドメインの配信ステータス

ドメイン、ネットワーク オーナー、および内部ユーザの検索では、検索テキストに完全に一致させるか、入力したテキストで始まる項目（たとえば、「ex」で始まる場合は「example.com」に一致します）を検索するかを選択します。

IPv4 アドレス検索では、入力したテキストが最大で 4 IP オクテット（ドット付き 10 進表記）の先頭部として常に解釈されます。たとえば「17」と入力すると、17.0.0.0 ~ 17.255.255.255 の範囲が検索されます。17.0.0.1 には一致しますが、172.0.0.1 には一致しません。完全一致検索の場合は、4 オクテットすべてを入力するだけです。IP アドレス検索は、CIDR 形式 (17.16.0.0/12) もサポートしています。

IPv6 アドレス検索では、AsyncOS は次の形式をサポートします。

- 2001:db8:2004:4202::0-2001:db8:2004:4202::ff
- 2001:db8:2004:4202::
- 2001:db8:2004:4202::23
- 2001:db8:2004:4202::/64

すべての検索は、ページで現在選択されている時間範囲に限定されます。

レポートに含まれるメッセージの詳細の表示

手順

-
- ステップ 1** レポート ページのテーブルにある青色の番号をクリックします。
(一部のテーブルにのみ、これらのリンクはあります)。
この番号に関連するメッセージがメッセージ トラッキングで表示されます。
- ステップ 2** 下にスクロールして、リストを表示します。
-

関連項目

- [「メッセージ トラッキングの検索結果の使用」\(P.25-4\)](#)

[マイレポート (My Reports)] ページ

既存のレポートのページからチャート (グラフ) とテーブルを組み合わせ、カスタム レポートページを作成できます。

目的	操作内容
カスタム レポート ページにモジュールを追加します。	<ol style="list-style-type: none"> [モニタ (Monitor)] > [マイ レポート (My Reports)] に移動し、モジュールの右上で [X] をクリックして必要としないサンプル モジュールを削除します。 次のいずれかを実行します。 <ul style="list-style-type: none"> カスタム レポートに追加するには、[モニタ (Monitor)] メニューの下のレポート ページのモジュールにある [マイ レポートに追加 (+ My Reports)] ボタンをクリックします。 [モニタ (Monitor)] > [マイ レポート (My Reports)] に移動し、特定のセクションで [マイ レポートに追加 (+ My Reports)] ボタンをクリックし、追加するレポート モジュールを選択します。検索しているレポートを表示するには、各セクションで [レポート モジュールに追加 (+ Report Module)] をチェックする必要があります。 モジュールがデフォルト設定に追加されます。ユーザがカスタマイズした (たとえば、カラムの追加、削除、または順序変更をした) モジュールを追加した場合は、追加した後これらのモジュールを再度カスタマイズします。元のモジュールの時間範囲は保持されません。 別に凡例を持つチャート (たとえば、[概要 (Overview)] ページからのグラフ) を追加する場合は、別途凡例を追加します。必要に応じて、説明するデータの隣にドラッグ アンド ドロップします。 <p>注 :</p> <ul style="list-style-type: none"> 特定のレポート ページの特定のモジュールは、上記の方法のいずれかを使用した場合のみ使用できます。ある方式を使用してモジュールを追加できない場合は、他の方法を試してください。 カスタム レポート レポートには、次のモジュールは追加できません。 <ul style="list-style-type: none"> アウトブレイク フィルタ レポート ページの [過去 1 年間のウイルス アウトブレイク サマリー (Past Year Virus Outbreak Summary)] チャートおよび [過去 1 年間のウイルス アウトブレイク (Past Year Virus Outbreaks)] テーブル すべてのレポートの検索結果 各モジュールは一度だけ追加できます。すでに特定のモジュールをレポートに追加している場合は、追加オプションが利用できなくなっています。
カスタム レポート ページの表示	<ol style="list-style-type: none"> [モニタ (Monitor)] > [マイ レポート (My Reports)] を選択します。 [時間範囲 (Time Range)] セクションのレポートの場合 : すべてのレポートのページ用に選定された時間範囲は [マイレポート (My Reports)] ページのすべてのモジュールに適用されます。表示する時間範囲を選択します。 <p>新しく追加されたモジュールは関連するセクションの上部に表示されます。</p>
カスタム レポート ページでのモジュールの再配置	目的の場所にモジュールをドラッグ アンド ドロップします。
カスタム レポート ページからのモジュールの削除	モジュールの右上にある [X] をクリックします。

[概要 (Overview)] ページ

[概要 (Overview)] ページには、隔離および (このページの [システム概要 (System Overview)] セクションの) アウトブレイク フィルタのステータスの概要などお使いのアプリアンスのメッセージ アクティビティの概要が示されます。[概要 (Overview)] ページには、グラフや、送受信メッセージの詳細なメッセージ数も表示されます。このページを使用して、ゲートウェイから出入りするすべての

メールのフローをモニタできます。送受信メールの [サマリー詳細 (Summary Detail)] では、クリーン、Stopped By Reputation Filtering (SBRS)、無効な受信者として停止、スパム検出、ウイルス検出、コンテンツ フィルタによる停止、および「クリーン」と見なされるメッセージに分類されたメッセージの数と割合が示されます。

[概要 (Overview)] ページは、アプライアンスが、着信メール (たとえば、レピュテーション フィルタリングによって停止されたメッセージ) に関して SenderBase レピュテーション サービスと連携する方法を強調表示します。[概要 (Overview)] ページでは、次の操作を実行できます。

- ゲートウェイを「出入り」するすべてのメールのメールトレンド グラフを表示する。
- 試行されたメッセージ、Stopped By Reputation Filtering (SBRS) メッセージ、受信者が無効なメッセージ、スパムとしてマークされたメッセージ、ウイルス陽性としてマークされたメッセージ、およびクリーン メッセージの数を経時的に表示する。
- システム ステータスおよびローカル隔離のサマリーを表示する。
- Threat Operations Center (TOC) で入手可能な情報に基づいて、現在のウイルスの発生情報やウイルス以外の発生情報を確認する。

[概要 (Overview)] ページは、[システム概要 (System Overview)] セクションおよび送受信メールのグラフとサマリーのセクションの 2 つに分かれています。

システム概要 (System Overview)

[概要 (Overview)] ページの [システム概要 (System Overview)] セクションは、システム ダッシュボードとして機能し、システムおよびワーク キュー ステータス、隔離ステータス、発生アクティビティなどのアプライアンスに関する詳細を示します。

ステータス (Status)

このセクションでは、アプライアンスおよび着信メール処理の現在のステータスの概要が示されます。

[システム ステータス (System Status)] : 次のいずれかの状態です。

- オンライン (Online)
- リソース保護 (Resource Conservation)
- 配信停止 (Delivery Suspended)
- 受信停止 (Receiving Suspended)
- ワーク キュー一時停止 (Work Queue Paused)
- オフライン (Offline)

詳細については、第 30 章「CLI による管理およびモニタリング」を参照してください。

[受信メッセージ (Incoming Messages)] : 1 時間あたりの着信メールの平均レート。

[ワーク キュー (Work Queue)] : ワーク キュー内の処理待ちメッセージの数。

[システム ステータス (System Status)] ページに移動するには、[システム ステータス詳細 (System Status Details)] リンクをクリックします。

システム隔離 (System Quarantines)

このセクションには、アプライアンスでのディスク使用量別の上位 3 つの隔離に関する情報 (隔離の名前、隔離の使用度 (ディスク領域)、現在の隔離エリア内のメッセージ数など) が表示されます。


[内部隔離 (Local Quarantines)] ページに移動するには、[内部隔離 (Local Quarantines)] リンクをクリックします。

ウイルス脅威レベル (Virus Threat Level)

ここでは、Threat Operations Center (TOC) から報告される、Outbreak のステータスを示します。また、隔離の使用度 (ディスク領域)、隔離内のメッセージ数など、アウトブレイク隔離のステータスを示します。アウトブレイク隔離は、アプライアンスでアウトブレイク フィルタ機能をイネーブルに設定した場合のみ表示されます。





(注) 脅威レベル インジケータを機能させるためには、ファイアウォールで「downloads.ironport.com」に対してポート 80 を開く必要があります。あるいは、ローカル更新サーバを指定した場合は、脅威レベル インジケータがそのアドレスを使用します。また、[サービスのアップデート (Service Updates)] ページを使用してダウンロード用のプロキシを設定済みの場合、脅威レベル インジケータは、正しくアップデートされます。詳細については、「サービスのアップデート」(P.29-22) を参照してください。

外部 Threat Operations Center ウェブ サイトを表示するには、[アウトブレイクの詳細 (Outbreak Details)] をクリックします。このリンクを機能させるには、お使いのアプライアンスでインターネットに接続する必要があります。[個別のウィンドウ (Separate Window)] アイコン () は、クリックすると別個のウィンドウにリンクが開かれることを示します。これらのウィンドウを表示できるようにするには、ブラウザのポップアップ ブロックを設定する必要があります。

送受信のサマリーとグラフ

送受信のサマリーのセクションでは、システム上のすべてのメール アクティビティのリアルタイム アクティビティへのアクセスが提供され、送受信メールのグラフとメール サマリーで構成されています。ユーザは、[時間範囲 (Time Range)] メニューを使用して報告対象となるタイムフレームを選択できます。選択したタイムフレームは、すべての電子メール セキュリティ モニタ ページで使用されます。メッセージの各タイプまたはカテゴリに関する説明は以下のとおりです (「電子メールの分類」(P.26-8) を参照)。

メール トレンド グラフ (左側、 26-1) では、リアルタイムでの着信メールの分析結果が示されます。

メール トレンド グラフでは、メール フローが視覚的に表示されますが、サマリー テーブル (右側、 26-1) では、同じ情報の数値的な内訳が示されます。サマリー テーブルには、各メッセージタイプの割合と実数 (試行されたメッセージ、脅威メッセージ、クリーン メッセージの総数を含む) が含まれています。

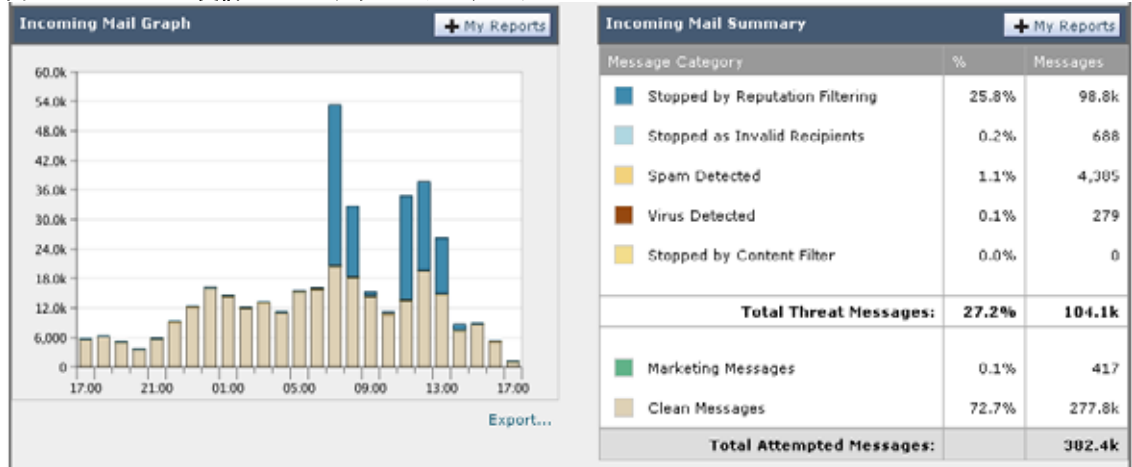
送信グラフおよびサマリーでも、送信メールに関する同様の情報が示されます。

電子メール セキュリティ モニタでのメッセージ集計に関する注意事項

電子メール セキュリティ モニタが着信メールの集計に使用する方法は、メッセージあたりの受信者の数によって異なります。たとえば、example.com から 3 人の受信者に送信された着信メッセージは、この送信者からの 3 通として集計されます。

レピュテーション フィルタによってブロックされたメッセージは、実際にはワーク キューに入らないので、アプライアンスは、着信メッセージの受信者のリストにはアクセスできません。この場合、乗数を使用して受信者の数が予測されます。この乗数はシスコによって算出されたもので、既存の顧客データの大規模なサンプリング研究に基づいています。

図 26-1 受信メールのグラフとサマリー テーブル



電子メールの分類

[概要 (Overview)] ページおよび [受信メール (Incoming Mail)] ページで報告されるメッセージは、次のように分類されます。

[レピュテーション フィルタによる停止 (Stopped by Reputation Filtering)] : HAT ポリシーによってブロックされたすべての接続数に固定乗数 (「電子メールセキュリティ モニタでのメッセージ集計に関する注意事項」(P.26-7) を参照) を乗じた値に受信調整によってブロックされたすべての受信者数を加えた値。

[無効な受信者 (Invalid Recipients)] : 従来の LDAP 拒否によって拒否されたすべての受信者数にすべての RAT 拒否数を加えた値。

[スパム メッセージ検出 (Spam Messages Detected)] : アンチスパム スキャン エンジンで陽性、または疑いありとして検出されたメッセージ、およびスパムとウイルスの両方で陽性と検出されたメッセージの総数。

[ウイルス メッセージ検出 (Virus Messages Detected)] : ウイルス陽性だがスパムではないと検出されたメッセージの総数および割合。



(注)

スキャンできないメッセージまたは暗号化されたメッセージを配信するようにアンチウイルス設定を行った場合、これらのメッセージは、ウイルス陽性としてではなく、クリーン メッセージとして集計されます。それ以外の場合は、メッセージはウイルス陽性として集計されます。

[コンテンツ フィルタによる停止 (Stopped by Content Filter)] : コンテンツ フィルタによって阻止されたメッセージの総数。

[マーケティングメッセージ (Marketing Messages)] : アンチスパム スキャンで決定された、問題のない送信元からのマーケティング メッセージの総数。この項目は、マーケティング データがシステムにある場合に限り表示されます。

[正常なメッセージ (Clean Messages)] : 受け入れられ、ウイルスでもスパムでもないと思われたメール。受信者単位のスキャンアクション (個々のメール ポリシーで処理される分裂したメッセージなど) を考慮したときに受信されたクリーン メッセージを最も正確に表したものです。ただし、ウイルス陽性またはスパム陽性としてマークされたにもかかわらず配信されたメッセージは集計されないの、実際のメッセージの配信数と、このクリーン メッセージの数は異なる可能性があります。



(注)

メッセージフィルタに一致し、フィルタによってドロップされたり、バウンスされたりしないメッセージは、クリーンとして処理されます。メッセージフィルタによってドロップされたか、バウンスされたメッセージは、総数に含まれません。

メッセージの分類方法

メッセージは電子メールパイプラインを通過するので、複数のカテゴリに該当する場合があります。たとえば、スパム陽性またはウイルス陽性とマークされたメッセージが、コンテンツ フィルタにも一致することがあります。これらの優先ルールに続いて、アウトブレイク フィルタによる隔離（この場合、メッセージが隔離から解放されるまで集計されず、ワーク キューによる処理が再び行われます）の次にスパム陽性、ウイルス陽性、および一致するコンテンツ フィルタなどさまざまな判定が行われます。

たとえば、メッセージがスパム陽性とマークされると、アンチスパム設定がスパム陽性のメッセージをドロップするように設定されている場合には、このメッセージがドロップされ、スパム カウンタが増分します。さらに、スパム陽性のメッセージを引き続きパイプラインで処理し、以降のコンテンツ フィルタがこのメッセージをドロップ、バウンス、または隔離するようにアンチスパム設定が設定されている場合にも、スパム カウンタは増分します。メッセージがスパム陽性またはウイルス陽性ではない場合、コンテンツ フィルタ カウントが増分するだけです。

[受信メール (Incoming Mail)] ページ

[受信メール (Incoming Mail)] ページでは、お使いのアプライアンスに接続するすべてのリモートホストの電子メールセキュリティ モニタ機能によって収集されたリアルタイム情報に関して報告を行うメカニズムが提供されます。これにより、メール送信者の IP アドレス、ドメイン、および組織（ネットワーク オーナー）に関する詳細を収集できます。メール送信者の IP アドレス、ドメイン、組織については、送信者プロフィール検索を実行できます。

[受信メール (Incoming Mail)] ページには、[ドメイン (Domain)]、[IP アドレス (IP Address)]、および [ネットワーク所有者 (Network Owner)] の 3 種類のビューが用意されており、システムに接続するリモートホストのスナップショットが選択したビューで提供されます。

アプライアンスで設定済みのすべてのパブリック リスナーにメールを送信した上位ドメイン（ビューに応じて、IP アドレスまたはネットワーク オーナー）の表（[受信メールの詳細 (Incoming Mail Details)]）が表示されます。ゲートウェイに入ったすべてのメールのフローをモニタできます。任意のドメイン/IP/ネットワーク オーナーをクリックしてドリルダウンし、送信者プロフィール ページ（クリックしたドメイン/IP/ネットワーク オーナーに固有の [受信メール (Incoming Mail)] ページ）のこの送信者に関する詳細にアクセスできます。

[受信メール (Incoming Mail)] は、一連のページ（[受信メール (Incoming Mail)]、送信者プロフィール、および送信者グループ レポート）を含むように拡張することもできます。[受信メール (Incoming Mail)] ページでは、次の操作を実行できます。

- メール送信者の IP アドレス、ドメイン、または組織（ネットワーク オーナー）に関する検索を実行する。
- 送信者グループ レポートを表示して、特定の送信者グループおよびメール フロー ポリシー アクションによる接続を確認する。詳細については、「[送信者グループ レポート](#)」(P.26-16) を参照してください。
- 試行されたものの、セキュリティ サービス（レピュテーション フィルタリング、アンチスパム、アンチウイルスなど）によってブロックされたメッセージの数など、メール送信者に関する詳細な統計情報を確認する。

- アンチスパムまたはアンチウイルス セキュリティ サービスによって測定される、大量のスパムまたはウイルス電子メールを送信した送信者別にソートする。
- SenderBase レピュテーション サービスを使用して特定の IP アドレス、ドメイン、および組織の間関係のドリルダウンと分析を行い、送信者に関する詳細を取得する。
- 特定の送信者をドリルダウンして、送信者の SenderBase レピュテーション スコア、ドメインが直近に一致した送信者グループなど SenderBase レピュテーション サービスから送信者に関する詳細を取得する。送信者を送信者グループに追加する。
- アンチスパムまたはアンチウイルス セキュリティ サービスによって測定される、大量のスパムまたはウイルス電子メールを送信した特定の送信者をドリルダウンする。
- ドメインに関する情報を収集したら、(必要に応じて) ドメイン、IP アドレス、またはネットワーク オーナーのプロファイル ページから [送信者グループに追加 (Add to Sender Group)] をクリックして、既存の送信者グループに IP アドレス、ドメイン、または組織を追加できます。「[電子メールを受信するためのゲートウェイの設定](#)」(P.5-1) を参照してください。

受信メール

[受信メール (Incoming Mail)] ページでは、システムで設定済みのすべてのパブリック リスナーのリアルタイム アクティビティへのアクセスが提供され、受信数の上位ドメイン (脅威メッセージの総数別およびクリーン メッセージの総数別) および [受信メールの詳細 (Incoming Mail Details)] リストという 2 つのセクションで構成されます。

図 26-2 着信メールのグラフ：脅威メッセージの総数およびクリーン メッセージの総数

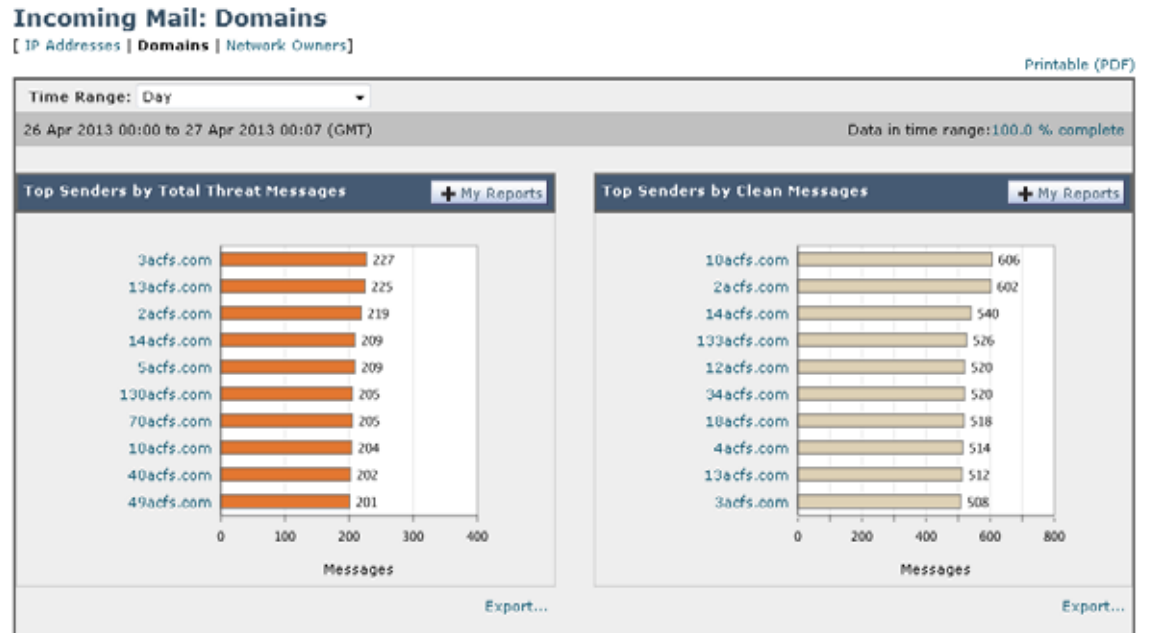


図 26-3 Incoming Mail Details

Incoming Mail Details + My Reports

Items Displayed: 10

Sender Domain	Total Attempted	Stopped by Reputation Filtering (?)	Stopped as Invalid Recipients	Spam Detected	Virus Detected	Stopped by Content Filter	Total Threat	Clean
10acfs.com	810	0	32	140	0	32	204	606
2acfs.com	821	0	35	144	0	40	219	602
14acfs.com	749	0	41	130	0	38	209	540
133acfs.com	705	0	29	126	0	24	179	526
12acfs.com	711	0	35	118	0	38	191	520
34acfs.com	697	0	31	124	0	22	177	520
18acfs.com	711	0	23	134	0	36	193	518
4acfs.com	702	0	32	118	2	36	188	514
13acfs.com	737	0	27	156	0	42	225	512
3acfs.com	735	0	49	144	0	34	227	508

Columns... | Export...

[受信メールの詳細 (Incoming Mail Details)] リストに含まれるデータの説明については、「[受信メールの詳細 (Incoming Mail Details)] リスト」(P.26-12) を参照してください。

メールトレンドグラフにおける時間範囲に関する注意事項

電子メールセキュリティ モニタ機能は、ゲートウェイに流入するメールに関するデータを常に記録します。データは 60 秒ごとに更新されますが、システムに表示されるデータは、現在のシステム時間よりも 120 秒遅れます。表示される結果に含める時間範囲を指定できます。データはリアルタイムでモニタリングされているので、情報は定期的に更新され、データベースで集計されます。

表 26-1 の時間範囲オプションから選択します。

表 26-1 電子メール セキュリティ モニタ機能で使用可能な時間範囲

GUI で選択した時間範囲	定義
時 (Hour)	直近の 60 分 + 最大 5 分
日 (Day)	直近の 24 時間と直近の 60 分
週 (Week)	直近の 7 日 + 当日の経過した時間
30 日 (30 days)	直近の 30 日 + 当日の経過した時間
90 日 (90 days)	直近の 90 日 + 当日の経過した時間
昨日 (Yesterday)	00:00 ~ 23:59 (午前 0 時 ~ 午後 11:59)
先月 (Previous Calendar Month)	その月の最初の日の 00:00 ~ その月の最後の日の 23:59
カスタム範囲 (Custom Range)	指定した開始の日付と時間および終了の日付と時間で囲まれた範囲

集中化レポートをイネーブルにしていると、表示される時間範囲オプションが異なります。集中管理レポート モードの詳細については、第 38 章「Cisco コンテンツ セキュリティ管理アプライアンスの集中型サービス」を参照してください。

[受信メールの詳細 (Incoming Mail Details)] リスト

アプライアンスのパブリック リスナーに接続した上位送信者が、[受信メール (Incoming Mail)] ページの下部にある受信された外部ドメイン リストの表に選択したビューで表示されます。データをソートするには、カラム見出しをクリックします。各種のカテゴリの説明については、「電子メールの分類」(P.26-8) を参照してください。

ダブル DNS ルックアップの実行によって、リモート ホストの IP アドレス (つまり、ドメイン) が取得され、有効性が検証されます。ダブル DNS ルックアップおよび送信者検証の詳細については、「電子メールを受信するためのゲートウェイの設定」(P.5-1) を参照してください。

送信者の詳細のリストには、[サマリー (Summary)] と [すべて (All)] の 2 つのビューがあります。

デフォルトの [送信者の詳細 (Sender Detail)] ビューでは、各送信者が試行したメッセージの総数が示され、カテゴリ別の内訳が含まれます。カテゴリは、[概要 (Overview)] ページの [受信メール サマリー (Incoming Mail Summary)] グラフと同じ (クリーン メッセージ、レピュテーションフィルタリングによる阻止、無効な受信者、スパムを検出、コンテンツ フィルタ、およびマーケティング メッセージによる阻止の数) です。また、脅威メッセージ (レピュテーションによって阻止されたメッセージや、無効な受信者、スパム、およびウイルスとして阻止されたメッセージ) の総数も示されます。

[レピュテーション フィルタによる停止 (Stopped by Reputation Filtering)] の値は、次の複数の要素に基づいて算出されます。

- この送信者からの「調整された」メッセージの数
- 拒否されたまたは TCP 拒否の接続数 (部分的に集計されます)
- 接続あたりのメッセージ数に使用される、保守的に見積もった乗数

アプライアンスに重い負荷がかけられている場合、拒否された接続の正確な数を送信者別に維持できません。その代わりに、拒否された接続の数は、各時間間隔で最も顕著だった送信者についてのみ維持されます。この場合、表示される値は「下限」、つまり少なくともこの数のメッセージが阻止されたと解釈できます。

**(注)**

[概要 (Overview)] ページの [レピュテーション フィルタによる停止 (Stopped by Reputation Filtering)] の総数は、すべての拒否された接続の完全な集計値に常に基づいています。送信者別の接続数だけが、負荷のために常に限定的です。

表示できる追加のカラムは次のとおりです。

[接続拒否 (Connections Rejected)] : HAT ポリシーによってブロックされたすべての接続。アプライアンスに重い負荷がかけられている場合、拒否された接続の正確な数を送信者別に維持できません。その代わりに、拒否された接続の数は、各時間間隔で最も顕著だった送信者についてのみ維持されます。

[接続承認 (Connections Accepted)] : 受け入れられたすべての接続。

[受信者スロットルによる停止 (Stopped by Recipient Throttling)] : [レピュテーション フィルタによる停止 (Stopped by Reputation Filtering)] のコンポーネントです。HAT 上限値 (1 時間当たりの最大受信者数、メッセージあたりの最大受信者数、または接続あたりの最大メッセージ数) のいずれかを越えたために、阻止された受信メッセージの数を表します。この値と、拒否されたか、TCP 拒否の接続に関連する受信メッセージの予測値とが合計されて、[レピュテーション フィルタによる停止 (Stopped by Reputation Filtering)] が算出されます。

テーブルの下部にある [列 (Column)] リンクをクリックすると、カラムの表示/非表示が切り替わります。

このリストは、カラム見出しリンクをクリックするとソートされます。カラム見出しの横にある小さな三角形は、データの現在のソートに使用されているカラムを示します。

[合計脅威件数 (Total Threat)] : (レピュテーションにより阻止された、無効な受信者、スパム、およびウイルスとして阻止された) 脅威メッセージの総数

「ドメイン情報がありません (No Domain Information)」

アプライアンスに接続したものの、ダブル DNS ルックアップで検証できなかったドメインは、専用ドメイン [ドメイン情報がありません (No Domain Information)] に自動的に分類されます。これらの種類の検証されないホストは、送信者の検証によって管理できます。「[電子メールを受信するためのゲートウェイの設定](#)」(P.5-1) を参照してください。

リストに表示される送信者の数は、[表示された項目 (Items Displayed)] メニューから選択できます。

詳細の問い合わせ

電子メール セキュリティ モニタのテーブルに表示された送信者については、その送信者 (または [ドメイン情報がありません (No Domain Information)] リンク) をクリックして特定の送信者に関する詳細をドリルダウンします。結果は送信者プロファイル ページに表示され、SenderBase レピュテーション サービスからのリアルタイム情報が含まれます。送信者プロファイル ページからは、特定の IP アドレスまたはネットワーク オーナーに関する詳細をドリルダウンできます。「[データが読み込まれる報告ページ : 送信者プロファイル ページ](#)」(P.26-13) を参照。

[受信メール (Incoming Mail)] ページの下部にある [送信者グループのレポート (Sender Groups Report)] リンクをクリックして、別のレポート (送信者グループ レポート) を表示することもできます。送信者グループ レポートの詳細については、「[送信者グループ レポート](#)」(P.26-16) を参照してください。

データが読み込まれる報告ページ : 送信者プロファイル ページ

[受信メール (Incoming Mail)] ページにある [受信メールの詳細 (Incoming Mail Details)] テーブルをクリックすると、その結果として [送信者プロファイル ページ](#) が表示されます。このページには、特定の IP アドレス、ドメイン、または組織 (ネットワーク オーナー) のデータが含まれています。送信

者プロフィール ページには、送信者の詳細情報が示されます。任意のネットワーク オーナーまたは IP アドレスの送信者プロフィール ページは、[受信メール (Incoming Mail)] ページまたは他の送信者プロフィール ページで特定の項目をクリックしてアクセスできます。ネットワーク オーナーは、ドメインを含むエンティティであり、ドメインは、IP アドレスを含むエンティティです。この関係および SenderBase レピュテーション サービスとの関係の詳細については、「[電子メールを受信するためのゲートウェイの設定](#)」(P.5-1) を参照してください。

IP アドレス、ネットワーク オーナーおよびドメインに関して表示される送信者プロフィール ページは、多少異なります。それぞれのページには、この送信者からの着信メールに関するグラフおよびサマリー テーブルが含まれます。グラフの下には、この送信者に関連するドメインまたは IP アドレスを表示する表 (個々の IP アドレスの送信者プロフィール ページには、詳細なリストは含まれません)、およびこの送信者の現在の SenderBase 情報、送信者グループ情報、およびネットワーク 情報を含む情報 セクションがあります。

- ネットワーク オーナー プロフィール ページには、ネットワーク オーナー、およびこのネットワーク オーナーに関連するドメインや IP アドレスに関する情報が含まれます。
- ドメイン プロフィール ページには、このドメインおよびこのドメインに関連する IP アドレスに関する情報が含まれます。
- IP アドレス プロフィール ページには、IP アドレスのみに関する情報が含まれます。

各送信者プロフィール ページには、ページの下部の現在の情報テーブルに次のデータが含まれます。

- SenderBase レピュテーション サービスからの**グローバル**情報。たとえば、次の情報です。
 - IP アドレス、ドメイン名、またはネットワーク オーナー
 - ネットワーク オーナーのカテゴリ (ネットワーク オーナーのみ)
 - CIDR 範囲 (IP アドレスのみ)
 - IP アドレス、ドメイン、またはネットワーク オーナーの日単位マグニチュードおよび月単位マグニチュード
 - この送信者から最初のメッセージを受信してからの日数
 - 最後の送信者グループと DNS が検証されたかどうか (IP アドレス送信者プロフィール ページのみ)

日単位マグニチュードは、直近 24 時間にドメインが送信したメッセージの数の基準です。地震の測定に使用されるリヒター スケールと同様に、SenderBase マグニチュードは、10 を基数とする対数目盛を使用して算出されるメッセージの量の基準です。目盛の最大理論値は 10 に設定されます。これは、世界の電子メール メッセージの量 (約 100 億メッセージ/日) に相当します。対数目盛を使用した場合、1 ポイントのマグニチュードの増加は、実際の量の 10 倍の増加に相当します。

月単位マグニチュードは、直近 30 日間に送信された電子メールの量に基づいて割合が算出される点を除いて、日単位マグニチュードと同じ方法を使用して算出されます。

- 平均マグニチュード (IP アドレスのみ)
- 総累積量/30 日の量 (IP アドレス プロフィール ページのみ)
- Bonded Sender ステータス (IP アドレス プロフィール ページのみ)
- SenderBase レピュテーション スコア (IP アドレス プロフィール ページのみ)
- 最初のメッセージからの日数 (ネットワーク オーナー プロフィール ページおよびドメイン プロフィール ページのみ)
- このネットワーク オーナーに関連するドメインの数 (ネットワーク オーナー プロフィール ページおよびドメイン プロフィール ページのみ)
- このネットワーク オーナーの IP アドレスの数 (ネットワーク オーナー プロフィール ページおよびドメイン プロフィール ページのみ)

- 電子メールの送信に使用された IP アドレスの数 (ネットワーク オーナー ページのみ)

SenderBase レピュテーション サービスによって提供されるすべての情報を示すページを表示するには、[SenderBase からの詳細情報 (More from SenderBase)] リンクをクリックします。

- メールフロー統計情報。送信者について収集された、指定した時間範囲にわたる電子メール セキュリティ モニタ情報を含みます。
- このネットワーク オーナーによって管理されるドメインおよび IP アドレスに関する詳細は、ネットワーク オーナー プロファイル ページに表示されます。ドメイン内の IP アドレスに関する詳細は、ドメイン ページに表示されます。

ドメイン プロファイル ページから特定の IP アドレスをドリルダウンするか、ドリルアップして組織プロフィール ページを表示できます。また、そのテーブルの下部にある [列 (Columns)] リンクをクリックすることにより、[IP アドレス (IP Addresses)] テーブル内の送信者アドレスごとの [DNS 検証 (DNS Verified)] ステータス、SBR (SenderBase レピュテーション スコア)、および [最新の送信者グループ (Last Sender Group)] を表示することもできます。そのテーブル内の任意のカラムを非表示にすることもできます。

ネットワーク オーナー プロファイル ページから、そのテーブルの下部にある [列 (Columns)] リンクをクリックすることにより、[ドメイン (Domains)] テーブル内のドメインごとの [接続拒否 (Connections Rejected)]、[接続承認 (Connections Accepted)]、および [受信者スロットルによる停止 (Stopped by Recipient Throttling)] 情報を表示できます。そのテーブル内の任意のカラムを非表示にすることもできます。

システムの管理者の場合は、これらの各ページで (必要に応じて) エンティティのチェックボックスをクリックしてから [送信者グループに追加 (Add to Sender Group)] をクリックし、送信者グループにネットワーク オーナー、ドメイン、または IP アドレスを追加することもできます。

また、送信者の現在の情報テーブルの送信者グループ情報の下にある [送信者グループに追加 (Add to Sender Group)] リンクをクリックして、送信者グループに送信者を追加することもできます。送信者を送信者グループに追加する方法の詳細については、「電子メールを受信するためのゲートウェイの設定」(P.5-1) を参照してください。当然ながら、必ずしも変更を行う必要はありません。セキュリティ サービスに着信メールを処理させることもできます。

図 26-4 ネットワーク オーナーの現在の情報

Current Information for EXAMPLE.COM	
Current Information from SenderBase	Sender Group Information
Network Owner Category: NSP Daily Magnitude: 7.8 Monthly Magnitude: 7.5 Days Since First Message from this Network Owner: -- days Number of Domains Associated with this Network Owner: 1,928 Number of IP Addresses Used to Send Mail: 3.7M	Last Sender Group: UNKNOWNLIST
More from SenderBase	Add to Sender Group...

送信者プロフィールの検索

特定の送信者を検索するには、[クイック検索 (Quick Search)] ボックスに IP アドレス、ドメイン、または組織名を入力します。

送信者プロフィール ページが送信者の情報と共に表示されます。「データが読み込まれる報告ページ: 送信者プロフィール ページ」(P.26-13) を参照してください。

図 26-5 ドメイン プロファイル ページ (1/2)

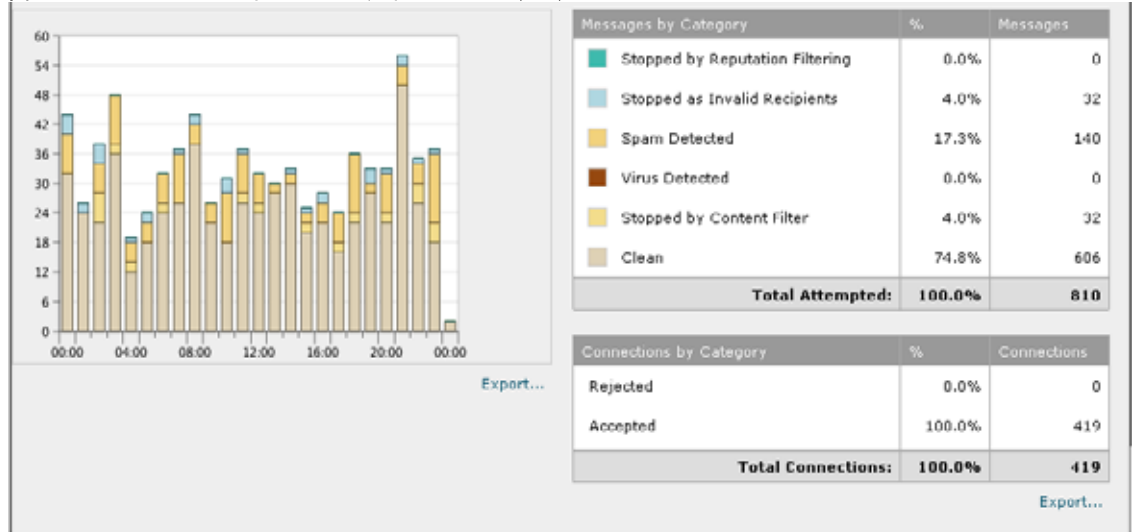


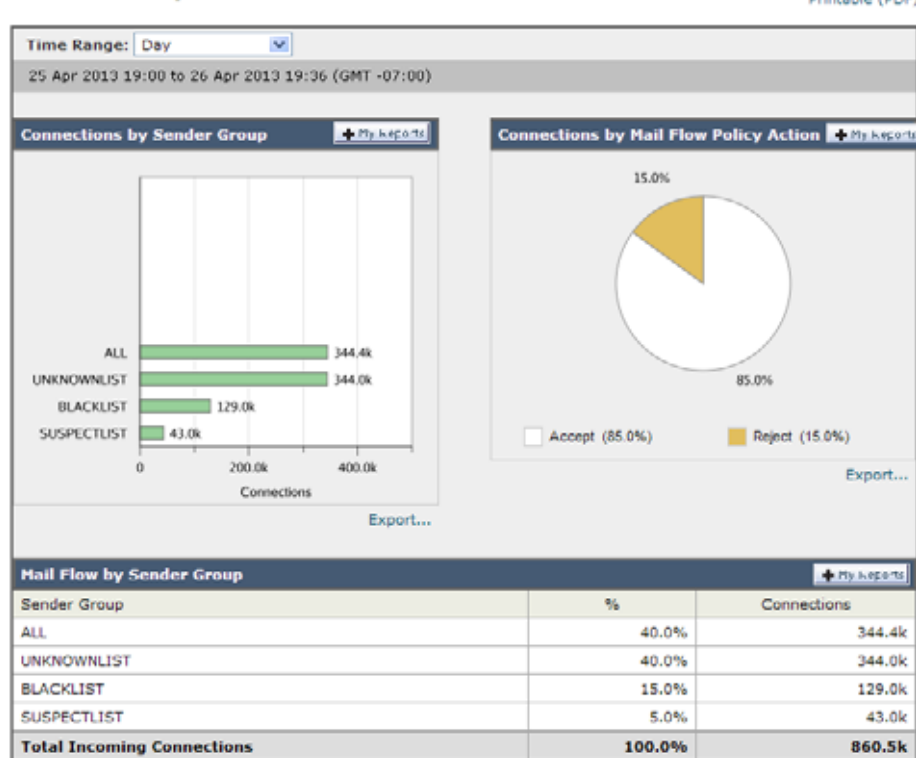
図 26-6 ドメイン プロファイル ページ (2/2)

Sender IP Address	Hostname	Total Attempted	Stopped by Reputation Filtering ?	Stopped as Invalid Recipients	Spam Detected	Virus Detected	Stopped by Content Filter	Total Threat	Clean
172.16.0.1	...161.29.10acfs.com	6	0	0	0	0	0	0	6
192.168.0.1	...99.150.10acfs.com	6	0	0	0	0	0	0	6
10.10.10.10	...182.0.10acfs.com	4	0	0	0	0	0	0	4
209.165.202.158	...51.234.10acfs.com	4	0	0	0	0	0	0	4
10.19.21.3	...82.159.10acfs.com	6	0	0	2	0	0	2	4
209.165.201.1	...126.46.10acfs.com	4	0	0	0	0	0	0	4
192.168.255.254	...21.42.10acfs.com	4	0	0	0	0	0	0	4
172.31.255.254	...66.208.10acfs.com	4	0	0	0	0	0	0	4
10.255.255.254	...8.203.10acfs.com	4	0	0	0	0	0	0	4
209.165.202.129	...84.126.10acfs.com	4	0	0	0	0	0	0	4

送信者グループ レポート

送信者グループ レポートは、送信者グループ別およびメールフロー ポリシー アクション別の接続のサマリーを提供し、SMTP 接続およびメールフロー ポリシーのトレンドを確認できるようにします。[送信者グループによるメールフロー (Mail Flow by Sender Group)] リストには、各送信者グループの割合および接続数が示されます。[メールフロー ポリシー アクションによる接続 (Connections by Mail Flow Policy Action)] グラフは、各メールフローポリシー アクションの接続の割合を示します。このページには、ホスト アクセス テーブル (HAT) ポリシーの有効性の概要が示されます。HAT の詳細については、「電子メールを受信するためのゲートウェイの設定」(P.5-1) を参照してください。

図 26-7 送信者グループ レポート ページ
Sender Groups



送信先 (Outgoing Destinations)

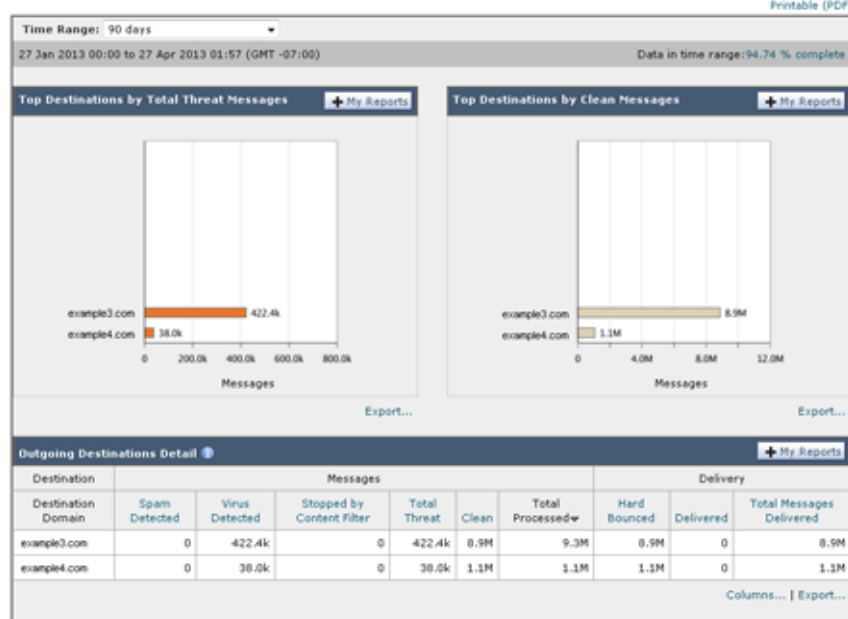
[送信先 (Outgoing Destinations)] ページには、メールの送信先ドメインに関する情報が示されます。このページは、2つのセクションで構成されます。ページの上部は、発信脅威メッセージ別の上位宛先および発信クリーンメッセージの上位宛先を示すグラフで構成されます。ページの下部には、総受信者数別にソートされた (デフォルト設定) 全カラムを示す表が表示されます。

レポート対象の時間範囲 (時間や週など)、またはカスタムの範囲を選択できます。グラフまたは詳細リストのデータは、すべてのレポートと同様に [エクスポート (Export)] リンクを使用して CSV 形式にエクスポートできます。

[送信先 (Outgoing Destinations)] ページを使用すると、次の情報を入手できます。

- アプライアンスのメール送信先
- 各ドメインに送信されるメールの量
- クリーン、スパム陽性、またはコンテンツ フィルタによる阻止のメールの割合
- 配信されたメッセージおよび宛先サーバによってハードバウンズされたメッセージの数

図 26-8 [送信先 (Outgoing Destinations)] ページ
Outgoing Destinations



送信メッセージ送信者 (Outgoing Senders)

[送信メッセージ送信者 (Outgoing Senders)] ページでは、ネットワーク内の IP アドレスおよびドメインから送信されるメールの量および種類に関する情報が示されます。このページを表示すると、ドメイン別または IP アドレス別に結果を表示できます。各ドメインによって送信されたメールの量を確認する場合にはドメイン別の結果、最も多いウイルス メッセージを送信している、または最も多くコンテンツ フィルタをトリガーしている IP アドレスを表示する場合には IP アドレス別の結果を表示することが推奨されます。

このページは、2つのセクションで構成されます。ページの左側は、総脅威メッセージ別の上位送信者を示すグラフです。総脅威メッセージには、スパムもしくはウイルス陽性のメッセージ、またはコンテンツ フィルタをトリガーしたメッセージが含まれます。ページの上部の右側は、クリーンメッセージ別の上位送信者を表示するグラフです。ページの下部には、総メッセージ数別にソートされた (デフォルト設定) 全カラムを示す表が表示されます。



(注)

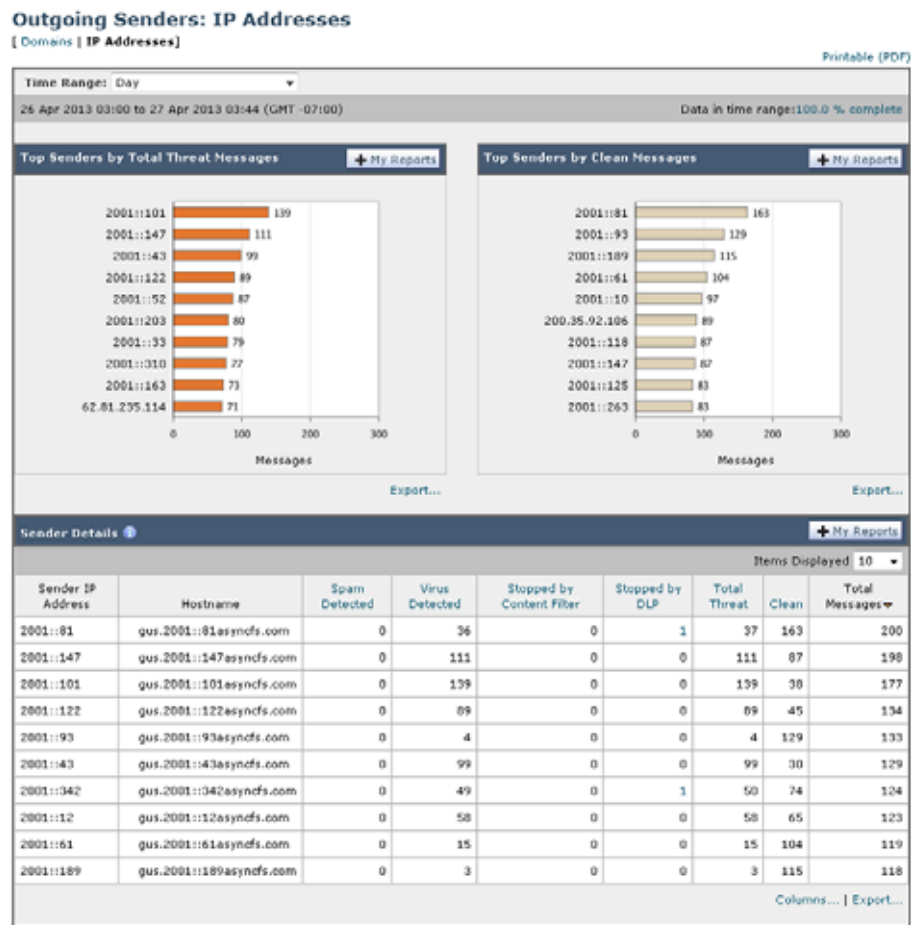
このページには、メッセージ配信に関する情報は表示されません。特定のドメインからのバウンスされたメッセージの数などの配信情報は、[送信処理ステータス (Delivery Status)] ページを使用して追跡できます。

レポート対象の時間範囲 (時間や週など)、またはカスタムの範囲を選択できます。グラフまたは詳細リストのデータは、すべてのレポートと同様に [エクスポート (Export)] リンクを使用して CSV 形式にエクスポートできます。

[送信メッセージ送信者 (Outgoing Senders)] ページを使用すると、次の情報を入手できます。

- 最も多くのウイルスまたはスパム陽性の電子メールを送信した IP アドレス
- 最も頻繁にコンテンツ フィルタをトリガーした IP アドレス
- 最も多くのメールを送信するドメイン

図 26-9 [送信メッセージ送信者 (Outgoing Senders)] ページ (IP アドレスを表示中)



[送信処理ステータス (Delivery Status)] ページ

特定の受信者ドメインに対する配信の問題を疑ったり、仮想ゲートウェイ アドレスに関する情報収集を行ったりする場合には、[モニタ (Monitor)] > [送信処理ステータス ページ (Delivery Status Page)] をクリックすると、特定の受信者ドメインに関連する電子メール操作に関するモニタリング情報が提供されます。

[送信処理ステータス (Delivery Status)] ページには、CLI で `tophosts` コマンドを使用した場合と同じ情報が表示されます (詳細については、第 30 章「CLI による管理およびモニタリング」の「電子メール キューの構成の確認」を参照してください)。

このページには、直近 3 時間以内にシステムによって配信されたメッセージの上位 20、50、または 100 の受信者ドメインのリストが表示されます。各統計情報のカラム見出しのリンクをクリックすることによって、最新のホスト ステータス、アクティブな受信者 (デフォルト)、切断した接続、配信された受信者、ソフト バウンス イベント、およびハード バウンス受信者別にソートできます。

- 特定のドメインを検索するには、[ドメイン名: (Domain Name:)] フィールドにドメイン名を入力し、[検索 (Search)] をクリックします。
- 表示されているドメインをドリルダウンするには、ドメイン名のリンクをクリックします。

[送信処理ステータス詳細 (Delivery Status Details)] ページに結果が表示されます。



(注)

受信者ドメインで任意のアクティビティが発生すると、このドメインが「アクティブ」となり、[概要 (Overview)] ページに表示されます。たとえば、配信の問題があるためにメールが発信キューにとどまると、この受信者ドメインは、引き続き発信メールの概要に表示されます。

配信の再試行

後で配信されるようにスケジュール設定されているメッセージは、[すべての送信を再試行 (Retry All Delivery)] をクリックすると、ただちに再試行できます。[すべての送信を再試行 (Retry All Delivery)] では、キューに含まれるメッセージがただちに配信されるようにスケジュールを変更できます。「ダウン」としてマークされたすべてのドメインおよびスケジュール設定されているか、ソフトバウンスされたメッセージは、ただちに配信されるためにキューに入れられます。

特定の宛先ドメインに向けての配信を再実行するには、ドメイン名のリンクをクリックします。[送信処理ステータス詳細 (Delivery Status Details)] ページで、[送信を再試行 (Retry Delivery)] をクリックします。

CLI で `delivernow` コマンドを使用して、ただちに配送するようにメッセージのスケジュールを変更することもできます。詳細については、「[電子メールの即時配信スケジュール](#)」(P.30-34) を参照してください。

[送信処理ステータス詳細 (Delivery Status Details)] ページ

特定の受信者ドメインに関する統計情報を検索するには、[送信処理ステータス詳細 (Delivery Status Details)] ページを使用します。このページには、CLI 内で `hoststatus` コマンドを使用した場合と同じ情報 (メール ステータス、カウンタ、およびゲージ) が表示されます (詳細については、[第 30 章「CLI による管理およびモニタリング」](#)の「メール ホストのステータスのモニタリング」を参照してください)。特定のドメインを検索するには、[ドメイン名: (Domain Name:)] フィールドにドメイン名を入力し、[検索 (Search)] をクリックします。`altsrchost` 機能を使用している場合、仮想ゲートウェイのアドレス情報が表示されます。

図 26-10 [送信処理ステータス (Delivery Status)] ページ
Delivery Status

Printable (PDF)

Outgoing Destinations Status							+ My Reports
						Items Displayed 10	
							Retry All Delivery
Destination Domain	Latest Host Status	Active Recipients	Connections Out	Delivered Recipients	Soft Bounced	Hard Bounced	
example1.com	Down	7	0	0	0	0	
example2.com	Up	3	0	4.0M	221.1k	220.7k	
example3.com	Down	0	0	0	0	170	
example4.com	Down	0	0	0	0	5,161	

[内部ユーザ (Internal Users)] ページ

[内部ユーザ (Internal Users)] ページでは、内部ユーザによって送受信されたメールに関する情報が、電子メール アドレスごとに表示されます (単一ユーザの複数の電子メール アドレスが、リストに表示される場合があります。レポートでは、電子メール アドレスはまとめられません)。

このページは、クリーン着信メッセージ別およびクリーン発信メッセージ別の上位ユーザを示すグラフとユーザ メール フローの詳細の 2 つのセクションで構成されます。レポート対象の時間範囲 (時間、日、週、または月) を選択できます。グラフまたは詳細リストのデータは、すべてのレポートと同様に [エクスポート (Export)] リンクを使用して CSV 形式にエクスポートできます。

[ユーザ メール フローの詳細 (User Mail Flow Details)] リストでは、送受信メールが電子メール アドレスごとに [正常 (Clean)]、[スパム検出 (Spam Detected)] (着信のみ)、[ウイルス検出 (Virus Detected)]、および [コンテンツ フィルタの一致数 (Content Filter Matches)] に分類されます。このリストは、カラム見出しをクリックしてソートできます。

内部ユーザ レポートを使用すると、次の情報を入手できます。

- 最も多くの外部メールを送信したユーザ
- 最も多くのクリーン電子メールを受信したユーザ
- 最も多くのスパムを受信したユーザ
- コンテンツ フィルタをトリガーしたユーザとそのコンテンツ フィルタの種類
- 電子メールをコンテンツ フィルタで捕捉されたユーザ

着信内部ユーザとは、**Rcpt To:** アドレスに基づいてシステムで電子メールを受信する対象ユーザのことです。発信内部ユーザは **Mail From:** アドレスに基づいており、内部ネットワーク内の送信者が送信している電子メールの種類を追跡する場合に役立ちます。

一部の送信メール (バウンスなど) の送信者は、**null** です。これらの送信者は、送信および「不明」に集計されます。

内部ユーザの [内部ユーザの詳細 (Internal User Details)] ページを表示するには、この内部ユーザをクリックします。

内部ユーザの詳細 (Internal User Details)

[内部ユーザの詳細 (Internal User Details)] ページでは、各カテゴリ ([スパム検出 (Spam Detected)]、[ウイルス検出 (Virus Detected)]、[コンテンツ フィルタによる停止 (Stopped By Content Filter)]、および [正常 (Clean)]) のメッセージ数を示す送受信メッセージの内訳など指定したユーザに関する詳細情報が示されます。送受信コンテンツ フィルタおよび DLP ポリシーの一致も示されます。

図 26-11 [内部ユーザの詳細 (Internal User Details)] ページ
Internal User: prin@ironport.com

Incoming Messages		Outgoing Messages	
Spam Detected:	4,390	Spam Detected:	0
Virus Detected:	2	Virus Detected:	0
Stopped by Content Filter:	0	Stopped by Content Filter:	0
Marketing:	2,051	Clean:	0
Clean:	20.2k	Total Outgoing Messages:	0
Total Incoming Messages:	26.6k		

Incoming Content Filter Matches		Outgoing Content Filter Matches	
Content Filter	Messages	No data was found in the selected time range	
QuarantineSpamandBCCCorpus	4,132		
DeliverSpamandBCCCorpus	246		
Total Incoming Matches:	4,378		

コンテンツ フィルタの詳細情報を対応するコンテンツ フィルタ情報ページに表示するには、そのコンテンツ フィルタ名をクリックします（「[コンテンツ フィルタ (Content Filters)] ページ」(P.26-25) を参照）。この方法を使用すると、特定のコンテンツ フィルタに一致したメールを送受信したユーザのリストも取得できます。

特定の内部ユーザの検索

特定の内部ユーザ（電子メール アドレス）は、[内部ユーザ (Internal Users)] ページおよび [内部ユーザの詳細 (Internal User Details)] ページの下部にある検索フォームから検索できます。検索テキストに完全に一致させるか、入力したテキストで始まる項目を検索するか（たとえば、「ex」で始まる項目を検索する場合、「example.com」が一致します）を選択します。

[DLP インシデント (DLP Incidents)] ページ

[DLP インシデント (DLP Incidents)] ページには、送信メールで発生した Data Loss Prevention (DLP) ポリシー違反インシデントに関する情報が示されます。アプライアンスでは、[送信メールポリシー (Outgoing Mail Policies)] テーブルでイネーブルにした DLP 電子メール ポリシーを使用して、ユーザが送信した機密データを検出します。DLP ポリシーに違反する送信メッセージが発生するたびに、インシデントとして報告されます。

DLP インシデント レポートを使用すると、次のような情報を取得できます。

- ユーザが送信した機密データの種類
- これらの DLP インシデントの重大度
- これらのメッセージのうち、配信されたメッセージの数
- これらのメッセージのうち、ドロップされたメッセージの数
- これらのメッセージの送信者

[DLP インシデント (DLP Incidents)] ページは、次の 2 つの主なセクションで構成されます。

- 重大度 ([低 (Low)], [中 (Medium)], [高 (High)], [クリティカル (Critical)]) 別の上位 DLP インシデントおよびポリシーの一致数を集約する DLP インシデントのトレンド グラフ
- [DLP インシデントの詳細 (DLP Incidents Details)] リスト

レポート対象の時間範囲 (時間や週など)、またはカスタムの範囲を選択できます。グラフまたは詳細リストのデータは、すべてのレポートと同様に [エクスポート (Export)] リンクを使用して CSV 形式にエクスポートするか、[印刷用 (PDF) (Printable (PDF))] リンクを使用して PDF 形式にエクスポートできます。英語以外の言語での PDF の生成については、「[レポートに関する注意事項](#)」(P.26-45) を参照してください。

図 26-12 DLP インシデント グラフ : [重大度別上位インシデント (Top Incidents by Severity)]、[インシデント サマリー (Incident Summary)]、および [DLP ポリシー一致の上位 (Top DLP Policy Matches)]

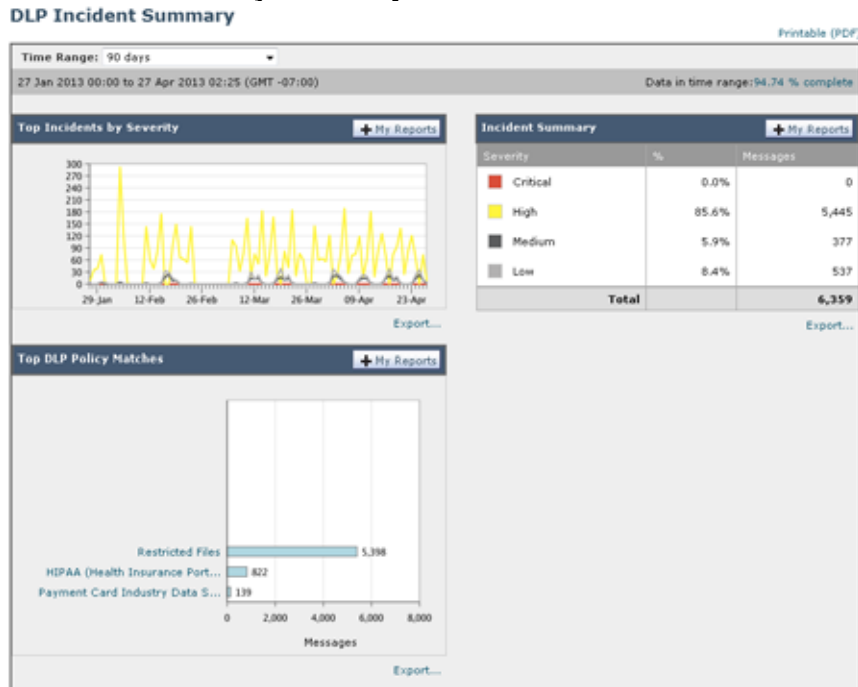


図 26-13 DLP インシデントの詳細 (DLP Incidents Details)

DLP Incident Details + My Reports

DLP Policy	Low	Medium	High	Critical	Total	Delivered (encrypted)	Delivered (clear)	Dropped
Restricted Files	0	0	5,398	0	5,398	0	0	0
HIPAA (Health Insurance Portability and Accountability Act)	445	377	0	0	822	0	0	822
Payment Card Industry Data Security Standard (PCI-DSS)	92	0	47	0	139	0	0	0

Columns... | Export...

ポリシーによって検出された DLP インシデントに関する詳細情報を表示するには、DLP ポリシーの名前をクリックします。この方法を使用すると、ポリシーによって検出された、機密データを含むメールを送信したユーザのリストを取得できます。

DLP インシデントの詳細 (DLP Incidents Details)

アプライアンスの送信メール ポリシーで現在イネーブルの DLP ポリシーは、[DLP インシデント (DLP Incidents)] ページの下部にある [DLP インシデントの詳細 (DLP Incidents Details)] テーブルに表示されます。詳細情報を表示するには、DLP ポリシーの名前をクリックします。

[DLP インシデントの詳細 (DLP Incidents Details)] テーブルには、ポリシーごとの DLP インシデントの数に加えて、重大度レベル別の内訳、クリアに配信されたメッセージの数、暗号化されて配信されたメッセージの数、ドロップされたメッセージの数が示されます。データをソートするには、カラム見出しをクリックします。

[DLP ポリシー詳細 (DLP Policy Detail)] ページ

[DLP インシデントの詳細 (DLP Incidents Details)] テーブルで DLP ポリシーの名前をクリックした場合、その結果として表示される [DLP ポリシー詳細 (DLP Policy Detail)] ページにそのポリシーに関する DLP インシデントデータが表示されます。このページには、重大度に基づいた DLP インシデントのグラフが表示されます。

このページには、DLP ポリシーに違反したメッセージを送信した各内部ユーザを表示する、ページ下部にある [送信者別インシデント (Incidents by Sender)] リストも含まれます。このリストには、このポリシーに関するユーザごとの DLP インシデントの総数に加えて、重大度レベル別の内訳、メッセージのいずれかがクリアに配信されたか、暗号化されて配信されたか、ドロップされたかが示されます。[送信者別インシデント (Incidents by Sender)] リストを使用すると、組織の機密データをネットワーク外のユーザに送信した可能性のあるユーザを検索できます。

図 26-14 DLP ポリシーの詳細グラフ : [重大度別上位インシデント (Top Incidents by Severity)], [インシデントサマリー (Incident Summary)]

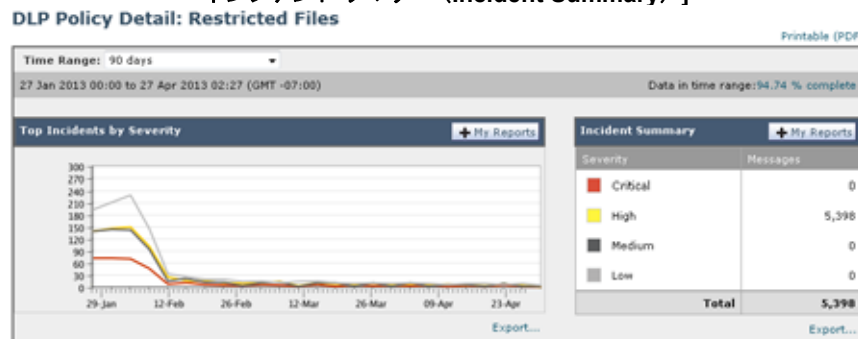


図 26-15 DLP Policy Incidents by Sender

Sender	Low	Medium	High	Critical	Total	Delivered (encrypted)	Delivered (clear)	Dropped
user@test.com	698	453	480	227	1,858	0	0	0
testuserFP1@test.com	171	0	0	57	228	0	0	0
testuseridentities@test.com	114	0	0	0	114	0	0	0
testuserTenoc@test.com	0	112	0	0	112	0	0	0
testuser200cc@test.com	0	0	0	57	57	0	0	0
testuser25cc@test.com	0	0	57	0	57	0	0	0
testusercontact_IPAddr_visa@test.com	0	0	57	0	57	0	0	0
testusercontact_visa@test.com	0	0	57	0	57	0	0	0
testuserCreditcard_sev_high@test.com	0	0	57	0	57	0	0	0
testuserCritical_violation_DL@test.com	0	57	0	0	57	0	0	0

送信者名をクリックすると、[内部ユーザ (Internal Users)] ページが開きます。詳細については、[内部ユーザ (Internal Users)] ページ (P.26-21) を参照してください。

[コンテンツ フィルタ (Content Filters)] ページ

[コンテンツ フィルタ (Content Filters)] ページには、送受信コンテンツ フィルタの上位一致 (最も多くのメッセージに一致したコンテンツ フィルタ) に関する情報が 2 種類の形式 (棒グラフとリスト) で表示されます。[コンテンツ フィルタ (Content Filters)] ページを使用すると、コンテンツ フィルタごとまたはユーザごとに企業ポリシーを確認し、次の情報を取得できます。

- 受信メールまたは送信メールによってトリガーされた回数の最も多いコンテンツ フィルタ
- 特定のコンテンツ フィルタをトリガーしたメールを送受信した上位ユーザ

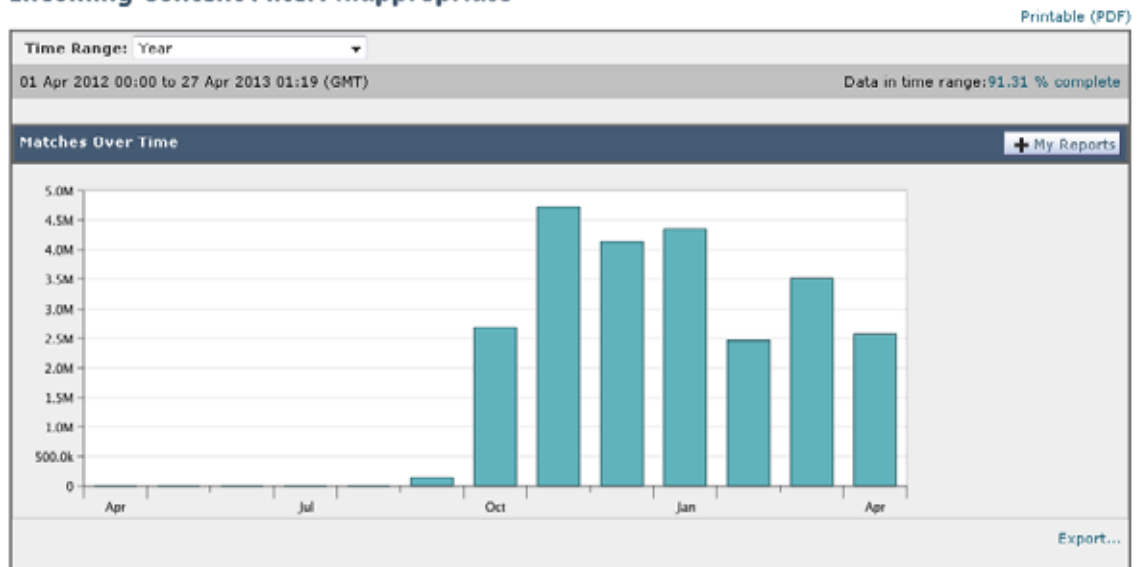
リストのコンテンツ フィルタ名をクリックすると、[コンテンツ フィルタの詳細 (Content Filter Details)] ページにこのフィルタに関する詳細を表示できます。

コンテンツ フィルタの詳細 (Content Filter Details)

[コンテンツ フィルタの詳細 (Content Filter Details)] には、このフィルタの経時的な一致および内部ユーザ別の一致が表示されます。

[内部ユーザ別の一致 (Matches by Internal User)] セクションでは、ユーザ名をクリックして内部ユーザ (電子メール アドレス) の [内部ユーザの詳細 (Internal User Details)] ページを表示できます ([内部ユーザの詳細 (Internal User Details)] (P.26-22) を参照)。

図 26-16 [コンテンツ フィルタ (Content Filters)] ページ
Incoming Content Filter: Inappropriate



[アウトブレイク フィルタ (Outbreak Filters)] ページ

[アウトブレイク フィルタ (Outbreak Filters)] ページには、お使いのアプライアンスのアウトブレイク フィルタの現在のステータスおよび設定に加えて、最近の発生状況やアウトブレイク フィルタによって隔離されたメッセージに関する情報が示されます。このページを使用して、対象を絞ったウイルス、詐欺、およびフィッシング攻撃に対する防御をモニタできます。

[タイプ別脅威 (Threats By Type)] セクションには、アプライアンスによって受信された脅威メッセージのさまざまなタイプが示されます。[脅威サマリー (Threat Summary)] セクションには、[ウイルス (Virus)]、[フィッシング (Phish)]、および [Scam] によるメッセージの内訳が示されます。

[過去 1 年間のアウトブレイク サマリー (Past Year Outbreak Summary)] には、この 1 年間にわたるグローバル発生およびローカル発生が表示されるので、ローカル ネットワークのトレンドとグローバルなトレンドを比較できます。グローバル発生リストは、すべての発生 (ウイルスとウイルス以外の両方) の上位集合です。これに対して、ローカル発生は、お使いのアプライアンスに影響を与えたウイルス発生に限定されています。ローカル感染発生データには、ウイルス以外の脅威は含まれません。グローバル感染発生データは、アウトブレイク隔離で現在設定されているしきい値を超えた、Threat Operations Center によって検出されたすべての発生を表します。ローカル感染発生データは、アウトブレイク隔離で現在設定されているしきい値を超えた、このアプライアンスで検出されたすべてのウイ

ルス発生を表します。[ローカル保護の合計時間 (Total Local Protection Time)] は、Threat Operations Center による各ウイルス発生を検出と、主要ベンダーによるアンチウイルス シグニチャの解放との時間差に常に基づいています。必ずしもすべてのグローバル発生が、お使いのライセンスに影響を与えるわけではありません。「--」値は、保護時間が存在しないか、アンチウイルス ベンダーからシグニチャ時間を入手できないことを示します (一部のベンダーは、シグニチャ時間を報告しません)。これは、保護時間がゼロであることを示すのではなく、保護時間の算出に必要な情報を入手できないことを示します。

[隔離されたメッセージ (Quarantined Messages)] セクションでは、アウトブレイク フィルタの隔離状況の概要が示されます。これは、アウトブレイク フィルタが捕捉した潜在的な脅威メッセージの数を把握するのに役立つ尺度です。隔離されたメッセージは、解放時に集計されます。通常、メッセージはアンチウイルスおよびアンチスパム ルールが使用可能になる前に隔離されます。メッセージが解放されると、アンチウイルスおよびアンチスパム ソフトウェアによってスキャンされ、陽性か、クリーンかを判定されます。発生トラッキングの動的性質により、メッセージが隔離エリア内にあるときでも、メッセージの隔離ルール (および関連付けられる発生) が変更される場合があります。(隔離エリアに入った時点ではなく) 解放時にメッセージを集計することにより、件数の変動による混乱を防ぎます。

[脅威の詳細 (Threat Details)] リストには、脅威のカテゴリ (ウイルス、詐欺、またはフィッシング)、脅威の名前、脅威の説明、識別されたメッセージの数などの、特定の発生に関する情報が表示されます。ウイルス発生の場合は [過去 1 年間のウイルス アウトブレイク (Past Year Virus Outbreaks)] に、発生の名前と ID、ウイルス発生が初めてグローバルに検出された日時、アウトブレイク フィルタによって提供される保護時間、および隔離されたメッセージの数が含まれます。左側のメニューを使用して、グローバル発生またはローカル発生のいずれか、および表示するメッセージの数を選択できます。このリストは、カラム見出しをクリックしてソートできます。

[最初にグローバルで確認した日時 (First Seen Globally)] の時間は、世界最大の電子メールおよび Web モニタリング ネットワークである SenderBase のデータに基づいて、Threat Operations Center によって決定されます。[保護時間 (Protection Time)] は、Threat Operations Center による各脅威の検出と、主要ベンダーによるアンチウイルス シグニチャの解放との時間差に基づいています。

「--」値は、保護時間が存在しないか、アンチウイルス ベンダーからシグニチャ時間を入手できないことを示します (一部のベンダーは、シグニチャ時間を報告しません)。保護時間がゼロであることを示しているわけではありません。むしろ、保護時間の算出に必要な情報を入手できないことを意味します。

[アウトブレイク フィルタ (Outbreak Filters)] ページを使用すると、次の情報を取得できます。

- 隔離されているメッセージの数と、それらの脅威のタイプ
- ウイルス発生に対するアウトブレイク フィルタ機能のリードタイム
- グローバル ウイルス発生と比較したローカル ウイルスの発生状況

図 26-17 [アウトブレイク フィルタ (Outbreak Filters)] ページ
Outbreak Filters



[ウイルス タイプ (Virus Types)] ページ

[ウイルス タイプ (Virus Types)] ページでは、ネットワークに侵入したウイルスおよびネットワークから送信されたウイルスの概要が示されます。[ウイルス タイプ (Virus Types)] ページには、お使いのアプリケーションで稼働するウイルス スキャン エンジンによって検出されたウイルスが表示されます。このレポートを使用して、特定のウイルスに対して特定のアクションを実行することが推奨されます。たとえば、PDF ファイルに組み込まれることが判明しているウイルスを大量に受信している場合、PDF が添付されているメッセージを隔離するフィルタ アクションを作成することが推奨されます。

複数のウイルス スキャン エンジンを実行している場合、[ウイルス タイプ (Virus Types)] ページには、イネーブルになっているすべてのウイルス スキャン エンジンの結果が含まれます。ページに表示されるウイルスの名前は、ウイルス スキャン エンジンによって判定された名前です。複数のスキャン エンジンが 1 つのウイルスを検出した場合、同じウイルスに対して複数のエントリが存在する可能性があります。

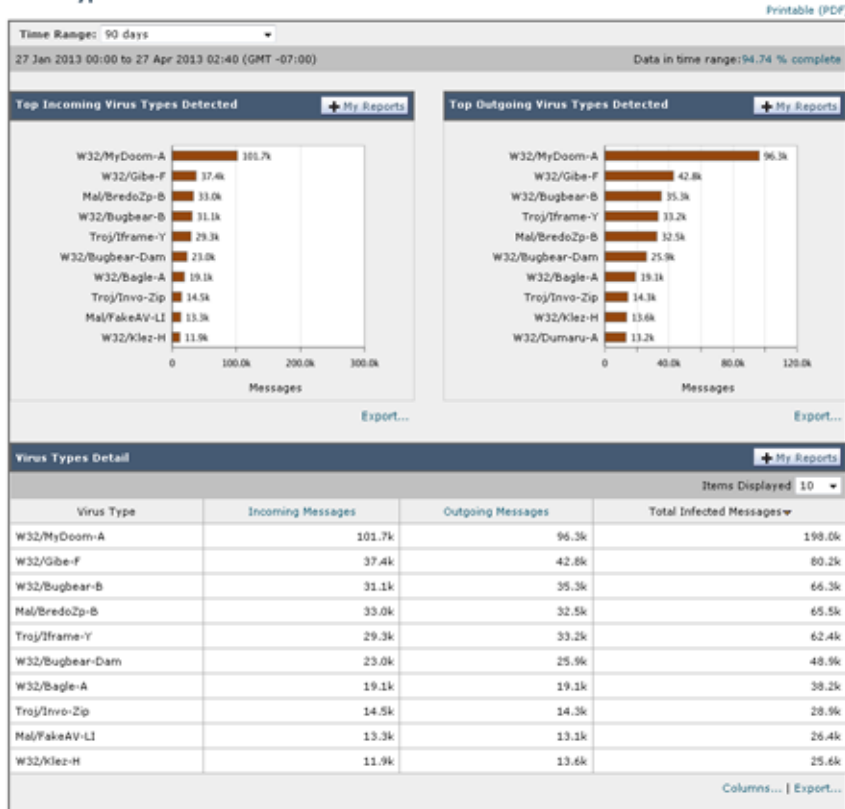
[ウイルス タイプ (Virus Types)] ページには、ネットワークに侵入したウイルスおよびネットワークで送受信されたウイルスの概要が表示されます。[検出した受信ウイルスの上位 (Top Incoming Virus Detected)] セクションには、ネットワークに送信されたウイルスのチャート ビューが降順で表示されます。[検出した送信ウイルスの上位 (Top Outgoing Virus Detected)] セクションには、ネットワークから送信されたウイルスのチャート ビューが降順で表示されます。



(注)

ウイルスに感染したメッセージをネットワークに送信したホストを表示するには、[受信メール (Incoming Mail)] ページに移動し、同じ報告期間を指定して、ウイルス陽性別にソートします。同様に、ネットワーク内でウイルス陽性の電子メールを送信した IP アドレスを表示するには、[送信メッセージ送信者 (Outgoing Senders)] ページを表示し、ウイルス陽性メッセージ別にソートします。

図 26-18 [ウイルス タイプ (Virus Types)] ページ



[ウイルス タイプの詳細 (Virus Types Details)] リストには、感染した送受信メッセージ、および感染メッセージの総数など特定のウイルスに関する情報が表示されます。感染した受信メッセージの詳細リストには、ウイルスの名前およびこのウイルスに感染した受信メッセージの総数が表示されます。同様に、送信メッセージの詳細リストには、ウイルスの名前およびこのウイルスに感染した送信メッセージの総数が表示されます。ウイルスの種類の詳細は、[受信メッセージ (Incoming Messages)]、[送信メッセージ (Outgoing Messages)]、または [感染したメッセージの合計数 (Total Infected Messages)] 別にソートできます。

[TLS 接続 (TLS Connections)] ページ

[TLS 接続 (TLS Connections)] ページには、メールの送受信に使用される TLS 接続の全体的な使用状況が表示されます。このレポートでは、TLS 接続を使用してメールを送信する各ドメインの詳細についても示されます。

[TLS 接続 (TLS Connections)] ページを使用すると、次の情報を測定できます。

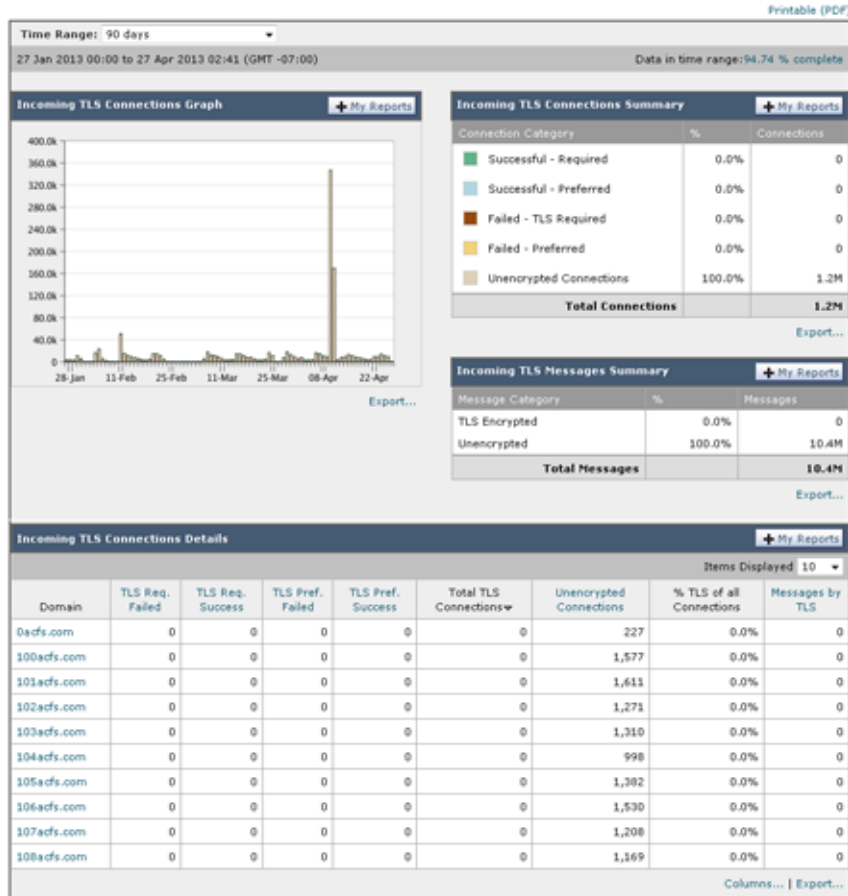
- 送受信接続による、全体的な TLS の使用割合
- TLS 接続に成功したパートナー
- TLS 接続に成功しなかったパートナー
- TLS 認証に問題のあるパートナー
- パートナーが TLS を使用したメールの全体的な割合

[TLS 接続 (TLS Connections)] ページは、着信接続に関するセクションと、発信接続に関するセクションに分かれています。各セクションには、詳細情報が含まれたグラフ、サマリー、および表が含まれています。

グラフには、指定した時間範囲にわたる、送受信 TLS の暗号化された接続および暗号化されない接続のビューが表示されます。グラフには、メッセージの総量、暗号化された/暗号化されないメッセージの量、成功/失敗した TLS 暗号化メッセージの量が表示されます。グラフでは、TLS が必須であった接続と、TLS が単に優先された接続が区別されます。

表には、暗号化されたメッセージを送受信するドメインの詳細が表示されます。ドメインごとに、成功/失敗した必須の TLS 接続と優先された TLS 接続の数、試行された TLS 接続の総数（成功したか失敗したかにかかわらず）、および暗号化されていない接続の総数を表示できます。また、TLS が試行されたすべての接続の割合、および正常に送信された暗号化メッセージの総数（TLS が優先か必須かにかかわらず）も表示できます。この表の下部にある [列 (Columns)] リンクをクリックすることにより、カラムの表示/非表示を切り替えることができます。

図 26-19 TLS 接続レポート：着信接続
TLS Connections



[受信 SMTP 認証 (Inbound SMTP Authentication)] ページ

[受信 SMTP 認証 (Inbound SMTP Authentication)] ページには、クライアント証明書の使用情報、および電子メールセキュリティアプライアンスとユーザのメールクライアント間で SMTP セッションを認証するための SMTP AUTH コマンドが表示されます。アプライアンスは、証明書または SMTP AUTH コマンドを受け入れると、メールクライアントへの TLS 接続を確立します。クライアントはこの接続を使用してメッセージを送信します。アプライアンスは、これらの試行をユーザ単位で追跡できないため、レポートには、ドメイン名とドメイン IP アドレスに基づいて SMTP 認証の詳細が表示されます。

次の情報を確認するには、このレポートを使用します。

- SMTP 認証を使用している着信接続の総数
- クライアント証明書を使用している接続の数
- SMTP AUTH を使用している接続の数
- SMTP 認証を使用しようとして、接続が失敗したドメイン
- SMTP 認証が失敗した一方で、フォールバックを正常に使用している接続の数

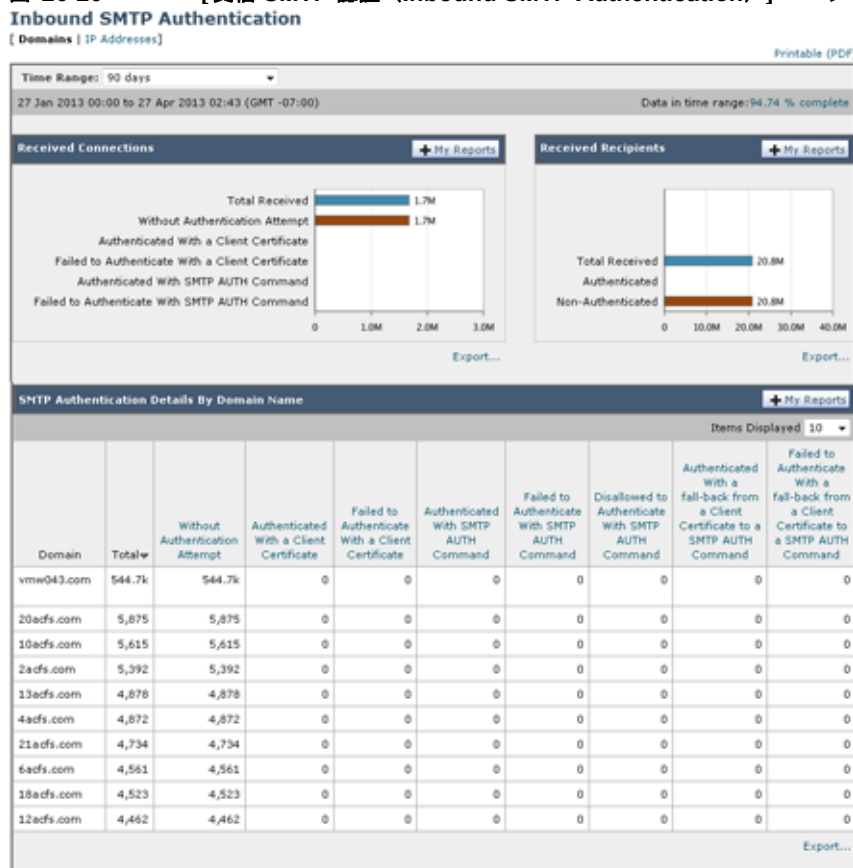
[受信 SMTP 認証 (Inbound SMTP Authentication)] ページには、受信した接続のグラフ、SMTP 認証接続を試行したメール受信者のグラフ、および接続の認証試行の詳細を含むテーブルが表示されます。

[受信した接続 (Received Connections)] グラフでは、指定した時間範囲において SMTP 認証を使用して接続を認証しようとしたメール クライアントの着信接続が表示されます。このグラフには、アプリケーションが受信した接続の総数、SMTP 認証を使用して認証を試行しなかった接続の数、クライアント証明書を使用して認証が失敗および成功した接続の数、SMTP AUTH コマンドを使用して認証が失敗および成功した接続の数が表示されます。

[受信した受信者 (Received Recipients)] グラフには、SMTP 認証を使用して、メッセージを送信するために電子メール セキュリティ アプリケーションへの接続を認証しようとしたメール クライアントを所有する受信者の数が表示されます。このグラフでは、接続が認証された受信者の数、および接続が認証されなかった受信者の数も示されます。

[SMTP 認証の詳細 (SMTP Authentication details)] テーブルには、メッセージを送信するために電子メール セキュリティ アプリケーションへの接続を認証しようとしたユーザを含むドメインの詳細が表示されます。ドメインごとに、クライアント証明書を使用した接続試行 (成功または失敗) の数、SMTP AUTH コマンドを使用した接続試行 (成功または失敗) の数、およびクライアント証明書接続試行が失敗した後、SMTP AUTH にフェールバックした接続の数を表示できます。ページ上部のリンクを使用して、ドメイン名またはドメイン IP アドレス別にこの情報を表示できます。

図 26-20 [受信 SMTP 認証 (Inbound SMTP Authentication)] ページ



[レート制限 (Rate Limits)] ページ

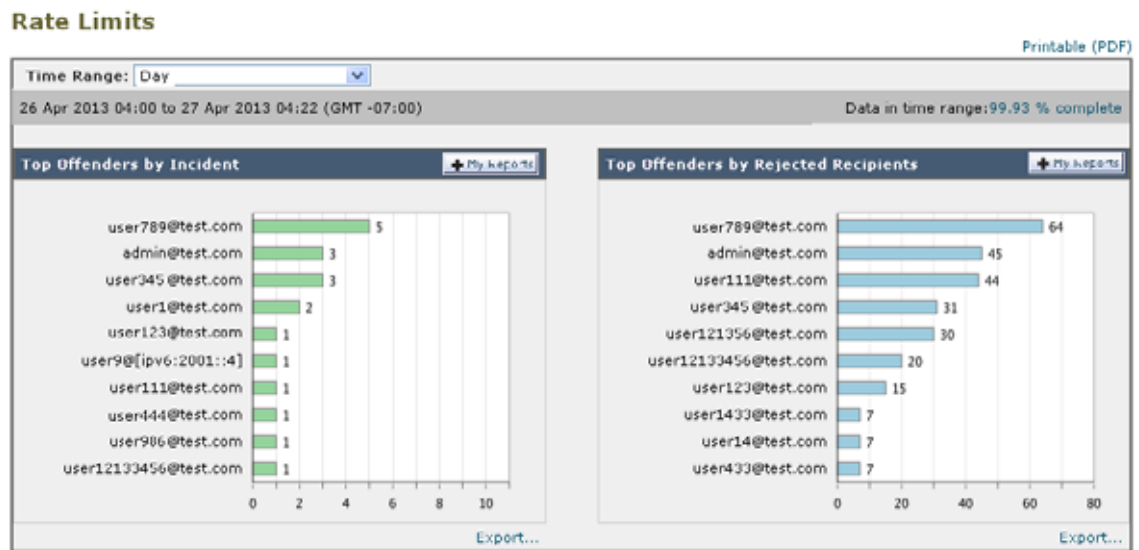
エンベロープ送信者ごとのレート制限を使用すると、メール送信者アドレスに基づいて、個々の送信者からの時間間隔ごとの電子メールメッセージ受信者数を制限できます。[レート制限 (Rate Limits)] レポートには、この制限を最も上回った送信者が表示されます。

このレポートは、以下を特定する場合に役立ちます。

- 大量のスパムを送信するために使用される可能性のある信用できないユーザ アカウント
- 通知、アラート、自動報告などに電子メールを使用する組織内の制御不能アプリケーション
- 内部請求やリソース管理のために、組織内で電子メールを過剰に送信している送信元
- スпамとは見なされないが、大量の着信電子メール トラフィックを送信している送信元

内部送信者に関する統計情報を含む他のレポート ([内部ユーザ (Internal Users)]、[送信メッセージ送信者 (Outgoing Senders)] など) では、送信されたメッセージの数のみ計測されます。これらのレポートでは、少数のメッセージを多数の受信者に送信した送信者は識別されません。

図 26-21 [レート制限 (Rate Limits)] ページ



[上位攻撃者 (インシデント別) (Top Offenders by Incident)] チャートには、設定済み制限よりも多くの受信者にメッセージを最も頻繁に送信しようとしたエンベロープ送信者が表示されます。各試行が 1 インシデントに相当します。このチャートでは、すべてのリスナーからのインシデント数が集計されます。

[上位攻撃者 (拒否した受信者別) (Top Offenders by Rejected Recipients)] チャートには、設定済みの制限を上回る、最も多くの受信者にメッセージを送信したエンベロープ送信者が表示されます。このチャートでは、すべてのリスナーからの受信者数が集計されます。

エンベロープ送信者によるレート制限の設定、または既存のレート制限の変更については、「[メールフロー ポリシーを使用した着信メッセージのルール の定義](#)」(P.7-15) を参照してください。

[システム容量 (System Capacity)] ページ

[システム容量 (System Capacity)] ページでは、ワーク キュー内のメッセージ数、ワーク キューで費やした平均時間、送受信メッセージ (量、サイズ、件数)、全体的な CPU 使用率、機能別の CPU 使用率、メモリ ページ スワップ情報などシステム負荷の詳細が示されます。

[システム容量 (System Capacity)] ページを使用すると、次の情報を確認できます。

- アプライアンスが推奨キャパシティを超えて、設定の最適化または追加アプライアンスが必要になった時間
- キャパシティの問題が今後発生する可能性を示すシステム挙動の過去のトレンド
- 最も多くのリソースを使用したシステムの部分 (トラブルシューティングを支援するため)

お使いのアプライアンスをモニタして、メッセージの量に対してキャパシティが適切であることを確認することが重要です。量は、時間の経過に伴って必ず増加しますが、適切にモニタリングしていれば、追加キャパシティまたは設定変更を予防的に適用できます。システム キャパシティをモニタする最も効果的な方法は、全体的な量、ワーク キュー内のメッセージ、およびリソース節約モードのインシデントを追跡することです。

- **量**: 「通常」のメッセージ量と環境内での「異常」な増加を把握することが重要です。経時的にこのデータを追跡して、量の増加を測定します。[受信メール (Incoming Mail)] ページおよび [送信メール (Outgoing Mail)] ページを使用すると、経時的に量を追跡できます。詳細については、

[システム容量 (System Capacity)] : [受信メール (Incoming Mail)] (P.26-36) および [システム容量 (System Capacity)] : [送信メール (Outgoing Mail)] (P.26-37) を参照してください。

- **ワーク キュー** : ワーク キューは、スパム攻撃の吸収とフィルタリングを行い、有害メッセージの異常な増加を処理する、「緩衝装置」として設計されています。しかしワーク キューは、負荷のかかっているシステムを示す最良の指標であり、長く、頻繁なワーク キューのバックアップは、キャパシティの問題を示している可能性があります。[ワーク キュー (WorkQueue)] ページを使用すると、ワーク キュー内でメッセージが費やした平均時間およびワーク キュー内のアクティビティを追跡できます。詳細については、[システム容量 (System Capacity)] : [ワークキュー (Workqueue)] (P.26-35) を参照してください。
- **リソース節約モード** : アプライアンスがオーバーロードになると、「リソース節約モード」(RCM) になり、CRITICAL システム アラートが送信されます。このモードは、デバイスを保護し、未処理分のメッセージを処理できるように設計されています。お使いのアプライアンスは、頻繁に RCM になるのではなく、メール量が非常に多い場合または異常に増加した場合にのみ RCM になる必要があります。頻繁な RCM アラートは、システムがオーバーロードになりつつあることを示している可能性があります。リソース節約モードは、[システム容量 (System Capacity)] ページでは追跡できません。

[システム容量 (System Capacity)] : [ワークキュー (Workqueue)]

[ワークキュー (Workqueue)] ページには、ワークキュー内でメッセージが費やした平均時間 (スパム隔離またはポリシー、ウイルス、およびアウトブレイク隔離で費やした時間は除く) が表示されます。1 時間から 1 月までの時間範囲を表示できます。平均は、メール配信を遅延させた短期間のイベントおよびシステム上の負荷の長期トレンドの両方を識別するのに役立ちます。



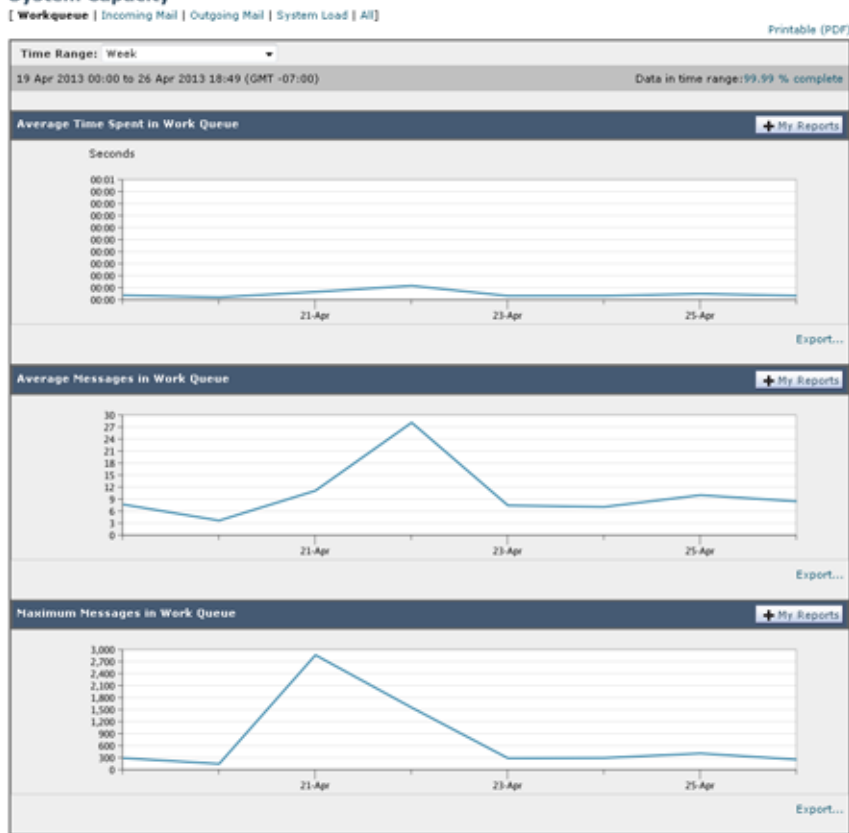
(注)

隔離からワーク キューにメッセージが解放される場合、「ワーク キュー内の平均時間」メトリックではこの時間が無視されます。これにより、重複集計と隔離で費やされた延長時間による統計の歪みを回避できます。

このレポートでは、指定期間のワーク キュー内のメッセージの量および同期間のワーク キュー内の最大メッセージ数も示されます。

[Workqueue] グラフにおける不定期のスパイクは、正常であり、発生する可能性があります。スパイクの発生頻度が高くなり、長期間にわたって同様の状態が続く場合、キャパシティの問題を示している可能性があります。[Workqueue] ページを確認するときは、ワーク キュー バックアップの頻度を測定し、10,000 メッセージを超えるワーク キュー バックアップに注意することが推奨されます。

図 26-22 [システム容量 (System Capacity)]: [ワークキュー (Workqueue)]



[システム容量 (System Capacity)]: [受信メール (Incoming Mail)]

[受信メール (Incoming Mail)] ページには、着信接続、着信メッセージの総数、平均メッセージ サイズ、着信メッセージの総サイズが示されます。結果を、指定した時間範囲に制限できます。ご自身の環境における通常のメッセージ量とスパイクのトレンドを理解しておくことが重要です。[受信メール (Incoming Mail)] ページを使用すると、経時的にメール量の増加を追跡し、システム キャパシティの計画を立てることができます。着信メール データと送信者プロフィール データを比較して、特定のドメインからネットワークに送信される電子メールの量のトレンドを表示することも推奨されます。



(注)

着信接続数の増加は、必ずしもシステム負荷に影響を与えるわけではありません。

図 26-23 [システム容量 (System Capacity)] : [受信メール (Incoming Mail)] (1/2 ページ)

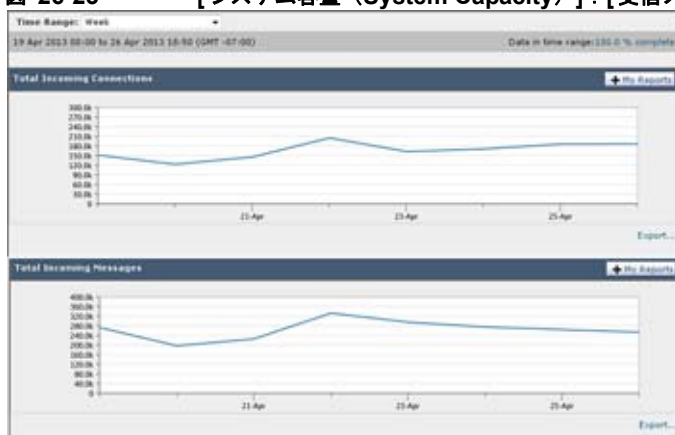
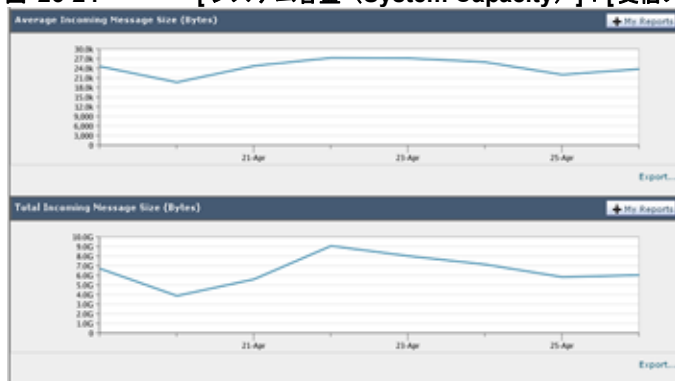


図 26-24 [システム容量 (System Capacity)] : [受信メール (Incoming Mail)] (2/2 ページ)



[システム容量 (System Capacity)] : [送信メール (Outgoing Mail)]

[送信メール (Outgoing Mail)] ページには、発信接続、発信メッセージの総数、平均メッセージ サイズ、着信メッセージの総サイズが示されます。結果を、指定した時間範囲に制限できます。ご自身の環境における通常のメッセージ量とスパイクのトレンドを理解しておくことが重要です。[送信メール (Outgoing Mail)] ページを使用すると、経時的にメール量の増加を追跡し、システム キャパシティの計画を立てることができます。発信メール データと発信宛先データを比較して、特定のドメインまたは IP アドレスから送信される電子メールの量のトレンドを表示することも推奨されます。

図 26-25 [システム容量 (System Capacity)]: [送信メール (Outgoing Mail)] (1/2 ページ)

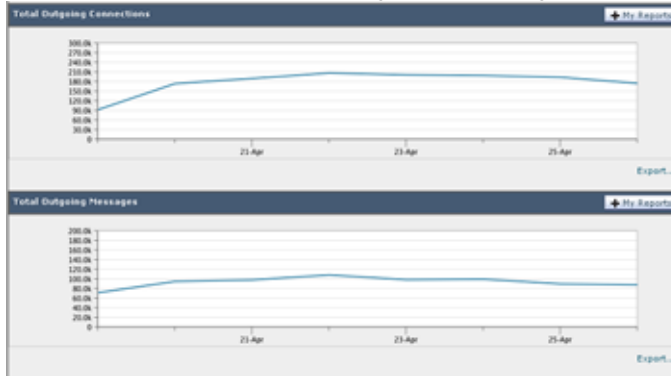
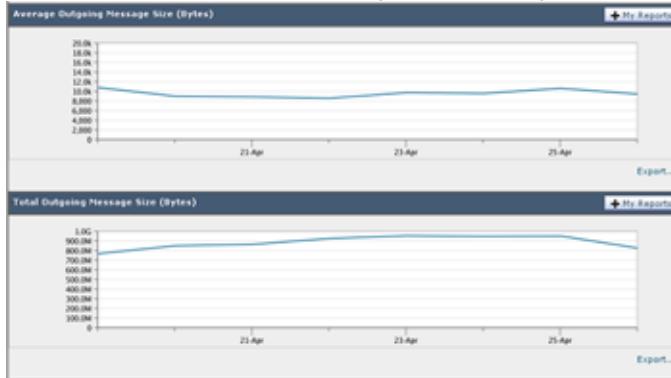


図 26-26 [システム容量 (System Capacity)]: [送信メール (Outgoing Mail)] (2/2 ページ)

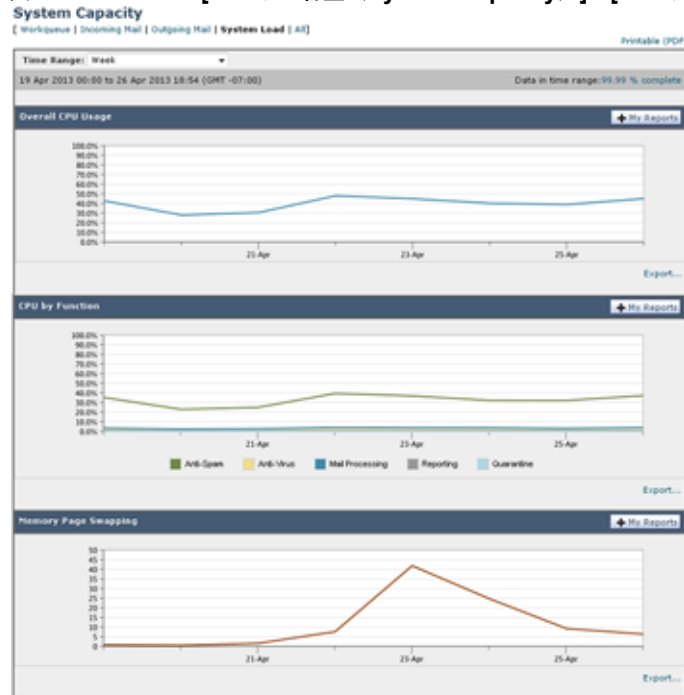


[システム容量 (System Capacity)]: [システムの負荷 (System Load)]

システム負荷レポートには、お使いのアプライアンスでの総 CPU 使用率が示されます。AsyncOS は、アイドル状態の CPU リソースを使用してメッセージスループットを向上させるように最適化されています。CPU 使用率が高くても、必ずしもシステムキャパシティの問題を示すわけではありません。CPU 使用率が高く、かつ高ボリュームのメモリ ページスワッピングが発生する場合、キャパシティの問題の可能性があります。このページでは、メール処理、スパムおよびウイルス エンジン、レポート、および隔離などさまざまな機能によって使用される CPU の量を表示するグラフも示されます。機能別 CPU のグラフは、システム上で最も多くのリソース使用する製品の領域を示す良い指標です。アプライアンスの最適化が必要な場合、このグラフは、調整やディセーブル化の必要な機能を判断するのに役立ちます。

メモリ ページスワッピングのグラフは、システムによるディスクへのページングが必要な頻度を示します。

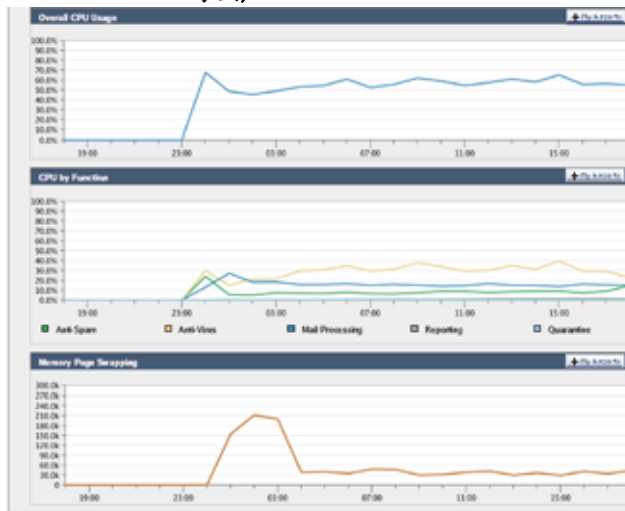
図 26-27 [システム容量 (System Capacity)] : [システムの負荷 (System Load)]



メモリ ページ スワッピングに関する注意事項

システムは、定期的にメモリをスワップするように設計されているので、一部のメモリ スワッピングは起こり得るものであり、アプライアンスの問題を示すものではありません。システムが常に高ボリュームのメモリ スワッピングを行う場合以外は、メモリ スワッピングは正常であり、起こり得る挙動です (特に C160 アプライアンスの場合)。たとえば、図 26-28 に、高ボリュームのメモリ スワッピングを常に行うシステムを示します。パフォーマンスを向上させるには、ネットワークにアプライアンスを追加するか、設定を調整して、最大のスループットを確保することが必要な場合もあります。

図 26-28 [システム容量 (System Capacity)]: [システムの負荷 (System Load)] (高負荷時のシステム)



[システム容量 (System Capacity)]: [すべて (All)]

[すべて (All)] ページでは、これまでのすべてのシステム キャパシティ レポートを単一のページに統合し、さまざまなレポート同士の関係を表示することができます。たとえば、過剰なメモリ スワッピングの発生と同時期にメッセージ キューが高いことを確認できます。これは、キャパシティの問題の兆候である可能性があります。このページを PDF として保存し、後で参照するために (またはサポート スタッフと共有するために) システム パフォーマンスのスナップショットを保存することが推奨されます。英語以外の言語での PDF の生成については、「[レポートに関する注意事項](#)」(P.26-45) を参照してください。

[システム ステータス (System Status)] ページ

[システム ステータス (System Status)] ページには、システムのすべてのリアルタイム メールおよび DNS アクティビティの詳細が表示されます。表示される情報は、CLI で `status detail` コマンドおよび `dnsstatus` コマンドを使用して入手できる情報と同じです。status detail コマンドの詳細については、第 30 章「[CLI による管理およびモニタリング](#)」の「[詳細な電子メール ステータスのモニタリング](#)」を参照してください。dnsstatus コマンドの詳細については、同章の「[DNS ステータスの確認](#)」を参照してください。

[システム ステータス (System Status)] ページは、[システム ステータス (System Status)]、[ゲージ (Gauges)]、[レート (Rates)]、および [カウンタ (Counters)] の 4 つのセクションで構成されます。

システム ステータス (System Status)

[システム ステータス (System Status)] セクションには、[メール システムのステータス (Mail System Status)] および [バージョン情報 (Version Information)] が示されます。

メール システムのステータス (Mail System Status)

[メール システムのステータス (Mail System Status)] セクションには、次の情報が含まれます。

- システム ステータス (システム ステータスの詳細については、「[ステータス \(Status\)](#)」 (P.26-6) を参照してください)。
- ステータスが報告された最終時刻。
- アプライアンスのアップタイム。
- システム内の最も古いメッセージ (配信用にまだキューに入っていないメッセージも含む)。

バージョン情報 (Version Information)

[バージョン情報 (Version Information)] セクションには、次の情報が含まれます。

- アプライアンスのモデル名。
- インストールされている AsyncOS オペレーティング システムのバージョンとビルド日。
- AsyncOS オペレーティング システムのインストール日。
- 接続先のシステムのシリアル番号。

この情報は、Cisco Customer Support に問い合わせる場合に役立ちます (「[テクニカル サポートの使用](#)」 (P.36-29) を参照)。

ゲージ (Gauges)

[ゲージ (Gauges)] には、次のようにキューおよびリソース使用率について示されます。

- メール処理キュー (Mail Processing Queue)
- キュー内のアクティブ受信者 (Active Recipients in Queue)
- キュー スペース (Queue Space)
- CPU 使用率 (CPU Utilization)

メール ゲートウェイ アプライアンスは、AsyncOS プロセスが消費している CPU 率を参照します。CASE は、アンチスパム スキャン エンジンおよびアウトブレイク フィルタ プロセスなど複数のアイテムを参照します。

- 一般的なリソース使用率 (General Resource Utilization)
- ログに使用されているディスク容量 (Logging Disk Utilization)

レート (Rates)

[レート (Rates)] セクションには、次の受信者に関する処理率が示されます。

- メール処理レート (Mail Handling Rates)
- 処理済みの割合 (Completion Rates)

カウンタ (Counters)

システム統計情報用の累積電子メール モニタリング カウンタをリセットし、カウンタの最終リセット日時を表示することができます。リセットは、システム カウンタおよびドメインごとのカウンタに影響します。リセットは、再試行スケジュールに関連する配信キュー内のメッセージのカウンタには影響しません。



(注)

管理者グループまたはオペレータグループに属するユーザアカウントのみが、カウンタをリセットできます。ゲストグループ内で作成したユーザアカウントでは、カウンタをリセットできません。詳細については、「[ユーザアカウントを使用する作業](#)」(P.28-1)を参照してください。

カウンタをリセットするには、[カウンタをリセット (Reset Counters)] をクリックします。このボタンは、CLI の `resetcounters` コマンドと同様の機能を提供します。詳細については、「[電子メール モニタリング カウンタのリセット](#)」(P.30-23)を参照してください。

- メール処理イベント (Mail Handling Events)
- 処理済みイベント (Completion Events)
- ドメイン キー イベント (Domain Key Events)
- DNS ステータス (DNS Status)

CSV データの取得

電子メール セキュリティ モニタで図やグラフの作成に使用されたデータは、CSV 形式で取得できます。CSV データにアクセスする方法は、次の 2 つです。

- **電子メールによる CSV レポートの配信。** 電子メールで配信される、またはアーカイブされる CSV レポートを生成できます。この配信方法は、電子メール セキュリティ モニタ ページに表示される各表に関する個別レポートを必要とする場合、または内部ネットワークにアクセスできないユーザに CSV データを送信する場合に便利です。

Comma-Separated Value (CSV; カンマ区切り) レポート タイプは、スケジュール設定されたレポートの表形式データを含む ASCII テキスト ファイルです。各 CSV ファイルには、最大 100 行を含めることができます。レポートに複数の種類の表が含まれる場合、各表に対して別個の CSV ファイルが作成されます。単一のレポートの複数の CSV ファイルは、単一の .zip ファイルに圧縮されて、アーカイブ ファイルの保存オプションを提供するか、個別の電子メール メッセージに添付されて電子メールで配信されます。

スケジュール設定されたレポートまたはオンデマンド レポートの詳細については、「[レポートインダクションの概要](#)」(P.26-44)を参照してください。

- **HTTP による CSV ファイルの取得。** 電子メール セキュリティ モニタ機能で図やグラフの作成に使用されたデータは、HTTP を使用して取得できます。この配信方法は、他のツールを使用してデータの詳細分析を実行する予定の場合に役立ちます。たとえば、未加工データのダウンロード、処理、および他のシステムでの結果表示を行う自動スクリプトによって、データの取得を自動化できます。

自動プロセスによる CSV データの取得

必要とする HTTP クエリーを最も容易に取得する方法は、必要な種類のデータを表示するように電子メール セキュリティ モニタ ページの 1 つを設定することです。次に、[エクスポート (Export)] リンクをコピーできます。これがダウンロード URL です。このようにデータ取得を自動化した場合、ダウンロード URL 内のパラメータを固定し、変更しないことが重要です (下記を参照)。

ダウンロード URL はコード化されるので、(適切な HTTP 認証を使用して) 同じクエリーを実行し、同様のデータセットを取得できる外部スクリプトにコピーできます。このスクリプトでは、Basic HTTP 認証またはクッキー認証を使用できます。自動プロセスで CSV データを取得する場合は、次の事項に注意する必要があります。

- URL の再利用時に関する時間範囲の選択（過去 1 時間、1 日、1 週間など）。URL をコピーして「過去 1 日」の CSV データセットを取得する場合、この URL を次に使用する際には、URL の再送信時から「過去 1 日」を対象とする新しいデータセットを取得します。時間範囲の選択は保持され、CSV クエリー文字列（たとえば `date_range=current_day`）に表示されます。
- データセットのフィルタリングおよび分類の優先順位。フィルタは保持され、クエリー文字列に表示されます。レポートでは、フィルタはほとんど使用されません。1 つの例としては、発生レポートにおける「グローバル/ローカル」発生セレクトが挙げられます。
- CSV ダウンロードでは、選択した時間範囲について表内のデータのすべての行が返されます。
- CSV では、タイムスタンプおよびキーで指示された表内のデータの行が返されます。スプレッドシートアプリケーションを使用するなどして、別個のステップで更にソートできます。
- 最初の行には、レポートに示される表示名に一致するカラム見出しが含まれています。タイムスタンプ（「[タイムスタンプ](#)」(P.26-43) を参照）およびキー（「[キー](#)」(P.26-43) を参照）も表示されます。

URL のサンプル

```
http://example.com/monitor/content_filters?format=csv&sort_col_ss_0_0_0=MAIL_CONTENT_FILTER_INCOMING.RECIPIENTS_MATCHED&section=ss_0_0_0&date_range=current_day&sort_order_ss_0_0_0=desc&report_def_id=mga_content_filters
```

Basic HTTP 認証クレデンシャルの追加

URL に Basic HTTP 認証クレデンシャルを指定する例を次に示します。

```
http://example.com/monitor/
```

次のようになります。

```
http://username:password@example.com/monitor/
```

ファイル形式

ダウンロードされるファイルは CSV 形式であり、ファイル拡張子は `.csv` です。ファイル見出しは、デフォルトのファイル名であり、レポートの名前に始まり、レポートのセクションが続きます。

タイムスタンプ

データのストリーミングを行うエクスポートには、各行の時間「間隔」について開始タイムスタンプおよび終了タイムスタンプが示されます。2 種類の開始タイムスタンプおよび終了タイムスタンプ（数値形式および人間が読み取れる文字列形式）が提供されます。タイムスタンプは GMT 時間です。これにより、アプライアンスが複数の時間帯にある場合、ログの集約が容易になります。

あまりないことですが、データが他のソースのデータとマージされる場合には、エクスポート ファイルにタイムスタンプは含まれません。たとえば、発生の詳細のエクスポートでは、レポートのデータと Threat Operations Center (TOC) データがマージされ、タイムスタンプが不適切になります。これは、間隔が存在しないためです。

キー

レポートにキーが表示されない場合であっても、エクスポートには、レポート テーブル キーが含まれます。キーが表示される場合、レポートに表示される表示名がカラム見出しとして使用されます。それ以外の場合は、「key0」、「key1」などのカラム見出しが表示されます。

ストリーミング

大部分のエクスポートでは、データをクライアントにストリーミングで戻します。これは、データ量が非常に大きい可能性があるからです。しかし、一部のエクスポートでは、ストリーミング データではなく結果セット全体を返します。通常、レポート データが非レポート データ（発生の詳細など）と集約される場合が該当します。

レポーティングの概要

AsyncOS におけるレポーティングには、次の 3 つの基本動作が含まれます。

- 日単位、週単位、または月単位で実行されるスケジュール設定されたレポートを作成できます。
- ただちにレポートを生成できます（「オンデマンド」レポート）。
- 以前実行したレポートのアーカイブ版を表示できます（スケジュール設定されたレポートおよびオンデマンド レポートの両方）。

スケジュール設定されたレポートおよびオンデマンド レポートは、[モニタ (Monitor)] > [定期レポート (Scheduled Reports)] ページから設定できます。アーカイブ済みレポートは、[モニタ (Monitor)] > [アーカイブ レポート (Archived Reports)] ページから表示できます。

アプライアンスは、生成した最新のレポートを保持します（すべてのレポートに対して、最大で合計 1000 バージョン）。必要に応じた数（ゼロも含む）のレポート受信者を定義できます。電子メール受信者を指定しない場合でも、レポートはアーカイブされます。レポートを多数のアドレスに送信する必要がある場合、個別に受信者を設定するよりも、メーリングリストを作成するほうが容易です。

デフォルトでは、スケジュール設定された各レポートのうち、直近の 12 のレポートがアーカイブされます。レポートは、アプライアンスの /saved_reports ディレクトリに保管されます（詳細については、[付録 A 「アプライアンスへのアクセス」](#) を参照してください）。

スケジュール設定されたレポートの種類

次のレポートの種類から選択できます。

- コンテンツ フィルタ
- 配信ステータス
- DLP インシデント サマリー
- 要約
- 着信メール サマリー
- 内部ユーザ サマリー
- 発信先
- 発信メール サマリー
- 発信送信者：ドメイン
- 送信者グループ
- システム キャパシティ
- TLS 接続
- アウトブレイク フィルタ
- ウイルスの種類

各レポートは、対応する電子メール セキュリティ モニタ ページのサマリーで構成されます。したがって、たとえばコンテンツ フィルタ レポートでは、[**モニタ (Monitor)**] > [**コンテンツ フィルタ (Content Filters)**] ページに表示される情報のサマリーが示されます。要約レポートは、[**モニタ (Monitor)**] > [**概要 (Overview)**] ページに基づいています。

レポートに関する注意事項

PDF 形式のコンテンツ フィルタ レポートは、最大 40 のコンテンツ フィルタに制限されます。完全なリストは、CSV 形式のレポートで入手できます。



(注) Windows コンピュータ上で中国語、日本語、または韓国語の PDF を生成するには、[Adobe.com](https://www.adobe.com) から該当するフォント パックをダウンロードしてローカル コンピュータにインストールすることも必要です。

レポート用返信アドレスの設定

レポートに返信アドレスを設定するには、「[アプライアンスに生成されるメッセージの返信アドレスの設定](#)」(P.29-29) を参照してください。CLI から、`addressconfig` コマンドを使用します。

レポートの管理

アーカイブ済みのスケジュール設定されたレポートは、作成、編集、削除、および表示を行うことができます。ただちにレポートを実行することもできます (オンデマンド レポート)。コンテンツ フィルタ、DLP インシデント サマリー、要約、着信メール サマリー、内部ユーザ サマリー、発信メール サマリー、送信者グループ、およびアウトブレイク フィルタの各レポートを使用できます。これらのレポートの管理および表示については、後述します。



(注) クラスタ モードでは、レポートを表示できません。マシン モードの場合、レポートを表示できます。

[**モニタ (Monitor)**] > [**定期レポート (Scheduled Reports)**] ページには、アプライアンスで生成済みのスケジュール設定されたレポートのリストが示されます。


スケジュール設定されたレポート

スケジュール設定されたレポートは、日単位、週単位、または月単位で実行するようにスケジュール設定できます。レポートを実行する時間を選択できます。レポートを実行する時間には関係なく、指定した期間 (たとえば、過去 3 日または前の 1 か月) のデータのみが含まれます。午前 1 時に実行するようにスケジュール設定されている日単位のレポートには、前の日 (午前 0 時~午前 0 時) のデータが含まれることに注意してください。

お使いのアプライアンスは、デフォルトのレポート セットがスケジュール設定された状態で出荷されています。このレポート セットのいずれかを使用したり、変更や削除を行ったりすることができます。

自動的に生成するレポートのスケジュール

手順

-
- ステップ 1** [モニタ (Monitor)] > [定期レポート (Scheduled Reports)] ページで、[定期レポートを追加 (Add Scheduled Report)] をクリックします。
- ステップ 2** レポートの種類を選択します。選択したレポートの種類に応じて、異なるオプションを使用できます。使用可能なスケジュール設定されたレポートの種類の詳細については、「[スケジュール設定されたレポートの種類](#)」(P.26-44) を参照してください。
- ステップ 3** レポートのわかりやすいタイトルを入力します。AsyncOS では、レポート名が一意かどうかは確認されません。混乱を避けるために、同じ名前でも複数のレポートを作成しないでください。
- ステップ 4** レポート データの時間範囲を選択します (アウトブレイク フィルタ レポートでは、このオプションを使用できません)。
- ステップ 5** レポートの形式を選択します。
- [PDF]。配信用、アーカイブ用、またはその両方の用途で PDF 形式のドキュメントを作成します。[PDF レポートをプレビュー (Preview PDF Report)] をクリックすると、ただちに PDF ファイルでレポートを表示できます。
英語以外の言語での PDF の生成については、「[レポートに関する注意事項](#)」(P.26-45) を参照してください。
 - [CSV]。カンマ区切りの表データを含む ASCII テキスト ファイルを作成します。各 CSV ファイルには、最大 100 行を含めることができます。レポートに複数の種類の表が含まれる場合、各表に対して別個の CSV ファイルが作成されます。
- ステップ 6** 使用可能な場合は、レポート オプションを指定します。レポートによっては、レポート オプションはありません。
- ステップ 7** スケジュールおよび配信オプションを指定します。電子メール アドレスを指定しない場合、レポートはアーカイブされますが、いずれの受信者にも送信されません。
-  **(注)** 外部アカウント (Yahoo または Gmail など) にレポートを送信する場合、外部アカウントのホワイトリストにレポート返信アドレスを追加して、レポートの電子メールが誤ってスパムに分類されないようにすることが推奨されます。
-
- ステップ 8** [送信 (Submit)] をクリックします。変更内容を確定します。
-

スケジュール設定されたレポートの編集

手順

-
- ステップ 1** [サービス (Services)] > [集約管理レポート (Centralized Reporting)] ページでリストのレポート タイトルをクリックします。
- ステップ 2** 変更を行います。
- ステップ 3** 変更内容を送信し、確定します。
-

スケジュール設定されたレポートの削除

手順

- ステップ 1** [サービス (Services)] > [集約管理レポート (Centralized Reporting)] ページで、削除するレポートに対応するチェックボックスをオンにします。



(注) スケジュール設定されたレポートをすべて削除するには、[すべて (All)] チェックボックスをオンにします。

- ステップ 2** [削除 (Delete)] をクリックします。

- ステップ 3** 削除を確認し、変更内容を確定させます。

削除されたレポートのアーカイブ版は、自動的に削除されるわけではありません。

アーカイブ済みのレポート

[モニタ (Monitor)] > [アーカイブ レポート (Archived Reports)] ページでは、使用可能なアーカイブ済みのレポートのリストが表示されます。[レポートのタイトル (Report Title)] カラムの名前をクリックすると、レポートを表示できます。[今すぐレポートを生成 (Generate Report Now)] をクリックすると、ただちにレポートを生成できます。

リストに表示されるレポートの種類をフィルタリングするには、[表示 (Show)] メニューを使用します。リストをソートするには、カラム見出しをクリックします。

アーカイブ済みのレポートは、自動的に削除されます。スケジュール設定された各レポートの最大 12 インスタンス (最大 1000 レポート) が保存され、新たなレポートが追加されると、古いレポートが削除されてレポートの数は 1000 に維持されます。12 インスタンスという制限は、レポートの種類に対してではなく、個別のスケジュール設定された各レポートに対して適用されます。

図 26-29 アーカイブ済みのレポート
Archived Reports

Available Reports			
Report Title	Type	Time Range	Generated on
Virus Outbreaks	Virus Outbreaks	Custom	Thu 19 Oct 2006 17:32 (GMT)
Incoming Mail Summary	Incoming Mail Summary	Calendar Week	Thu 19 Oct 2006 17:31 (GMT)
Executive Summary	Executive Summary	Calendar Week	Thu 19 Oct 2006 17:31 (GMT)
Content Filters	Content Filters	Calendar Week	Thu 19 Oct 2006 17:31 (GMT)

オンデマンド レポートの生成

レポートは、スケジュールを設定しなくても生成できます。これらのオンデマンド レポートも指定したタイム フレームに基づいていますが、ただちに生成できます。

手順

-
- ステップ 1** [アーカイブ レポート (Archived Reports)] ページで [今すぐレポートを生成 (Generate Report Now)] をクリックします。
- ステップ 2** レポートの種類を選択し、必要に応じてタイトルを編集します。AsyncOS では、レポート名が一意かどうかは確認されません。混乱を避けるために、同じ名前でも複数のレポートを作成しないでください。使用可能なスケジュール設定されたレポートの種類の詳細については、「[スケジュール設定されたレポートの種類](#)」(P.26-44) を参照してください。
- ステップ 3** レポート データの時間範囲を選択します (ウイルス発生レポートでは、このオプションを使用できません)。カスタムの範囲を作成した場合は、その範囲がリンクとして表示されます。範囲を変更するには、そのリンクをクリックします。
- ステップ 4** レポートの形式を選択します。
- [PDF]。配信用、アーカイブ用、またはその両方の用途で PDF 形式のドキュメントを作成します。[PDF レポートをプレビュー (Preview PDF Report)] をクリックすると、ただちに PDF ファイルでレポートを表示できます。英語以外の言語での PDF の生成については、「[レポートに関する注意事項](#)」(P.26-45) を参照してください。
 - [CSV]。カンマ区切りの表データを含む ASCII テキスト ファイルを作成します。各 CSV ファイルには、最大 100 行を含めることができます。レポートに複数の種類の表が含まれる場合、各表に対して別個の CSV ファイルが作成されます。任意のレポート オプションを指定します。
- ステップ 5** レポートをアーカイブするかどうかを選択します (アーカイブする場合には、レポートが [アーカイブ レポート (Archived Reports)] ページに表示されます)。
- ステップ 6** レポートを電子メールで送信するかどうか、レポートの送信先の電子メール アドレスを指定します。
- ステップ 7** [このレポートを配信 (Deliver this Report)] をクリックしてレポートを生成し、受信者に配信するか、このレポートをアーカイブします。
- ステップ 8** 変更内容を確定します。
-

電子メール レポートのトラブルシューティング

問題 メッセージ トラッキングで詳細情報を表示するためにドリル ダウンすると、予期しない結果が表示されます。

ソリューション これはレポーティングおよびメッセージ トラッキングが同時にイネーブルにされていない、正常に動作していない、そして (セキュリティ管理アプライアンス上に集中的に保存するのではなく) データをローカルに保存している場合に発生する可能性があります。各機能のデータ (レポートおよびメッセージ トラッキング) は、他の機能 (レポートまたはメッセージ トラッキング) がイネーブルおよび動作しているかどうかに関係なく、機能がイネーブルにされてアプライアンス上で動作している間のみ保存されます。そのため、レポートにはメッセージ トラッキングで使用できないデータが含まれることがあり、その反対も起こり得ます。



CHAPTER 27

隔離

- 「隔離の概要」 (P.27-1)
- 「ポリシー、ウイルス、およびアウトブレイク隔離の管理」 (P.27-3)
- 「ポリシー、ウイルス、またはアウトブレイク隔離のメッセージの操作」 (P.27-11)
- 「スパム隔離の概要」 (P.27-19)
- 「スパム隔離の設定」 (P.27-19)
- 「スパム隔離内のメッセージの管理」 (P.27-33)
- 「送信者に基づいて電子メール配信を制御するセーフリストおよびブロックを使用」 (P.27-36)

隔離の概要

電子メールセキュリティ アプライアンスが危険性のあるスパム、マルウェア、または組織で許可されていないコンテンツを送受信メッセージで検出した場合、すぐに削除してしまわずに隔離エリアに送信します。隔離エリアはこれらのコンテンツを電子メールセキュリティ アプライアンス またはシスコのコンテンツセキュリティ管理アプライアンスで一定期間安全に保持し、ユーザがそれらを評価するまで、またはメッセージの安全性を適切に評価できるアップデートまで待ちます。

組織での隔離の使用例

- **ポリシーの実施。** 人事担当部門または法務部門が、それらに不快な情報や秘密情報などの許可されない情報が含まれていないか確認します。
- **ウイルス隔離。** ユーザへのウイルスの拡散を防ぐためのアンチウイルス スキャン エンジンによって、暗号化メッセージや感染メッセージまたはスキャン不可能とマークされたメッセージを保管します。
- **アウトブレイクの防止。** アウトブレイク フィルタによってウイルスのアウトブレイクの一部または小規模なマルウェア攻撃としてフラグ付けされたメッセージを、アンチ ウイルスまたはアンチスパム アップデートがリリースされるまで保管します。
- **スパム管理。** エンド ユーザまたは管理者は、必要なメッセージの削除を防ぐために、メッセージがスパムであるかどうか判断します。

隔離のタイプ

隔離タイプ	隔離名	システムにデフォルトで作成されるか	説明	追加情報
ウイルス (Virus)	Virus	Yes	アンチウイルス エンジンによる判定に従って、マルウェアを送信する可能性のあるメッセージを保持します。	<ul style="list-style-type: none"> 「ポリシー、ウイルス、およびアウトブレイク隔離の管理」(P.27-3) 「ポリシー、ウイルス、またはアウトブレイク隔離のメッセージの操作」(P.27-11)
アウトブレイク (Outbreak)	Outbreak	Yes	アウトブレイク フィルタによってスパムまたはマルウェアの可能性があると検出されたメッセージを保持します。	
ポリシー (Policy)	Policy	Yes	メッセージ フィルタ、コンテンツ フィルタ、DLP メッセージアクションによって検出されたメッセージを保持します。 デフォルトのポリシー隔離が作成されています。	
	Unclassified	Yes	メッセージ フィルタ、コンテンツ フィルタ、DLP メッセージアクションで指定した隔離が削除された場合にのみ、メッセージを保持します。 この隔離をフィルタまたはメッセージアクションに対してり当てることはできません。	
	(自分で作成するポリシー隔離)	No	メッセージ フィルタ、コンテンツ フィルタおよび DLP メッセージアクションで使用するために作成するポリシー隔離。	
スパム (Spam)	Spam	Yes	メッセージの受信者または管理者が確認するように、スパムおよびその疑いのあるメッセージを保持します。	<ul style="list-style-type: none"> 「スパム隔離の概要」(P.27-19) 「スパム隔離の設定」(P.27-19) 「送信者に基づいて電子メール配信を制御するセーフリストおよびブロックを使用」(P.27-36)

ローカル隔離

- [ポリシー、ウイルス、およびアウトブレイク隔離の管理](#)
- [ポリシー、ウイルス、またはアウトブレイク隔離のメッセージの操作](#)

ポリシー、ウイルス、およびアウトブレイク隔離の管理

- [「ポリシー、ウイルス、およびアウトブレイク隔離に対するディスク領域の割り当て」 \(P.27-3\)](#)
- [「隔離エリアのメッセージ保存期間」 \(P.27-4\)](#)
- [「自動的に処理された隔離メッセージのデフォルト アクション」 \(P.27-5\)](#)
- [「システムが作成した隔離の設定の確認」 \(P.27-5\)](#)
- [「ポリシー隔離の作成」 \(P.27-6\)](#)
- [「ポリシー、ウイルス、アウトブレイク隔離の設定の編集方法」 \(P.27-7\)](#)
- [「フィルタおよびメッセージアクションに割り当てる隔離を決定する」 \(P.27-7\)](#)
- [「ポリシー隔離の削除について」 \(P.27-8\)](#)
- [「隔離のステータス、容量、アクティビティのモニタリング」 \(P.27-8\)](#)
- [「ポリシー隔離のパフォーマンス」 \(P.27-9\)](#)
- [「隔離のディスク領域の使用状況についてのアラート」 \(P.27-9\)](#)
- [「ポリシー隔離とロギング」 \(P.27-9\)](#)
- [「メッセージ処理作業の他のユーザへの分配」 \(P.27-10\)](#)
- [「クラスタ設定におけるポリシー、ウイルス、およびアウトブレイク隔離について」 \(P.27-11\)](#)
- [「ポリシー、ウイルス、アウトブレイク隔離の設定の集約方法」 \(P.27-11\)](#)

ポリシー、ウイルス、およびアウトブレイク隔離に対するディスク領域の割り当て

ポリシー、ウイルス、アウトブレイク隔離は、ハードウェア モデルによってサイズが異なる、単一のディスク領域のプールを共有します。

複数の隔離のメッセージは、1 つの隔離のメッセージと同じ容量のディスク領域を消費します。

表 27-1 すべてのポリシー、ウイルス、アウトブレイク隔離の合計ディスク容量

モデル	ポリシーおよびウイルス隔離の合計ディスク容量 (MB 単位) (アウトブレイク フィルタ無効)	ポリシー、ウイルス、アウトブレイク隔離の合計ディスク容量 (MB 単位) (アウトブレイク フィルタ有効)
C100V	2560	3584
C160		
C170		
C360	4096	6144
C360(D)		
C370		
C380		
C300V	10240	13312
C600V		
C660		
C670		
C680		
X1060		
X1070		

関連項目

- 「隔離のステータス、容量、アクティビティのモニタリング」 (P.27-8)
- 「隔離のディスク領域の使用状況についてのアラート」 (P.27-9)
- 「隔離エリアのメッセージ保存期間」 (P.27-4)

隔離エリアのメッセージ保存期間

メッセージは次のタイミングで隔離から自動的に削除されます。

- 通常の期限切れ：隔離エリア内のメッセージが保存期間を満了する場合です。各隔離エリアのメッセージの保存期間を指定します。各メッセージには、それぞれ独自の有効期限があり、隔離のリストに表示されます。このトピックで説明される別の状況が発生しなければ、メッセージは指定された時間が経過するまで保管されます。



(注) アウトブレイク フィルタ隔離エリアでのメッセージの通常の保存期間は、アウトブレイク隔離ではなく各メールのアウトブレイク フィルタ セクションで設定します。

- 早期の期限切れ：設定した保存期間に到達する前にメッセージが隔離エリアから強制的に削除される場合です。これは次の場合に発生する可能性があります。
 - 「ポリシー、ウイルス、およびアウトブレイク隔離に対するディスク領域の割り当て」 (P.27-3) で定義した、すべての隔離エリアのサイズ制限に達する。

サイズ制限に到達すると、隔離に関係なく、古いメッセージから処理されます。すべての隔離エリアのサイズがサイズ制限未満に戻るまで、各メッセージに対してデフォルトアクションが実行されます。このポリシーは、先入れ先出し（FIFO）です。複数の隔離のメッセージは、最新の有効期限に基づいて期限切れになります。

（任意）ディスク容量不足によるリリースまたは削除から除外するように、個々の隔離を設定できます。すべての隔離で除外するように設定してディスク容量が満杯になった場合、新しいメッセージのための領域を確保するために隔離エリア内のメッセージが配信されます。

ディスク容量のマイルストーンについてアラートが送信されます。「[隔離のディスク領域の使用状況についてのアラート](#)」(P.27-9) を参照してください。

- まだメッセージを保持している隔離を削除します。

メッセージが隔離から自動的に削除される場合、デフォルトアクションがメッセージに対して実行されます。「[自動的に処理された隔離メッセージのデフォルトアクション](#)」(P.27-5) を参照してください。

保存期間への時間調整の影響

- サマータイムとアプライアンスのタイムゾーンの変更は保存期間に影響しません。
- 隔離の保存期間を変更すると、新しいメッセージにだけ新しい有効期限が適用されます。
- システムクロックを変更すると、以前期限切れになるはずだったメッセージが次の最も適切な時間に期限切れになります。
- システムクロックの変更は期限切れの処理中のメッセージには適用されません。

自動的に処理された隔離メッセージのデフォルトアクション

デフォルトアクションは、「[隔離エリアのメッセージ保存期間](#)」(P.27-4) に記述されるいずれかの状況が発生した場合、ポリシー、ウイルス、アウトブレイク隔離エリア内のメッセージに対して実行されます。

2つの主要なデフォルトアクションがあります。

- [削除 (Delete)] : メッセージが削除されます。
- [リリース (Release)] : メッセージが解放されて配信されます。

リリース時に、メッセージはアンチウイルスまたはアンチスパムエンジンによって再スキャンされる場合があります。詳細については、「[隔離されたメッセージの再スキャンについて](#)」(P.27-18) を参照してください。

さらに、予定される保存期間よりも前にリリースされるメッセージには、X-Header の追加などの操作が行われる場合があります。詳細については、「[ポリシー隔離の作成](#)」(P.27-6) を参照してください。

システムが作成した隔離の設定の確認

隔離を使用する前に、未分類隔離などのデフォルトの隔離設定をカスタマイズします。

ポリシー隔離の作成

はじめる前に

- 保存期間やデフォルトアクションなど、隔離エリア内のメッセージが自動的に管理される方法を確認します。「[隔離エリアのメッセージ保存期間](#)」(P.27-4)、および「[自動的に処理された隔離メッセージのデフォルトアクション](#)」(P.27-5)を参照してください。
- 各隔離エリアにアクセスできるユーザを決め、ユーザおよびカスタムユーザロールを適宜作成します。詳細については、「[隔離にアクセスできるユーザグループ](#)」(P.27-10)を参照してください。

手順

ステップ 1 [モニタ (Monitor)] > [ポリシー、ウイルスおよびアウトブレイク隔離 (Policy, Virus, and Outbreak Quarantines)] を選択します。

ステップ 2 [ポリシー隔離の追加 (Add Policy Quarantine)] をクリックします。

ステップ 3 情報を入力します。

次の点を考慮してください。

- 隔離の名前は変更できません。
- 隔離ディスク領域が一杯になった場合でも、指定した保存期間の終了前にこの隔離メッセージを処理されたくない場合、[メッセージに対してデフォルトのアクションを適用して空き容量を増やす (Free up space by applying default action on messages upon space overflow)] の選択を解除します。

このオプションはすべての隔離では選択しないでください。システムは、少なくとも 1 つの隔離エリアからメッセージを削除して、領域を確保する必要があります。

- デフォルトアクションとして [リリース (Release)] を選択すると、保存期間が経過する前にリリースされるメッセージに適用される追加のアクションを指定できます。

オプション	情報
件名の変更 (Modify Subject)	追加するテキストを入力し、そのテキストを元のメッセージの件名の前と後ろのどちらに追加するかを選択します。 たとえば、受信者に不適切なコンテンツを含む可能性があるメッセージであることを警告します。 (注) 非 ASCII 文字を含む件名を正しく表示するために、件名は RFC 2047 に従って表記されている必要があります。
X-Header の追加 (Add X-Header)	X-Header ではメッセージで実行されたアクションを記録できます。これはたとえば、特定のメッセージが配信された理由についての照会を処理する際に役立つ場合があります。 名前と値を入力します。 例： Name =Inappropriate-release-early Value = True
添付ファイルの削除 (Strip Attachments)	添付ファイルを削除すると、このようなファイル中に存在する可能性のあるウイルスから保護します。

ステップ 4 この隔離エリアにアクセス可能なユーザを指定してください。

ユーザ	情報
ローカル ユーザ	ローカル ユーザ リストには、隔離エリアにアクセスできるロールを持つユーザだけが含まれます。 すべての管理者は隔離にすべてのアクセス権限を持つため、リストでは管理者権限を持つユーザを除外します。
外部認証されたユーザ	外部認証を設定する必要があります。
カスタム ユーザ ロール	このオプションは、隔離へのアクセス権限を持つ少なくとも 1 つのカスタム ユーザ ロールを作成している場合のみ表示されます。

ステップ 5 変更内容を送信し、確定します。

次の作業

メッセージおよびコンテンツ フィルタ、メッセージを隔離エリアに移動する DLP メッセージアクションを作成します。第 9 章「メッセージフィルタを使用した電子メール ポリシーの適用」、第 11 章「コンテンツ フィルタ」、および「メッセージアクション」(P.15-33) を参照してください。

ポリシー、ウイルス、アウトブレイク隔離の設定の編集方法



(注)

- 隔離の名前は変更できません。
- 「保存期間への時間調整の影響」(P.27-5) も参照してください。

隔離の設定を変更するには、[モニタ (Monitor)] > [ポリシー、ウイルスおよびアウトブレイク隔離 (Policy, Virus, and Outbreak Quarantines)] を選択し、隔離名をクリックします。

フィルタおよびメッセージアクションに割り当てる隔離を決定する

隔離に関連付けられているメッセージ フィルタ、コンテンツ フィルタおよび DLP メッセージアクションを表示できます。

手順

- ステップ 1** [モニタ (Monitor)] > [ポリシー、ウイルスおよびアウトブレイク隔離 (Policy, Virus, and Outbreak Quarantines)] をクリックします。
- ステップ 2** 確認するポリシー隔離の名前をクリックします。
- ステップ 3** ページの下部までスクロールし、[関連付けられたメッセージフィルタ/コンテンツ フィルタ/DLP メッセージアクション (Associated Message Filters/Content Filters/DLP Message Actions)] を照会します。

ポリシー隔離の削除について

- ポリシー隔離を削除する前に、アクティブなフィルタまたはメッセージアクションと関連付けられているかどうかを確認します。「[フィルタおよびメッセージアクションに割り当てる隔離を決定する](#)」(P.27-7) を参照してください。
- フィルタまたはメッセージアクションに割り当てられている場合でも、ポリシー隔離を削除できます。
- 空でない隔離を削除する場合、ディスクがいっぱいになった際にメッセージを削除しないオプションを選択した場合でも、隔離で定義されたデフォルトアクションはすべてのメッセージに適用されます。「[自動的に処理された隔離メッセージのデフォルトアクション](#)」(P.27-5) を参照してください。
- フィルタまたはメッセージアクションと関連付けられた隔離を削除した後、フィルタまたはメッセージアクションにより隔離されたメッセージは未分類隔離に送られます。隔離を削除する前に、未分類隔離のデフォルト設定をカスタマイズする必要があります。
- 未分類隔離は削除できません。

隔離のステータス、容量、アクティビティのモニタリング

内容	操作内容
スパム隔離以外のすべての隔離で現在使用できる領域	[モニタ (Monitor)] > [ポリシー、ウイルスおよびアウトブレイク隔離 (Policy, Virus, and Outbreak Quarantines)] を選択し、表の真下を参照してください。
現在すべての隔離が使用している合計容量	[モニタ (Monitor)] > [システム ステータス (System Status)] を選択し、[隔離に使用されるキュー スペース (Queue Space Used by Quarantine)] を探します。
現在各隔離に使用されている容量	[モニタ (Monitor)] > [ポリシー、ウイルスおよびアウトブレイク隔離 (Policy, Virus, and Outbreak Quarantines)] を選択し、隔離名をクリックして、隔離の名前の直下にある表の行で、この情報を検索します。
現在すべての隔離にあるメッセージの総数	[モニタ (Monitor)] > [システム ステータス (System Status)] を選択し、[隔離内のアクティブ メッセージ (Active Messages in Quarantine)] を探します。
現在各隔離にあるメッセージ数	[モニタ (Monitor)] > [ポリシー、ウイルスおよびアウトブレイク隔離 (Policy, Virus, and Outbreak Quarantines)] を選択し、該当の隔離行を表で探します。
すべての隔離による総 CPU 使用率	[モニタ (Monitor)] > [システム ステータス (System Status)] を選択し、[CPU 使用率 (CPU Utilization)] セクションを確認します。
最後のメッセージが各隔離に送信された日時 (隔離間の移動を除く)	[モニタ (Monitor)] > [ポリシー、ウイルスおよびアウトブレイク隔離 (Policy, Virus, and Outbreak Quarantines)] を選択し、該当の隔離行を表で探します。

内容	操作内容
ポリシー隔離が作成された日時	[モニタ (Monitor)] > [ポリシー、ウイルスおよびアウトブレイク隔離 (Policy, Virus, and Outbreak Quarantines)] を選択し、隔離名をクリックして、隔離の名前の直下にある表の行で、この情報を検索します。 作成日および作成者の名前は、システムが作成した隔離では使用できません。
ポリシー隔離の作成者の名前	
隔離に関連付けられたフィルタおよびメッセージアクション	「 フィルタおよびメッセージアクションに割り当てる隔離を決定する 」(P.27-7) を参照してください。

ポリシー隔離のパフォーマンス

ポリシー隔離エリアに保存されたメッセージは、ハードドライブ容量に加えて、システムメモリを使用します。1つのアプライアンスのポリシー隔離エリア内で数十万メッセージを保存すると、過剰なメモリ使用によりアプライアンスのパフォーマンスが低下することがあります。アプライアンスでのメッセージの隔離、削除、および解放により多くの時間が必要になるため、メッセージ処理の速度が低下し、電子メールパイプラインが渋滞します。

シスコは、電子メールセキュリティアプライアンスが標準レートで電子メールを処理できるようにポリシー隔離で保存するメッセージを平均 20,000 未満にすることを推奨します。

隔離のメッセージ数を調べるには、「[隔離のステータス、容量、アクティビティのモニタリング](#)」(P.27-8) を参照してください。

隔離のディスク領域の使用状況についてのアラート

ポリシー、ウイルスおよびアウトブレイク隔離エリアの合計容量が 75% 以上、85% 以上および 95% 以上になると、アラートが送信されます。このチェックは、メッセージが隔離エリアに入れられたときに実行されます。たとえば、メッセージが隔離に追加されたときに隔離エリアの合計サイズが指定容量の 75% 以上に増加すると、アラートが送信されます。

アラートの詳細については、[第 29 章「アラート」](#) を参照してください。

ポリシー隔離とロギング

AsyncOS により、隔離されるすべてのメッセージが個別にロギングされます。

```
Info: MID 482 quarantined to "Policy" (message filter:policy_violation)
```

括弧内には、メッセージを隔離させたメッセージフィルタまたはアウトブレイクフィルタ機能のルールが出力されます。メッセージが入れられる隔離ごとに独立したログエントリが生成されます。

また、AsyncOS により、隔離エリアから除去されるメッセージも個別にロギングされます。

```
Info: MID 483 released from quarantine "Policy" (queue full)
```

```
Info: MID 484 deleted from quarantine "Anti-Virus" (expired)
```

メッセージがすべての隔離エリアから除去され、完全に削除されるか、配信用にスケジュールされると、それらのメッセージはシステムによって次のように個別にロギングされます。

```
Info: MID 483 released from all quarantines
```

```
Info: MID 484 deleted from all quarantines
```

メッセージが再注入されると、新しいメッセージ ID (MID) を持つ新しいメッセージオブジェクトがシステムによって作成されます。このことは、次のように新しい MID 「by 行」がある既存のログメッセージを使用してロギングされます。

```
Info: MID 483 rewritten to 513 by System Quarantine
```

メッセージ処理作業の他のユーザへの分配

メッセージの処理および確認タスクを、他の管理者ユーザへ分配することができます。次に例を示します。

- 人事部門のチームはポリシー隔離の確認と管理ができます。
- 法務部門のチームは Confidential Material 隔離を管理できます。

隔離の設定を指定する際に、これらのユーザにアクセス権限を割り当てます。隔離にユーザを追加するには、追加するユーザがすでに存在する必要があります。

各ユーザは、すべてまたは一部の隔離にアクセスできるようにすることも、まったくアクセスできないようにすることもできます。隔離の閲覧を許可されていないユーザに対しては、GUI または CLI の隔離のリスト表示のどの場所でも、その隔離の存在は一切表示されません。

関連項目

- 「[隔離にアクセスできるユーザグループ](#)」 (P.27-10)
- 「[ユーザアカウントを使用する作業](#)」 (P.28-1)
- 「[外部認証 \(External Authentication\)](#)」 (P.28-21)
- 「[委任管理のためのカスタム ユーザ ロールの管理](#)」 (P.28-7)

隔離にアクセスできるユーザグループ

ユーザが隔離にアクセスできるようにする際に、実行できるアクションはユーザグループごとに異なります。

- 管理者グループのユーザは、隔離エリアの作成、設定、削除、集約化、および隔離されたメッセージを管理することができます。
- オペレータ、ゲスト、読み込み専用オペレータ、ヘルプデスク ユーザおよび隔離管理権限を持つカスタム ユーザ ロールは、隔離エリア内のメッセージの検索、閲覧および処理が可能ですが、隔離の設定変更、作成、削除、または集約することはできません。各隔離にどのユーザがアクセスできるかを指定します。
- Technicians グループに属するユーザは隔離にアクセスできません。

また、メッセージトラッキングおよびデータ消失防止など、関連機能のアクセス権限によって、[隔離 (Quarantine)] ページで表示されるオプションおよび情報が変わります。たとえば、メッセージトラッキングにアクセスできないユーザの場合、そのユーザにはメッセージトラッキングリンクおよび隔離されたメッセージに関する情報が表示されません。

クラスタ設定におけるポリシー、ウイルス、およびアウトブレイク隔離について

集中管理のためにクラスタで電子メールセキュリティアプライアンスを導入する場合、隔離エリアのディスク領域がモデルによって異なるため、ポリシー、ウイルスおよびアウトブレイク隔離はマシンレベルでのみ設定できます。

ポリシー、ウイルス、アウトブレイク隔離の設定の集約方法

シスコのコンテンツセキュリティ管理アプライアンス上でポリシー、ウイルス、およびアウトブレイク隔離を中央集中型にできます。詳細については、「一元化されたポリシー、ウイルス、アウトブレイク隔離について」(P.38-4) およびお使いのセキュリティ管理アプライアンスのユーザマニュアルを参照してください。

ポリシー、ウイルス、またはアウトブレイク隔離のメッセージの操作

- 「隔離エリア内のメッセージの表示」(P.27-11)
- 「ポリシー、ウイルスおよびアウトブレイク隔離のメッセージの検索」(P.27-12)
- 「手動で隔離メッセージを処理」(P.27-13)
- 「複数の隔離エリアにあるメッセージ」(P.27-14)
- 「メッセージの詳細およびメッセージ内容の表示」(P.27-15)
- 「隔離されたメッセージの再スキャンについて」(P.27-18)
- 「アウトブレイク隔離」(P.27-18)

隔離エリア内のメッセージの表示

目的	操作内容
隔離エリアのすべてのメッセージを表示する	<p>[モニタ (Monitor)] > [ポリシー、ウイルスおよびアウトブレイク隔離 (Policy, Virus, and Outbreak Quarantines)] を選択します。</p> <p>表の関連する隔離の行で、[メッセージ (Messages)] 列の青い番号をクリックします。</p>
アウトブレイク隔離エリアのメッセージを表示する	<ul style="list-style-type: none"> • [モニタ (Monitor)] > [ポリシー、ウイルスおよびアウトブレイク隔離 (Policy, Virus, and Outbreak Quarantines)] を選択します。 <p>表の関連する隔離の行で、[メッセージ (Messages)] 列の青い番号をクリックします。</p> <ul style="list-style-type: none"> • 「ルールサマリーによる管理リンク」(P.27-19) を参照してください。

目的	操作内容
隔離エリアのメッセージのリスト内で移動する	[前へ (Previous)]、[次へ (Next)]、ページ番号または二重矢印のリンクをクリックします。二重矢印を使用すると、リストの先頭 ([<<]) または最後 ([>>]) のページに移動します。
隔離エリアのメッセージのリストをソートする	カラム見出しをクリックします (カラムに複数の項目が含まれる場合と [その他の隔離 (In other quarantines)] カラムを除く)。
テーブル カラムのサイズを変更する	カラム見出し間の境界線をドラッグします。
メッセージの隔離の原因となるコンテンツを表示する	「一致した内容の表示」 (P.27-15) を参照してください。

隔離されたメッセージおよび国際文字セット

メッセージの件名に国際文字セット (2 バイト、可変長、および非 ASCII の符号化) の文字が含まれる場合、[ポリシー隔離 (Policy Quarantine)] ページでは、非 ASCII 文字の件名行が復号化された形式で表示されます。

ポリシー、ウイルスおよびアウトブレイク隔離のメッセージの検索



(注)

- ポリシー、ウイルスおよびアウトブレイク隔離の検索では、スパム隔離メッセージは見つかりません。
- ユーザは、アクセスできる隔離メッセージだけを検索および表示することができます。

手順

ステップ 1 [モニタ (Monitor)] > [ポリシー、ウイルスおよびアウトブレイク隔離 (Policy, Virus, and Outbreak Quarantines)] を選択します。

ステップ 2 [隔離全体を検索 (Search Across Quarantines)] ボタンをクリックします。



ヒント アウトブレイク隔離に対して、各アウトブレイク ルールによって隔離されたすべてのメッセージも検索できます。アウトブレイク テーブル行で [ルール サマリーによる管理 (anage by Rule Summary)] リンクをクリックします

ステップ 3 検索する隔離を選択します。

ステップ 4 (任意) 他の検索条件を入力します。

- [エンベロープ送信者 (Envelope Sender)] および [エンベロープ受信者 (Envelope Recipient)] には任意の文字を入力できます。エントリの検証は実行されません。

- 検索結果には、指定した条件のすべてに一致するメッセージだけが含まれます。たとえば、[エンベロープ受信者 (Envelope Recipient)] および [件名 (Subject)] を指定した場合は、[エンベロープ受信者 (Envelope Recipient)] および [件名 (Subject)] に指定された単語の両方に一致するメッセージだけが返されます。

次の作業

これらの検索結果は、隔離のリストを使用するのと同様に使用できます。詳細については、「[手動で隔離メッセージを処理](#)」(P.27-13) を参照してください。

手動で隔離メッセージを処理

手動でメッセージを処理する場合は、[メッセージアクション (Message Actions)] ページからメッセージのメッセージアクションを手動で選択します。



(注)

RSA Enterprise Manager を導入していれば、電子メールセキュリティアプライアンスまたは Enterprise Manager で、隔離されたメッセージを表示できますが、メッセージにアクションを実行するには Enterprise Manager を使用します。Enterprise Manager については、[第 15 章「データ消失防止」](#) を参照してください。

メッセージで次の処理を実行することができます。

- 削除
- リリース
- 隔離エリアで予定していた終了の遅延
- 指定した電子メールアドレスにメッセージのコピーを送信する
- ある隔離エリアから別の隔離エリアにメッセージを移動する

通常、次の実行時に表示されたリストのメッセージに処理を行うことができます。ただし、すべての状況ですべてのアクションが使用できるわけではありません。

- [モニタ (Monitor)] > [ポリシー、ウイルスおよびアウトブレイク隔離 (Policy, Virus, and Outbreak Quarantines)] ページの隔離リストから、隔離エリア内のメッセージ番号をクリックします。
- [隔離全体を検索 (Search Across Quarantines)] をクリックします。
- 隔離の名前をクリックし、隔離内を検索します。

次の手順で、これらの操作を複数のメッセージで同時に実行できます。

- メッセージリストの上部の選択リストからオプションを選択する。
- ページの各メッセージの横のチェックボックスを選択する。
- メッセージリストの上部のテーブル見出しでチェックボックスを選択する。これは画面に表示されているすべてのメッセージにアクションを適用されます。他のページのメッセージは影響を受けません。

その他のオプションもアウトブレイク隔離エリアのメッセージに利用可能です。「[アウトブレイク隔離 (Outbreak Quarantine)] および [ルール サマリーによる管理 (Manage by Rule Summary)] ビュー」(P.14-20) を参照してください。

関連項目

- 「複数の隔離エリアにあるメッセージ」(P.27-14)
- 「自動的に処理された隔離メッセージのデフォルトアクション」(P.27-5)

メッセージのコピーの送信

メッセージのコピーは、Administrators グループに属しているユーザだけが送信できます。

メッセージのコピーを送信するには、[コピーの送信先: (Send Copy To:)] フィールドに電子メールアドレスを入力し、[送信 (Submit)] をクリックします。メッセージのコピーを送信しても、そのメッセージに対してその他のアクションが実行されることはありません。

ポリシー隔離エリア間のメッセージの移動について

1 つのアプライアンス上で、1 つのポリシー隔離から別の隔離に手でメッセージを移動できます。

別の隔離にメッセージを移動する場合次のようになります。

- 有効期限は変わりません。メッセージは、元の隔離の保持期限が適応されます。
- 一致したコンテンツおよび他の関連情報を含め、メッセージが隔離された理由は変更されません。
- あるメッセージが複数の隔離にあり、すでにメッセージのコピーを保持している場所にメッセージを移動した場合、移動したメッセージのコピーの有効期限および隔離の理由は、移動先の隔離エリアに元からあるメッセージのコピーを上書きします。

複数の隔離エリアにあるメッセージ

メッセージが他の 1 つまたは複数の隔離エリア内にある場合、他の隔離エリアにアクセス権があるかどうかにかかわらず、隔離メッセージリストの [その他の隔離 (In other quarantines)] カラムに [はい (Yes)] と表示されます。

複数の隔離エリアにあるメッセージ

- メッセージが存在するすべての隔離エリアから解放されるまで、配信されません。特定の隔離エリアから削除されても、配信されません。
- メッセージが存在するすべての隔離エリアから削除または解放されるまで、どの隔離エリアからも削除されません。

メッセージを解放しようとするユーザはそれらのメッセージが存在する隔離の一部にしかアクセスできない場合があるため、次のルールが適用されます。

- メッセージは、自身が存在するすべての隔離エリアから解放されるまで、どの隔離エリアからも解放されません。
- メッセージは、いずれかの隔離エリア内で削除済みとマークされると、他の隔離エリアからも配信できなくなります。(ただし、解放はできます)。

メッセージが複数の隔離エリア内にキューイングされ、ユーザがそのうちの 1 つまたは複数の隔離にアクセスできない場合は、次のことが起こります。

- ユーザは、ユーザがアクセスできる各隔離についてそのメッセージが存在するかどうか通知されます。

- GUI は、ユーザがアクセスできる隔離のスケジュールされた保存期間の終了日時のみを表示します。(同じメッセージに対して、隔離ごとに別々の終了日時が存在します)。
- ユーザは、そのメッセージを保管している他の隔離の名前を知らされません。
- ユーザには、一致したコンテンツでアクセスできない隔離エリアにメッセージが格納されているものは表示されません。
- メッセージの解放は、ユーザがアクセスできるキューにだけ効果があります。
- ユーザがアクセスできない他の隔離エリアにもメッセージがキューイングされている場合、残りの隔離にアクセスできるユーザによって処理されるまで (あるいは早期または通常の期限切れによって「正常に」メッセージが解放されるまで)、そのメッセージは変更されずに隔離エリア内に残ります。

メッセージの詳細およびメッセージ内容の表示

メッセージの内容を表示したり、[隔離されたメッセージ (Quarantined Message)] ページにアクセスしたりするには、メッセージの件名行をクリックします。

[隔離されたメッセージ (Quarantined Message)] には、[隔離の詳細 (Quarantine Details)] と [メッセージの詳細 (Message Details)] の 2 つのセクションがあります。

[隔離されたメッセージ (Quarantined Message)] ページから、メッセージを読んだり、メッセージアクションを選択したり、メッセージのコピーを送信したり、ウイルス検査を実行したりできます。また、メッセージが隔離エリアから解放されるときに **Encrypt on Delivery** フィルタ アクションによって暗号化されるかどうかを確認することもできます。

[メッセージの詳細 (Message Details)] セクションには、メッセージ本文、メッセージヘッダー、および添付ファイルが表示されます。メッセージ本文は最初の 100 KB だけが表示されます。メッセージがそれよりも長い場合は、最初の 100 KB が表示され、その後に省略記号 (...) が続きます。実際のメッセージが切り捨てられることはありません。この処置は表示目的のためだけに行われます。[メッセージの詳細 (Message Details)] の下部にある [メッセージ部分 (Message Parts)] セクション内の [メッセージ本文 (message body)] をクリックすることにより、メッセージ本文をダウンロードできます。また、添付ファイルのファイル名をクリックすることにより、メッセージの任意の添付ファイルをダウンロードすることもできます。

ウイルスの含まれるメッセージを表示する場合、ご使用のコンピュータにデスクトップ アンチウイルス ソフトウェアがインストールされていると、そのアンチウイルス ソフトウェアから、ウイルスが検出されると警告される場合があります。これは、ご使用のコンピュータに対して脅威ではないため、無視しても問題ありません。

メッセージについてさらに詳細な情報を表示するには、[メッセージトラッキング (Message Tracking)] リンクをクリックします。



(注)

特別なアウトブレイク隔離の場合、追加の機能を利用できます。「[アウトブレイク隔離](#)」(P.27-18) を参照してください。

一致した内容の表示

Attachment Content 条件、Message Body または Attachment 条件、Message 本文条件、または Attachment 内容条件と一致するメッセージに対して隔離アクションを設定した場合、隔離されたメッセージ内の一致した内容を表示できます。メッセージ本文を表示する場合、DLP ポリシー違反の一致

を除き、一致した内容が黄色で強調表示されます。また、`$MatchedContent` アクション変数を使用して、メッセージの一致した内容やコンテンツ フィルタの一致をメッセージの件名に含めることもできます。

一致した内容が添付ファイルに含まれる場合は、その判定結果が **DLP** ポリシー違反、コンテンツ フィルタ条件、メッセージ フィルタ条件、または画像解析のいずれによるものかに関係なく、添付ファイルの内容がその隔離理由とともに表示されます。

メッセージ フィルタまたはコンテンツ フィルタのルールをトリガーしたローカル隔離内のメッセージを表示すると、フィルタ アクションを実際にはトリガーしなかった内容が（フィルタ アクションをトリガーした内容とともに）GUI で表示されることがあります。GUI の表示は、該当コンテンツを特定するための目安として使用するもので、該当コンテンツの完全なリストであるとは限りません。この現象が発生するのは、GUI でコンテンツの照合に使用しているロジックがフィルタと比べて厳密でないためです。この問題はメッセージ本文での検索についてのみ発生します。メッセージの各パート内の一致文字列をそれに対応するフィルタ ルールとともに一覧表示するテーブルは正しく表示されます。

図 27-1 ポリシー隔離エリア内で表示された一致内容

Attachment Name	Matched Content	Condition
FP1.1.txt	<ul style="list-style-type: none"> MS 38930 USA Facilities 662-646-0523 jsamuelson@acmecorp.com 7/17/06 4929132070312710 Acme Corp Irene Gibbs 808 Sumner Street Greenwood MS 38930 USA Publishing 662-646-0522 igibbs@acmecorp.com 2/1/07 4405231592071060 Acme Corp Kathy Lopez 808 Sumner Street Greenwood MS 38930 USA Marketing 662-646-0541 klopez@acmecorp.com 2/1/07 4716298862510192 Acme Corp Marty Smith 808 Sumner Street Greenwood MS 38930 USA Engineering 662-646-0542 	DLP Classifier: Contact Information

```

Headers
X-IronPort-AV: E=Sophos;i="4.43,202,1246010600";
d="txt?scan=208";a="178202"
Received: from d2.vmw023-bsd04.ibqa (HELO vmw023-bsd04.ibqa) ([172.22.107.1])
by c360q02.ibqa with ESMTP; 28 Jul 2009 16:25:03 +0530
Message-ID: <792087.518002035-sendEmail@vmw023-bsd04>
From: "user1@test.com" <user1@test.com>
To: "user1@test.com" <user1@test.com>
Subject: DLPTEST
Date: Tue, 28 Jul 2009 08:42:11 +0000
X-Mailer: sendEmail-1.55
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="----MIME delimiter for sendEmail-538525.714612664"

Message
Test

Message Parts
Name          Size  Details
[message body] 6     ASCII text, with CRLF line terminators
FP1.1.txt     1K   ASCII text

```

添付ファイルのダウンロード

[メッセージ部分 (Message Parts)] または [一致した内容 (Matched Content)] セクション内の添付ファイルのファイル名をクリックすることにより、メッセージの添付ファイルをダウンロードできます。AsyncOS から、未知の送信元からの添付ファイルにはウイルスが含まれる可能性があることを示す警告が表示され、続行するかどうか尋ねられます。ウイルスが含まれる可能性がある添付ファイルは、ユーザ自身の自己責任においてダウンロードしてください。[メッセージ部分 (Message Parts)] セクション内の [メッセージ本文 (message body)] をクリックすることにより、メッセージ本文をダウンロードすることもできます。

ウイルスの検査

メッセージがウイルスに感染していないかどうかを検査するには、[テスト開始 (Start Test)] をクリックします。アンチウイルス シグニチャが最新のものであることを確認できるまで、メッセージの保管に隔離を使用します。

ウイルスの検査では、オリジナルのメッセージではなく、メッセージのコピーがアンチウイルス エンジンに送信されます。アンチウイルス エンジンの判定結果は、[隔離 (Quarantines)] エリアの上に表示されます。

隔離されたメッセージの再スキャンについて

隔離されたすべてのキューからメッセージが解放される時、アプライアンスおよび最初にメッセージを隔離したメール ポリシーでイネーブルにされている機能によって、次の再スキャンが発生します。

- ポリシーおよびウイルス隔離から解放されるメッセージはアンチウイルス エンジンによって再スキャンされます。
- アウトブレイク 隔離エリアから解放されたメッセージは、アンチスパムおよびアンチウイルス エンジンによって再スキャンされます。(アウトブレイク 隔離におけるメッセージの再スキャンについては、[第 14 章「アウトブレイク フィルタ」](#)を参照してください)

再スキャン時に、判定結果が前回そのメッセージを処理したときの判定結果と一致する場合、そのメッセージは再隔離されません。逆に、判定が異なると、そのメッセージは別の隔離に送信される可能性があります。

原理的に、メッセージの隔離が無限に繰り返されることはないようになっています。たとえば、メッセージが暗号化されていて、その結果、Virus 隔離に送信されるとします。管理者がそのメッセージを解放しても、アンチウイルス エンジンはまだそのメッセージを復号化できません。しかし、そのメッセージは再隔離されない必要があります。再隔離されるとループ状態となり、そのメッセージは隔離エリアからまったく解放されなくなります。2 回とも判定は同じ結果になるので、システムは 2 回めには Virus 隔離を無視します。

アウトブレイク隔離

アウトブレイク 隔離は、アウトブレイク フィルタ機能の有効なライセンス キーが入力されている場合に存在します。アウトブレイク フィルタ機能では、しきい値セットに従ってメッセージがアウトブレイク 隔離に送信されます。詳細については、[第 14 章「アウトブレイク フィルタ」](#)を参照してください。

アウトブレイク 隔離は、他の隔離と同様の機能を持ち、メッセージを検索したり、メッセージを解放または削除したりなどできます。

アウトブレイク 隔離には、他の隔離では使用できない追加の機能があります ([ルール サマリーによる管理 (Manage by Rule Summary)] リンク、メッセージの詳細を表示しているときのシスコへの送信機能、およびスケジュールされた保存期間の終了日時で検索結果内のメッセージを並べ替えるオプション)。

アウトブレイク フィルタ機能のライセンスの有効期限が切れると、メッセージをアウトブレイク 隔離にそれ以上追加できなくなります。隔離エリア内に現在存在するメッセージの保存期間が終了してアウトブレイク 隔離が空になると、GUI の隔離リストにアウトブレイク 隔離は表示されなくなります。

アウトブレイク隔離のメッセージの再スキャン

アウトブレイク 隔離に入れられたメッセージは、新しく公開されたルールによってもう脅威ではないと見なされると、自動的に解放されます。

アプライアンス上でアンチスパムおよびアンチウイルスがイネーブルになっている場合、スキャン エンジンは、メッセージに適用されるメール フロー ポリシーに基づいて、アウトブレイク 隔離から解放されたすべてのメッセージをスキャンします。

ルール サマリーによる管理リンク

隔離リストでアウトブレイク隔離の横にある [ルール サマリーによる管理 (Manage by Rule Summary)] リンクをクリックして、[ルール サマリーによる管理 (Manage by Rule Summary)] ページを表示します。隔離エリア内のすべてのメッセージに対し、それらのメッセージを隔離させた感染防止ルールに基づいてメッセージ アクション (Release、Delete、Delay Exit) を実行できます。これは、アウトブレイク隔離から多数のメッセージを片付ける場合に適しています。詳細については、次の項を参照してください [アウトブレイク隔離 (Outbreak Quarantine)] および [ルール サマリーによる管理 (Manage by Rule Summary)] ビュー (P.14-20)。

偽陽性または不審なメッセージをシスコへ報告

アウトブレイク隔離内のメッセージについてメッセージの詳細を表示しているとき、偽陽性または不審なメッセージを報告するためにそのメッセージをシスコへ送信できます。

手順

-
- ステップ 1** アウトブレイク隔離エリア内のメッセージの移動
 - ステップ 2** [メッセージの詳細 (Message Details)] セクションで、[シスコにコピーを送信する (Send a Copy to Cisco Systems)] チェックボックスを選択します。
 - ステップ 3** [送信 (Send)] をクリックします。
-

スパム隔離の概要

AsyncOS 管理者はスパム隔離にあるメッセージをすべて表示できますが、通常、メッセージの受信者であるエンド ユーザは、隔離されたメッセージを別の Web インターフェイスを使用して表示できません。

電子メールセキュリティ アプライアンス に保存されるローカル スパム隔離または別のシスコのコンテンツ セキュリティ管理アプライアンスに保存される外部スパム隔離を利用できます。

- [スパム隔離の設定](#)
- [スパム隔離内のメッセージの管理](#)
- [送信者に基づいて電子メール配信を制御するセーフリストおよびブロックを使用](#)

関連項目

- [第 13 章「アンチスパム」](#)

スパム隔離の設定

AsyncOS は、スパムおよびその疑いのあるものをスパム隔離に送信するように設定できます。また、スパムおよびその疑いのあるメッセージが隔離されたことをユーザに通知する電子メールを送信するように、システムを設定することもできます。この通知には、スパム隔離に現在入っているそのユーザ宛のメッセージの要約が含まれます。ユーザは、メッセージを確認し、それらを自分の受信箱に配信するか、それとも削除するかを決定できます。また、ユーザはその隔離されたメッセージ全体を検索するこ

とができます。ユーザはこの通知を利用して隔離にアクセスできますが、Web ブラウザから直接アクセスすることもできます（この場合は認証が必要です。「[スパム隔離へのエンド ユーザ アクセスの設定](#)」(P.27-24) を参照)。

システムは、隔離領域をすべて消費することを避けるために、メールがスパム隔離から定期的かつ自動的に削除されるように、自動メンテナンスを設定できます。スパム隔離は、エンド ユーザ宛のスパムおよびその疑いのあるメッセージを保管することを目的として使用されます。

各電子メール セキュリティ アプライアンスでは、アンチスパム機能がイネーブルになっている場合、ローカルのスパム隔離をイネーブルにすることができます。また、各アプライアンスは、外部のスパム隔離を参照することもできます。この隔離は、別のコンテンツ セキュリティ アプライアンス上で設定されます（通常はシスコのコンテンツ セキュリティ 管理アプライアンス。詳細については、[第 38 章「Cisco コンテンツ セキュリティ 管理アプライアンスの集中型サービス」](#)を参照してください）。

なお、ローカルと外部の両方のスパム隔離がイネーブルになっている場合、ローカルのスパム隔離が使用されます。

スパム隔離へのメッセージの送信方法

表 27-2 スпам隔離へのメッセージの送信方法

	操作内容	追加情報
ステップ1	スパム隔離を有効にします。	<ul style="list-style-type: none"> ローカル隔離を有効にする：「ローカルのスパム隔離のイネーブル化」 (P.27-20)。 または 外部隔離を追加する：「外部のスパム隔離の設定」 (P.27-27)。
ステップ2	スパム隔離でメッセージを処理する方法を設定します。	<ul style="list-style-type: none"> 「ローカルのスパム隔離の設定」 (P.27-23)。 外部隔離の設定については、お使いのセキュリティ管理アプライアンスのマニュアルを参照してください。
ステップ3	ユーザ グループのスパム隔離設定を行います。	「スパム対策ポリシーの定義」 (P.13-8) を参照してください。

関連項目

- 「[メッセージがスパムかどうかスキャンするためのアプライアンスの設定方法](#)」 (P.13-2)

ローカルのスパム隔離のイネーブル化とディセーブル化

- 「[ローカルのスパム隔離のイネーブル化](#)」 (P.27-20)
- 「[ローカルのスパム隔離のディセーブル化](#)」 (P.27-21)

ローカルのスパム隔離のイネーブル化

ローカルのスパム隔離をイネーブルにすると、AsyncOS は、外部のスパム隔離が設定されても、ローカルのスパム隔離を使用します。

手順

- ステップ 1 [モニタ (Monitor)] > [スパム隔離 (Spam Quarantine)] をクリックします。
- ステップ 2 スパム隔離の [有効 (Enable)] をクリックします。
- ステップ 3 スパム隔離がイネーブルになります。



(注) スパム隔離が設定されていない場合は、[スパム隔離の編集 (Edit Spam Quarantine)] ページが表示されます。

- ステップ 4 変更内容を送信し、確定します。

ローカルのスパム隔離のディセーブル化

電子メール セキュリティ アプライアンスでローカルのスパム隔離をディセーブルにします。

手順

- ステップ 1 [モニタ (Monitor)] > [スパム隔離 (Spam Quarantine)] をクリックします。
- ステップ 2 スパム隔離の [設定 (Settings)] カラム内にある [編集 (Edit)] をクリックします。
- ステップ 3 [スパム隔離設定 (Spam Quarantine Settings)] セクションで、[スパム隔離を有効にする (Enable Spam Quarantine)] チェックボックスをオフにします。
- ステップ 4 変更内容を送信し、確定します。

ローカルのスパム隔離がディセーブルになっているとき、その隔離エリア内にメッセージが存在する場合は、[モニタ (Monitor)] > [スパム隔離 (Spam Quarantine)] ページのリンクで隔離の [すべて削除 (Delete All)] をクリックします。

ディセーブルにされたスパム隔離とメール ポリシー

スパム隔離がディセーブルにされると、スパムまたはその疑いのあるメッセージを隔離するように設定されたメール ポリシーは、メッセージを配信するように設定が変更されます。

ローカルのスパム隔離から外部の隔離への移行

ローカルの C-Series または X-Series アプライアンス上で現在使用中のローカルのスパム隔離を、そのローカル隔離内のメッセージにアクセスできるようにしたまま、セキュリティ管理アプライアンスアプライアンスをホストとする外部のスパム隔離に移行する場合は、次の戦略の使用を検討します。

- アンチスパム設定の設定：セキュリティ管理アプライアンスを代替ホストとして指定して、メールポリシーにアンチスパム設定を設定します。この処置により、ローカル隔離にアクセス可能なまま、新しいスパムは外部の隔離に送信されます。
- より短い有効期限の設定：ローカル隔離に対して Schedule Delete After 設定をより短い期間に設定します。

- 残っているすべてのメッセージを削除：ローカル隔離内に残っているすべてのメッセージを削除するには、その隔離をディセーブルにし、ローカル隔離のページで [すべて削除 (Delete All)] リンクをクリックします（「[スパム隔離からのメッセージの削除](#)」(P.27-35) を参照）。このリンクは、まだメッセージが残っているローカルのスパム隔離がディセーブルになっているときにだけ使用可能になります。

これで、移行中に新しいメッセージがローカル隔離に入らないようにしながら、ローカル隔離のディセーブル化と外部の隔離のイネーブル化をできるようになります。

スパム隔離の設定

スパム隔離の設定

隔離サイズ、削除/保存ポリシー、デフォルト言語、および通知のイネーブル化またはディセーブル化を設定します。デフォルトでは、ローカルのスパム隔離は自己管理型になっています。つまり、この隔離がイネーブルになると、設定された期間後にスパムが自動的に削除されます。隔離エリアが満杯になった場合は、古いスパムから削除されます。スパム隔離の外観および動作は、カスタム ロゴやログイン ページ メッセージの指定も含め、設定およびカスタマイズできます。「[ローカルのスパム隔離用のスパム隔離設定](#)」(P.27-23) を参照してください。

ローカルのスパム隔離内にあるメッセージを表示したり、操作したりする AsyncOS Operator ユーザを指定します。AsyncOS に作成されたすべての Administrator レベルのユーザ（デフォルトの「admin」ユーザなど）は、スパム隔離に対して自動的にアクセスおよび変更できるようになります。Operator は、隔離の内容を表示できますが、隔離の設定を変更できない場合があります。「[スパム隔離の管理ユーザの設定](#)」(P.27-24) を参照してください。

スパム隔離へのアクセス

各エンド ユーザがスパム隔離内にある自分宛のメッセージを Web ブラウザからじかにアクセスおよび管理することを許可します。アクセスを許可されたユーザは、スパム通知を受信したかどうかに関係なく、隔離エリアからメッセージを表示、検索、解放、および削除できるようになります。メッセージ本文を表示するか、非表示にするかを指定します。使用されるエンド ユーザ認証を指定できます (LDAP、Active Directory、IMAP/POP、またはなし)。「[スパム隔離へのエンド ユーザ アクセスの設定](#)」(P.27-24) を参照してください。「なし」を指定すると、エンド ユーザは、通知メッセージに含まれるリンク経由でしかスパム隔離にアクセスできなくなり、認証は使用されなくなります（ユーザ名とパスワードは必要ありません）。

表 27-3 エンド ユーザの認証とアクセス

認証	ユーザのアクセス方法
LDAP	URL、通知
メールボックス (IMAP/POP)	URL、通知
なし	通知のみ
無効	アクセス不可能 (通知がイネーブルになっている場合、[スパム通知 (Spam Notifications)] セクションで設定された [バウンス メッセージの送信先: (Deliver Bounce Messages To:)] のアドレスに通知が送信されます)

スパム通知

通知とは、スパム隔離内にある各ユーザ宛の新しいスパム メッセージを要約したものです。スパム通知をイネーブルにし、その内容を設定します。スパム通知の内容には、差出人アドレス、件名、メッセージ本文、メッセージ形式、バウンス アドレス、通知スケジュールなどがあります。スパム隔離へのアクセスがイネーブルになっている場合、ユーザは、LDAP やメールボックスの認証を使用しなくても、通知によって自分宛の隔離されたメッセージにアクセスできるようになります。通知は、電子メールが隔離されている各エンベロープ受信者（メーリング リストおよびその他のエイリアスを含む）に送信されます。各メーリング リストは、単一の要約を受信します。つまり、各メーリング リストの購読者は、全員が同じ通知を受信することになり、その隔離にログインしてメッセージを解放したり、削除したりできます。この場合、ユーザが隔離にアクセスして、通知に示されたメッセージを表示しようとしても、それらのメッセージは他のユーザによってすでに削除されている可能性もあります。複数のエイリアスに属していたり、複数の電子メール アドレスを使用したりしているユーザは、複数の通知を受信します（「複数の通知の受信」(P.27-31) を参照）。「エンドユーザに送信されるスパム通知の設定」(P.27-25) を参照してください。



(注)

スパム通知がイネーブルになっていても、スパム隔離へのアクセスがイネーブルになっていなければ、通知は [バウンス メッセージの送信先: (Deliver Bounce Messages To:)] のアドレスに送信されます。

ローカルのスパム隔離の設定

ローカルのスパム隔離がイネーブルになった後（「ローカルのスパム隔離のイネーブル化とディセーブル化」(P.27-20) を参照）、隔離の設定を編集して、スパム隔離と、それをユーザがどのように操作するのかを設定できます。

ローカルのスパム隔離を設定するには、[モニタ (Monitor)] > [スパム隔離 (Spam Quarantine)] ページでスパム隔離の [設定 (Settings)] カラム内にある [編集 (Edit)] をクリックします。

ローカルのスパム隔離用のスパム隔離設定

手順

- ステップ 1** [モニタ (Monitor)] > [スパム隔離 (Spam Quarantine)] を選択します。
- ステップ 2** スパム隔離の [設定 (Settings)] カラム内にある [編集 (Edit)] をクリックします。
- ステップ 3** [スパム隔離設定 (Spam Quarantine Settings)] セクション内で、隔離エリアの最大サイズを指定します。
- ステップ 4** 隔離エリアが満杯になったら古いメッセージから削除するように隔離を設定できます。チェックボックスをオフにすると、満杯の隔離エリアに新しいメッセージは追加されなくなります。隔離エリアが満杯になることでアプライアンス上にメッセージの待ち行列（渋滞）ができることがないように、この機能をイネーブルにすることを推奨します。
- ステップ 5** メッセージを削除する前の保管日数を指定します。あるいは、自動削除をスケジュールしないことを選択することもできます。隔離エリアの容量が満杯になるのを防ぐために、古いメッセージから削除するように隔離を設定することを推奨します。
- ステップ 6** デフォルトの言語を指定します。
- ステップ 7** 解放されたメッセージのコピーを分析用にシスコへ送信するように隔離を設定できます。隔離をそのように設定することを推奨します。

■ スпам隔離の設定

ステップ 8 エンド ユーザが隔離を確認するときに表示されるページをカスタマイズします。カスタム ロゴをアップロードします (任意)。このロゴは、ユーザがログインして隔離されたメッセージを確認するときに、スパム隔離のページの最上部に表示されます。

- このロゴは、最大で 550 X 50 ピクセルの .jpg、.gif、または .png ファイルにする必要があります。
- ロゴ ファイルを指定しなければ、スパム隔離のデフォルトのロゴが使用されます。



(注) カスタム ロゴを指定すると、デフォルトロゴは削除されます。

ステップ 9 ログイン ページメッセージを指定します。このメッセージは、隔離を表示する前に、エンド ユーザに対してログインを要求するときに表示されます。

ステップ 10 変更内容を送信し、確定します。



(注) セキュリティ管理アプライアンスを設定する場合の詳細については、『Cisco Content Security Management Appliance User Guide』を参照してください。

スパム隔離の管理ユーザの設定

スパム隔離の管理ユーザを指定できます。この場合の「管理」とは、スパム隔離へのユーザのアクセス権を示します。管理ユーザのリストには、隔離権限を持つカスタム ユーザ ロールに属するオペレータ、ヘルプ デスク ユーザ、読み取り専用オペレータ、および委任管理者を追加できます。管理者レベルのユーザ (デフォルトの admin ユーザを含む) はすべて、自動的にスパム隔離の管理ユーザであると見なされます。したがって、それらのユーザは、Available カラムや Authorized Users カラムに表示されません。

手順

ステップ 1 ローカル、外部認証、またはカスタム ロール (委任管理者) から、適切なユーザのタイプのリンクをクリックします。

ステップ 2 追加するユーザを選択します。

ステップ 3 [追加 (Add)] をクリックします。

Operator レベルのユーザおよび委任管理者は、スパム隔離内のメッセージを表示できますが、隔離の設定を編集できないことに注意してください。管理ユーザは、メッセージを表示し、設定を変更できます。

ステップ 4 変更内容を送信し、確定します。

スパム隔離へのエンド ユーザ アクセスの設定

エンド ユーザが直接スパム隔離にアクセスすることを許可します。

手順

ステップ 1 [モニタ (Monitor)] > [スパム隔離 (Spam Quarantine)] を選択します。

ステップ 2 スпам隔離の [設定 (Settings)] カラム内にある [編集 (Edit)] をクリックします。

- ステップ 3** [エンドユーザ隔離へのアクセスを有効にする (Enable End-User Quarantine Access)] セクションまでスクロールします。
- ステップ 4** [エンドユーザ隔離へのアクセスを有効にする (Enable End-User Quarantine Access)] と書かれたチェックボックスをオンにします。Administrator ユーザは、このチェックボックスがオンかオフかに関係なく、隔離にアクセスできます。
- ステップ 5** メッセージが解放される前に、メッセージ本文を表示するかどうかを指定します。このチェックボックスをオンにすると、ユーザは、スパム隔離ページからメッセージ本文を表示できなくなります。代わりとして、隔離されたメッセージの本文を表示するには、そのメッセージを解放してから、ユーザのメールアプリケーション (Outlook など) で表示する必要があります。これは、すべての閲覧された電子メールがアーカイブされなければならない場合のコンプライアンスの問題と特に関係しています。
- ステップ 6** エンドユーザが (電子メール通知経由ではなく) Web ブラウザから隔離を直接表示しようとする場合に、それらのエンドユーザを認証するために使用する方式を指定します。メールボックス認証または LDAP 認証を使用できます。

認証をイネーブルにしなくても、スパム隔離へのエンドユーザのアクセスを許可することに注意してください。この場合、ユーザは通知メッセージに含まれるリンク経由で隔離にアクセスでき、システムはユーザの認証を行いません。認証なしのエンドユーザアクセスをイネーブルにする場合は、[エンドユーザ認証 (End-User Authentication)] ドロップダウンメニューで [None] を選択します。

LDAP 認証 : LDAP サーバまたはアクティブなエンドユーザ認証クエリーが設定されていない場合は、[システム管理 (System Administration)] > [LDAP] リンクをクリックして、LDAP サーバ設定とエンドユーザ認証クエリー スtring を設定します。LDAP 認証の設定方法の詳細については、『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「LDAP Queries」を参照してください。

メールボックス認証 : 認証に LDAP ディレクトリを使用しないサイトの場合、隔離は、ユーザの電子メールアドレスとパスワードの正当性を、それらのユーザのメールボックスが保持されている標準ベースの IMAP または POP サーバに対して検証することもできます。Web UI にログインするとき、ユーザは各自の完全な電子メールアドレスとメールボックス パスワードを入力します。この情報を使用して、メールボックス サーバに隔離のユーザとしてのログインが試行されます。ログインに成功すれば、そのユーザは認証されます。その後、ただちにログアウトするので、ユーザの受信箱に対して行われる変更はありません。メールボックス認証の使用は、LDAP ディレクトリを稼働しないサイトに適していますが、電子メール エイリアス宛に送られてきたメッセージをメールボックス認証でユーザに提示できません。

タイプ (IMAP または POP) を選択します。サーバ名と、安全な接続に SSL を使用するかどうかを指定します。サーバのポート番号を入力します。未修飾のユーザ名の後ろに追加するドメイン (example.com など) を入力します。

POP サーバがバナー内で APOP サポートをアドバタイズしている場合、セキュリティ上の理由から (つまり、パスワードが平文で送信されるのを回避するために)、Cisco アプライアンスは APOP のみを使用します。一部またはすべてのユーザに対して APOP がサポートされていない場合は、APOP をアドバタイズしないように POP サーバを設定する必要があります。

- ステップ 7** 変更内容を送信し、確定します。

エンドユーザに送信されるスパム通知の設定

スパム通知とは、スパム隔離内にメッセージが存在するときに、エンドユーザに送信される電子メールメッセージのことです。通知には、そのユーザ宛 (LDAP によるユーザ認証の場合は、LDAP リポジトリ内でそのユーザに関連付けられている電子メールアドレス宛。「スパム隔離へのエンドユーザ

「アクセスの設定」(P.27-24)を参照)の隔離されたスパムまたはその疑いのあるメッセージのリストが含まれます。さらに、各ユーザがそれぞれの隔離されたメッセージを表示するために使用するリンクも含まれます。通知は、イネーブルにされた後、ここで設定されたスケジュールに従って送信されます。

スパム通知により、エンドユーザが隔離にログインするための代替方法が提供されます。ユーザは、受信した電子メール通知を介して隔離にアクセスします(その隔離に対して通知がイネーブルになっている場合)。メッセージの件名をクリックすると、ユーザは、その通知が送信された電子メールアドレスの隔離の UI にログインします。この方法によるスパム隔離へのアクセスには、LDAP 認証もメールボックス認証も必要ありません。この方法によるログインでは、アプライアンスが電子メール通知にスパム隔離エイリアス統合クエリーを使用していない限り、エンドユーザが所有する他のエイリアス宛の隔離対象メッセージは表示されないことに注意してください。Cisco アプライアンスで処理した後に展開される配布リストに通知が送信された場合、複数の受信者がそのリストに対する同じ隔離にアクセスできます。

電子メールエイリアスを所有するユーザや複数の電子メールアドレスを使用するユーザは、複数のスパム通知を受信する可能性があります。複数の通知は、エイリアス統合機能を使用して一部の発生を防ぐことができます。LDAP サーバまたはアクティブなエイリアス統合クエリーがセットアップされていない場合は、[システム管理 (System Administration)] > [LDAP] リンクをクリックして、LDAP サーバ設定とエイリアス統合クエリー スtring を設定します。詳細については、このマニュアル内の「導入上の考慮事項」(P.27-29)と「複数の通知の受信」(P.27-31)に加え、『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「LDAP Queries」も参照してください。

手順

-
- ステップ 1** [スパム通知を有効にする (Enable Spam Notifications)] チェックボックスをオンにして、スパム通知をイネーブルにします。
- ステップ 2** 通知の差出人アドレスを入力します。ユーザは、このアドレスを、自分の電子メールクライアントでサポートされる任意の「ホワイトリスト」に追加できます(「導入上の考慮事項」(P.27-29)を参照)。
- ステップ 3** 通知の件名を入力します。
- ステップ 4** 通知のカスタマイズされたタイトルを入力します。
- ステップ 5** メッセージ本文をカスタマイズします。AsyncOS では、メッセージ本文に挿入されると、個々のエンドユーザに対応した実際の値に展開されるいくつかのメッセージ変数がサポートされています。たとえば、%username% は、ユーザに対して通知が生成される時、そのユーザの実際のの名前に展開されます。サポートされるメッセージ変数には、次のものがあります。
- [新規メッセージ数 (New Message Count)] (%new_message_count%) : ユーザの最後のログイン以後の新しいメッセージの数。
 - [総メッセージ数 (Total Message Count)] (%total_message_count%) : エンドユーザ隔離内にあるこのユーザ宛のメッセージの数。
 - [メッセージ保存期間 (Days Until Message Expires)] (%days_until_expire%)
 - [隔離 URL (Quarantine URL)] (%quarantine_url%) : 隔離にログインし、メッセージを表示するための URL。
 - [ユーザ名 (Username)] (%username%)
 - [新規メッセージテーブル (New Message Table)] (%new_quarantine_messages%) : 隔離エリア内にあるこのユーザ宛の新しいメッセージのリスト。
- これらのメッセージ変数は、[Message Body] フィールドのテキスト内に直接入力して、メッセージ本文に挿入できます。あるいは、変数を挿入する場所にカーソルを配置してから、右側の [メッセージ変数 (Message Variables)] リスト内にある変数の名前をクリックすることもできます。
- ステップ 6** メッセージ形式 (HTML、テキスト、または HTML/テキスト) を選択します。

- ステップ 7** バウンス アドレスを指定します (バウンスされた通知がこのアドレスに送信されます)。
- ステップ 8** 必要に応じて、異なるアドレスで同じ LDAP ユーザに送信されたメッセージを統合できます。
- ステップ 9** 通知スケジュールを設定します。通知を月に一度、週に一度、または日に 1 回以上送信するように (週末の有無も含めて) 設定できます。
- ステップ 10** 変更内容を送信し、確定します。

外部のスパム隔離の設定

スパムおよびその疑いのあるスパムを別の Cisco Content Security アプライアンス上に設定された外部のスパム隔離に送信できます。詳細については、[第 38 章「Cisco コンテンツ セキュリティ管理アプライアンスの集中型サービス」](#)を参照してください。

外部のスパム隔離を使用する場合、隔離の設定は、その Cisco Content Security アプライアンス上で行います。Cisco Content Security アプライアンス上でローカルと外部のスパム隔離を両方ともイネーブルにした場合、ローカルのスパム隔離がその設定とともに優先されます。

セキュリティ管理アプライアンス (外部隔離) から解放されるメッセージは、RAT、ドメイン例外、エイリアシング、着信フィルタ、マスカレード、バウンス検証、およびワーク キューをスキップします。

外部のスパム隔離の追加

手順

- ステップ 1** [セキュリティ サービス (Security Services)] > [集約管理サービス (Centralized Services)] > [スパム隔離 (Spam Quarantine)] を選択します。
- ステップ 2** [隔離を追加 (Add Quarantine)] をクリックします。
- ステップ 3** 隔離の名前を入力します。この名前に意味はありません。参照目的でのみ使用されます。
- ステップ 4** IP アドレスとポート番号を入力します。この IP アドレスとポート番号は、M-Series アプライアンス上で [スパム隔離の設定 (Spam Quarantines Settings)] ページ内に指定されています (詳細については、『Cisco Content Security Management Appliance User Guide』を参照してください)。
- ステップ 5** 変更内容を送信し、確定します。

外部のスパム隔離の編集

手順

- ステップ 1** [セキュリティ サービス (Security Services)] > [集約管理サービス (Centralized Services)] > [スパム隔離 (Spam Quarantine)] を選択します。
- ステップ 2** [設定 (Settings)] カラム内にある [編集 (Edit)] をクリックします。
- ステップ 3** 設定を変更します。

ステップ 4 変更内容を送信し、確定します。

外部のスパム隔離の削除

Cisco Content Security アプライアンスには、外部のスパム隔離を 1 つしか指定できません。外部のスパム隔離の削除では、その隔離自体が削除されることはなく、その隔離エリア内のデータは少しも変更されないことに注意してください。代わりに、その外部スパム隔離に対する参照がローカルマシンから削除されます。

手順

- ステップ 1** [セキュリティ サービス (Security Services)] > [集約管理サービス (Centralized Services)] > [スパム隔離 (Spam Quarantine)] を選択します。
 - ステップ 2** [設定 (Settings)] カラム内にある [編集 (Edit)] をクリックします。
 - ステップ 3** [設定の削除 (Remove Settings)] をクリックします。
 - ステップ 4** AsyncOS で、隔離を削除するかどうかを確認するメッセージが表示されます。
 - ステップ 5** [削除 (Delete)] をクリックします。
-

Web ブラウザからスパム隔離へのアクセスのイネーブル化

ローカルのスパム隔離をイネーブルにした後、スパム隔離の HTTP または HTTPS サービスを IP インターフェイス上でイネーブルにします。

手順

- ステップ 1** [ネットワーク (Network)] > [IP インターフェイス (IP Interfaces)] を選択します。
 - ステップ 2** インターフェイス名をクリックします (この例では、Management インターフェイスを使用します)。
 - ステップ 3** スпам隔離の [HTTP] または [HTTPS] チェックボックスを選択します。
 - ステップ 4** サービスの適切なポート番号を入力します。
 - ステップ 5** (任意) スпам隔離の HTTP 要求を HTTPS にリダイレクトするかどうかを選択します。
 - ステップ 6** (任意) スпам隔離にアクセスするためのデフォルトのインターフェイスにするかどうかを選択します (通知および隔離ログインがこのインターフェイス上で開始されます)。隔離の URL 内のインターフェイスのホスト名を使用するか、それともカスタム URL を指定するかを選択します。
 - ステップ 7** 変更内容を送信し、確定します。
-

スパムを隔離するためのメール ポリシーの設定

ローカルのスパム隔離をイネーブルにした後（または外部のスパム隔離を追加した後）、スパムまたはスパムの疑いのあるメッセージをその隔離エリアに送信するように、メール ポリシーを設定できます。メールをスパム隔離に送信できるようにするために、Cisco IronPort アンチスパム スキャンがメール ポリシーでイネーブルにされる必要があることに注意してください。

スパムまたはその疑いのあるメッセージをスパム隔離に送信するようにメール ポリシーを設定するには、次の手順を実行します。

手順

-
- ステップ 1** [メール ポリシー (Mail Policies)] > [受信メール ポリシー (Incoming Mail Policies)] ページで、対応するメール ポリシーの [スパム対策 (Anti-Spam)] カラム内にあるリンクをクリックします。
 - ステップ 2** [スパムと確定された場合の設定 (Positively-Identified Spam Settings)] セクション内で、[このアクションをメッセージに適用する (Apply This Action to Message)] オプションに [スパム隔離 (Spam Quarantine)] を選択します。
 - ステップ 3** 必要に応じて、スパムの疑いのあるメッセージやマーケティング電子メールに対してもこの設定を繰り返します。
 - ステップ 4** 変更内容を送信し、確定します。
-

導入上の考慮事項

ここでは、スパム隔離を導入する際に注意すべき、さまざまなヒントと情報を提供します。

ディスク容量

表 27-4 に、各アプライアンス上でスパム隔離に使用可能なディスク スペースを示します。

表 27-4 スпам隔離に使用可能なディスク スペース

モデル	ディスク領域 (単位: GB)
C160/170	5
C360/370	15
C660/670	30
X1060/1070	30

スパム隔離にアクセスするエンド ユーザ

エンド ユーザは、受信した通知内のリンク経由でスパム隔離にアクセスできます。この方法で隔離にアクセスする場合、LDAP 認証や IMAP/POP 認証は必要ありません（エンド ユーザは自分自身を認証する必要がありません）。通知メッセージ内に存在するリンクには有効期限がないことに注意してください。エンド ユーザは、これらのリンクを使用すれば、認証しなくても、自分宛の隔離されたメッセージを表示できます。

ユーザは、自分の Web ブラウザにリンクを直接入力して隔離にアクセスすることもできます。Web ブラウザに入力した URL 経由で隔離にアクセスする場合、ユーザは認証を行う必要があります。認証方式 (LDAP または「メールボックス」(IMAP/POP)) は、隔離設定の [エンド ユーザ隔離アクセス (End User Quarantine Access)] セクション内で定義されます (「[スパム隔離へのエンド ユーザ アクセスの設定](#)」(P.27-24) を参照)。

LDAP 認証プロセス

1. ユーザが自分のユーザ名とパスワードを Web UI ログイン ページに入力します。
2. スпам隔離は、匿名検索を実行するように、または指定された「サーバログイン」DN とパスワードによる認証ユーザとして、指定された LDAP サーバに接続します。Active Directory の場合、一般に「グローバル カタログ ポート」(6000 番台) 上でサーバ接続を確立する必要があり、検索を実行するために、スパム隔離がバインドできる低い特権 LDAP ユーザを作成する必要があります。
3. 次に、スパム隔離は、指定された BaseDN とクエリー スtring を使用してユーザを検索します。ユーザの LDAP レコードが見つかったら、スパム隔離は、そのレコードの DN を抽出し、ユーザ レコードの DN と最初にユーザが入力したパスワードを使用してディレクトリへのバインドを試みます。このパスワード チェックに成功すると、ユーザは正しく認証されます。しかしまだ、スパム隔離は、そのユーザに対してどのメールボックスの内容を表示するのかが決定する必要があります。
4. メッセージは、受信者のエンベロープ アドレスを使用してスパム隔離に保管されます。ユーザのパスワードが LDAP に対して検証された後、スパム隔離は、「プライマリ電子メール属性」を LDAP レコードから取得して、どのエンベロープ アドレスの隔離されたメッセージを表示する必要があるのかが決定します。「プライマリ電子メール属性」には、電子メールアドレスが複数格納されている場合があります。これらのアドレスを使用して、隔離からどのエンベロープ アドレスが認証ユーザに対して表示される必要があるのかが決定されます。

IMAP/POP 認証プロセス

1. メール サーバ設定に応じて、ユーザは、自分のユーザ名 (joe) または電子メールアドレス (joe@example.com) と、パスワードを Web UI ログイン ページに入力します。ユーザに電子メールアドレスをフルに入力する必要があるのか、ユーザ名だけを入力すればよいのか知らせるために、ログイン ページ メッセージを変更できます (「[スパム隔離へのエンド ユーザ アクセスの設定](#)」(P.27-24) を参照)。
2. スпам隔離は、IMAP サーバまたは POP サーバに接続し、入力されたログイン名 (ユーザ名または電子メールアドレス) とパスワードを使用して IMAP/POP サーバへのログインを試みます。パスワードが受け入れられると、そのユーザは認証されたと見なされ、スパム隔離はただちに IMAP/POP サーバからログアウトします。
3. ユーザが認証された後、スパム隔離は、ユーザの電子メールアドレスに基づいて、そのユーザ宛の電子メールのリストを作成します。
 - スпам隔離の設定において、修飾のないユーザ名 (joe など) に追加するドメインを指定している場合は、このドメインを後ろに追加してできる完全修飾電子メールアドレスを使用して、隔離エリア内の一致するエンベロープが検索されます。
 - それ以外の場合、スパム隔離は、入力された電子メールアドレスを使用して、一致するエンベロープを検索します。

スパム隔離にログインするための URL の決定

エンド ユーザがスパム隔離に直接アクセスするために使用できる URL は、マシンのホスト名と、隔離がイネーブルになっている IP インターフェイス上の設定 (HTTP/S とポート番号) から作成されます。次の例を参考にしてください。

```
HTTP://mail3.example.com:82
```

設定例

POP/IMAP の設定例 :

IMAP および POP の場合 (単一ドメイン) :

- サーバ名を入力します。
- サーバで SSL を使用するように設定している場合は、SSL をイネーブルにします。
- [未修飾ユーザ名にドメインを追加 (Append Domain to Unqualified Usernames)] をイネーブルにし、ユーザのログイン用にエンベロープのドメインをこれに設定します。

IMAP の詳細については、ワシントン大学の Web サイトを参照してください。

<http://www.washington.edu/imap/>

通知のテスト

電子メール セキュリティ マネージャでテスト用のメール ポリシーを設定することにより、通知をテストできます。この場合、単一のユーザに対してだけ、スパムを隔離させます。その後、スパム隔離の通知設定で、[スパム通知を有効にする (Enable Spam Notification)] チェックボックスをオンにし、[エンドユーザ隔離へのアクセスを有効にする (Enable End-User Quarantine Access)] チェックボックスをオフにします。これにより、[バウンスされたメッセージの送信先 (Deliver Bounced Messages To)] フィールドに設定された管理者だけが、隔離内の新しいスパムについて通知されます。

エンド ユーザでの通知の確実な受信

エンド ユーザに対して、スパム隔離からの通知電子メールの差出人アドレスを各自のメール アプリケーション (Outlook、Thunderbird など) の迷惑メール設定にある「ホワイトリスト」へ追加することを推奨してください。

複数の通知の受信

ユーザは、複数の電子メール エイリアスに属しているか、複数の電子メール アドレスを使用していると、複数の通知を受信します。また、電子メールを受信する LDAP グループに属しているユーザもこれに当てはまります。

表 27-5 アドレス/エイリアスに応じた通知数

ユーザ	電子メール アドレス	エイリアス	通知数
Sam	sam@example.com		1
Mary	mary@example.com	dev@example.com、 qa@example.com、 pm@example.com	4
Joe	joe@example.com、 admin@example.com	hr@example.com	3



(注)

LDAP を使用していない場合で、エンド ユーザが複数の電子メール通知を受信することがないようにする必要がある場合は、通知をディセーブルにすることを検討します。この場合、代わりとして、エンド ユーザが隔離に直接アクセスできるようにし、LDAP または POP/IMAP で認証します。

各ユーザに対して存在するメッセージの確認

認証の方式によっては (LDAP または IMAP/POP)、ユーザに対してスパム隔離内に複数の電子メールアドレス宛のメールが存在する可能性があります。

LDAP 認証を使用する場合、LDAP ディレクトリ内でプライマリ電子メール属性に複数の値が設定されていると、それらの値 (アドレス) のすべてがユーザに関連付けられます。したがって、隔離エリア内には、LDAP ディレクトリでエンド ユーザに関連付けられたすべての電子メールアドレス宛の隔離されたメッセージが存在します。

しかし、ユーザが通知経由で隔離に直接アクセスする場合、あるいは認証方式が IMAP/POP の場合、隔離にはそのユーザの電子メールアドレス (または通知が送信されたアドレス) 宛のメッセージしか表示されません。エンド ユーザ認証の動作の詳細については、「[スパム隔離にアクセスするエンド ユーザ](#)」(P.27-29) を参照してください。

スパム隔離内では、電子メールアドレスの大文字と小文字が区別されないことに注意してください。たとえば、Admin@example.com 宛と admin@example.com 宛の電子メールは、両方とも「admin@example.com」に関連付けられたユーザの隔離エリア内に存在します。

隔離対象のメールのアドレスを制限

複数のメール ポリシーを使用して ([メール ポリシー (Mail Policies)] > [受信メール ポリシー (Incoming Mail Policy)]、メールの隔離対象から除外する受信者アドレスのリストを指定できます。そのメール ポリシーにアンチスパムを設定する際、隔離の代わりに [配信 (Deliver)] または [ドロップ (Drop)] を選択します。

デフォルト エンコーディング

AsyncOS では、メッセージ ヘッダーに指定されたエンコーディングに基づいてメッセージの文字セットが決定されます。しかし、ヘッダーに指定されたエンコーディングが実際のテキストと一致していないと、そのメッセージは、スパム隔離内で閲覧される際に正しく表示されません。このような状況は、スパム メッセージの場合に発生することがよくあります。

デフォルト エンコーディングの指定

着信電子メールのヘッダーに文字セットのエンコーディングが指定されていない場合、アプライアンスを設定して、デフォルト エンコーディングを指定できます。そうすることにより、そのようなメッセージをスパム隔離内で正しく表示するのに役立ちます。

ただし、デフォルト エンコーディングを指定すると、他の文字セットのメッセージが正しく表示されなくなる可能性があります。これは、メッセージ ヘッダーにエンコーディングが指定されていないメッセージに対してのみ適用されます。一般に、このカテゴリに入るメールの多くが 1 つの特定のエンコーディングになると予測される場合にだけ、デフォルト エンコーディングを設定します。たとえば、隔離されるメールのうち、メッセージ ヘッダーに文字セットのエンコーディングが指定されていないものの多くが日本語 (ISO-2022-JP) の場合、(下の scanconfig->setup オプションにおいて) 「Configure encoding to use when none is specified for plain body text or anything with MIME type plain/text or plain/html.」のプロンプトが表示された際に、オプション 12 を選択します。

メッセージ ヘッダーにエンコーディングを指定していないメッセージに対してデフォルト エンコーディングを設定するには、CLI から scanconfig->setup コマンドを使用します。次の例では、デフォルトとして UTF-8 が設定されます。

```
mail3.example.com> scanconfig
```



```
There are currently 7 attachment type mappings configured to be SKIPPED.
```

```
Choose the operation you want to perform:
```

- NEW - Add a new entry.
- DELETE - Remove an entry.
- SETUP - Configure scanning behavior.
- IMPORT - Load mappings from a file.
- EXPORT - Save mappings to a file.
- PRINT - Display the list.
- CLEAR - Remove all entries.

```
[ ]> setup
```

```
[ ... ]
```

```
Configure encoding to use when none is specified for plain body text or anything with  
MIME type plain/text or plain/html.
```

```
1. US-ASCII
```

```
2. Unicode (UTF-8)
```

```
3. Unicode (UTF-16)
```

```
[ ... list of encodings ... ]
```

```
13. Japanese (EUC)
```

```
[1]> 2
```

```
Encoding set to "Unicode (UTF-8)".
```

スパム隔離内のメッセージの管理

ここでは、管理者の視点から、ローカルまたは外部のスパム隔離内にあるメッセージの操作方法について説明します。管理者が隔離を表示する場合、その隔離エリアに含まれるすべてのメッセージを利用できます。

管理者として、スパム隔離内のメッセージに対して次のアクションを実行できます。

- メッセージの表示
- メッセージの配信
- メッセージの削除
- メッセージの検索

スパム隔離内でのメッセージの検索

手順

ステップ 1 エンベロープ受信者を指定します。



(注) アドレスの一部を入力できます。

ステップ 2 入力した受信者に検索結果が厳密に一致する必要があるか、あるいは入力した値が検索結果のアドレスの一部、先頭、または末尾のいずれと一致する必要があるかを選択します。

ステップ 3 検索の対象期間を入力します。カレンダー アイコンをクリックして、日付を選択します。

ステップ 4 差出人アドレスを指定し、入力した値が検索結果のアドレスの一部、全体、先頭、または末尾のいずれと一致する必要があるかを選択します。

ステップ 5 [検索 (Search)] をクリックします。検索基準に一致するメッセージがページの [検索 (Search)] セクションの下に表示されます。

大量メッセージの検索

スパム隔離内に大量のメッセージが収集されている場合、および検索条件が絞り込まれていない場合、クエリーの結果が返されるまでに非常に長い時間がかかる可能性があり、場合によってはタイムアウトします。

その場合、検索を再実行するかどうか確認されます。大量の検索が同時に複数実行されると、パフォーマンスに悪影響を与える可能性があることに注意してください。

スパム隔離内のメッセージの表示

メッセージのリストにより、スパム隔離内のメッセージが表示されます。一度に表示されるメッセージの件数を選択できます。カラム見出しをクリックすることにより、表示をソートできます。同じカラムを再びクリックすると、逆順にソートされます。

メッセージの件名をクリックしてメッセージを表示します。これには、本文とヘッダーが含まれます。メッセージは、[メッセージの詳細 (Message Details)] ページに表示されます。メッセージの最初の 20 KB が表示されます。メッセージがそれよりも長い場合、表示は 20 KB で打ち切れ、メッセージの最後にあるリンクからメッセージをダウンロードできます。

[メッセージの詳細 (Message Details)] ページから、メッセージを削除したり ([削除 (Delete)] を選択)、[リリース (Release)] を選択してメッセージを解放したりできます。メッセージを解放すると、そのメッセージは配信されます。

メッセージについてさらに詳細な情報を表示するには、[メッセージトラッキング (Message Tracking)] リンクをクリックします。

添付ファイルを含むメッセージの表示

添付ファイルを含むメッセージを表示すると、メッセージの本文が表示された後、添付ファイルのリストが続いて表示されます。

HTML メッセージの表示

スパム隔離では、HTML ベースのメッセージは近似で表示されます。画像は表示されません。

符号化されたメッセージの表示

Base64 で符号化されたメッセージは、復号化されてから表示されます。

スパム隔離内のメッセージの配信

メッセージを解放して配信するには、解放する 1 つまたは複数のメッセージの隣にあるチェックボックスをクリックし、ドロップダウンメニューから [リリース (Release)] を選択します。その後、[送信 (Submit)] をクリックします。

ページに現在表示されているすべてのメッセージを自動で選択するには、見出し行にあるチェックボックスをクリックします。

解放されたメッセージは、それ以降の電子メールパイプライン内のワークキューの処理をスキップして、宛先キューへ直接進みます。

スパム隔離からのメッセージの削除

スパム隔離では、メッセージが一定時間後に自動で削除されるように設定できます。また、スパム隔離が最大サイズに達したら、古いものから順にメッセージが自動で削除されるように設定することもできます。スパム隔離からメッセージを手動で削除することも可能です。

個別のメッセージを削除するには、削除するメッセージの隣にあるチェックボックスをクリックし、ドロップダウンメニューから [削除 (Delete)] を選択します。その後、[送信 (Submit)] をクリックします。ページに現在表示されているすべてのメッセージを自動で選択するには、見出し行にあるチェックボックスをクリックします。

スパム隔離内のすべてのメッセージを削除するには、その隔離をディセーブルにし（「ローカルのスパム隔離のディセーブル化」(P.27-21) を参照）、[すべてのメッセージを削除 (Delete All Messages)] リンクをクリックします。リンクの末尾にある括弧内の数字は、スパム隔離内のメッセージの件数です。

送信者に基づいて電子メール配信を制御するセーフリストおよびブロックを使用

エンド ユーザによるセーフリストとブロックリストの作成を可能にして、どの電子メールがスパムとして処理されるかをより適切に制御できます。セーフリストにより、ユーザは、特定のユーザまたはドメインがスパムとして処理されないようにできます。それに対してブロックリストでは、特定のユーザまたはドメインが常にスパムとして処理されるようにできます。セーフリストとブロックリストの設定は、スパム隔離から設定されます。そのため、スパム隔離をイネーブルにし、この機能を使用するように設定する必要があります。セーフリスト/ブロックリスト機能がイネーブルにされると、各エンドユーザは、自分の電子メール アカウントに対してセーフリストとブロックリストを維持できるようになります。



(注)

セーフリストとブロックリストは、メールがスパムとして処理されるのを防止したり、メールがスパムとして処理されることを保証したりします。ただし、セーフリストやブロックリストを設定しても、電子メールに対するウイルスのスキャンや、内容に関連したメール ポリシーの基準をメッセージが満たすかどうかの判定は、アプライアンスで実行されます。メッセージは、セーフリストに該当しても、他のスキャン設定に従って配信されない場合があります。

セーフリスト/ブロックリスト データベース

ユーザがセーフリストまたはブロックリストにエントリを追加すると、そのエントリは Cisco アプライアンス上のデータベースに保管されます。

- シスコのコンテンツ セキュリティ管理アプライアンスを使用する場合、このデータベースは、セキュリティ管理アプライアンス上に保存され、関連するすべての電子メール セキュリティ アプライアンス上で定期的に更新と同期が行われます。
- スパム隔離が電子メール セキュリティ アプライアンス上にホスティングされる場合、セーフリスト/ブロックリスト データベースは、そのアプライアンス上に維持されます。
- 複数の電子メール セキュリティ アプライアンスをセキュリティ管理アプライアンスなしで使用する場合、データベースと設定を手動で同期する必要があります。

セーフリスト/ブロックリストの設定およびデータベースを異なる電子メール セキュリティ アプライアンス間で同期する方法の詳細については、「セーフリストとブロックリストの設定とデータベースの同期」(P.27-39) を参照してください。

バックアップ .CSV データベースを利用する方法については、「セーフリスト/ブロックリスト データベースのバックアップと復元」(P.27-38) を参照してください。

シスコのコンテンツ セキュリティ管理アプライアンスでのセーフリストおよびブロックリストの利用の詳細については、『Cisco Content Security Management Appliance User Guide』を参照してください。

セーフリストとブロックリストの作成およびメンテナンス

セーフリストとブロックリストは、エンド ユーザによって作成およびメンテナンスされます。ただし、この機能をイネーブルにし、ブロックリスト内のエントリに一致する電子メール メッセージの配信設定を設定するのは管理者です。セーフリストとブロックリストを作成し、メンテナンスするには、管理者とエンドユーザが次の作業を実行します。

- **管理者作業。**管理者は、スパム隔離のイネーブル化と設定、セーフリスト/ブロックリスト機能のイネーブル化、セーフリスト/ブロックリスト データベースのバックアップと復元、異なるアプライアンス間でのセーフリスト/ブロックリスト データベースの同期、およびログ、アラート、カスタム ヘッダーによるセーフリストとブロックリストに関する問題のトラブルシューティングを行います。管理者作業の詳細については、「セーフリストとブロックリストの作成およびメンテナンスの概要」(P.27-37) を参照してください。
- **エンドユーザ作業。**エンドユーザは、エンドユーザ スпам隔離によって自分のセーフリストとブロックリストの設定を作成します。エンドユーザは、自分のセーフリスト/ブロックリスト設定にアクセスするために、(スパム隔離通知内のリンクをクリックする代わりに) ログイン作業が必要になる場合があります。エンドユーザ スпам隔離から、エンドユーザは、[オプション (Options)] メニューを使用してセーフリストとブロックリストを作成できます。あるいは、隔離された電子メールのリストから、セーフリスト設定を作成できます。エンドユーザ作業の詳細については、「セーフリストとブロックリストを設定するためのエンドユーザ作業」(P.27-40) を参照してください。

セーフリストとブロックリストのメッセージ配信

セーフリストとブロックリストをイネーブルにすると、アプライアンスは、アンチスパム スキャンの直前にセーフリスト/ブロックリスト データベースに対してメッセージをスキャンします。アプライアンスがエンドユーザのセーフリスト/ブロックリスト設定に一致する送信者またはドメインを検出した場合、受信者が複数存在すると (および各受信者のセーフリスト/ブロックリスト設定が異なると)、そのメッセージは分裂します。たとえば、受信者 A と受信者 B の両方に送信されるメッセージがあるとし、受信者 A のセーフリストにはこのメッセージの送信者のエントリがありますが、受信者 B にはセーフリストにもブロックリストにもエントリがありません。この場合、メッセージは 2 つのメッセージ ID で 2 つのメッセージに分割されます。受信者 A に送信されるメッセージは、セーフリストに一致していることが *X-SLBL-Result-* セーフリスト ヘッダーによってマークされ、アンチスパム スキャンをスキップします。一方、受信者 B 宛のメッセージは、アンチスパム スキャン エンジンによってスキャンされます。その後、どちらのメッセージもパイプライン (アンチウイルス スキャン、コンテンツ ポリシーなど) を続行し、設定されているすべての設定に従います。

メッセージの送信者またはドメインがブロックリストに含まれる場合、配信の動作は、ブロックリスト アクション設定によって決まります。セーフリストの配信の場合と同様に、セーフリスト/ブロックリスト設定の異なる複数の受信者が存在すると、そのメッセージは分裂します。分裂したメッセージのうちブロックリストに含まれるものは、ブロックリスト アクション設定に応じて隔離されるかドロップされます。ブロックリスト アクションの設定が隔離を実行するようになっている場合、そのメッセージはスキャンされ、最終的に隔離されます。ブロックリスト アクションがドロップに設定されている場合、そのメッセージは、セーフリスト/ブロックリスト スキャンの直後にドロップされます。

セーフリストとブロックリストはスパム隔離内で管理されているため、配信の動作は、他のアンチスパム設定にも左右されます。たとえば、アンチスパム スキャンをスキップするように HAT で「Accept」メール フロー ポリシーを設定すると、そのリスナー上でメールを受信するユーザは、自分のセーフリストとブロックリストの設定がそのリスナー上で受信されたメールに適用されなくなります。同様に、一部のメッセージ受信者についてアンチスパム スキャンをスキップするメールフロー ポリシーを作成すると、それらの受信者は、自分のセーフリストとブロックリストの設定が適用されなくなります。

セーフリストとブロックリストの作成およびメンテナンスの概要

セーフリストとブロック リストを使用するには、次の作業を実行します。

- **スパム隔離のイネーブル化と設定。**セーフリストとブロックリストはスパム隔離からアクセスされるため、セーフリストとブロックリストを使用するにはこの機能をイネーブルにする必要があります。詳細については、「スパム隔離の設定」(P.27-19) を参照してください。

- **セーフリスト/ブロックリスト機能のイネーブル化と設定。** スпам隔離をイネーブルにした後、セーフリスト/ブロックリスト機能をイネーブルにし、設定します。ブロックリストの電子メールに対するブロックリストアクション（隔離または削除）も設定する必要があります。詳細については、「セーフリストとブロックリストの設定」(P.27-38)を参照してください。
- **セーフリスト/ブロックリスト データベースのバックアップと復元。** アップグレードするとき、セーフリスト/ブロックリスト データベースをバックアップし、復元する作業が必要になります。詳細については、「セーフリスト/ブロックリスト データベースのバックアップと復元」(P.27-38)を参照してください。
- **セーフリスト/ブロックリスト データベースの同期。** エンド ユーザがセーフリストまたはブロックリストのエントリを入力すると、それらの設定はデータベースに保存されます。このデータベースは、AsyncOS が電子メールを処理する際に使用するデータベースと定期的に同期されます。スパム隔離がセキュリティ管理アプライアンス上に維持されている場合、管理者は、電子メールセキュリティアプライアンスと同期するようにセーフリスト/ブロックリスト データベースを設定する必要があります。詳細については、「セーフリストとブロックリストの設定とデータベースの同期」(P.27-39)を参照してください。
- **セーフリストとブロックリストのトラブルシューティング。** セーフリストとブロックリストをトラブルシューティングするために、ログ、アラートを確認できます。詳細については、「セーフリストとブロックリストのトラブルシューティング」(P.27-40)を参照してください。

セーフリストとブロック リストの設定

はじめる前に

セーフリストとブロックリストを設定する前に、スパム隔離をイネーブルにし、設定しておく必要があります。

手順

-
- ステップ 1** [モニタ (Monitor)] > [スпам隔離 (Spam Quarantine)] を選択します。
 - ステップ 2** [エンドユーザセーフリスト/ブロックリスト設定 (End-User Safelist/Blocklist)] セクションで、[有効 (Enable)] を選択してから、[設定を編集 (Edit Settings)] を選択します。
 - ステップ 3** [セーフリスト/ブロックリスト機能を有効にする (Enable Safelist/Blocklist Feature)] を選択します。
 - ステップ 4** [ブロックリストアクション (Blocklist Action)] に [隔離 (Quarantine)] または [削除 (Delete)] を選択します。
 - ステップ 5** [ユーザごとの最大リスト項目数 (Maximum List Items Per User)] を指定します。この値は、ユーザが各セーフリストとブロックリストに載せることのできるアドレスまたはドメインの最大数を表します。
 - ステップ 6** [送信 (Submit)] をクリックします。
-

セーフリスト/ブロックリスト データベースのバックアップと復元

セーフリスト/ブロックリスト データベースのバックアップを保存するには、Cisco アプライアンスでデータベースを .CSV ファイルとして保存します。 .CSV ファイルは、アプライアンスの設定が格納される XML 設定ファイルとは別に保管されます。アプライアンスをアップグレードする場合、またはインストール ウィザードを実行する場合、セーフリスト/ブロックリスト データベースを .CSV ファイルにバックアップする必要があります。

ファイルをバックアップすると、アプライアンスによって、.CSV ファイルが次の命名規約に従って /configuration ディレクトリに保存されます。

```
slbl<timestamp><serial number>.csv
```

バックアップと復元は、GUI の [システム管理 (System Administration)] > [設定ファイル (Configuration File)] ページか、CLI で slblconfig コマンドを使用して実行できます。

データベースを /configuration ディレクトリにバックアップするには、CLI から、slblconfig -> export コマンドを使用します。バックアップからデータベースを復元するには、slblconfig -> import コマンドを使用します。/configuration ディレクトリのバックアップ ファイルのリストから、使用するデータベースを選択します。無効なエントリを無視するかどうかを選択できます。

データベースのバックアップと復元に GUI を使用します。

手順

-
- ステップ 1** [システム管理 (System Administration)] > [設定ファイル (Configuration File)] から、[エンドユーザ セーフリスト/ブロックリスト データベース (End-User Safelist/Blocklist Database)] セクションに移動します。
- ステップ 2** データベースを .CSV ファイルにバックアップするには、[今すぐバックアップ (Backup Now)] をクリックします。
- ステップ 3** データベースを復元するには、[リストアするファイルを選択 (Select File to Restore)] をクリックします。
- アプライアンスにより、configuration ディレクトリに保管されているバックアップ ファイルのリストが表示されます。
- ステップ 4** 復元するセーフリスト/ブロックリスト バックアップ ファイルを選択し、[リストア (Restore)] をクリックします。
-

セーフリストとブロックリストの設定とデータベースの同期

エンドユーザがセーフリストまたはブロックリストを作成すると、その設定はデータベースに保存されます。スパム隔離がセキュリティ管理アプライアンス上に存在する場合、セーフリスト/ブロックリスト設定が着信メールに適用される前に、このデータベースを C-Series アプライアンス上のデータベースと同期する必要があります。スパム隔離が C-Series アプライアンス上に存在する場合は、このデータベースを、メールキューを処理するときに使用される読み取り専用データベースと同期する必要があります。これらのデータベースを自動で同期するのにかかる時間は、アプライアンスのモデルによって異なります。次の表に、セーフリストとブロックリストの更新についてのデフォルトの設定を示します。

表 27-6 セーフリストとブロックリストの設定の同期

アプライアンス	同期時間
C160/170	10 分
C360/C370	15 分
C660/C670	30 分
X1060/X1070	60 分
M660	120 分
M1050/M1060	240 分

C-Series アプライアンスのグループをセキュリティ管理アプライアンスなしで使用する場合は、セーフリスト/ブロックリストの設定とデータベースはマシン間で同期する必要があります。

集中管理機能を使用して複数の Cisco アプライアンスを設定する場合は、集中管理を使用して管理者設定を設定できます。集中管理を使用しない場合は、マシン間で設定が整合していることを手動で確認できます。

FTP を使用してアプライアンスにアクセスする方法の詳細については、『Cisco IronPort AsyncOS for Email Configuration Guide』の「Accessing the Appliance」を参照してください。

セーフリストとブロックリストのトラブルシューティング

各エンドユーザは、それぞれ独自のセーフリストとブロックリストを維持します。管理者は、エンドユーザアカウントにそのユーザのログイン名とパスワードでログインした場合にのみ、エンドユーザのセーフリストまたはブロックリストにアクセスできます。セーフリストとブロックリストに関する問題をトラブルシューティングするために、ログファイルまたはシステムアラートを表示できます。

電子メールがセーフリスト/ブロックリスト設定によってブロックされると、そのアクションが ISQ_logs またはアンチスパム ログファイルにロギングされます。セーフリストに含まれる電子メールは、セーフリストに一致していることが *X-SLBL-Result* セーフリストヘッダーによってマークされます。ブロックリストに含まれる電子メールは、ブロックリストに一致していることが *X-SLBL-Result-Blocklist* ヘッダーによってマークされます。

アラートは、データベースが作成または更新されたり、データベースの変更またはセーフリスト/ブロックリストプロセスの実行においてエラーが発生したりすると送信されます。

アラートの詳細については、第 29 章「アラート」を参照してください。

ログファイルの詳細については、第 34 章「ロギング」を参照してください。

セーフリストとブロックリストを設定するためのエンドユーザ作業

エンドユーザは、特定の送信者からのメッセージをスパムの判定から除外するために、セーフリストを作成できます。また、特定の送信者からのメッセージを常にスパムとして扱うために、ブロックリストを使用できます。たとえば、エンドユーザは、もう興味のないメーリングリストから電子メールを受信している場合があります。そのようなユーザは、このメーリングリストからの電子メールが自分の受信箱に送信されないように、その送信者を自分のブロックリストに追加できます。また他方で、エンドユーザは、スパムではない特定の送信者からの電子メールが自分のスパム隔離に送信されていることに気づくこともあります。これらの送信者からの電子メールが隔離されないようにするために、エンドユーザはそれらの送信者を自分のセーフリストに追加できます。



(注)

セーフリスト/ブロックリスト設定は、システム管理者が設定する他の設定の影響を受けます。

セーフリストとブロックリストを利用するために、エンドユーザは次の作業を実行する必要があります。

- **セーフリストとブロックリストにアクセスします。** 認証の設定によっては、エンドユーザは自分のスパム隔離アカウントにログインする必要があります。詳細については、「[セーフリストとブロックリストへのアクセス](#)」(P.27-41)を参照してください。
- **セーフリスト エントリを追加します。** ユーザは、スパム隔離内の [オプション (Options)] メニューまたは隔離されたメッセージのリストからセーフリスト エントリを追加します。詳細については、「[セーフリストへのエントリの追加](#)」(P.27-41)を参照してください。

- **ブロックリスト エントリを追加します。** ユーザは、スパム隔離内の [オプション (Options)] メニューからブロックリスト エントリを追加します。詳細については、「[ブロックリストへの送信者の追加](#)」(P.27-42) を参照してください。

セーフリストとブロックリストへのアクセス

LDAP 認証またはメールボックス (IMAP/POP) 認証を使用してアカウントが認証されるエンド ユーザは、セーフリストとブロックリストにアクセスするために、スパム隔離に対して自分のアカウントにログインする必要があります。これらのエンド ユーザは、通常はスパム通知経由で自分のメッセージにアクセスしているとしても (この場合は一般に認証を必要としません)、自分のアカウントにログインしなければなりません。エンドユーザ認証が [NONE] に設定されている場合、エンド ユーザは、セーフリスト/ブロックリスト設定にアクセスする際に自分のアカウントにログインする必要はありません。

セーフリスト エントリとブロックリスト エントリの構文

各エントリは、次の形式でセーフリストとブロックリストに追加できます。

- user@domain.com
- server.domain.com
- domain.com

エンド ユーザは、同じ送信者またはドメインをセーフリストとブロックリストの両方に同時には追加できません。ただし、エンド ユーザがあるドメインをセーフリストに追加し、そのドメインに所属するユーザの電子メール アドレスをブロックリストに追加した場合、アプライアンスは両方のルールを適用します (逆の場合も同様です)。たとえば、エンド ユーザが *example.com* をセーフリストに追加し、*george@example.com* をブロックリストに追加すると、アプライアンスは、*example.com* からのすべてのメールをスパムかどうかスキャンせずに配信しますが、*george@example.com* からのメールはスパムとして処理します。

エンド ユーザは、*.domain.com* のような構文を使用して、サブドメインの範囲を許可したり、ブロックしたりはできません。ただし、エンド ユーザは、*server.domain.com* のような構文を使用して、特定のドメインを明示的にブロックすることはできます。

セーフリストへのエントリの追加

エンド ユーザは、次の 2 つの方法で送信者をセーフリストに追加できます。

隔離されたメッセージの送信者のセーフリストへの追加

エンド ユーザは、メッセージがエンド ユーザ隔離に送信された場合、その送信者をセーフリストに追加できます。

手順

- ステップ 1** エンドユーザ隔離から、メッセージの横にあるチェックボックスをオンにします。
- ステップ 2** ドロップダウン メニューから [リリースしてセーフリストに追加 (Release and Add to Safelist)] を選択します。

■ 送信者に基づいて電子メール配信を制御するセーフリストおよびブロックを使用

指定したメールのエンベロープ送信者と差出人ヘッダーが両方ともセーフリストに追加されます。解放されたメッセージは、それ以降の電子メールパイプライン内のワークキューの処理をスキップして、宛先キューへ直接進みます。

隔離されたメッセージのない送信者のセーフリストへの追加

手順

- ステップ 1 スпам隔離から、右上にある [オプション (Options)] ドロップダウンメニューを選択します。
- ステップ 2 [セーフリスト (Safelist)] を選択します。
- ステップ 3 [セーフリスト (Safelist)] ダイアログボックスから、電子メール アドレスまたはドメインを入力します。ドメインと電子メールアドレスは、コンマで区切って複数入力できます。
- ステップ 4 [リストに追加 (Add to List)] をクリックします。

ブロックリストへの送信者の追加

アプライアンスは、ブロックリスト内のエントリと一致する電子メール アドレスまたはドメインからのメールを受信すると、そのメールをスパムとして処理します。このメールは、セーフリスト/ブロックリスト アクション設定に応じて、拒否されるか、隔離されます。



- (注) セーフリスト エントリとは異なり、ブロックリスト エントリは、エンドユーザ隔離内の [オプション (Options)] メニューからだけ追加できます。

手順

- ステップ 1 エンドユーザ隔離から、右上にある [オプション (Options)] ドロップダウンメニューを選択します。
- ステップ 2 ブロックリストに追加するドメインまたは電子メールアドレスを入力します。ドメインと電子メールアドレスは、コンマで区切って複数入力できます。
- ステップ 3 [リストに追加 (Add to List)] をクリックします。



CHAPTER 28

管理タスクの分散

- 「ユーザ アカウントを使用する作業」 (P.28-1)
- 「委任管理のためのカスタム ユーザ ロールの管理」 (P.28-7)
- 「パスワード」 (P.28-17)
- 「電子メール セキュリティ アプライアンスの設定」 (P.28-24)
- 「セキュア シェル (SSH) キーの管理」 (P.28-27)

ユーザ アカウントを使用する作業

Cisco アプライアンスには、ユーザ アカウントを追加する 2 つの方法があります。Cisco アプライアンス自体でユーザ アカウントを作成する方法と、LDAP または RADIUS ディレクトリなどの独自の中央認証システムを使用してユーザ認証をイネーブにする方法です。ユーザと外部認証ソースへの接続を管理するには、[システム管理 (System Administration)] > [ユーザ (Users)] ページを使用します (または、CLI で `userconfig` コマンドを使用します)。ユーザを認証するために外部ディレクトリを使用することについては、「外部認証 (External Authentication)」 (P.28-21) を参照してください。

システムのデフォルトのユーザ アカウントである `admin` はすべての管理権限を持っています。`admin` ユーザ アカウントは削除できませんが、パスワードを変更してアカウントをロックすることはできません。

新しいユーザ アカウントを作成する場合は、そのユーザを定義済みのユーザ ロールまたはカスタム ユーザ ロールに割り当てます。各ロールには、システム内での異なるレベルの権限が含まれます。

アプライアンスで作成できる各ユーザ アカウントの数に制限はありませんが、システムで予約されている名前とユーザ アカウントは作成できません。たとえば、「operator」や「root」などの名前のユーザ アカウントは作成できません。

表 28-1 は、ユーザ アカウントで使用可能なロールを示しています。

表 28-1 ユーザ ロールの一覧

ユーザロール	説明
admin	<p>admin ユーザはシステムのデフォルト ユーザ アカウントであり、すべての管理権限を持っています。便宜上、admin ユーザ アカウントをここに記載しましたが、これはユーザ ロールを使用して割り当てることはできず、パスワードの変更以外、編集や削除もできません。</p> <p>resetconfig コマンドと revert コマンドを発行できるのは、admin ユーザだけです。</p>
Administrator	<p>Administrator ロールを持つユーザ アカウントはシステムのすべての設定に対する完全なアクセス権を持っています。ただし、resetconfig コマンドと revert コマンドにアクセスできるのは admin ユーザだけです。</p> <p>(注) AsyncOS は、GUI から電子メールセキュリティ アプライアンスを同時に設定する複数の管理者をサポートしません。</p>
Technician	<p>Technician ロールを持つユーザ アカウントはシステムのアップグレード、アプライアンスの再起動、ライセンス キーの管理を実行できます。Technician は、アプライアンスをアップグレードするために以下の処理も実行できます。</p> <ul style="list-style-type: none"> • 電子メールの配信および受信の一時停止。 • ワークキューとリスナーのステータスの表示。 • 設定ファイルの保存および電子メール送信。 • セーフリストとブロックリストのバックアップ。Technician はこれらのリストを復元できません。 • クラスタからのアプライアンスの接続解除。 • Cisco テクニカル サポートへのリモート サービス アクセスのイネーブル化またはディセーブル化。 • サポート要求の申請。
Operator	<p>Operator ロールを持つユーザ アカウントは次のことができません。</p> <ul style="list-style-type: none"> • ユーザ アカウントの作成または編集。 • resetconfig コマンドの発行。 • アプライアンスのアップグレード • systemsetup コマンドの発行またはシステム設定ウィザードの実行。 • adminaccessconfig コマンドの発行。 • 隔離機能の実行（作成、編集、削除、および隔離の中央集中を含む）。 • ユーザ名とパスワード以外の LDAP サーバ プロファイル設定の変更（LDAP が外部認証に対してイネーブルになっている場合）。 <p>これら以外は、Administrator ロールと同じ権限を持ちます。</p>
Guest	<p>Guest ロールを持つユーザ アカウントはステータス情報だけを参照できます。Guest ロールを持つユーザは、アクセスが隔離でイネーブルの場合、隔離エリア内のメッセージを管理できます。Guest ロールを持つユーザはメッセージ トラッキングにアクセスできません。</p>

表 28-1 ユーザ ロールの一覧

ユーザロール	説明
Read-Only Operator	<p>Read-Only Operator ロールを持つユーザは、設定情報を参照するアクセス権を持っています。Read-Only Operator ロールを持つユーザは、機能の設定方法を確認するために変更を行って送信できますが、保存できません。このロールのユーザは、アクセスが隔離でイネーブルの場合、隔離エリア内のメッセージを管理できます。</p> <p>このロールのユーザは、以下にはアクセスできません。</p> <ul style="list-style-type: none"> ファイル システム、FTP、SCP。 作成、編集、削除、または隔離の中央集中の設定。
Help Desk User	<p>Help Desk User ロールを持つユーザがアクセスできるのは次のものに制限されます。</p> <ul style="list-style-type: none"> メッセージ トラッキング。 隔離エリア内のメッセージの管理。 <p>このロールを持つユーザは、CLI を含めたこれ以外のシステムにはアクセスできません。このロールのユーザがそのデバイスを管理する前に、各隔離アクセスをイネーブルにする必要があります。</p>
Custom user role	<p>Custom user role を持つユーザ アカウントはそのロールに割り当てられている電子メール セキュリティ機能にのみアクセスできます。アクセスできる機能は、DLP ポリシー、電子メール ポリシー、レポート、隔離、ローカル メッセージ トラッキング、暗号化プロファイル、およびトレース デバッグ ツールの任意の組み合わせになります。このユーザはシステム設定機能にはアクセスできません。Custom user role を定義できるのは管理者だけです。詳細については、「委任管理のためのカスタム ユーザ ロールの管理」(P.28-7) を参照してください。</p> <p>(注) Custom user role に割り当てられているユーザは、CLI にアクセスできません。</p>

表 28-1 に定義されているロールはすべて GUI と CLI の両方にアクセスできます。ただし、Help Desk User と Custom user role は GUI にのみアクセスできます。

ユーザを認証するために LDAP ディレクトリを使用する場合は、ユーザ ロールに個々のユーザではなくディレクトリ グループを割り当てます。ユーザ ロールにディレクトリ グループを割り当てると、そのグループの各ユーザはそのユーザ ロールで定義された権限を受け取ります。詳細については、「[外部認証 \(External Authentication\)](#)」(P.28-21) を参照してください。

ユーザの管理

[システム管理 (System Administration)] > [ユーザ (Users)] ページで、ユーザを管理できます。

[ユーザ (Users)] ページには、システムの既存のユーザが一覧 (ユーザ名、氏名、およびユーザ タイプまたはグループを含む) で表示されます。

[ユーザ (Users)] ページからは、次の操作が行えます。

- 新しいユーザの追加。詳細については、「[ユーザの追加](#)」(P.28-4) を参照してください。
- ユーザの削除。詳細については、「[ユーザの削除](#)」(P.28-5) を参照してください。

- ユーザの編集。ユーザのパスワードの変更、ユーザのアカウントのロックおよびロック解除など。詳細については、「[ユーザの編集](#)」(P.28-4) を参照してください。
- ローカル アカウント用のユーザ アカウントとパスワード設定値の設定。詳細については、「[制限的なユーザ アカウントとパスワードの設定値の設定](#)」(P.28-18) を参照してください。
- ユーザを認証するために LDAP または RADIUS ディレクトリを使用するようアプライアンスをイネーブルにする。詳細については、「[外部認証 \(External Authentication\)](#)」(P.28-21) を参照してください。
- メッセージ トラッキング内の DLP Matched Content への管理者以外のアクセスをイネーブルにする。詳細については、「[メッセージ トラッキングでの機密情報へのアクセスの制御](#)」(P.28-5) を参照してください。

ユーザの追加

はじめる前に

ユーザが使用するユーザ ロールを設定します。詳細については、[表 28-1](#) を参照してください。

手順

-
- ステップ 1** [システム管理 (System Administration)] > [ユーザ (Users)] を選択します。
 - ステップ 2** [ユーザを追加 (Add User)] をクリックします。
 - ステップ 3** ユーザのログイン名を入力します。一部の単語 («operator» や «root» など) は予約されています。
 - ステップ 4** ユーザの氏名を入力します。
 - ステップ 5** 定義済みのユーザ ロールまたはカスタム ユーザ ロール (Custom user role) を選択します。



(注) 新しいユーザ ロールを作成して、このユーザ アカウントに適用することができます。詳細については、「[委任管理のためのカスタム ユーザ ロールの管理](#)」(P.28-7) を参照してください。

- ステップ 6** パスワードを入力し、パスワードを再入力します。パスワードは、[ローカル ユーザ アカウントとパスワードの設定 (Local User Account & Password Settings)] セクションで定義されているルールに準拠している必要があります。詳細については、「[制限的なユーザ アカウントとパスワードの設定値の設定](#)」(P.28-18) を参照してください。
 - ステップ 7** 変更内容を送信し、確定します。
-

ユーザの編集

パスワードなどを変更するには、この手順を使用します。

手順

-
- ステップ 1** [システム管理 (System Administration)] > [ユーザ (Users)] を選択します。
 - ステップ 2** [ユーザ (Users)] 一覧でユーザの名前をクリックします。
 - ステップ 3** ユーザに対して変更を行います。

ステップ 4 変更内容を送信し、確定します。

ユーザの削除

手順

- ステップ 1** [ユーザ (Users)] 一覧でユーザの名前に対応するゴミ箱のアイコンをクリックします。
- ステップ 2** 表示される警告ダイアログで [削除 (Delete)] をクリックして、削除を確定します。
- ステップ 3** 変更内容を確定します。

メッセージ トラッキングでの機密情報へのアクセスの制御

データ消失防止 (DLP) ポリシーに違反するメッセージには、一般的に企業の秘密情報、またはカード番号や健康の記録を含む個人情報などの機密情報が含まれています。デフォルトで、この内容はメッセージ トラッキング結果に表示されているメッセージの [メッセージの詳細 (Message Details)] ページにある [DLP に一致した内容 (DLP Matched Content)] タブに表示されます。

管理者ユーザは常にこの内容を確認できます。ただし、割り当てられた定義済みまたはカスタム ロールに基づいてメッセージ トラッキングへのアクセス権を持つユーザに対してこのタブと内容を非表示にすることもできます。

はじめる前に

DLP 機密データをメッセージ トラッキングに表示するかどうかを決定する一致したコンテンツのロギングをイネーブルにするかどうかを設定します。「[メッセージ トラッキングの機密 DLP データの表示または非表示](#)」(P.15-38) を参照してください。

手順

- ステップ 1** [システム管理 (System Administration)] > [ユーザ (Users)] ページに移動します。
- ステップ 2** [DLP トラッキング権限 (DLP Tracking Privileges)] で、[設定を編集 (Edit Settings)] をクリックします。
- ステップ 3** メッセージ トラッキングでの DLP データへのアクセス権を付与するロールを選択します。
メッセージ トラッキングにアクセスできないカスタム ロールはこの情報を見ることができないため、表示されません。
- ステップ 4** 変更内容を送信し、確定します。
この設定を有効にするには、[セキュリティ サービス (Security Services)] で以下の機能がイネーブルになっている必要があります。
 - メッセージ トラッキング
 - RSA Email DLP
 - [RSA メール DLP (RSA Email DLP)] > [一致したコンテンツのロギング (Matched Content Logging)]

複数のユーザをサポートする追加コマンド : who、whoami、last

次に、アプライアンスへの複数ユーザアクセスをサポートするコマンドを示します。

- who コマンドは、CLI からシステムにログインしたすべてのユーザ、ログイン時間、アイドル時間、およびユーザがログインしたリモート ホストを一覧表示します。

```
mail3.example.com> who
```

```
Username  Login Time  Idle Time  Remote Host  What
=====  =====  =====  =====  =====
admin     03:27PM    0s         10.1.3.201   cli
```

- Whoami コマンドは、現在ログインしているユーザのユーザ名および氏名と、ユーザが属しているグループを表示します。

```
mail3.example.com> whoami
```

```
Username: admin
Full Name: Administrator
Groups: admin, operators, config, log, guest
```

- last コマンドは、アプライアンスに最近ログインしていたユーザを表示します。また、リモートホストの IP アドレス、ログイン時間、ログアウト時間、および合計時間も表示されます。

```
mail3.example.com> last
```

```
Username  Remote Host  Login Time          Logout Time          Total Time
=====  =====  =====  =====  =====
admin     10.1.3.67    Sat May 15 23:42    still logged in     15m
admin     10.1.3.67    Sat May 15 22:52    Sat May 15 23:42    50m
admin     10.1.3.67    Sat May 15 11:02    Sat May 15 14:14    3h 12m
admin     10.1.3.67    Fri May 14 16:29    Fri May 14 17:43    1h 13m
shutdown                               Fri May 14 16:22
shutdown                               Fri May 14 16:15
admin     10.1.3.67    Fri May 14 16:05    Fri May 14 16:15    9m
```



```

admin      10.1.3.103   Fri May 14 16:12   Fri May 14 16:15   2m
admin      10.1.3.103   Thu May 13 09:31   Fri May 14 14:11   1d 4h 39m
admin      10.1.3.135   Fri May 14 10:57   Fri May 14 10:58   0m
admin      10.1.3.67    Thu May 13 17:00   Thu May 13 19:24   2h 24m

```

委任管理のためのカスタム ユーザ ロールの管理

カスタム ユーザ ロールを設計し、組織内でのそれぞれのロールに一致した特定の責任をユーザに委任することができます。委任管理者は、それぞれが責任を負う電子メールセキュリティ機能にのみアクセスでき、それぞれのロールに関連しないシステム設定機能にはアクセスできません。委任管理を行うことで、アプライアンスの電子メールセキュリティ機能に対するユーザのアクセスを、定義済みの Administrator、Operator、および Help Desk User ロールより柔軟に制御できるようになります。

たとえば、電子メールセキュリティ アプライアンスの特定ドメインの電子メールポリシーの管理に参与しているユーザがいる場合に、それらのユーザに、定義済みの Administrator および Operator ロールで付与されるシステム管理やセキュリティ サービスの設定機能にはアクセスさせたくないことがあります。それぞれのユーザに管理するメールポリシーへのアクセス権限、およびそれらのポリシーで処理されるメッセージを管理するために使用できる他の電子メールセキュリティ機能（メッセージトラッキングやポリシー隔離など）を付与できるメールポリシー管理者用のカスタム ユーザ ロールを作成できます。

GUI で [システム管理 (System Administration)] > [ユーザの役割 (User Roles)] ページを使用して（または、CLI で `userconfig -> role` コマンドを使用して）、カスタム ユーザ ロールを定義し、それぞれが責任を負う電子メールセキュリティ機能（メールポリシー、RSA Email DLP ポリシー、電子メールレポート、および隔離など）を管理します。委任管理者が管理できる電子メールセキュリティ機能の一覧については、「[アクセス権限の割り当て](#)」(P.28-9) を参照してください。カスタム ロールは、[システム管理 (System Administration)] > [ユーザ (Users)] ページを使用して、ローカル ユーザアカウントを追加または編集するときにも作成できます。詳細については、「[ユーザアカウント追加時のカスタム ユーザ ロールの定義](#)」(P.28-14) を参照してください。

カスタム ユーザ ロールを作成する際には、そのロールの責任が他の委任管理者の責任と重複しすぎないようにする必要があります。たとえば、複数の委任管理者が同じコンテンツ フィルタに対する責任を持ち、そのコンテンツ フィルタを異なるメールポリシーで使用する場合、1 人の委任管理者がそのフィルタに加えた変更により、他の委任管理者が管理しているメールポリシーに意図せぬ悪影響を及ぼすことがあります。

カスタム ユーザ ロールを作成すると、他のユーザ ロールと同様にローカル ユーザと外部認証グループをそのカスタム ユーザ ロールに割り当てることができます。詳細については、「[ユーザアカウントを使用する作業](#)」(P.28-1) を参照してください。カスタム ロールに割り当てられているユーザは CLI にアクセスできないことに注意してください。

図 28-1 は、電子メールセキュリティ アプライアンスに定義されているカスタム ユーザ ロールの一覧と各ロールに割り当てられているアクセス権限を示しています。

図 28-1 カスタム ユーザ ロールの一覧
User Roles

Custom User Roles for Delegated Administration										
Role Name	Privileges							Assigned Users	Duplicate	Delete
	Email Policies	Data Loss Prevention	Reporting	Message Tracking	Trace	Quarantines	Encryption Profiles			
DLP Administrator	No Access	DLP Policies: 3	Relevant Reports*	Available	No Access	No Access	Feature Disabled	susan1		
Policy Administrator	Incoming Policies: 1 Content Filters: 0 Outgoing Policies: 1 Content Filters: 0	No Access	Relevant Reports*	Available	No Access	Quarantines: 1	Feature Disabled	grace1		
Quarantine Manager	No Access	No Access	No Access	No Access	No Access	Quarantines: 3	Feature Disabled	jessie1		

* Report access for this role is controlled by the Mail Policy and DLP privileges.

Key: View restricted to editable items

[アカウント権限 (Account Privileges)] ページ

委任管理者がアプライアンスにログインすると、[アカウント権限 (Account Privileges)] ページに委任管理者が責任を持つセキュリティ機能へのリンク、およびそれぞれのアクセス権限についての簡単な説明が表示されます。委任管理者は、[オプション (Options)] メニューで [アカウント権限 (Account Privileges)] を選択することでこのページに戻ることができます。委任管理者は、Web ページの上部にあるメニューを使用して、管理する機能にアクセスすることもできます。

図 28-2 は、メールポリシー、電子メール レポーティング、メッセージ トラッキング、および隔離にアクセスできる委任管理者の [アカウント権限 (Account Privileges)] ページを示しています。

図 28-2 委任管理者の [アカウント権限 (Account Privileges)] ページ
Account Privileges (bob1)

Mail Policies	Incoming Mail Policies (1) Incoming Content Filters (1) Outgoing Mail Policies (1) Outgoing Content Filters (None Assigned) <i>Configure Email Policies and Content Filters.</i>
Email Reporting	Policy Reporting and DLP Reporting <i>View and analyze email traffic.</i>
Message Tracking	Message Tracking <i>Track messages.</i>
Quarantine	Manage Message Quarantines (1) <i>Manage messages in assigned Quarantines.</i>

アクセス権限の割り当て

カスタム ユーザ ロールを作成する場合、委任管理者が責任を負うセキュリティ機能へのアクセス レベルを定義します。

委任管理者が管理できるセキュリティ機能は以下のとおりです。

- 送受信のメール ポリシーとコンテンツ フィルタ。
- データ消失防止 (DLP) ポリシー。
- 電子メール レポーティング。
- メッセージ トラッキング。
- トレース デバッグ ツール。
- スпам、ポリシー、ウイルス、およびアウトブレイク 隔離。
- Cisco 電子メール暗号化プロファイル。

カスタム ユーザ ロールのアクセス レベルを定義したら、委任管理者が責任を負うことになる具体的なメール ポリシー、コンテンツ フィルタ、DLP ポリシー、隔離、または暗号化プロファイルを割り当てる必要があります。

たとえば、異なる RSA Email DLP ポリシーに対して責任を負う 2 つの異なる DLP ポリシー管理者 ロールを作成できます。1 つのロールは企業の秘密保持や許容範囲での使用に関する DLP 違反にのみ責任を負い、他のロールはプライバシー保護に関する DLP 違反に責任を負うようにできます。DLP ポリシーへのアクセスに加えて、これらのカスタム ユーザ ロールにはメッセージ データのトラッキング、隔離とレポートの表示に対する権限を割り当てることもできます。それらのロールは、メッセージ トラッキングの使用において責任を負うポリシーに関連する DLP 違反を検索できます。

カスタム ユーザ ロールに割り当てることができる責任については、[ユーザの役割 (User Roles)] ページの [代表管理者用のカスタムのユーザ役割 (Custom User Roles for Delegated Administration)] テーブル内の割り当て済み権限のリンクをクリックして確認できます。「[カスタム ユーザ ロールの責任のアップデート](#)」(P.28-15) を参照してください。

メール ポリシーとコンテンツ フィルタ

メール ポリシーとコンテンツ フィルタのアクセス権限では、電子メール セキュリティ アプライアンスの送受信メール ポリシーとコンテンツ フィルタへの委任管理者のアクセス レベルを定義します。特定のメール ポリシーとコンテンツ フィルタをカスタム ユーザ ロールに割り当て、そのロールに属する委任管理者、および Operator と Administrator だけがメール ポリシーとコンテンツ フィルタを管理できるようにすることができます。

このアクセス権限を持つすべての委任管理者は、デフォルトの送受信メール ポリシーを表示できますが、すべてのアクセス権限を持っている場合のみそれらのポリシーを編集できます。

アクセス権限を持つすべての委任管理者は、それぞれのメール ポリシーで使用する新しいコンテンツ フィルタを作成できます。委任管理者が作成したコンテンツ フィルタは、そのカスタム ユーザ ロールに割り当てられている他の委任管理者が使用できます。いずれのカスタム ユーザ ロールにも割り当てられていないコンテンツ フィルタはパブリックであり、メール ポリシーのアクセス権限を持つすべての委任管理者が表示できます。Operator や Administrator が作成したコンテンツ フィルタは、デフォルトでパブリックです。委任管理者は、それぞれのカスタム ユーザ ロールに割り当てられているメール ポリシーの既存のコンテンツ フィルタはすべてイネーブルまたはディセーブルにできますが、パブリック コンテンツ フィルタは変更も削除もできません。

委任管理者が自分のポリシー以外のメール ポリシーで使用されているコンテンツ フィルタを削除した場合、またはそのコンテンツ フィルタが他のカスタム ユーザ ロールに割り当てられている場合、AsyncOS はそのコンテンツ フィルタをシステムから削除しません。代わりに、AsyncOS はそのカスタム ユーザ ロールからコンテンツ フィルタのリンクを解除し、委任管理者のメール ポリシーから削除します。そのコンテンツ フィルタは、他のカスタム ユーザ ロールとメール ポリシーでは引き続き使用可能です。

委任管理者は、それぞれのコンテンツ フィルタで任意のテキスト リソースやディクショナリを使用できますが、GUI で [テキスト リソース (Text Resources)] ページや [ディクショナリ (Dictionaries)] ページにアクセスして、それらを表示または変更することはできません。委任管理者は、新しいテキスト リソースやディクショナリを作成することもできません。

送信メール ポリシーの場合、委任管理者は DLP ポリシーをイネーブルまたはディセーブルできますが、DLP ポリシーの権限も持っている場合を除き、DLP の設定をカスタマイズすることはできません。

メール ポリシーとコンテンツ フィルタ用の以下のアクセス レベルのいずれかをカスタム ユーザ ロールに割り当てることができます。

- アクセスなし (No access)** : 委任管理者は電子メール セキュリティ アプライアンスのメール ポリシーとコンテンツ フィルタを表示も編集もできません。
- 割り当てられた隔離を表示、割り当てられた隔離を編集 (View assigned, edit assigned)** : 委任管理者はカスタム ユーザ ロールに割り当てられているメール ポリシーとコンテンツ フィルタを表示および編集でき、新しいコンテンツ フィルタを作成できます。委任管理者は、ポリシーのアンチスパム、アンチウイルス、およびアウトブレイク フィルタの設定を編集できます。委任管理者はポリシーに対してそれぞれのコンテンツ フィルタをイネーブルにでき、責任があるものかどうかに関係なく、そのポリシーに割り当てられている既存のコンテンツ フィルタをディセーブルにできます。委任管理者はメール ポリシーの名前、その送信者、受信者、またはグループを変更することはできません。委任管理者は、それぞれのカスタム ユーザ ロールに割り当てられているメール ポリシーのコンテンツ フィルタの順序を変更できます。
- すべてを表示、割り当てられた隔離を編集 (View all, edit assigned)** : 委任管理者は、アプライアンスのすべてのメール ポリシーとコンテンツ フィルタを表示できますが、そのカスタム ユーザ ロールに割り当てられているもののみ編集できます。

すべてを表示、すべてを編集 (フルアクセス) (View all, edit all (full access)) : 委任管理者は、アプライアンスのすべてのメール ポリシーとコンテンツ フィルタ (デフォルトのメール ポリシーを含む) に対するすべてのアクセス権限を持ち、新しいメール ポリシーを作成できます。委任管理者は、すべてのメール ポリシーの送信者、受信者、およびグループを変更できます。メール ポリシーの順序を変更することもできます。

[ユーザの役割 (User Roles)] ページの [電子メールセキュリティ マネージャ (Email Security Manager)] または [代表管理者用のカスタムのユーザ役割 (Custom User Roles for Delegated Administration)] テーブルを使用して、個々のメール ポリシーとコンテンツ フィルタをカスタム ユーザ ロールに割り当てることができます。

[代表管理者用のカスタムのユーザ役割 (Custom User Roles for Delegated Administration)] テーブルを使用したメール ポリシーとコンテンツ フィルタの割り当ての詳細については、「[カスタム ユーザ ロールの責任のアップデート](#)」(P.28-15) を参照してください。

DLP ポリシー

DLP ポリシーのアクセス権限では、電子メールセキュリティ アプライアンス の DLP Policy Manager を介した DLP ポリシーへの委任管理者のアクセス レベルを定義します。DLP ポリシーを特定のカスタム ユーザ ロールに割り当て、オペレータと管理者に加えて、委任管理者にそれらのポリシーを管理させることができます。DLP アクセス権を持つ委任管理者は、データ消失防止の Global Settings ページから DLP 設定ファイルをエクスポートできます。管理者およびオペレータだけが RSA Email DLP から RSA Enterprise Manager (またはその逆) の間に使用されている DLP モードを変更できます。

委任管理者がメール ポリシー権限も保持している場合は、RSA Email DLP ポリシーをカスタマイズできます。委任管理者は、それぞれの RSA Email DLP ポリシーの任意のカスタム DLP ディクショナリを使用できますが、カスタム DLP ディクショナリは表示も変更もできません。

RSA Email DLP ポリシー用の以下のアクセス レベルのいずれかをカスタム ユーザ ロールに割り当てることができます。

- **アクセスなし (No access)** : 委任管理者は 電子メールセキュリティ アプライアンス の RSA Email DLP ポリシーを表示も編集もできません。
- **割り当てられた隔離を表示、割り当てられた隔離を編集 (View assigned, edit assigned)** : 委任管理者は DLP Policy Manager を使用して、カスタム ユーザ ロールに割り当てられている RSA Email DLP ポリシーを表示および編集できます。委任管理者は、DLP Policy Manager 内の DLP ポリシーの名前変更も順序変更もできません。委任管理者は DLP 設定をエクスポートできます。
- **すべてを表示、割り当てられた隔離を編集 (View all, edit assigned)** : 委任管理者はカスタム ユーザ ロールに割り当てられている RSA Email DLP ポリシーを表示および編集できます。委任管理者は DLP 設定をエクスポートできます。委任管理者は、そのカスタム ユーザ ロールに割り当てられていない RSA Email DLP ポリシーをすべて表示できますが、編集することはできません。委任管理者は、DLP Policy Manager 内の DLP ポリシーの順序変更やポリシー名の変更はできません。
- **すべてを表示、すべてを編集 (フルアクセス) (View all, edit all (full access))** : 委任管理者は、アプライアンスのすべての RSA Email DLP ポリシーに対するすべてのアクセス権限を持ち、新しいポリシーを作成することもできます。委任管理者は、DLP Policy Manager 内の DLP ポリシーの順序を変更できます。また、アプライアンスで使用する DLP モードを変更できません。

[ユーザの役割 (User Roles)] ページの [DLP ポリシー マネージャ (DLP Policy Manager)] または [代表管理者用のカスタムのユーザ役割 (Custom User Roles for Delegated Administration)] テーブルを使用して、個々の RSA メール DLP ポリシーをカスタム ユーザ ロールに割り当てることができます。

RSA メール DLP ポリシーや DLP Policy Manager の詳細については、[第 15 章「データ消失防止」](#) を参照してください。

[代表管理者用のカスタムのユーザ役割 (Custom User Roles for Delegated Administration)] の一覧を使用して RSA Email DLP ポリシーを割り当てる方法の詳細については、「[カスタム ユーザ ロールの責任のアップデート](#)」(P.28-15) を参照してください。

電子メール レポートティング

電子メール レポートティングのアクセス権限では、カスタム ユーザ ロールのメール ポリシー、コンテンツ フィルタ、および RSA Email DLP ポリシーへのアクセス権限に従い、委任管理者が表示できるレポートと [電子メール セキュリティ モニタ (Email Security Monitor)] ページを定義します。それらのレポートは割り当てられているポリシーに対してフィルタリングされていません。委任管理者は、自分が責任を負っていないメールと DLP ポリシーのレポートを表示できます。

電子メール レポートティング用の以下のアクセス レベルのいずれかをカスタム ユーザ ロールに割り当てることができます。

- **No access (アクセスなし)** : 委任管理者は、電子メール セキュリティ アプライアンスのレポートを表示できません。
- **関連するレポートを表示 (View relevant reports)** : 委任管理者は、[電子メール セキュリティ モニタ (Email Security Monitor)] ページにあるそれぞれのメール ポリシー、コンテンツ フィルタ、および DLP ポリシーのアクセス権限に関連するレポートを表示できます。メール ポリシーとコンテンツ フィルタのアクセス権限がある委任管理者は、以下の [電子メール セキュリティ モニタ (Email Security Monitor)] ページを表示できます。
 - 概要 (Overview)
 - 受信メール (Incoming Mail)
 - 発信先 (Outgoing Destinations)
 - 送信メッセージ送信者 (Outgoing Senders)
 - 内部ユーザ (Internal Users)
 - コンテンツ フィルタ (Content Filters)
 - ウイルス アウトブレイク (Virus Outbreaks)
 - ウイルスの種類 (Virus Types)
 - アーカイブ済みのレポート (Archived Reports)

DLP ポリシーのアクセス権限がある委任管理者は、以下の [電子メール セキュリティ モニタ (Email Security Monitor)] ページを表示できます。

- 概要 (Overview)
- DLP インシデント (DLP Incidents)
- アーカイブ済みのレポート (Archived Reports)
- **すべてのレポートを表示 (View all reports)** : 委任管理者は、電子メール セキュリティ アプライアンスのすべてのレポートと [電子メール セキュリティ モニタ (Email Security Monitor)] ページを表示できます。

電子メール レポートティングと [電子メール セキュリティ モニタ (Email Security Monitor)] の詳細については、第 26 章「[電子メール セキュリティ モニタの使用方法](#)」(P.1) の章を参照してください。

メッセージ トラッキング

メッセージ トラッキングのアクセス権限では、カスタム ユーザ ロールに割り当てられている委任管理者がメッセージ トラッキングへのアクセス権限を持つかどうかを定義します。メッセージ トラッキングには、[システム管理 (System Administration)] > [ユーザ (Users)] ページで [DLP トラッキング ポリシー (DLP Tracking Policies)] オプションがイネーブルになっていて、カスタム ユーザ ロールに DLP ポリシーのアクセス権限もある場合に、組織の DLP ポリシー違反となる可能性があるメッセージの内容も含まれます。

委任管理者はそれぞれに割り当てられている RSA Email DLP ポリシーに対する DLP 違反のみ検索できます。

メッセージ トラッキングの詳細については、第 25 章「メッセージ トラッキング」(P.1) を参照してください。

委任管理者に、メッセージ トラッキング内の一致した DLP の内容を表示するためのアクセスを許可する方法の詳細については、「[メッセージ トラッキングでの機密情報へのアクセスの制御](#)」(P.28-5) を参照してください。

トレース (trace)

トレースのアクセス権限では、カスタム ユーザ ロールに割り当てられている委任管理者がトレースを使用して、システムを介したメッセージ フローをデバッグできるかどうかを定義します。アクセス権限がある委任管理者は、トレースを実行して、生成されるすべての出力を表示できます。トレース結果は、委任管理者のメールまたは DLP ポリシー権限に基づきフィルタリングはされません。

トレースの使用方法の詳細については、「[テスト メッセージを使用したメール フローのデバッグ：トレース](#)」(P.36-1) を参照してください。

隔離

隔離のアクセス権限では、委任管理者が割り当てられた隔離を管理できるかどうかを定義します。委任管理者は、割り当てられた隔離内の任意のメッセージを表示して、メッセージの解放や削除などのアクションを実行できますが、隔離の設定 (サイズ、保存期間など) の変更、隔離の作成や削除はできません。

[モニタ (Monitor)] > [隔離 (Quarantines)] ページまたは [ユーザの役割 (User Roles)] ページの [代表管理者用のカスタムのユーザ役割 (Custom User Roles for Delegated Administration)] テーブルを使用して、任意の隔離をカスタム ユーザ ロールに割り当てることができます。

隔離の詳細については、第 27 章「隔離」(P.1) を参照してください。

[代表管理者用のカスタムのユーザ役割 (Custom User Roles for Delegated Administration)] 一覧を使用して隔離を割り当て方法の詳細については、「[カスタム ユーザ ロールの責任のアップデート](#)」(P.28-15) を参照してください。

暗号化プロファイル

暗号化プロファイルのアクセス権限では、委任管理者がコンテンツ フィルタまたは DLP ポリシーの編集時に、それぞれのカスタム ユーザ ロールに割り当てられている暗号化プロファイルを使用できるかどうかを定義します。暗号化プロファイルは、メールまたは DLP ポリシーのアクセス権限があるカスタム ユーザ ロールにのみ割り当てることができます。カスタム ロールに割り当てられない暗号化プロファイルは、メールまたは DLP ポリシー権限を持つすべての委任管理者が使用できます。委任管理者はいずれの暗号化プロファイルも表示または変更できません。

暗号化プロファイルは、[セキュリティ サービス (Security Services)] > [IronPort メール暗号化 (IronPort Email Encryption)] ページを使用して暗号化プロファイルを作成または編集するときに割り当てることができます。

カスタム ユーザ ロールの定義

GUI で [ユーザの役割 (User Roles)] ページを使用して (または CLI で `userconfig -> role` コマンドを使用して)、新しいユーザ ロールを定義し、そのロールのアクセス権限を割り当てます。[ユーザの役割 (User Roles)] ページには、アプライアンスの既存のすべてのカスタム ユーザ ロールと各ロールのアクセス権限が表示されます。

手順

-
- ステップ 1 [システム管理 (System Administration)] > [User Roles (ユーザの役割)] を選択します。
 - ステップ 2 [ユーザ役割の追加 (Add User Role)] をクリックします。
 - ステップ 3 ユーザ ロールの名前を入力します。
 - ステップ 4 ユーザ ロールの説明とその権限を入力します。
 - ステップ 5 ユーザ ロールのアクセス権限を選択します。(各タイプのアクセス権限の詳細については、「[アクセス権限の割り当て](#)」(P.28-9) を参照してください)。
 - ステップ 6 変更内容を送信し、確定します。
-

ユーザ アカウント追加時のカスタム ユーザ ロールの定義

電子メールセキュリティ アプライアンスに対してローカル ユーザ アカウントの追加または編集を行う際に、新しいカスタム ユーザ ロールを作成できます。

ユーザ アカウントの追加の詳細については、「[ユーザの管理](#)」(P.28-3) を参照してください。

手順

-
- ステップ 1 [システム管理 (System Administration)] > [ユーザ (Users)] ページに移動します。
 - ステップ 2 [ユーザを追加 (Add User)] をクリックします。
 - ステップ 3 ユーザ アカウント作成時には、[カスタム役割 (Custom Roles)] を選択します。
 - ステップ 4 [役割を追加 (Add Role)] を選択します。
 - ステップ 5 新しいロールの名前を入力します。
 - ステップ 6 新しいユーザ アカウントを送信します。
AsyncOS により、新しいユーザ アカウントとカスタム ユーザ ロールが追加されたという通知が表示されます。
 - ステップ 7 [システム管理 (System Administration)] > [ユーザの役割 (User Roles)] ページに移動します。
 - ステップ 8 [代表管理者用のカスタムのユーザ役割 (Custom User Roles for Delegated Administration)] テーブルでカスタム ユーザ ロールの名前をクリックします。
 - ステップ 9 ユーザ ロールの説明とその権限を入力します。

ステップ 10 ユーザ ロールのアクセス権限を選択します。(各タイプのアクセス権限の詳細については、「[アクセス権限の割り当て](#)」(P.28-9) を参照してください。)

ステップ 11 変更内容を送信し、確定します。

カスタム ユーザ ロールの責任のアップデート

GUI の上部にあるメニューを使用して個々のセキュリティ機能をブラウズしてカスタム ユーザ ロールに責任を割り当てることができる一方、[ユーザの役割 (User Roles)] ページの [代表管理者用のカスタムのユーザ役割 (Custom User Roles for Delegated Administration)] テーブルでは、委任管理者が 1 つの場所で管理できるすべてのセキュリティ機能 (暗号化プロファイルを除く) へのリンクを統合できます。テーブルでカスタム ユーザ グループのアクセス権限の名前をクリックすると、アプライアンスのすべてのメール ポリシー、コンテンツ フィルタ、アクティブな RSA Email DLP ポリシー、または隔離の一覧が表示され、それらにアクセスできるその他すべてのカスタム ユーザ ロールの名前が表示されます。

たとえば、[図 28-3](#) は、電子メールセキュリティ アプライアンスで使用可能なアクティブな RSA Email DLP ポリシーの一覧を示しています。また、DLP ポリシーへのアクセス権限がある他のカスタム ユーザ グループも表示されています。この一覧から、管理者は、委任管理者が DLP Policy Manager で使用する DLP ポリシーを選択できます。

図 28-3 委任管理者が使用可能な DLP ポリシー
User Role: DLP Administrator > DLP Policies

Active DLP Policies for Outgoing Mail			
Include	Order	DLP Policy	Other Roles with Edit Access
<input checked="" type="checkbox"/>	1	Payment Card Industry Data Security Standard (PCI-DSS)	Domain Admin
<input checked="" type="checkbox"/>	2	California SB-1386	Domain Admin
<input type="checkbox"/>	3	Restricted Files	Domain Admin

Cancel Submit

手順

ステップ 1 [システム管理 (System Administration)] > [ユーザの役割 (User Roles)] ページに移動します。

ステップ 2 アップデートするカスタム ユーザ ロールのアクセス権限の名前をクリックします。

AsyncOS により、アプライアンスで使用可能なすべてのメール ポリシー、コンテンツ フィルタ、DLP ポリシー、または隔離の一覧、およびその他すべての割り当て済みカスタム ユーザ ロールの名前が表示されます。

ステップ 3 委任管理者に責任を割り当てるメール ポリシー、コンテンツ フィルタ、DLP ポリシー、または隔離を選択します。

ステップ 4 変更内容を送信し、確定します。

カスタム ユーザ ロールの編集

手順

- ステップ 1 [システム管理 (System Administration)] > [ユーザの役割 (User Roles)] ページに移動します。
- ステップ 2 [代表管理者用のカスタムのユーザ役割 (Custom User Roles for Delegated Administration)] 一覧でユーザ ロールの名前をクリックします。
- ステップ 3 ユーザ ロールに変更を加えます。
- ステップ 4 変更内容を送信し、確定します。

カスタム ユーザ ロールの複製

同様のアクセス権限がある複数のカスタム ユーザ ロールを作成し、異なるユーザのセットに異なる責任を割り当てたいことがあります。たとえば、電子メールセキュリティアプライアンスが複数ドメインのメッセージを処理する場合、同様のアクセス権限だが、ドメインに基づく異なるメール ポリシーに対する権限であるカスタム ユーザ ロールを作成することができます。こうすることで、委任管理者は、他の委任管理者の責任を妨げることなくそれぞれのドメインのメール ポリシーを管理できます。

手順

- ステップ 1 [システム管理 (System Administration)] > [ユーザの役割 (User Roles)] ページに移動します。
- ステップ 2 [代表管理者用のカスタムのユーザ役割 (Custom User Roles for Delegated Administration)] 一覧で、複製するユーザ ロールに対応する複製アイコンをクリックします。
- ステップ 3 カスタム ユーザ ロールの名前を変更します。
- ステップ 4 新しいカスタム ユーザ ロールに必要なすべてのアクセス権限の変更を行います。
- ステップ 5 変更内容を送信し、確定します。

カスタム ユーザ ロールの削除

カスタム ロールが削除されると、ユーザは未割り当て状態になり、アプライアンスにアクセスできなくなります。複数の個人に割り当てられたカスタム ユーザ ロールを削除すると、警告メッセージを受信しません。削除したカスタム ユーザ ロールに割り当てられていたすべてのユーザを再割り当てする必要があります。

手順

- ステップ 1 [システム管理 (System Administration)] > [ユーザの役割 (User Roles)] ページに移動します。
- ステップ 2 [代表管理者用のカスタムのユーザ役割 (Custom User Roles for Delegated Administration)] 一覧で、削除するユーザ ロールに対応するゴミ箱のアイコンをクリックします。
- ステップ 3 表示される警告ダイアログで [削除 (Delete)] をクリックして、削除を確定します。

ステップ 4 変更内容を確定します。

パスワード

パスワードの変更

ユーザは GUI の上部にある [オプション (Options)] > [パスワードの変更 (Change Password)] リンクを使用して自分のパスワードを変更できます。

古いパスワードを入力し、次に新しいパスワードを入力して確認のためにそのパスワードを再入力します。[送信 (Submit)] をクリックします。ログアウトされ、画面にログが表示されます。

CLI で、`password` コマンドまたは `passwd` コマンドを使用してパスワードを変更します。**admin** ユーザアカウントのパスワードを忘れた場合は、パスワードをリセットするためにカスタマー サポート プロバイダーにご連絡ください。

`password` コマンドでは、セキュリティのために古いパスワードの入力が必要です。



(注) パスワードの変更はすぐに有効になり、変更の確定は必要ではありません。

ユーザ アカウントのロックおよびロック解除

ユーザ アカウントのロックは、ローカル ユーザがアプライアンスにログインするのを防止します。ユーザ アカウントは、次のいずれかの場合にロックされることがあります。

- AsyncOS は、ユーザが [ローカルユーザアカウントとパスワードの設定 (Local User Account & Password Settings)] セクションで定義されている失敗ログイン試行の最大回数を超えた場合にユーザ アカウントをロックします。
- 管理者は、[システム管理 (System Administration)] > [ユーザ (Users)] ページを使用して、セキュリティ目的でユーザ アカウントを手動でロックできます。

[ユーザ役割の編集 (Edit User)] ページでユーザ アカウントを表示すると、AsyncOS によりユーザ アカウントがロックされた理由が表示されます。

ユーザ アカウントをロック解除するには、[ユーザ (Users)] 一覧でユーザ名をクリックしてユーザ アカウントを開き、[アカウントのロック解除 (Unlock Account)] をクリックします。

ローカル ユーザ アカウントを手動でロックするには、[ユーザ (Users)] 一覧でユーザ名をクリックしてユーザ アカウントを開き、[アカウントのロック (Lock Account)] をクリックします。AsyncOS は、ユーザがアプライアンスにログインできなくなるというメッセージを表示し、継続するかどうかを問い合わせてきます。

ユーザが設定した試行回数を超えた後でログインに失敗した場合、すべてのローカル ユーザ アカウントをロックするように設定することもできます。詳細については、「[制限的なユーザ アカウントとパスワードの設定値の設定](#)」(P.28-18) を参照してください。



(注) admin アカウントをロックした場合は、シリアル コンソール ポートへのシリアル通信接続経由で admin としてログインしてロック解除するしかありません。admin ユーザは、admin アカウントがロックされた場合でも、シリアル コンソール ポートを使用して常にアプライアンスにアクセスできます。シリアル コンソール ポートを使用してアプライアンスにアクセスする方法の詳細については、「[アプライアンスへの接続](#)」(P.3-8) を参照してください。

制限的なユーザ アカウントとパスワードの設定値の設定

ユーザ アカウントとパスワードの制限を定義して、組織全体にパスワード ポリシーを強制的に適用することができます。ユーザ アカウントとパスワードの制限は、Cisco アプライアンスで定義されているローカル ユーザに適用されます。次の設定値を設定できます。

- **ユーザ アカウントのロック。** ユーザがアカウントからロックアウトされるまでの、ログイン試行の失敗回数を定義できます。
- **パスワード持続期間のルール。** ログイン後にユーザがパスワードの変更を要求されるまでの、パスワードの使用期間を定義できます。
- **パスワードのルール。** どの文字が任意で、どの文字が必須かなど、ユーザが選択できるパスワードの種類を定義できます。

ユーザ アカウントとパスワードの制限は、[システム管理 (System Administration)] > [ユーザ (Users)] ページの [ローカル ユーザ アカウントとパスワードの設定 (Local User Account and Password Settings)] セクションで定義します。

手順

- ステップ 1** [システム管理 (System Administration)] > [ユーザ (Users)] を選択します。
- ステップ 2** [ローカル ユーザ アカウントとパスワードの設定 (Local User Account and Password Settings)] セクションまでページを下にスクロールします。
- ステップ 3** [設定を編集 (Edit Settings)] をクリックします。
- ステップ 4** [表 28-2](#) で説明されている設定を設定します。

表 28-2 ローカル ユーザ アカウントとパスワードの設定

設定	説明
ユーザ アカウントのロック (User Account Lock)	<p>ユーザが正常にログインできない場合に、ユーザ アカウントをロックするかどうかを決定します。アカウントがロックされるまでの、ログイン失敗回数を指定します。1 ~ 60 の範囲で任意の数字を入力できます。デフォルト値は 5 です。</p> <p>アカウントのロックを設定する場合は、ログインを試みているユーザに表示するメッセージを入力します。テキストは 7 ビット ASCII 文字を使用して入力します。このメッセージは、管理者によってロックされているユーザが正しいパスワードをアカウントに入力するときだけ表示されます。このメッセージは、ログイン試行の失敗によってロックされたアカウントには表示されません。</p> <p>ユーザ アカウントがロックされた場合、管理者は GUI で [ユーザの編集 (Edit User)] ページを使用するか、userconfig CLI コマンドを使用してロックを解除できます。</p> <p>失敗したログインの試行は、ユーザが接続しているマシンや、接続のタイプ (SSH または HTTP など) に関係なく、ユーザ別に追跡されます。ユーザがログインに成功すると、失敗ログイン試行の回数は 0 にリセットされます。</p> <p>失敗ログイン試行の最大回数に達したためにユーザ アカウントがロックアウトされると、管理者にアラートが送信されます。このアラートは「Info」重大度レベルに設定されます。</p> <p>(注) 個々のユーザ アカウントを手動でロックすることもできます。詳細については、「ユーザ アカウントのロックおよびロック解除」(P.28-17) を参照してください。</p>
Password Reset (パスワードのリセット)	<p>管理者がユーザのパスワードを変更した後で、ユーザにパスワードを強制的に変更させるかどうかを選択します。</p> <p>パスワードが期限切れになった後で、ユーザにパスワードを強制的に変更させるかどうかを選択することもできます。ユーザがパスワードを変更するまでのパスワードの存続日数を入力します。1 から 366 までの任意の数を入力できます。デフォルトは 90 です。</p> <p>期限切れ後にユーザにパスワードを強制的に変更させる場合は、次のパスワード期限に関する通知を表示できます。期限切れの何日前に通知が行われるかを選択します。</p> <p>パスワードが期限切れになると、ユーザは次回ログイン時にアカウントパスワードを強制的に変更させられます。</p> <p>(注) ユーザ アカウントがパスワードチャレンジの代わりに SSH キーを使用している場合でも、Password Reset ルールが適用されます。SSH キーを持つユーザ アカウントが期限切れになると、そのユーザは古いパスワードを入力するか、管理者に依頼して、パスワードを手動で変更し、アカウントに関連付けられたキーを変更してもらう必要があります。詳細については、「セキュア シェル (SSH) キーの管理」(P.28-27) を参照してください。</p>

表 28-2 ローカル ユーザ アカウントとパスワードの設定 (続き)

設定	説明
パスワードの規則 (Password Rules) : 必要な最小文字<数>。 (Require at <number> least characters.)	パスワードに含める最小文字数を入力します。 ゼロを含む番号を入力できます。
パスワードの規則 (Password Rules) : 数字 (0 ~ 9) が 1 文字以上必要です。(Require at least one number (0-9).)	パスワードに数字を少なくとも 1 文字含める必要があるかどうかを選択します。
パスワードの規則 (Password Rules) : 特殊文字が 1 文字以上必要です。(Require at least one special character.)	パスワードに 1 文字以上の特殊文字を含める必要があるかどうかを決定します。パスワードには、次の特殊文字を使用できます。 ~ ? ! @ # \$ % ^ & * - _ + = \ / [] () < > { } ` ' " ; : , .
パスワードの規則 (Password Rules) : ユーザ名とその変形をパスワードとして使用することはできません。(Ban usernames and their variations as passwords.)	関連付けられているユーザ名またはユーザ名のバリエーションと同じパスワードが認められるかどうかを選択します。ユーザ名のバリエーションが禁止されている場合、以下のルールがパスワードに適用されます。 <ul style="list-style-type: none"> パスワードは、大文字と小文字の違いがあってもユーザ名とは同じにできません。 パスワードは、大文字と小文字の違いがあってもユーザ名を反転したものと同じにできません。 パスワードは、以下の文字を置き換えた、ユーザ名または反転したユーザ名とは同じにできません。 <ul style="list-style-type: none"> 「a」の代わりに「@」または「4」 「e」の代わりに「3」 「i」の代わりに「!」、「!」、または「1」 「o」の代わりに「0」 「s」の代わりに「\$」または「5」 「t」の代わりに「+」または「7」
パスワードの規則 (Password Rules) : 直近<number>個のパスワードを再使用することはできません。(Ban reuse of the last <number> passwords.)	ユーザにパスワードの変更を強制する場合に、最近使用したパスワードを選択できるかどうかを決定します。最近のパスワードの再利用を禁止した場合、再利用を禁止する最近のパスワードの個数を入力します。 1 ~ 15 の範囲で任意の数字を入力できます。デフォルトは 3 です。

ステップ 5 変更内容を送信し、確定します。

外部認証 (External Authentication)

ネットワークの LDAP または RADIUS ディレクトリにユーザ情報を保存する場合は、外部ディレクトリを使用してアプライアンスにログインするユーザを認証するよう Cisco アプライアンスを設定できます。認証のために外部ディレクトリを使用するようアプライアンスを設定するには、GUI で [システム管理 (System Administration)] > [ユーザ (Users)] ページを使用するか、CLI で `userconfig` コマンドと `external` サブコマンドを使用します。

外部認証がイネーブルであり、ユーザが電子メールセキュリティアプライアンスにログインすると、アプライアンスは最初に、ユーザがシステム定義の「admin」アカウントであるかどうかを確認します。ユーザがシステム定義の「admin」アカウントでない場合、アプライアンスは最初に設定された外部サーバをチェックしてユーザがそこで定義されたかどうかを確認します。アプライアンスが最初の外部サーバに接続できなければ、アプライアンスは一覧の次の外部サーバをチェックします。

LDAP サーバの場合は、ユーザが外部サーバで認証に失敗すると、アプライアンスは電子メールセキュリティアプライアンスで定義されたローカルユーザとしてユーザを認証しようとします。そのユーザが外部サーバまたはアプライアンスに存在しない場合、またはユーザが間違ったパスワードを入力した場合は、アプライアンスへのアクセスが拒否されます。

外部 RADIUS サーバに接続できなければ、一覧の次のサーバが試行されます。すべてのサーバに接続できない場合、アプライアンスは電子メールセキュリティアプライアンスで定義されたローカルユーザとしてユーザを認証しようとします。ただし、外部 RADIUS サーバが何らかの理由（パスワード間違いやユーザ未登録など）でユーザを拒否すると、アプライアンスへのアクセスは拒否されます。

LDAP 認証のイネーブル化

ユーザを認証するために LDAP ディレクトリを使用する以外に、LDAP グループを Cisco ユーザロールに割り当てることができます。たとえば、IT グループのユーザを管理者ユーザロールに割り当てたり、Support グループのユーザをヘルプデスクユーザロールに割り当てたりできます。1 人のユーザが複数の LDAP グループに属しており、それぞれユーザロールが異なる場合は、最も限定的なロールのアクセス許可が AsyncOS によってそのユーザに付与されます。たとえば、ユーザが Operator 権限を持つグループと Help Desk User 権限を持つグループに属する場合、AsyncOS はユーザに Help Desk User ロールの権限を割り当てます。



(注)

外部ユーザが LDAP グループのユーザロールを変更する場合、外部ユーザはアプライアンスからログアウトし、再びログインする必要があります。このユーザは新しいロールの権限を持ちます。

はじめる前に

LDAP サーバの LDAP サーバプロファイルおよび外部認証クエリーを定義します。詳細については、[第 22 章「LDAP クエリー」](#)を参照してください。

手順

- ステップ 1** [システム管理 (System Administration)] > [ユーザ (Users)] を選択します。
- ステップ 2** [Web 認証 (Web Authentication)] セクションまでスクロールします。
- ステップ 3** [有効 (Enable)] をクリックします。
- ステップ 4** [外部認証を有効にする (Enable External Authentication)] チェックボックスをオンにします。
- ステップ 5** 認証タイプとして [LDAP] を選択します。
- ステップ 6** Web ユーザインターフェイスで、外部認証クレデンシャルを保存する時間を入力します。

- ステップ 7** ユーザを認証する LDAP 外部認証クエリーを選択します。
- ステップ 8** タイムアウトするまでアプライアンスがサーバからの応答を待つ時間を秒単位で入力します。
- ステップ 9** アプライアンスで認証する LDAP ディレクトリからのグループ名を入力し、グループのユーザに対するロールを選択します。
- ステップ 10** また、[行を追加 (Add Row)] をクリックして別のディレクトリ グループを追加することもできます。アプライアンスが認証する各ディレクトリ グループに対して、ステップ 9 とステップ 10 を繰り返します。
- ステップ 11** 変更内容を送信し、確定します。

RADIUS 認証のイネーブル化

ユーザを認証するために RADIUS ディレクトリを使用し、ユーザのグループを Cisco ロールに割り当てることもできます。RADIUS サーバは CLASS 属性をサポートする必要があります (AsyncOS は RADIUS ディレクトリのユーザを Cisco ユーザ ロールに割り当てるために CLASS 属性を使用します)。AsyncOS は、RADIUS サーバと通信するために Password Authentication Protocol (PAP; パスワード認証プロトコル) と Challenge Handshake Authentication Protocol (CHAP; チャレンジハンドシェイク認証プロトコル) の 2 つの認証プロトコルをサポートします。

RADIUS ユーザを Cisco ユーザ ロールに割り当てるには、最初に RADIUS サーバで <radius-group> という文字列値を使用して CLASS 属性を設定します (これは Cisco ユーザ ロールにマップされます)。CLASS 属性には文字、数字、およびダッシュを含めることができますが、先頭にダッシュを使用することはできません。AsyncOS は CLASS 属性で複数の値をサポートしません。CLASS 属性またはマップされていない CLASS 属性がないグループに属する RADIUS ユーザはアプライアンスにログインできません。

アプライアンスが RADIUS サーバと通信できない場合、ユーザはアプライアンスのローカル ユーザアカウントでログインできます。



(注) 外部ユーザが RADIUS グループのユーザ ロールを変更する場合、外部ユーザはアプライアンスからログアウトし、再びログインする必要があります。このユーザは新しいロールの権限を持ちます。

手順

- ステップ 1** [システム管理 (System Administration)] > [ユーザ (Users)] ページで、[有効 (Enable)] をクリックします。
- ステップ 2** まだイネーブルになっていない場合は、[外部認証 (External Authentication)] オプションを確認します。
- ステップ 3** RADIUS サーバのホスト名を入力します。
- ステップ 4** RADIUS サーバのポート番号を入力します。デフォルトのポート番号は 1812 です。
- ステップ 5** RADIUS サーバの共有秘密パスワードを入力します。
- ステップ 6** タイムアウトになる前にサーバからの応答をアプライアンスが待機する秒数を入力します。
- ステップ 7** (任意) [行を追加 (Add Row)] をクリックして別の RADIUS サーバを追加します。各 RADIUS サーバについてステップ 3 から 6 を繰り返して行ってください。



(注) 最大 10 台の RADIUS サーバを追加できます。

ステップ 8 RADIUS サーバに接続し再認証するまで AsyncOS が外部認証クレデンシャルを保存する秒数を [外部認証キャッシュタイムアウト (External Authentication Cache Timeout)] フィールドに入力します。デフォルトは 0 です。



(注) RADIUS サーバがワンタイム パスワード (たとえば、トークンから作成されるパスワード) を使用する場合、ゼロ (0) を入力します。値をゼロに設定すると、AsyncOS は、現在のセッション中に認証のために RADIUS サーバに再アクセスしません。

ステップ 9 グループ マッピングの設定

設定	説明
外部認証されたユーザを複数のローカルの役割に割り当てます。(Map externally authenticated users to multiple local roles.)	<p>AsyncOS は、RADIUS CLASS 属性に基づいて、RADIUS ユーザをアプライアンス ロールに割り当てます。CLASS 属性の要件：</p> <ul style="list-style-type: none"> • 3 文字以上 • 253 文字以下 • コロン、カンマ、または改行文字なし • 各 RADIUS ユーザに対し 1 つ以上のマップ済み CLASS 属性 (この設定を使用する場合、AsyncOS は、マップ済み CLASS 属性のない RADIUS ユーザへのアクセスを拒否します)。 <p>複数の CLASS 属性のある RADIUS ユーザの場合、AsyncOS は最も制限されたロールを割り当てます。たとえば、Operator ロールにマッピングされている CLASS 属性と、Read-Only Operator ロールにマッピングされている CLASS 属性の 2 つが RADIUS ユーザにある場合、AsyncOS は、Operator ロールよりも制限された Read-Only Operator ロールに RADIUS ユーザを割り当てます。</p> <p>次のアプライアンス ロールは、制限の少ないものから順番に並べられています。</p> <ul style="list-style-type: none"> • admin • Administrator • Technician • Operator • Read-Only Operator • Help Desk User • Guest
外部で認証されたすべてのユーザを管理者役割にマッピングします。(Map all externally authenticated users to the Administrator role.)	<p>AsyncOS は RADIUS ユーザを Administrator ロールに割り当てます。</p>

ステップ 10 外部認証されたすべてのユーザを管理者ロールまたはタイプ別のアプライアンスのユーザ ロールにマッピングするかを選択します。

ステップ 11 タイプの異なるロールにユーザをマッピングする場合、RADIUS CLASS 属性で定義したグループ名を [グループ名 (Group Name)] または [ディレクトリ (Directory)] フィールドに入力し、[役割 (Role)] フィールドからアプライアンス ロールを選択します。[行を追加 (Add Row)] をクリックして、より多くの役割のマッピングを追加できます。

ユーザ ロール タイプの詳細については、「[ユーザ アカウントを使用する作業](#)」(P.28-1) を参照してください。

ステップ 12 変更内容を送信し、確定します。

電子メール セキュリティ アプライアンスの設定

AsyncOS では電子メール セキュリティ アプライアンスへのユーザ アクセスを管理するために、管理者は Web UI セッションのタイムアウトや、アプライアンスにアクセス可能なユーザ IP アドレスと組織のプロキシ サーバ IP アドレスを規定したアクセス リストなどを制御できます。

IP ベースのネットワーク アクセスの設定

アプライアンスに直接接続するユーザおよび逆プロキシで接続するユーザ (リモート ユーザに逆プロキシを使用する組織の場合) のアクセス リストを作成して、電子メール セキュリティ アプライアンスにアクセスするユーザの IP アドレスを制御できます。

直接接続 (Direct Connections)

電子メール セキュリティ アプライアンスに接続可能なマシンの IP アドレス、サブネット、または CIDR アドレスを指定できます。ユーザは、アクセス リストの IP アドレスを持つすべてのマシンから、アプライアンスにアクセスできます。リストに含まれていないアドレスからアプライアンスに接続しようとするユーザは、アクセスを拒否されます。

プロキシ経由の接続

リモート ユーザのマシンと電子メール セキュリティ アプライアンスの間で逆プロキシ サーバが使用される組織のネットワークの場合、AsyncOS ではアプライアンスに接続可能なプロキシの IP アドレスを含むアクセス リストを作成できます。

逆プロキシを使用している場合でも、AsyncOS は、ユーザ接続が許可されている IP アドレスのリストと照合して、リモート ユーザのマシンの IP アドレスを検証します。リモート ユーザの IP アドレスを電子メール セキュリティ アプライアンスに送信するには、プロキシで `x-forwarded-for` HTTP ヘッダーをアプライアンスへの接続要求に含める必要があります。

`x-forwarded-for` ヘッダーは非 RFC 標準 HTTP ヘッダーであり、形式は次のとおりです。

```
x-forwarded-for: client-ip, proxy1, proxy2, ... CRLF.
```

このヘッダーの値はカンマ区切りの IP アドレスのリストであり、左端のアドレスがリモート ユーザ マシンのアドレスで、その後、接続要求を転送した一連の各プロキシのアドレスが続きます。(ヘッダー名を設定可能です)。電子メール セキュリティ アプライアンスは、ヘッダーのリモート ユーザの IP アドレスおよび接続プロキシの IP アドレスを、アクセス リストで許可されたユーザ IP アドレスやプロキシ IP アドレスと照合します。



(注) AsyncOS は、`x-forwarded-for` ヘッダーで IPv4 アドレスだけをサポートします。

アクセス リストの作成

GUI の [ネットワーク アクセス (Network Access)] ページまたは CLI の `adminaccessconfig > ipaccess` コマンドから、ネットワーク アクセス リストを作成できます。

AsyncOS には、アクセス リストに対する次の 4 つの異なる制御モードが用意されています。

- **[すべてを許可 (Allow All)]** このモードでは、アプライアンスへのすべての接続が許可されます。これが、デフォルトの動作モードです。
- **[特定の接続のみを許可 (Only Allow Specific Connections)]** このモードは、ユーザの IP アドレスが、アクセス リストに含まれている IP アドレス、IP 範囲、または CIDR 範囲と一致する場合に、ユーザのアプライアンスへの接続を許可します。
- **[Only Allow Specific Connections Through Proxy (特定のプロキシ経由接続のみを許可)]** このモードは、次の条件が満たされた場合に、逆プロキシを介したユーザのアプライアンスへの接続を許可します。
 - 接続プロキシの IP アドレスが、[プロキシ サーバ (Proxy Server)] フィールドのアクセス リストの IP アドレスに含まれている。
 - プロキシで、接続要求に `x-forwarded-header` HTTP ヘッダーが含まれている。
 - `x-forwarded-header` の値が空ではない。
 - リモートユーザの IP アドレスが `x-forwarded-header` に含まれ、それがアクセス リスト内の IP アドレス、IP 範囲、または CIDR 範囲と一致する。
- **[特定の直接またはプロキシ経由接続のみを許可 (Only Allow Specific Connections Directly or Through Proxy)]** このモードは、ユーザの IP アドレスが、アクセス リストに含まれている IP アドレス、IP 範囲、または CIDR 範囲と一致する場合に、ユーザの逆プロキシを介した、あるいは直接的なアプライアンスへの接続を許可します。プロキシ経由接続の条件は、[特定のプロキシ経由接続のみを許可 (Only Allow Specific Connections Through Proxy)] モードと同じです。

次のいずれかの条件が `true` の場合、変更を送信して確定した後、アプライアンスにアクセスできなくなることがありますので注意してください。

- [特定の接続のみを許可 (Only Allow Specific Connections)] を選択し、現在のマシンの IP アドレスがリストに含まれていない場合。
- [特定のプロキシ経由接続のみを許可 (Only Allow Specific Connections Through Proxy)] を選択し、現在アプライアンスに接続されているプロキシの IP アドレスがプロキシリストに存在せず、許可されている IP アドレスのリストに送信元 IP ヘッダーの値が存在しない場合。
- [特定の直接またはプロキシ経由接続のみを許可 (Only Allow Specific Connections Directly or Through Proxy)] を選択し、
 - 許可されている IP アドレスのリストに送信元 IP ヘッダーの値が存在しない場合
または
 - 許可されている IP アドレスのリストに送信元 IP ヘッダーの値が存在せず、アプライアンスに接続されたプロキシの IP アドレスが許可されているプロキシのリストに存在しない場合。

手順

- ステップ 1** [システム管理 (System Administration)] > [Network Access (ネットワーク アクセス)] を選択します。

- ステップ 2** [設定を編集 (Edit Settings)] をクリックします。
- ステップ 3** アクセス リストの制御モードを選択します。
- ステップ 4** ユーザがアプライアンスへの接続が許可される IP アドレスを入力します。
IP アドレス、IP アドレス範囲または CIDR 範囲を入力できます。複数のエントリを区切るには、カンマを使用します。
- ステップ 5** プロキシ経由の接続が許可されている場合は、次の情報を入力します。
- アプライアンスへの接続が許可されているプロキシの IP アドレス。複数のエントリを区切るには、カンマを使用します。
 - プロキシがアプライアンスに送信する発信元の IP ヘッダーの名前。これには、リモート ユーザ マシンの IP アドレスと、要求を転送したプロキシ サーバの IP アドレスが含まれます。デフォルトでは、ヘッダーの名前は x-forwarded-for です。
- ステップ 6** 変更内容を送信し、確定します。

Web UI セッション タイムアウトの設定

非アクティブな状態によりログアウトになるまで、電子メール セキュリティ アプライアンスの Web UI にログイン可能な期間を指定できます。この Web UI セッション タイムアウトは、admin を含めて、すべてのユーザに適用され、また HTTP セッションと HTTPS セッションの両方に使用されます。

AsyncOS によってユーザがログアウトされると、アプライアンスはユーザの Web ブラウザをログイン ページにリダイレクトします。



(注) Web UI セッション タイムアウトは Cisco スпам隔離セッションには適用されません。このセッションには 30 分のタイムアウトが設定されており、変更できません。

手順

- ステップ 1** [システム管理 (System Administration)] > [Network Access (ネットワーク アクセス)] を選択します。
- ステップ 2** [設定を編集 (Edit Settings)] をクリックします。
- ステップ 3** ログアウトになるまでの非アクティブ時間を分単位で入力します。5 ~ 1440 分のタイムアウト期間を定義できます。
- ステップ 4** 変更内容を送信し、確定します。

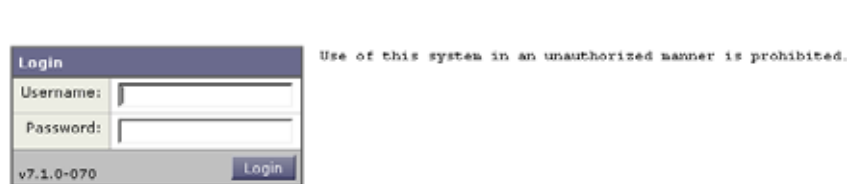
ログイン バナーの追加

ユーザが SSH、Telnet、FTP、または Web UI からログインしようとした際に、「ログイン バナー」と呼ばれるメッセージを表示するように電子メール セキュリティ アプライアンスを設定できます。ログイン バナーは、CLI でログイン プロンプトの上部に表示され、GUI でログイン プロンプトの右側に表示されるカスタマイズ可能なテキストです。ログイン バナーを使用して、内部のセキュリティ情報またはアプライアンスのベスト プラクティスに関する説明を表示できます。たとえば、許可しないアプライアンスの使用を禁止する簡単な注意文言を作成したり、ユーザがアプライアンスに対して行った変更を確認する企業の権利に関する詳細な警告を作成したりできます。

CLI の `adminaccessconfig > banner` コマンドを使用して、ログイン バナーを作成します。ログイン バナーは、80 x 25 のコンソールに収まるように最大 2000 文字になっています。ログイン バナーは、アプライアンスの `/data/pub/configuration` ディレクトリにあるファイルからインポートできます。バナーを作成したら、変更内容を確定します。

図 28-4 は、Web UI ログイン画面に表示されたログイン バナーを示しています。

図 28-4 バナーが表示された Web UI ログイン画面



セキュア シェル (SSH) キーの管理

`sshconfig` コマンドを使用すると、システムで設定されたユーザ アカウント (`admin` アカウントを含む) の `authorized_keys` ファイルに Secure Shell (SSH; セキュア シェル) 公開ユーザ キーを追加したり、それらのキーを削除したりできます。これにより、パスワード チャレンジではなく SSH キーを使用してユーザ アカウントを認証できるようになります。RSA ベース認証と DSA キー タイプを持つ SSH プロトコルバージョン 1 (SSH1) と SSH プロトコルバージョン 2 (SSH2) の両方がサポートされます。SSH1 は `setup` サブコマンドを使用してディセーブルにできます。



(注) Cisco アプライアンスから他のホスト マシンへのログ ファイルの SCP プッシュを実行する場合に使用されるホスト キーを設定するには、`logconfig -> hostkeyconfig` を使用します。詳細については、[第 34 章「ロギング」](#)を参照してください。

`hostkeyconfig` を使用すると、リモート ホストのキーをスキャンし、Cisco アプライアンスに追加できます。



(注) CLI に新しいキーを直接貼り付ける場合は、空白行で `Enter` または `Return` を押してキーの入力を終了します。

次の例では、`admin` アカウントに対して新しい公開キーがインストールされます。

```
mail3.example.com> sshconfig
```

```
Currently installed keys for admin:
```

```
Choose the operation you want to perform:
```

```
- NEW - Add a new key.
```

```
- USER - Switch to a different user to edit.
```

```
- SETUP - Configure general settings.

[ ]> new

Please enter the public SSH key for authorization.

Press enter on a blank line to finish.

[cut and paste public key for user authentication here]

Currently installed keys for admin:

1. ssh-dss AAAAB3NzaC1kc3MAA...CapRrgxcY= (admin@example.com)

Choose the operation you want to perform:

- NEW - Add a new key.
- EDIT - Modify a key.
- DELETE - Remove a key.
- PRINT - Display a key.

[ ]>
```

SSH1 のディセーブル化

SSH1 をディセーブル (またはイネーブル) にするには、`sshconfig` コマンドの `setup` サブコマンドを使用します。

```
mail3.example.com> sshconfig

Currently installed keys for admin:

Choose the operation you want to perform:

- NEW - Add a new key.
- USER - Switch to a different user to edit.
- SETUP - Configure general settings.
```

```
[ ]> setup

Choose the operation you want to perform:

- DISABLE - Disable SSH v1

[ ]> disable

Currently installed keys for admin:

Choose the operation you want to perform:

- NEW - Add a new key.
- USER - Switch to a different user to edit.
- SETUP - Configure general settings

[ ]>

mail3.example.com> commit
```

リモート SSH コマンド実行

CLI では、リモート SSH コマンド実行を使用してコマンドを実行できます。コマンドのリストについては、[Appendix A, “AsyncOS Quick Reference Guide”](#) を参照してください。たとえば、Cisco アプライアンスで `admin` アカウントに対して SSH 公開キーが設定されている場合は、チャレンジされないリモート ホストから次のコマンドを実行できます。

```
# ssh admin@mail3.example.com status

Enter "status detail" for more information.

Status as of: Mon Jan 20 17:24:15 2003

Last counter reset: Mon Jan 20 17:08:21 2003

System status: online

[rest of command deleted]
```




CHAPTER 29

システム管理



(注)

このセクションに記載されている機能またはコマンドには、ルーティングの優先順位に影響を与えるものや、影響を受けるものが含まれています。詳細については、「[IP アドレス、インターフェイス、およびルーティング](#)」(P.B-3)を参照してください。

- 「[Cisco アプライアンスの管理](#)」(P.29-1)
- 「[ライセンス キー](#)」(P.29-5)
- 「[設定ファイルファイルの管理](#)」(P.29-7)
- 「[AsyncOS のアップグレード](#)」(P.29-15)
- 「[アップグレードおよびアップデートをダウンロードするための設定](#)」(P.29-18)
- 「[サービスのアップデート](#)」(P.29-22)
- 「[リモート電源管理のイネーブル化](#)」(P.29-24)
- 「[AsyncOS の以前のバージョンへの復元](#)」(P.29-25)
- 「[アプライアンスに生成されるメッセージの返信アドレスの設定](#)」(P.29-29)
- 「[アラート](#)」(P.29-30)
- 「[ネットワーク設定値の変更](#)」(P.29-52)
- 「[システム時刻](#)」(P.29-57)
- 「[ビューのカスタマイズ](#)」(P.29-59)

Cisco アプライアンスの管理

以下のタスクでは、Cisco アプライアンス内の一般的な機能を簡単に管理できます。次の操作とコマンドについて説明します。

- shutdown
- reboot
- suspend
- offline
- resume
- resetconfig
- version

- updateconfig
- upgrade

Cisco アプライアンスのシャットダウンおよび再起動

アプライアンスをシャットダウンまたは再起動した後は、配信キューにあるメッセージを失うことなく、アプライアンスを後で再起動できます。

この操作は、CLI で shutdown コマンドまたは reboot コマンドを使用して実行できるほか、次のように GUI で実行することもできます。

手順

-
- ステップ 1** [システム管理 (System Administration)] > [シャットダウン/サスペンド (Shutdown/Suspend)] を選択します。
- ステップ 2** [システム オペレーション (System Operations)] セクションで、[操作 (Operation)] ドロップダウンリストから [シャットダウン (Shutdown)] または [再起動 (Reboot)] を選択します。
- ステップ 3** 開いている接続が、強制的に閉じられることなく完了できるまでの許容時間を秒数の単位で入力します。
- デフォルトの遅延値は 30 秒です。
- ステップ 4** [確定する (Commit)] をクリックします。
-

電子メールの受信と配信の一時停止

電子メールの受信と配信を一時停止すると、マシンを再起動した後も一時停止した状態が継続します。CLI で suspend コマンドを使用するか、GUI を使用します。

手順

-
- ステップ 1** [システム管理 (System Administration)] > [シャットダウン/サスペンド (Shutdown/Suspend)] を選択します。
- ステップ 2** [メールの操作 (Mail Operations)] セクションで、一時停止する機能またはリスナーを選択します。
- アプライアンスに複数のリスナーが存在する場合は、リスナー単位で電子メールの受信を停止することもできます。
- ステップ 3** 開いている接続が、強制的に閉じられることなく完了できるまでの許容時間を秒数の単位で入力します。
- 開いている接続が存在しない場合、システムはただちにオフラインになります。
- デフォルトの遅延値は 30 秒です。
- ステップ 4** [確定する (Commit)] をクリックします。
-

次の作業

一時停止したサービスを再開する準備が整っている場合は、「一時停止している電子メールの受信と配信の再開」(P.29-3) を参照してください。

一時停止している電子メールの受信と配信の再開

AsyncOS CLI で `resume` コマンドを実行すると、Cisco AsyncOS オペレーティング システム (`suspenddel` または `suspend` コマンドの使用後) が通常の動作状態に戻ります。

手順

-
- ステップ 1** [システム管理 (System Administration)] > [シャットダウン/サスペンド (Shutdown/Suspend)] を選択します。
 - ステップ 2** [メールの操作 (Mail Operations)] セクションで、再開する機能またはリスナーを選択します。アプライアンスに複数のリスナーが存在する場合は、リスナー単位で電子メールの受信を再開できません。
 - ステップ 3** [確定する (Commit)] をクリックします。
-

CLI を使用したアプライアンスのオフライン化

シスコのサポートからそのように指示された場合、Cisco IronPort AsyncOS をオフライン状態にします。

システムがオフラインの場合：

- 着信電子メール接続は受け入れられません。
- 発信電子メール配信は停止されます。
- ログ転送が停止されます。
- CLI はアクセス可能のままになります。

手順

-
- ステップ 1** `offline` コマンドを使用します。
 - ステップ 2** 開いている接続を強制的に閉じるまでに待機する秒数を指定します。
-

出荷時の初期状態へのリセット

アプライアンスを物理的に移動する際、出荷時の初期状態で始めなければならない場合があります。[システム管理 (System Administration)] > [設定ファイル (Configuration File)] ページの [設定情報のリセット (Reset Configuration)] セクションまたは `resetconfig` コマンドを使用すると、すべての Cisco AsyncOS の設定値が出荷時デフォルト値にリセットされます。このコマンドを実行すると元に

戻せないため、ユニットを移動する場合や、設定の問題を解決する最後の手段としてのみ使用してください。設定のリセット後にシステム セットアップ ウィザードまたは `systemsetup` コマンドを実行することを推奨します。



(注)

`resetconfig` コマンドは、アプライアンスがオフライン状態にあるときにのみ動作します。`resetconfig` コマンドが完了すると、`systemsetup` コマンドを再び実行する前であってもアプライアンスがオンライン状態に戻ります。ただし、メール配信は再開されないため、メール配信に戻ってオンにする必要があります。



警告

`resetconfig` コマンドを実行すると、すべてのネットワーク設定が出荷時デフォルト値に戻ります。場合によっては、CLI から切断され、アプライアンスに接続するために使用したサービス (FTP、Telnet、SSH、HTTP、HTTPS) がディセーブルにされ、`userconfig` コマンドで作成した追加のユーザアカウントが削除されます。このコマンドは、シリアル インターフェイスを使用するか、またはデフォルトの Admin ユーザアカウントから管理ポート上のデフォルト設定を使用して CLI に再接続できない場合は使用しないでください。

resetconfig コマンド

```
mail3.example.com> offline

Delay (seconds, minimum 30):

[30]> 45

Waiting for listeners to exit...

Receiving suspended.

Waiting for outgoing deliveries to finish...

Mail delivery suspended.

mail3.example.com> resetconfig

Are you sure you want to reset all configuration values? [N]> Y

All settings have been restored to the factory default.
```

AsyncOS のバージョン情報の表示

Cisco アプライアンスに現在インストールされている AsyncOS のバージョンを確認するには、GUI の [モニタ (Monitor)] メニューから [システム概要 (System Overview)] ページを使用するか (「システムステータス (System Status)」(P.26-40) を参照)、CLI で `version` コマンドを使用します。

ライセンス キー

ライセンス キーの追加および管理

ライセンス キーは物理アプライアンスのシリアル番号とイネーブルにされる機能に固有です (あるシステムのキーを別のシステムで再使用することはできません)。



(注)

電子メール セキュリティ仮想アプライアンスのライセンス キーは仮想アプライアンスのライセンス ファイルに含まれ、個別にインストールできません。詳細については、「Cisco 電子メール セキュリティ仮想アプライアンスのライセンス」(P.29-6) を参照してください。

CLI のライセンス キーを使用するには、`featurekey` コマンドを使用します。

手順

- ステップ 1** [システム管理 (System Administration)] > [ライセンス キー (Feature Keys)] を選択します。
- ステップ 2** アクションの実行 :

目的	操作内容
実行中のライセンス キーのステータスを表示します	[シリアル番号 <serial number> のライセンス キー (Feature Keys for <serial number>)] セクションを確認します。
アプライアンスに対して発行されていて、まだアクティベーションされていないライセンス キーを表示します	[保留中のライセンス (Pending Activation)] セクションを確認します。 自動ダウンロードおよびアクティベーションを有効にしている場合は、ライセンス キーはこのリストには表示されません。
最近発行されたライセンスキーを確認する	[保留中のライセンス (Pending Activation)] セクションで、[新しいキーをチェック (Check for New Keys)] ボタンをクリックします。 これはライセンス キーの自動ダウンロードおよびアクティベーションを有効にしていない場合、または次の自動チェックの前にライセンス キーをダウンロードする必要がある場合に役立ちます。
発行されたライセンス キーをアクティブ化します	[保留中のライセンス (Pending Activation)] リストで、[選択したキーを有効化 (Activate Selected Keys)] をクリックします。

目的	操作内容
新しいライセンス キーを追加します	[機能の有効化 (Feature Activation)] セクションを使用します。

関連項目

- 「ライセンス キーのダウンロードとアクティベーションの自動化」 (P.29-6)

ライセンス キーのダウンロードとアクティベーションの自動化

このアプライアンスに対して発行されたライセンス キーを自動的にチェック、ダウンロードおよびアクティブ化するようアプライアンスを設定できます。

手順

- ステップ 1** [システム管理 (System Administration)] > [ライセンス キーの設定 (Feature Key Settings)] を選択します。
- ステップ 2** [ライセンス キー設定の編集 (Edit Feature Key Settings)] をクリックします。
- ステップ 3** 新しいライセンス キーのチェック頻度を確認するには、(?) ヘルプ ボタンをクリックしてください。
- ステップ 4** 設定事項を指定します。
- ステップ 5** 変更内容を送信し、確定します。

関連項目

- 「ライセンス キーの追加および管理」 (P.29-5)

期限切れライセンス キー

(GUI から) アクセスしようとしている機能のライセンス キーの有効期限が切れている場合は、Cisco の担当者またはサポート組織までご連絡ください。

Cisco 電子メール セキュリティ仮想アプライアンスのライセンス

Cisco 電子メール セキュリティ仮想アプライアンスは、ホスト上で仮想アプライアンスを実行するための追加ライセンスが必要です。このライセンスは複数のクローニングされた仮想アプライアンスに対して使用できます。

このライセンスをインストールするには、loadlicense CLI コマンドを実行します。CLI にライセンスをコピー アンド ペーストするか、コマンドを実行する前に FTP を使用してアプライアンスの configuration ディレクトリにアップロードします。ライセンスはシステム セットアップ ウィザードを実行する前に、アプライアンスにインストールされている必要があります。

ライセンス キーは仮想アプライアンスのライセンスに含まれています。ライセンス キーは、キーがまだアクティベートされていなくても、ライセンスと同時に失効します。新しいライセンス キーを購入すると、新しい仮想アプライアンスのライセンスをダウンロードおよびインストールする必要があります。

仮想アプライアンスのライセンスにライセンス キーが含まれているため、シスコのスパム対策またはアウトブレイク フィルタなどの AsyncOS 機能の 30 日間評価はありません。



(注) 仮想アプライアンスのライセンスをインストールする前に、テクニカル サポートは利用できません。

電子メール セキュリティ仮想アプライアンスの設定および実行の詳細については、『Cisco Content Security Virtual Appliance Installation Guide』を参照してください。

設定ファイルファイルの管理

Cisco アプライアンス内のすべての設定は、1 つの設定ファイルで管理できます。このファイルは Extensible Markup Language (XML) 形式で保持されます。

このファイルは次の複数の方法で使用できます。

- 設定ファイルを別のシステムに保存し、重要な設定データをバックアップおよび保持できます。アプライアンスの設定を間違えた場合、保存した最新の設定ファイルにロールバックできます。
- 既存の設定ファイルをダウンロードし、アプライアンスの全体の設定を簡単に確認できます (多くの新しいブラウザは XML ファイルを直接レンダリングできます)。これにより、現在の設定に存在する可能性がある小さなエラー (タイピング エラーなど) をトラブルシューティングできます。
- 既存の設定ファイルをダウンロードし、変更を行い、そのファイルを同じアプライアンスにアップロードできます。この場合は、実質的に設定の変更を行うために CLI と GUI の両方が「バイパス」されます。
- FTP アクセスを使用して設定ファイル全体をアップロードしたり、設定ファイルの一部または全体を CLI に直接貼り付けたりできます。
- ファイルは XML 形式であるため、設定ファイルのすべての XML エンティティを定義する、関連付けられた Document Type Definition (DTD) も提供されます。XML 設定ファイルをアップロードする前にこの DTD をダウンロードして XML 設定ファイルを検証できます (XML 検証ツールはインターネットで簡単に入手できます)。

XML 設定ファイルを使用した複数のアプライアンスの管理

- ある Cisco アプライアンスから既存の設定ファイルをダウンロードし、変更を行い、別のアプライアンスにアップロードできます。これにより、複数の Cisco アプライアンスのインストールを簡単に管理できるようになります。現時点では、設定ファイルを C/X シリーズ アプライアンスから M シリーズ アプライアンスにロードできません。
- ある Cisco からダウンロードされた既存の設定ファイルを複数のサブセクションに分割できます。(複数のアプライアンス環境の) すべてのアプライアンスで共通するこれらのセクションを変更し、サブセクションの更新時にこれらのセクションを他のアプライアンスにロードできます。

たとえば、Global Unsubscribe コマンドをテストするためにテスト環境でアプライアンスを使用できます。グローバル配信停止リストを適切に設定した場合は、テスト アプライアンスのグローバル配信停止設定セクションをすべての実稼働アプライアンスにロードできます。

GUI を使用した設定ファイルの管理

GUI を使用して Cisco アプライアンスの設定ファイルを管理するには、[システム管理 (System Administration)] タブの [設定ファイル (Configuration File)] リンクをクリックします。

[設定ファイル (Configuration File)] ページには次の 3 つのセクションがあります。

- [現在の設定 (Current Configuration)] : 現在の設定ファイル ファイル保存およびエクスポートするために使用します。
- [設定をロード (Load Configuration)] : 設定ファイル全体または一部をロードするために使用します。
- [設定情報のリセット (Reset Configuration)] : 現在の設定を出荷時デフォルト値にリセットするために使用します (リセット前に設定を保存する必要があります)。

現在の設定ファイルの保存およびエクスポート

[システム管理 (System Administration)] > [設定ファイル (Configuration File)] ページの [現在の設定 (Current Configuration)] のセクションを使用すると、現在の設定ファイルを、ローカルマシンに保存したり、アプライアンスで保存したり (FTP/SCP ルートの configuration ディレクトリに保存されます)、指定されたアドレスに電子メールで送信したりできます。

チェックボックスをクリックすることにより、ユーザのパスワードをマスクできます。パスワードをマスクすると、元の暗号化されたパスワードが、エクスポートまたは保存されたファイルで「*****」に置き換えられます。ただし、パスワードがマスクされた設定ファイルを AsyncOS に再びロードすることはできないことに注意してください。

設定ファイルのロード

[システム管理 (System Administration)] > [設定ファイル (Configuration File)] ページの [設定をロード (Load Configuration)] のセクションを使用して新しい設定情報を Cisco アプライアンスにロードします。情報は次の 3 つのいずれかの方法でロードできます。

- configuration ディレクトリに情報を格納し、アップロードする。
- 設定ファイルをローカルマシンから直接アップロードする。
- GUI に設定情報を直接貼り付ける。

パスワードがマスクされた設定ファイルはロードできません。

どの方法の場合でも、設定の上部に次のタグを含める必要があります。

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<config>
  ... your configuration information in valid XML
</config>
```


</config> 閉じタグは設定情報の後に指定する必要があります。XML 構文の値は、Cisco アプライアンスの configuration ディレクトリにある DTD (Document Type Definition) を使用して解析および検証されます。DTD ファイルの名前は config.dtd です。loadconfig コマンドを使用したときにコマンドラインで検証エラーが報告された場合、変更はロードされません。設定ファイルをアップロードする前に、アプライアンスの外部で DTD をダウンロードし、設定ファイルを検証できます。

いずれの方法の場合でも、設定ファイル全体 (最上位のタグである <config></config> 間で定義された情報) または設定ファイルの *complete* および *unique* サブセクション (上記の宣言タグが含まれ、<config></config> タグ内に存在する場合) をインポートできます。

「complete (完全)」とは、DTD で定義されたサブセクションの開始タグおよび終了タグ全体が含まれることを意味します。たとえば、次の内容をアップロードまたは解析します。

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<config>
  <autosupport_enabled>0</autosu
</config>
```

この場合は、アップロード中に検証エラーが発生します。ただし、

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<config>
  <autosupport_enabled>0</autosupport_enabled>
</config>
```

この場合は、検証エラーが発生しません。

「unique (一意)」とは、アップロードまたは貼り付けられる設定ファイルのサブセクションが、設定として多義的でないことを意味します。たとえば、システムは 1 つのホスト名しか持つことができないため、次の内容 (宣言と <config></config> タグを含む) をアップロードすることは可能です。

```
<hostname>mail4.example.com</hostname>
```

ただし、システムでは複数のリスナーを定義できるため (リスナーごとに異なる受信者アクセステーブルが定義されます)、

```
<rat>
  <rat_entry>
    <rat_address>ALL</rat_address>
    <access>RELAY</access>
```

```

    </rat_entry>

</rat>

```

上記の内容だけをアップロードすることは多義的と見なされ、「完全」な構文であっても許可されません。

**警告**

設定ファイルまたは設定ファイルのサブセクションをアップロードまたは解析する場合は、待機中の可能性がある、保存されていない変更が破棄されることがあります。

空白タグと 省略されたタグ

設定ファイルのセクションをアップロードまたは解析する場合は注意が必要です。タグを含めないと、設定ファイルのアップロード時に設定の値が変更されません。ただし、空白タグを含めると、設定の問題が解消されます。

たとえば、

```
<listeners></listeners>
```

上記の内容をアップロードすると、システムからすべてのリスナーが削除されます。

**警告**

設定ファイルのサブセクションをアップロードしたり、貼り付けたりした場合、GUI または CLI から切断され、大量の設定データが破壊されることがあります。管理ポートで別のプロトコル、シリアルインターフェイス、またはデフォルト設定を使用してアプライアンスに再接続できない場合は、このコマンドでサービスをディセーブルにしないでください。また、DTD で定義された設定構文がよくわからない場合は、このコマンドを使用しないでください。新しい設定ファイルをアップロードする前に、必ず設定データをバックアップしてください。

ログ サブスクリプションのパスワードのロードについての注意事項

パスワードが必要なログ サブスクリプションを含む設定ファイルをロードしようとしても（たとえば、FTP プッシュを使用）、loadconfig コマンドは不明なパスワードについて警告しません。FTP プッシュが失敗し、logconfig コマンドを使用して正しいパスワードを設定するまで警告が生成されます。

文字セット エンコーディングについての注意事項

XML 設定ファイルの「encoding」属性は、ファイルをオフラインで操作するために使用している文字セットに関係なく、「ISO-8859-1」である必要があります。showconfig コマンド、saveconfig コマンド、または mailconfig コマンドを発行するたびにエンコーディング属性がファイルで指定されることに注意してください。

```
<?xml version="1.0" encoding="ISO-8859-1"?>
```

現時点では、このエンコーディングを持つ設定ファイルだけをロードできます。

現在の設定のリセット

現在の設定をリセットすると、Cisco アプライアンスが元の出荷時デフォルト値に戻ります。リセットする前に設定を保存する必要があります。GUI でこのボタンを使用して設定をリセットすることは、クラスタリング環境ではサポートされていません。

「出荷時の初期状態へのリセット」(P.29-3) を参照してください。

設定ファイル用の CLI コマンド

次のコマンドを使用すると、設定ファイルを操作できます。

- showconfig
- mailconfig
- saveconfig
- loadconfig
- resetconfig (「出荷時の初期状態へのリセット」(P.29-3) を参照)

showconfig、mailconfig、および saveconfig コマンド

コンフィギュレーション コマンドの showconfig、mailconfig、および saveconfig の場合は、電子メールで送信されるファイルまたは表示されるファイルにパスワードを含めるかどうかを選択することを求められます。パスワードを含めないことを選択すると、パスワードフィールドが空白のままになります。セキュリティの問題を心配する場合は、パスワードを含めないことを選択できます。ただし、loadconfig コマンドを使用してロードされた場合、パスワードがない設定ファイルは失敗します。「ログ サブスクリプションのパスワードのロードについての注意事項」(P.29-10) を参照してください。



(注) パスワードを含めることを選択した場合 (「Do you want to include passwords?」に「yes」と回答します) に設定ファイルを保存、表示、または電子メールで送信するとき、パスワードは暗号化されます。ただし、秘密キーと証明書は暗号化されない PEM 形式で含められます。

Showconfig コマンドは、現在の設定を画面に出力します。

```
mail3.example.com> showconfig
```

```
Do you want to include passwords? Please be aware that a configuration without passwords will fail when reloaded with loadconfig.
```

```
<?xml version="1.0" encoding="ISO-8859-1"?>
```

```
<!DOCTYPE config SYSTEM "config.dtd">
```

```
<!--
```

```
Product: IronPort model number Messaging Gateway Appliance(tm)
```

```
Model Number: model number

Version: version of AsyncOS installed

Serial Number: serial number

Current Time: current time and date
```

[The remainder of the configuration file is printed to the screen.]

mailconfig コマンドを使用して、現在の設定をユーザに電子メールで送信します。メッセージには config.xml という名前の XML 形式の設定ファイルが添付されます。

```
mail3.example.com> mailconfig
```

```
Please enter the email address to which you want to send
the configuration file.
```

```
[> administrator@example.com
```

```
Do you want to include passwords? Please be aware that a configuration without passwords
will fail when reloaded with loadconfig. [N]> y
```

```
The configuration file has been sent to administrator@example.com.
```

saveconfig コマンドは、一意のファイル名を使用して設定ファイルをアプライアンスの configuration ディレクトリに保存します。

```
mail3.example.com> saveconfig
```

```
Do you want to include passwords? Please be aware that a configuration without passwords
will fail when reloaded with loadconfig. [N]> y
```

```
File written on machine "mail3.example.com" to the location
"/configuration/C360-420E874BB4B3C41C5C71-1419B58528A0-20120105T214041.xml".
Configuration saved.
```

```
mail3.example.com>
```

loadconfig コマンド

Cisco アプライアンスに新しい設定情報をロードするには `loadconfig` を使用します。情報は次の 2 つのいずれかの方法でロードできます。

- `configuration` ディレクトリに情報を格納し、アップロードする。
- CLI に設定情報を直接貼り付ける。

詳細については、「[設定ファイルのロード](#)」(P.29-8) を参照してください。

CLI を使用した設定変更のアップロード

手順

-
- ステップ 1** CLI の外部で、アプライアンスの `configuration` ディレクトリにアクセスできることを確認します。詳細については、[付録 A 「アプライアンスへのアクセス」](#) を参照してください。
- ステップ 2** 設定ファイル全体または設定ファイルのサブセクションをアプライアンスの `configuration` ディレクトリに格納するか、`saveconfig` コマンドで作成した既存の設定を編集します。
- ステップ 3** CLI 内で、`loadconfig` コマンドを使用して、ステップ 2 で示されたディレクトリに格納した設定ファイルをロードするか、テキスト (XML 構文) を CLI に直接貼り付けます。
-

この例では、`changed.config.xml` という名前のファイルがアップロードされ、変更が保存されます。

```
mail3.example.com> loadconfig
```

```
1. Paste via CLI
2. Load from file
```

```
[1]> 2
```

```
Enter the name of the file to import:
```

```
[1]> changed.config.xml
```

```
Values have been loaded.
```

```
Be sure to run "commit" to make these settings active.
```

```
mail3.example.com> commit
```

この例では、新しい設定ファイルをコマンドラインに直接貼り付けます（空白行で Ctrl+D を押すと貼り付けコマンドが終了します）。次に、システム設定ウィザードを使用して、デフォルトのホスト名、IP アドレス、およびデフォルトのゲートウェイ情報を変更します（詳細は、「[システム セットアップ ウィザードの使用方法](#)」(P.3-12) を参照してください)。これで、変更が確定されます。

```
mail3.example.com> loadconfig
```

1. Paste via CLI
2. Load from file

```
[1]> 1
```

Paste the configuration file now. Press CTRL-D on a blank line when done.

[The configuration file is pasted until the end tag </config>. Control-D is entered on a separate line.]

Values have been loaded.

Be sure to run "commit" to make these settings active.

```
mail3.example.com> systemsetup
```

[The system setup wizard is run.]

```
mail3.example.com> commit
```

Please enter some comments describing your changes:

```
[ ]> pasted new configuration file and changed default settings via  
systemsetup
```

AsyncOS のアップグレード

	目的	参照先
ステップ1	アップグレード設定値を設定します。電子メールセキュリティ アプライアンスがアップグレード情報をダウンロードする方法に関する設定値を設定します。たとえば、アップグレードイメージをダウンロードする場所を選択できます。これらのダウンロード用にネットワークも設定する必要があります。	「アップグレードおよびアップデートをダウンロードするためのサーバ設定」(P.29-22)
ステップ2	AsyncOS をアップグレードします。アップグレード設定値を設定した後は、アプライアンスの AsyncOS のバージョンをアップグレードします。	「GUI からの AsyncOS のアップグレード」(P.29-15)



(注) アップグレード手順用のバッチ コマンドは、http://www.cisco.com/en/US/products/ps10154/prod_command_reference_list.html 『Cisco AsyncOS CLI Reference Guide』に記載されています。

AsyncOS のアップグレードの準備

ベスト プラクティスとして、次の手順を実行したアップグレードの準備を推奨します。

手順

- ステップ 1 XML コンフィグ ファイルのオフボックスを保存します。
- ステップ 2 セーフリスト/ブロックリスト機能を使用している場合、リストのオフボックスをエクスポートします。
- ステップ 3 すべてのリスナーを一時停止します。CLI からのアップグレードを実行する場合は、suspendlistener コマンドを使用します。GUI からのアップグレードを実行する場合は、リスナーの停止が自動的に実行されます。
- ステップ 4 キューが空になるまで待ちます。CLI の workqueue コマンドでワークキュー内のメッセージ数を表示するか、rate コマンドでアプライアンスのメッセージスループットをモニタすることができます。



(注) アップグレード後、再びリスナーをイネーブルにします。

GUI からの AsyncOS のアップグレード

アップグレードのダウンロードとインストール

1 回の操作でダウンロードとインストールを行うか、またはバックグラウンドでダウンロードして後でインストールできます。



(注) AsyncOS を Cisco IronPort AsyncOS からではなくローカル サーバから 1 回の操作でダウンロードとアップグレードする場合は、アップグレードはダウンロード中に即座に実行されます。アップグレードプロセスの開始時に、バナーが 10 秒間表示されます。このバナーが表示されている間は、Ctrl を押した状態で C を押すと、ダウンロードの開始前にアップグレードプロセスを終了できません。

はじめる前に

- シスコから直接アップグレードをダウンロードするか、またはネットワーク上のサーバからアップグレードイメージをホストするかを選択します。次に、選択した方式をサポートするようにネットワークをセットアップします。そして、選択した入手先からアップグレードを入手するためにアプライアンスを設定します。「[アップグレードおよびアップデートをダウンロードするための設定](#)」(P.29-18) および「[アップグレードおよびアップデートをダウンロードするためのサーバ設定](#)」(P.29-22) を参照してください。
- ここで、アップグレードをインストールする場合は、「[AsyncOS のアップグレードの準備](#)」(P.29-15) の手順を実行します。
- クラスタ化されたシステムのアップグレードをインストールする場合は、「[クラスタ内のマシンのアップグレード](#)」(P.35-13) を参照してください。
- アップグレードをダウンロードするだけの場合、インストールの準備が完了するまでの前提条件はありません。

手順

- ステップ 1** [システム管理 (System Administration)] > [システム アップグレード (System Upgrade)] を選択します。
- ステップ 2** [アップグレード オプション (Upgrade Options)] をクリックします。
- ステップ 3** 次のオプションを選択します。

目的	操作内容
1 回の操作でアップグレードのダウンロードとインストールを実行する	[ダウンロードしてインストール (Download and Install)] をクリックします。 すでにインストーラをダウンロードしたことがある場合、既存のダウンロードを上書きするよう求められます。
アップグレード インストーラをダウンロードします。	[ダウンロードのみ (Download only)] をクリックします。 すでにインストーラをダウンロードしたことがある場合、既存のダウンロードを上書きするよう求められます。 インストーラはサービスを中断することなく、バックグラウンドでダウンロードします。
ダウンロードしたアップグレード インストーラのインストール	[インストール (Install)] をクリックします。 このオプションは、インストーラがダウンロードされている場合にのみ表示されます。 インストールする AsyncOS のバージョンは、[インストール (Install)] オプションの下に表示されます。

ステップ 4 以前にダウンロードしたインストーラでインストールする場合を除き、利用可能なアップグレードのリストから AsyncOS のバージョンを選択します。

ステップ 5 インストール中の場合、次に従います。

- a. 現在の設定をアプライアンス上の configuration ディレクトリに保存するかどうかを選択します。
- b. 設定ファイルでパスワードをマスクするかどうかを選択します。



(注) マスクされたパスワードが記載された設定ファイルは、GUI の [設定ファイル (Configuration File)] ページや CLI の loadconfig コマンドからロードできません。

- c. 設定ファイルのコピーを電子メールで送信する場合は、ファイルを送信する電子メールアドレスを入力します。複数の電子メール アドレスを指定する場合は、カンマで区切ります。

ステップ 6 [続行 (Proceed)] をクリックします。

ステップ 7 インストール中の場合、次に従います。

- a. プロセス中のプロンプトに答える準備をしてください。
応答するまでプロセスは中断されます。
ページの上部の近くに、経過表示バーが表示されます。
- b. プロンプトで、[今すぐ再起動 (Reboot Now)] をクリックします。
- c. 約 10 分後、アプライアンスにアクセスしてログインします。
アップグレードの問題を修正するためにアプライアンスの電源を再投入する必要があると思われる場合は、再起動後 20 分以上が経過してから再投入してください。

次の作業

- プロセスが中断された場合、プロセスを再開する必要があります。
- アップグレードをダウンロードしてインストールしなかった場合は次のとおりです。
アップグレードをインストールする準備ができたなら、「始める前に」の項の前提条件も含め次の手順を最初から実行しますが、[インストール (Install)] オプションを選択します。
- アップグレードをインストールした場合、次のとおりです。
 - リスナーを再びイネーブル (再開) にします。
 - 新しいシステムの設定ファイルを保存します。詳細については、「[設定ファイルファイルの管理](#)」(P.29-7) を参照してください。
- アップグレードが完了したら、再びリスナーをイネーブルにします。

バックグラウンド ダウンロードのキャンセルまたは削除ステータスの表示

手順

ステップ 1 [システム管理 (System Administration)] > [システム アップグレード (System Upgrade)] を選択します。

ステップ 2 [アップグレード オプション (Upgrade Options)] をクリックします。

ステップ 3 次のオプションを選択します。

目的	操作内容
ダウンロード ステータスの表示	ページの真ん中を確認してください。 進行中のダウンロードおよびダウンロードが完了してインストールされるのを待っているものがない場合は、ダウンロードのステータス情報は表示されません。
ダウンロードのキャンセル	ページの中央にある、[ダウンロードをキャンセル (Cancel Download)] ボタンをクリックします。 このオプションは、ダウンロード進行中にのみ表示されます。
ダウンロードされたインストーラの削除	ページの中央にある、[ファイルを削除 (Delete File)] ボタンをクリックします。 このオプションは、インストーラがダウンロードされている場合にのみ表示されます。

ステップ 4 (任意) アップグレード ログを確認します。

アップグレードおよびアップデートをダウンロードするための設定

電子メール セキュリティ アプライアンスが AsyncOS アップグレードおよびアップデートダウンロードする方法を設定します。Cisco では、ストリーミングおよびリモートの 2 つのアップグレードおよびアップデート方法 (または「ソース」) を用意しています。

ストリーミング アップグレードおよびアップデートでは、Cisco アプライアンスは直接 Cisco アップデート サーバからファイルをダウンロードします。各 Cisco アプライアンスは、個別にファイルをダウンロードします。詳細については、「[Cisco IronPort サーバからのアップグレードおよびアップデートのダウンロード](#)」(P.29-19) を参照してください。

リモート アップグレードおよびアップデートでは、Cisco アプライアンスはネットワーク内のサーバからファイルをダウンロードします。Cisco から 1 回だけファイルをダウンロードし、Cisco アプライアンスに供給します。詳細については、「[ローカル サーバからのアップグレードおよびアップデート](#)」(P.29-20) を参照してください。

[セキュリティ サービス (Security Services)] > [サービスのアップデート (Service Updates)] ページを使用して、これらのプロセスのためにシステムを設定し、アップグレードおよびアップデート方法を選択します (デフォルトはストリーミングです)。詳細については、「[アップグレードおよびアップデートをダウンロードするためのサーバ設定](#)」(P.29-22) を参照してください。オプションで、CLI の updateconfig コマンドを使用することもできます。

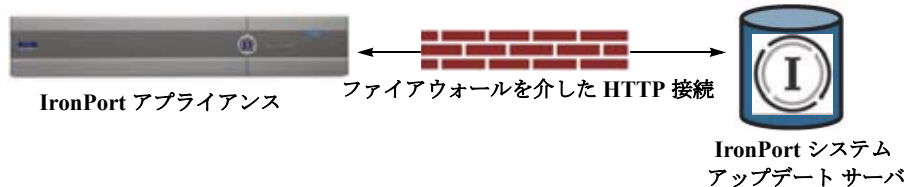
クラスタ化されたシステムのアップグレード

クラスタ化されたマシンをアップグレードする場合は、「[クラスタ内のマシンのアップグレード](#)」(P.35-13) を参照してください。

Cisco IronPort サーバからのアップグレードおよびアップデートのダウンロード

Cisco アプライアンスは、アップグレードおよびアップデートを検索するために、Cisco アップデートサーバに直接接続できます。

図 29-1 ストリーミングアップデートの方法



Cisco Systems では分散サーバアーキテクチャを使用して、世界中のお客様が AsyncOS アップグレードおよびサービスアップデートをすぐにダウンロードできるようにしています。この分散サーバアーキテクチャにより、Cisco アップデートサーバはダイナミック IP アドレスを使用します。厳密なファイアウォールポリシーがある場合は、代わりに静的な場所の設定が必要になることがあります。詳細については、「[厳密なファイアウォール環境でアップグレードとアップデートを受信するためのアプライアンスの設定](#)」(P.29-19) を参照してください。

ダウンロードのためのネットワークの設定

ポート 80 および 443 による Cisco アップデートサーバからのアップグレードのダウンロードを許可する、ファイアウォールのルールを作成する必要があります。

厳密なファイアウォール環境でアップグレードとアップデートを受信するためのアプライアンスの設定

Cisco IronPort アップグレードおよびアップデートサーバは、ダイナミック IP アドレスを使用します。ファイアウォールポリシーを厳しく設定している場合、アップデートおよび AsyncOS アップグレードに対して静的な参照先を設定する必要がある場合があります。

手順

- ステップ 1** Cisco カスタマーサポートに問い合わせ、スタティック URL アドレスを取得します。
- ステップ 2** ポート 80 によるスタティック IP アドレスからのアップグレードおよびアップデートのダウンロードを許可する、ファイアウォールのルールを作成します。
- ステップ 3** [セキュリティ サービス (Security Services)] > [サービスのアップデート (Service Updates)] を選択します。
- ステップ 4** [アップデート設定を編集 (Edit Update Settings)] をクリックします。
- ステップ 5** [アップデート設定を編集 (Edit Update Settings)] ページの [アップデートサーバ (イメージ) (Update Servers (images))] セクションで、[ローカルアップデートサーバ (Local Update Servers)] を選択し、ステップ 1 で受け取った AsyncOS アップグレードおよび McAfee Anti-Virus 定義ファイルのスタティック URL を [ベース URL (Base URL)] フィールドに入力します。
- ステップ 6** IronPort アップデートサーバが [アップデートサーバ (リスト) (Update Servers (list))] セクションで選択されていることを確認します。

ステップ 7 変更内容を送信し、確定します。

ローカル サーバからのアップグレードおよびアップデート

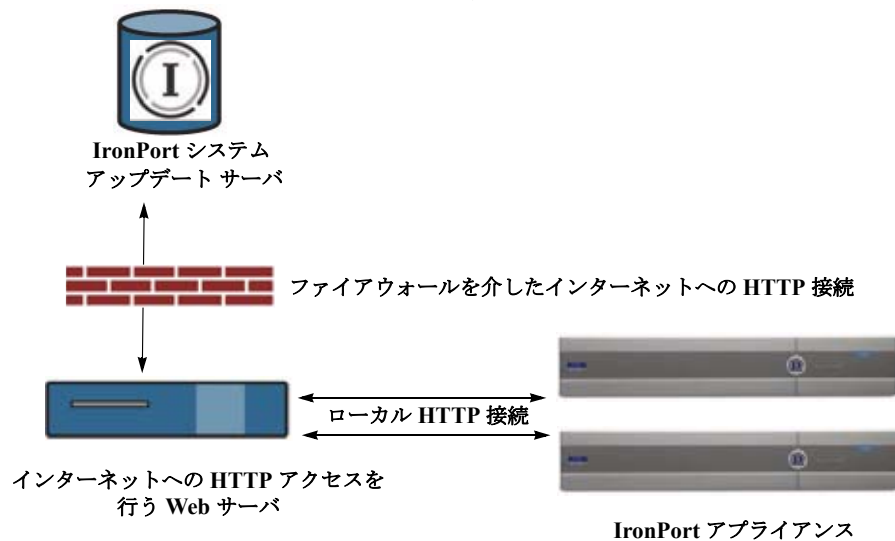
直接 Cisco アップデート サーバからアップグレードを取得するのではなく、AsyncOS アップグレード イメージをローカル サーバにダウンロードし、所有するネットワーク内からアップグレードをホスティングできます。この機能を使用して、インターネットにアクセスできるネットワーク上のすべてのサーバに HTTP でアップグレード イメージをダウンロードします。アップデート イメージをダウンロードする場合は、内部 HTTP サーバ（アップデート マネージャ）を設定し、Cisco アプライアンスで AsyncOS イメージをホスティングすることができます。

アプライアンスがインターネットにアクセスできない場合や、ダウンロードに使用するミラー サイトへのアクセスが組織で制限される場合はローカル サーバを使用します。ローカル サーバから各アプライアンスへの AsyncOS アップグレードのダウンロードは、通常 Cisco IronPort サーバからのダウンロードよりも高速です。



(注) AsyncOS アップグレードに限りローカル サーバを使用することを推奨します。セキュリティアップデート イメージにローカル アップデート サーバを使用する場合、ローカル サーバは Cisco IronPort から自動的にセキュリティ アップデートを受信しないため、ネットワーク上のアプライアンスは常に最新のセキュリティ サービスであるわけではない可能性があります。

図 29-2 リモート アップデートの方法



手順

- ステップ 1 アップグレード ファイルを取得および供給するようにローカル サーバを設定します。
- ステップ 2 アップグレード ファイルをダウンロードします。
- ステップ 3 GUI の [セキュリティ サービス (Security Services)] > [サービスのアップデート (Service Updates)] ページまたは CLI の `updateconfig` コマンドのいずれかを使用して、ローカル サーバを使用するようにアプライアンスを設定します。

ステップ 4 [システム管理 (System Administration)] > [システム アップグレード (System Upgrade)] ページまたは CLI の upgrade コマンドのいずれかを使用して、アプライアンスをアップグレードします。

ローカル サーバからアップグレードするためのハードウェアおよびソフトウェア要件

AsyncOS アップグレード ファイルのダウンロードでは、次の要件を備えた内部ネットワークにシステムを構築する必要があります。

- Cisco Systems アップデート サーバへのインターネット アクセス。
- Web ブラウザ ([「ブラウザ要件」 \(P.2-1\)](#) を参照)。



(注)

今回のリリースでアップデート サーバのアドレスへの HTTP アクセスを許可するファイアウォール設定値を設定する必要がある場合、特定の IP アドレスではなく DNS 名を使用する必要があります。

AsyncOS アップデート ファイルのホスティングでは、次の要件を備えた内部ネットワークにサーバを構築する必要があります。

- Web サーバ : たとえば、Microsoft Internet Information Services (IIS; インターネット インフォメーション サービス) または Apache オープン ソース サーバでは、次の要件を満たしている必要があります。
 - 24 文字を超えるディレクトリまたはファイル名の表示をサポートしていること
 - ディレクトリの参照ができること
 - 匿名認証 (認証不要) または基本 (「シンプル」) 認証の設定ができること
 - 各 AsyncOS アップデート イメージ用に最低 350 MB 以上の空きディスク領域が存在すること

ローカル サーバでのアップグレード イメージのホスト

ローカル サーバの設定が完了したら、http://updates.ironport.com/fetch_manifest.html にアクセスしてアップグレード イメージの ZIP ファイルをダウンロードします。イメージをダウンロードするには、(物理アプライアンスの) シリアル番号または (仮想アプライアンスの) VLN および Cisco アプライアンスのバージョン番号を入力します。利用可能なアップグレードのリストが表示されます。ダウンロードするアップグレードのバージョンをクリックし、ディレクトリ構造を変更せずにローカル サーバのルート ディレクトリにある ZIP ファイルを解凍します。アップグレード イメージを使用するには、[アップデート設定を編集 (Edit Update Settings)] ページで (または CLI の updateconfig を使用して) ローカル サーバを使用するようにアプライアンスを設定します。

ローカル サーバは、ネットワーク上の Cisco アプライアンスで利用可能な AsyncOS アップグレードをダウンロード済みのアップグレード イメージに限定する XML ファイルもホスティングします。このファイルは「マニフェスト」と呼ばれます。マニフェストはアップグレード イメージの ZIP ファイルの asyncos ディレクトリに配置されています。ローカル サーバのルート ディレクトリにある ZIP ファイルを解凍したら、[アップデート設定を編集 (Edit Update Settings)] ページで (または CLI の updateconfig を使用して)、XML ファイルの完全な URL (ファイル名を含む) を入力します。

リモート アップグレードの詳細については、Cisco ナレッジ ベースを参照するか、Cisco サポート プロバイダーにお問い合わせください。

サービスのアップデート

次のサービスは最大の効果得るために更新する必要があります。

- ライセンスキー
- McAfee Anti-Virus の定義
- PXE エンジン
- Sophos Anti-Virus の定義
- IronPort アンチ スпам ルール
- アウトブレイク フィルタ ルール
- タイム ゾーンルール



(注) RSA Email DLP エンジンとコンテンツ照合分類子の設定は、[セキュリティ サービス (Security Services)] > [RSA メール DLP (RSA Email DLP)] ページで扱われます。詳細については、「[DLP エンジンおよびコンテンツ照合分類子の更新について](#)」(P.15-39) を参照してください。

サービス アップデートの設定は、DLP アップデートを除いてアップデートを受け取るすべてのサービスに使用されます。DLP アップデートを除いて、任意のサービスにそれぞれ設定を指定できません。

プロキシ サーバを経由したアップデート

Cisco アプライアンスは、(デフォルトで) Cisco のアップデート サーバに直接接続して、アップデートを受け取るように設定されます。この接続は、ポート 80 の HTTP によって確立され、コンテンツは暗号化されます。ファイアウォールでこのポートを開くことを避ける場合は、アップデートされたルールをアプライアンスで受け取ることができる、プロキシ サーバおよび具体的なポートを定義できます。

プロキシ サーバを使用する場合は、任意で認証およびポートを指定できます。



(注) プロキシ サーバを定義すると、プロキシ サーバを使用するように設定されているすべてのサービス アップデートで、そのプロキシ サーバが *自動的に* 使用されます。任意のサービスのアップデートのために、プロキシ サーバをオフにはできません。

アップグレードおよびアップデートをダウンロードするためのサーバ設定

アプライアンスにアップグレードおよびアップデートをダウンロードするために必要なサーバ情報および接続情報を指定します。

AsyncOS のアップグレードとサービスのアップデートに同じまたは異なる設定を使用できます。

はじめる前に

アプライアンスがシスコから直接アップグレードおよびアップデートをダウンロードするか、または代わりにネットワーク上のローカル サーバでこれらのイメージをホスティングするかを設定します。次に、選択した方法をサポートするようにネットワークをセット アップします。「[アップグレードおよびアップデートをダウンロードするための設定](#)」(P.29-18) のすべての内容を参照してください。

手順

- ステップ 1** [セキュリティ サービス (Security Services)] > [サービスのアップデート (Service Updates)] を選択します。
- ステップ 2** [アップデート設定を編集 (Edit Update Settings)] をクリックします。
- ステップ 3** オプションを入力します。

設定	説明
アップデート サーバ (イメージ) (Update Servers (images))	<p>Cisco IronPort AsyncOS アップグレード イメージを、Cisco IronPort アップデート サーバまたはネットワーク上のローカル サーバのどちらからダウンロードするかを選択します。デフォルトは、アップグレードおよびアップデートの両方で Cisco IronPort アップデート サーバです。</p> <p>アップグレードとアップデートに同じ設定を使用するには、表示されるフィールドに情報を入力します。</p> <p>ローカル アップデート サーバを選択した場合は、アップグレードおよびアップデートのダウンロードに使用するサーバのベース URL とポート番号を入力します。サーバが認証を必要とする場合、有効なユーザ名とパスワードも入力します。</p> <p>AsyncOS アップグレードおよび McAfee Anti-Virus 定義ファイルにそれぞれ別の設定を入力するには、[クリックして AsyncOS の異なる設定を使用する (Click to use different settings for AsyncOS)] リンクをクリックします。</p> <p>(注) Cisco Intelligent Multi-Scan でサードパーティのアンチスパム ルールのアップデートをダウンロードするには、別のローカルサーバが必要です。</p>
アップデート サーバ (リスト) (Update Servers (lists))	<p>導入に適したアップグレードおよびアップデートのみ各アプライアンスで利用できることを確認するために、Cisco IronPort は関連するファイルのマニフェスト リストを生成します。</p> <p>利用可能なアップグレードおよびサービス アップデートのリスト (マニフェスト XML ファイル) を、Cisco IronPort アップデート サーバまたはネットワーク上のローカル サーバのどちらからダウンロードするかを選択します。</p> <p>アップデートおよび AsyncOS アップグレードのためのサーバの指定は、別のセクションに分かれています。デフォルトのアップグレードおよびアップデートは Cisco IronPort アップデート サーバです。</p> <p>ローカル アップデート サーバを選択した場合、サーバのファイル名および HTTP ポート番号を含む、各リストのマニフェスト XML ファイルのフルパスを入力します。ポートのフィールドを空のままにした場合、AsyncOS はポート 80 を使用します。サーバが認証を必要とする場合、有効なユーザ名とパスワードを入力します。</p>

設定	説明
自動アップデート (Automatic Updates)	<p>Sophos および McAfee Anti-Virus 定義ファイル、Cisco Anti-Spam ルール、Cisco Intelligent Multi-Scan ルール、PXE Engine アップデート、アウトブレイク フィルタ ルール、時間帯ルールに対する自動アップデートとアップデート間隔（アプライアンスがアップデートを確認する頻度）をイネーブルにします。</p> <p>数字の後に秒、分、時間を表す s（秒）、m（分）および h（時）を含めません。自動更新をディセーブルにするには、0（ゼロ）を入力します。</p> <p>(注) [セキュリティ サービス (Security Services)] > [RSA メール DLP (RSA Email DLP)] ページからのみ、DLP の自動アップデートを有効にできます。ただし、最初にすべてのサービスの自動アップデートをイネーブルにする必要があります。詳細については、「DLP エンジンおよびコンテンツ照合分類子の更新について」(P.15-39) を参照してください。</p>
インターフェイス (Interface)	表示されているセキュリティ コンポーネントのアップデートをアップデート サーバに問い合わせる際に使用するネットワーク インターフェイスを選択します。利用可能なプロキシデータ インターフェイスが表示されません。デフォルトでは、アプライアンスは使用するインターフェイスを選択します。
HTTP プロキシ サーバ (HTTP Proxy Server)	GUI に表示されているサービスで使用されるオプションのプロキシ サーバ。 プロキシ サーバを指定すると、すべてのサービスのアップデートのために使用できます。
HTTPS プロキシ サーバ (HTTPS Proxy Server)	HTTPS を使用したオプションのプロキシ サーバ。HTTPS プロキシ サーバを定義すると、GUI に表示されているサービスのアップデートで使用されます。

ステップ 4 変更内容を送信し、確定します。

自動アップデートの設定

手順

- ステップ 1** [セキュリティ サービス (Security Services)] > [サービスのアップデート (Service Updates)] ページに移動し、[アップデート設定を編集 (Edit Update Settings)] をクリックします。
- ステップ 2** チェックボックスをオンにして、自動アップデートをイネーブルにします。
- ステップ 3** アップデート間隔（次のアップデートの確認までに待機する時間）を入力します。数字の後に m（分）および h（時）を追加します。最大アップデート間隔は 1 時間です。

リモート電源管理のイネーブル化

アプライアンス シャーシの電源をリモートでリセットする機能は、C380 および C680 ハードウェアでのみ使用できます。

アプライアンスの電源をリモートでリセットする場合は、このセクションで説明されている手順を使用して、この機能を事前にイネーブルにし、設定しておく必要があります。

はじめる前に

- 専用リモート電源管理ポートをセキュア ネットワークに直接、ケーブル接続します。詳細については、ハードウェア インストール ガイドを参照してください。
- ファイアウォールを通過するために必要なポートを開くなど、アプライアンスがリモート アクセス可能であることを確認します。
- この機能では、専用のリモート電源管理インターフェイス用に一意の IPv4 アドレスが必要です。このインターフェイスは、このセクションで説明されている手順でのみ設定可能です。ipconfig コマンドを使用して設定することはできません。
- アプライアンスの電源を再投入するには、Intelligent Platform Management Interface (IPMI) バージョン 2.0 をサポートするデバイスを管理できるサードパーティ製ツールが必要です。このようなツールを使用できるように準備されていることを確認します。
- コマンドライン インターフェイスへのアクセスに関する詳細については、CLI のリファレンス ガイドを参照してください。

手順

-
- ステップ 1** SSH、Telnet、またはシリアル コンソール ポートを使用して、コマンドライン インターフェイスにアクセスします。
- ステップ 2** 管理者権限を持つアカウントを使用してログインします。
- ステップ 3** 次のコマンドを入力します。
- ```
remotepower
setup
```
- ステップ 4** プロンプトに従って、次の情報を指定します。
- この機能専用の IP アドレスと、ネットマスクおよびゲートウェイ。
  - 電源の再投入コマンドを実行するために必要なユーザ名とパスワード。
- これらのクレデンシャルは、アプライアンスへのアクセスに使用する他のクレデンシャルに依存しません。
- ステップ 5** commit を入力して変更を保存します。
- ステップ 6** 設定をテストして、アプライアンスの電源をリモートで管理できることを確認します。
- ステップ 7** 入力したクレデンシャルが、将来、いつでも使用できることを確認します。たとえば、この情報を安全な場所に保管し、このタスクを実行する必要がある管理者が、必要なクレデンシャルにアクセスできるようにします。
- 

### 関連項目

- [「アプライアンスの電源のリモート リセット」 \(P.36-28\)](#)

## AsyncOS の以前のバージョンへの復元

AsyncOS には、緊急時に AsyncOS オペレーティング システムを以前の認定済みのビルドに戻す機能があります。



(注) AsyncOS 7.0 にアップグレードした後は、バージョン 6.5 よりも前の AsyncOS には戻せません。

## 利用可能なバージョン

アップグレードは主要なサブシステムを一方向に変換するため、復元プロセスは複雑で、Cisco Quality Assurance チームによる認定が必要です。Cisco では、AsyncOS バージョンに対して固有のバージョンの CASE、Sophos、アウトブレイク フィルタを認証しています。以前のすべてのバージョンの AsyncOS オペレーティング システムが復元に利用できるわけではありません。最初にこの機能がサポートされた AsyncOS バージョンは AsyncOS 5.5.0 です。これより以前のバージョンの AsyncOS はサポートされていません。

## 復元の影響に関する重要な注意事項

Cisco アプライアンスにおける `revert` コマンドの使用は、非常に破壊的な操作になります。このコマンドはすべての設定ログおよびデータベースを破壊します。管理インターフェイスのネットワーク情報のみが保存されます。他のすべてのネットワーク設定は削除されます。さらに、復元はアプライアンスが再設定されるまでメール処理を中断します。このコマンドはネットワーク設定を破壊するため、`revert` コマンドを発行する場合は Cisco アプライアンスへの物理的なローカル アクセスが必要になります。



警告

戻し先のバージョンの設定ファイルが必要です。設定ファイルに下位互換性は**ありません**。

## AsyncOS の復元

### 手順

**ステップ 1** 戻し先のバージョンの設定ファイルがあることを確認してください。設定ファイルに下位互換性は**ありません**。設定ファイルを取得するには、ファイルを電子メールでユーザ自身に送信するか、ファイルを FTP で取得します。簡単な方法は、CLI の `mailconfig` コマンドを実行する方法です。

**ステップ 2** アプライアンスの現在の設定のバックアップ コピーを、(パスワードをマスクしない状態で) 別のマシンに保存します。



(注) このコピーは、バージョンを戻した後にロードする設定ファイルではありません。

**ステップ 3** セーフリスト/ブロックリスト機能を使用する場合は、セーフリスト/ブロックリスト データベースを別のマシンにエクスポートします。

**ステップ 4** メール キューが空になるまで待ちます。

**ステップ 5** バージョンを戻すアプライアンスの CLI にログインします。

`revert` コマンドの実行時には、いくつかの警告プロンプトが発行されます。これらの警告プロンプトに同意すると、すぐにバージョンを戻す動作が開始します。このため、復元に向けた準備手順が完了するまで、復元プロセスを開始しないでください。

**ステップ 6** CLI から `revert` コマンドを発行します。



**(注)** 復元プロセスは時間のかかる処理です。復元が完了して、Cisco アプライアンスへのコンソール アクセスが再び利用可能になるまでには、15 ~ 20 分かかります。

次に、revert コマンドの例を示します。

```
mail.mydomain.com> revert
```

```
This command will revert the appliance to a previous version of AsyncOS.
```

```
WARNING: Reverting the appliance is extremely destructive.
```

```
The following data will be destroyed in the process:
```

- all configuration settings (including listeners)
- all log files
- all databases (including messages in Virus Outbreak and Policy quarantines)
- all reporting data (including saved scheduled reports)
- all message tracking data
- all IronPort Spam Quarantine message and end-user safelist/blocklist data

```
Only the network settings will be preserved.
```

```
Before running this command, be sure you have:
```

- saved the configuration file of this appliance (with passwords unmasked)
- exported the IronPort Spam Quarantine safelist/blocklist database to another machine (if applicable)
- waited for the mail queue to empty

```
Reverting the device causes an immediate reboot to take place.
```

```
After rebooting, the appliance reinitializes itself and reboots again to the desired version.
```

This command will revert the appliance to a previous version of AsyncOS.

WARNING: Reverting the appliance is extremely destructive.

The following data will be destroyed in the process:

- all configuration settings (including listeners)
- all log files
- all databases (including messages in Virus Outbreak and Policy quarantines)
- all reporting data (including saved scheduled reports)
- all message tracking data
- all IronPort Spam Quarantine message and end-user safelist/blocklist data

Only the network settings will be preserved.

Before running this command, be sure you have:

- saved the configuration file of this appliance (with passwords unmasked)
- exported the IronPort Spam Quarantine safelist/blocklist database to another machine (if applicable)
- waited for the mail queue to empty

Reverting the device causes an immediate reboot to take place.

After rebooting, the appliance reinitializes itself and reboots again to the desired version.

```

=====
Available version Install date
1. 5.5.0-236 Tue Aug 28 11:03:44 PDT 2007
2. 5.5.0-330 Tue Aug 28 13:06:05 PDT 2007
3. 5.5.0-418 Wed Sep 5 11:17:08 PDT 2007

Please select an AsyncOS version: 2

You have selected "5.5.0-330".

The system will now reboot to perform the revert operation.

```

- ステップ 7** アプライアンスが 2 回再起動するまで待ちます。
- ステップ 8** マシンが 2 回再起動したら、シリアル コンソールで `interfaceconfig` コマンドを使用して、アクセス可能な IP アドレスをインターフェイスに設定します。
- ステップ 9** 設定したインターフェイスの 1 つで FTP または HTTP をイネーブルにします。
- ステップ 10** 作成した XML 設定ファイルを FTP で取得するか、または GUI インターフェイスに貼り付けます。
- ステップ 11** 戻し先のバージョンの XML 設定ファイルをロードします。
- ステップ 12** セーフリスト/ブロックリスト機能を使用する場合は、セーフリスト/ブロックリストデータベースをインポートして復元します。
- ステップ 13** 変更内容を確定します。

復元が完了した Cisco アプライアンスは、選択された AsyncOS バージョンを使用して稼働します。

## アプライアンスに生成されるメッセージの返信アドレスの設定

AsyncOS によって、次のタイミングで生成されるメールのエンベロープ送信者を設定できます。

- Anti-Virus 通知
- バウンス
- 通知 (`notify()` および `notify-copy()` フィルタの動作)
- 隔離通知 (および隔離管理機能における「コピー送信」)
- レポート

返信アドレスの表示、ユーザ、およびドメイン名を指定できます。ドメイン名に仮想ゲートウェイドメインの使用を選択することもできます。

システムで生成された電子メールメッセージの返信アドレスを GUI または `addressconfig` コマンドを使用して CLI で変更できます。

#### 手順

- 
- ステップ 1** [システム管理 (System Administration)] > [返信先アドレス (Return Addresses)] ページに移動します。
- ステップ 2** [設定を編集 (Edit Settings)] をクリックします。
- ステップ 3** 1 つまたは複数のアドレスへの変更
- ステップ 4** 変更内容を送信し、確定します。
- 

## アラート

アラートとは、Cisco アプライアンスで発生しているイベントに関する情報が記載されている、電子メールによる通知のことです。これらのイベントにはマイナーからメジャーまでの重要度（または重大度）レベルがあり、一般的にアプライアンスの特定のコンポーネントまたは機能に関連しています。アラートは、Cisco アプライアンスで生成されます。送信するアラートメッセージの種類、重大度、および送信するユーザを非常に詳細なレベルで指定できます。アラートは、GUI の [システム管理 (System Administration)] > [アラート (Alerts)] ページ（または CLI の `alertconfig` コマンド）で管理します。

## アラートの概要

アラート機能は 3 つの主要な部分から構成されます。

- [アラート (Alerts)] : アラート受信者（アラートを受信する電子メール アドレス）、および受信者に送信されるアラート通知（重大度およびアラート タイプ）。
- [アラート設定 (Alert Settings)] : アラート送信者 ([FROM:] アドレス、次に重複したアラートを送信するまでに待機する秒数、および `AutoSupport` をイネーブルにするかどうか（およびオプションで毎週 `AutoSupport` レポートを送信するかどうか）などのアラート機能に関する全般的な動作を指定します。
- [トップアラート (Top Alerts)] : アプライアンスで生成された最新のアラートのリスト。

## アラート : アラート受信者、アラート分類、および重要度

アラートとは、アラート受信者に送信される、ハードウェアやアンチウイルスの問題など特定の機能（またはアラート分類）に関する情報が記載された電子メールメッセージまたは通知のことです。アラート受信者とは、アラート通知が送信される電子メール アドレスのことです。通知に含まれる情報は、アラート分類と重大度によって決まります。アラート受信者に送信するアラート分類と重大度を指定できます。アラート エンジンでは、送信するアラートの種類とアラート受信者を詳細に制御できます。たとえば、アラート受信者が `System`（アラートの種類）に関する `Critical`（重大度）の情報が送信されたときのみ通知を受信するように設定することで、アラート受信者に特定のアラートのみを送信するように設定できます。また、一般的な設定値も設定できます（「アラート設定値の設定」(P.29-34) を参照してください）。

すべてのアラートのリストについては、「アラート リスト」(P.29-35) を参照してください。

## アラート分類

AsyncOS では、次のアラート分類を送信します。

- システム (System)
- ハードウェア (Hardware)
- アップデータ (Updater)
- アウトブレイク フィルタ (Outbreak Filters)
- ウイルス対策 (Anti-Virus)
- スпам対策 (Anti-Spam)
- ディレクトリ獲得攻撃防御 (Directory Harvest Attack Prevention)

## 重大度

アラートは、次の重大度に従って送信されます。

- [クリティカル (Critical)] : すぐに対処が必要です。
- [警告 (Warning)] : 今後モニタリングが必要な問題またはエラー。すぐに対処が必要な可能性もあります。
- [情報 (Information)] : デバイスのルーティン機能で生成される情報。

## アラート設定

アラート設定では、アラートの全般的な動作と設定を制御します。設定には次のような項目があります。

- **RFC 2822 Header From** : アラートを送信するタイミング (アドレスを入力するか、デフォルトの「alert@<hostname>」を使用します)。また、`alertconfig -> from` コマンドを使用して、この値を CLI で設定することもできます。
- 重複したアラートを送信するまでに待機する秒数の初期値。
- 重複したアラートを送信するまでに待機する秒数の最大値。
- **AutoSupport** のステータス (イネーブルまたはディセーブル)。
- **Information** レベルの **System** アラートを受信するように設定されたアラート受信者への、**AutoSupport** の毎週のステータス レポートの送信。

## 重複したアラートの送信

AsyncOS が重複したアラートを送信するまでに待機する秒数の初期値を指定できます。この値を 0 に設定した場合、重複したアラートのサマリーは送信されず、代わりにすべての重複したアラートがリアルタイムに送信されます (短時間に大量の電子メールを受信する可能性があります)。重複したアラートを送信するまでに待機する秒数は、アラートを送信するたびに増加します。増加する秒数は、前回の待機間隔の 2 倍の値を足した秒数です。つまり、この値を 5 秒に設定すると、アラートは 5 秒後、15 秒後、35 秒後、75 秒後、155 秒後、315 秒後といった間隔で送信されます。

最終的に、送信間隔は非常に大きな秒数になります。[ 重複するアラートを送信するまでの最大待機時間 (秒) (**Maximum Number of Seconds to Wait Before Sending a Duplicate Alert**) ] フィールドを使用して、待機間隔の秒数に制限を設けることができます。たとえば、初期値を 5 秒に設定し、最大値を 60 秒に設定すると、アラートは 5 秒後、15 秒後、35 秒後、60 秒後、120 秒後といった間隔で送信されます。

## SMTP ルートおよびアラート

アプライアンスから [アラート受信者 (Alert Recipient)] で指定されたアドレスに送信されるアラートは、該当の送信先に対して定義された SMTP ルートに従います。

## Cisco AutoSupport

十分なサポートと今後のシステム変更の設計を可能にするため、システムで生成されたすべてのアラートメッセージをシスコに送信するように Cisco アプライアンスを設定できます。この機能は AutoSupport と呼ばれ、シスコによるお客様のニーズへのプロアクティブな対応に役立ちます。また、AutoSupport はシステムの稼働時間、status コマンドの出力、および使用されている AsyncOS バージョンを通知するレポートを毎週送信します。

デフォルトでは、アラートタイプが System で重大度レベルが Information のアラートを受信するように設定されているアラート受信者は、シスコに送信される各メッセージのコピーを受信します。内部にアラートメッセージを毎週送信しない場合は、この設定をディセーブルにできます。この機能をイネーブ爾またはディセーブルにするには、「アラート設定値の設定」(P.29-34) を参照してください。

## アラート メッセージ

アラートメッセージは標準的な電子メールメッセージです。Header From: アドレスは設定できますが、メッセージのその他の部分は自動的に生成されます。

## アラートの From アドレス

[設定を編集 (Edit Settings)] ボタンまたは CLI (『Cisco AsyncOS CLI Reference Guide』を参照) を使用して、Header From: アドレスを設定できます。

## アラートの件名

アラートの電子メールメッセージの件名は、次の形式に従っています。

```
Subject: [severity]-[hostname]: ([class]) short message
```

## アラートの配信

アラートメッセージは Cisco アプライアンス内の問題の通知に使用されるため、送信に AsyncOS の標準メール配信システムを使用しません。代わりに、アラートメッセージは AsyncOS で重大なシステム故障が発生しても動作するように設計された、個別に並行動作する電子メールシステムで処理されません。

アラートメールシステムは、AsyncOS と同一の設定を共有しません。このため、アラートメッセージは、次のように他のメール配信とは若干異なる動作をする可能性があります。

- アラートメッセージは、標準の DNS MX レコードおよび A レコードのルックアップを使用して配信されます。
  - 5.X 以前の AsyncOS バージョンでは、アラートメッセージは smtproutes を使用しません。
  - アラートメッセージは DNS エントリを 30 分間キャッシュし、そのキャッシュは 30 分ごとにリフレッシュされます。このため、DNS 障害時にもアラートが出力されます。



- アラート メッセージはワーク キューを通過しないため、ウイルスまたはスパムのスキャン対象外です。メッセージ フィルタまたはコンテンツ フィルタの処理対象にも含まれません。
- アラート メッセージは配信キューを通過しないため、バウンスのプロファイルまたは送信先制御の制限には影響を受けません。

## アラート メッセージの例

```
Date: 23 Mar 2005 21:10:19 +0000

To: joe@example.com

From: IronPort C60 Alert [alert@example.com]

Subject: Critical-example.com: (Anti-Virus) update via http://newproxy.example.com
failed

The Critical message is:

update via http://newproxy.example.com failed

Version: 4.5.0-419

Serial Number: XXXXXXXXXXXX-XXXXXXX

Timestamp: Tue May 10 09:39:24 2005

For more information about this error, please see

http://support.ironport.com

If you desire further information, please contact your support provider.
```

## アラート受信者の追加



(注) システムのセットアップ時に **AutoSupport** をイネーブルにした場合、指定した電子メールアドレスにすべての重大度およびクラスのアラートを受信します (デフォルト)。この設定はいつでも変更できます。

### 手順

- ステップ 1** [システム管理 (System Administration)] > [アラート (Alerts)] ページに移動します。
- ステップ 2** [受信者を追加 (Add Recipient)] をクリックします。

- ステップ 3** 受信者の電子メール アドレスを入力します。複数のアドレスをカンマで区切って入力することもできます。
- ステップ 4** 受信するアラートの重大度を選択します。
- ステップ 5** 変更内容を送信し、確定します。

## アラート設定値の設定

アラート設定はグローバルな設定であるため、すべてのアラートの動作に影響します。



(注) 後から確認するためにアプライアンスに保存するアラートの数を定義するには `alertconfig` CLI コマンドを使用します。

## アラート設定値の編集

### 手順

- ステップ 1** [アラート (Alerts)] ページで [設定を編集 (Edit Settings)] をクリックします。
- ステップ 2** アラートの送信に使用する Header From: アドレスを入力するか、[自動生成 (Automatically Generated)] (「alert@<hostname>」を自動生成) を選択します。
- ステップ 3** 重複したアラートを送信するまでに待機する秒数を指定する場合は、チェックボックスをオンにします。詳細については、「[重複したアラートの送信](#)」(P.29-31) を参照してください。
- 重複したアラートを送信するまでに待機する秒数の初期値を指定します。
  - 重複したアラートを送信するまでに待機する秒数の最大値を指定します。
- ステップ 4** [IronPort AutoSupport] オプションをオンにすることで、AutoSupport をイネーブルにできます。AutoSupport の詳細については、「[Cisco AutoSupport](#)」(P.29-32) を参照してください。
- AutoSupport がイネーブルの場合、Information レベルの System アラートを受信するように設定されたアラート受信者に、毎週 AutoSupport レポートが送信されます。チェックボックスを外すことでディセーブルにできます。
- ステップ 5** 変更内容を送信し、確定します。

## トップアラートの表示

電子メール セキュリティ アプライアンスは最新のアラートを保存するので、アラートメッセージを消失または削除した場合に GUI および CLI の両方で表示できます。これらのアラートは、アプライアンスからダウンロードできません。

最新のアラートのリストを表示するには、[アラート (Alerts)] ページにある [トップアラートを表示 (View Top Alerts)] ボタンをクリックするか、CLI で `displayalerts` コマンドを使用します。GUI でアラートを、日付、レベル、クラス、テキスト、受信者によって調整します。

デフォルトでは、アプライアンスは [ トップ アラート (Top Alerts) ] ウィンドウに表示するために最大 50 個のアラートを保存します。アプライアンスが保存するアラートの数を編集するには、CLI で `alertconfig -> setup` コマンドを使用します。この機能を無効にするにはアラートの数を 0 に変更します。

## アラート リスト

次の表に、分類したアラートのリストを示します。表には、アラート名 (Cisco で使用される内部記述子)、アラートの実際のテキスト、説明、重大度 (**critical**、**information**、または **warning**) およびメッセージのテキストに含まれるパラメータ (存在する場合) が含まれています。アラートの実際のテキストでは、パラメータ値は置き換えられます。たとえば、次のアラート メッセージではメッセージのテキストに「\$ip」が記述されています。アラート生成時に「\$ip」は実際の IP アドレスに置き換えられます。

## アンチスパム アラート

表 29-1 に、AsyncOS で生成される可能性があるさまざまなアンチスパムに関するアラートのリストを示します。この表には、アラートの説明とアラートの重大度が含まれています。

表 29-1 発生する可能性があるアンチスパム アラートのリスト

| アラート名              | メッセージと説明                                                                                            | パラメータ                                                                     |
|--------------------|-----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| AS.SERVER.ALERT    | \$engine anti-spam - \$message \$tb<br>Critical。アンチスパム エンジンに障害が発生した場合に送信されます。                       | 「engine」: アンチスパム エンジンのタイプ。<br>「message」: ログ メッセージ。<br>「tb」: イベントのトレースバック。 |
| AS.TOOL.INFO_ALERT | Update - \$engine - \$message<br>Information。アンチスパム エンジンに問題が発生した場合に送信されま                            | 「engine」: アンチスパム エンジンの名前。<br>「message」: メッセージ。                            |
| AS.TOOL.ALERT      | Update - \$engine - \$message<br>Critical。アンチスパム エンジンの管理に使用されるツールの 1 つに問題があり、アップデートが中止される場合に送信されます。 | 「engine」: アンチスパム エンジンの名前。<br>「message」: メッセージ。                            |

## アンチウイルス アラート

表 29-2 に、AsyncOS で生成される可能性があるさまざまなアンチウイルスに関するアラートのリストを示します。この表には、アラートの説明とアラートの重大度が含まれています。

表 29-2 発生する可能性があるアンチウイルス アラートのリスト

| アラート名                                  | メッセージと説明                                                                                    | パラメータ                                                                                               |
|----------------------------------------|---------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| AV.SERVER.ALERT/<br>AV.SERVER.CRITICAL | \$engine antivirus - \$message \$tb                                                         | 「 <b>engine</b> 」: アンチウイルスエンジンのタイプ。<br>「 <b>message</b> 」: ログメッセージ。<br>「 <b>tb</b> 」: イベントのトレースバック。 |
|                                        | Critical。アンチウイルス スキャン エンジンに重大な問題が発生した場合に送信されます。                                             |                                                                                                     |
| AV.SERVER.ALERT.INFO                   | \$engine antivirus - \$message \$tb                                                         | 「 <b>engine</b> 」: アンチウイルスエンジンのタイプ。<br>「 <b>message</b> 」: ログメッセージ。<br>「 <b>tb</b> 」: イベントのトレースバック。 |
|                                        | Information。アンチウイルス スキャン エンジンに情報イベントが発生した場合に送信されます。                                         |                                                                                                     |
| AV.SERVER.ALERT.WARN                   | \$engine antivirus - \$message \$tb                                                         | 「 <b>engine</b> 」: アンチウイルスエンジンのタイプ。<br>「 <b>message</b> 」: ログメッセージ。<br>「 <b>tb</b> 」: イベントのトレースバック。 |
|                                        | Warning。アンチウイルス スキャン エンジンに問題が発生した場合に送信されます。                                                 |                                                                                                     |
| MAIL.ANTIVIRUS.<br>ERROR_MESSAGE       | MID \$mid antivirus \$what error \$tag                                                      | 「 <b>mid</b> 」: MID<br>「 <b>what</b> 」: 発生したエラー。<br>「 <b>tag</b> 」: ウイルス発生名 (設定されている場合)。            |
|                                        | Critical。メッセージのスキャン中に、アンチウイルス スキャンがエラーを生成した場合に送信されます。                                       |                                                                                                     |
| MAIL.SCANNER.<br>PROTOCOL_MAX_RETRY    | MID \$mid is malformed and cannot be scanned by \$engine.                                   | 「 <b>mid</b> 」: MID<br>「 <b>engine</b> 」: 使用されているエンジン。                                              |
|                                        | Critical。メッセージが不正なため、スキャン エンジンにメッセージのスキャンに失敗しました。再試行の最大回数を超過したため、メッセージはエンジンにスキャンされずに処理されます。 |                                                                                                     |

## ディレクトリ獲得攻撃（DHAP）アラート

表 29-3 に、AsyncOS で生成される可能性があるさまざまな DHAP に関するアラートのリストを示します。この表には、アラートの説明とアラートの重大度が含まれています。

表 29-3 発生する可能性があるディレクトリ獲得攻撃アラートのリスト

| アラート名           | メッセージと説明                                                                                                            | パラメータ |
|-----------------|---------------------------------------------------------------------------------------------------------------------|-------|
| LDAP.DHAP_ALERT | LDAP: Potential Directory Harvest Attack detected. See the system mail logs for more information about this attack. |       |
|                 | Warning。ディレクトリ獲得攻撃の可能性を検出した場合に送信されます。                                                                               |       |

## ハードウェア アラート

表 29-4 に、AsyncOS で生成される可能性があるさまざまなハードウェア アラートのリストを示します。この表には、アラートの説明とアラートの重大度が含まれています。

表 29-4 発生する可能性があるハードウェア アラートのリスト

| アラート名                                 | メッセージと説明                                                                                                                     | パラメータ                                                     |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------|
| INTERFACE.ERRORS                      | Port \$port: has detected \$in_err input errors, \$out_err output errors, \$col collisions please check your media settings. | 「port」：インターフェイス名。<br>「in_err」：最後のメッセージからの入力エラー数。          |
|                                       | Warning。インターフェイス エラーを検出した場合に送信されます。                                                                                          | 「out_err」：最後のメッセージからの出力エラー数。<br>「col」：最後のメッセージからのパケット衝突数。 |
| MAIL.MEASUREMENTS_FILESYSTEM          | The \$file_system partition is at \$capacity% capacity                                                                       | 「file_system」：ファイルシステムの名前。                                |
|                                       | Warning。ディスク パーティションが 75 % の使用率に近づいた場合に送信されます。                                                                               | 「capacity」：ファイルシステムの使用率 (%)。                              |
| MAIL.MEASUREMENTS_FILESYSTEM.CRITICAL | The \$file_system partition is at \$capacity% capacity                                                                       | 「file_system」：ファイルシステムの名前。                                |
|                                       | Critical。ディスク パーティションが 90 % の使用率に達した場合 (95 %、96 %、97 % など) に送信されます。                                                          | 「capacity」：ファイルシステムの使用率 (%)。                              |
| SYSTEM.RAID_EVENT_ALERT               | A RAID-event has occurred: \$error                                                                                           | 「error」：RAID エラーのテキスト。                                    |
|                                       | Warning。重大な RAID-event が発生した場合に送信されます。                                                                                       |                                                           |
| SYSTEM.RAID_EVENT_ALERT_INFO          | A RAID-event has occurred: \$error                                                                                           | 「error」：RAID エラーのテキスト。                                    |
|                                       | Information。RAID-event が発生した場合に送信されます。                                                                                       |                                                           |

## Cisco スпам隔離アラート

表 29-5 に、AsyncOS で生成される可能性があるさまざまな Cisco スпам隔離に関するアラートのリストを示します。この表には、アラートの説明とアラートの重大度が含まれています。

表 29-5 発生する可能性がある Cisco スпам隔離アラートのリスト

| アラート名                       | メッセージと説明                                                      | パラメータ                                                                                        |
|-----------------------------|---------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| ISQ.CANNOT_CONNECT_OFF_BOX  | ISQ: Could not connect to off-box quarantine at \$host:\$port | 「 <b>host</b> 」: オフボックス隔離のアドレス。<br>「 <b>port</b> 」: オフボックス隔離に接続するポート。                        |
|                             | Information. AsyncOS が (オフボックス) IP アドレスに接続できない場合に送信されます。      |                                                                                              |
| ISQ.CRITICAL                | ISQ: \$msg                                                    | 「 <b>msg</b> 」: 表示されるメッセージ                                                                   |
|                             | Critical. Cisco スпам隔離に重大なエラーが発生した場合に送信されます。                  |                                                                                              |
| ISQ.DB_APPROACHING_FULL     | ISQ: Database over \$threshold% full                          | 「 <b>threshold</b> 」: アラートを開始する使用率のしきい値                                                      |
|                             | Warning. Cisco スпам隔離データベースがフルに近い場合に送信されます。                   |                                                                                              |
| ISQ.DB_FULL                 | ISQ: database is full                                         |                                                                                              |
|                             | Critical. Cisco スпам隔離データベースがフルになった場合に送信されます。                 |                                                                                              |
| ISQ.MSG_DEL_FAILED          | ISQ: Failed to delete MID \$mid for \$rcpt: \$reason          | 「 <b>mid</b> 」: MID<br>「 <b>rcpt</b> 」: 受信者または「all」(全員)<br>「 <b>reason</b> 」: メッセージが削除されない理由 |
|                             | Warning. Cisco スпам隔離からの電子メールの削除に失敗した場合に送信されます。               |                                                                                              |
| ISQ.MSG_NOTIFICATION_FAILED | ISQ: Failed to send notification message: \$reason            | 「 <b>reason</b> 」: 通知が送信されない理由                                                               |
|                             | Warning. 通知メッセージの送信に失敗した場合に送信されません。                           |                                                                                              |
| ISQ.MSG_QUAR_FAILED         |                                                               |                                                                                              |
|                             | Warning. メッセージの隔離に失敗した場合に送信されます。                              |                                                                                              |
| ISQ.MSG_RLS_FAILED          | ISQ: Failed to release MID \$mid to \$rcpt: \$reason          | 「 <b>mid</b> 」: MID<br>「 <b>rcpt</b> 」: 受信者または「all」(全員)<br>「 <b>reason</b> 」: メッセージが開放されない理由 |
|                             | Warning. メッセージの開放に失敗した場合に送信されます。                              |                                                                                              |

表 29-5 発生する可能性がある Cisco スпам隔離アラートのリスト (続き)

| アラート名                        | メッセージと説明                                                            | パラメータ                    |
|------------------------------|---------------------------------------------------------------------|--------------------------|
| ISQ.MSG_RLS_FAILED_UNK_RCPTS | ISQ: Failed to release MID \$mid: \$reason                          | 「mid」: MID               |
|                              | Warning。受信者が不明のため、メッセージの開放に失敗した場合に送信されます。                           | 「reason」: メッセージが開放されない理由 |
| ISQ.NO_EU_PROPS              | ISQ: Could not retrieve \$user's properties.Setting defaults        | 「user」: エンドユーザ名          |
|                              | Information。AsyncOS がユーザの情報を取得できない場合に送信されます。                        |                          |
| ISQ.NO_OFF_BOX_HOST_SET      | ISQ: Setting up off-box ISQ without setting host                    |                          |
|                              | Information。AsyncOS が外部隔離を参照するように設定されているものの、外部隔離が定義されていない場合に送信されます。 |                          |

## セーフリスト/ブロックリスト アラート

次の表に、AsyncOS で生成される可能性があるさまざまなセーフリスト/ブロックリストに関するアラートのリストを示します。この表には、アラートの説明とアラートの重大度が含まれています。

表 29-6 発生する可能性があるセーフリスト/ブロックリストアラートのリスト

| アラート名                   | メッセージと説明                                                                                      | パラメータ                     |
|-------------------------|-----------------------------------------------------------------------------------------------|---------------------------|
| SLBL.DB.RECOVERY_FAILED | SLBL: Failed to recover End-User Safelist/Blocklist database: '\$error'.                      | 「error」: エラーの理由           |
|                         | Critical。セーフリスト/ブロックリスト データベースの復旧に失敗しました。                                                     |                           |
| SLBL.DB.SPACE_LIMIT     | SLBL: End-User Safelist/Blocklist database exceeded allowed disk space: \$current of \$limit. | 「current」: データベース使用量 (MB) |
|                         | Critical。セーフリスト/ブロックリスト データベースが許容されたディスク領域を超過しました。                                            | 「limit」: 設定された制限使用量 (MB)  |

## システム アラート

表 29-7 に、AsyncOS で生成される可能性があるさまざまなシステム アラートのリストを示します。この表には、アラートの説明とアラートの重大度が含まれています。

表 29-7 発生する可能性があるシステム アラートのリスト

| アラート名                                       | メッセージと説明                                                                                                                                  | パラメータ                                                                   |
|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| COMMON.APP_FAILURE                          | An application fault occurred: \$error                                                                                                    | 「error」: エラーのテキスト<br>(通常はトレースバック)                                       |
|                                             | Warning。不明なアプリケーション障害が発生した場合に送信されます。                                                                                                      |                                                                         |
| COMMON.KEY_EXPIRED_ALERT                    | Your "\$feature" key has expired.Please contact your authorized Cisco sales representative.                                               | 「feature」: 有効期限が切れる機能の名前。                                               |
|                                             | Warning。ライセンス キーの有効期限が切れた場合に送信されます。                                                                                                       |                                                                         |
| COMMON.KEY_EXPIRING_ALERT                   | Your "\$feature" key will expire in under \$days day(s).Please contact your authorized Cisco sales representative.                        | 「feature」: 有効期限が切れる機能の名前。<br>「days」: 有効期限が切れるまでの日数。                     |
|                                             | Warning。ライセンス キーの有効期限が切れる場合に送信されます。                                                                                                       |                                                                         |
| COMMON.KEY_FINAL_EXPIRING_ALERT             | This is a final notice.Your "\$feature" key will expire in under \$days day(s).Please contact your authorized Cisco sales representative. | 「feature」: 有効期限が切れる機能の名前。<br>「days」: 有効期限が切れるまでの日数。                     |
|                                             | Warning。ライセンス キーの有効期限が切れる場合の最後の通知として送信されます。                                                                                               |                                                                         |
| DNS.BOOTSTRAP_FAILED                        | Failed to bootstrap the DNS resolver.Unable to contact root servers.                                                                      |                                                                         |
|                                             | Warning。アプライアンスがルート DNS サーバに問い合わせることができない場合に送信されます。                                                                                       |                                                                         |
| INTERFACE.FAILOVER.FAILURE_BACKUP_DETECTED  | Standby port \$port on \$pair_name failure                                                                                                | 「port」: 検出されたポート<br>「pair_name」: フェールオーバーのペア名。                          |
|                                             | Warning。バックアップ NIC ペアリング インターフェイスが故障した場合に送信されます。                                                                                          |                                                                         |
| INTERFACE.FAILOVER.FAILURE_BACKUP_RECOVERED | Standby port \$port on \$pair_name okay                                                                                                   | 「port」: 故障したポート<br>「pair_name」: フェールオーバーのペア名。                           |
|                                             | Information。NIC ペアのフェールオーバーが復旧した場合に送信されます。                                                                                                |                                                                         |
| INTERFACE.FAILOVER.FAILURE_DETECTED         | Port \$port failure on \$pair_name, switching to \$port_other                                                                             | 「port」: 故障したポート。<br>「port_other」: 新しいポート。<br>「pair_name」: フェールオーバーのペア名。 |
|                                             | Critical。インターフェイス故障により、NIC ペアリング フェールオーバーが検出された場合に送信されます。                                                                                 |                                                                         |



表 29-7 発生する可能性があるシステム アラートのリスト (続き)

| アラート名                                                 | メッセージと説明                                                                                                      | パラメータ                                                                         |
|-------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| INTERFACE.FAILOVER.<br>FAILURE_DETECTED_NO_<br>BACKUP | Port \$port_other on \$pair_name is down, can't switch to \$port_other                                        | 「port」: 故障したポート。<br>「port_other」: 新しいポート。<br>「pair_name」: フェールオーバーのペア名。       |
|                                                       | Critical。インターフェイス故障により NIC ペアリング フェールオーバーは検出されたけれども、バックアップインターフェイスが利用できない場合に送信されます。                           |                                                                               |
| INTERFACE.FAILOVER.<br>FAILURE_RECOVERED              | Recovered network on \$pair_name using port \$port                                                            | 「port」: 故障したポート<br>「pair_name」: フェールオーバーのペア名。                                 |
|                                                       | Information。NIC ペアのフェールオーバーが復旧した場合に送信されます。                                                                    |                                                                               |
| INTERFACE.FAILOVER.<br>MANUAL                         | Manual failover to port \$port on \$pair_name                                                                 | 「port」: 新しいアクティブポート。<br>「pair_name」: フェールオーバーのペア名。                            |
|                                                       | Information。別の NIC ペアへの手動フェールオーバーが検出された場合に送信されます。                                                             |                                                                               |
| COMMON.INVALID_FILTER                                 | Invalid \$class: \$error                                                                                      | 「class」: 「Filter」、<br>「SimpleFilter」などのいずれか。<br>「error」: フィルタが無効な理由に関する追加の情報。 |
|                                                       | Warning。無効なフィルタが存在する場合に送信されます。                                                                                |                                                                               |
| LDAP.GROUP_QUERY_<br>FAILED_ALERT                     | LDAP: Failed group query \$name, comparison in filter will evaluate as false                                  | 「name」: クエリーの名前。                                                              |
|                                                       | Critical。LDAP グループ クエリーに失敗した場合に送信されます。                                                                        |                                                                               |
| LDAP.HARD_ERROR                                       | LDAP: work queue processing error in \$name reason \$why                                                      | 「name」: クエリーの名前。<br>「why」: エラーが発生した理由。                                        |
|                                                       | Critical。LDAP クエリーが (すべてのサーバで試行した後) 完全に失敗した場合に送信されます。                                                         |                                                                               |
| LOG.ERROR.*                                           | Critical。さまざまなロギング エラー。                                                                                       |                                                                               |
| MAIL.PERRCPT.LDAP_<br>GROUP_QUERY_FAILED              | LDAP group query failure during per-recipient scanning, possible LDAP misconfiguration or unreachable server. |                                                                               |
|                                                       | Critical。各受信者のスキャン時に LDAP グループ クエリーに失敗した場合に送信されます。                                                            |                                                                               |
| MAIL.QUEUE.ERROR.*                                    | Critical。メール キューのさまざまなハードエラー。                                                                                 |                                                                               |

表 29-7 発生する可能性があるシステム アラートのリスト (続き)

| アラート名                               | メッセージと説明                                                                                                                                                                                                                                                                                                                                                                                            | パラメータ                                                                                                                                              |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| MAIL.RES_CON_START_ALERT.MEMORY     | This system (hostname: \$hostname) has entered a 'resource conservation' mode in order to prevent the rapid depletion of critical system resources. RAM utilization for this system has exceeded the resource conservation threshold of \$memory_threshold_start%. The allowed receiving rate for this system will be gradually decreased as RAM utilization approaches \$memory_threshold_halt%.   | <p>「hostname」: ホストの名前。</p> <p>「memory_threshold_start」: メモリのターピットを開始するパーセントしきい値。</p> <p>「memory_threshold_halt」: メモリがフルのためにシステムが停止するパーセントしきい値。</p> |
|                                     | Critical。メモリ使用率がシステムリソース節約しきい値を超過した場合に送信されます。                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                    |
| MAIL.RES_CON_START_ALERT.QUEUE_SLOW | This system (hostname: \$hostname) has entered a 'resource conservation' mode in order to prevent the rapid depletion of critical system resources. The queue is overloaded and is unable to maintain the current throughput.                                                                                                                                                                       | <p>「hostname」: ホストの名前。</p>                                                                                                                         |
|                                     | Critical。メールキューが過負荷となり、システムリソース節約がイネーブルになった場合に送信されます。                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                    |
| MAIL.RES_CON_START_ALERT.QUEUE      | This system (hostname: \$hostname) has entered a 'resource conservation' mode in order to prevent the rapid depletion of critical system resources. Queue utilization for this system has exceeded the resource conservation threshold of \$queue_threshold_start%. The allowed receiving rate for this system will be gradually decreased as queue utilization approaches \$queue_threshold_halt%. | <p>「hostname」: ホストの名前。</p> <p>「queue_threshold_start」: キューのターピットを開始するパーセントしきい値。</p> <p>「queue_threshold_halt」: キューがフルのためにシステムが停止するパーセントしきい値。</p>   |
|                                     | Critical。キュー使用率がシステムリソース節約しきい値を超過した場合に送信されます。                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                    |

表 29-7 発生する可能性があるシステム アラートのリスト (続き)

| アラート名                            | メッセージと説明                                                                                                                                                                                                                                                                                                                                                                                                                                          | パラメータ                                                                                                                |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|
| MAIL.RES_CON_START_ALERT.WORKQ   | This system (hostname: \$hostname) has entered a 'resource conservation' mode in order to prevent the rapid depletion of critical system resources. Listeners have been suspended because the current work queue size has exceeded the threshold of \$suspend_threshold. Listeners will be resumed once the work queue size has dropped to \$resume_threshold. These thresholds may be altered via use of the 'tarpit' command on the system CLI. | 「hostname」: ホストの名前。<br>「suspend_threshold」: リスナーが一時停止されるワークキューの下限サイズ。<br>「resume_threshold」: リスナーが再開されるワークキューの上限サイズ。 |
|                                  | Information。ワークキューのサイズが大きすぎるため、リスナーが一時停止された場合に送信されます。                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                      |
| MAIL.RES_CON_START_ALERT         | This system (hostname: \$hostname) has entered a 'resource conservation' mode in order to prevent the rapid depletion of critical system resources.                                                                                                                                                                                                                                                                                               | 「hostname」: ホストの名前。                                                                                                  |
|                                  | Critical。アプライアンスが「リソース節約」モードに入った場合に送信されます。                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                      |
| MAIL.RES_CON_STOP_ALERT          | This system (hostname: \$hostname) has exited 'resource conservation' mode as resource utilization has dropped below the conservation threshold.                                                                                                                                                                                                                                                                                                  | 「hostname」: ホストの名前。                                                                                                  |
|                                  | Information。アプライアンスの「リソース節約」モードが解除された場合に送信されます。                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                      |
| MAIL.WORK_QUEUE_PAUSED_NATURAL   | work queue paused, \$num msgs, \$reason                                                                                                                                                                                                                                                                                                                                                                                                           | 「num」: ワークキューに存在するメッセージ数。<br>「reason」: ワークキューが中断された理由。                                                               |
|                                  | Critical。ワークキューが中断された場合に送信されます。                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                      |
| MAIL.WORK_QUEUE_UNPAUSED_NATURAL | work queue resumed, \$num msgs                                                                                                                                                                                                                                                                                                                                                                                                                    | 「num」: ワークキューに存在するメッセージ数。                                                                                            |
|                                  | Critical。ワークキューが再開された場合に送信されます。                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                      |
| NTP.NOT_ROOT                     | Not running as root, unable to adjust system time                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                      |
|                                  | Warning。Sent when the Cisco appliance is unable to adjust time because NTP is not running as root.                                                                                                                                                                                                                                                                                                                                                |                                                                                                                      |

表 29-7 発生する可能性があるシステム アラートのリスト (続き)

| アラート名                              | メッセージと説明                                                                                                                                                                                                                                                                    | パラメータ                                                         |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|
| QUARANTINE.ADD_DB_ERROR            | Unable to quarantine MID \$mid - quarantine system unavailable                                                                                                                                                                                                              | 「mid」: MID                                                    |
|                                    | Critical。メッセージを隔離エリアに送ることができない場合に送信されます。                                                                                                                                                                                                                                    |                                                               |
| QUARANTINE.DB_UPDATE_FAILED        | Unable to update quarantine database (current version: \$version; target \$target_version)                                                                                                                                                                                  | 「version」: 検出されたスキーマバージョン。<br>「target_version」: 対象のスキーマバージョン。 |
|                                    | Critical。隔離データベースがアップデートできない場合に送信されます。                                                                                                                                                                                                                                      |                                                               |
| QUARANTINE.DISK_SPACE_LOW          | The quarantine system is unavailable due to a lack of space on the \$file_system partition.                                                                                                                                                                                 | 「file_system」: ファイルシステムの名前。                                   |
|                                    | Critical。隔離用のディスク領域がフルになった場合に送信されます。                                                                                                                                                                                                                                        |                                                               |
| QUARANTINE.THRESHOLD_ALERT         | Quarantine "\$quarantine" is \$full% full                                                                                                                                                                                                                                   | 「quarantine」: 隔離エリアの名前。<br>「full」: 隔離エリアの容量使用率。               |
|                                    | Warning。隔離エリアの容量使用率が 5 %、50 %、または 75 % に達した場合に送信されます。                                                                                                                                                                                                                       |                                                               |
| QUARANTINE.THRESHOLD_ALERT.SERIOUS | Quarantine "\$quarantine" is \$full% full                                                                                                                                                                                                                                   | 「quarantine」: 隔離エリアの名前。<br>「full」: 隔離エリアの容量使用率。               |
|                                    | Critical。隔離エリアの容量使用率が 95 % に達した場合に送信されます。                                                                                                                                                                                                                                   |                                                               |
| REPORTD.DATABASE_OPEN_FAILED_ALERT | The reporting system has encountered a critical error while opening the database. In order to prevent disruption of other services, reporting has been disabled on this machine. Please contact customer support to have reporting enabled. The error message is: \$err_msg | 「err_msg」: 発生したエラーメッセージ                                       |
|                                    | Critical。レポート エンジンがデータベースを開けない場合に送信されます。                                                                                                                                                                                                                                    |                                                               |

表 29-7 発生する可能性があるシステム アラートのリスト (続き)

| アラート名                                      | メッセージと説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | パラメータ                                                                                    |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| REPORTD.AGGREGATION_DISABLED_ALERT         | <p>Processing of collected reporting data has been disabled due to lack of logging disk space. Disk usage is above \$threshold percent. Recording of reporting events will soon become limited and reporting data may be lost if disk space is not freed up (by removing old logs, etc.). Once disk usage drops below \$threshold percent, full processing of reporting data will be restarted automatically.</p> <p>Warning。システムのディスク領域が不足している場合に送信されます。ログ エントリに関するディスク使用率がログ使用率のしきい値を超過すると、reportd は集約をディセーブルにし、アラートを送信します。</p> | 「 <b>threshold</b> 」: しきい値                                                               |
| REPORTING.CLIENT.UPDATE_FAILED_ALERT       | <p>Reporting Client: The reporting system has not responded for an extended period of time (\$duration).</p> <p>Warning。レポート エンジンがレポート データを保存できなかった場合に送信されます。</p>                                                                                                                                                                                                                                                                                                                                                                 | 「 <b>duration</b> 」: クライアントがレポート デーモンへの問い合わせを試行する時間。この値は、人間が読み取れる形式の文字列です (「1h 3m 27s」)。 |
| REPORTING.CLIENT.JOURNAL_FULL              | <p>Reporting Client: The reporting system is unable to maintain the rate of data being generated. Any new data generated will be lost.</p> <p>Critical。レポート エンジンが新規データを保存できない場合に送信されます。</p>                                                                                                                                                                                                                                                                                                                                       |                                                                                          |
| REPORTING.CLIENT.JOURNAL_FREE              | <p>Reporting Client: The reporting system is now able to handle new data.</p> <p>Information。レポート エンジンが再び新規データを保存できるようになった場合に送信されます。</p>                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                          |
| PERIODIC_REPORTS.REPORT_TASK.BUILD_FAILURE | <p>A failure occurred while building periodic report '\$report_title'. This subscription has been removed from the scheduler.</p> <p>Critical。レポート エンジンがレポートを作成できない場合に送信されます。</p>                                                                                                                                                                                                                                                                                                                                                 | 「 <b>report_title</b> 」: レポートのタイトル                                                       |

表 29-7 発生する可能性があるシステム アラートのリスト (続き)

| アラート名                                                | メッセージと説明                                                                                                                    | パラメータ                                                |
|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|
| PERIODIC_REPORTS.<br>REPORT_TASK.EMAIL_<br>FAILURE   | A failure occurred while emailing periodic report '\$report_title'. This subscription has been removed from the scheduler.  | 「report_title」: レポートのタイトル                            |
|                                                      | Critical。レポートを電子メールで送信できなかった場合に送信されます。                                                                                      |                                                      |
| PERIODIC_REPORTS.<br>REPORT_TASK.ARCHIVE_FA<br>ILURE | A failure occurred while archiving periodic report '\$report_title'. This subscription has been removed from the scheduler. | 「report_title」: レポートのタイトル                            |
|                                                      | Critical。レポートをアーカイブできなかった場合に送信されます。                                                                                         |                                                      |
| SENDERBASE.ERROR                                     | Error processing response to query \$query: response was \$response                                                         | 「query」: クエリーするアドレス。<br>「response」: 受信した応答の raw データ。 |
|                                                      | Information。SenderBase からの応答を処理中にエラーが発生した場合に送信されます。                                                                         |                                                      |
| SMTPAUTH.FWD_SERVER_F<br>AILED_ALERT                 | SMTP Auth: could not reach forwarding server \$ip with reason: \$why                                                        | 「ip」: リモート サーバの IP。<br>「why」: エラーが発生した理由。            |
|                                                      | Warning。SMTP 認証転送サーバが到達不能である場合に送信されます。                                                                                      |                                                      |
| SMTPAUTH.LDAP_QUERY_F<br>AILED                       | SMTP Auth: LDAP query failed, see LDAP debug logs for details.                                                              |                                                      |
|                                                      | Warning。LDAP クエリーが失敗した場合に送信されます。                                                                                            |                                                      |
| SYSTEM.HERMES_<br>SHUTDOWN_FAILURE.<br>REBOOT        | While preparing to \${what}, failed to stop mail server gracefully: \${error} \$what:=reboot                                | 「error」: 発生したエラー。                                    |
|                                                      | Warning。再起動中のシステムをシャットダウンしている際に問題が発生した場合に送信されます。                                                                            |                                                      |
| SYSTEM.HERMES_<br>SHUTDOWN_FAILURE.<br>SHUTDOWN      | While preparing to \${what}, failed to stop mail server gracefully: \${error} \$what:=shut down                             | 「error」: 発生したエラー。                                    |
|                                                      | Warning。システムをシャットダウンしている際に問題が発生した場合に送信されます。                                                                                 |                                                      |
| SYSTEM.<br>RCPTVALIDATION.UPDATE_<br>FAILED          | Error updating recipient validation data: \$why                                                                             | 「why」: エラー メッセージ。                                    |
|                                                      | Critical。受信者検証のアップデートに失敗した場合に送信されます。                                                                                        |                                                      |

表 29-7 発生する可能性があるシステム アラートのリスト (続き)

| アラート名                          | メッセージと説明                                                   | パラメータ                       |
|--------------------------------|------------------------------------------------------------|-----------------------------|
| SYSTEM.SERVICE_TUNNEL.DISABLED | Tech support: Service tunnel has been disabled             |                             |
|                                | Information。Cisco サポート サービス用に作成されたトンネルがディセーブルの場合に送信されます。   |                             |
| SYSTEM.SERVICE_TUNNEL.ENABLED  | Tech support: Service tunnel has been enabled, port \$port | 「port」: サービス トンネルに使用されるポート。 |
|                                | Information。Cisco サポート サービス用に作成されたトンネルがイネーブルの場合に送信されます。    |                             |

## アップデート アラート

表 29-8 に、AsyncOS で生成される可能性があるさまざまなアップデート アラートのリストを示します。

表 29-8 発生する可能性があるアップデート アラートのリスト

| アラート名                                  | メッセージと説明                                                                                                                                                                                                                    | パラメータ                                                       |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|
| UPDATER.APP.UPDATE_ABORTED             | \$app abandoning updates until a new version is published. The \$app application tried and failed \$attempts times to successfully complete an update. This may be due to a network configuration issue or temporary outage | 「app」: アプリケーションの名前。<br>「attempts」: 試行した回数。                  |
|                                        | Warning。アプリケーションはアップデートを中止しています。                                                                                                                                                                                            |                                                             |
| UPDATER.UPDATERD.MANIFEST_FAILED_ALERT | The updater has been unable to communicate with the update server for at least \$threshold.                                                                                                                                 | 「threshold」: 人間が読み取れるしきい値の文字列。                              |
|                                        | Warning。サーバのマニフェストの取得に失敗しました。                                                                                                                                                                                               |                                                             |
| UPDATER.UPDATERD.RELEASE_NOTIFICATION  | \$mail_text                                                                                                                                                                                                                 | 「mail_text」: 通知するテキスト。<br>「notification_subject」: 通知するテキスト。 |
|                                        | Warning。リリースの通知です。                                                                                                                                                                                                          |                                                             |
| UPDATER.UPDATERD.UPDATE_FAILED         | Unknown error occurred: \$traceback                                                                                                                                                                                         | 「traceback」: トレースバック。                                       |
|                                        | Critical。アップデートの実行に失敗しました。                                                                                                                                                                                                  |                                                             |

## アウトブレイク フィルタ アラート

表 29-9 に、AsyncOS で生成される可能性があるさまざまなアウトブレイク フィルタに関するアラートのリストを示します。この表には、アラートの説明とアラートの重大度が記載されています。アウトブレイク フィルタは、隔離（具体的にはアウトブレイク隔離）で使用されるシステム アラートでも参照される場合があることに注意してください。

表 29-9 発生する可能性があるアウトブレイク フィルタ アラートのリスト

| アラート名                   | メッセージと説明                                                                                                                                                                                                                                                  | パラメータ                                                                                               |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| VOF.GTL_THRESHOLD_ALERT | Cisco Outbreak Filters Rule Update Alert:\$stext All rules last updated at: \$stime on \$date.                                                                                                                                                            | 「 <b>text</b> 」: アップデートアラートのテキスト。<br>「 <b>time</b> 」: 最終アップデートの時刻。<br>「 <b>date</b> 」: 最終アップデートの日付。 |
|                         | Information。アウトブレイク フィルタのしきい値が変更された場合に送信されます。                                                                                                                                                                                                             |                                                                                                     |
| AS.UPDATE_FAILURE       | \$engine update unsuccessful.This may be due to transient network or DNS issues, HTTP proxy configuration causing update transmission errors or unavailability of downloads.ironport.com.The specific error on the appliance for this failure is: \$error | 「 <b>engine</b> 」: アップデートに失敗したエンジン。<br>「 <b>error</b> 」: 発生したエラー。                                   |
|                         | Warning。アンチスパム エンジンまたは CASE ルールのアップデートに失敗した場合に送信されます。                                                                                                                                                                                                     |                                                                                                     |

## クラスタリング アラート

表 29-9 に、AsyncOS で生成される可能性があるさまざまなクラスタリングに関するアラートのリストを示します。この表には、アラートの説明とアラートの重大度が記載されています。

表 29-10 発生する可能性があるクラスタリング アラートのリスト

| アラート名                       | メッセージと説明                                                                                                                     | パラメータ                                                                                                           |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| CLUSTER.CC_ERROR.AUTH_ERROR | Error connecting to cluster machine \$name at IP \$ip - \$error - \$why\$error:=Machine does not appear to be in the cluster | 「 <b>name</b> 」: マシンのホスト名およびシリアル番号（またはいずれか）。<br>「 <b>ip</b> 」: リモート ホストの IP。<br>「 <b>why</b> 」: エラーに関する詳細なテキスト。 |
|                             | Critical。認証エラーが発生した場合に送信されます。マシンがクラスタのメンバでない場合に起きる可能性があります。                                                                  |                                                                                                                 |



表 29-10 発生する可能性があるクラスタリングアラートのリスト（続き）

| アラート名                           | メッセージと説明                                                                                                                       | パラメータ                                                   |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------|
| CLUSTER.CC_ERROR.DROPPED        | Error connecting to cluster machine \$name at IP \$ip - \$error - \$why\$error:=Existing connection dropped                    | 「name」：マシンのホスト名およびシリアル番号（またはいずれか）。<br>「ip」：リモートホストの IP。 |
|                                 | Warning。クラスタへの接続がドロップされた場合に送信されます。                                                                                             | 「why」：エラーに関する詳細なテキスト。                                   |
| CLUSTER.CC_ERROR.FAILED         | Error connecting to cluster machine \$name at IP \$ip - \$error - \$why\$error:=Connection failure                             | 「name」：マシンのホスト名およびシリアル番号（またはいずれか）。<br>「ip」：リモートホストの IP。 |
|                                 | Warning。クラスタへの接続に失敗した場合に送信されます。                                                                                                | 「why」：エラーに関する詳細なテキスト。                                   |
| CLUSTER.CC_ERROR.FORWARD_FAILED | Error connecting to cluster machine \$name at IP \$ip - \$error - \$why\$error:=Message forward failed, no upstream connection | 「name」：マシンのホスト名およびシリアル番号（またはいずれか）。<br>「ip」：リモートホストの IP。 |
|                                 | Critical。アプリケーションがクラスタのマシンにデータを転送できなかった場合に送信されます。                                                                              | 「why」：エラーに関する詳細なテキスト。                                   |
| CLUSTER.CC_ERROR.NOROUTE        | Error connecting to cluster machine \$name at IP \$ip - \$error - \$why\$error:=No route found                                 | 「name」：マシンのホスト名およびシリアル番号（またはいずれか）。<br>「ip」：リモートホストの IP。 |
|                                 | Critical。マシンがクラスタの別のマシンへのルートを取得できなかった場合に送信されます。                                                                                | 「why」：エラーに関する詳細なテキスト。                                   |
| CLUSTER.CC_ERROR.SSH_KEY        | Error connecting to cluster machine \$name at IP \$ip - \$error - \$why\$error:=Invalid host key                               | 「name」：マシンのホスト名およびシリアル番号（またはいずれか）。<br>「ip」：リモートホストの IP。 |
|                                 | Critical。無効な SSH ホストキーがあった場合に送信されます。                                                                                           | 「why」：エラーに関する詳細なテキスト。                                   |

表 29-10 発生する可能性があるクラスタリングアラートのリスト (続き)

| アラート名                            | メッセージと説明                                                                                                          | パラメータ                                                                                               |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| CLUSTER.CC_ERROR.TIMEOUT         | Error connecting to cluster machine \$name at IP \$ip - \$error - \$why\$error:=Operation timed out               | <p>「name」: マシンのホスト名およびシリアル番号 (またはいずれか)。</p> <p>「ip」: リモートホストの IP。</p> <p>「why」: エラーに関する詳細なテキスト。</p> |
|                                  | Warning。指定された操作がタイムアウトした場合に送信されます。                                                                                |                                                                                                     |
| CLUSTER.CC_ERROR_NOIP            | Error connecting to cluster machine \$name - \$error - \$why                                                      | <p>「name」: マシンのホスト名およびシリアル番号 (またはいずれか)。</p> <p>「why」: エラーに関する詳細なテキスト。</p>                           |
|                                  | Critical。アプライアンスがクラスタの別のマシンの有効な IP アドレスを取得できなかった場合に送信されます。                                                        |                                                                                                     |
| CLUSTER.CC_ERROR_NOIP.AUTH_ERROR | Error connecting to cluster machine \$name - \$error - \$why\$error:=Machine does not appear to be in the cluster | <p>「name」: マシンのホスト名およびシリアル番号 (またはいずれか)。</p> <p>「why」: エラーに関する詳細なテキスト。</p>                           |
|                                  | Critical。クラスタのマシンに接続する際に認証エラーが発生した場合に送信されます。マシンがクラスタのメンバーでない場合に起きる可能性があります。                                       |                                                                                                     |
| CLUSTER.CC_ERROR_NOIP.DROPPED    | Error connecting to cluster machine \$name - \$error - \$why\$error:=Existing connection dropped                  | <p>「name」: マシンのホスト名およびシリアル番号 (またはいずれか)。</p> <p>「why」: エラーに関する詳細なテキスト。</p>                           |
|                                  | Warning。マシンがクラスタの別のマシンの有効な IP アドレスを取得できず、クラスタへの接続がドロップした場合に送信されます。                                                |                                                                                                     |
| CLUSTER.CC_ERROR_NOIP.FAILED     | Error connecting to cluster machine \$name - \$error - \$why\$error:=Connection failure                           | <p>「name」: マシンのホスト名およびシリアル番号 (またはいずれか)。</p> <p>「why」: エラーに関する詳細なテキスト。</p>                           |
|                                  | Warning。不明な接続エラーが発生し、マシンがクラスタの別のマシンの有効な IP アドレスを取得できなかった場合に送信されます。                                                |                                                                                                     |

表 29-10 発生する可能性があるクラスタリングアラートのリスト（続き）

| アラート名                                | メッセージと説明                                                                                                            | パラメータ                                                                           |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| CLUSTER.CC_ERROR_NOIP.FORWARD_FAILED | Error connecting to cluster machine \$name - \$error - \$why\$error:=Message forward failed, no upstream connection | <p>「name」：マシンのホスト名およびシリアル番号（またはいずれか）。</p> <p>「why」：エラーに関する詳細なテキスト。</p>          |
|                                      | Critical。マシンがクラスタの別のマシンの有効な IP アドレスを取得できず、アプライアンスがマシンにデータを転送できなかった場合に送信されます。                                        |                                                                                 |
| CLUSTER.CC_ERROR_NOIP.NOROUTE        | Error connecting to cluster machine \$name - \$error - \$why\$error:=No route found                                 | <p>「name」：マシンのホスト名およびシリアル番号（またはいずれか）。</p> <p>「why」：エラーに関する詳細なテキスト。</p>          |
|                                      | Critical。マシンがクラスタの別のマシンの有効な IP アドレスを取得できず、別のマシンへのルートを取得できなかった場合に送信されます。                                             |                                                                                 |
| CLUSTER.CC_ERROR_NOIP.SSH_KEY        | Error connecting to cluster machine \$name - \$error - \$why\$error:=Invalid host key                               | <p>「name」：マシンのホスト名およびシリアル番号（またはいずれか）。</p> <p>「why」：エラーに関する詳細なテキスト。</p>          |
|                                      | Critical。マシンがクラスタの別のマシンの有効な IP アドレスを取得できず、有効な SSH ホスト キーを取得できなかった場合に送信されます。                                         |                                                                                 |
| CLUSTER.CC_ERROR_NOIP.TIMEOUT        | Error connecting to cluster machine \$name - \$error - \$why\$error:=Operation timed out                            | <p>「name」：マシンのホスト名およびシリアル番号（またはいずれか）。</p> <p>「why」：エラーに関する詳細なテキスト。</p>          |
|                                      | Warning。マシンがクラスタの別のマシンの有効な IP アドレスを取得できず、指定された操作がタイムアウトした場合に送信されます。                                                 |                                                                                 |
| CLUSTER.SYNC.PUSH_ALERT              | Overwriting \$sections on machine \$name                                                                            | <p>「name」：マシンのホスト名およびシリアル番号（またはいずれか）。</p> <p>「sections」：送信中のクラスタ セクションのリスト。</p> |
|                                      | Critical。設定データが同期から外れ、リモートホストに送信された場合に送信されます。                                                                       |                                                                                 |

## ネットワーク設定値の変更

この項では、Cisco アプライアンスのネットワーク操作の設定に使用する機能について説明します。これらの機能では、「システム セットアップ ウィザードの使用方法」(P.3-12) でシステム セットアップ ウィザード (または `systemsetup` コマンド) を利用して設定したホスト名、DNS、およびルーティングの設定値に直接アクセスできます。

ここでは、次の機能について説明します。

- `sethostname`
- DNS 設定 (GUI および `dnsconfig` コマンドを利用)
- ルーティング設定 (GUI、`routeconfig` コマンドおよび `setgateway` コマンドを利用)
- `dnsflush`
- パスワード
- ネットワーク アクセス
- ログイン バナー

## システム ホスト名の変更

ホスト名は、CLI プロンプトでシステムを識別する際に使用されます。完全修飾ホスト名を入力する必要があります。`sethostname` コマンドは、Cisco アプライアンスの名前を設定します。新規ホスト名は、`commit` コマンドを発行して初めて有効になります。

### sethostname コマンド

```
oldname.example.com> sethostname
```

```
[oldname.example.com]> mail3.example.com
```

```
oldname.example.com>
```

ホスト名の変更を有効にするには、`commit` コマンドを入力する必要があります。ホスト名の変更を確定すると、CLI プロンプトに新しいホスト名が表示されます。

```
oldname.example.com> commit
```

```
Please enter some comments describing your changes:
```

```
[]> Changed System Hostname
```

```
Changes committed: Mon Jan 01 12:00:01 2003
```

プロンプトに新規ホスト名が次のように表示されます。mail3.example.com>

## ドメイン ネーム システム (DNS) 設定値の設定

GUI の [ネットワーク (Network)] メニューの [DNS] ページまたは `dnsconfig` コマンドで、Cisco アプライアンスの DNS 設定値を設定できます。

次の設定値を設定できます。

- インターネットの DNS サーバまたはユーザ独自の DNS サーバを利用するか、および使用する具体的なサーバ
- DNS トラフィックに使用するインターフェイス
- 逆引き DNS ルックアップがタイムアウトするまでに待機する秒数
- DNS キャッシュのクリア

### DNS サーバの指定

Cisco AsyncOS では、インターネットのルート DNS サーバ、ユーザ独自の DNS サーバ、またはインターネットのルート DNS サーバおよび指定した権威 DNS サーバを使用できます。インターネットのルート サーバを使用するときは、特定のドメインに使用する代替サーバを指定することもできます。代替 DNS サーバは単一のドメインに適用されるため、当該ドメインに対する権威サーバ（最終的な DNS レコードを提供）である必要があります。

AsyncOS では、インターネットの DNS サーバを使用しない場合に「スプリット」DNS サーバをサポートしています。ユーザ独自の内部サーバを使用している場合は、例外のドメインおよび関連する DNS サーバを指定することもできます。

「スプリット」DNS を設定しているときは、`in-addr.arpa` (PTR) エントリも同様に設定する必要があります。このため、たとえば「`.eng`」クエリーをネームサーバ `1.2.3.4` にリダイレクトする際に、すべての `.eng` エントリが `172.16` ネットワークにある場合、スプリット DNS 設定に「`eng,16.172.in-addr.arpa`」を指定する必要があります。

### 複数エントリとプライオリティ

入力する各 DNS サーバに、数値でプライオリティを指定できます。AsyncOS では、プライオリティが 0 に最も近い DNS サーバの使用を試みます。DNS サーバが応答しない場合、AsyncOS は次のプライオリティを持つサーバの使用を試みます。同じプライオリティを持つ DNS サーバに複数のエントリを指定する場合、システムはクエリーを実行するたびに同じプライオリティを持つ DNS サーバをリストからランダムに選びます。システムは最初のクエリーの有効期限が切れるか「タイムアウト」するまで短時間待機し、その後次のクエリーに対しては前回よりも少し長い時間待機します。その後も同様です。待機時間は、DNS サーバの正確な合計数と設定されているプライオリティに依存します。タイムアウトの長さはプライオリティに関係なく、すべての IP アドレスで同じです。最初のプライオリティには最も短いタイムアウトが設定されており、次のプライオリティにはより長いタイムアウトが設定されています。最終的なタイムアウト時間は約 60 秒です。1 つのプライオリティを設定している場合、該当のプライオリティに対する各サーバのタイムアウトは 60 秒になります。2 つのプライオリティを設定している場合、最初のプライオリティに対する各サーバのタイムアウトは 15 秒になり、次のプライオリティに対する各サーバのタイムアウトは 45 秒になります。プライオリティが 3 つの場合、タイムアウトは 5 秒、10 秒、45 秒になります。

たとえば、4 つの DNS サーバを設定し、2 つにプライオリティ 0 を、1 つにプライオリティ 1 を、もう 1 つにプライオリティ 2 を設定したとします。

表 29-11 DNS サーバ、プライオリティ、およびタイムアウト間隔の例

| プライオリティ | サーバ             | タイムアウト (秒) |
|---------|-----------------|------------|
| 0       | 1.2.3.4、1.2.3.5 | 5、5        |
| 1       | 1.2.3.6         | 10         |
| 2       | 1.2.3.7         | 45         |

AsyncOS は、プライオリティ 0 に設定された 2 つのサーバをランダムに選択します。プライオリティ 0 のサーバが 1 つダウンしている場合、もう 1 つのサーバが使用されます。プライオリティ 0 のサーバが両方ダウンしている場合、プライオリティ 1 のサーバ (1.2.3.6) が使用され、最終的にプライオリティ 2 (1.2.3.7) のサーバが使用されます。

タイムアウト時間はプライオリティ 0 のサーバは両方とも同じであり、プライオリティ 1 のサーバにはより長い時間が設定され、プライオリティ 2 のサーバにはさらに長い時間が設定されます。

## インターネット ルート サーバの使用

Cisco AsyncOS DNS リゾルバは、高性能な電子メール配信に必要な大量の同時 DNS 接続を収容できるように設計されています。



(注)

デフォルト DNS サーバにインターネット ルート サーバ以外を設定することを選択した場合、設定されたサーバは権威サーバとなっていないドメインのクエリを再帰的に解決できる必要があります。

## 逆引き DNS ルックアップのタイムアウト

Cisco アプライアンスは電子メールの送受信の際、リスナーに接続しているすべてのリモート ホストに対して「二重 DNS ルックアップ」の実行を試みます (二重 DNS ルックアップを実行することで、システムはリモート ホストの IP アドレスの正当性を確保および検証します。これは、接続元ホストの IP アドレスに対する逆引き DNS (PTR) ルックアップと、それに続く PTR ルックアップ結果に対する正引き DNS (A) ルックアップからなります。その後、システムは A ルックアップの結果が PTR ルックアップの結果と一致するかどうかをチェックします。結果が一致しない場合、または A レコードが存在しない場合は、システムは IP アドレスのみを使用してホスト アクセス テーブル (HAT) 内のエントリと照合します)。この特別なタイムアウト時間は上記ルックアップのみに適用され、「複数エントリとプライオリティ」(P.29-53) で説明している一般的な DNS タイムアウトとは関係ありません。

デフォルト値は、20 秒です。秒数に 0 を入力することで、すべてのリスナーに対してグローバルに逆引き DNS ルックアップのタイムアウトをディセーブルにできます。

値を 0 秒に設定した場合、逆引き DNS ルックアップは試行されず、代わりに標準のタイムアウト応答がすぐに返されます。また、受信ホストの証明書にホストの IP ルックアップにマッピングされた一般名 (CN) がある場合、TLS 認証接続を求めるドメインにアプライアンスがメールを送信するのを防止します。

## DNS アラート

アプライアンスの再起動時に、メッセージ「Failed to bootstrap the DNS cache」が付与されたアラートが生成される場合がたまにあります。メッセージは、システムによるプライマリ DNS サーバへの問い合わせができなかったことを示しています。この事象は、ネットワーク接続が確立される前に DNS サ

ブシステムがオンラインになった場合、ブートのタイミングで発生します。このメッセージが別のタイミングで表示された場合、ネットワーク問題が発生しているか、または DNS 設定で有効なサーバが指定されていないことを示しています。

## DNS キャッシュのクリア

GUI の [キャッシュをクリア (Clear Cache)] ボタン、または `dnsflush` コマンドを使用して、DNS キャッシュのすべての情報をクリアします (`dnsflush` コマンドの詳細については、『*Cisco AsyncOS CLI Reference Guide*』を参照してください)。ローカル DNS システムが変更された際に、この機能を使用できます。コマンドはすぐに実行され、キャッシュの再投入中に一時的に性能が低下する可能性があります。

## グラフィカル ユーザ インターフェイスを使用した DNS 設定値の設定

### 手順

- ステップ 1** [ネットワーク (Network)] > [DNS] を選択します。
- ステップ 2** [設定を編集 (Edit Settings)] をクリックします。
- ステップ 3** インターネットのルート DNS サーバまたはユーザ独自の DNS サーバを使用するか、またはインターネットのルート DNS サーバを使用して代替 DNS サーバを指定するかを選択します。
- ステップ 4** ユーザ独自の DNS サーバを使用する場合は、サーバ ID を入力し [行を追加 (Add Row)] をクリックします。各サーバでこの作業を繰り返します。ユーザ独自の DNS サーバを入力する場合は、プライオリティも同時に指定します。詳細については、「DNS サーバの指定」(P.29-53) を参照してください。
- ステップ 5** あるドメインに対して代替 DNS サーバを指定する場合は、ドメインと代替 DNS サーバの IP アドレスを入力します。[行を追加 (Add Row)] をクリックし、ドメインを追加します。



(注) ドメイン名をカンマで区切ることで、1 つの DNS サーバに対して複数のドメインを入力できます。IP アドレスをカンマで区切ることで、複数の DNS サーバを入力することもできます。

- ステップ 6** DNS トラフィック用のインターフェイスを選択します。
- ステップ 7** 逆引き DNS ルックアップを中止するまでに待機する秒数を入力します。
- ステップ 8** [キャッシュをクリア (Clear Cache)] をクリックして、DNS キャッシュをクリアすることもできます。
- ステップ 9** 変更内容を送信し、確定します。

## TCP/IP トラフィック ルートの設定

一部のネットワーク環境では、標準のデフォルト ゲートウェイ以外のトラフィック ルートを使用する必要があります。GUI の [ネットワーク (Network)] タブの [ルーティング (Routing)] ページ、または CLI の `routeconfig` コマンドから、スタティック ルートを管理できます。

## GUI を使用したスタティック ルートの管理

[ ネットワーク (Network) ] タブの [ ルーティング (Routing) ] ページから、スタティック ルートの作成、編集または削除ができます。電子メールセキュリティアプライアンスでは、インターネットプロトコルバージョン 4 (IPv4) およびインターネットプロトコルバージョン 6 (IPv6) スタティック ルートの両方を使用できるため、[ ルーティング (Routing) ] ページでそれぞれ作成および管理ができます。このページからデフォルトの IPv4 および IPv6 ゲートウェイも変更できます。

### スタティック ルートの追加

#### 手順

- ステップ 1** [ ルーティング (Routing) ] ページで作成するスタティック ルートのタイプのために、[ ルートを追加 (Add Route) ] をクリックします。[ スタティックルートを追加 (Add Static Route) ] ページが表示されます。
- ステップ 2** ルートの名前を入力します。
- ステップ 3** 宛先 IP アドレスを入力します。
- ステップ 4** ゲートウェイの IP アドレスを入力します。
- ステップ 5** 変更内容を送信し、確定します。

### スタティック ルートの削除

#### 手順

- ステップ 1** [ スタティック ルート (Static Routes) ] のリストから、スタティック ルート名に対応するゴミ箱アイコンをクリックします。
- ステップ 2** 表示される警告ダイアログで [ 削除 (Delete) ] をクリックして、削除を確定します。
- ステップ 3** 変更内容を確定します。

### スタティック ルートの編集

#### 手順

- ステップ 1** [ スタティック ルート (Static Routes) ] のリストでルートの名前をクリックします。
- ステップ 2** ルートの設定を変更します。
- ステップ 3** 変更内容を確定します。



## デフォルト ゲートウェイの変更

### 手順

- 
- ステップ 1** [ルーティング (Routing)] ページで変更するインターネット プロトコル バージョンのために、ルート リストで [デフォルト ルート (Default Route)] をクリックします。
  - ステップ 2** ゲートウェイの IP アドレスを変更します。
  - ステップ 3** 変更内容を送信し、確定します。
- 

## デフォルト ゲートウェイの設定

GUI の [ネットワーク (Network)] メニューの [スタティック ルート (Static Routes)] ページ ([「デフォルト ゲートウェイの変更」\(P.29-57\)](#) を参照) または CLI の `setgateway` コマンドから、デフォルト ゲートウェイを設定できます。

## システム時刻

Cisco アプライアンスのシステム時刻の設定、使用する時間帯の設定、または NTP サーバとクエリー インターフェ이스の選択を行うには、GUI の [システム管理 (System Administration)] メニューから [タイム ゾーン (Time Zone)] ページまたは [時刻設定 (Time Settings)] ページを使用するか、CLI の `ntpconfig` コマンド、`settime` コマンドおよび `settz` コマンドを使用します。

AsyncOS で使用される時間帯ファイルは、[システム管理 (System Administration)] > [時刻設定 (Time Settings)] ページ、または `tzupdate` CLI コマンドで確認することもできます。

## 時間帯の選択

[タイム ゾーン (Time Zone)] ページ (GUI の [システム管理 (System Administration)] メニューから利用可能) では、Cisco アプライアンスの時間帯を表示します。特定の時間帯または GMT オフセットを選択できます。

### 手順

- 
- ステップ 1** [システム管理 (System Administration)] > [タイム ゾーン (Time Zone)] ページで、[設定を編集 (Edit Settings)] をクリックします。
  - ステップ 2** 地域、国、および時間帯をプルダウン メニューから選択します。
  - ステップ 3** 変更内容を送信し、確定します。
-

## GMT オフセットの選択

### 手順

- 
- ステップ 1** [システム管理 (System Administration)] > [タイムゾーン (Time Zone)] ページで、[設定を編集 (Edit Settings)] をクリックします。
- ステップ 2** 地域のリストから [GMT オフセット (GMT Offset)] を選択します。
- ステップ 3** [タイムゾーン (Time Zone)] リストでオフセットを選択します。オフセットは、GMT (グリニッジ子午線) に達するために足し引きする必要がある時間を示しています。時間の前にマイナス記号 (「-」) が付いている場合、グリニッジ子午線の東側にあたります。プラス記号 (「+」) の場合、グリニッジ子午線の西側にあたります。
- ステップ 4** 変更内容を送信し、確定します。
- 

## 時刻設定の編集

次の方法の 1 つを使用して、Cisco アプライアンスの時間設定を編集できます。

- ネットワーク タイム プロトコル (NTP) を使用する
- 手動

## ネットワーク タイム プロトコル (NTP) を使用したアプライアンス システム時刻の設定

### 手順

- 
- ステップ 1** [システム管理 (System Administration)] > [時刻設定 (Time Settings)] ページに移動します。
- ステップ 2** [設定を編集 (Edit Settings)] をクリックします。
- ステップ 3** [時刻の設定方法 (Time Keeping Method)] セクションで、[NTP (Network Time Protocol) を使用 (Use Network Time Protocol)] を選択します。
- ステップ 4** NTP サーバのアドレスを入力し、[行を追加 (Add Row)] をクリックします。複数の NTP サーバを追加できます。
- ステップ 5** NTP サーバをリストから削除するには、サーバのゴミ箱アイコンをクリックします。
- ステップ 6** NTP クエリー用のインターフェイスを選択します。これは、NTP クエリーが発信される IP アドレスになります。
- ステップ 7** 変更内容を送信し、確定します。
- 

## アプライアンス システム時刻の手動設定

### 手順

- 
- ステップ 1** [システム管理 (System Administration)] > [時刻設定 (Time Settings)] ページに移動します。
- ステップ 2** [設定を編集 (Edit Settings)] をクリックします。

- ステップ 3** [時刻の設定方法 (Time Keeping Method) ] セクションで、[時刻を手動で設定 (Set Time Manually) ] を選択します。
- ステップ 4** 月、日、年、時、分、および秒を入力します。
- ステップ 5** [A.M.] または [P.M.] を選択します。
- ステップ 6** 変更内容を送信し、確定します。

## ビューのカスタマイズ

- 「お気に入りページの使用」 (P.29-59)
- 「ユーザ プリファレンスの設定」 (P.29-59)

## お気に入りページの使用

(ローカル認証された管理ユーザ限定) よく利用するページのクイック アクセス リストを作成できます。

| 目的                      | 操作内容                                                                                                                                           |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| お気に入りリストにページを追加する       | 追加するページに移動し、ウィンドウの右上部付近にある [お気に入り (My Favorites) ] メニューから [このページをお気に入りに追加 (Add This Page To My Favorites) ] を選択します。<br>お気に入りへの変更は確定操作は必要ありません。 |
| お気に入りの順序を変更する           | [お気に入り (My Favorites) ] > [お気に入りをすべて表示 (View All My Favorites) ] を選択し、適切な順序にお気に入りをドラッグします。                                                     |
| お気に入りを削除する              | [お気に入り (My Favorites) ] > [お気に入りをすべて表示 (View All My Favorites) ] を選択し、お気に入りを削除します。                                                             |
| お気に入りページに移動する           | ウィンドウの右上部付近にある [お気に入り (My Favorites) ] からページを選択します。                                                                                            |
| カスタム レポート ページを表示または作成する | 「[マイレポート (My Reports) ] ページ」 (P.26-4) を参照してください。                                                                                               |

## ユーザ プリファレンスの設定

ローカル ユーザは、言語などの各アカウントに固有のプリファレンス設定を定義できます。これらの設定は、ユーザがアプライアンスに最初にログインしたときにデフォルトで適用されます。プリファレンス設定はユーザごとに保存され、どのクライアントマシンからユーザがアプライアンスにログインしても同じです。

ユーザの設定を変更したけれども確定していない場合、再度ログインした際にデフォルト値に戻されません。



(注) この機能は、外部認証されたユーザは使用できません。これらのユーザは、[ オプション (Options) ] メニューから直接言語を選択できます。

### 手順

- ステップ 1** プリファレンス設定を定義するユーザ アカウントでアプライアンスにログインします。
- ステップ 2** [ オプション (Options) ] > [ 環境設定 (Preferences) ] を選択します。[ オプション (Options) ] メニューは、ウィンドウの上部右側にあります。
- ステップ 3** [ 設定を編集 (Edit Preferences) ] をクリックします。
- ステップ 4** 設定を行います。

| プリファレンス設定                                                        | 説明                                             |
|------------------------------------------------------------------|------------------------------------------------|
| 言語の表示 (Language Display)                                         | AsyncOS for Web が Web インターフェイスおよび CLI で使用する言語。 |
| ランディング ページ (Landing Page)                                        | アプライアンスにユーザ ログインしたときに表示されるページ。                 |
| 表示されるレポート時間範囲 (デフォルト) (Reporting Time Range Displayed (default)) | レポート タブにレポートを表示するデフォルトの時間範囲。                   |
| 表示されるレポート行数 (Number of Reporting Rows Displayed)                 | 各レポートにデフォルトで表示されるデータの行数。                       |

- ステップ 5** 変更内容を送信し、確定します。
- ステップ 6** ページ下部の [ 前のページに戻る (Return to previous page) ] リンクをクリックします。



## CHAPTER 30

# CLI による管理およびモニタリング

---

- 「CLI を使用した管理およびモニタリングの概要」 (P.30-1)
- 「CLI を使用したモニタリング」 (P.30-6)
- 「電子メール キューの管理」 (P.30-24)
- 「SNMP モニタリング」 (P.30-39)

## CLI を使用した管理およびモニタリングの概要

CLI を使用した電子メール セキュリティ アプライアンスの管理およびモニタリングには次のようなタスクがあります。

- メッセージ アクティビティのモニタリング。
  - アプライアンスが電子メール パイプラインで処理している未処理メッセージ、受信者、バウンス受信者の数
  - 最後の 1 分、5 分、または 15 分の間隔に基づくメッセージ配信またはバウンス メッセージの時間レート
- システム リソースのモニタリング 例：
  - メモリ使用量
  - ディスク容量
  - 接続数
- 簡易ネットワーク管理プロトコル (SNMP) を使用する、システムの機能障害のモニタリング。例：
  - ファン障害
  - 更新の失敗
  - 異常に高いアプライアンスの温度
- パイプライン内の電子メールの管理。例：
  - キュー内の受信者の削除
  - 別のホストへのメッセージのリダイレクト
  - 受信者の削除またはメッセージのリダイレクトによるキューのクリア
  - 電子メールの受信、送信、またはワーク キュー処理の一時停止または再開
  - 特定のメッセージの検索

## 使用可能なモニタリング コンポーネントの読み取り

- 「使用可能なモニタリング コンポーネントの読み取り」 (P.30-2)
- 「イベント カウンタの読み取り」 (P.30-2)
- 「システム ゲージの読み取り」 (P.30-4)
- 「配信およびバウンスされたメッセージのレートの読み取り」 (P.30-6)

## イベント カウンタの読み取り

カウンタは、システム内の各種イベントの現在までの合計を示します。カウンタごとに、そのカウンタのリセット以降、最後のシステム再起動以降、およびシステムの存続期間に発生したイベントの合計数を表示できます。

カウンタは、イベントが発生するごとに増加し、次の 3 つのバージョンで表示されます。

|                 |                                     |
|-----------------|-------------------------------------|
| <b>Reset</b>    | resetcounters コマンドによる最後のカウンタ リセット以降 |
| <b>Uptime</b>   | 最後のシステム再起動以降                        |
| <b>Lifetime</b> | Cisco アプライアンスの存続期間中の合計              |

表 30-1 に、Cisco アプライアンスをモニタするときを使用できるカウンタとその説明を示します。



(注)

これは、全体的なリストです。表示されるカウンタは、選択した表示オプションまたはコマンドによって異なります。このリストは参照用として使用してください。

表 30-1 カウンタ

| 統計                                 | 説明                                   |
|------------------------------------|--------------------------------------|
| <b>Receiving</b>                   |                                      |
| <b>Messages Received</b>           | 配信キューに受信されたメッセージ。                    |
| <b>Recipients Received</b>         | 受信されたすべてのメッセージの受信者。                  |
| <b>Generated Bounce Recipients</b> | システムによってバウンスが生成され、配信キューに挿入された対象の受信者。 |

表 30-1 カウンタ (続き)

| 統計                             | 説明                                                                                                                                                                                                             |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Rejection</b>               |                                                                                                                                                                                                                |
| <b>Rejected Recipients</b>     | 受信者アクセス テーブル (RAT) によって、または早期接続終了などの予期しないプロトコル ネゴシエーションによって配信キューへの受信を拒否された受信者。                                                                                                                                 |
| <b>Dropped Messages</b>        | フィルタ ドロップ アクションの一致によって配信キューへの受信を拒否されたメッセージ、またはブラック ホール キューイング リスナーによって受信されたメッセージ。エイリアス テーブル内の /dev/null エントリ宛てのメッセージは、ドロップされたメッセージと見なされます。アンチスパム フィルタリング (システムでイネーブルになっている場合) によってドロップされたメッセージも、このカウンタに計上されます。 |
| <b>Queue</b>                   |                                                                                                                                                                                                                |
| <b>Soft Bounced Events</b>     | ソフト バウンス イベントの数。複数回ソフト バウンスしたメッセージには、複数のソフト バウンス イベントが設定されます。                                                                                                                                                  |
| <b>Completion</b>              |                                                                                                                                                                                                                |
| <b>Completed Recipients</b>    | ハード バウンスされた受信者、配信された受信者、および削除された受信者の総合計。配信キューから削除されたすべての受信者。                                                                                                                                                   |
| <b>Hard Bounced Recipients</b> | DNS ハード バウンス、5XX ハード バウンス、フィルタ ハード バウンス、期限切れハード バウンス、およびその他のハード バウンスの総合計。受信者へのメッセージの配信に失敗し、配信がただちに終了となったものを表します。                                                                                               |
| <b>DNS Hard Bounces</b>        | 受信者へのメッセージの配信試行中に検出された DNS エラー。                                                                                                                                                                                |
| <b>5XX Hard Bounces</b>        | 受信者へのメッセージの配信試行中に、宛先メール サーバから「5XX」応答コードが返されたものを表します。                                                                                                                                                           |
| <b>Expired Hard Bounces</b>    | 配信キューに許容されている最大時間、または最大接続試行回数を超えているメッセージ受信者。                                                                                                                                                                   |
| <b>Filter Hard Bounces</b>     | 一致フィルタの bounce アクションによってプリエンプトされた受信者の配信。アンチスパム フィルタリング (システムでイネーブルになっている場合) によってドロップされたメッセージも、このカウンタに計上されます。                                                                                                   |
| <b>Other Hard Bounces</b>      | メッセージ配信中の予期しないエラー。または、メッセージ受信者が <code>bouncerecipients</code> コマンドによって明示的にバウンスされたものを表します。                                                                                                                      |
| <b>Delivered Recipients</b>    | メッセージが正常に配信された受信者。                                                                                                                                                                                             |
| <b>Deleted Recipients</b>      | <code>deleterecipients</code> コマンドによって明示的に削除されたメッセージ受信者、またはグローバル配信停止リストに合致するメッセージ受信者の合計。                                                                                                                       |
| <b>Global Unsubscribe Hits</b> | グローバル配信停止設定との一致により削除されたメッセージ受信者。                                                                                                                                                                               |
| <b>Current IDs</b>             |                                                                                                                                                                                                                |
| <b>Message ID (MID)</b>        | 配信キューに挿入されたメッセージに割り当てられた最後のメッセージ ID。MID は、Cisco アプライアンスによって受信されたすべてのメッセージに関連付けられており、メール ログで追跡できます。MID は、 $2^{31}$ でゼロにリセットされます。                                                                                |

表 30-1 カウンタ (続き)

| 統計                             | 説明                                                                                  |
|--------------------------------|-------------------------------------------------------------------------------------|
| Injection Connection ID (ICID) | リスナー インターフェイスへの接続に割り当てられた最後のインジェクション接続 ID。ICID は $2^{31}$ でロール オーバー (ゼロにリセット) されます。 |
| Delivery Connection ID (DCID)  | 宛先メール サーバへの接続に割り当てられた最後の配信接続 ID。DCID は $2^{31}$ でロール オーバー (ゼロにリセット) されます。           |

## システム ゲージの読み取り

ゲージは、メモリ、ディスク スペース、またはアクティブ接続などのシステム リソースの現在の使用率を示します。

表 30-2 に、Cisco アプライアンスをモニタするときに表示できるゲージとその説明を示します。



(注)

これは、全体的なリストです。表示されるゲージは、選択した表示オプションまたはコマンドによって異なります。このリストは参照用として使用してください。

表 30-2 ゲージ

| 統計                     | 説明                                                                                                                                                                                                                                                   |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System Gauges</b>   |                                                                                                                                                                                                                                                      |
| RAM Utilization        | システムによる物理 Random Access Memory (RAM; ランダム アクセス メモリ) の使用率。                                                                                                                                                                                            |
| CPU Utilization        | CPU 使用率。                                                                                                                                                                                                                                             |
| Disk I/O Utilization   | ディスク I/O の使用率。<br><br>(注) Disk I/O Utilization ゲージには、既知の値の測定は表示されません。このゲージには、これまでにシステムで確認され、最後の再起動以降の最大値に対して測定された I/O 使用率が表示されます。したがって、ゲージに 100 % と表示されている場合、システムでは起動後最も高いレベルの I/O 使用率が発生しています (必ずしも、システム全体の 100 % の物理ディスク I/O を表すものではありません)。        |
| Resource Conservation  | 0 ~ 60 または 999 の値。0 ~ 60 の数値は、重要なシステム リソースの急速な消費を防止するために、システムがメッセージの受け入れを減らしている度合いを表しています。数値が大きいほど、受け入れを減らす度合いが大きくなります。ゼロは、受け入れの減少がないことを示します。このゲージに 999 と表示されている場合、システムは「リソース節約モード」になっており、メッセージは受け入れられません。システムがリソース節約モードかどうかに関係なく、アラート メッセージは送信されます。 |
| Disk Utilization: Logs | ログに使用されているディスクの割合。ステータス ログには LogUsd、XML ステータスには log_used として表示されます。                                                                                                                                                                                  |



表 30-2 ゲージ (続き)

| 統計                                  | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Connections Gauges</b>           |                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Current Inbound Connections</b>  | リスナー インターフェイスへの現在の着信接続。                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Current Outbound Connections</b> | 宛先メール サーバへの現在の発信接続。                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Queue Gauges</b>                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Active Recipients</b>            | 配信キュー内のメッセージ受信者。Unattempted Recipients と Attempted Recipients の合計。                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Unattempted Recipients</b>       | Active Recipients のサブカテゴリ。配信がまだ試行されていない、キュー内のメッセージ受信者。                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Attempted Recipients</b>         | Active Recipients のサブカテゴリ。試行されたものの、ソフト バウンス イベントによって失敗した配信の対象となっている、キュー内のメッセージ受信者。                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Messages in Work Queue</b>       | キューに入る前に、エイリアス テーブル拡張、マスカレード、アンチスパム、アンチウイルス スキャン、メッセージ フィルタ、および LDAP クエリーによる処理を待つメッセージの数。                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Messages in Quarantine</b>       | 隔離エリア内にあるメッセージに、解放または削除されたが実際の処理がまだ行われていないメッセージを足した一意の数。たとえば、Outbreak からすべての隔離対象メッセージを解放すると、Outbreak の合計メッセージ数はただちにゼロになりますが、このフィールドでは、完全に配信されるまでの隔離対象メッセージが反映されます。                                                                                                                                                                                                                                                                                         |
| <b>Destinations in Memory</b>       | メモリ内の宛先ドメインの数。メッセージの配信先となる各ドメインに対して、宛先オブジェクトがメモリ内に作成されます。そのドメインに対するすべてのメールが配信された後、宛先オブジェクトは 3 時間保持されます。3 時間のうちに、そのドメインに対して新しいメッセージがバインドされなければ、オブジェクトは期限切れとなり、宛先は (tophosts コマンドなどで) 報告されなくなります。1 つのドメインだけにメールを配信する場合、このカウンタは「1」になります。メッセージを送信したことがない (または、長い時間アプライアンスによってメッセージが処理されていない) 場合、カウンタは「0」になります。<br><br>仮想ゲートウェイを使用している場合、各仮想ゲートウェイの宛先ドメインには別個の宛先オブジェクトが作成されます (たとえば、3 つの異なる仮想ゲートウェイから yahoo.com に配信している場合、yahoo.com が 3 つの宛先オブジェクトとしてカウントされます)。 |
| <b>Kilobytes Used</b>               | 使用されるキュー ストレージ (キロバイト単位)。                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Kilobytes in Quarantine</b>      | 隔離対象メッセージに使用されるキュー ストレージ。メッセージ サイズと、上記の Messages in Quarantine にカウントされている受信者ごとに 30 バイトを足した値になります。この計算では通常、使用されるスペースが過大に見積もられます。                                                                                                                                                                                                                                                                                                                            |
| <b>Kilobytes Free</b>               | 残りのキュー ストレージ (キロバイト単位)。                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## 配信およびバウンスされたメッセージのレートの読み取り

すべてのレートは、クエリーが作成された特定の時点における、1 時間あたりの平均イベント発生レートを示します。レートには、過去 1 分間、5 分間、および 15 分間という 3 つの間隔で 1 時間あたりの平均レートが計算されます。

たとえば、Cisco アプライアンスが 1 分で 100 の受信者を受信すると、1 分間隔に対するレートは 1 時間あたり 6,000 となります。5 分間隔に対するレートは 1 時間あたり 1,200 となり、15 分間隔に対するレートは 1 時間あたり 400 となります。レートは、1 分間のレートが継続した場合の 1 時間あたりの平均レートを示すように計算されます。したがって、1 分で 100 件のメッセージのほうが 15 分で 100 件のメッセージよりもレートは高くなります。

表 30-3 に、Cisco アプライアンスをモニタするときを使用できるレートとその説明を示します。



(注)

これは、全体的なリストです。表示されるレートは、選択した表示オプションまたはコマンドによって異なります。このリストは参照用として使用してください。

表 30-3 レート

| 統計                             | 説明                                                                                                                                          |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Messages Received</b>       | 1 時間あたりに配信キューに挿入されるメッセージのレート。                                                                                                               |
| <b>Recipients Received</b>     | 1 時間あたりに配信キューに挿入されるすべてのメッセージに対する受信者数のレート。                                                                                                   |
| <b>Soft Bounced Events</b>     | 1 時間あたりのソフト バウンス イベント数のレート (複数回ソフト バウンスしたメッセージには、複数のソフト バウンス イベントが設定されます)。                                                                  |
| <b>Completed Recipients</b>    | ハード バウンスされた受信者、配信された受信者、および削除された受信者の総合計のレート。配信キューから削除された受信者は、完了済みと見なされます。                                                                   |
| <b>Hard Bounced Recipients</b> | 1 時間あたりの DNS ハード バウンス、5XX ハード バウンス、フィルタ ハード バウンス、期限切れハード バウンス、およびその他のハード バウンスの総合計のレート。ハード バウンスとは、受信者へのメッセージの配信試行に失敗し、その配信がただちに終了されることをいいます。 |
| <b>Delivered Recipients</b>    | 受信者に正常に配信された 1 時間あたりのメッセージ数のレート。                                                                                                            |

## CLI を使用したモニタリング

- 「電子メール ステータスのモニタリング」 (P.30-7)
- 「詳細な電子メール ステータスのモニタリング」 (P.30-9)
- 「メール ホストのステータスのモニタリング」 (P.30-12)
- 「電子メール キューの構成の確認」 (P.30-16)
- 「リアルタイム アクティビティの表示」 (P.30-17)
- 「着信電子メール接続のモニタリング」 (P.30-20)
- 「DNS ステータスの確認」 (P.30-22)
- 「電子メール モニタリング カウンタのリセット」 (P.30-23)

- 「アクティブな TCP/IP サービスの識別」 (P.30-24)



(注)

グラフィカル ユーザ インターフェイス (GUI) で Cisco アプライアンスをモニタすることもできます。第 32 章「GUI でのその他の作業」を参照してください。

## 電子メール ステータスのモニタリング

Cisco アプライアンスにおける電子メール動作のステータスをモニタすることが必要になることがあります。status コマンドは、電子メール動作についてモニタされる情報のサブセットを返します。返された統計情報は、カウンタとゲージのいずれかの形式で表示されます。カウンタは、システム内の各種イベントの現在までの合計を示します。カウンタごとに、そのカウンタのリセット以降、最後のシステム再起動以降、およびシステムの存続期間に発生したイベントの合計数を表示できます。ゲージは、メモリ、ディスク スペース、またはアクティブ接続などのシステム リソースの現在の使用率を示します。

各項目の説明については、「CLI を使用した管理およびモニタリングの概要」 (P.30-1) を参照してください。

表 30-4 メール ステータス

| 統計                 | 説明                                                                                                                                                                |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Status as of       | 現在のシステム日時を表示します。                                                                                                                                                  |
| Last counter reset | カウンタが最後にリセットされた時刻を表示します。                                                                                                                                          |
| System status      | online、offline、receiving suspended、または delivery suspended。ステータスが receiving suspended になるのは、すべてのリスナーが一時停止した場合のみです。すべてのリスナーに対する受信と配信が一時停止されると、ステータスは offline になります。 |
| Oldest Message     | システムによる配信を待つ、最も古いメッセージを表示します。                                                                                                                                     |
| Features           | featurekey コマンドによってシステムにインストールされた特別な機能を表示します。                                                                                                                     |

## 例

```
mail3.example.com> status
```

```
Status as of: Thu Oct 21 14:33:27 2004 PDT
Up since: Wed Oct 20 15:47:58 2004 PDT (22h 45m 29s)
Last counter reset: Never
System status: Online
Oldest Message: 4 weeks 46 mins 53 secs
```

| Counters:                 | Reset      | Uptime  | Lifetime   |
|---------------------------|------------|---------|------------|
| Receiving                 |            |         |            |
| Messages Received         | 62,049,822 | 290,920 | 62,049,822 |
| Recipients Received       | 62,049,823 | 290,920 | 62,049,823 |
| Rejection                 |            |         |            |
| Rejected Recipients       | 3,949,663  | 11,921  | 3,949,663  |
| Dropped Messages          | 11,606,037 | 219     | 11,606,037 |
| Queue                     |            |         |            |
| Soft Bounced Events       | 2,334,552  | 13,598  | 2,334,552  |
| Completion                |            |         |            |
| Completed Recipients      | 50,441,741 | 332,625 | 50,441,741 |
| Current IDs               |            |         |            |
| Message ID (MID)          |            |         | 99524480   |
| Injection Conn. ID (ICID) |            |         | 51180368   |
| Delivery Conn. ID (DCID)  |            |         | 17550674   |

| Gauges:                | Current |
|------------------------|---------|
| Connections            |         |
| Current Inbound Conn.  | 0       |
| Current Outbound Conn. | 14      |

```
Queue

Active Recipients 7,166

Messages In Work Queue 0

Messages In Quarantine 16,248

Kilobytes Used 387,143

 Kilobytes In Quarantine 338,206

Kilobytes Free 39,458,745

mail3.example.com>
```

## 詳細な電子メール ステータスのモニタリング

`status detail` コマンドは、電子メール動作についてモニタされた詳細な情報を返します。返された統計情報は、カウンタ、レート、およびゲージのいずれかのカテゴリで表示されます。カウンタは、システム内の各種イベントの現在までの合計を示します。カウンタごとに、そのカウンタのリセット以降、最後のシステム再起動以降、およびシステムの存続期間に発生したイベントの合計数を表示できます。ゲージは、メモリ、ディスク スペース、またはアクティブ接続などのシステム リソースの現在の使用率を示します。すべてのレートは、クエリーが作成された特定の時点における、1 時間あたりの平均イベント発生レートを示します。レートには、過去 1 分間、5 分間、および 15 分間という 3 つの間隔で 1 時間あたりの平均レートが計算されます。各項目の説明については、「[CLI を使用した管理およびモニタリングの概要](#)」(P.30-1) を参照してください。

## 例

```
mail3.example.com> status detail

Status as of: Thu Jun 30 13:09:18 2005 PDT
Up since: Thu Jun 23 22:21:14 2005 PDT (6d 14h 48m 4s)
Last counter reset: Tue Jun 29 19:30:42 2004 PDT
System status: Online
Oldest Message: No Messages
Feature - IronPort Anti-Spam: 17 days
Feature - Sophos: Dormant/Perpetual
Feature - Outbreak Filters: Dormant/Perpetual
Feature - Central Mgmt: Dormant/Perpetual

Counters: Reset Uptime Lifetime

Receiving
 Messages Received 2,571,967 24,760 3,113,176
 Recipients Received 2,914,875 25,450 3,468,024
 Gen. Bounce Recipients 2,165 0 7,451

Rejection
 Rejected Recipients 1,019,453 792 1,740,603
 Dropped Messages 1,209,001 66 1,209,028

Queue
 Soft Bounced Events 11,236 0 11,405

Completion
 Completed Recipients 2,591,740 49,095 3,145,002
 Hard Bounced Recipients 2,469 0 7,875
 DNS Hard Bounces 199 0 3,235
 5XX Hard Bounces 2,151 0 4,520
 Expired Hard Bounces 119 0 120
```

```

 Filter Hard Bounces 0 0 0
 Other Hard Bounces 0 0 0
 Delivered Recipients 2,589,270 49,095 3,137,126
 Deleted Recipients 1 0 1
 Global Unsub. Hits 0 0 0
 DomainKeys Signed Msgs 10 9 10

Current IDs

 Message ID (MID) 7615199
 Injection Conn. ID (ICID) 3263654
 Delivery Conn. ID (DCID) 1988479

Rates (Events Per Hour): 1-Minute 5-Minutes 15-Minutes

Receiving

 Messages Received 180 300 188
 Recipients Received 180 300 188

Queue

 Soft Bounced Events 0 0 0

Completion

 Completed Recipients 360 600 368
 Hard Bounced Recipients 0 0 0
 Delivered Recipients 360 600 368

Gauges: Current

System

 RAM Utilization 1%
 CPU Utilization

 MGA 0%
 AntiSpam 0%

```

|                         |            |
|-------------------------|------------|
| AntiVirus               | 0%         |
| Disk I/O Utilization    | 0%         |
| Resource Conservation   | 0          |
| Connections             |            |
| Current Inbound Conn.   | 0          |
| Current Outbound Conn.  | 0          |
| Queue                   |            |
| Active Recipients       | 0          |
| Unattempted Recipients  | 0          |
| Attempted Recipients    | 0          |
| Messages In Work Queue  | 0          |
| Messages In Quarantine  | 19         |
| Destinations In Memory  | 3          |
| Kilobytes Used          | 473        |
| Kilobytes In Quarantine | 473        |
| Kilobytes Free          | 39,845,415 |



(注)

新たにインストールされたアプライアンスでは、最も古いメッセージカウンタにメッセージが示される場合がありますが、実際にはカウンタに示される受信者はありません。リモートホストが接続されており、メッセージの受信が非常に遅い（つまり、メッセージを受信するまでに数分かかる）場合には、受信された受信者カウンタに「0」と表示され、最も古いメッセージカウンタに「1」と表示されることがあります。これは、最も古いメッセージカウンタに進行中のメッセージが表示されるためです。接続が最終的にドロップされると、カウンタはリセットされます。

## メールホストのステータスのモニタリング

特定の受信者ホストへの配信に問題があると思われる場合や、仮想ゲートウェイアドレスに関する情報を収集する場合には、`hoststatus` コマンドを実行するとそれらの情報を表示できます。`hoststatus` コマンドは、特定の受信者ホストに関する電子メール動作のモニタリング情報を返します。コマンドには、取得するホスト情報のドメインを入力する必要があります。AsyncOS キャッシュに格納されている DNS 情報と、受信者ホストから最後に返されたエラーも表示されます。返されるデータは、最後に実行した `resetcounters` コマンドからの累積です。返される統計情報は、カウンタとゲージの 2 つのカテゴリに表示されます。各項目の説明については、「[CLI を使用した管理およびモニタリングの概要](#)」(P.30-1) を参照してください。



また、`hoststatus` コマンドに固有のその他のデータも返されます。

表 30-5 `hoststatus` コマンドのその他のデータ

| 統計                                  | 説明                                                                                                                                                                                                                             |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Pending Outbound Connections</b> | 開いている接続や作業中の接続とは対照的な、宛先メール ホストへの保留中、または「初期」接続。Pending Outbound Connections は、プロトコルのグリーティングの段階にまだ達していない接続です。                                                                                                                    |
| <b>Oldest Message</b>               | このドメインに対する配信キュー内で最も古いアクティブ受信者の経過時間。このカウンタは、ソフト バウンス イベントやホストの停止によって配信できない、キュー内のメッセージの経過時間を判断するのに役立ちます。                                                                                                                         |
| <b>Last Activity</b>                | このフィールドは、そのホストにメッセージ配信が試みられるたびに更新されます。                                                                                                                                                                                         |
| <b>Ordered IP Addresses</b>         | このフィールドには、IP アドレスの Time To Live (TTL; 存続可能時間)、MX レコードに応じた IP アドレスの優先順位、および実際のアドレスが表示されます。MX レコードは、ドメインに対するメール サーバの IP アドレスを指定します。1 つのドメインが複数の MX レコードを持つことができます。各 MX レコードのメール サーバには優先順位が割り当てられます。優先順位の数値が最も小さい MX レコードが優先されます。 |
| <b>Last 5XX error</b>               | このフィールドには、ホストから返された最新の「5XX」ステータス コードと説明が表示されます。このフィールドが表示されるのは、5XX エラーが存在する場合のみです。                                                                                                                                             |
| <b>MX Records</b>                   | MX レコードは、ドメインに対するメール サーバの IP アドレスを指定します。1 つのドメインが複数の MX レコードを持つことができます。各 MX レコードのメール サーバには優先順位が割り当てられます。優先順位の数値が最も小さい MX レコードが優先されます。                                                                                          |
| <b>SMTP Routes for this host</b>    | このドメインに対して SMTP ルートが定義されている場合は、ここに表示されます。                                                                                                                                                                                      |
| <b>Last TLS Error</b>               | このフィールドには、最新の発信 TLS 接続エラーの説明と、アプライアンスが確立を試みた TLS 接続のタイプが表示されます。このフィールドが表示されるのは、TLS エラーが存在する場合のみです。                                                                                                                             |

## 仮想ゲートウェイ

次の仮想ゲートウェイ情報は、仮想ゲートウェイ アドレスを設定している場合のみ表示されます（「[電子メールを受信するためのゲートウェイの設定](#)」を参照してください）。

表 30-6 `hoststatus` コマンドのその他の仮想ゲートウェイ データ

| 統計                    | 説明                                                                                                   |
|-----------------------|------------------------------------------------------------------------------------------------------|
| <b>Host up/down</b>   | 同じ名前のグローバル <code>hoststatus</code> フィールドと同じ定義。仮想ゲートウェイ アドレスごとに追跡されます。                                |
| <b>Last Activity</b>  | 同じ名前のグローバル <code>hoststatus</code> フィールドと同じ定義。仮想ゲートウェイ アドレスごとに追跡されます。                                |
| <b>Recipients</b>     | このフィールドも、グローバル <code>hoststatus</code> コマンドの定義に対応します。Active Recipients フィールド：仮想ゲートウェイ アドレスごとに追跡されます。 |
| <b>Last 5XX error</b> | このフィールドには、ホストから返された最新の 5XX ステータス コードと説明が表示されます。このフィールドが表示されるのは、5XX エラーが存在する場合のみです。                   |

## 例

```
mail3.example.com> hoststatus

Recipient host:

[]> aol.com

Host mail status for: 'aol.com'

Status as of: Tue Mar 02 15:17:32 2010

Host up/down: up

Counters:

Queue

 Soft Bounced Events 0

Completion

 Completed Recipients 1
 Hard Bounced Recipients 1
 DNS Hard Bounces 0
 5XX Hard Bounces 1
 Filter Hard Bounces 0
 Expired Hard Bounces 0
 Other Hard Bounces 0
 Delivered Recipients 0
 Deleted Recipients 0

Gauges:

Queue

 Active Recipients 0
 Unattempted Recipients 0
 Attempted Recipients 0
```

```

Connections

Current Outbound Connections 0

Pending Outbound Connections 0

Oldest Message No Messages

Last Activity Tue Mar 02 15:17:32 2010

Ordered IP addresses: (expiring at Tue Mar 02 16:17:32 2010)

Preference IPs

15 64.12.137.121 64.12.138.89 64.12.138.120

15 64.12.137.89 64.12.138.152 152.163.224.122

15 64.12.137.184 64.12.137.89 64.12.136.57

15 64.12.138.57 64.12.136.153 205.188.156.122

15 64.12.138.57 64.12.137.152 64.12.136.89

15 64.12.138.89 205.188.156.154 64.12.138.152

15 64.12.136.121 152.163.224.26 64.12.137.184

15 64.12.138.120 64.12.137.152 64.12.137.121

MX Records:

Preference TTL Hostname

15 52m24s mailin-01.mx.aol.com

15 52m24s mailin-02.mx.aol.com

15 52m24s mailin-03.mx.aol.com

15 52m24s mailin-04.mx.aol.com

Last 5XX Error:

550 REQUESTED ACTION NOT TAKEN: DNS FAILURE

(at Tue Mar 02 15:17:32 2010 GMT) IP: 10.10.10.10

```

```

Last TLS Error: Required - Verify

TLS required, STARTTLS unavailable
(at Tue Mar 02 15:17:32 2010 GMT) IP: 10.10.10.10

```

```
Virtual gateway information:
```

```

=====
example.com (PublicNet_017):
Host up/down: up
Last Activity Wed June 22 13:47:02 2005
Recipients 0

```



(注)

仮想ゲートウェイ アドレス情報は、altsrchost 機能を使用している場合のみ表示されます。

## 電子メール キューの構成の確認

電子メール キューに関する現在の情報を取得し、特定の受信者ホストに配信の問題（キューの増大など）があるかどうかを判断するには、tophosts コマンドを使用します。tophosts コマンドは、キュー内の上位 20 の受信者のリストを返します。リストは、アクティブ受信者、発信接続、配信済み受信者、ソフトバウンス イベント、およびハードバウンスされた受信者など、さまざまな統計情報別にソートできます。各項目の説明については、「[CLI を使用した管理およびモニタリングの概要](#)」(P.30-1) を参照してください。

## 例

```
mail3.example.com> tophosts

Sort results by:

1. Active Recipients
2. Connections Out
3. Delivered Recipients
4. Soft Bounced Events
5. Hard Bounced Recipients

[1]> 1

Status as of: Mon Nov 18 22:22:23 2003

 Active Conn. Deliv. Soft Hard
Recipient Host Recip Out Recip. Bounced Bounced
1 aol.com 365 10 255 21 8
2 hotmail.com 290 7 198 28 13
3 yahoo.com 134 6 123 11 19
4 excite.com 98 3 84 9 4
5 msn.com 84 2 76 33 29

mail3.example.com>
```

## リアルタイム アクティビティの表示

Cisco アプライアンスではリアルタイム モニタリングが可能であり、システムにおける電子メール アクティビティの進捗状況を確認できます。rate コマンドは、電子メール動作に関するリアルタイム モニタリング情報を返します。この情報は、ユーザが指定した間隔で定期的に更新されます。rate コマンドを停止するには、Ctrl+C を使用します。

表 30-7 に、表示されるデータを示します。

表 30-7 rate コマンドのデータ

| 統計                          | 説明                                                      |
|-----------------------------|---------------------------------------------------------|
| <b>Connections In</b>       | 着信接続の数。                                                 |
| <b>Connections Out</b>      | 発信接続の数。                                                 |
| <b>Recipients Received</b>  | システムに受信された受信者の合計数。                                      |
| <b>Recipients Completed</b> | 完了した受信者の合計数。                                            |
| <b>Delta</b>                | 最後のデータ アップデート以降変化した、Received 受信者数および Completed 受信者数の差異。 |
| <b>Queue Used</b>           | メッセージキューのサイズ (キロバイト単位)。                                 |

## 例

```
mail3.example.com> rate
```

```
Enter the number of seconds between displays.
```

```
[10]> 1
```

```
Hit Ctrl-C to return to the main prompt.
```

```
Time Connections Recipients Recipients Queue
 In Out Received Delta Completed Delta K-Used
23:37:13 10 2 41708833 0 40842686 0 64
23:37:14 8 2 41708841 8 40842692 6 105
23:37:15 9 2 41708848 7 40842700 8 76
23:37:16 7 3 41708852 4 40842705 5 64
23:37:17 5 3 41708858 6 40842711 6 64
23:37:18 9 3 41708871 13 40842722 11 67
23:37:19 7 3 41708881 10 40842734 12 64
23:37:21 11 3 41708893 12 40842744 10 79
^C
```

hostrate コマンドは、特定のメール ホストに関するリアルタイムのモニタリング情報を返します。この情報は、status detail コマンドのサブセットです（「[詳細な電子メール ステータスのモニタリング](#)」(P.30-9) を参照）。

表 30-8 hostrate コマンドのデータ

| 統計                               | 説明                                                    |
|----------------------------------|-------------------------------------------------------|
| Host Status                      | 特定のホストの現在のステータス (up、down、または unknown)。                |
| Current Connections Out          | ホストに対する現在の発信接続数。                                      |
| Active Recipients in Queue       | キュー内の特定のホストに対するアクティブ受信者の合計数。                          |
| Active Recipients in Queue Delta | 最後の既知のホスト ステータス以降変化した、キュー内の特定のホストに対するアクティブ受信者の合計数の差異。 |
| Delivered Recipients Delta       | 最後の既知のホスト ステータス以降変化した、キュー内の特定のホストに対する配信済み受信者の合計数の差異。  |

表 30-8 hostrate コマンドのデータ

| 統計                                   | 説明                                                          |
|--------------------------------------|-------------------------------------------------------------|
| <b>Hard Bounced Recipients Delta</b> | 最後の既知のホスト ステータス以降変化した、キュー内の特定のホストに対するハード バウンスされた受信者の合計数の差異。 |
| <b>Soft Bounce Events Delta</b>      | 最後の既知のホスト ステータス以降変化した、キュー内の特定のホストに対するソフト バウンスされた受信者の合計数の差異。 |

hostrate コマンドを停止するには、Ctrl+C を使用します。

## 例

```
mail3.example.com> hostrate
```

```
Recipient host:
```

```
[]> aol.com
```

```
Enter the number of seconds between displays.
```

```
[10]> 1
```

```

 Time Host CrtCncOut ActvRcp ActvRcp DlvRcp HrdBncRcp SftBncEvt
 Status Delta Delta Delta Delta
23:38:23 up 1 0 0 4 0 0
23:38:24 up 1 0 0 4 0 0
23:38:25 up 1 0 0 12 0 0
^C

```

## 着信電子メール接続のモニタリング

大量の送信者を識別するため、またはシステムへの着信接続をトラブルシューティングするために、Cisco アプライアンスに接続しているホストのモニタが必要になる場合があります。topin コマンドは、システムに接続しているリモート ホストのスナップショットを示します。このスナップショットには、



特定のリスナーに接続しているリモート IP アドレスごとに 1 つの行を持つテーブルが表示されます。同じ IP アドレスから異なるリスナーへの 2 つの接続に対しては、テーブルに 2 つの行が作成されます。表 30-9 に、`topin` コマンドを使用したときに表示されるフィールドの説明を示します。

表 30-9 `topin` コマンドのデータ

| 統計                       | 説明                                                |
|--------------------------|---------------------------------------------------|
| <b>Remote Hostname</b>   | リモートホストのホスト名。リバース DNS ルックアップによって取得されます。           |
| <b>Remote IP Address</b> | リモートホストの IP アドレス。                                 |
| <b>listener</b>          | 接続を受信している、Cisco アプライアンス上のリスナーのニックネーム。             |
| <b>Connections In</b>    | コマンドが実行されたときに開いていた、指定の IP アドレスを持つリモートホストからの同時接続数。 |

システムは、リバース DNS ルックアップによってリモートホスト名を検索してから、フォワード DNS ルックアップによってその名前を検証します。フォワードルックアップで元の IP アドレスにならない場合、またはリバース DNS ルックアップに失敗した場合、テーブルのホスト名カラムには IP アドレスが表示されます。送信者検証プロセスの詳細については、「[送信者の検証](#)」(P.7-28) を参照してください。

## 例

```
mail3.example.com> topin
```

```
Status as of: Sat Aug 23 21:50:54 2003
```

| # | Remote hostname         | Remote IP addr. | listener   | Conn. In |
|---|-------------------------|-----------------|------------|----------|
| 1 | mail.remotedomain01.com | 172.16.0.2      | Incoming01 | 10       |
| 2 | mail.remotedomain01.com | 172.16.0.2      | Incoming02 | 10       |
| 3 | mail.remotedomain03.com | 172.16.0.4      | Incoming01 | 5        |
| 4 | mail.remotedomain04.com | 172.16.0.5      | Incoming02 | 4        |
| 5 | mail.remotedomain05.com | 172.16.0.6      | Incoming01 | 3        |
| 6 | mail.remotedomain06.com | 172.16.0.7      | Incoming02 | 3        |
| 7 | mail.remotedomain07.com | 172.16.0.8      | Incoming01 | 3        |
| 8 | mail.remotedomain08.com | 172.16.0.9      | Incoming01 | 3        |
| 9 | mail.remotedomain09.com | 172.16.0.10     | Incoming01 | 3        |

|    |                         |             |            |   |
|----|-------------------------|-------------|------------|---|
| 10 | mail.remotedomain10.com | 172.16.0.11 | Incoming01 | 2 |
| 11 | mail.remotedomain11.com | 172.16.0.12 | Incoming01 | 2 |
| 12 | mail.remotedomain12.com | 172.16.0.13 | Incoming02 | 2 |
| 13 | mail.remotedomain13.com | 172.16.0.14 | Incoming01 | 2 |
| 14 | mail.remotedomain14.com | 172.16.0.15 | Incoming01 | 2 |
| 15 | mail.remotedomain15.com | 172.16.0.16 | Incoming01 | 2 |
| 16 | mail.remotedomain16.com | 172.16.0.17 | Incoming01 | 2 |
| 17 | mail.remotedomain17.com | 172.16.0.18 | Incoming01 | 1 |
| 18 | mail.remotedomain18.com | 172.16.0.19 | Incoming02 | 1 |
| 19 | mail.remotedomain19.com | 172.16.0.20 | Incoming01 | 1 |
| 20 | mail.remotedomain20.com | 172.16.0.21 | Incoming01 | 1 |

## DNS ステータスの確認

`dnsstatus` コマンドは、DNS ルックアップおよびキャッシュ情報の統計を表示するカウンタを返します。カウンタごとに、そのカウンタの最後のリセット以降、最後のシステム再起動以降、およびシステムの存続期間中に発生したイベントの合計数を表示できます。

表 30-10 に、使用可能なカウンタを示します。

表 30-10 `dnsstatus` コマンドのデータ

| 統計                      | 説明                                          |
|-------------------------|---------------------------------------------|
| <b>DNS Requests</b>     | ドメイン名を解決するためのシステム DNS キャッシュに対する上位レベルの非反復要求。 |
| <b>Network Requests</b> | DNS 情報を取得するためのネットワーク（非ローカル）への要求。            |
| <b>Cache Hits</b>       | レコードが検出されて返された、DNS キャッシュへの要求。               |
| <b>Cache Misses</b>     | レコードが検出されなかった、DNS キャッシュへの要求。                |

表 30-10 dnsstatus コマンドのデータ (続き)

| 統計               | 説明                                                                                                                                                                                                                                                          |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cache Exceptions | レコードが検出されたものの、ドメインが不明である、DNS キャッシュへの要求。                                                                                                                                                                                                                     |
| Cache Expired    | レコードが検出された、DNS キャッシュへの要求。<br>キャッシュでは、使用状況が考慮され、古すぎるレコードは破棄されます。<br><br>Time To Live (TTL; 存続可能時間) を超えていても、多くのエントリがキャッシュに存在する場合があります。これらのエントリは使用されない限り、期限切れカウンタには含まれません。キャッシュがフラッシュされると、有効なエントリと無効 (古すぎる) エントリの両方が削除されます。フラッシュ動作によって、期限切れカウンタが変更されることはありません。 |

## 例

```
mail3.example.com> dnsstatus

Status as of: Sat Aug 23 21:57:28 2003

Counters: Reset Uptime Lifetime

DNS Requests 211,735,710 8,269,306 252,177,342
Network Requests 182,026,818 6,858,332 206,963,542
Cache Hits 474,675,247 17,934,227 541,605,545
Cache Misses 624,023,089 24,072,819 704,767,877
Cache Exceptions 35,246,211 1,568,005 51,445,744
Cache Expired 418,369 7,800 429,015

mail3.example.com>
```

## 電子メール モニタリング カウンタのリセット

resetcounters コマンドは、累積する電子メール モニタリング カウンタをリセットします。リセットは、グローバル カウンタとホスト単位のカウンタに影響します。リセットは、再試行スケジュールに関連する配信キュー内のメッセージのカウンタには影響しません。



(注) GUI で、カウンタをリセットすることもできます。[[システム ステータス \(System Status\) \] ページ \(P.26-40\)](#) を参照してください。

## 例

```
mail3.example.com> resetcounters
```

```
Counters reset: Mon Jan 01 12:00:01 2003
```

## アクティブな TCP/IP サービスの識別

電子メール セキュリティ アプライアンスで使用されるアクティブな TCP/IP サービスを識別するには、コマンドライン インターフェイスで `tcpsservices` コマンドを使用します。

## 電子メール キューの管理

Cisco AsyncOS では、電子メール キュー内のメッセージに対する動作を実行できます。電子メール キュー内のメッセージは、削除、バウンス、一時停止、またはリダイレクトすることができます。また、キュー内の古いメッセージを検索、削除、およびアーカイブすることもできます。

## キュー内の受信者の削除

特定の受信者が配信されていない場合や、電子メール キューをクリアする場合には、`deleterecipients` コマンドを使用します。`deleterecipients` コマンドでは、配信を待つ特定の受信者を削除することによって、電子メール配信キューを管理できます。削除される受信者は、受信者の宛先である受信者ホストによって、または、メッセージエンベロープの **Envelope From** 行に指定された特定のアドレスで識別されるメッセージ送信者によって識別されます。または、配信キュー内のすべてのメッセージ (すべてのアクティブ受信者) を一度に削除することもできます。



(注) `deleterecipients` 機能を実行するには、Cisco アプライアンスをオフラインまたは配信一時停止の状態にすることを推奨します ([「CLI を使用したアプライアンスのオフライン化」 \(P.29-3\)](#) または [「電子メールの受信と配信の一時停止」 \(P.29-2\)](#) を参照)。



(注) この機能はどの状態でも使用できますが、機能の実行中に一部のメッセージが配信される可能性があります。

受信者ホストおよび送信者の一致は、同一文字列の一致である必要があります。ワイルドカードは使用できません。deleterecipients コマンドは、削除されるメッセージの合計数を返します。また、メール ログ サブスクリプション (IronPort テキスト形式のみ) が設定されている場合、メッセージの削除は別個の行としてログに記録されます。

## 例

```
mail3.example.com> deletereipients
```

```
Please select how you would like to delete messages:
```

1. By recipient host.
2. By Envelope From address.
3. All.

```
[1]>
```

Cisco アプライアンスには、必要に応じて受信者を削除するための各種のオプションが用意されています。次に、受信者ホスト別の受信者の削除、Envelope From アドレスによる削除、およびキュー内のすべての受信者の削除の例を示します。

## 受信者ドメインによる削除

Please enter the hostname for the messages you wish to delete.

```
[]> example.com
```

Are you sure you want to delete all messages being delivered to "example.com"? [N]> **Y**

Deleting messages, please wait.

100 messages deleted.

## Envelope From アドレスによる削除

Please enter the Envelope From address for the messages you wish to delete.

```
[]> mailadmin@example.com
```

Are you sure you want to delete all messages with the Envelope From address of "mailadmin@example.com"? [N]> **Y**

Deleting messages, please wait.

100 messages deleted.

## すべて削除

Are you sure you want to delete all messages in the delivery queue (all active recipients)? [N]> **Y**

Deleting messages, please wait.

1000 messages deleted.

## キュー内の受信者のバウンス

deleterecipients コマンドと同様に、bouncerecipients コマンドでは、配信を待つ特定の受信者をハードバウンスすることによって、電子メール配信キューを管理できます。メッセージのバウンスは、bounceconfig コマンドに指定された通常のリバウンドメッセージ設定に従います。



(注) `bouncerecipients` 機能を実行するには、Cisco アプライアンスをオフラインまたは配信一時停止の状態にすることを推奨します（「CLI を使用したアプライアンスのオフライン化」(P.29-3) または「電子メールの受信と配信の一時停止」(P.29-2) を参照）。



(注) この機能はどの状態でも使用できますが、機能の実行中に一部のメッセージが配信される可能性があります。

受信者ホストおよび送信者の一致は、同一文字列の一致である必要があります。ワイルドカードは使用できません。`bouncerecipients` コマンドは、バウンスされたメッセージの合計数を返します。



(注) `bouncerecipients` 機能ではリソースが集中的に使用され、完了までに数分かかる場合があります。オフラインまたは配信一時停止の状態の場合は、バウンスメッセージの実際の送信（ハードバウンス生成がオンの場合）は、`resume` コマンドを使用して Cisco AsyncOS をオンライン状態にした後でのみ開始されます。

## 例

```
mail3.example.com> bouncerecipients
```

```
Please select how you would like to bounce messages:
```

1. By recipient host.
2. By Envelope From address.
3. All.

```
[1]>
```

バウンスされる受信者は、宛先受信者ホストによって、またはメッセージエンベロープの **Envelope From** 行に指定された特定のアドレスで識別されるメッセージ送信者によって識別されます。または、配信キュー内のすべてのメッセージを一度にバウンスすることもできます。

## 受信者ホストによるバウンス

Please enter the hostname for the messages you wish to bounce.

```
[> example.com
```

Are you sure you want to bounce all messages being delivered to "example.com"? [N]> **Y**

Bouncing messages, please wait.

100 messages bounced.

## Envelope From アドレスによるバウンス

Please enter the Envelope From address for the messages you wish to bounce.

```
[> mailadmin@example.com
```

Are you sure you want to bounce all messages with the Envelope From address of "mailadmin@example.com"? [N]> **Y**

Bouncing messages, please wait.

100 messages bounced.

## すべてバウンス

Are you sure you want to bounce all messages in the queue? [N]> **Y**

Bouncing messages, please wait.

1000 messages bounced.

## キュー内のメッセージのリダイレクト

`redirectrecipients` コマンドを使用すると、電子メール配信キュー内のすべてのメッセージを別のリレー ホストにリダイレクトできます。受信者を、このホストから大量の SMTP メールを受け入れる準備ができていないホストまたは IP アドレスにリダイレクトすると、メッセージがバウンスするだけでなく、メールが失われる可能性もあることに注意してください。





## 警告

メッセージを、/dev/null を宛先とする受信側ドメインにリダイレクトすると、メッセージが失われます。メールをこのようなドメインにリダイレクトしても、CLI に警告は表示されません。メッセージをリダイレクトする前に、受信側ドメインがあるかどうか SMTP ルートを確認してください。

## 例

次に、すべてのメールを example2.com ホストにリダイレクトする例を示します。

```
mail3.example.com> redirectrecipients
```

```
Please enter the hostname or IP address of the machine you want to send all mail to.
```

```
[> example2.com
```

```
WARNING: redirecting recipients to a host or IP address that is not prepared to accept large volumes of SMTP mail from this host will cause messages to bounce and possibly result in the loss of mail.
```

```
Are you sure you want to redirect all mail in the queue to "example2.com"? [N]> y
```

```
Redirecting messages, please wait.
```

```
246 recipients redirected.
```

## キュー内の受信者に基づいたメッセージの表示

showrecipients コマンドを使用すると、電子メール配信キューからのメッセージが受信者ホストまたは Envelope From アドレスごとに表示されます。また、キュー内のすべてのメッセージを表示することもできます。

## 例

次に、すべての受信者ホストへのキュー内のメッセージの例を示します。

```
mail3.example.com> showrecipients
```

```
Please select how you would like to show messages:
```

1. By recipient host.
2. By Envelope From address.
3. All.

```
[1]> 3
```

```
Showing messages, please wait.
```

| MID/  | Bytes/  | Sender/                 | Subject |
|-------|---------|-------------------------|---------|
| [RID] | [Atmps] | Recipient               |         |
| 1527  | 1230    | user123456@ironport.com | Testing |
| [0]   | [0]     | 9554@example.com        |         |
| 1522  | 1230    | user123456@ironport.com | Testing |
| [0]   | [0]     | 3059@example.com        |         |
| 1529  | 1230    | user123456@ironport.com | Testing |
| [0]   | [0]     | 7284@example.com        |         |
| 1530  | 1230    | user123456@ironport.com | Testing |
| [0]   | [0]     | 8243@example.com        |         |
| 1532  | 1230    | user123456@ironport.com | Testing |
| [0]   | [0]     | 1820@example.com        |         |
| 1531  | 1230    | user123456@ironport.com | Testing |
| [0]   | [0]     | 9595@example.com        |         |
| 1518  | 1230    | user123456@ironport.com | Testing |
| [0]   | [0]     | 8778@example.com        |         |
| 1535  | 1230    | user123456@ironport.com | Testing |
| [0]   | [0]     | 1703@example.com        |         |

```
1533 1230 user123456@ironport.com Testing
[0] [0] 3052@example.com

1536 1230 user123456@ironport.com Testing
[0] [0] 511@example.com
```

## 電子メール配信の一時停止

メンテナンスやトラブルシューティングのために電子メールの配信を一時的に停止するには、`suspenddel` コマンドを使用します。`suspenddel` コマンドは、Cisco AsyncOS を配信一時停止の状態にします。この状態には、次のような特徴があります。

- 発信電子メール配信は停止されます。
- 着信電子メール接続は受け入れられます。
- ログ転送は続行します。
- CLI はアクセス可能のままになります。

`suspenddel` コマンドを実行すると、開いていた発信接続が閉じられ、新規の接続は開かれませんが、`suspenddel` コマンドはただちに開始され、確立しているすべての接続を正常に閉じることができます。配信一時停止の状態から通常の動作に戻すには、`resumedel` コマンドを使用します。



(注)

「delivery suspend」状態は、システムを再起動しても保持されます。`suspenddel` コマンドを使用してからアプライアンスを再起動する場合は、`resumedel` コマンドを使用して再起動してから配信を再開する必要があります。

## 例

```
mail3.example.com> suspenddel

Enter the number of seconds to wait before abruptly closing connections.

[30]>

Waiting for outgoing deliveries to finish...

Mail delivery suspended.
```

## 電子メール配信の再開

resumedel コマンドは、suspenddel コマンドの使用後に Cisco AsyncOS を通常の動作状態に戻します。

## 構文

```
resumedel

mail3.example.com> resumedel

Mail delivery resumed.
```

## 電子メールの受信の一時停止

すべてのリスナーに対して電子メールの受信を一時停止するには、suspendlistener コマンドを使用します。受信が一時停止されている間、システムはリスナーの特定のポートへの接続を受け入れません。

これは、このリリースの AsyncOS で変更された動作です。以前のリリースでは、システムは接続を受け入れ、次のように応答してから接続解除していました。

- SMTP: 421 *hostname* Service not available, closing transaction channel
- QMQP: ZService not available



(注)

「receiving suspend」状態は、システムを再起動しても保持されます。suspendlistener コマンドを使用してからアプライアンスを再起動する場合、リスナーでメッセージの受信を再開するには、resumelister コマンドを使用する必要があります。

## 構文

```
suspendlistener
mail3.example.com> suspendlistener

Choose the listener(s) you wish to suspend.

Separate multiple entries with commas.

1. All
2. InboundMail
3. OutboundMail

[1]> 1

Enter the number of seconds to wait before abruptly closing connections.

[30]>

Waiting for listeners to exit...

Receiving suspended.

mail3.example.com>
```

## 電子メールの受信の再開

resumelistener コマンドは、suspendlistener コマンドの使用後に Cisco AsyncOS を通常の動作状態に戻します。

## 構文

```
resumelistener
mail3.example.com> resumelistener

Choose the listener(s) you wish to resume.

Separate multiple entries with commas.

1. All
2. InboundMail
```

```
3. OutboundMail
[1]> 1

Receiving resumed.

mail3.example.com>
```

## 電子メールの配信と受信の再開

resume コマンドは、配信と受信の両方を再開します。

### 構文

```
resume

mail3.example.com> resume

Receiving resumed.

Mail delivery resumed.

mail3.example.com>
```

## 電子メールの即時配信スケジュール

delivernow コマンドを使用すると、後で配信するようにスケジュールされた受信とホストをただちに再試行できます。delivernow コマンドでは、キュー内の電子メールに即時配信を再スケジュールすることができます。down のマークが付いたすべてのドメインと、スケジュールされたメッセージまたはソフト バウンスされたメッセージが、即時配信のキューに入れられます。

delivernow コマンドは、キュー内の（スケジュールされた、およびアクティブな）すべての受信者または特定の受信者に対して呼び出すことができます。特定の受信を選択する際は、即時配信をスケジュールする受信者のドメイン名を入力する必要があります。システムは、文字列全体の文字と長さを照合します。

### 構文

```
delivernow

mail3.example.com> delivernow

Please choose an option for scheduling immediate delivery.

1. By recipient host
```

```
2. All messages

[1]> 1

Please enter the domain to schedule for immediate delivery.

[]> recipient.example.com

Rescheduling all messages to recipient.example.com for immediate delivery.

mail3.example.com>
```

## ワーク キューの休止

LDAP 受信者アクセス、マスカレード、LDAP 再ルーティング、メッセージフィルタ、スパム対策、およびアンチウイルス スキャン エンジンの処理は、すべて「ワーク キュー」で実行されます。処理フローについては「ルーティングおよび配信機能の設定」(P.21-1)、「ワーク キュー内のメッセージ」ゲージの説明については表 30-2 (P.30-4) を参照してください。workqueue コマンドを使用して、ワークキュー部分のメッセージ処理を手動で休止することができます。

たとえば、多くのメッセージがワーク キュー内にあるときに、LDAP サーバの設定を変更する必要があるとします。おそらく、LDAP 受信者アクセス クエリーに基づいて、メッセージをバウンスからドロップに切り替えようとする。または、キューを休止して、最新のアンチウイルス スキャン エンジンの定義ファイルを手動で確認 (antivirusupdate コマンドを使用) する可能性もあります。workqueue コマンドを使用すると、ワークキューを休止してから再開することで、処理を停止した状態で他の設定変更を行うことができます。

ワーク キューを休止してから再開すると、そのイベントがログに記録されます。次に例を示します。

```
Sun Aug 17 20:01:36 2003 Info: work queue paused, 1900 msgs S
Sun Aug 17 20:01:39 2003 Info: work queue resumed, 1900 msgs
```

次の例では、ワーク キューが中止されます。

```
mail3.example.com> workqueue

Status as of: Sun Aug 17 20:02:30 2003 GMT

Status: Operational

Messages: 1243

Choose the operation you want to perform:
```

```
- STATUS - Display work queue status
- PAUSE - Pause the work queue
- RATE - Display work queue statistics over time
```

```
[> pause
```

```
Manually pause work queue? This will only affect unprocessed messages. [N]> y
```

```
Reason for pausing work queue:
```

```
[> checking LDAP server
```

```
Status as of: Sun Aug 17 20:04:21 2003 GMT
```

```
Status: Paused by admin: checking LDAP server
```

```
Messages: 1243
```



(注)

---

理由の入力は任意です。理由を入力しないと、その理由は「Manually paused by user」としてログに記録されます。

---

次の例では、ワーク キューが再開されます。

```
mail3.example.com> workqueue
```

```
Status as of: Sun Aug 17 20:42:10 2003 GMT
```

```
Status: Paused by admin: checking LDAP server
```

```
Messages: 1243
```

```
Choose the operation you want to perform:
```

```
- STATUS - Display work queue status
- RESUME - Resume the work queue
- RATE - Display work queue statistics over time
```

```
[> resume
```



```
Status: Operational

Messages: 1243
```

## 古いメッセージの検索およびアーカイブ

時折、古くなったメッセージが配信できずに、キューに留まっていることがあります。これらのメッセージは削除したり、アーカイブしたりすることができます。これには、`showmessage` CLI コマンドを使用して、所定のメッセージ ID に対応するメッセージを表示します。`oldmessage` CLI コマンドを使用すると、システム上の最も古い非隔離メッセージが表示されます。その後は、任意で `removemessage` を使用して、所定のメッセージ ID に対応するメッセージを安全に削除できます。このコマンドでは、ワーク キュー、再試行キュー、または宛先キュー内のメッセージのみを削除できます。メッセージがこれらのキューのいずれにもない場合は、削除できません。

また、`archivemessage[mid]` CLI コマンドを使用して、所定のメッセージ ID に対応するメッセージを `configuration` ディレクトリ内の `mbox` ファイルにアーカイブすることもできます。

`oldmessage` コマンドを使用して、隔離エリア内のメッセージのメッセージ ID を取得することはできません。ただし、メッセージ ID がわかっている場合は、指定のメッセージを表示したり、アーカイブしたりすることができます。メッセージがワーク キュー、再試行キュー、または宛先キューにないと、`removemessage` コマンドでメッセージを削除することはできません。



(注) Cisco スпам隔離内のメッセージに対しては、これらのキュー管理コマンドを実行できません。

## 構文

```
archivemessage

example.com> archivemessage
```

Enter the MID to archive and remove.

```
[0]> 47
```

MID 47 has been saved in file `oldmessage_47.mbox` in the configuration directory

```
example.com>
```

## 構文

```
oldmessage

example.com> oldmessage
```

```
MID 9: 1 hour 5 mins 35 secs old
```

```

Received: from example.com ([172.16.0.102])
 by example.com with SMTP; 14 Feb 2007 22:11:37 -0800

From: user123@example.com

To: 4031@test.example2.com

Subject: Testing

Message-Id: <20070215061136.68297.16346@example.com>

```

## システム内のメッセージのトラッキング

findevent CLI コマンドは、オンボックスのメール ログ ファイルを使用して、システム内のメッセージのトラッキング（追跡）プロセスを容易にします。findevent CLI コマンドを使用すると、メッセージ ID の検索、またはサブジェクト ヘッダー、エンベロープ送信者、またはエンベロープ受信者に対する正規表現の一致検索によって、メール ログから特定のメッセージを検索できます。現在のログ ファイルやすべてのログ ファイルの結果を表示することも、ログ ファイルを日付別で表示することもできます。ログ ファイルを日付別で表示する場合は、特定の日付か、日付の範囲を指定できます。

ログを表示するメッセージを識別した後は、findevent コマンドによって、分裂情報（分裂したログメッセージ、バウンス、およびシステム生成メッセージ）を含む、そのメッセージ ID に対するログ情報を表示できます。次に、findevent CLI コマンドで、サブジェクト ヘッダーに「confidential」とあるメッセージの受信と配信を追跡する例を示します。

```

example.com> findevent

Please choose which type of search you want to perform:

1. Search by envelope FROM
2. Search by Message ID
3. Search by Subject
4. Search by envelope TO

[1]> 3

Enter the regular expression to search for.

[]> confidential

Currently configured logs:

1. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll

Enter the number of the log you wish to use for message tracking.

[]> 1

```

```
Please choose which set of logs to search:
```

1. All available log files
2. Select log files by date list
3. Current log file

```
[3]> 3
```

```
The following matching message IDs were found. Please choose one to show additional log information:
```

1. MID 4 (Tue Jul 31 17:37:35 2007) sales: confidential

```
[1]> 1
```

```
Tue Jul 31 17:37:32 2007 Info: New SMTP ICID 2 interface Data 1 (172.19.1.86) address 10.251.20.180 reverse dns host unknown verified no
Tue Jul 31 17:37:32 2007 Info: ICID 2 ACCEPT SG None match ALL SBRS None
Tue Jul 31 17:37:35 2007 Info: Start MID 4 ICID 2
Tue Jul 31 17:37:35 2007 Info: MID 4 ICID 2 From: <user@example.com>
Tue Jul 31 17:37:35 2007 Info: MID 4 ICID 2 RID 0 To: <ljohnson@example02.com>
Tue Jul 31 17:37:35 2007 Info: MID 4 Subject 'sales: confidential'
Tue Jul 31 17:37:35 2007 Info: MID 4 ready 4086 bytes from <user@example.com>
Tue Jul 31 17:37:35 2007 Info: MID 4 matched all recipients for per-recipient policy DEFAULT in the inbound table
Tue Jul 31 17:37:35 2007 Info: ICID 2 close
Tue Jul 31 17:37:37 2007 Info: MID 4 interim verdict using engine: CASE spam negative
Tue Jul 31 17:37:37 2007 Info: MID 4 using engine: CASE spam negative
Tue Jul 31 17:37:37 2007 Info: MID 4 interim AV verdict using Sophos CLEAN
Tue Jul 31 17:37:37 2007 Info: MID 4 antivirus negative
Tue Jul 31 17:37:37 2007 Info: MID 4 queued for delivery
Tue Jul 31 17:37:37 2007 Info: Delivery start DCID 0 MID 4 to RID [0]
Tue Jul 31 17:37:37 2007 Info: Message done DCID 0 MID 4 to RID [0]
Tue Jul 31 17:37:37 2007 Info: MID 4 RID [0] Response '/null'
Tue Jul 31 17:37:37 2007 Info: Message finished MID 4 done
```

## SNMP モニタリング

Cisco AsyncOS オペレーティング システムは、SNMP (簡易ネットワーク管理プロトコル) を使用したシステム ステータスのモニタリングをサポートしています。これには、シスコのエンタープライズ MIB、ASYNCOS-MAIL-MIB が含まれます。ASYNCOS-MAIL-MIB を使用することで、管理者は、システムの状態をモニタしやすくなります。また、このリリースには、RFC 1213 および 1907 に規定されている MIB-II の読み取り専用のサブセットが実装されています (SNMP の詳細については、RFC 1065、1066、および 1067 を参照してください)。次の点に注意してください。

- SNMP は、デフォルトでオフになります。
- SNMP SET 動作 (コンフィギュレーション) は実装されません。
- AsyncOS は SNMPv1、v2、および v3 をサポートしています。
- このサービスをイネーブルにするには、パスワード認証と DES 暗号化を伴う SNMPv3 の使用が必須です (SNMPv3 の詳細については、RFC 2571 ~ 2575 を参照してください)。SNMP システム ステータスのモニタリングをイネーブルにするには、少なくとも 8 文字の SNMPv3 パスフレーズ

を設定する必要があります。最初に SNMPv3 パスフレーズを入力するときは、確認のためにそのパスフレーズを再入力する必要があります。次に snmpconfig コマンドを実行するときは、コマンドにこのフレーズが「記憶」されています。

- SNMPv3 ユーザ名は v3get です。

```
> snmpwalk -v 3 -l AuthNoPriv -u v3get -a MD5 ironport mail.example.com
```

- SNMPv1 または SNMPv2 のみを使用する場合は、コミュニティストリングを設定する必要があります。コミュニティストリングは、public にデフォルト設定されません。
- SNMPv1 および SNMPv2 の場合、どのネットワークからの SNMP GET 要求を受け入れるかを指定する必要があります。
- トラップを使用するには、SNMP マネージャ (AsyncOS には含まれていません) が実行中であり、その IP アドレスがトラップターゲットとして入力されている必要があります (ホスト名を使用できますが、その場合、トラップは DNS が動作しているときに限り機能します)。

snmpconfig コマンドを使用して、アプライアンスの SNMP システム ステータスを設定します。インターフェイスの値を選択し、設定し終わると、アプライアンスは SNMPv3 GET 要求に応答します。これらのバージョン 3 要求には、一致するパスワードが含まれている必要があります。デフォルトでは、バージョン 1 および 2 要求は拒否されます。イネーブルにする場合は、バージョン 1 および 2 要求に一致するコミュニティストリングが含まれている必要があります。

## MIB ファイル

Cisco システムには、「Structure of Management Information」(SMI) ファイルだけでなく、次の「エンタープライズ」MIB が用意されています。

- ASYNCOS-MAIL-MIB.txt : Cisco アプライアンス用のエンタープライズ MIB の SNMPv2 互換の説明。
- IRONPORT-SMI.txt : IronPort の SNMP 管理対象製品における ASYNCOS-MAIL-MIB の役割を定義します。

これらのファイルは、Cisco アプライアンスに付属のドキュメンテーション CD に収録されています。また、Cisco カスタマー サポートを通じてこれらのファイルを要求することもできます。

## ハードウェア オブジェクト

Intelligent Platform Management Interface Specification (IPMI) 準拠のハードウェア センサーが温度、ファン速度、および電源モジュール ステータスを報告します。

表 30-11 に、どのモデルでどのハードウェア派生オブジェクトをモニタリングに使用できるかを示します。表示されている数字は、モニタできるオブジェクトのインスタンスの数です。たとえば、C10 アプライアンスの 3 つのファン、および C300/C600/X1000 アプライアンスの 6 つのファンについてクエリーを送信できます。

表 30-11 Cisco アプライアンスごとのハードウェア オブジェクトの数

| モデル     | CPU 温度 | 周囲温度 | バックプレーン温度 | ライザー温度 | ファン | 電源ステータス | ディスクステータス | NIC リンク |
|---------|--------|------|-----------|--------|-----|---------|-----------|---------|
| C10/100 | 1      | 1    | 0         | 0      | 3   | 0       | 2         | 2       |

表 30-11 Cisco アプライアンスごとのハードウェア オブジェクトの数

| モデル             | CPU 温度 | 周囲温度 | バックプレーン温度 | ライザー温度 | ファン | 電源ステータス | ディスクステータス    | NIC リンク                                  |
|-----------------|--------|------|-----------|--------|-----|---------|--------------|------------------------------------------|
| C30/C60         | 0      | 0    | 0         | 0      | 0   | 0       | 2 (C60 は 4)  | 3                                        |
| C300/C600/X1000 | 2      | 1    | 1         | 1      | 6   | 2       | 4 (C300 は 2) | 3 (ファイバーインターフェース搭載の C600 と X1000 の場合は 5) |
| C350/C650/X1050 | 2      | 1    | 0         | 0      | 4   | 2       | 4 (C350 は 2) | 3 (ファイバーインターフェース搭載の C650 と x1050 の場合は 5) |

いずれのモデルでも、SNMP を使用してディスク ドライブの状態とネットワーク インターフェイスのリンク ステータスをモニタできます。

## ハードウェア トラップ

表 30-12 に、ハードウェア トラップが送信される温度およびハードウェアの条件を示します。

表 30-12 ハードウェア トラップ：温度およびハードウェアの条件

| モデル             | 高温 (CPU) | 高温 (周囲) | 高温 (バックプレーン) | 高温 (ライザー) | ファン障害 | 電源モジュール | RAID    | リンク     |
|-----------------|----------|---------|--------------|-----------|-------|---------|---------|---------|
| C10/C100        | 90C      | 47C     | NA           | NA        | 0 RPM | ステータス変更 | ステータス変更 | ステータス変更 |
| C30/C60         | NA       | NA      | NA           | NA        | NA    | NA      | ステータス変更 | ステータス変更 |
| C300/C600/X1000 | 90C      | 47C     | 72C          | 62C       | 0 RPM | ステータス変更 | ステータス変更 | ステータス変更 |
| C350/C650/X1050 | 90C      | 47C     | NA           | NA        | 0 RPM | ステータス変更 | ステータス変更 | ステータス変更 |

ステータス変更トラップは、ステータスが変更されると送信されます。ファン障害および高温トラップは、5 秒ごとに送信されます。その他のトラップは、障害条件アラームトラップです。これらのトラップは、ステータスが（良好から障害へ）変更されたときに一度だけ送信されます。ハードウェアステータステーブルにポーリングを送信して、致命的な状況になる前に潜在的なハードウェア障害を識別することを推奨します。重大値の 10 % 以内の温度を不安原因と考えることができます。

障害条件アラームトラップは、個々のコンポーネントの致命的な障害を示しますが、システム全体の障害の原因になるとは限りません。たとえば、C600 アプライアンスで 1 つのファンまたは電源モジュールに障害が発生しても、アプライアンスは動作し続けます。

## SNMP トラップ

SNMP には、1 つまたは複数の条件が満たされたときに管理アプリケーション（通常は、SNMP 管理コンソール）に知らせるためのトラップ（または通知）を送信する機能が備わっています。トラップとは、トラップを送信するシステムのコンポーネントに関するデータを含むネットワークパケットです。トラップは、SNMP エージェント（この場合は Cisco アプライアンス）で、ある条件が満たされた場合に生成されます。条件が満たされると、SNMP エージェントは SNMP パケットを形成し、標準の SNMP トラップポートであるポート 162 経由で送信します。次の例では、トラップターゲット snmp-monitor.example.com およびトラップコミュニティストリングが入力されています。これは、Cisco アプライアンスから SNMP トラップを受信する SNMP 管理コンソールソフトウェアを実行しているホストです。

インターフェイスに対して SNMP をイネーブルにするときに、SNMP トラップを設定（特定のトラップをイネーブルまたはディセーブルに）できます。トラップターゲットの入力を求められたときに、複数のトラップターゲットを指定するには、カンマで区切った IP アドレスを 10 個まで入力できます。

## CLI の例

次の例では、snmpconfig コマンドを使用して、ポート 161 の「PublicNet」インターフェイスで SNMP をイネーブルにしています。バージョン 3 のパスフレーズが入力され、確認のために再入力されています。システムは、バージョン 1 および 2 要求を処理するように設定されており、これらのバージョン 1 および 2 からの GET 要求に対してコミュニティストリング public が入力されています。トラップターゲット snmp-monitor.example.com が入力されています。最後に、システムの場所と連絡先情報が入力されています。

```
mail3.example.com> snmpconfig
```

```
Current SNMP settings:
```

```
SNMP Disabled.
```

```
Choose the operation you want to perform:
```

```
- SETUP - Configure SNMP.
```

```
[]> setup
```

```
Do you want to enable SNMP? [N]> y
```

```
Please choose an IP interface for SNMP requests.
```

1. Data 1 (192.168.1.1/24: mail3.example.com)
2. Data 2 (192.168.2.1/24: mail3.example.com)
3. Management (192.168.44.44/24: mail3.example.com)

```
[1]>
```

```
Enter the SNMPv3 passphrase.
```

```
>
```

```
Please enter the SNMPv3 passphrase again to confirm.
```

```
>
```

```
Which port shall the SNMP daemon listen on?
```

```
[161]>
```

```
Service SNMP V1/V2c requests? [N]> y
```

```
Enter the SNMP V1/V2c community string.
```

```
[>] public
```

```
From which network shall SNMP V1/V2c requests be allowed?
```

```
[192.168.2.0/24]>
```

```
Enter the Trap target (IP address recommended). Enter "None" to disable traps.
```

```
[None]> 10.1.1.29
```

```
Enter the Trap Community string.
```

```
[>] tcomm
```

## Enterprise Trap Status

|                             |         |
|-----------------------------|---------|
| 1. RAIDStatusChange         | Enabled |
| 2. fanFailure               | Enabled |
| 3. highTemperature          | Enabled |
| 4. keyExpiration            | Enabled |
| 5. linkDown                 | Enabled |
| 6. linkUp                   | Enabled |
| 7. powerSupplyStatusChange  | Enabled |
| 8. resourceConservationMode | Enabled |
| 9. updateFailure            | Enabled |

Do you want to change any of these settings? [N]> **y**

Do you want to disable any of these traps? [Y]>

Enter number or numbers of traps to disable. Separate multiple numbers with commas.

[ ]> **1,8**

## Enterprise Trap Status

|                             |          |
|-----------------------------|----------|
| 1. RAIDStatusChange         | Disabled |
| 2. fanFailure               | Enabled  |
| 3. highTemperature          | Enabled  |
| 4. keyExpiration            | Enabled  |
| 5. linkDown                 | Enabled  |
| 6. linkUp                   | Enabled  |
| 7. powerSupplyStatusChange  | Enabled  |
| 8. resourceConservationMode | Disabled |
| 9. updateFailure            | Enabled  |

Do you want to change any of these settings? [N]>



Enter the System Location string.

```
[Unknown: Not Yet Configured]> Network Operations Center - west; rack #31, position 2
```

Enter the System Contact string.

```
[snmp@localhost]> Joe Administrator, x8888
```

Current SNMP settings:

Listening on interface "Data 1" 192.168.2.1/24 port 161.

SNMP v3: Enabled.

SNMP v1/v2: Enabled, accepting requests from subnet 192.168.2.0/24.

SNMP v1/v2 Community String: public

Trap target: 10.1.1.29

Location: Network Operations Center - west; rack #31, position 2

System Contact: Joe Administrator, x8888

```
mail3.example.com>
```





## CHAPTER 31

# SenderBase Network Participation

---

- 「SenderBase Network Participation の概要」 (P.31-1)
- 「SenderBase との統計の共有」 (P.31-1)
- 「よくあるご質問」 (P.31-2)

## SenderBase Network Participation の概要

SenderBase は、電子メール管理者による送信者の調査、電子メールの正規送信元の識別、およびスパム送信者のブロックに役立つように設計された、電子メールのレピュテーション サービスです。

SenderBase ネットワークに参加しているお客様は、使用するすべてのサービスの機能向上のため、シスコがお客様の組織の集約された電子メールトラフィックの統計情報を収集することを許可します。参加は任意です。シスコは、メッセージ属性の要約データおよび Cisco アプライアンスがどのように各種メッセージを処理したかに関する情報のみを収集します。たとえば、シスコは、メッセージの本文もメッセージの件名も収集しません。個人を特定できる情報や、組織を特定する情報は、機密情報として扱われます。

## SenderBase との統計の共有

### 手順

- 
- ステップ 1** [セキュリティ (Security Services)] > [SenderBase] に移動します。
  - ステップ 2** [グローバル設定を編集 (Edit Global Settings)] をクリックします。
  - ステップ 3** ボックスをチェックして、SenderBase Information Service との統計データの共有をイネーブルにします。  
このボックスをオンにすると、アプライアンスの機能がグローバルにイネーブルになります。イネーブルにした場合、(Cisco Anti-Spam スキャンがイネーブルになっているかどうかに関係なく) データの収集およびデータの収集に Context Adaptive Scanning Engine (CASE) が使用されます。
  - ステップ 4** (任意) プロキシ サーバをイネーブルにして、SenderBase Information Service と統計データを共有します。

ルールのアップデートを取得するようにプロキシサーバを定義する場合は、追加で表示されるフィールドに、プロキシサーバに接続する際に使用する認証済みのユーザ名、パスワード、および特定のポートも設定できます。これらの設定を編集する方法については、「システム時刻」(P.29-57)を参照してください。また、CLI の `senderbaseconfig` コマンドを使用して同様の設定を行うこともできます。

## よくあるご質問

シスコは、プライバシーが重要であると認識しており、プライバシーを考慮してサービスを設計および操作しています。SenderBase Network Participation に登録した場合は、シスコは組織の電子メールトラフィックに関する集約した統計情報を収集しますが、個人を特定できる情報を収集したり、使用したりすることはありません。シスコが収集した、ユーザまたは組織を特定できる可能性のある情報は、すべて極秘として扱われます。

### なぜ参加する必要があるのですか。

SenderBase Network に参加していただくことで、IronPort がお客様に役立てるようになります。スパム、ウイルス、およびディレクトリ獲得攻撃などの、電子メールをベースとした脅威が組織に影響を及ぼすことを止めるには、IronPort とデータを共有していただくことが重要になります。参加が特に重要になる例として、次のような場合があります。

- お客様の組織を特に標的とした電子メール攻撃では、提供したデータがお客様自身を保護する主要な情報源となります。
- お客様の組織が、最初に新しいグローバルな電子メール攻撃を受けた組織の 1 つであった場合、IronPort と共有したデータにより、新しい脅威に対応するスピードが大幅に向上します。

### どのようなデータを共有するのですか。

データは、メッセージ属性の要約情報および Cisco アプライアンスがどのように各種メッセージを処理したかに関する情報です。メッセージの本文すべてを収集するわけではありません。繰り返しになりますが、シスコに提供された、ユーザまたは組織を特定できる可能性のある情報は、すべて極秘として扱われます（後述の「シスコは、共有されたデータがセキュアであることをどのように確認していますか。」(P.31-4)を参照してください）。

表 31-1 および表 31-2 に、「人間にわかりやすい」形式でサンプルのログ エントリを説明します。

表 31-1 Cisco アプライアンスごとに共有される統計情報

| 項目                     | サンプル データ                          |
|------------------------|-----------------------------------|
| MGA ID                 | MGA 10012                         |
| タイムスタンプ                | 2005 年 7 月 1 日午前 8 時～午前 8:05 のデータ |
| ソフトウェア バージョン番号         | MGA バージョン 4.7.0                   |
| ルール セットのバージョン番号        | アンチスパム ルール セット 102                |
| アンチウイルス アップデート間隔       | 10 分ごとにアップデート                     |
| 隔離エリアのサイズ              | 500 MB                            |
| 隔離可能メッセージ数             | 現在 50 件のメッセージを隔離可能                |
| ウイルス スコアしきい値           | 脅威レベル 3 以上のメッセージを隔離               |
| 隔離されたメッセージのウイルス スコアの合計 | 120                               |

表 31-1 Cisco アプライアンスごとに共有される統計情報 (続き)

| 項目                                                    | サンプル データ                                                 |
|-------------------------------------------------------|----------------------------------------------------------|
| 隔離されたメッセージ数                                           | 30 (平均スコア 4)                                             |
| 最大隔離時間                                                | 12 時間                                                    |
| アンチウイルス結果との相関による隔離理由および隔離解除理由で分類した、アウトブレイク隔離メッセージ数の内訳 | .exe ルールにより 50 件を隔離<br>手動で 30 件を隔離解除。このうち 30 件すべてがウイルス陽性 |
| 隔離解除の際に実行されたアクションで分類した、アウトブレイク隔離メッセージ数の内訳             | 10 件のメッセージは隔離解除後に添付ファイルを削除                               |
| メッセージ隔離時間の合計                                          | 20 時間                                                    |

表 31-2 IP アドレスごとに共有される統計情報

| 項目                                              | サンプル データ                                                                               |
|-------------------------------------------------|----------------------------------------------------------------------------------------|
| アプライアンスのさまざまな段階におけるメッセージ数                       | アンチウイルス エンジンにより発見 : 100<br>アンチスパム エンジンにより発見 : 80                                       |
| アンチスパムとアンチウイルスのスコア合計および判断                       | 2,000 (発見されたすべてのメッセージに対するアンチスパム スコアの合計)                                                |
| さまざまなアンチスパム ルールおよびアンチウイルス ルールの組み合わせにヒットしたメッセージ数 | 100 件のメッセージがルール A および B にヒット<br>50 件のメッセージがルール A のみにヒット                                |
| 接続数                                             | 20 SMTP 接続                                                                             |
| 受信者の総数および無効数                                    | 総受信者数 50<br>無効な受信者数 10                                                                 |
| ハッシュされたファイル名 : (a)                              | <one-way-hash>.zip という名前のアーカイブされた添付ファイル内で、ファイル <one-way-hash>.pif が検出                  |
| 難読化されたファイル名 : (b)                               | ファイル aaaaaaa.zip 内で、ファイル aaaaaaa0.aaa.pif が検出                                          |
| URL ホスト名 (c)                                    | メッセージ内で www.domain.com へのリンクが検出                                                        |
| 難読化された URL パス (d)                               | メッセージ内で aaa000aa/aa00aaa というパスを持つホスト名 www.domain.com へのリンクが検出                          |
| スパムおよびウイルス スキャン結果ごとのメッセージ数                      | スパム陽性 10 件<br>スパム陰性 10 件<br>スパムの疑い 5 件<br>ウイルス陽性 4 件<br>ウイルス陰性 16 件<br>ウイルス スキャン不可 5 件 |
| さまざまなアンチスパムおよびアンチウイルス判断によるメッセージ数                | スパム 500 件、ハム 300 件                                                                     |
| サイズ レンジ内のメッセージ数                                 | 30 ~ 35 K の範囲に 125 件                                                                   |
| さまざまな拡張子タイプごとの数                                 | 300 個の「.exe」添付ファイル                                                                     |

表 31-2 IP アドレスごとに共有される統計情報

| 項目                                      | サンプル データ (続き)                                                                 |
|-----------------------------------------|-------------------------------------------------------------------------------|
| 添付ファイル タイプ、本当のファイル タイプ、およびコンテナ タイプの相関関係 | 100 個の添付ファイルの拡張子が「.doc」ですが、実際には「.exe」<br><br>50 個の添付ファイルが zip 内に含まれた「.exe」拡張子 |
| 拡張子および本当のファイル タイプと添付ファイル サイズの相関関係       | 30 個の添付ファイルが 50 ~ 55 K の範囲の「.exe」                                             |

- (a) ファイル名は一方方向ハッシュ (MD5) でエンコードされます。
- (b) ファイル名は難読化された形式で送信されます。この形式では、すべての小文字の ASCII 文字 ([a ~ z]) は「a」、すべての大文字の ASCII 文字 ([A ~ Z]) は「A」、すべてのマルチバイト UTF-8 文字は (その他の文字セットにプライバシーを提供するため)「x」に、すべての ASCII 数字 ([0 ~ 9]) は「0」に置換され、その他すべてのシングル バイト文字 (空白文字、句読点など) はそのまま保持されます。たとえば、ファイル Britney1.txt.pif は Aaaaaaa0.aaa.pif と表示されます。
- (c) IP アドレスと同様に、URL ホスト名はコンテンツを提供する Web サーバを指定します。ユーザ名およびパスワードのような、秘密情報は含まれません、
- (d) ホスト名に続く URL 情報は、ユーザの個人情報が漏えいしないように難読化されています。

## シスコは、共有されたデータがセキュアであることをどのように確認していますか。

SenderBase Network への参加に同意すると、次のように処理されます。

- Cisco アプライアンスから送信されたデータは、セキュアなプロトコル HTTPS を使用して Cisco SenderBase Network サーバに送信されます。
- お客様のデータはすべて、シスコで慎重に取り扱われます。このデータは、セキュアな場所に保存され、データへのアクセスは、企業の電子メール セキュリティ製品およびサービスの向上またはカスタマー サポートの提供のためにデータにアクセスする必要があるシスコの従業員および請負業者に限られます。
- データに基づいてレポートまたは統計情報が作成された場合、電子メールの受信者またはお客様の企業を特定する情報が、シスコ以外で共有されることはありません。

## データを共有することで Cisco アプライアンスのパフォーマンスに影響はありますか。

シスコは、ほとんどのお客様には若干のパフォーマンス上の影響があると認識しています。IronPort は、電子メール配信プロセスの一環として、既存のデータを記録します。その後、アプライアンス上でお客様のデータが集約され、通常 5 分ごとに SenderBase サーバに一括送信されます。HTTPS を介して転送されるデータの総サイズは、一般的な企業の電子メール トラフィック帯域幅の 1% 未満と予想しています。

イネーブルにした場合、(Cisco Anti-Spam スキャンがイネーブルになっているかどうかに関係なく) データの収集およびデータの収集に Context Adaptive Scanning Engine (CASE) が使用されます。



(注)

SenderBase Network への参加を選択すると、「本文スキャン」が各メッセージに対して実行されます。これは、メッセージに適用されたフィルタなどのアクションにより本文スキャンが起動されたかどうかに関係なく実行されます。本文スキャンの詳細については、「[本文スキャンルール](#)」(P.9-29) を参照してください。

不明点は、Cisco カスタマー サポートまでお問い合わせください。「[Cisco サポート コミュニティ](#)」(P.1-7) を参照してください。

### その他の方法でデータを共有できますか。

シスコがより高品質のセキュリティ サービスを提供できるようにするために、ご協力をお考えのお客様のために、追加データの提供を可能にするコマンドを用意しています。このより高レベルのデータ共有では、メッセージに含まれる添付ファイルの明確なファイル名、ハッシュされていないテキスト、および URL のホスト名も提供されます。この機能の詳細について関心をお持ちの場合は、システム エンジニアまたは Cisco カスタマー サポートにお問い合わせください。







## CHAPTER 32

# GUI でのその他の作業

---

グラフィカル ユーザ インターフェイス (GUI) は、システムのモニタリングおよび設定用の一部のコマンドライン インターフェイス (CLI) コマンドに代わる Web ベースのインターフェイスです。GUI を使用することにより、Cisco AsyncOS コマンド構文を知らなくても、単純な Web ベース インターフェイスを使用してシステムをモニタできます。

この章は、次の内容で構成されています。

- 「Cisco グラフィカル ユーザ インターフェイス (GUI)」 (P.32-7)
- 「GUI のシステム情報」 (P.32-11)
- 「GUI からの XML ステータスの収集」 (P.32-12)

## Cisco グラフィカル ユーザ インターフェイス (GUI)

インターフェイスに対して HTTP、HTTPS、またはその両方のサービスをイネーブルにすると、GUI にアクセスし、ログインできるようになります。詳細については、『Cisco IronPort AsyncOS for Email Configuration Guide』の「Overview」の章を参照してください。

### インターフェイスでの GUI のイネーブル化

システムはデフォルトで、管理インターフェイス (Cisco C150/160 アプライアンスの Data 1) に対して HTTP がイネーブルになった状態で出荷されます。

GUI をイネーブルにするには、コマンドライン インターフェイスで `interfaceconfig` コマンドを実行し、接続するインターフェイスを編集してから、HTTP サービスまたはセキュア HTTP サービス、あるいはその両方をイネーブルにします。



(注) また、いずれかのインターフェイスで GUI をイネーブルにした後は、[ネットワーク (Network)] > [IP インターフェイス (IP Interfaces)] ページを使用して、別のインターフェイスに対して GUI をイネーブルまたはディセーブルにすることもできます。詳細については、「IP インターフェイス」(P.A-1) を参照してください。

---



(注) インターフェイスでセキュア HTTP をイネーブルにするには、証明書をインストールする必要があります。詳細については、『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「HTTPS の証明書のイネーブル化」を参照してください。

---

いずれかのサービスについても、サービスを有効にするポートを指定します。デフォルトでは、HTTP はポート 80、HTTPS はポート 443 でイネーブルになります。1 つのインターフェイスで両方のサービスをイネーブルにすると、HTTP 要求をセキュア サービスに自動的にリダイレクトできます。

さらに、このインターフェイス (HTTP または HTTPS 経由) で GUI にアクセスしようとするすべてのユーザは (「[ユーザ アカウントを使用する作業](#)」(P.28-1) を参照)、標準ユーザ名とパスワードのログイン ページで自分自身を認証する必要があります。



(注) GUI にアクセスするには、まず、commit コマンドを使用して変更を保存する必要があります。

次の例では、GUI は Data 1 インターフェイスでイネーブルになります。interfaceconfig コマンドは HTTP はポート 80、HTTPS はポート 443 でイネーブルにするために使用されます。(デモ証明書は certconfig コマンドが実行できるようになるまで HTTP 用に一時的に使用されます。より多くの情報については、『『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』』の「Installing Certificates on the Cisco Appliance」を参照してください)。ポート 80 への HTTP 要求は自動的に Data1 インターフェイスのポート 443 に方向を変更するように設定されています。

## 例

```
mail3.example.com> interfaceconfig

Currently configured interfaces:

1. Data 1 (192.168.1.1/24 on Data1: mail3.example.com)
2. Data 2 (192.168.2.1/24 on Data2: mail3.example.com)
3. Management (192.168.42.42/24 on Management: mail3.example.com)

Choose the operation you want to perform:

- NEW - Create a new interface.
- EDIT - Modify an interface.
- GROUPS - Define interface groups.
- DELETE - Remove an interface.

[]> edit

Enter the number of the interface you wish to edit.

[]> 1

IP interface name (Ex: "InternalNet"):

[Data 1]>

Would you like to configure an IPv4 address for this interface (y/n)? [Y]>

IPv4 Address (Ex: 192.168.1.2):

[192.168.1.1]>

Netmask (Ex: "255.255.255.0" or "0xffffffff"):

[24]>
```

```
Would you like to configure an IPv6 address for this interface (y/n)? [N]>
```

```
Ethernet interface:
```

```
1. Data 1
```

```
2. Data 2
```

```
3. Management
```

```
[1]>
```

```
Hostname:
```

```
[mail3.example.com]>
```

```
Do you want to enable Telnet on this interface? [N]>
```

```
Do you want to enable SSH on this interface? [N]>
```

```
Do you want to enable FTP on this interface? [N]>
```

```
Do you want to enable HTTP on this interface? [N]> y
```

```
Which port do you want to use for HTTP?
```

```
[80]> 80
```

```
Do you want to enable HTTPS on this interface? [N]> y
```

```
Which port do you want to use for HTTPS?
```

```
[443]> 443
```

```
You have not entered a certificate. To assure privacy, run
```

```
'certconfig' first. You may use the demo certificate
```

```
to test HTTPS, but this will not be secure.

Do you really wish to use a demo certificate? [N]> y

Both HTTP and HTTPS are enabled for this interface, should HTTP requests
redirect to the secure service? [Y]> y

Currently configured interfaces:

1. Data 1 (192.168.1.1/24 on Data 1: mail3.example.com)
2. Data 2 (192.168.2.1/24 on Data 2: mail3.example.com)
3. Management (192.168.42.42/24 on Management: mail3.example.com)

Choose the operation you want to perform:

- NEW - Create a new interface.
- EDIT - Modify an interface.
- GROUPS - Define interface groups.
- DELETE - Remove an interface.

[]>

mail3.example.com> commit

Please enter some comments describing your changes:

[]> enabled HTTP, HTTPS for Data 1

Changes committed: Mon Jul 7 13:21:23 2003

mail3.example.com>
```

## GUI のシステム情報

- [システム概要 (System Overview)] ページでは、次のことができます。
  - 主要システムのステータスとパフォーマンスの一部の情報を示す履歴グラフおよびテーブルを表示する。

- アプライアンスにインストールされている Cisco AsyncOS オペレーティング システムのバージョンを表示する。
  - 主要統計情報のサブセットを表示する。
- [システムステータス (System Status) ] ページには、システムのすべてのリアルタイム メールおよび DNS アクティビティの詳細が表示されます。また、システム統計情報のカウンタをリセットしたり、カウンタが最後にリセットされた時刻を表示したりすることもできます。

## GUI からの XML ステータスの収集

- XML ページを通じてステータスを表示するか、XML ステータス情報にプログラムでアクセスします。

XML ステータス機能は、電子メールのモニタリング統計情報にプログラムでアクセスする方法を提供します。最新のブラウザによっては、XML データを直接表示できるものもあります。

次の表に示す GUI の各ページの情報は、対応する URL にアクセスすることにより、動的な XML 出力としても使用できます。

| GUI のページ名                                                    | 対応する XML ステータス URL                                        |
|--------------------------------------------------------------|-----------------------------------------------------------|
| メール ステータス (Mail Status)                                      | <code>http://hostname/xml/status</code>                   |
| 特定のホストのホスト メール ステータス (Host Mail Status for a Specified Host) | <code>http://hostname/xml/hoststatus?hostname=host</code> |
| DNS ステータス (DNS Status)                                       | <code>http://hostname/xml/dnsstatus</code>                |
| 上位着信ドメイン (Top Incoming Domains)                              | <code>http://hostname/xml/topin</code>                    |
| 上位発信ドメイン (Top Outgoing Domains)                              | <code>http://hostname/xml/tophosts</code>                 |

<sup>a</sup> このページはデフォルトで、アクティブ受信者の番号順にソートされます。この順番を変更するには、URL に「?sort=**order**」を付加します。ここで、**order** は **conn\_out**、**deliv\_recip**、**soft\_bounced**、または **hard\_bounced** です。



## CHAPTER 33

# 高度なネットワーク構成

この章では、NIC ペアリング、VLAN、Direct Server Return など、一般に etherconfig コマンドを使って利用できる高度なネットワーク構成について説明します。

- 「イーサネット インターフェイスのメディア設定」 (P.33-1)
- 「ネットワーク インターフェイス カードのペアリング/チーミング」 (P.33-3)
- 「仮想ローカルエリア ネットワーク (VLAN)」 (P.33-9)
- 「Direct Server Return」 (P.33-16)
- 「イーサネット インターフェイスの最大伝送単位」 (P.33-21)

## イーサネット インターフェイスのメディア設定

イーサネット インターフェイスのメディア設定にアクセスするには、etherconfig コマンドを使用します。個々のイーサネット インターフェイスが現在の設定とともに一覧表示されます。インターフェイスを選択すると、可能なメディア設定が表示されます。例については、「[メディア設定の編集例](#)」 (P.33-2) を参照してください。

## etherconfig を使ったイーサネット インターフェイスのメディア設定の編集

etherconfig コマンドを使って、イーサネット インターフェイスのデュプレックス設定 (全二重/半二重) や速度 (10/100/1000 Mbps) を設定できます。デフォルトでは、インターフェイスが自動的にメディア設定を選択しますが、場合によってはこの設定を上書きする必要があります。



(注) 『Cisco IronPort AsyncOS for Email Configuration Guide』の「Setup and Installation」の説明に従って GUI のシステム設定ウィザード (またはコマンドライン インターフェイスの systemsetup コマンド) を完了し、変更を確定した場合は、デフォルトのイーサネット インターフェイス設定がアプライアンスにすでに設定されています。



(注) 一部の Cisco アプライアンスには光ファイバ ネットワーク インターフェイス オプションが含まれます。装備されている場合は、各アプライアンス上の使用可能なインターフェイスのリストに 2 つの追加イーサネット インターフェイス (Data 3 と Data 4) が表示されます。これらのギガビット光ファイバ

インターフェイスは、異種混在構成で銅線 (Data 1、Data 2、および Management) インターフェイスとペアにすることができます。「ネットワーク インターフェイス カードのペアリング/チーミング」(P.33-3) を参照してください。

## メディア設定の編集例

```
mail3.example.com> etherconfig

Choose the operation you want to perform:

- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
- MTU - View and configure MTU.

[]> media

Ethernet interfaces:

1. Data 1 (Autoselect: <100baseTX full-duplex>) 00:06:5b:f3:ba:6d
2. Data 2 (Autoselect: <100baseTX full-duplex>) 00:06:5b:f3:ba:6e
3. Management (Autoselect: <100baseTX full-duplex>) 00:02:b3:c7:a2:da

Choose the operation you want to perform:

- EDIT - Edit an ethernet interface.

[]> edit

Enter the name or number of the ethernet interface you wish to edit.

[]> 2

Please choose the Ethernet media options for the Data 2 interface.

1. Autoselect
2. 10baseT/UTP half-duplex
```



```
3. 10baseT/UTP full-duplex
4. 100baseTX half-duplex
5. 100baseTX full-duplex
6. 1000baseTX half-duplex
7. 1000baseTX full-duplex

[1]> 5
```

```
Ethernet interfaces:
```

```
1. Data 1 (Autoselect: <100baseTX full-duplex>) 00:06:5b:f3:ba:6d
2. Data 2 (100baseTX full-duplex: <100baseTX full-duplex>) 00:06:5b:f3:ba:6e
3. Management (Autoselect: <100baseTX full-duplex>) 00:02:b3:c7:a2:da
```

```
Choose the operation you want to perform:
```

```
- EDIT - Edit an ethernet interface.
```

```
[]>
```

```
Choose the operation you want to perform:
```

```
- MEDIA - View and edit ethernet media settings.
```

```
- PAIRING - View and configure NIC Pairing.
```

```
- VLAN - View and configure VLANs.
```

```
- LOOPBACK - View and configure Loopback.
```

```
- MTU - View and configure MTU.
```

```
[]>
```

## ネットワーク インターフェイス カードのペアリング/チーミング

NIC ペアリングで 2 つの物理データ ポートを組み合わせることにより、NIC からアップストリームのイーサネット ポートへのデータ パスに障害が発生した場合に、バックアップイーサネット インターフェイスを提供できます。ペアリングでは、基本的に各イーサネット インターフェイスをプライマリ インターフェイスおよびバックアップ インターフェイスとして設定します。プライマリ インターフェ

イスに障害が発生した場合（つまり、NIC とアップストリーム ノード間のキャリアが途切れた場合）は、バックアップ インターフェイスがアクティブになり、アラートが送信されます。Cisco のマニュアルでは、「NIC ペアリング」と「NIC チーミング」は同義語です。



(注)

NIC ペアリングは電子メール セキュリティ 仮想アプライアンスで使用できません。

十分な数のデータ ポートがあれば、複数の NIC ペアを作成できます。ペアを作成するときは、任意のデータ ポートを組み合わせることができます。次の例を参考にしてください。

- Data 1 と Data 2
- Data 3 と Data 4
- Data 2 と Data 3
- その他

一部の Cisco アプライアンスには光ファイバ ネットワーク インターフェイス オプションが含まれます。装備されている場合は、各アプライアンス上の使用可能なインターフェイスのリストに 2 つの追加イーサネット インターフェイス (Data 3 と Data 4) が表示されます。これらのギガビット光ファイバ インターフェイスは、異種混在構成で銅線 (Data 1、Data 2、および Management) インターフェイスとペアにすることができます。

## NIC ペアリングと VLAN

VLAN (「仮想ローカル エリア ネットワーク (VLAN)」(P.33-9) を参照) は、プライマリ インターフェイスにのみ設定できます。

## NIC ペアの名前

NIC ペアを作成するときは、そのペアを参照するときに使用する名前を指定する必要があります。バージョン 4.5 よりも前の AsyncOS で作成した NIC ペアには、アップグレード後、自動的に「Pair 1」というデフォルト名が指定されます。

NIC ペアリングに関して生成されたアラートは、特定の NIC ペアを名前参照します。

## NIC ペアリング/チーミングの設定とテスト

イーサネットのメディア設定を確認したら、etherconfig コマンドを使って NIC ペアリングを設定します。ペアを参照するときに使用する名前を入力するように求められます。

アクティブなインターフェイスを切り替えるには、failover サブコマンドを使用します。プライマリ NIC がオンライン状態に戻っても、自動的にプライマリ NIC には切り替わりません。その場合は、(failover コマンドを使用して) 明示的にプライマリ NIC に切り替えるか、バックアップ NIC に障害が発生するまで、バックアップ インターフェイスがアクティブな状態を維持します。「NIC ペアリングに対する failover サブコマンドの使用」(P.33-7) を参照してください。

NIC ペアを削除するには、delete サブコマンドを使用します。

NIC ペアリングを設定するときは、failover を除くすべての設定変更で確定が必要であることに注意してください。failover コマンドは、NIC ペアリングの設定を確定した後 15 秒ごとに行われるポーリングの次の間隔で強制的にフェールオーバーを実行します。

## NIC ペアリングと既存のリスナー

リスナーが割り当てられたインターフェイスで NIC ペアリングをイネーブルにすると、バックアップ インターフェイスに割り当てられた全リスナーの削除、再割り当て、ディセーブル化のいずれかを選択するように求められます。

## etherconfig コマンドを使った NIC ペアリングのイネーブル化



(注) NIC ペアリングは電子メール セキュリティ 仮想アプライアンスで使用できません。

```
mail3.example.com> etherconfig
```

```
Choose the operation you want to perform:
```

- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
- MTU - View and configure MTU.

```
[> pairing
```

```
Paired interfaces:
```

```
Choose the operation you want to perform:
```

- NEW - Create a new pairing.

```
[> new
```

```
Please enter a name for this pair (Ex: "Pair 1"):
```

```
[> Pair 1
```

```
Warning: The backup (Data 2) for the NIC Pair is currently configured with one or more IP addresses. If you continue, the Data 2 interface will be deleted.
```

```
Do you want to continue? [N]> y
```

```
The interface you are deleting is currently used by listener "OutgoingMail".
```

```
What would you like to do?
```

1. Delete: Remove the listener and all its settings.
2. Change: Choose a new interface.
3. Ignore: Leave the listener configured for interface "Data 2" (the listener will be disabled until you add a new interface named "Data 2" or edit the listener's settings).

```
[1]>
```

```
Listener OutgoingMail deleted for mail3.example.com.
```

```
Interface Data 2 deleted.
```

```
Paired interfaces:
```

```
1. Pair 1:
```

```
 Primary (Data 1) Active, Link is up
```

```
 Backup (Data 2) Standby, Link is up
```

```
Choose the operation you want to perform:
```

- FAILOVER - Manually failover to other port.
- DELETE - Delete a pairing.
- STATUS - Refresh status.

```
[]>
```

```
mail3.example.com> commit
```



(注)

---

NIC ペアを作成したら、必ずテストしてください。詳細については、「[NIC ペアリングの確認](#)」(P.33-9) を参照してください。

---

## NIC ペアリングに対する failover サブコマンドの使用

この例では、手動のフェールオーバーを実行し、Data 2 インターフェイスを強制的にプライマリ インターフェイスにします。CLI で変更を確認するには、status サブコマンドを実行する必要があります。

```
mail3.example.com> etherconfig
```

```
Choose the operation you want to perform:
```

- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
- MTU - View and configure MTU.

```
[> pairing
```

```
Paired interfaces:
```

```
1. Pair 1:
```

```
 Primary (Data 1) Active, Link is up
```

```
 Backup (Data 2) Standby, Link is up
```

```
Choose the operation you want to perform:
```

- FAILOVER - Manually failover to other port.
- DELETE - Delete a pairing.
- STATUS - Refresh status.

```
[> failover
```

```
Paired interfaces:
```

```
1. Pair 1:
```

```
 Primary (Data 1) Active, Link is up
```

```
 Backup (Data 2) Standby, Link is up
```

## ■ ネットワーク インターフェイス カードのペアリング/チーミング

```
Choose the operation you want to perform:

- FAILOVER - Manually failover to other port.

- DELETE - Delete a pairing.

- STATUS - Refresh status.
```

```
[> status
```

```
Paired interfaces:
```

```
1. Pair 1:
```

```
 Primary (Data 1) Standby, Link is up
```

```
 Backup (Data 2) Active, Link is up
```

```
Choose the operation you want to perform:

- FAILOVER - Manually failover to other port.

- DELETE - Delete a pairing.

- STATUS - Refresh status.
```

```
[>
```

```
Choose the operation you want to perform:

- MEDIA - View and edit ethernet media settings.

- PAIRING - View and configure NIC Pairing.

- VLAN - View and configure VLANs.

- LOOPBACK - View and configure Loopback.

- MTU - View and configure MTU.
```

```
[>
```

## NIC ペアリングの確認

### 手順

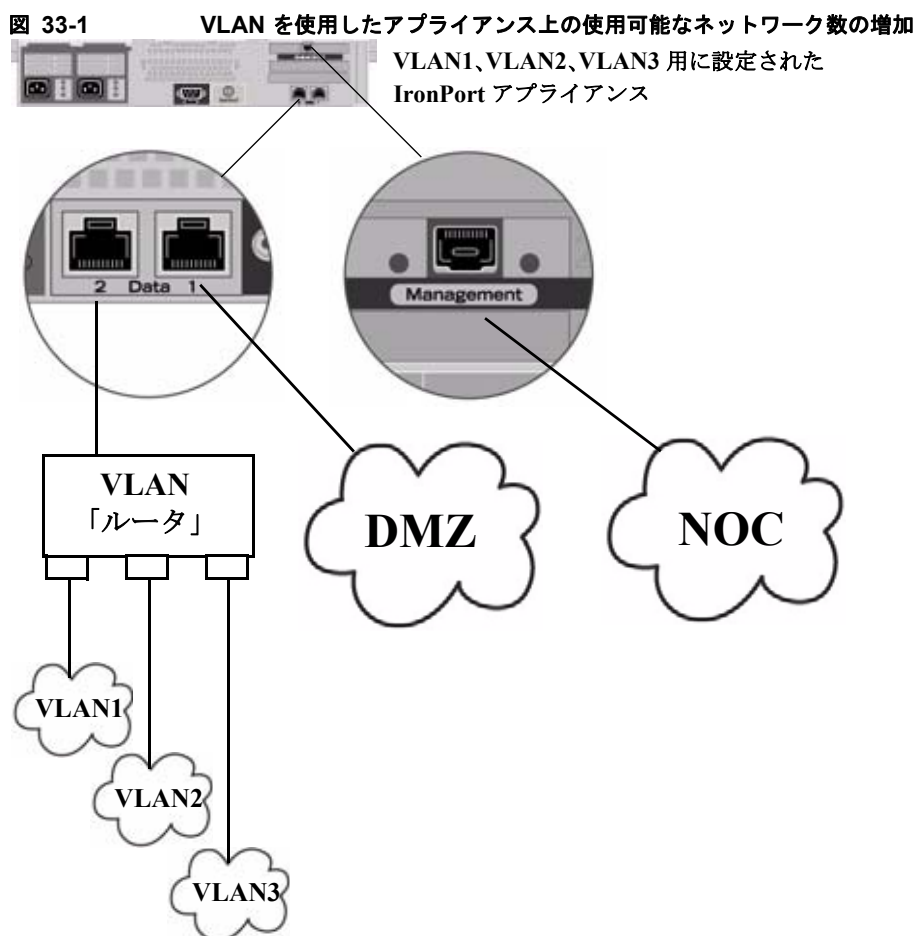
- ステップ 1** CLI の ping コマンドを使って、ペアになっているインターフェイスをテストします。NIC ペアと同じサブネット上に存在し、独立したソースによって ping が返ることが確認された IP アドレスに対して、次のように ping を実行します。

```
mail3.example.com> ping x.x.x.x
```

- ステップ 2** failover コマンドを実行します (etherconfig -> pairing -> failover)。15 秒間待機します。
- ステップ 3** バックアップ NIC がアクティブなインターフェイスになったら、再度 CLI の ping コマンドを使って、ペアになっているインターフェイスをテストします。
- ステップ 4** 最後に、再度 failover を実行して NIC ペアをデフォルトの (プライマリ インターフェイスがアクティブな) 状態に戻します。

## 仮想ローカル エリア ネットワーク (VLAN)

VLAN は、物理データ ポートにバインドされた仮想的なローカル エリア ネットワークです。VLAN を設定することにより、Cisco アプライアンスが接続できるネットワークの数を、装備されている物理的なインターフェイスの数よりも増やすことができます。たとえば、Cisco C6x アプライアンスには Data 1、Data 2、および管理の 3 つのインターフェイスがあります。VLAN を使って、既存のリスナーに対応する別個の「ポート」上に追加のネットワークを定義できます。(詳細については、[付録 A 「アプライアンスへのアクセス」](#)を参照してください)。任意の物理ネットワーク ポートに複数の VLAN を設定できます。[図 33-1](#) に、Data 2 インターフェイスに複数の VLAN を設定する例を示します。



VLAN を使ってネットワークを分割することにより、セキュリティを向上させたり、管理作業を軽減したり、帯域幅を拡大したりできます。VLAN は、「VLAN DDDD」という形式の名前を持つ動的な「データ ポート」として表示されます。「DDDD」は最大 4 桁の ID です (たとえば、VLAN 2、VLAN 4094 など)。AsyncOS は、最大 30 の VLAN をサポートします。同じ Cisco アプライアンス上で重複する VLAN ID は設定できません。

## VLAN と物理ポート

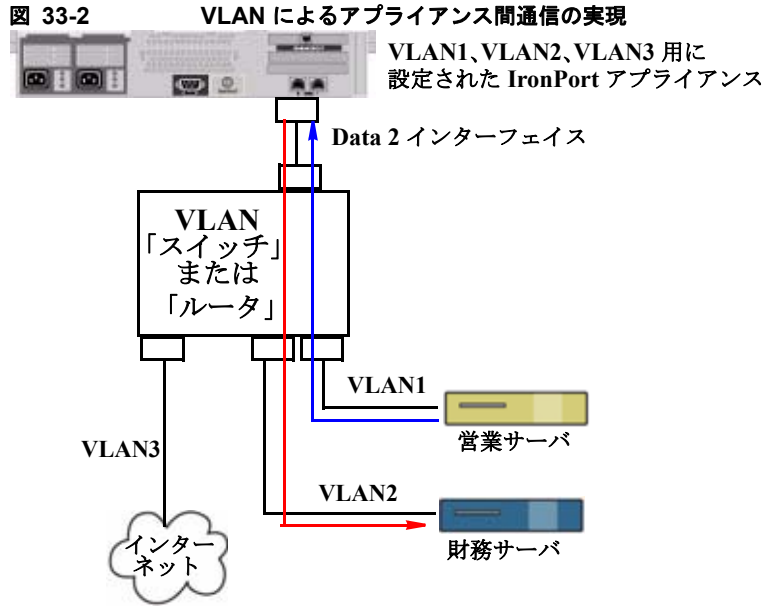
物理ポートを VLAN に追加するために IP アドレスを設定する必要はありません。VLAN を作成した物理ポートに VLAN 以外のトラフィックを受信する IP アドレスを設定できるため、VLAN のトラフィックと VLAN 以外のトラフィックの両方を同じインターフェイスで受信できます。

VLAN は、一部の Cisco X10x、C3x、および C6x アプライアンスで使用可能な光ファイバデータポートを含むすべての「Data」ポートおよび「Management」ポート上に作成できます。

VLAN は、NIC ペアリング (ペアになっている NIC で使用可能) や Direct Server Return (DSR) とともに使用できます。

図 33-2 は、VLAN の制限事項のために直接通信できない 2 台のメールサーバが Cisco アプライアンス経由でどのようにメールを送信するかを示す使用例です。青い線は、営業ネットワーク (VLAN1) からアプライアンスに送信されたメールを示しています。アプライアンスはこのメールを通常どおりに処理し、配信時に VLAN の情報を含むタグをパケットに追加します (赤い線)。





## VLAN の管理

VLAN の作成、編集、および削除を行うには、`etherconfig` コマンドを使用します。作成した VLAN は、[ ネットワーク (Network) ] > [ インターフェイス (Interfaces) ] ページまたは CLI の `interfaceconfig` コマンドを使って設定できます。必ずすべての変更を確認してください。

### etherconfig コマンドによる新しい VLAN の作成

この例では、Data 1 ポート上に 2 つの VLAN (VLAN 31 と VLAN 34) を作成します。

```
mail3.example.com> etherconfig

Choose the operation you want to perform:

- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
- MTU - View and configure MTU.

[]> vlan

VLAN interfaces:
```

Choose the operation you want to perform:

- NEW - Create a new VLAN.

[> **new**

VLAN ID for the interface (Ex: "34"):

[> **34**

Enter the name or number of the ethernet interface you wish bind to:

1. Data 1

2. Data 2

3. Management

[1]> **1**

VLAN interfaces:

1. VLAN 34 (Data 1)

Choose the operation you want to perform:

- NEW - Create a new VLAN.

- EDIT - Edit a VLAN.

- DELETE - Delete a VLAN.

[> **new**

VLAN ID for the interface (Ex: "34"):

[> **31**

Enter the name or number of the ethernet interface you wish bind to:

1. Data 1

2. Data 2

3. Management

```
[1]> 1
```

```
VLAN interfaces:
```

```
1. VLAN 31 (Data 1)
```

```
2. VLAN 34 (Data 1)
```

```
Choose the operation you want to perform:
```

```
- NEW - Create a new VLAN.
```

```
- EDIT - Edit a VLAN.
```

```
- DELETE - Delete a VLAN.
```

```
[]>
```

```
Choose the operation you want to perform:
```

```
- MEDIA - View and edit ethernet media settings.
```

```
- PAIRING - View and configure NIC Pairing.
```

```
- VLAN - View and configure VLANs.
```

```
- LOOPBACK - View and configure Loopback.
```

```
- MTU - View and configure MTU.
```

```
[]>
```

## interfaceconfig コマンドによる VLAN 上の IP インターフェイスの作成

この例では、VLAN 31 イーサネット インターフェイス上に新しい IP インターフェイスを作成します。



(注)

---

インターフェイスに変更を加えると、アプライアンスとの接続が閉じることがあります。

---

```
mail3.example.com> interfaceconfig
```

```
Currently configured interfaces:
```

```
1. Data 1 (10.10.1.10/24: example.com)
```

```
2. Management (10.10.0.10/24: example.com)
```

Choose the operation you want to perform:

- NEW - Create a new interface.
- EDIT - Modify an interface.
- GROUPS - Define interface groups.
- DELETE - Remove an interface.

[ ]> **new**

Please enter a name for this IP interface (Ex: "InternalNet"):

[ ]> **InternalVLAN31**

Would you like to configure an IPv4 address for this interface (y/n)? [Y]>

IPv4 Address (Ex: 10.10.10.10):

[ ]> **10.10.31.10**

Netmask (Ex: "255.255.255.0" or "0xffffffff00"):  
[255.255.255.0]>

Would you like to configure an IPv6 address for this interface (y/n)? [N]>

Ethernet interface:

1. Data 1
2. Data 2
3. Management
4. VLAN 31
5. VLAN 34

[1]> **4**

```
Hostname:

[]> mail31.example.com

Do you want to enable Telnet on this interface? [N]>

Do you want to enable SSH on this interface? [N]>

Do you want to enable FTP on this interface? [N]>

Do you want to enable HTTP on this interface? [N]>

Do you want to enable HTTPS on this interface? [N]>

Currently configured interfaces:

1. Data 1 (10.10.1.10/24: example.com)
2. InternalVLAN31 (10.10.31.10/24: mail31.example.com)
3. Management (10.10.0.10/24: example.com)

Choose the operation you want to perform:

- NEW - Create a new interface.
- EDIT - Modify an interface.
- GROUPS - Define interface groups.
- DELETE - Remove an interface.

[]>

mail3.example.com> commit
```

[ネットワーク (Network) ]> [リスナー (Listeners) ] ページを使って VLAN を設定することもできます。

図 33-3 GUI で新しい IP インターフェイスを作成するときに VLAN を使用する  
Add IP Interface

| IP Interface Settings                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                 |         |      |                              |    |                                 |    |                              |    |                               |    |                                |     |
|-----------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|------|------------------------------|----|---------------------------------|----|------------------------------|----|-------------------------------|----|--------------------------------|-----|
| Name:                                                                                                                 | InternalVLAN31                                                                                                                                                                                                                                                                                                                                                                                                                  |         |      |                              |    |                                 |    |                              |    |                               |    |                                |     |
| Ethernet Port:                                                                                                        | VLAN 31                                                                                                                                                                                                                                                                                                                                                                                                                         |         |      |                              |    |                                 |    |                              |    |                               |    |                                |     |
| IP Address:                                                                                                           | 10.10.31.10                                                                                                                                                                                                                                                                                                                                                                                                                     |         |      |                              |    |                                 |    |                              |    |                               |    |                                |     |
| Netmask:                                                                                                              | 255.255.255.0                                                                                                                                                                                                                                                                                                                                                                                                                   |         |      |                              |    |                                 |    |                              |    |                               |    |                                |     |
| Hostname:                                                                                                             | mail31.example.com                                                                                                                                                                                                                                                                                                                                                                                                              |         |      |                              |    |                                 |    |                              |    |                               |    |                                |     |
| Services:                                                                                                             | <table border="1"> <thead> <tr> <th>Service</th> <th>Port</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> FTP</td> <td>21</td> </tr> <tr> <td><input type="checkbox"/> Telnet</td> <td>23</td> </tr> <tr> <td><input type="checkbox"/> SSH</td> <td>22</td> </tr> <tr> <td><input type="checkbox"/> HTTP</td> <td>80</td> </tr> <tr> <td><input type="checkbox"/> HTTPS</td> <td>443</td> </tr> </tbody> </table> | Service | Port | <input type="checkbox"/> FTP | 21 | <input type="checkbox"/> Telnet | 23 | <input type="checkbox"/> SSH | 22 | <input type="checkbox"/> HTTP | 80 | <input type="checkbox"/> HTTPS | 443 |
| Service                                                                                                               | Port                                                                                                                                                                                                                                                                                                                                                                                                                            |         |      |                              |    |                                 |    |                              |    |                               |    |                                |     |
| <input type="checkbox"/> FTP                                                                                          | 21                                                                                                                                                                                                                                                                                                                                                                                                                              |         |      |                              |    |                                 |    |                              |    |                               |    |                                |     |
| <input type="checkbox"/> Telnet                                                                                       | 23                                                                                                                                                                                                                                                                                                                                                                                                                              |         |      |                              |    |                                 |    |                              |    |                               |    |                                |     |
| <input type="checkbox"/> SSH                                                                                          | 22                                                                                                                                                                                                                                                                                                                                                                                                                              |         |      |                              |    |                                 |    |                              |    |                               |    |                                |     |
| <input type="checkbox"/> HTTP                                                                                         | 80                                                                                                                                                                                                                                                                                                                                                                                                                              |         |      |                              |    |                                 |    |                              |    |                               |    |                                |     |
| <input type="checkbox"/> HTTPS                                                                                        | 443                                                                                                                                                                                                                                                                                                                                                                                                                             |         |      |                              |    |                                 |    |                              |    |                               |    |                                |     |
| Redirect HTTP Requests to HTTPS: <input type="checkbox"/> Enable Redirect (HTTP and HTTPS Services will be turned on) |                                                                                                                                                                                                                                                                                                                                                                                                                                 |         |      |                              |    |                                 |    |                              |    |                               |    |                                |     |
| <div style="display: flex; justify-content: space-between;"> <span>Cancel</span> <span>Submit</span> </div>           |                                                                                                                                                                                                                                                                                                                                                                                                                                 |         |      |                              |    |                                 |    |                              |    |                               |    |                                |     |

## Direct Server Return

Direct Server Return (DSR) は、同じ Virtual IP (VIP; 仮想 IP) を共有する複数の Cisco アプライアンス間で負荷を分散するための軽量負荷分散メカニズムをサポートする機能です。

DSR は、Cisco アプライアンスの「ループバック」イーサネット インターフェイス上に作成された IP インターフェイスを介して実装されます。



(注) Cisco アプライアンスの負荷分散の設定は、このマニュアルでは取り上げません。

## Direct Server Return のイネーブル化

DSR をイネーブルにするには、参加している各アプライアンスの「ループバック」イーサネット インターフェイスをイネーブルにします。次に、CLI の `interfaceconfig` コマンドまたは GUI の [ネットワーク (Network)] > [インターフェイス (Interfaces)] ページを使ってループバック インターフェイス上に Virtual IP (VIP; 仮想 IP) を持つ IP インターフェイスを作成します。最後に、CLI の `listenerconfig` コマンドまたは GUI の [ネットワーク (Network)] > [リスナー (Listeners)] ページを使って新しい IP インターフェイス上にリスナーを作成します。必ずすべての変更を確定してください。

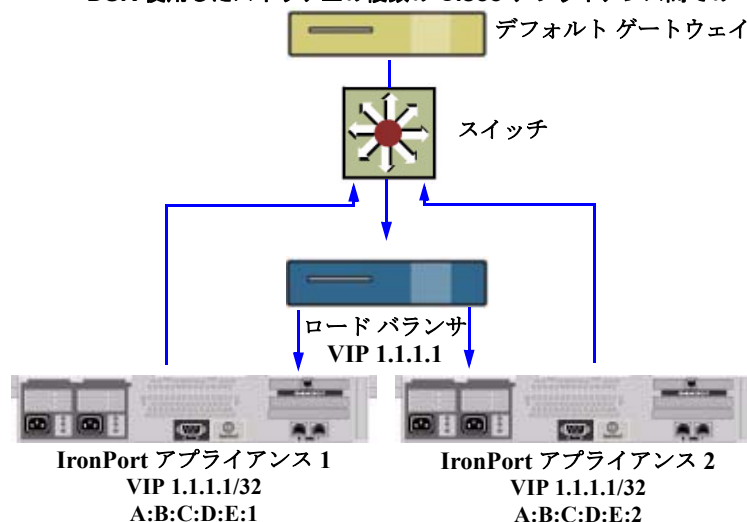


(注) ループバック インターフェイスを使用した場合、アプライアンスはそのインターフェイスの ARP 応答を発行しません。

DSR をイネーブルにするときは、次のルールが適用されます。

- すべてのシステムが同じ Virtual IP (VIP; 仮想 IP) アドレスを使用します。
- すべてのシステムがロード バランサと同じスイッチおよびサブネット上にある必要があります。

図 33-4 DSR 使用したスイッチ上の複数の Cisco アプライアンス間でのロード バランス



## etherconfig コマンドによるループバック インターフェイスのイネーブル化

イネーブルになったループバック インターフェイスは、他のインターフェイス (Data 1 など) と同じように扱われます。

```
mail3.example.com> etherconfig
```

```
Choose the operation you want to perform:
```

- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
- MTU - View and configure MTU.

```
[]> loopback
```

```
Currently configured loopback interface:
```

```
Choose the operation you want to perform:
```

- ENABLE - Enable Loopback Interface.

```
[]> enable
```

```
Currently configured loopback interface:
```

```
1. Loopback
```

```
Choose the operation you want to perform:
```

```
- DISABLE - Disable Loopback Interface.
```

```
[]>
```

```
Choose the operation you want to perform:
```

```
- MEDIA - View and edit ethernet media settings.
```

```
- PAIRING - View and configure NIC Pairing.
```

```
- VLAN - View and configure VLANs.
```

```
- LOOPBACK - View and configure Loopback.
```

```
- MTU - View and configure MTU.
```

```
[]>
```

## interfaceconfig コマンドによるループバック上の IP インターフェイスの作成

ループバック インターフェイス上に IP インターフェイスを作成します。

```
mail3.example.com> interfaceconfig
```

```
Currently configured interfaces:
```

```
1. Data 1 (10.10.1.10/24: example.com)
```

```
2. InternalV1 (10.10.31.10/24: mail31.example.com)
```

```
3. Management (10.10.0.10/24: example.com)
```

```
Choose the operation you want to perform:
```

```
- NEW - Create a new interface.
```

```
- EDIT - Modify an interface.
```

```
- GROUPS - Define interface groups.
```

```
- DELETE - Remove an interface.
```



```
[> new
```

```
Please enter a name for this IP interface (Ex: "InternalNet"):
```

```
[> LoopVIP
```

```
Would you like to configure an IPv4 address for this interface (y/n)? [Y]>
```

```
IPv4 Address (Ex: 10.10.10.10):
```

```
[> 10.10.1.11
```

```
Netmask (Ex: "255.255.255.0" or "0xffffffff"):
```

```
[255.255.255.0]> 255.255.255.255
```

```
Would you like to configure an IPv6 address for this interface (y/n)? [N]>
```

```
Ethernet interface:
```

```
1. Data 1
```

```
2. Data 2
```

```
3. Loopback
```

```
4. Management
```

```
5. VLAN 31
```

```
6. VLAN 34
```

```
[1]> 3
```

```
Hostname:
```

```
[> example.com
```

```
Do you want to enable Telnet on this interface? [N]>
```

```
Do you want to enable SSH on this interface? [N]>

Do you want to enable FTP on this interface? [N]>

Do you want to enable HTTP on this interface? [N]>

Do you want to enable HTTPS on this interface? [N]>

Currently configured interfaces:

1. Data 1 (10.10.1.10/24: example.com)
2. InternalV1 (10.10.31.10/24: mail31.example.com)
3. LoopVIP (10.10.1.11/24: example.com)
4. Management (10.10.0.10/24: example.com)

Choose the operation you want to perform:

- NEW - Create a new interface.
- EDIT - Modify an interface.
- GROUPS - Define interface groups.
- DELETE - Remove an interface.

[]>

mail3.example.com> commit
```

## 新しい IP インターフェイス上のリスナーの作成

GUI または CLI を使って新しい IP インターフェイス上にリスナーを作成します。たとえば、[図 33-5](#) に示すように、新たに作成した IP インターフェイスを GUI の [リスナーを追加 (Add Listener) ] ページで選択できます。

図 33-5 新しいループバック IP インターフェイス上のリスナーの作成  
Add Listener

| Listener Settings            |                                                                                                                                                                                                                                                                                                       |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name:                        | <input type="text"/>                                                                                                                                                                                                                                                                                  |
| Type of Listener:            | <input checked="" type="radio"/> Public<br><input type="radio"/> Private                                                                                                                                                                                                                              |
| Interface:                   | <input type="text" value="Data 1 (10.10.1.10/24; example.com)"/> TCP Port: <input type="text" value="25"/>                                                                                                                                                                                            |
| Bounce Profile:              | <input type="text" value="Data 1 (10.10.1.10/24; example.com)"/><br><input type="text" value="InternalV1 (10.10.31.10/24; mail31.example.com)"/><br><input type="text" value="LoopVIP (10.10.11.10/24; mail11.example.com)"/><br><input type="text" value="Management (10.10.2.10/24; example.com)"/> |
| Disclaimer Above:            | <input type="text" value="Management (10.10.2.10/24; example.com)"/><br><small>Disclaimer text will be applied above the message body.</small>                                                                                                                                                        |
| Disclaimer Below:            | <input type="text" value="None"/><br><small>Disclaimer text will be applied below the message body.</small>                                                                                                                                                                                           |
| SMTP Authentication Profile: | <input type="text" value="None"/>                                                                                                                                                                                                                                                                     |
| Certificate:                 | <input type="text" value="System Default"/>                                                                                                                                                                                                                                                           |

## イーサネット インターフェイスの最大伝送単位

最大伝送単位 (MTU) は、イーサネット インターフェイスが受け入れる最大のデータ単位です。etherconfig コマンドを使用してイーサネット インターフェイスの MTU を減らすことができます。イーサネット インターフェイスが受け入れることができる最大 MTU のデフォルト MTU サイズは 1500 バイトです。

インターフェイスの MTU を編集するには:

```
mail3.example.com> etherconfig
```

```
Choose the operation you want to perform:
```

- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
- MTU - View and configure MTU.

```
[]> mtu
```

```
Ethernet interfaces:
```

1. Data 1 mtu 1400
2. Data 2 default mtu 1500
3. Management default mtu 1500

Choose the operation you want to perform:

- EDIT - Edit an ethernet interface.

[> **edit**

Enter the name or number of the ethernet interface you wish to edit.

[> 2

Please enter a non-default (1500) MTU value for the Data 2 interface.

[> **1200**

Ethernet interfaces:

1. Data 1 mtu 1400

2. Data 2 mtu 1200

3. Management default mtu 1500

Choose the operation you want to perform:

- EDIT - Edit an ethernet interface.

[>



# CHAPTER 34

## ロギング

---

Cisco 電子メール セキュリティ アプライアンスの重要な機能に、ロギング機能があります。AsyncOS は多くのログ タイプを生成し、さまざまなタイプの情報を記録できます。ログ ファイルには、システムの各種コンポーネントによる通常のアクティビティとエラーの記録が保持されます。この情報は、Cisco アプライアンスをモニタするときや、パフォーマンスのトラブルシューティングまたはチェックを行うときに役立つ場合があります。

- 「概要」 (P.34-1)
- 「ログ タイプ」 (P.34-9)
- 「ログ サブスクリプション」 (P.34-39)

### 概要

- 「ログ ファイルおよびログ サブスクリプションについて」 (P.34-1)
- 「ログ タイプ」 (P.34-2)
- 「ログ取得方法」 (P.34-7)

### ログ ファイルおよびログ サブスクリプションについて

ログは、AsyncOS の電子メール動作に関する重要な情報を収集する、簡潔で効率的な方法です。これらのログには、Cisco アプライアンスでのアクティビティに関する情報が記録されます。情報は、パウンス ログや配信ログなど、表示するログによって異なります。

ほとんどのログは、プレーンテキスト (ASCII) 形式で記録されますが、配信ログはリソースの効率性を保つためにバイナリ形式で記録されます。ASCII テキスト情報は、任意のテキスト エディタで読むことができます。

シスコは、複数の Cisco アプライアンスからのログに対応する集中化レポートおよびトラッキング ツールとして、M-Series セキュリティ管理アプライアンス提供しています。詳細については、Cisco の担当者にお問い合わせください。

ログ サブスクリプションはログ タイプを名前、ログ レベル、およびサイズや宛先情報などのその他の制約に関連付けます。同じログ タイプで複数のサブスクリプションを使用できます。

## ログ タイプ

ログ タイプは、メッセージデータ、システム統計情報、バイナリまたはテキストデータなど、生成されたログにどの情報が記録されるかを示します。ログ タイプは、ログ サブスクリプションを作成するときに選択します。詳細については、「[ログ サブスクリプション](#)」(P.34-39) を参照してください。

Cisco AsyncOS for Email では、次のログ タイプが生成されます。

表 34-1 ログ タイプ

| ログ                          | 説明                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>IronPort テキスト メール ログ</b> | テキスト メール ログには、電子メール システムの動作に関する情報が記録されます。たとえば、メッセージの受信、メッセージの配信試行、接続のオープンとクローズ、バウンス、TLS 接続などです。                                                                                                                                                                                                                                                                                         |
| <b>qmail 形式メール ログ</b>       | qmail 形式配信ログには、次の配信ログと同じ電子メール システムの動作に関する情報が記録されますが、qmail 形式で格納されます。                                                                                                                                                                                                                                                                                                                    |
| <b>配信ログ</b>                 | 配信ログには、Cisco アプライアンスの電子メール配信動作に関する重要な情報が記録されます。たとえば、配信試行時の各受信者の配信やバウンスに関する情報などです。ログ メッセージは「ステートレス」です。つまり、関連するすべての情報が各ログ メッセージに記録されるので、ユーザは、現在の配信試行に関する情報について前のログ メッセージを参照する必要がありません。配信ログは、リソースの効率性を保つためにバイナリ形式で記録されます。配信ログ ファイルは、提供されるユーティリティを使用して XML または CSV (カンマ区切り値) 形式に変換し、後処理する必要があります。変換ツールは、次の場所にあります。<br><a href="http://support.ironport.com">http://support.ironport.com</a> |
| <b>バウンス ログ</b>              | バウンス ログには、バウンスされた受信者の情報が記録されます。バウンスされた各受信者を記録する情報には、メッセージ ID、受信者 ID、エンベロープ送信元アドレス、エンベロープ宛先アドレス、受信者がバウンスされる理由、および受信者ホストからの応答コードが含まれます。また、バウンスされた各受信者メッセージの一定量を記録するように選択することもできます。この容量はバイト単位で定義され、デフォルトはゼロです。                                                                                                                                                                             |
| <b>ステータス ログ</b>             | このログ ファイルには、status detail および dnsstatus などの CLI ステータス コマンドで検出されたシステムの統計情報が記録されます。記録期間は、logconfig の setup サブコマンドを使用して設定します。ステータス ログでレポートされるカウンタまたはレートは、前回カウンタがリセットされた時点からの値です。                                                                                                                                                                                                           |
| <b>ドメイン デバッグ ログ</b>         | ドメイン デバッグ ログには、Cisco アプライアンスと指定の受信者ホスト間の SMTP 会話でのクライアントとサーバの通信が記録されます。このログ タイプは、特定の受信者ホストに関する問題のデバッグに使用できます。ログ ファイルに記録する SMTP セッションの総数を指定する必要があります。セッションが記録されるにつれ、この数は減少していきます。ログ サブスクリプションを削除または編集して、すべてのセッションが記録される前にドメイン デバッグを停止できます。                                                                                                                                               |
| <b>インジェクション デバッグ ログ</b>     | インジェクション デバッグ ログには、Cisco アプライアンスと、システムに接続している指定のホスト間の SMTP 会話記録されます。インジェクション デバッグ ログは、インターネット上の Cisco アプライアンスとホスト間の通信に関する問題をトラブルシューティングするのに役立ちます。                                                                                                                                                                                                                                       |

表 34-1 ログタイプ (続き)

| ログ            | 説明                                                                                                                                                                                                                                                                                                                     |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| システム ログ       | システム ログには、ブート情報、DNS ステータス情報、および commit コマンドを使用してユーザが入力したコメントが記録されます。システム ログは、アプライアンスの基本的な状態のトラブルシューティングに役立ちます。                                                                                                                                                                                                         |
| CLI 監査ログ      | CLI 監査ログには、システム上のすべての CLI アクティビティが記録されます。                                                                                                                                                                                                                                                                              |
| FTP サーバ ログ    | FTP ログには、インターフェイスでイネーブルになっている FTP サービスの情報が記録されます。接続の詳細とユーザ アクティビティが記録されます。                                                                                                                                                                                                                                             |
| GUI ログ        | HTTP ログを参照してください。                                                                                                                                                                                                                                                                                                      |
| HTTP ログ       | HTTP ログには、インターフェイスでイネーブルになっている HTTP サービス、セキュア HTTP サービス、またはその両方のサービスに関する情報が記録されます。HTTP を介してグラフィカル ユーザ インターフェイス (GUI) にアクセスするため、HTTP ログは基本的に、CLI 監査ログの GUI 版になっています。GUI でアクセスされるセッション データ (新しいセッション、セッションの期限切れ) やページが記録されます。<br><br>これらのログには、SMTP トランザクションに関する情報 (たとえば、アプライアンスから電子メールで送信されるスケジュール済みレポートに関する情報) も記録されます。 |
| NTP ログ        | NTP ログには、設定されている任意の Network Time Protocol (NTP; ネットワーク タイム プロトコル) サーバとアプライアンス間の会話が記録されます。詳細については、『Cisco IronPort AsyncOS for Email Configuration Guide』の「System Administration」の章の「Editing the Network Time Protocol (NTP) Configuration (Time Keeping Method)」を参照してください。                                              |
| LDAP デバッグ ログ  | LDAP デバッグ ログは、LDAP インストールのデバッグを目的としています (『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「LDAP Queries」を参照してください)。Cisco アプライアンスが LDAP サーバに送信しているクエリーに関する有用な情報がここに記録されます。                                                                                                                               |
| アンチスパム ログ     | アンチスパム ログには、最新のアンチスパム ルールのアップデート受信に関するステータスなど、システムのアンチスパム スキャン機能のステータスが記録されます。また、Context Adaptive Scanning Engine に関するすべてのログもここに記録されます。                                                                                                                                                                                |
| アンチスパム アーカイブ  | アンチスパム スキャン機能をイネーブルにすると、スキャンされ、「メッセージのアーカイブ」アクションに関連付けられたメッセージがここにアーカイブされます。この形式は、mbox 形式のログ ファイルです。アンチスパム エンジンの詳細については、『Cisco IronPort AsyncOS for Email Configuration Guide』の「Anti-Spam」の章を参照してください。                                                                                                                 |
| アンチウイルス ログ    | アンチウイルス ログには、最新のアンチウイルス アイデンティティ ファイルのアップデート受信に関するステータスなど、システムのアンチウイルス スキャン機能のステータスが記録されます。                                                                                                                                                                                                                            |
| アンチウイルス アーカイブ | アンチウイルス エンジンをイネーブルにすると、スキャンされ、「メッセージのアーカイブ」アクションに関連付けられたメッセージがここにアーカイブされます。この形式は、mbox 形式のログ ファイルです。詳細については、『Cisco IronPort AsyncOS for Email Configuration Guide』の「Anti-Virus」の章を参照してください。                                                                                                                             |

表 34-1 ログタイプ (続き)

| ログ                     | 説明                                                                                                                                                                                                                                                  |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| スキャン ログ                | スキャン ログには、スキャン エンジンに関するすべての LOG および COMMON メッセージが保持されます (『Cisco IronPort AsyncOS for Email Configuration Guide』の「System Administration」の章の「Alerts」を参照してください)。これは一般に、アプリケーションの障害、送信されたアラート、失敗したアラート、およびログ エラー メッセージになります。このログは、システム全体のアラートには適用されません。 |
| IronPort スпам隔離ログ      | IronPort スпам隔離ログには、Cisco スпам隔離プロセスに関連付けられたアクションが記録されます。                                                                                                                                                                                           |
| IronPort スпам隔離 GUI ログ | IronPort スпам隔離ログには、GUI を介した設定、エンド ユーザ認証、およびエンド ユーザ アクション (電子メールの解放など) を含む、Cisco スпам隔離に関連付けられたアクションが記録されます。                                                                                                                                        |
| SMTP 会話ログ              | SMTP 会話ログには、着信および発信 SMTP 会話のすべての部分が記録されます。                                                                                                                                                                                                          |
| セーフリスト/ブロックリスト ログ      | セーフリスト/ブロックリスト ログには、セーフリスト/ブロックリストの設定に関するデータとデータベースが記録されます。                                                                                                                                                                                         |
| レポート ログ                | レポート ログには、集中化レポート サービスのプロセスに関連付けられたアクションが記録されます。                                                                                                                                                                                                    |
| レポート クエリー ログ           | レポート クエリー ログには、アプライアンスで実行されるレポート クエリーに関連付けられたアクションが記録されます。                                                                                                                                                                                          |
| アップデート ログ              | アップデート ログには、McAfee アンチウイルス定義のアップデートなど、システム サービスのアップデートに関するイベントが記録されます。                                                                                                                                                                              |
| トラッキング ログ              | トラッキング ログには、トラッキング サービスのプロセスに関連付けられたアクションが記録されます。トラッキング ログは、メール ログのサブセットです。                                                                                                                                                                         |
| 認証ログ                   | 認証ログには、成功したユーザ ログインと失敗したログイン試行が記録されます。                                                                                                                                                                                                              |
| コンフィギュレーション履歴ログ        | コンフィギュレーション履歴ログは、どのような電子メールセキュリティ アプライアンスの変更がいつ行われたかの情報を記録します。ユーザが変更をコミットするたびに、新しい設定履歴ログが作成されます。                                                                                                                                                    |
| アップグレード ログ             | アップグレードのダウンロードとインストールに関するステータス情報。                                                                                                                                                                                                                   |



## ログ タイプの特徴

表 34-2 に、各ログ タイプの特徴をまとめます。

表 34-2 ログ タイプの比較

|                  | 記載内容     |       |           |                |           |             |           |      |            |            |                  |            |           |      |
|------------------|----------|-------|-----------|----------------|-----------|-------------|-----------|------|------------|------------|------------------|------------|-----------|------|
|                  | トランザクション | ステータス | テキストとして記録 | mbox ファイルとして記録 | バイナリとして記録 | 定期的なステータス情報 | メッセージ受信情報 | 配信情報 | 個々のハードバウンス | 個々のソフトバウンス | インジェクション SMTP 会話 | ヘッダー ログイング | SMTP 会話配信 | 設定情報 |
| IronPort メール ログ  | •        |       | •         |                |           | •           | •         | •    | •          | •          |                  | •          |           |      |
| qmail 形式配信 ログ    |          | •     |           | •              |           |             | •         | •    | •          |            |                  | •          |           |      |
| 配信ログ             |          | •     |           | •              |           |             | •         | •    | •          |            |                  | •          |           |      |
| バウンス ログ          | •        |       | •         |                |           |             |           |      | •          | •          |                  | •          |           |      |
| ステータス ログ         |          | •     | •         |                |           | •           |           |      |            |            |                  |            |           |      |
| ドメイン デバッグ ログ     | •        |       | •         |                |           |             |           | •    | •          | •          |                  |            | •         |      |
| インジェクション デバッグ ログ | •        |       | •         |                |           |             | •         |      |            |            | •                |            |           |      |
| システム ログ          | •        |       | •         |                |           | •           |           |      |            |            |                  |            |           |      |
| CLI 監査ログ         | •        |       | •         |                |           | •           |           |      |            |            |                  |            |           |      |
| FTP サーバ ログ       | •        |       | •         |                |           | •           |           |      |            |            |                  |            |           |      |
| HTTP ログ          | •        |       | •         |                |           | •           |           |      |            |            |                  |            |           |      |
| NTP ログ           | •        |       | •         |                |           | •           |           |      |            |            |                  |            |           |      |
| LDAP ログ          | •        |       | •         |                |           | •           |           |      |            |            |                  |            |           |      |
| アンチスパム ログ        | •        |       | •         |                |           | •           |           |      |            |            |                  |            |           |      |
| アンチスパム アーカイブ ログ  |          |       |           | •              |           |             |           |      |            |            |                  |            |           |      |
| アンチウイルス ログ       | •        |       | •         |                |           | •           |           |      |            |            |                  |            |           |      |
| アンチウイルス アーカイブ    |          |       |           | •              |           |             |           |      |            |            |                  |            |           |      |
| スキャン ログ          | •        |       | •         |                |           | •           |           |      |            |            |                  |            |           | •    |
| IronPort スパム隔離   | •        |       | •         |                |           | •           |           |      |            |            |                  |            |           |      |

表 34-2 ログタイプの比較 (続き)

|                    | トランザクション | スタートレス | テキストとして記録 | mbox ファイルとして記録 | バイナリとして記録 | 記載内容        |           |      |            |            |  | インジェクション SMTP 会話 | ヘッダー ログ | SMTP 会話配信 | 設定情報 |   |
|--------------------|----------|--------|-----------|----------------|-----------|-------------|-----------|------|------------|------------|--|------------------|---------|-----------|------|---|
|                    |          |        |           |                |           | 定期的なステータス情報 | メッセージ受信情報 | 配信情報 | 個々のハードバウンス | 個々のソフトバウンス |  |                  |         |           |      |   |
| IronPort スパム隔離 GUI | •        |        | •         |                |           | •           |           |      |            |            |  |                  |         |           |      |   |
| セーフリスト/ブロックリストログ   | •        |        | •         |                |           | •           |           |      |            |            |  |                  |         |           |      |   |
| レポーティングログ          | •        |        | •         | •              |           |             |           |      |            |            |  |                  |         |           |      |   |
| レポーティングクエリーログ      | •        |        | •         | •              |           |             |           |      |            |            |  |                  |         |           |      |   |
| アップデートログ           |          |        | •         |                |           |             |           |      |            |            |  |                  |         |           |      |   |
| トラッキングログ           | •        |        |           | •              | •         | •           | •         | •    | •          | •          |  | •                |         |           |      |   |
| 認証ログ               | •        |        | •         |                |           |             |           |      |            |            |  |                  |         |           |      |   |
| コンフィギュレーション履歴ログ    | •        |        | •         |                |           |             |           |      |            |            |  |                  |         |           |      | • |

## ログ取得方法

ログ ファイルは、次のいずれかのファイル転送プロトコルに基づいて取得できます。プロトコルは、グラフィカル ユーザ インターフェイスでサブスクリプションを作成または編集するときに設定するか、ログサブスクリプションのプロセス中に `logconfig` コマンドを使用して設定します。

表 34-3 ログ転送プロトコル

|                    |                                                                                                                                                                                                                                                                                                                                              |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>手動でダウンロード</b>   | <p>この方法では、[ ログ サブスクリプション (Log Subscriptions) ] ページにあるログ ディレクトリへのリンクをクリックし、アクセスするログ ファイルをクリックすることによって、いつでもログ ファイルにアクセスできます。ブラウザによっては、ブラウザ ウィンドウでのファイルの表示、またはそれをテキスト ファイルとして開いたり保存することができます。この方法は HTTP (S) プロトコルを使用し、デフォルトの取得方法になっています。</p> <p>(注) この方法を使用すると、この方法を CLI で指定した場合でも、レベル (マシン、グループ、またはクラスタ) には関係なく、クラスタ内のどのコンピュータのログも取得できません。</p> |
| <b>FTP プッシュ</b>    | <p>この方法では、リモート コンピュータ上の FTP サーバに定期的にログ ファイルをプッシュします。サブスクリプションには、リモート コンピュータ上のユーザ名、パスワード、および宛先ディレクトリが必要です。ログ ファイルは、設定したロールオーバー スケジュールに基づいて転送されます。</p>                                                                                                                                                                                         |
| <b>SCP プッシュ</b>    | <p>この方法では、リモート コンピュータ上の SCP サーバに定期的にログ ファイルをプッシュします。この方法には、SSH1 または SSH2 プロトコルを使用するリモート コンピュータ上の SSH SCP サーバが必要です。サブスクリプションには、リモート コンピュータ上のユーザ名、SSH キー、および宛先ディレクトリが必要です。ログ ファイルは、設定したロールオーバー スケジュールに基づいて転送されます。</p>                                                                                                                          |
| <b>Syslog プッシュ</b> | <p>この方法では、リモート syslog サーバにログ メッセージを送信します。この方法は、RFC 3164 に準拠しています。syslog サーバのホスト名を送信し、ログの転送に UDP または TCP を使用するよう選択する必要があります。使用するポートは 514 です。ログのファシリティは選択できますが、ログ タイプのデフォルトはドロップダウンメニューであらかじめ選択されています。syslog プッシュを使用して転送できるのは、テキストベースのログだけです。</p>                                                                                              |

## ログ ファイル名とディレクトリ構造

Cisco AsyncOS は、ログ サブスクリプション名に基づいて各ログ サブスクリプションのディレクトリを作成します。ディレクトリ内の実際のログ ファイル名は、ユーザが指定したログ ファイル名、ログ ファイルが開始されたときのタイムスタンプ、および単一文字のステータス コードで構成されます。ログのファイル名は、次の形式で作成されます。

```
/LogSubscriptionName/LogFilename.@timestamp.statuscode
```

ステータス コードは、`.current` または `.s` (保存済みを示す) になります。`saved` (保存済み) ステータスのログ ファイルだけを転送または削除するようにしてください。

## ログのロールオーバーおよび転送スケジュール

ログ ファイルはログ サブスクリプションによって作成され、到達したユーザ指定の最初の条件 (最大ファイル サイズまたはスケジュール設定されたロールオーバー) に基づいて、ロールオーバー (および、プッシュ ベースの取得オプションが選択されている場合は転送) されます。最大ファイル サイズとスケジュール設定されたロールオーバーの時間間隔の両方を設定するには、CLI で、または GUI の [ ログ サブスクリプション (Log Subscriptions) ] ページで `logconfig` コマンドを使用します。また、

GUI の [今すぐロールオーバー (Rollover Now)] ボタン、または CLI の `rollovernow` コマンドを使用して、選択したログ サブスクリプションをロールオーバーすることもできます。ロールオーバーのスケジュール設定の詳細については、「[ログ サブスクリプションのロールオーバー](#)」(P.34-44) を参照してください。

手動のダウンロードを使用して取得されたログは、指定した最大数（デフォルトは 10 ファイル）に達するか、またはシステムでログ ファイル用にさらにスペースが必要になるまで保存されます。

## デフォルトでイネーブルになるログ

Cisco アプライアンスは、次のログ サブスクリプションがデフォルトでイネーブルになった状態で事前に設定されています（適用したライセンス キーによって、その他のログが設定される場合があります）。デフォルトでは、取得方法は「手動でのダウンロード」です。

表 34-4 事前に設定されるログ サブスクリプション

| ログ番号 | ログ サブスクリプション名        | ログ タイプ                 |
|------|----------------------|------------------------|
| 1    | antispam             | アンチスパム ログ              |
| 2    | antivirus            | アンチウイルス ログ             |
| 3    | asarchive            | アンチスパム アーカイブ           |
| 4    | authentication       | 認証ログ                   |
| 5    | avarchive            | アンチウイルス アーカイブ          |
| 6    | bounces              | バウンス ログ                |
| 7    | cli_logs             | CLI 監査ログ               |
| 8    | encryption           | 暗号化                    |
| 9    | error_logs           | IronPort テキスト メール ログ   |
| 10   | euq_logs             | IronPort スпам隔離ログ      |
| 11   | euqgui_logs          | IronPort スпам隔離 GUI ログ |
| 12   | ftpd_logs            | FTP サーバ ログ             |
| 13   | gui_logs             | HTTP ログ                |
| 14   | mail_logs            | IronPort テキスト メール ログ   |
| 15   | reportd_logs         | レポーティング ログ             |
| 16   | reportingqueryd_logs | レポーティング クエリー ログ        |
| 17   | scanning             | スキャン ログ                |
| 18   | slbld_logs           | セーフリスト/ブロックリスト ログ      |
| 19   | sntpd_logs           | NTP ログ                 |
| 20   | ステータスが               | ステータス ログ               |
| 21   | system_logs          | システム ログ                |
| 22   | trackerd_logs        | トラッキング ログ              |
| 23   | updater_logs         | アップデート ログ              |

エラーだけが含まれるように 1 に設定された `error_logs` を除き、事前に設定されるすべてのログ サブスクリプションのログ レベルは 3 になります。詳細については、「[ログ レベル](#)」(P.34-40) を参照してください。新規のログ サブスクリプションの作成、または既存のログ サブスクリプションの変更については、「[ログ サブスクリプション](#)」(P.34-39) を参照してください。

## ログタイプ

- 「IronPort テキスト メール ログの使用」 (P.34-10)
- 「IronPort 配信ログの使用」 (P.34-16)
- 「IronPort バウンス ログの使用」 (P.34-18)
- 「IronPort ステータス ログの使用」 (P.34-20)
- 「IronPort ドメイン デバッグ ログの使用」 (P.34-23)
- 「IronPort インジェクション デバッグ ログの使用」 (P.34-24)
- 「IronPort システム ログの使用」 (P.34-25)
- 「IronPort CLI 監査ログの使用」 (P.34-26)
- 「IronPort FTP サーバ ログの使用」 (P.34-27)
- 「IronPort HTTP ログの使用」 (P.34-28)
- 「IronPort NTP ログの使用」 (P.34-29)
- 「スキャン ログの使用」 (P.34-29)
- 「IronPort アンチスパムの使用」 (P.34-30)
- 「IronPort アンチウイルス ログの使用」 (P.34-30)
- 「IronPort スпам隔離ログの使用」 (P.34-31)
- 「IronPort スпам隔離 GUI ログの使用」 (P.34-31)
- 「IronPort LDAP デバッグ ログの使用」 (P.34-32)
- 「セーフリスト/ブロックリスト ログの使用」 (P.34-33)
- 「レポーティング ログの使用」 (P.34-34)
- 「レポーティング クエリー ログの使用」 (P.34-35)
- 「アップデート ログの使用」 (P.34-36)
- 「トラッキング ログについて」 (P.34-37)
- 「認証ログの使用」 (P.34-38)

## ログ ファイル内のタイムスタンプ

次のログ ファイルには、ログ自体の開始日と終了日、AsyncOS のバージョン、および GMT オフセット (秒単位でログの始まりにのみ表示) が含まれます。

- アンチウイルス ログ
- LDAP ログ
- システム ログ
- メール ログ

## IronPort テキスト メール ログの使用

これらのログには、電子メールの受信、電子メールの配信、およびバウンスの詳細が記録されます。ステータス情報も、1 分ごとにメール ログに書き込まれます。これらのログは、特定のメッセージの配信を理解し、システム パフォーマンスを分析するうえで有益な情報源となります。

これらのログに、特別な設定は必要ありません。ただし、添付ファイル名を表示するには、適切なシステムの設定が必要です。添付ファイル名は、常に記録されるわけではありません。詳細については、「[メッセージ トラッキングのイネーブル化](#)」(P.25-1) および「[メッセージ トラッキングの概要](#)」(P.25-1) を参照してください。

表 34-5 に、テキスト メール ログに表示される情報を示します。

表 34-5 テキスト メール ログの統計情報

| 統計    | 説明                                                                                                                                 |
|-------|------------------------------------------------------------------------------------------------------------------------------------|
| ICID  | Injection Connection ID (インジェクション接続 ID)。システムに対する個々の SMTP 接続を表す数値 ID であり、この接続で 1 個から数千個のメッセージが送信されます。                               |
| DCID  | Delivery Connection ID (配信接続 ID)。別のサーバに対する個々の SMTP 接続を表す数値 ID であり、この接続で 1 個から数千個のメッセージが配信されます。1 つのメッセージ送信で一部または全部の RID が一緒に配信されます。 |
| RCID  | RPC Connection ID (RPC 接続 ID)。Cisco スпам隔離に対する個々の RPC 接続を表す数値 ID です。この ID を使用して、Cisco スпам隔離との間で送受信されるメッセージを追跡します。                 |
| MID   | メッセージ ID。この ID を使用して、メッセージのフローをログで追跡します。                                                                                           |
| RID   | Recipient ID (受信者 ID) : 各メッセージ受信者に ID が割り当てられます。                                                                                   |
| New   | 新規の接続が開始されました。                                                                                                                     |
| Start | 新規のメッセージが開始されました。                                                                                                                  |

## IronPort テキスト メール ログの解釈

ログ ファイルを解釈するためのガイドとして、次のサンプルを使用してください。



(注)

ログ ファイルの各行には、番号が割り当てられません。ここでは、単にサンプル用として番号が割り当てられています。

表 34-6 テキスト メール ログの詳細

|   |                                                                                                                                                |
|---|------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Mon Apr 17 19:56:22 2003 Info: New SMTP ICID 5 interface Management (10.1.1.1) address 10.1.1.209 reverse dns host remotehost.com verified yes |
| 2 | Mon Apr 17 19:57:20 2003 Info: Start MID 6 ICID 5                                                                                              |
| 3 | Mon Apr 17 19:57:20 2003 Info: MID 6 ICID 5 From: <sender@remotehost.com>                                                                      |
| 4 | Mon Apr 17 19:58:06 2003 Info: MID 6 ICID 5 RID 0 To: <mary@yourdomain.com>                                                                    |
| 5 | Mon Apr 17 19:59:52 2003 Info: MID 6 ready 100 bytes from <sender@remotehost.com>                                                              |
| 6 | Mon Apr 17 19:59:59 2003 Info: ICID 5 close                                                                                                    |
| 7 | Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 8 interface 192.168.42.42 address 10.5.3.25                                                       |
| 8 | Mon Mar 31 20:10:58 2003 Info: Delivery start DCID 8 MID 6 to RID [0]                                                                          |

表 34-6 テキスト メール ログの詳細 (続き)

|    |                                                                     |
|----|---------------------------------------------------------------------|
| 9  | Mon Mar 31 20:10:58 2003 Info: Message done DCID 8 MID 6 to RID [0] |
| 10 | Mon Mar 31 20:11:03 2003 Info: DCID 8 close                         |

前述のログ ファイルを読み取るためのガイドとして、表 34-7 を使用してください。

表 34-7 テキスト メール ログの例の詳細

| 行番号 | 説明                                                                                                         |
|-----|------------------------------------------------------------------------------------------------------------|
| 1.  | システムに対して新しい接続が開始され、インジェクション ID (ICID) 「5」が割り当てられました。この接続は管理 IP インターフェイスで受信され、10.1.1.209 のリモート ホストで開始されました。 |
| 2.  | クライアントから MAIL FROM コマンドが実行された後、メッセージにメッセージ ID (MID) 「6」が割り当てられました。                                         |
| 3.  | 送信者アドレスが識別され、受け入れられます。                                                                                     |
| 4.  | 受信者が識別され、受信者 ID (RID) 「0」が割り当てられました。                                                                       |
| 5.  | MID 5 が受け入れられ、ディスクに書き込まれ、確認応答されました。                                                                        |
| 6.  | 受信が成功し、受信接続が終了しました。                                                                                        |
| 7.  | 次に、メッセージ配信プロセスが開始されます。192.168.42.42 から 10.5.3.25 への配信に、配信接続 ID (DCID) 「8」が割り当てられました。                       |
| 8.  | RID 「0」へのメッセージ配信が開始されました。                                                                                  |
| 9.  | RID 「0」への MID 6 の配信に成功しました。                                                                                |
| 10. | 配信接続が終了しました。                                                                                               |

## テキスト メール ログ エントリの例

次に、さまざまな状況に基づいたいくつかのサンプル ログ エントリを示します。

### メッセージのインジェクションおよび配信

1 人の受信者に対するメッセージが Cisco アプライアンスにインジェクトされます。メッセージは正常に配信されます。

```
Wed Jun 16 21:42:34 2004 Info: New SMTP ICID 282204970 interface mail.example.com
(1.2.3.4) address 2.3.4.5 reverse dns host unknown verified no
```

```
Wed Jun 16 21:42:34 2004 Info: ICID 282204970 SBRS None
```

```
Wed Jun 16 21:42:35 2004 Info: Start MID 200257070 ICID 282204970
```

```
Wed Jun 16 21:42:35 2004 Info: MID 200257070 ICID 282204970 From: <someone@foo.com>
```

```
Wed Jun 16 21:42:36 2004 Info: MID 200257070 ICID 282204970 RID 0 To: <user@example.com>
```

```
Wed Jun 16 21:42:38 2004 Info: MID 200257070 Message-ID
'<37gva9$5uvbhe@mail.example.com>'
```

```
Wed Jun 16 21:42:38 2004 Info: MID 200257070 Subject 'Hello'
```

```
Wed Jun 16 21:42:38 2004 Info: MID 200257070 ready 24663 bytes from <someone@foo.com>
```

```

Wed Jun 16 21:42:38 2004 Info: MID 200257070 antivirus negative

Wed Jun 16 21:42:38 2004 Info: MID 200257070 queued for delivery

Wed Jun 16 21:42:38 2004 Info: New SMTP DCID 2386069 interface 1.2.3.4 address 1.2.3.4

Wed Jun 16 21:42:38 2004 Info: Delivery start DCID 2386069 MID 200257070 to RID [0]

Wed Jun 16 21:42:38 2004 Info: ICID 282204970 close

Wed Jun 16 21:42:38 2004 Info: Message done DCID 2386069 MID 200257070 to RID [0]
[('X-SBRS', 'None')]

Wed Jun 16 21:42:38 2004 Info: MID 200257070 RID [0] Response 2.6.0
<37gva9$5uvbhe@mail.example.com> Queued mail for delivery

Wed Jun 16 21:42:43 2004 Info: DCID 2386069 close

```

### 正常なメッセージ配信

```

Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 5 interface 172.19.0.11 address
63.251.108.110

Mon Mar 31 20:10:58 2003 Info: Delivery start DCID 5 MID 4 to RID [0]

Mon Mar 31 20:10:58 2003 Info: Message done DCID 5 MID 4 to RID [0]

Mon Mar 31 20:11:03 2003 Info: DCID 5 close

```

### 失敗したメッセージ配信 (ハード バウンス)

2 人の受信者が指定されたメッセージが Cisco アプライアンスにインジェクトされます。配信時に、宛先ホストが 5XX エラーを返しました。これは、メッセージをどちらの受信者にも配信できなかったことを示します。Cisco アプライアンスは送信者に通知し、キューから受信者を削除します。

```

Mon Mar 31 20:00:23 2003 Info: New SMTP DCID 3 interface 172.19.0.11 address
64.81.204.225

Mon Mar 31 20:00:23 2003 Info: Delivery start DCID 3 MID 4 to RID [0, 1]

Mon Mar 31 20:00:27 2003 Info: Bounced: DCID 3 MID 4 to RID 0 - 5.1.0 - Unknown address
error ('550', ['<george@yourdomain.com>... Relaying denied']) []

Mon Mar 31 20:00:27 2003 Info: Bounced: DCID 3 MID 4 to RID 1 - 5.1.0 - Unknown address
error ('550', ['<jane@yourdomain.com>... Relaying denied']) []

Mon Mar 31 20:00:32 2003 Info: DCID 3 close

```



### ソフトバウンスの後の正常な配信

メッセージが Cisco アプライアンスにインジェクトされます。最初の配信試行で、メッセージはソフトバウンスして、その後の配信キューに入れられます。2 回目の試行でメッセージは正常に配信されません。

```
Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 5 interface 172.19.0.11 address 63.251.108.110
```

```
Mon Mar 31 20:00:23 2003 Info: Delivery start DCID 3 MID 4 to RID [0, 1]
```

```
Mon Mar 31 20:00:23 2003 Info: Delayed: DCID 5 MID 4 to RID 0 - 4.1.0 - Unknown address error ('466', ['Mailbox temporarily full.'])[]
```

```
Mon Mar 31 20:00:23 2003 Info: Message 4 to RID [0] pending till Mon Mar 31 20:01:23 2003
```

```
Mon Mar 31 20:01:28 2003 Info: DCID 5 close
```

```
Mon Mar 31 20:01:28 2003 Info: New SMTP DCID 16 interface PublicNet address 172.17.0.113
```

```
Mon Mar 31 20:01:28 2003 Info: Delivery start DCID 16 MID 4 to RID [0]
```

```
Mon Mar 31 20:01:28 2003 Info: Message done DCID 16 MID 4 to RID [0]
```

```
Mon Mar 31 20:01:33 2003 Info: DCID 16 close
```

### scanconfig コマンドのメッセージ スキャン結果

scanconfig コマンドを使用して、メッセージの構成要素を分解できない場合（添付ファイルを削除する場合）のシステムの動作を決定できます。オプションは、Deliver、Bounce、または Drop です。

次に、scanconfig を Deliver に設定した IronPort テキスト メール ログの例を示します。

```
Tue Aug 3 16:36:29 2004 Info: MID 256 ICID 44784 From: <test@virus.org>
```

```
Tue Aug 3 16:36:29 2004 Info: MID 256 ICID 44784 RID 0 To: <joe@example.com>
```

```
Tue Aug 3 16:36:29 2004 Info: MID 256 Message-ID '<137398.@virus.org>'
```

```
Tue Aug 3 16:36:29 2004 Info: MID 256 Subject 'Virus Scanner Test #22'
```

```
Tue Aug 3 16:36:29 2004 Info: MID 256 ready 1627 bytes from <test@virus.org>
```

```
Tue Aug 3 16:36:29 2004 Warning: MID 256, Message Scanning Problem: Continuation line seen before first header
```

```
Tue Aug 3 16:36:29 2004 Info: ICID 44784 close
```

```
Tue Aug 3 16:36:29 2004 Info: MID 256 antivirus positive 'EICAR-AV-Test'
```

```
Tue Aug 3 16:36:29 2004 Info: Message aborted MID 256 Dropped by antivirus
```

```
Tue Aug 3 16:36:29 2004 Info: Message finished MID 256 done
```

次に、scanconfig を drop に設定した IronPort テキスト メール ログの例を示します。

```
Tue Aug 3 16:38:53 2004 Info: Start MID 257 ICID 44785
Tue Aug 3 16:38:53 2004 Info: MID 257 ICID 44785 From: test@virus.org
Tue Aug 3 16:38:53 2004 Info: MID 257 ICID 44785 RID 0 To: <joe@example.com>
Tue Aug 3 16:38:53 2004 Info: MID 257 Message-ID '<392912.@virus.org>'
Tue Aug 3 16:38:53 2004 Info: MID 25781 Subject 'Virus Scanner Test #22'
Tue Aug 3 16:38:53 2004 Info: MID 257 ready 1627 bytes from <test@virus.org>
Tue Aug 3 16:38:53 2004 Warning: MID 257, Message Scanning Problem: Continuation line
seen before first header
Tue Aug 3 16:38:53 2004 Info: Message aborted MID 25781 Dropped by filter 'drop_zip_c'
Tue Aug 3 16:38:53 2004 Info: Message finished MID 257 done
Tue Aug 3 16:38:53 2004 Info: ICID 44785 close
```

### 添付ファイルのあるメッセージ

この例では、添付ファイル名の識別をイネーブルにするように、条件「Message Body Contains」を含むコンテンツ フィルタが設定されています。

```
Sat Apr 23 05:05:42 2011 Info: New SMTP ICID 28 interface Management (192.0.2.10)
address 224.0.0.10 reverse dns host test.com verified yes
Sat Apr 23 05:05:42 2011 Info: ICID 28 ACCEPT SG UNKNOWNLIST match sbrs[-1.0:10.0]
SBRs 0.0
Sat Apr 23 05:05:42 2011 Info: Start MID 44 ICID 28
Sat Apr 23 05:05:42 2011 Info: MID 44 ICID 28 From: <sender1@example.com>
Sat Apr 23 05:05:42 2011 Info: MID 44 ICID 28 RID 0 To: <recipient1@example.org>
Sat Apr 23 05:05:42 2011 Info: MID 44 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>'
Sat Apr 23 05:05:42 2011 Info: MID 44 Subject 'Message 001'
Sat Apr 23 05:05:42 2011 Info: MID 44 ready 240129 bytes from <sender1@example.com>
Sat Apr 23 05:05:42 2011 Info: MID 44 matched all recipients for per-recipient
policy DEFAULT in the inbound table
Sat Apr 23 05:05:42 2011 Info: ICID 28 close
Sat Apr 23 05:05:42 2011 Info: MID 44 interim verdict using engine: CASE
spam negative
Sat Apr 23 05:05:42 2011 Info: MID 44 using engine: CASE spam negative
```

```
Sat Apr 23 05:05:43 2011 Info: MID 44 attachment 'Banner.gif'
Sat Apr 23 05:05:43 2011 Info: MID 44 attachment '=D1=82=D0=B5=D1=81=D1=82.rst'
Sat Apr 23 05:05:43 2011 Info: MID 44 attachment 'Test=20Attachment.docx'
Sat Apr 23 05:05:43 2011 Info: MID 44 queued for delivery
```

3つの添付ファイルの2番目が Unicode であることに注意してください。Unicode を表示できない端末では、このような添付ファイルは quoted-printable 形式で表示されます。

## 生成またはリライトされたメッセージに対するログ エントリ

リライト/リダイレクト アクションなど一部の機能 (alt-rcpt-to フィルタ、アンチスパム RCPT リライト、bcc() アクション、アンチウイルス リダイレクションなど) によって、新しいメッセージが作成されます。ログに目を通して結果を確認し、必要に応じて MID や、場合によっては DCID を追加します。次のようなエントリが可能です。

```
Tue Jun 1 20:02:16 2004 Info: MID 14 generated based on MID 13 by bcc filter 'nonetest'
```

または

```
Tue Jan 6 15:03:18 2004 Info: MID 2 rewritten to 3 by antispaam
Fri May 14 20:44:43 2004 Info: MID 6 rewritten to 7 by alt-rcpt-to-filter filter
'testfilt'
```

「rewritten」エントリについては、ログ内で新しい MID の使用を示す行の後に表示される点に注目してください。

## Cisco スпам隔離エリアに送信されたメッセージ

メッセージを隔離エリアに送信すると、メール ログでは、RPC 接続を識別する RPC Connection ID (RCID; RPC 接続 ID) を使用して、隔離エリアとの間の移動が追跡されます。次のメール ログでは、スパムとしてタグが付けられたメッセージが Cisco スпам隔離に送信されています。

```
Wed Feb 14 12:11:40 2007 Info: Start MID 2317877 ICID 15726925
Wed Feb 14 12:11:40 2007 Info: MID 2317877 ICID 15726925 From: <HLD@chasehf.bfi0.com>
Wed Feb 14 12:11:40 2007 Info: MID 2317877 ICID 15726925 RID 0 To:
<stevel@healthtrust.org>
Wed Feb 14 12:11:40 2007 Info: MID 2317877 Message-ID
'<W1TH05606E5811BEA0734309D4BAF0.323.14460.pimailer44.DumpShot.2@email.chase.com>'
Wed Feb 14 12:11:40 2007 Info: MID 2317877 Subject 'Envision your dream home - Now make
it a reality'
Wed Feb 14 12:11:40 2007 Info: MID 2317877 ready 15731 bytes from <HLD@chasehf.bfi0.com>
```

```

Wed Feb 14 12:11:40 2007 Info: MID 2317877 matched all recipients for per-recipient
policy DEFAULT in the inbound table

Wed Feb 14 12:11:41 2007 Info: MID 2317877 using engine: CASE spam suspect

Wed Feb 14 12:11:41 2007 Info: EUQ: Tagging MID 2317877 for quarantine

Wed Feb 14 12:11:41 2007 Info: MID 2317877 antivirus negative

Wed Feb 14 12:11:41 2007 Info: MID 2317877 queued for delivery

Wed Feb 14 12:11:44 2007 Info: RPC Delivery start RCID 756814 MID 2317877 to local
IronPort Spam Quarantine

Wed Feb 14 12:11:45 2007 Info: EUQ: Quarantined MID 2317877

Wed Feb 14 12:11:45 2007 Info: RPC Message done RCID 756814 MID 2317877

Wed Feb 14 12:11:45 2007 Info: Message finished MID 2317877 done

```

## IronPort 配信ログの使用

配信ログには、AsyncOS の電子メール配信動作に関する重要な情報が記録されます。ログメッセージは「ステートレス」です。つまり、関連するすべての情報が各ログメッセージに記録されるので、ユーザは、現在の配信試行に関する情報について前のログメッセージを参照する必要がありません。

配信ログには、受信者ごとの電子メール配信動作に関連するすべての情報が記録されます。すべての情報は、論理的にレイアウトされ、シスコが提供するユーティリティを使用して変換した後は、人による読み取りが可能になります。変換ツールは、次の場所にあります。

<http://support.ironport.com>

配信ログは、リソースの効率性を保つためにバイナリ形式で記録されて転送されます。次の表に、配信ログに記録される情報を示します。

**表 34-8 配信ログの統計情報**

| 統計                     | 説明                                                               |
|------------------------|------------------------------------------------------------------|
| <b>Delivery status</b> | success (メッセージは正常に配信されました) または bounce (メッセージはハードバウンスされました)       |
| <b>Del_time</b>        | 配信時間                                                             |
| <b>Inj_time</b>        | インジェクション時間。del_time - inj_time = 受信者メッセージがキューに留まっていた時間。          |
| <b>Bytes</b>           | メッセージ サイズ                                                        |
| <b>Mid</b>             | メッセージ ID                                                         |
| <b>Ip</b>              | 受信者ホスト IP 受信者メッセージを受信またはバウンスしたホストの IP アドレス                       |
| <b>From</b>            | Envelope From (Envelope Sender または MAIL FROM としても知られます)          |
| <b>Source_ip</b>       | 送信元ホスト IP。着信メッセージのホストの IP アドレス。                                  |
| <b>Code</b>            | 受信者ホストからの SMTP 応答コード                                             |
| <b>Reply</b>           | 受信者ホストからの SMTP 応答メッセージ                                           |
| <b>Rcpt Rid</b>        | 受信者 ID。受信者 ID は <0> から始まります。複数の受信者が指定されたメッセージには、複数の受信者 ID が付きます。 |

表 34-8 配信ログの統計情報（続き）

| 統計       | 説明        |
|----------|-----------|
| To       | エンベロープ受信者 |
| Attempts | 配信試行回数    |

配信ステータスが bounce であった場合は、次の追加情報が配信ログに表示されます。

表 34-9 配信ログのバウンス情報

| 統計     | 説明                                                      |
|--------|---------------------------------------------------------|
| Reason | 配信時の SMTP 応答に対する RFC 1893 Enhanced Mail Status Code の解釈 |
| Code   | 受信者ホストからの SMTP 応答コード                                    |
| Error  | 受信者ホストからの SMTP 応答メッセージ                                  |

ログヘッダーを設定している場合（「メッセージヘッダーのログイン」(P.34-43) を参照）、ヘッダー情報は配信情報の後に表示されます。

表 34-10 配信ログのヘッダー情報

| 統計            | 説明                         |
|---------------|----------------------------|
| Customer_data | ログに記録されるヘッダーの始まりを示す XML タグ |
| Header Name   | ヘッダーの名前                    |
| Value         | ログに記録されるヘッダーの内容            |

## 配信ログ エントリの例

ここでは、さまざまな配信ログ エントリの例を示します。

## 正常なメッセージ配信

```
<success del_time="Fri Jan 09 15:34:20.234 2004" inj_time="Fri Jan 09 15:33:38.623 2004"
bytes="202" mid="45949" ip="10.1.1.1" from="campaign1@yourdomain.com"
source_ip="192.168.102.1" code="250" reply="sent">

<rcpt rid="0" to="alsdfj.ajsdf1@alsdfj.d2.qa25.qa" attempts="1" />

</success>
```

## 配信ステータス バウンス

```
<bounce del_time="Sun Jan 05 08:28:33.073 2003" inj_time="Mon Jan 05 08:28:32.929 2003"
bytes="4074" mid="94157762" ip="0.0.0.0" from="campaign1@yourdomain.com"
source_ip="192.168.102.1" reason="5.1.0 - Unknown address error" code="550"
error=["Requested action not taken: mailbox unavailable"]">

<rcpt rid="0" to="user@sampledomain.com" attempts="1" />

</bounce>
```

## ログヘッダー付きの配信ログ エントリ

```
<success del_time="Tue Jan 28 15:56:13.123 2003" inj_time="Tue Jan 28 15:55:17.696 2003"
bytes="139" mid="202" ip="10.1.1.13" from="campaign1@yourdomain.com"
source_ip="192.168.102.1" code="250" reply="sent">

<rcpt rid="0" to="user@sampledomain.com" attempts="1" />

<customer_data>

<header name="xname" value="sh"/>

</customer_data>

</success>
```

## IronPort バウンス ログの使用

バウンス ログには、バウンスされた各受信者に関するすべての情報が記録されます。表 34-11 に、バウンス ログに記録される情報を示します。

表 34-11 バウンス ログの統計情報

統計	説明
Timestamp	バウンス イベントの時刻
Log level	このバウンス ログの詳細レベル
Bounce type	Bounced または Delayed (ハードバウンスまたはソフトバウンスなど)
MID/RID	メッセージ ID および受信者 ID
From	エンベロープ送信者

表 34-11 バウンス ログの統計情報 (続き)

統計	説明
To	エンベロープ受信者
Reason	配信時の SMTP 応答に対する RFC 1893 Enhanced Mail Status Code の解釈
Response	受信者ホストからの SMTP 応答コードおよびメッセージ

また、ログに記録するメッセージサイズを指定しているか、ログヘッダーを設定している（「[メッセージヘッダーのログイン](#)」(P.34-43) を参照）場合、メッセージおよびヘッダー情報はバウンス情報の後に表示されます。

表 34-12 バウンス ログのヘッダー情報

ヘッダー	ヘッダー名およびヘッダーのコンテンツ。
Message	ログに記録されるメッセージのコンテンツ。

## バウンス ログ エントリの例

### ソフトバウンスされた受信者 (バウンス タイプ = Delayed)

```
Thu Dec 26 18:37:00 2003 Info: Delayed: 44451135:0
From:<campaign1@yourdomain.com> To:<user@sampledomain.com>
```

```
Reason: "4.1.0 - Unknown address error" Response: "('451',
['<user@sampledomain.com> Automated block triggered by suspicious
activity from your IP address (10.1.1.1). Have your system administrator
send e-mail to postmaster@sampledomain.com if you believe this block is
in error'])"
```

### ハードバウンスされた受信者 (バウンス タイプ = Bounced)

```
Thu Dec 26 18:36:59 2003 Info: Bounced: 45346670:0 From:<campaign1@yourdomain.com>
To:<user2@sampledomain.com>
```

```
Reason: "5.1.0 - Unknown address error" Response: "('550', ['There is no such active
account.'])"
```

### メッセージ本文およびログヘッダー付きのバウンス ログ

```
Wed Jan 29 00:06:30 2003 Info: Bounced: 203:0 From:<campaign1@yourdomain.com>
To:<user@sampledomain.com>
```

```
Reason:"5.1.2 - Bad destination host" Response: "('000', [])" Headers: ['xname:
userID2333']' Message: Message-Id:
```

```
<1u5jak$6b@yourdomain.com>\015\012xname: userID2333\015\012subject:
Greetings.\015\012\015\012Hi Tom:'
```



(注) テキスト文字列 \015\012 は、改行を表します (CRLF など)。

## IronPort ステータス ログの使用

ステータス ログには、`status`、`status detail`、および `dnsstatus` を含む CLI ステータス コマンドで検出されたシステム統計情報が記録されます。記録期間は、`logconfig` の `setup` サブコマンドを使用して設定します。ステータス ログでレポートされるカウンタまたはレートは、前回カウンタがリセットされた時点からの値です。



## ステータス ログの読み取り

表 34-13 に、ステータス ログ ラベルと、一致するシステム統計情報を示します。

表 34-13 ステータス ログの統計情報

統計	説明
CPULd	CPU 使用率
DskIO	ディスク I/O 使用率
RAMUtil	RAM 使用率
QKUsd	使用されているキュー (キロバイト単位)
QKFre	空いているキュー (キロバイト単位)
CrtMID	メッセージ ID (MID)
CrtICID	インジェクション接続 ID (ICID)
CRTDCID	配信接続 ID (DCID)
InjMsg	インジェクトされたメッセージ
InjRcp	インジェクトされた受信者
GenBncRcp	生成されたバウンス受信者
RejRcp	拒否された受信者
DrpMsg	ドロップされたメッセージ
SftBncEvt	ソフトバウンスされたイベント
CmpRcp	完了した受信者
HrdBncRcp	ハードバウンスされた受信者
DnsHrdBnc	DNS ハードバウンス
5XXHrdBnc	5XX ハードバウンス
FltrHrdBnc	フィルタ ハードバウンス
ExpHrdBnc	期限切れハードバウンス
OtrHrdBnc	その他のハードバウンス
DlvRcp	配信された受信者
DelRcp	削除された受信者
GlbUnsbHt	グローバル配信停止リストとの一致数
ActvRcp	アクティブ受信者
UnatmptRcp	未試行受信者
AtmptRcp	試行受信者
CrtCncIn	現在の着信接続
CrtCncOut	現在の発信接続
DnsReq	DNS 要求
NetReq	ネットワーク要求
CchHit	キャッシュ ヒット
CchMis	キャッシュ ミス
CchEct	キャッシュ例外
CchExp	キャッシュ期限切れ

表 34-13 ステータス ログの統計情報 (続き)

統計	説明
<b>CPUTTm</b>	アプリケーションが使用した合計 CPU 時間
<b>CPUETm</b>	アプリケーションが開始されてからの経過時間
<b>MaxIO</b>	メール プロセスに対する 1 秒あたりの最大ディスク I/O 動作
<b>RamUsd</b>	割り当て済みのメモリ (バイト単位)
<b>SwIn</b>	スワップインされたメモリ
<b>SwOut</b>	スワップアウトされたメモリ
<b>SwPgIn</b>	ページインされたメモリ
<b>SwPgOut</b>	ページアウトされたメモリ
<b>MMLen</b>	システム内の合計メッセージ数
<b>DstInMem</b>	メモリ内の宛先オブジェクト数
<b>ResCon</b>	リソース保持の <b>tarpit</b> 値 (大量のシステム負荷により、着信メールの受け入れがこの秒数だけ遅延します)
<b>WorkQ</b>	ワーク キューにある現在のメッセージ数
<b>QuarMsgs</b>	ポリシー、ウイルス、およびアウトブレイク隔離にある個々のメッセージ数 (複数の隔離エリアに存在するメッセージは一度だけカウントされます)
<b>QuarQKUsd</b>	ポリシー、ウイルス、およびアウトブレイク隔離メッセージによって使用されるキロバイト
<b>LogUsd</b>	使用されるログパーティションの割合
<b>AVLd</b>	アンチウイルス スキャンで使用される CPU の割合
<b>CmrkLd</b>	Cloudmark アンチスパム スキャンで使用される CPU の割合
<b>SophLd</b>	Sophos アンチスパム スキャンで使用される CPU の割合
<b>McafLd</b>	McAfee アンチウイルス スキャンで使用される CPU の割合
<b>CASELd</b>	CASE スキャンで使用される CPU の割合
<b>TotalLd</b>	CPU の合計消費量
<b>LogAvail</b>	ログ ファイルに使用できるディスク スペース
<b>EuQ</b>	Cisco スпам隔離内の推定メッセージ数
<b>EuqRis</b>	Cisco スпам隔離解放キュー内の推定メッセージ数

## ステータス ログの例

```

Fri Feb 24 15:14:39 2006 Info: Status: CPULd 0 DskIO 0 RAMUtil 2 QKUsd 0 QKFre 8388608
CrtMID 19036 CrtICID 35284 CrtDCID 4861 InjMsg 13889 InjRcp 14230 GenBncRcp 12 RejRcp
6318 DrpMsg 7437 SftBncEvt 1816 CmpRcp 6813 HrdBncRcp 18 DnsHrdBnc 2 5XXHrdBnc 15
FltrHrdBnc 0 ExpHrdBnc 1 OtrHrdBnc 0 DlvRcp 6793 DelRcp 2 GlbUnsbHt 0 ActvRcp 0
UnatmptRcp 0 AtmptRcp 0 CrtCncIn 0 CrtCncOut 0 DnsReq 143736 NetReq 224227 CchHit 469058
CchMis 504791 CchEct 15395 CchExp 55085 CPUTTm 228 CPUETm 181380 MaxIO 350 RAMUsd
21528056 MMLen 0 DstInMem 4 ResCon 0 WorkQ 0 QuarMsgs 0 QuarQKUsd 0 LogUsd 3 AVLd 0 BMLd
0 CASELd 3 TotalLd 3 LogAvail 17G EuQ 0 EuqRls 0

```

## IronPort ドメイン デバッグ ログの使用

ドメイン デバッグ ログには、Cisco アプライアンスと指定の受信者ホスト間の SMTP 会話でのクライアントとサーバの通信が記録されます。このログタイプは主に、特定の受信者ホストに関する問題のデバッグに使用されます。

表 34-14 ドメイン デバッグ ログの統計情報

統計	説明
Timestamp	バウンス イベントの時刻
Log level	このバウンス ログの詳細レベル
From	エンベロープ送信者
To	エンベロープ受信者
Reason	配信時の SMTP 応答に対する RFC 1893 Enhanced Mail Status Code の解釈
Response	受信者ホストからの SMTP 応答コードおよびメッセージ

## ドメイン デバッグ ログの例

```

Sat Dec 21 02:37:22 2003 Info: 102503993 Sent: 'MAIL FROM:<daily@dailyf-y-i.net>'

Sat Dec 21 02:37:23 2003 Info: 102503993 Rcvd: '250 OK'

Sat Dec 21 02:37:23 2003 Info: 102503993 Sent: 'RCPT TO:<LLLSMILE@aol.com>'

Sat Dec 21 02:37:23 2003 Info: 102503993 Rcvd: '250 OK'

Sat Dec 21 02:37:23 2003 Info: 102503993 Sent: 'DATA'

Sat Dec 21 02:37:24 2003 Info: 102503993 Rcvd: '354 START MAIL INPUT, END WITH "." ON A
LINE BY ITSELF'

Sat Dec 21 02:37:24 2003 Info: 102503993 Rcvd: '250 OK'

```

## IronPort インジェクション デバッグ ログの使用

インジェクション デバッグ ログには、Cisco アプライアンスと、システムに接続している指定のホスト間の SMTP 会話が記録されます。インジェクション デバッグ ログは、インターネットから接続を開始するクライアントと Cisco アプライアンス間の通信に関する問題をトラブルシューティングするのに役立ちます。このログでは、2 つのシステム間で伝送されたすべてのバイトが記録され、接続ホストに「送信」または接続ホストから「受信」に分類されます。

記録するホストの会話を指定するには、IP アドレス、IP 範囲、ホスト名、または部分ホスト名を指定する必要があります。IP 範囲内で接続している IP アドレスがすべて記録されます。部分ドメイン内のホストがすべて記録されます。システムは、接続している IP アドレスに対してリバース DNS ルックアップを実行して、ホスト名に変換します。DNS に対応する PTR レコードがない IP アドレスは、ホスト名に一致しません。

記録するセッション数も指定する必要があります。

インジェクション デバッグ ログ内の各行には、表 34-15 に示す情報が含まれます。

**表 34-15** インジェクション デバッグ ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻。
ICID	インジェクション接続 ID は、別のログ サブスクリプションで同じ接続に関連付けることができる固有識別子です。
Sent/Received	「Sent to」と記された行は、接続ホストに送信された実際のバイトです。「Rcvd from」と記された行は、接続ホストから受信した実際のバイトです。
IP Address	接続ホストの IP アドレス。

## インジェクション デバッグ ログの例

```

Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '220 postman.example.com
ESMTP\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'HELO
mail.remotehost.com\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '250
postman.example.com\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'MAIL
FROM:<sender@remotehost.com>\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '250 sender
<sender@remotehost.com> ok\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'RCPT
TO:<recipient@example.com>\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '250 recipient
<recipient@example.com> ok\015\012'

Wed Apr 2 14:30:04 Info: 6216 Rcvd from '172.16.0.22': 'DATA\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '354 go ahead\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'To:
recipient@example.com\015\012Date: Apr 02 2003 10:09:44\015\012Subject: Test
Subject\015\012From: Sender <sender@remotehost.com>\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'This is the content of the
message'

Wed Apr 2 14:30:04 Info: 6216 Sent to '172.16.0.22': '250 ok\015\012'

Wed Apr 2 14:30:04 Info: 6216 Rcvd from '172.16.0.22': 'QUIT\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '221
postman.example.com\015\012'

```

## IronPort システム ログの使用

表 34-16 システム ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻。
Message	ログに記録されたイベント。

## システム ログの例

次のシステム ログの例は、**commit** を実行したユーザの名前と入力されたコメントを含む、いくつかの **commit** エントリを示しています。

```

Wed Sep 8 18:02:45 2004 Info: Version: 4.0.0-206 SN: XXXXXXXXXXXXX-XXX

Wed Sep 8 18:02:45 2004 Info: Time offset from UTC: 0 seconds

Wed Sep 8 18:02:45 2004 Info: System is coming up

Wed Sep 8 18:02:49 2004 Info: bootstrapping DNS cache

Wed Sep 8 18:02:49 2004 Info: DNS cache bootstrapped

Wed Sep 8 18:13:30 2004 Info: PID 608: User admin commit changes: SSW>Password

Wed Sep 8 18:17:23 2004 Info: PID 608: User admin commit changes: Completed Web::SSW

Thu Sep 9 08:49:27 2004 Info: Time offset from UTC: -25200 seconds

Thu Sep 9 08:49:27 2004 Info: PID 1237: User admin commit changes: Added a second CLI
log for examples

Thu Sep 9 08:51:53 2004 Info: PID 1237: User admin commit changes: Removed example CLI
log.

```

## IronPort CLI 監査ログの使用

表 34-17 CLI 監査ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻。
PID	コマンドが入力された特定の CLI セッションのプロセス ID。
Message	メッセージは、入力された CLI コマンド、CLI 出力（メニュー、リストなど）、および表示されるプロンプトで構成されます。

### CLI 監査ログの例

次の CLI 監査ログの例は、who および textconfig CLI コマンドが入力された PID 16434 の情報を示しています。

```

Thu Sep 9 14:35:55 2004 Info: PID 16434: User admin entered 'who'; prompt was
'\nmail3.example.com> '

Thu Sep 9 14:37:12 2004 Info: PID 16434: User admin entered 'textconfig'; prompt was
'\nUsername Login Time Idle Time Remote Host What\n=====
=====
=====
=====\nadmin Wed 11AM 3m 45s 10.1.3.14 tail\nadmin 02:32PM
0s 10.1.3.14 cli\nmail3.example.com> '

Thu Sep 9 14:37:18 2004 Info: PID 16434: User admin entered ''; prompt was '\nThere are
no text resources currently defined.\n\n\nChoose the operation you want to perform:\n-
NEW - Create a new text resource.\n- IMPORT - Import a text resource from a file.\n[> '

```

## IronPort FTP サーバ ログの使用

表 34-18 FTP サーバ ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻。
ID	接続 ID。FTP 接続ごとの別個の ID。
Message	ログ エントリのメッセージセクションは、ログファイル ステータス情報、または FTP 接続情報（ログイン、アップロード、ダウンロード、ログアウトなど）になります。

### FTP サーバ ログの例

次の FTP サーバ ログの例には、接続 (ID:1) が記録されています。着信接続の IP アドレスのほか、アクティビティ（ファイルのアップロードとダウンロード）およびログアウトが示されています。

```

Wed Sep 8 18:03:06 2004 Info: Begin Logfile

Wed Sep 8 18:03:06 2004 Info: Version: 4.0.0-206 SN: 00065BF3BA6D-9WFWC21

Wed Sep 8 18:03:06 2004 Info: Time offset from UTC: 0 seconds

Wed Sep 8 18:03:06 2004 Info: System is coming up

Fri Sep 10 08:07:32 2004 Info: Time offset from UTC: -25200 seconds

Fri Sep 10 08:07:32 2004 Info: ID:1 Connection from 10.1.3.14 on 172.19.0.86

Fri Sep 10 08:07:38 2004 Info: ID:1 User admin login SUCCESS

Fri Sep 10 08:08:46 2004 Info: ID:1 Upload wording.txt 20 bytes

Fri Sep 10 08:08:57 2004 Info: ID:1 Download words.txt 1191 bytes

Fri Sep 10 08:09:06 2004 Info: ID:1 User admin logout

```

## IronPort HTTP ログの使用

表 34-19 HTTP ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻。
ID	セッション ID
req	接続マシンの IP アドレス
user	接続ユーザのユーザ名
Message	実行されたアクションに関する情報。GET コマンド、POST コマンド、またはシステム ステータスなどが含まれる場合があります。

### HTTP ログの例

次の HTTP ログの例は、管理者ユーザと GUI の対話（システム設定ウィザードの実行など）を示しています。

```

Wed Sep 8 18:17:23 2004 Info: http service on 192.168.0.1:80 redirecting to https port 443

Wed Sep 8 18:17:23 2004 Info: http service listening on 192.168.0.1:80

Wed Sep 8 18:17:23 2004 Info: https service listening on 192.168.0.1:443

Wed Sep 8 11:17:24 2004 Info: Time offset from UTC: -25200 seconds

Wed Sep 8 11:17:24 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg POST /system_administration/system_setup_wizard HTTP/1.1 303

Wed Sep 8 11:17:25 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET /system_administration/ssw_done HTTP/1.1 200

Wed Sep 8 11:18:45 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET /monitor/incoming_mail_overview HTTP/1.1 200

Wed Sep 8 11:18:45 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET /monitor/mail_flow_graph?injector=&width=365&interval=0&type=recipientsin&height=190 HTTP/1.1 200

Wed Sep 8 11:18:46 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET /monitor/classification_graph?injector=&width=325&interval=0&type=recipientsin&height=190 HTTP/1.1 200

Wed Sep 8 11:18:49 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET /monitor/quarantines HTTP/1.1 200

```



## IronPort NTP ログの使用

表 34-20 NTP ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻。
Message	メッセージは、サーバへの Simple Network Time Protocol (SNTP; 簡易ネットワーク タイム プロトコル) クエリーまたは adjust: メッセージで構成されます。

### NTP ログの例

次の NTP ログの例は、アプライアンスから NTP ホストへの 2 度のポーリングを示しています。

```
Thu Sep 9 07:36:39 2004 Info: sntp query host 10.1.1.23 delay 653 offset -652
Thu Sep 9 07:36:39 2004 Info: adjust: time_const: 8 offset: -652us next_poll: 4096
Thu Sep 9 08:44:59 2004 Info: sntp query host 10.1.1.23 delay 642 offset -1152
Thu Sep 9 08:44:59 2004 Info: adjust: time_const: 8 offset: -1152us next_poll: 4096
```

## スキャン ログの使用

スキャン ログには、アプライアンスのスキャン エンジンのすべての LOG および COMMON メッセージが含まれています。使用可能な COMMON および LOG アラート メッセージのリストについては、『Cisco IronPort AsyncOS for Email Configuration Guide』の「System Administration」の章の「Alerts」を参照してください。

表 34-21 スキャン ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻。
Message	メッセージは、いずれかのスキャン エンジンのアプリケーションの障害、送信されたアラート、失敗したアラート、またはログ エラー メッセージで構成されています。

### スキャン ログの例

次のログの例は、Sophos アンチウイルスに関する警告アラートを送信しているアプライアンスの履歴を示しています。

```
Wed Feb 23 22:05:48 2011 Info: Internal SMTP system attempting to send a message to alerts@example.com with subject 'Warning <Anti-Virus> mail3.example.com: sophos antivirus - The Anti-Virus database on this system is...' (attempt #0).
```

```
Wed Feb 23 22:05:48 2011 Info: Internal SMTP system successfully sent a message to alerts@example.com with subject 'Warning <Anti-Virus> mail3.example.com: sophos antivirus - The Anti-Virus database on this system is...'.
```

```
Wed Feb 23 22:05:48 2011 Info: A Anti-Virus/Warning alert was sent to alerts@example.com with subject "Warning <Anti-Virus> mail3.example.com: sophos antivirus - The Anti-Virus database on this system is...".
```

## IronPort アンチスパムの使用

表 34-22 アンチスパム ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻。
Message	メッセージは、アンチスパム アップデートの確認と結果（エンジンまたはアンチスパム ルールのアップデートが必要であったかどうかなど）で構成されます。

### アンチスパム ログの例

次のアンチスパム ログの例は、アンチスパム エンジンによる、スパム定義のアップデートおよび CASE アップデートの確認を示しています。

```
Fri Apr 13 18:59:47 2007 Info: case antispam - engine (19103) : case-daemon: server
successfully spawned child process, pid 19111
```

```
Fri Apr 13 18:59:47 2007 Info: case antispam - engine (19111) : startup: Region profile:
Using profile global
```

```
Fri Apr 13 18:59:59 2007 Info: case antispam - engine (19111) : fuzzy: Fuzzy plugin v7
successfully loaded, ready to roll
```

```
Fri Apr 13 19:00:01 2007 Info: case antispam - engine (19110) : uribllocal: running URI
blocklist local
```

```
Fri Apr 13 19:00:04 2007 Info: case antispam - engine (19111) : config: Finished loading
configuration
```

## IronPort アンチウイルス ログの使用

表 34-23 アンチウイルス ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻。
Message	メッセージは、アンチウイルス アップデートの確認と結果（エンジンまたはウイルス定義のアップデートが必要であったかどうかなど）で構成されます。

### アンチウイルス ログの例

次のアンチウイルス ログの例は、Sophos アンチウイルス エンジンによる、ウイルス定義（IDE）とエンジン自体のアップデートの確認を示しています。

```
Thu Sep 9 14:18:04 2004 Info: Checking for Sophos Update
```

```
Thu Sep 9 14:18:04 2004 Info: Current SAV engine ver=3.84. No engine update needed
```

```
Thu Sep 9 14:18:04 2004 Info: Current IDE serial=2004090902. No update needed.
```

このログを一時的に DEBUG レベルに設定すると、アンチウイルス エンジンが所定のメッセージについて特定の結果を返した理由を診断するのに役立ちます。DEBUG ログ情報は冗長です。使用の際は注意してください。

## IronPort スпам隔離ログの使用

表 34-24 IronPort スпам ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻。
Message	メッセージは、実行されたアクション（メッセージの隔離、隔離エリアからの解放など）で構成されます。

### IronPort スпам隔離ログの例

次のログの例は、隔離から admin@example.com にメッセージ（MID 8298624）が解放されていることを示しています。

```
Mon Aug 14 21:41:47 2006 Info: ISQ: Releasing MID [8298624, 8298625] for all
Mon Aug 14 21:41:47 2006 Info: ISQ: Delivering released MID 8298624 (skipping work queue)
Mon Aug 14 21:41:47 2006 Info: ISQ: Released MID 8298624 to admin@example.com
Mon Aug 14 21:41:47 2006 Info: ISQ: Delivering released MID 8298625 (skipping work queue)
Mon Aug 14 21:41:47 2006 Info: ISQ: Released MID8298625 to admin@example.com
```

## IronPort スпам隔離 GUI ログの使用

表 34-25 IronPort スпам GUI ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻。
Message	メッセージは、ユーザ認証などの実行されたアクションで構成されます。

### IronPort スпам隔離 GUI ログの例

次のログの例は、成功した認証、ログイン、およびログアウトを示しています。

```
Fri Aug 11 22:05:28 2006 Info: ISQ: Serving HTTP on 192.168.0.1, port 82
Fri Aug 11 22:05:29 2006 Info: ISQ: Serving HTTPS on 192.168.0.1, port 83
Fri Aug 11 22:08:35 2006 Info: Authentication OK, user admin
Fri Aug 11 22:08:35 2006 Info: logout:- user:pqufOtL6vyI5StCqhCf0 session:10.251.23.228
```

```
Fri Aug 11 22:08:35 2006 Info: login:admin user:pqufOtL6vyI5StCqhCfO
session:10.251.23.228
```

```
Fri Aug 11 22:08:44 2006 Info: Authentication OK, user admin
```

## IronPort LDAP デバッグ ログの使用

表 34-26 LDAP デバッグ ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻。
Message	LDAP デバッグ メッセージ。

### LDAP デバッグ ログの例



(注)

ログ ファイルの各行には、番号が割り当てられません。ここでは、単にサンプル用として番号が割り当てられています。

```
1 Thu Sep 9 12:24:56 2004 Begin Logfile
2 Thu Sep 9 12:25:02 2004 LDAP: Masquerade query sun.masquerade address
employee@routing.qa to employee@mail.qa
3 Thu Sep 9 12:25:02 2004 LDAP: Masquerade query sun.masquerade address
employee@routing.qa to employee@mail.qa
4 Thu Sep 9 12:25:02 2004 LDAP: Masquerade query sun.masquerade address
employee@routing.qa to employee@mail.qa
5 Thu Sep 9 12:28:08 2004 LDAP: Clearing LDAP cache
6 Thu Sep 9 13:00:09 2004 LDAP: Query '(&(ObjectClass={g})(mailLocalAddress={a}))'
to server sun (sun.qa:389)
7 Thu Sep 9 13:00:09 2004 LDAP: After substitute, query is
'(&(ObjectClass=inetLocalMailRecipient)(mailLocalAddress=rroute.d00002b.loc@ldap.rou
te.local.add00002.qa))'
8 Thu Sep 9 13:00:09 2004 LDAP: connecting to server
9 Thu Sep 9 13:00:09 2004 LDAP: connected
10 Thu Sep 9 13:00:09 2004 LDAP: Query
(&(ObjectClass=inetLocalMailRecipient)(mailLocalAddress=rroute.d00002b.loc@ldap.rou
te.local.add00002.qa)) returned 1 results
11 Thu Sep 9 13:00:09 2004 LDAP: returning: [<LDAP:>]
```

前述のログ ファイルを読み取るためのガイドとして、使用してください。

表 34-27 LDAP デバッグ ログの例の詳細

行番号	説明
1.	ログ ファイルが開始されます。
2.	リスナーは、明確に「sun.masquerade」という LDAP クエリーによって、マスカレードに LDAP を使用するように設定されています。
3.	
4.	
5.	ユーザは手動で <code>ldapflush</code> を実行しています。
6.	クエリーは、 <code>sun.qa</code> 、ポート 389 に送信されます。クエリー テンプレートは <code>(&amp;(ObjectClass={g})(mailLocalAddress={a}))</code> です。
	<code>{g}</code> は、発信側フィルタ ( <code>rcpt-to-group</code> または <code>mail-from-group</code> ルール) で指定されたグループ名に置換されます。
	<code>{a}</code> は、当該のアドレスに置換されます。
7.	ここで代入 (前述のとおり) が実行されます。LDAP サーバに送信される前のクエリーはこのようになります。
8.	
9.	サーバへの接続がまだ確立されていないので、接続します。
10.	サーバに送信されるデータです。
11.	結果は、確実に空になります。つまり、1 つのレコードが返されますが、クエリーはフィールドを要求していないので、データは報告されません。これらは、データベースに一致があるかどうかをクエリーでチェックするときに、グループクエリーと許可クエリーの両方に使用されます。

## セーフリスト/ブロックリスト ログの使用

表 34-28 に、セーフリスト/ブロックリスト ログに記録される統計情報を示します。

表 34-28 セーフリスト/ブロックリスト ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻。
Message	メッセージは、ユーザ認証など、実行されたアクションで構成されます。

## セーフリスト/ブロックリスト ログの例

次のセーフリスト/ブロックリスト ログの例は、アプライアンスによって 2 時間ごとにデータベースのスナップショットが作成されていることを示しています。送信者がデータベースに追加された時刻も表示されます。

```
Fri Sep 28 14:22:33 2007 Info: Begin Logfile Fri Sep 28 14:22:33 2007 Info: Version:
6.0.0-425 SN: XXXXXXXXXXXXX-XXX Fri Sep 28 14:22:33 2007 Info: Time offset from UTC:
10800 seconds Fri Sep 28 14:22:33 2007 Info: System is coming up.
```

```
Fri Sep 28 14:22:33 2007 Info: SLBL: The database snapshot has been created.
```

```
Fri Sep 28 16:22:34 2007 Info: SLBL: The database snapshot has been created.
```

```
Fri Sep 28 18:22:34 2007 Info: SLBL: The database snapshot has been created.
```

```
Fri Sep 28 20:22:34 2007 Info: SLBL: The database snapshot has been created.
```

```
Fri Sep 28 22:22:35 2007 Info: SLBL: The database snapshot has been created.
```

```
.....
```

```
Mon Oct 1 14:16:09 2007 Info: SLBL: The database snapshot has been created.
```

```
Mon Oct 1 14:37:39 2007 Info: SLBL: The database snapshot has been created.
```

```
Mon Oct 1 15:31:37 2007 Warning: SLBL: Adding senders to the database failed.
```

```
Mon Oct 1 15:32:31 2007 Warning: SLBL: Adding senders to the database failed.
```

```
Mon Oct 1 16:37:40 2007 Info: SLBL: The database snapshot has been created.
```

## レポーティング ログの使用

表 34-29 に、レポーティング ログに記録される統計情報を示します。

表 34-29 レポーティング ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻。
Message	メッセージは、ユーザ認証など、実行されたアクションで構成されます。

### レポーティング ログの例

次のレポーティング ログの例は、情報ログ レベルに設定されたアプライアンスを示しています。

```
Wed Oct 3 13:39:53 2007 Info: Period minute using 0 (KB)
```

```
Wed Oct 3 13:39:53 2007 Info: Period month using 1328 (KB)
```

```
Wed Oct 3 13:40:02 2007 Info: Update 2 registered appliance at 2007-10-03-13-40
```

```
Wed Oct 3 13:40:53 2007 Info: Pages found in cache: 1304596 (99%). Not found: 1692
```

```

Wed Oct 3 13:40:53 2007 Info: Period hour using 36800 (KB)

Wed Oct 3 13:40:53 2007 Info: Period day using 2768 (KB)

Wed Oct 3 13:40:53 2007 Info: Period minute using 0 (KB)

Wed Oct 3 13:40:53 2007 Info: Period month using 1328 (KB)

Wed Oct 3 13:40:53 2007 Info: HELPER checkpointed in 0.00580507753533 seconds

Wed Oct 3 13:41:02 2007 Info: Update 2 registered appliance at 2007-10-03-13-41

Wed Oct 3 13:41:53 2007 Info: Pages found in cache: 1304704 (99%). Not found: 1692

Wed Oct 3 13:41:53 2007 Info: Period hour using 36800 (KB)

Wed Oct 3 13:41:53 2007 Info: Period day using 2768 (KB)

Wed Oct 3 13:41:53 2007 Info: Period minute using 0 (KB)

Wed Oct 3 13:41:53 2007 Info: Period month using 1328 (KB)

Wed Oct 3 13:42:03 2007 Info: Update 2 registered appliance at 2007-10-03-13-42

```

## レポートイング クエリー ログの使用

表 34-30 に、レポートイング クエリー ログに記録される統計情報を示します。

**表 34-30 レポートイング クエリー ログの統計情報**

統計	説明
Timestamp	バイトが送信された時刻。
Message	メッセージは、ユーザ認証など、実行されたアクションで構成されます。

### レポートイング クエリー ログの例

次のレポートイング クエリー ログの例は、アプライアンスによって、2007 年 8 月 29 日から 10 月 10 日までの期間で毎日の発信メール トラフィック クエリーが実行されていることを示しています。

```

Tue Oct 2 11:30:02 2007 Info: Query: Closing interval handle 811804479.

Tue Oct 2 11:30:02 2007 Info: Query: Closing interval handle 811804480.

Tue Oct 2 11:30:02 2007 Info: Query: Closing query handle 302610228.

Tue Oct 2 11:30:02 2007 Info: Query: Merge query with handle 302610229 for
['MAIL_OUTGOING_TRAFFIC_SUMMARY.
DETECTED_SPAM', 'MAIL_OUTGOING_TRAFFIC_SUMMARY.DETECTED_VIRUS',
'MAIL_OUTGOING_TRAFFIC_SUMMARY.THREAT_CONTENTEN
T_FILTER', 'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_CLEAN_RECIPIENTS',
'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_RECIP

```

```

PIENTS_PROCESSED'] for rollup period "day" with interval range 2007-08-29 to 2007-10-01
with key constraints

None sorting on ['MAIL_OUTGOING_TRAFFIC_SUMMARY.DETECTED_SPAM'] returning results from
0 to 2 sort_ascending

g=False.

Tue Oct 2 11:30:02 2007 Info: Query: Closing query handle 302610229.

Tue Oct 2 11:30:02 2007 Info: Query: Merge query with handle 302610230 for
['MAIL_OUTGOING_TRAFFIC_SUMMARY.

TOTAL_HARD_BOUNCES', 'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_RECIPIENTS_DELIVERED',
'MAIL_OUTGOING_TRAFFIC_SUMM

ARY.TOTAL_RECIPIENTS'] for rollup period "day" with interval range 2007-08-29 to
2007-10-01 with key constra

ints None sorting on ['MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_HARD_BOUNCES'] returning
results from 0 to 2 sort

_ascending=False.

Tue Oct 2 11:30:02 2007 Info: Query: Closing query handle 302610230.

```

## アップデータ ログの使用

表 34-31 アップデータ ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻。
Message	メッセージは、システム サービス アップデート情報のほか、AsyncOS によるアップデートの確認と、スケジュールされている次回アップデートの日時で構成されます。

### アップデータ ログの例

次のログの例は、アプライアンスが新規の McAfee アンチウイルス定義でアップデートされていることを示しています。

```

Fri Sep 19 11:07:51 2008 Info: Starting scheduled update

Fri Sep 19 11:07:52 2008 Info: Acquired server manifest, starting update 11

Fri Sep 19 11:07:52 2008 Info: Server manifest specified an update for mcafee

Fri Sep 19 11:07:52 2008 Info: mcafee was signalled to start a new update

Fri Sep 19 11:07:52 2008 Info: mcafee processing files from the server manifest

Fri Sep 19 11:07:52 2008 Info: mcafee started downloading files

```



```
Fri Sep 19 11:07:52 2008 Info: mcafee downloading remote file
"http://stage-updates.ironport.com/mcafee/dat/5388"

Fri Sep 19 11:07:52 2008 Info: Scheduled next update to occur at Fri Sep 19 11:12:52
2008

Fri Sep 19 11:08:12 2008 Info: mcafee started decrypting files

Fri Sep 19 11:08:12 2008 Info: mcafee decrypting file
"mcafee/dat/5388" with method "des3_cbc"

Fri Sep 19 11:08:17 2008 Info: mcafee started decompressing files

Fri Sep 19 11:08:17 2008 Info: mcafee started applying files

Fri Sep 19 11:08:17 2008 Info: mcafee applying file "mcafee/dat/5388"

Fri Sep 19 11:08:18 2008 Info: mcafee verifying applied files

Fri Sep 19 11:08:18 2008 Info: mcafee updating the client manifest

Fri Sep 19 11:08:18 2008 Info: mcafee update completed

Fri Sep 19 11:08:18 2008 Info: mcafee waiting for new updates

Fri Sep 19 11:12:52 2008 Info: Starting scheduled update

Fri Sep 19 11:12:52 2008 Info: Scheduled next update to occur at Fri Sep 19 11:17:52
2008

Fri Sep 19 11:17:52 2008 Info: Starting scheduled update

Fri Sep 19 11:17:52 2008 Info: Scheduled next update to occur at Fri Sep 19 11:22:52
2008
```

## トラッキング ログについて

トラッキング ログには、AsyncOS の電子メール動作に関する情報が記録されます。ログメッセージは、メール ログに記録されたメッセージのサブセットです。

トラッキング ログは、メッセージトラッキングデータベースを作成するため、アプライアンスのメッセージトラッキングコンポーネントで使用されます。ログファイルはデータベースの作成プロセスで消費されるので、トラッキングログは一過性のものになります。トラッキングログの情報は、人による読み取りや解析を目的とした設計になっていません。

Cisco セキュリティ管理アプライアンスを使用することで、複数の電子メールセキュリティアプライアンスからのトラッキング情報の表示もできます。

## 認証ログの使用

認証ログには、成功したユーザ ログインと失敗したログイン試行が記録されます。

表 34-32 認証ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻。
Message	メッセージは、アプライアンスにログインしようとしたユーザのユーザ名と、そのユーザが正常に認証されたかどうかという情報で構成されます。

### 認証ログの例

次のログの例は、「admin」、「joe」、および「dan」というユーザによるログイン試行を示しています。

```
Wed Sep 17 15:16:25 2008 Info: Begin Logfile
Wed Sep 17 15:16:25 2008 Info: Version: 6.5.0-262 SN: XXXXXXXX-XXXXX
Wed Sep 17 15:16:25 2008 Info: Time offset from UTC: 0 seconds
Wed Sep 17 15:18:21 2008 Info: User admin was authenticated successfully.
Wed Sep 17 16:26:17 2008 Info: User joe failed authentication.
Wed Sep 17 16:28:28 2008 Info: User joe was authenticated successfully.
Wed Sep 17 20:59:30 2008 Info: User admin was authenticated successfully.
Wed Sep 17 21:37:09 2008 Info: User dan failed authentication.
```

## コンフィギュレーション履歴ログの使用

コンフィギュレーション履歴ログは、設定ファイルで構成され、ユーザの名前、ユーザが変更を行った設定の場所の説明、変更を保存するときにユーザが入力したコメントがリストされた追加のセクションがあります。ユーザが変更をコミットするたびに、変更後の設定ファイルを含む新しいログが作成されます。

### 設定履歴ログの例

次の設定履歴ログの例は、システムへのログインを許可されているローカル ユーザを定義するテーブルにユーザ (admin) がゲスト ユーザを追加したことを示しています。

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<!--
XML generated by configuration change.
Change comment: added guest user
```

```
User: admin

Configuration are described as:

 This table defines which local users are allowed to log into the system.

Product: Cisco IronPort M160 Messaging Gateway(tm) Appliance

Model Number: M160

Version: 6.7.0-231

Serial Number: 000000000ABC-D000000

Number of CPUs: 1

Memory (GB): 4

Current Time: Thu Mar 26 05:34:36 2009

Feature "Cisco IronPort Centralized Configuration Manager": Quantity = 10, Time
Remaining = "25 days"

Feature "Centralized Reporting": Quantity = 10, Time Remaining = "9 days"

Feature "Centralized Tracking": Quantity = 10, Time Remaining = "30 days"

Feature "Centralized Spam Quarantine": Quantity = 10, Time Remaining = "30 days"

Feature "Receiving": Quantity = 1, Time Remaining = "Perpetual"

-->

<config>
```

## ログサブスクリプション

- 「ログサブスクリプションの設定」 (P.34-40)
- 「GUIでのログサブスクリプションの作成」 (P.34-41)
- 「ログインに対するグローバル設定」 (P.34-41)
- 「ログサブスクリプションのロールオーバー」 (P.34-44)
- 「ホストキーの設定」 (P.34-50)

## ログサブスクリプションの設定

[システム管理 (System Administration)] の [ログサブスクリプション (Log Subscriptions)] ページ (または CLI の `logconfig` コマンド) を使用して、ログサブスクリプションを設定します。ログサブスクリプションによって、エラーを含む AsyncOS アクティビティの情報を保存するログファイルが作成されます。ログサブスクリプションは、取得されるか、または別のコンピュータに配信 (プッシュ) されるかのどちらかです。一般に、ログサブスクリプションには次の属性があります。

表 34-33 ログファイルの属性

属性	説明
ログタイプ (Log type)	記録される情報のタイプと、ログサブスクリプションの形式を定義します。詳細については、表 34-1 「ログタイプ」 (P.2) を参照してください。
名前 (Name)	今後の参照に使用するログサブスクリプションのニックネーム。
ファイルサイズ別ロールオーバー (Rollover by File Size)	ファイルの最大サイズ。このサイズに到達すると、ローリングオーバーされます。
時刻によりロールオーバー (Rollover by Time)	ファイルのロールオーバーの時間間隔を設定します。
ログレベル (Log level)	ログサブスクリプションごとに詳細のレベルを設定します。
検索方法 (Retrieval method)	ログサブスクリプションが Cisco アプライアンスから取得される方法を定義します。
ログファイル名 (Log filename)	ディスクに書き込むときのファイルの物理名に使用されます。複数の Cisco アプライアンスを使用している場合、ログファイルを生成したシステムを識別するため、ログファイル名を固有にする必要があります。

## ログレベル

ログレベルによって、ログに送信される情報量が決定します。ログには、5 つの詳細レベルのいずれかを設定できます。詳細レベルを高くするほど大きいログファイルが作成され、システムのパフォーマンスが低下します。詳細レベルの高い設定には、詳細レベルの低い設定に保持されるすべてのメッセージと、その他のメッセージも含まれます。詳細レベルを上げるほど、システムのパフォーマンスは低下します。



(注) ログレベルは、すべてのメールログタイプに対して選択できます。

表 34-34 ログレベル

ログレベル	説明
クリティカル (Critical)	詳細レベルの最も低い設定。エラーだけがログに記録されます。この設定にすると、パフォーマンスやその他の重要なアクティビティをモニタできませんが、ログファイルがすぐには最大サイズに達しなくなります。このログレベルは、syslog レベル「Alert」と同等です。
警告 (Warning)	システムによって作成されたすべてのエラーと警告。この設定にすると、パフォーマンスやその他の重要なアクティビティをモニタできません。このログレベルは、syslog レベル「Warning」と同等です。
情報 (Information)	情報設定では、システムの秒単位の動作がキャプチャされます。たとえば、接続のオープンや配信試行などです。Information レベルは、ログに推奨される設定です。このログレベルは、syslog レベル「Info」と同等です。

表 34-34 ログレベル (続き)

ログレベル	説明
デバッグ (Debug)	エラーの原因を調べるときは、Debug ログレベルを使用します。この設定は一時的に使用し、後でデフォルトレベルに戻します。このログレベルは、syslog レベル「Debug」と同等です。
トレース (Trace)	Trace ログレベルは、開発者にのみ推奨されます。このレベルを使用すると、システムのパフォーマンスが大きく低下するので、推奨されません。このログレベルは、syslog レベル「Debug」と同等です。

## GUI でのログサブスクリプションの作成

### 手順

- ステップ 1 [システム管理 (System Administration)] > [ログサブスクリプション (Log Subscriptions)] を選択します。
- ステップ 2 [ログサブスクリプションを追加 (Add Log Subscription)] をクリックします。
- ステップ 3 ログタイプを選択し、ログ名 (ログディレクトリ用) とログファイル自体の名前を入力します。
- ステップ 4 AsyncOS がログファイルをロールオーバーする前の最大ファイルサイズ、およびロールオーバー間の時間間隔を指定します。ファイルのロールオーバーの詳細については、「[ログサブスクリプションのロールオーバー](#)」(P.34-44) を参照してください。
- ステップ 5 ログレベルを選択します。使用可能なオプションは、[クリティカル (Critical)]、[警告 (Warning)]、[情報 (Information)]、[デバッグ (Debug)]、または [トレース (Trace)] です。
- ステップ 6 ログの取得方法を設定します。
- ステップ 7 変更内容を送信し、確定します。

## ログサブスクリプションの編集

### 手順

- ステップ 1 [システム管理 (System Administration)] > [ログサブスクリプション (Log Subscriptions)] を選択します。
- ステップ 2 [ログ設定 (Log Settings)] カラムでログの名前をクリックします。
- ステップ 3 ログサブスクリプションを変更します。
- ステップ 4 変更内容を送信し、確定します。

## ログギングに対するグローバル設定

システムは、IronPort テキストメールログおよび IronPort ステータスログ内にシステムの測定を定期的に記録します。[システム管理 (System Administration)] > [ログサブスクリプション (Log Subscriptions)] ページの [グローバル設定 (Global Settings)] セクションにある [設定を編集 (Edit Settings)] ボタン (または、CLI の `logconfig -> setup` コマンド) を使用して、次の情報を設定します。

- システムの測定頻度。これは、システムが測定を記録するまで待機する時間 (秒単位) です。

- メッセージ ID ヘッダーを記録するかどうか。
- リモート応答ステータス コードを記録するかどうか。
- 元のメッセージのサブジェクト ヘッダーを記録するかどうか。
- メッセージごとにログに記録するヘッダーのリスト。

すべての IronPort ログには、次の 3 つのデータを任意で記録できます。

### 1. Message-ID

このオプションを設定すると、可能な場合はすべてのメッセージのメッセージ ID ヘッダーがログに記録されます。このメッセージ ID は、受信したメッセージから取得される場合と、AsyncOS 自体で生成される場合があります。次に例を示します。

```
Tue Apr 6 14:38:34 2004 Info: MID 1 Message-ID Message-ID-Content
```

### 2. Remote Response

このオプションを設定すると、可能な場合はすべてのメッセージのリモート応答ステータス コードがログに記録されます。次に例を示します。

```
Tue Apr 6 14:38:34 2004 Info: MID 1 RID [0] Response 'queued as 9C8B425DA7'
```

リモート応答文字列は、SMTP 会話配信時の DATA コマンドへの応答後に受信される、人が読み取ることのできるテキストです。この例では、接続ホストが data コマンドを実行した後のリモート応答が、「queued as 9C8B425DA7」となります。

[...]

```
250 ok hostname
```

```
250 Ok: queued as 9C8B425DA7
```

文字列の先頭にある空白や句読点（および、250 応答の場合は OK 文字）は除去されます。文字列の末尾については、空白だけが除去されます。たとえば、Cisco アプライアンスはデフォルトで、DATA コマンドに対して「250 Ok: Message MID accepted」という文字列で応答します。したがって、リモートホストが別の Cisco アプライアンスである場合は、文字列「Message MID accepted」がログに記録されます。

### 3. Original Subject Header

このオプションをイネーブルにすると、各メッセージの元のサブジェクトヘッダーがログに記録されます。

```
Tue May 31 09:20:27 2005 Info: Start MID 2 ICID 2
```

```
Tue May 31 09:20:27 2005 Info: MID 2 ICID 2 From: <mary@example.com>
```

```
Tue May 31 09:20:27 2005 Info: MID 2 ICID 2 RID 0 To: <joe@example.com>
```

```
Tue May 31 09:20:27 2005 Info: MID 2 Message-ID '<44e4n$2@example.com>'
```

```
Tue May 31 09:20:27 2005 Info: MID 2 Subject 'Monthly Reports Due'
```

## メッセージ ヘッダーのロギング

場合によっては、メッセージがシステムを通過するときに、メッセージのヘッダーの存在と内容を記録する必要があります。[ログサブスクリプションのグローバル設定 (Log Subscriptions Global Settings)] ページ (または、CLI の `logconfig -> logheaders` サブコマンド) に、記録するヘッダーを指定します。Cisco アプライアンスは、指定されたメッセージヘッダーを IronPort テキスト メール ログ、IronPort 配信ログ、および IronPort バウンス ログに記録します。ヘッダーが存在する場合、システムはヘッダーの名前と値を記録します。ヘッダーが存在しない場合は、ログに何も記録されません。



(注) システムは、ロギングに指定したヘッダーに関係なく、メッセージの記録処理中に随時、メッセージに存在するすべてのヘッダーを評価します。



(注) SMTP プロトコルについての RFC は、<http://www.faqs.org/rfcs/rfc2821.html> にあります。この RFC には、ユーザ定義のヘッダーが規定されています。



(注) `logheaders` コマンドを使用してヘッダーをログに記録するように設定している場合、ヘッダー情報は配信情報の後に表示されます。

表 34-35 ログ ヘッダー

ヘッダー名	ヘッダーの名前
値	ログに記録されるヘッダーの内容

たとえば、ログに記録するヘッダーとして「`date, x-subject`」を指定すると、メール ログに次の行が表示されます。

```
Tue May 31 10:14:12 2005 Info: Message done DCID 0 MID 3 to RID [0] [('date', 'Tue, 31
May 2005 10:13:18 -0700'), ('x-subject', 'Logging this header')]
```

## GUI を使用したロギングのグローバル設定

### 手順

- ステップ 1 [システム管理 (System Administration)] > [ログサブスクリプション (Log Subscriptions)] を選択します。
- ステップ 2 [グローバル設定 (Global Settings)] セクションまでスクロールします。
- ステップ 3 [設定を編集 (Edit Settings)] をクリックします。
- ステップ 4 システム測定頻度、メール ログにメッセージ ID ヘッダーを加えるかどうか、リモート応答を加えるかどうか、および各メッセージの元のサブジェクトヘッダーを加えるかどうかを含めた情報を指定します。
- ステップ 5 ログに加えるその他のヘッダーを入力します。

ステップ 6 変更内容を送信し、確定します。

## ログサブスクリプションのロールオーバー

アプライアンス上のログファイルが大きくなりすぎないようにするために、ログファイルがユーザ指定の最大ファイルサイズまたは時間間隔に達すると、AsyncOS は「ロールオーバー」を実行してログファイルをアーカイブし、着信するログデータのための新しいファイルを作成します。ログサブスクリプション用に定義された取得方法に基づいて、古いログファイルは取得のためにアプライアンス上に保管されるか、または外部のコンピュータに配信されます。アプライアンスからログファイルを取得する方法の詳細については、「[ログ取得方法](#)」(P.34-7) を参照してください。

AsyncOS は、ログファイルをロールオーバーするときに次のアクションを実行します。

- 現在のログファイルの名前をロールオーバーのタイムスタンプと、保存済みを示す文字「s」の拡張子を使用して変更します。
- 新しいログファイルを作成し、「current」の拡張子を使用して、そのファイルを最新として指定します。
- 新しく保存されたログファイルをリモートホストに転送します（プッシュベースの取得方法を使用している場合）。
- 同じサブスクリプションから、以前に失敗したログファイルをすべて転送します（プッシュベースの取得方法を使用している場合）。
- 保存すべきファイルの総数を超えた場合は、ログサブスクリプション内の最も古いファイルを削除します（ポーリングベースの取得方法を使用している場合）。

ログサブスクリプションのロールオーバーの設定は、GUI の [システム管理 (System Administration)] > [ログサブスクリプション (Log Subscriptions)] ページ、または CLI の `logconfig` コマンドを使用してサブスクリプションを作成または編集するときに定義します。ログファイルのロールオーバーをトリガーするために使用できる 2 つの設定は次のとおりです。

- 最大ファイルサイズ。
- 時間間隔。

図 34-1 に、GUI でログサブスクリプションに使用できるロールオーバーの設定を示します。

図 34-1 ログサブスクリプションのためのログファイルのロールオーバーの設定

Rollover by File Size:	<input type="text" value="10M"/> Maximum <small>(Add a trailing K or M to indicate size units.)</small>
Rollover by Time:	<input type="button" value="Custom Time Interval"/> Rollover every: <input type="text" value="4h 30m"/> <small>(Example: 120s, 5m 30s, 4h, 2d)</small>

## ファイルサイズによるロールオーバー

AsyncOS は、ログファイルで使用されるディスク領域が多くなりすぎないようにするために、最大ファイルサイズに達したログファイルをロールオーバーします。ロールオーバーのための最大ファイルサイズを定義する場合は、メガバイトを示す `m` とキロバイトを示す `k` のサフィックスを使用します。たとえば、ログファイルが 10 MB に達したら AsyncOS によってロールオーバーされるようにする場合は、「10m」と入力します。



## 時間によるロールオーバー

ロールオーバーを定期的に行われるようにスケジュールする場合は、次のいずれかの時間間隔を選択できます。

- **[None]**。AsyncOS は、ログ ファイルが最大ファイル サイズに達した場合にのみロールオーバーを実行します。
- **[カスタム時間間隔 (Custom Time Interval)]**。AsyncOS は、以前のロールオーバーから指定された時間が経過した後にロールオーバーを実行します。スケジュール設定されたロールオーバーのためのカスタムの時間間隔を作成するには、d、h、および m をサフィックスとして使用して、ロールオーバー間の日数、時間数、および分数を入力します。
- **[日次ロールオーバー (Daily Rollover)]**。AsyncOS は、毎日指定された時刻にロールオーバーを実行します。日単位のロールオーバーを選択した場合は、24 時間形式 (HH:MM) を使用して、AsyncOS がロールオーバーを実行する時刻を入力します。

GUI では、[日次ロールオーバー (Daily Rollover)] オプションのみが提供されます。CLI の `logconfig` コマンドを使用して日単位のロールオーバーを設定する場合は、[週次ロールオーバー (Weekly Rollover)] オプションを選択し、アスタリスク (\*) を使用して AsyncOS がすべての曜日にロールオーバーを実行することを指定します。

- **[週次ロールオーバー (Weekly Rollover)]**。AsyncOS は、1 つ以上の曜日の指定された時刻にロールオーバーを実行します。たとえば、毎週水曜日と金曜日の午前 0:00 にログ ファイルをロールオーバーするように AsyncOS を設定できます。週単位のロールオーバーを設定するには、ロールオーバーを実行する曜日と 24 時間形式 (HH:MM) の時刻を選択します。

CLI を使用している場合は、ダッシュ (-) を使用して日の範囲を指定するか、アスタリスク (\*) を使用してすべての曜日を指定するか、またはカンマ (,) を使用して複数の日と時刻を区切ることができます。

図 34-2 に、GUI で [週次ロールオーバー (Weekly Rollover)] オプションに使用できる設定を示します。



表 34-36 に、CLI を使用して、水曜日と金曜日の午前 0:00 (00:00) にログサブスクリプションのファイルをロールオーバーする方法を示します。

表 34-36 CLI での週単位のログ ロールオーバーの設定

```
Do you want to configure time-based log files rollover? [N]> y

Configure log rollover settings:

1. Custom time interval.

2. Weekly rollover.

[1]> 2

1. Monday

2. Tuesday

3. Wednesday

4. Thursday

5. Friday

6. Saturday

7. Sunday

Choose the day of week to roll over the log files. Separate multiple days with comma,
or use "*" to specify every day of a week. Also you can use dash to specify a range
like "1-5":

[]> 3, 5

Enter the time of day to rollover log files in 24-hour format (HH:MM). You can specify
hour as "*" to match every hour, the same for minutes. Separate multiple times of day
with comma:

[]> 00:00
```

## オンデマンドでのログサブスクリプションのロールオーバー

GUI を使用してログサブスクリプションをただちにロールオーバーするには、次の手順を実行します。

### 手順

- ステップ 1** [システム管理 (System Administration) ]>[ログサブスクリプション (Log Subscriptions) ] ページで、ロールオーバーするログの右側のチェックボックスをオンにします。
- ステップ 2** 任意で、[すべて (All) ] チェックボックスをオンにして、すべてのログをロールオーバー対象として選択できます。

- ステップ 3**    ロールオーバー対象として 1 つまたは複数のログを選択すると、[今すぐロールオーバー (Rollover Now)] ボタンがイネーブルになります。[今すぐロールオーバー (Rollover Now)] ボタンをクリックして、選択したログをロールオーバーします。

## GUI での最近のログ エントリの表示

GUI を介してログ ファイルを表示するには、[ログサブスクリプション (Log Subscriptions)] ページのテーブルの [ログ ファイル (Log Files)] カラムにあるログサブスクリプションをクリックします。ログサブスクリプションへのリンクをクリックすると、パスワードの入力を求められてから、そのサブスクリプションに対するログファイルの一覧が表示されます。次に、いずれかのログファイルをクリックして、ブラウザに表示したり、ディスクに保存したりすることができます。GUI を介してログを表示するには、管理インターフェイスで HTTP または HTTPS サービスをイネーブルにしておく必要があります。

図 34-3 ログサブスクリプションのグローバル設定  
Log Subscriptions

Configured Log Subscriptions					
Add Log Subscription...					
Log Settings	Type	Log Files	Rollover Interval	All <input type="checkbox"/> Rollover	Delete
antispam	Anti-Spam Logs	antispam/	None	<input type="checkbox"/>	
antivirus	Anti-Virus Logs	antivirus/	None	<input type="checkbox"/>	
asarchive	Anti-Spam Archive	asarchive/	None	<input type="checkbox"/>	
authentication	Authentication Logs	authentication/	None	<input type="checkbox"/>	
avarchive	Anti-Virus Archive	avarchive/	None	<input type="checkbox"/>	
bounces	Bounce Logs	bounces/	None	<input type="checkbox"/>	
cli_logs	CLI Audit Logs	cli_logs/	None	<input type="checkbox"/>	
encryption	Encryption Logs	encryption/	None	<input type="checkbox"/>	
error_logs	IronPort Text Mail Logs	error_logs/	None	<input type="checkbox"/>	
euq_logs	Spam Quarantine Logs	euq_logs/	None	<input type="checkbox"/>	
euqgui_logs	Spam Quarantine GUI Logs	euqgui_logs/	None	<input type="checkbox"/>	
ftpd_logs	FTP Server Logs	ftpd_logs/	None	<input type="checkbox"/>	
gui_logs	HTTP Logs	gui_logs/	None	<input type="checkbox"/>	
mail_logs	IronPort Text Mail Logs	mail_logs/	None	<input type="checkbox"/>	
reportd_logs	Reporting Logs	reportd_logs/	None	<input type="checkbox"/>	
reportqueryd_logs	Reporting Query Logs	reportqueryd_logs/	None	<input type="checkbox"/>	
scanning	Scanning Logs	scanning/	None	<input type="checkbox"/>	
sibld_logs	Safe/Block Lists Logs	sibld_logs/	None	<input type="checkbox"/>	
snmp_logs	SNMP Logs	snmp_logs/	None	<input type="checkbox"/>	
sntpd_logs	NTP logs	sntpd_logs/	None	<input type="checkbox"/>	
status	Status Logs	status/	None	<input type="checkbox"/>	
syslogs	System Logs	syslogs/	None	<input type="checkbox"/>	
system_logs	System Logs	system_logs/	None	<input type="checkbox"/>	
trackerd_logs	Tracking Logs	trackerd_logs/	None	<input type="checkbox"/>	
updater_logs	Updater Logs	updater_logs/	None	<input type="checkbox"/>	

## CLI での最近のログ エントリの表示 (tail コマンド)

AsyncOS では、アプライアンスに設定されたログの最新エントリを表示する tail コマンドをサポートしています。tail コマンドを実行し、現在設定されているログのうち、表示するログの番号を選択します。Ctrl+ C を押して、tail コマンドを終了します。

### 例

次に、tail コマンドを使用してシステム ログを表示する例を示します (このログは、特に commit コマンドによるユーザのコメントを追跡します)。また、tail コマンドでは、パラメータとして表示するログの名前 tail mail\_logs が受け入れられています。

```
mail3.example.com> tail
```

```
Currently configured logs:
```

1. "antispam" Type: "Anti-Spam Logs" Retrieval: Manual Download

2. "antivirus" Type: "Anti-Virus Logs" Retrieval: Manual Download
3. "asarchive" Type: "Anti-Spam Archive" Retrieval: Manual Download
4. "authentication" Type: "Authentication Logs" Retrieval: Manual Download
5. "avarchive" Type: "Anti-Virus Archive" Retrieval: Manual Download
6. "bounces" Type: "Bounce Logs" Retrieval: Manual Download
7. "cli\_logs" Type: "CLI Audit Logs" Retrieval: Manual Download
8. "encryption" Type: "Encryption Logs" Retrieval: Manual Download
9. "error\_logs" Type: "IronPort Text Mail Logs" Retrieval: Manual Download
10. "euq\_logs" Type: "IronPort Spam Quarantine Logs" Retrieval: Manual Download
11. "euqgui\_logs" Type: "IronPort Spam Quarantine GUI Logs" Retrieval: Manual Download
12. "ftpd\_logs" Type: "FTP Server Logs" Retrieval: Manual Download
13. "gui\_logs" Type: "HTTP Logs" Retrieval: Manual Download
14. "mail\_logs" Type: "IronPort Text Mail Logs" Retrieval: Manual Download
15. "reportd\_logs" Type: "Reporting Logs" Retrieval: Manual Download
16. "reportqueryd\_logs" Type: "Reporting Query Logs" Retrieval: Manual Download
17. "scanning" Type: "Scanning Logs" Retrieval: Manual Download
18. "sblld\_logs" Type: "Safe/Block Lists Logs" Retrieval: Manual Download
19. "sntpd\_logs" Type: "NTP logs" Retrieval: Manual Download
20. "status" Type: "Status Logs" Retrieval: Manual Download
21. "system\_logs" Type: "System Logs" Retrieval: Manual Download
22. "trackerd\_logs" Type: "Tracking Logs" Retrieval: Manual Download
23. "updater\_logs" Type: "Updater Logs" Retrieval: Manual Download

Enter the number of the log you wish to tail.

[ ]> 19

Press Ctrl-C to stop.

Mon Feb 21 12:25:10 2011 Info: PID 274: User system commit changes: Automated Update for Quarantine Delivery Host

```

Mon Feb 21 23:18:10 2011 Info: PID 19626: User admin commit changes:

Mon Feb 21 23:18:10 2011 Info: PID 274: User system commit changes: Updated filter logs
config

Mon Feb 21 23:46:06 2011 Info: PID 25696: User admin commit changes: Receiving
suspended.

^Cmail3.example.com>

```

## ホスト キーの設定

logconfig -> hostkeyconfig サブコマンドを使用して、Cisco アプライアンスから他のサーバにログをプッシュするときに、SSH で使用するホスト キーを管理します。SSH サーバには、秘密キーと公開キーの 2 つのホスト キーが必要です。秘密ホスト キーは SSH サーバにあり、リモート マシンから読み取ることはできません。公開ホスト キーは、SSH サーバと対話する必要がある任意のクライアント マシンに配信されます。



(注)

ユーザ キーを管理するには、「[セキュア シェル \(SSH\) キーの管理](#)」(P.28-27) を参照してください。

hostkeyconfig サブコマンドによって、次の機能が実行されます。

表 34-37 ホスト キーの管理 : サブコマンドのリスト

コマンド	説明
New	新しいキーを追加します。
Edit	既存のキーを変更します。
Delete	既存のキーを削除します。
Scan	ホスト キーを自動的にダウンロードします。
Print	キーを表示します。
Host	システム ホスト キーを表示します。これは、リモート システムの「known_hosts」ファイルに配置される値です。
Fingerprint	システム ホスト キーのフィンガープリントを表示します。
User	リモート マシンにログをプッシュするシステム アカウントの公開キーを表示します。これは、SCP プッシュ サブスクリプションを設定するときに表示されるキーと同じです。これは、リモート システムの「authorized_keys」ファイルに配置される値です。

次の例では、AsyncOS によってホスト キーがスキャンされ、ホスト用に追加されます。

```
mail3.example.com> logconfig
```

```
Currently configured logs:
```

```
[list of logs]
```

Choose the operation you want to perform:

- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.

[> **hostkeyconfig**

Currently installed host keys:

1. mail3.example.com ssh-dss [ key displayed ]

Choose the operation you want to perform:

- NEW - Add a new key.
- EDIT - Modify a key.
- DELETE - Remove a key.
- SCAN - Automatically download a host key.
- PRINT - Display a key.
- HOST - Display system host keys.
- FINGERPRINT - Display system host key fingerprints.
- USER - Display system user keys.

[> **scan**

Please enter the host or IP address to lookup.

[> **mail3.example.com**

Choose the ssh protocol type:

1. SSH1:rsa
2. SSH2:rsa

```
3. SSH2:dsa
4. All
[4]>

SSH2:dsa
mail3.example.com ssh-dss
[key displayed]

SSH2:rsa
mail3.example.com ssh-rsa
[key displayed]

SSH1:rsa
mail3.example.com 1024 35
[key displayed]

Add the preceding host key(s) for mail3.example.com? [Y]>

Currently installed host keys:
1. mail3.example.com ssh-dss [key displayed]
2. mail3.example.com ssh-rsa [key displayed]
3. mail3.example.com 1024 35 [key displayed]

Choose the operation you want to perform:
- NEW - Add a new key.
- EDIT - Modify a key.
- DELETE - Remove a key.
- SCAN - Automatically download a host key.
- PRINT - Display a key.
```



```
- HOST - Display system host keys.
- FINGERPRINT - Display system host key fingerprints.
- USER - Display system user keys.
[]>
```

```
Currently configured logs:
```

```
[list of configured logs]
```

```
Choose the operation you want to perform:
```

```
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
[]>
```

```
mail3.example.com> commit
```





## CHAPTER 35

# クラスタを使用した中央集中型管理

- 「クラスタを使用した中央集中型管理の概要」(P.35-1)
- 「クラスタの要件」(P.35-2)
- 「クラスタの構成」(P.35-2)
- 「クラスタの作成とクラスタへの参加」(P.35-4)
- 「クラスタの管理」(P.35-11)
- 「GUI でのクラスタの管理」(P.35-16)
- 「クラスタ通信」(P.35-19)
- 「ベスト プラクティスとよくあるご質問」(P.35-24)

## クラスタを使用した中央集中型管理の概要

Cisco の中央集中型管理機能（ライセンス キーを使って実行可能）を使用して複数のアプライアンスを同時に管理、設定することにより、管理に要する時間を短縮し、ネットワーク全体で設定の一貫性を確保することができます。複数のアプライアンスを管理するためにハードウェアを追加購入する必要はありません。中央集中型管理機能によって、ネットワーク内の信頼性、柔軟性、およびスケーラビリティが向上し、ローカル ポリシーを順守しながらグローバルな管理を行うことができます。

クラスタとは、設定情報を共有する一連のマシンのことです。クラスタの内部では、マシン（Cisco アプライアンス）がグループに分割されます。どのクラスタにも 1 つ以上のグループがあります。個々のマシンは、必ずいずれかのグループのメンバになります。管理者ユーザは、システムのさまざまな要素をクラスタ単位、グループ単位、またはマシン単位で設定できます。これにより、Cisco アプライアンスを、ネットワーク、地域、部署、または論理的な関係に基づいて分割できます。

クラスタはピアツーピアアーキテクチャで実装されるため、クラスタ内にマスター/スレーブの関係は存在しません。どのマシンにログインしても、クラスタの制御と管理を行うことができます。（ただし、一部のコンフィギュレーション コマンドは制限されます。「制限コマンド」(P.35-15) を参照してください）。

ユーザ データベースはクラスタ内のすべてのマシン間で共有されます。つまり、ユーザのセットと管理者（および対応するパスワード）はクラスタ全体で 1 つしか存在しません。クラスタに参加するすべてのマシンは 1 つの管理者パスワードを共有します。これをクラスタの管理パスワードと呼びます。

## クラスタの要件

- クラスタ内の各マシンには、DNS で解決可能なホスト名が必要です。代わりに IP アドレスを使用することもできますが、両者を混在させることはできません。

「DNS とホスト名の解決」(P.35-19) を参照してください。クラスタの通信は、通常、マシンの DNS ホスト名を使って開始されます。

- 1 つのクラスタは、全体として同じシリーズのマシンで構成されている必要があります (X シリーズと C シリーズには互換性があります)。

たとえば、Cisco X1000、C60、C600、C30、C300、および C10 アプライアンスを同じクラスタに含めることはできますが、C60 と A60 アプライアンスを同じクラスタに含めることはできません。互換性のないアプライアンスを既存のクラスタに追加しようとする、そのアプライアンスをクラスタに追加できない理由を示すエラーメッセージが表示されます。

- 1 つのクラスタは、全体として同じバージョンの AsyncOS を実行しているマシンで構成されている必要があります。

クラスタのメンバをアップグレードする方法については、「クラスタ内のマシンのアップグレード」(P.35-13) を参照してください。

- 各マシンは、SSH (通常はポート 22) と Cluster Communication Service (CCS) のいずれかを使ってクラスタに参加できます。

「クラスタ通信」(P.35-19) を参照してください。

- クラスタに参加したマシンは、SSH または CCS 経由で通信できます。使用するポートは設定可能です。SSH は通常ポート 22 上でイネーブルになっており、CCS はデフォルトでポート 2222 上でイネーブルになっていますが、どちらのサービスも別のポートに設定できます。

アプライアンスに対して開く必要がある通常のファイアウォールポートに加えて、クラスタ化されたマシンが CCS 経由で通信する場合は、各マシンが CCS ポート経由で相互に接続できる必要があります。「クラスタ通信」(P.35-19) を参照してください。

- クラスタの作成、クラスタへの参加、およびクラスタの設定を行うには、Command Line Interface (CLI; コマンドライン インターフェイス) の `clusterconfig` コマンドを使用する必要があります。

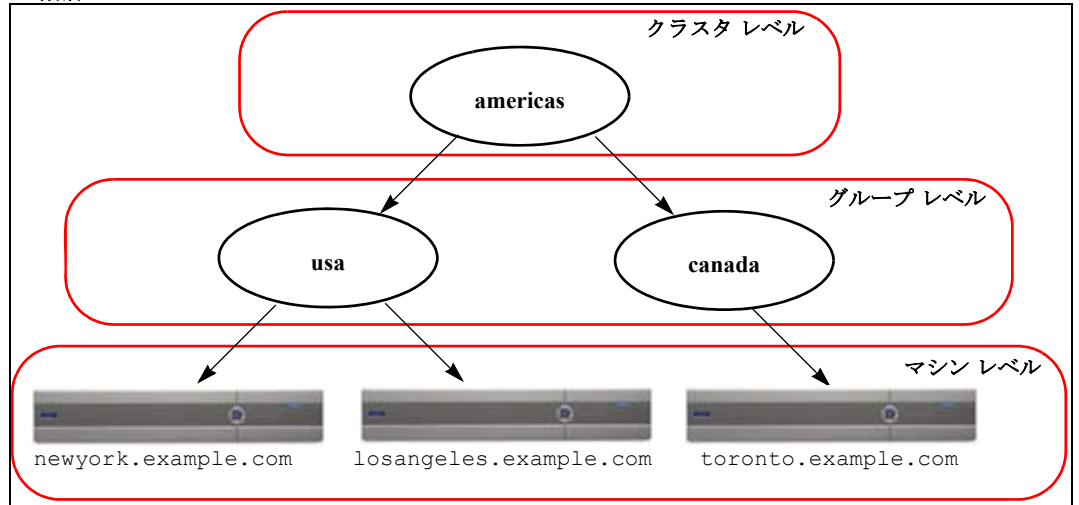
クラスタを作成した後は、クラスタ以外の設定を GUI または CLI から管理できます。

「クラスタの作成とクラスタへの参加」(P.35-4) および「GUI でのクラスタの管理」(P.35-16) を参照してください。

## クラスタの構成

クラスタでは、設定情報が 3 つのグループ (レベル) に分かれています。最上位レベルはクラスタの設定、中位レベルはグループの設定、最下位レベルはマシンごとの設定をそれぞれ表します。

図 35-1 クラスタのレベル階層



各レベルには、設定が可能なメンバが 1 つ以上存在します。これらをモードと呼びます。モードは特定のレベルに含まれる名前の付いたメンバを表します。たとえば、「usa」グループは図に示した 2 つのグループモードの 1 つです。レベルは一般的な用語ですが、モードは具体的なものを示します。モードは常に名前でも参照されます。図 35-1 に示したクラスタには 6 つのモードがあります。

設定は特定のレベルで設定されますが、それらは常に**特定のモードに対して**設定されます。すべてのモードに対する設定を 1 つのレベルで設定する必要はありません。クラスタモードは特別なケースです。クラスタは 1 つしか存在しないため、クラスタモードの設定はすべてクラスタレベルで設定されると言えます。

通常、ほとんどの設定はクラスタレベルで設定する必要があります。ただし、下位レベルで個別に設定された設定は上位レベルで設定された設定よりも優先されます。したがって、クラスタモードの設定をグループモードやマシンモードの設定で上書きできます。

たとえば、最初にクラスタモードでグッドネイバーテーブルを設定し、クラスタ内のすべてのマシンでその設定を使用するとします。次に、このテーブルをマシンモードでマシン newyork 用に設定します。この場合、クラスタ内の他のすべてのマシンは引き続きクラスタレベルで定義されたグッドネイバーテーブルを使用しますが、マシン newyork はクラスタの設定をマシンモードの個別の設定で上書きします。

特定のグループやマシン用にクラスタの設定を上書きする機能によって、非常に柔軟な設定が可能になります。ただし、多くの設定をマシンモードで個別に設定すると、クラスタの当初の目的である管理のしやすさが大きく損なわれます。

## 初期設定

ほとんどの機能については、新しいモードで設定を始めたときのデフォルトの初期設定は空です。設定が空であることとモードの設定が存在しないことは明確に区別されます。例として、1 つのグループと 1 台のマシンからなる非常に簡単なクラスタを考えます。LDAP クエリーがクラスタレベルで設定されているとします。グループレベルとマシンレベルでは何も設定されていません。

クラスタ	(LDAP クエリー : a、b、c)
グループ	
マシン	

ここで、グループに対して新しい LDAP クエリーの設定を作成したとします。その結果は次のようになります。

クラスタ	(LDAP クエリー : a、b、c)
グループ	(LDAP クエリー : なし)
マシン	

すると、クラスタ レベルの設定がグループ レベルの設定で上書きされますが、新しいグループ設定は初期状態では空です。グループ モードには、独自に設定された LDAP クエリーが実際には存在しません。このグループ内のマシンは、この「空の」LDAP クエリーをグループから継承します。

次に、このグループに次のような LDAP クエリーを追加します。

クラスタ	(LDAP クエリー : a、b、c)
グループ	(LDAP クエリー : d)
マシン	

これで、クラスタ レベルで設定されたクエリーとは別に、グループにもクエリーが設定されました。マシンはグループのクエリーを継承します。

## クラスタの作成とクラスタへの参加

クラスタの作成とクラスタへの参加は、Graphical User Interface (GUI; グラフィカル ユーザ インターフェイス) からはできません。クラスタの作成、クラスタへの参加、およびクラスタの設定を行うには、コマンドライン インターフェイス (CLI) を使用する必要があります。クラスタの作成後は、GUI と CLI のどちらからも設定を変更できます。

クラスタを作成する *前*に、必ず中央集中型管理ライセンス キーをイネーブルにしてください。



(注)

Cisco アプライアンスには、中央集中型管理機能の評価キーは付属していません。中央集中型管理機能をイネーブルにするには、30 日間の評価を要求するか、キーを購入する必要があります。キーをイネーブルにするには、CLI の `featurekey` コマンドまたは [システム管理 (System Administration)] > [ライセンス キー (Feature Keys)] ページを使用します。

## clusterconfig コマンド

マシン上でクラスタの作成やクラスタへの参加を行うには、`clusterconfig` コマンドを使用します。

- 新しいクラスタを作成すると、そのクラスタのすべての初期設定はそのクラスタを作成したマシンから継承されます。マシンがすでに「スタンドアロン」モードで設定されている場合は、クラスタを作成したときにそのスタンドアロンの設定が使用されます。
- マシンがクラスタに参加すると、そのマシンのすべてのクラスタ化可能な設定がクラスタ レベルから継承されます。つまり、そのマシン固有の設定 (IP アドレスなど) を除くすべての設定が消失し、そのマシンが参加したクラスタ、グループ、またはその両方の設定に置き換わります。マシンがすでに「スタンドアロン」モードで設定されている場合は、クラスタを作成するときそのスタンドアロンの設定が使用され、マシン レベルの設定は保持されません。

現在のマシンがまだクラスタに含まれていない場合は、`clusterconfig` コマンドを実行すると、既存のクラスタに参加するか、新しいクラスタを作成するかのオプションが表示されます。

```
newyork.example.com> clusterconfig
```

```
Do you want to join or create a cluster?
```

1. No, configure as standalone.
2. Create a new cluster.
3. Join an existing cluster over SSH.
4. Join an existing cluster over CCS.

```
[1]> 2
```

```
Enter the name of the new cluster.
```

```
[> americas
```

```
New cluster committed: Wed Jun 22 10:02:04 2005 PDT
```

```
Creating a cluster takes effect immediately, there is no need to commit.
```

```
Cluster americas
```

```
Choose the operation you want to perform:
```

- ADDGROUP - Add a cluster group.
- SETGROUP - Set the group that machines are a member of.
- RENAMEGROUP - Rename a cluster group.
- DELETEDGROUP - Remove a cluster group.
- REMOVEMACHINE - Remove a machine from the cluster.
- SETNAME - Set the cluster name.
- LIST - List the machines in the cluster.
- LISTDETAIL - List the machines in the cluster with detail.
- DISCONNECT - Temporarily detach machines from the cluster.

```
- RECONNECT - Restore connections with machines that were previously detached.
- PREPJOIN - Prepare the addition of a new machine over CCS.

[]>
```

この時点で、新しいクラスタにマシンを追加できます。これらのマシンは、SSH または CCS を使用して通信できます。

## 既存のクラスタへの参加

既存のクラスタに参加するには、クラスタに追加するホスト上で `clusterconfig` コマンドを実行します。SSH と CCS のどちらを使用してクラスタに参加するかを選択できます。

既存のクラスタにホストを参加させるには、次の要件を満たす必要があります。

- クラスタ内のマシンの SSH ホスト キーを検証できること
- クラスタ内のマシンの IP アドレスを知っており、そのマシンに (SSH や CCS 経由で) 接続できること
- クラスタに属するマシン上の管理ユーザの管理者パスワードを知っていること



(注)

クラスタにマシンを追加する前に、追加しようとしているすべてのマシンに中央集中型管理ライセンスキーをインストールする必要があります。あらかじめ中央集中型管理のライセンス キーがシステムにインストールされており、クラスタがすでに存在する場合は、CLI の `systemsetup` コマンドによるシステム設定ウィザードを使って既存のクラスタに参加することもできます。管理者パスワードの変更、アプリケーションのホスト名の設定、およびネットワーク インターフェイスと IP アドレスの設定の後、クラスタの作成とクラスタへの参加のいずれかを選択するプロンプトが表示されます。

## SSH を使った既存クラスタへの参加

次の表に、SSH オプションを使ってマシン「`losangeles.example.com`」をクラスタに追加する例を示します。

```
losangeles.example.com> clusterconfig
```

```
Do you want to join or create a cluster?
```

1. No, configure as standalone.
2. Create a new cluster.
3. Join an existing cluster over SSH.
4. Join an existing cluster over CCS.

```
[1]> 3
```



While joining a cluster, you will need to validate the SSH host key of the remote machine to which you are joining. To get the public host key

```
fingerprint of the remote host, connect to the cluster and run: logconfig ->
hostkeyconfig -> fingerprint.
```

WARNING: All non-network settings will be lost. System will inherit the values set at the group or cluster mode for the non-network settings. Ensure that the cluster settings are compatible with your network settings (e.g. dnsconfig settings)

Do you want to enable the Cluster Communication Service on

```
losangeles.example.com? [N]> n
```

Enter the IP address of a machine in the cluster.

```
[> IP address is entered
```

Enter the remote port to connect to. The must be the normal admin ssh port, not the CCS port.

```
[22]> 22
```

Enter the admin password for the cluster.

*The administrator password for the clustered machine is entered*

Please verify the SSH host key for IP address:

```
Public host key fingerprint: xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx
```

```
Is this a valid key for this host? [Y]> y
```

Joining cluster group Main\_Group.

Joining a cluster takes effect immediately, there is no need to commit.

Cluster americas

Choose the operation you want to perform:

```

- ADDGROUP - Add a cluster group.

- SETGROUP - Set the group that machines are a member of.

- RENAMEGROUP - Rename a cluster group.

- DELETEDGROUP - Remove a cluster group.

- REMOVEMACHINE - Remove a machine from the cluster.

- SETNAME - Set the cluster name.

- LIST - List the machines in the cluster.

- LISTDETAIL - List the machines in the cluster with detail.

- DISCONNECT - Temporarily detach machines from the cluster.

- RECONNECT - Restore connections with machines that were previously detached.

- PREPJOIN - Prepare the addition of a new machine over CCS.

[]>

(Cluster americas)>

```

## CCS を使った既存クラスタへの参加

SSH を使用できない場合は、代わりに CCS を使用します。CCS の唯一の利点は、そのポートではクラスタ通信しか行われない（ユーザ ログインや SCP など行われない）ことです。CCS を使って既存のクラスタにマシンを追加するには、`clusterconfig` の `prepjoin` サブコマンドを使ってクラスタに追加するマシンの準備を行います。次の例では、マシン「newyork」上で `prepjoin` コマンドを実行して、クラスタに追加するマシン「losangeles」の準備を行っています。

`prepjoin` コマンドを実行してから、クラスタに追加するホストの CLI で「`clusterconfig prepjoin print`」と入力し、現在クラスタに含まれているホストのコマンドラインにキーをコピーすることにより、クラスタに追加するホストのユーザ キーを取得します。

```

Choose the operation you want to perform:

- ADDGROUP - Add a cluster group.

- SETGROUP - Set the group that machines are a member of.

- RENAMEGROUP - Rename a cluster group.

- DELETEDGROUP - Remove a cluster group.

- REMOVEMACHINE - Remove a machine from the cluster.

- SETNAME - Set the cluster name.

- LIST - List the machines in the cluster.

- LISTDETAIL - List the machines in the cluster with detail.

```

- DISCONNECT - Temporarily detach machines from the cluster.
- RECONNECT - Restore connections with machines that were previously detached.
- PREPJOIN - Prepare the addition of a new machine over CCS.

```
[> prepjoin
```

```
Prepare Cluster Join Over CCS
```

```
No host entries waiting to be added to the cluster.
```

```
Choose the operation you want to perform:
```

- NEW - Add a new host that will join the cluster.

```
[> new
```

```
Enter the hostname of the system you want to add.
```

```
[> losangeles.example.com
```

```
Enter the serial number of the host mail3.example.com.
```

```
[> unique serial number is added
```

```
Enter the user key of the host losangeles.example.com. This can be obtained by typing
"clusterconfig prepjoin print" in the CLI on mail3.example.com. Press enter on a blank
line to finish.
```

```
unique user key from output of prepjoin print is pasted
```

```
Host losangeles.example.com added.
```

```
Prepare Cluster Join Over CCS
```

```
1. losangeles.example.com (serial-number)
```

```
Choose the operation you want to perform:
```

```
- NEW - Add a new host that will join the cluster.
- DELETE - Remove a host from the pending join list.

[]>
```

```
(Cluster americas)> commit
```

マシンがクラスタに追加された後は、`clusterconfig` コマンドを使ってクラスタのさまざまな設定が可能です。

```
(Cluster Americas)> clusterconfig
```

```
Cluster americas
```

```
Choose the operation you want to perform:
```

```
- ADDGROUP - Add a cluster group.
- SETGROUP - Set the group that machines are a member of.
- RENAMEGROUP - Rename a cluster group.
- DELETEGROUP - Remove a cluster group.
- REMOVEMACHINE - Remove a machine from the cluster.
- SETNAME - Set the cluster name.
- LIST - List the machines in the cluster.
- LISTDETAIL - List the machines in the cluster with detail.
- DISCONNECT - Temporarily detach machines from the cluster.
- RECONNECT - Restore connections with machines that were previously detached.
- PREPJOIN - Prepare the addition of a new machine over CCS.

[]>
```

## グループの追加

すべてのクラスタには 1 つ以上のグループが含まれている必要があります。新しいクラスタを作成すると、「Main\_Group」という名前のデフォルトのグループが自動的に作成されます。しかし、クラスタ内に追加のグループを作成することもできます。次の例は、既存のクラスタ内に追加のグループを作成し、そのグループにマシンを割り当てる方法を示しています。

## 手順

- ステップ 1** clusterconfig コマンドを実行します。
- ステップ 2** addgroup サブコマンドを選択し、新しいグループの名前を入力します。
- ステップ 3** setgroup サブコマンドを使用して、新しいグループに割り当てるマシンを選択します。

## クラスタの管理

### CLI でのクラスタの管理

クラスタに含まれるマシンでは、CLI を異なるモードに切り替えることができます。モードはあるレベルに含まれる特定の（名前の付いた）メンバを表していることを思い出してください。

CLI のモードに応じて、設定が変更される正確な場所が決まります。デフォルトは、ユーザがログインしたマシン（ログインホスト）を示す「マシン」モードです。

別のモードに切り替えるには、clustermode コマンドを使用します。

**表 35-1 クラスタの管理**

コマンド例	説明
clustermode	クラスタモードへの切り替えを確認するプロンプトが表示されます。
clustermode group northamerica	グループ「northamerica」用のグループモードに切り替わります。
clustermode machine losangeles.example.com	マシン「losangeles」用のマシンモードに切り替わります。

CLI プロンプトの表示が現在のモードに変わります。

```
(Cluster Americas)>
```

または

```
(Machine losangeles.example.com)>
```

マシンモードでは、プロンプトにマシンの完全修飾ドメイン名が表示されます。

## 設定のコピーと移動

すべての非制限コマンド（「制限コマンド」(P.35-15) を参照）に、新しい操作として CLUSTERSHOW と CLUSTERSET が追加されました。CLUSTERSHOW は、コマンド設定のモードを表示するときに使用します（「新たに追加された操作」(P.35-15) を参照）。CLUSTERSET 操作は、（現在のコマンドで設定できる）現在の設定をモード間またはレベル間で（たとえば、あるマシンからあるグループへ）移動またはコピーするときに使用します。

*copy* を使用すると、現在のモードの設定が保持されます。*move* を使用すると、現在のモードの設定がリセット（クリア）されます。つまり、移動した後は、現在のモードに設定が設定されなくなります。

たとえば、(*destconfig* コマンドで) グループ「northamerica」にグッド ネイバー テーブルを設定し、クラスタ全体にこの設定を適用する場合は、*destconfig* コマンド内で *clusterset* 操作を使って現在の設定をクラスタ モードにコピー（または移動）できます。（「新しい設定の実験」(P.35-12) を参照）。



### 警告

設定を移動またはコピーするときは、依存関係に矛盾が生じないように注意してください。たとえば、免責事項のスタンプが設定されたリスナーを別のマシンに移動またはコピーしても、その新しいマシンに同じ免責事項が設定されていない場合、新しいマシンでは免責事項のスタンプがイネーブルになりません。

## 新しい設定の実験

クラスタの最も効果的な使用方法の 1 つは、新しい設定を実験することです。まず、分離された環境で、マシン モードでの変更を行います。次に、設定に問題がなければ、設定変更を上位のクラスタ モードに移動し、すべてのマシンに適用します。

次の例は、あるマシンでリスナーの設定を変更し、準備ができればその設定をクラスタの残りのマシンにパブリッシュする手順を示しています。通常、リスナーはクラスタ レベルで設定されるため、この例では最初に設定をあるマシンのマシン モードに格下げしてから、設定の変更を行い、テストしています。このような実験的な変更は、クラスタ内の他のマシンで同じ変更を行う前に、1 つのマシン上でテストする必要があります。

### 手順

- ステップ 1** `clustermode cluster` コマンドを使ってクラスタ モードに変更します。  
`clustermode` コマンドは、モードをクラスタ、グループ、およびマシン レベルに変更するときに使用する CLI コマンドです。
- ステップ 2** `listenerconfig` を実行して、クラスタに設定されたリスナーの設定を表示します。
- ステップ 3** 実験するマシンを選び、`clusterset` コマンドを使って設定をクラスタから下位のマシン モードにコピーします。
- ステップ 4** 次のように `clustermode` コマンドを使って実験マシンのマシン モードに移行します。  
`clustermode machine newyork.example.com`
- ステップ 5** 実験マシンのマシン モードで `listenerconfig` コマンドを実行し、実験マシンに固有の変更を行います。
- ステップ 6** 変更を確定します。
- ステップ 7** 実験マシン上で設定変更の実験を続行し、必ず変更を確定します。

- ステップ 8** 新しい設定を他のすべてのマシンに適用する準備ができたなら、`clusterset` コマンドを使って設定を上位のクラスタ モードに移動します。
- ステップ 9** 変更を確定します。

## クラスタからの脱退（削除）

マシンをクラスタから永続的に削除するには、`clusterconfig` の `REMOVEMACHINE` 操作を使用します。マシンをクラスタから永続的に削除すると、その設定は「平板化」され、そのマシンはクラスタに含まれていたときと同じように動作します。たとえば、クラスタ モードのグローバル配信停止テーブルしかない場合にマシンをクラスタから削除すると、そのグローバル配信停止テーブルのデータがマシンのローカル設定にコピーされます。

## クラスタ内のマシンのアップグレード

クラスタには、異なるバージョンの AsyncOS を実行しているマシンを接続できません。

AsyncOS のアップグレードをインストールする前に、`clusterconfig` コマンドを使ってクラスタ内の各マシンを切断する必要があります。すべてのマシンをアップグレードしたら、`clusterconfig` コマンドを使ってクラスタを再接続します。マシンを同じバージョンにアップグレードする間は、2つのクラスタを別個に稼働させることができます。また、GUI の [アップグレード (Upgrades)] ページでクラスタ化されたマシンをアップグレードすることもできます。

バックグラウンドでアップグレードをダウンロードできるため、アップグレードをインストールする準備が整うまで、クラスタ内のマシンを切断する必要はありません。



**(注)** クラスタから個々のマシンを切断する前にアップグレード コマンドを使用すると、AsyncOS によってクラスタ内のすべてのマシンが切断されます。マシンをアップグレードする前に、各マシンをクラスタから切断することを推奨します。各マシンを切断してアップグレードしている間、他のマシンは引き続きクラスタとして動作します。

### 手順

- ステップ 1** クラスタ内のマシン上で、`clusterconfig` の `disconnect` 操作を使用します。たとえば、マシン `losangeles.example.com` を切断するには、`clusterconfig disconnect losangeles.example.com` と入力します。commit は必要ありません。
- ステップ 2** 必要に応じて、`suspendlistener` コマンドを使ってアップグレード処理中の新しい接続やメッセージの受信を停止します。
- ステップ 3** `upgrade` コマンドを実行して、AsyncOS を新しいバージョンにアップグレードします。
- (注)** クラスタ内のマシンをすべて切断するように求める警告または確認メッセージは無視してください。マシンがすでに切断されているため、この時点で AsyncOS によってクラスタ内の他のマシンが切断されることはありません。
- ステップ 4** マシンの AsyncOS のバージョンを選択します。アップグレードが完了すると、マシンが再起動します。
- ステップ 5** アップグレードされたマシン上で `resume` コマンドを使って新しいメッセージの受信を開始します。
- ステップ 6** クラスタ内のマシンごとにステップ 1 ~ 5 を繰り返します。



(注) クラスタからマシンを切断すると、そのマシンを使って他のマシンの設定を変更できません。クラスタの設定を変更することはできますが、設定の同期が取れなくなるため、マシンが切断されている間は設定を変更しないでください。

**ステップ 7** すべてのマシンをアップグレードした後で、アップグレードされたマシンごとに `clusterconfig` の `reconnect` 操作を実行してマシンを再接続します。たとえば、マシン `losangeles.example.com` を再接続するには、`clusterconfig reconnect losangeles.example.com` と入力します。クラスタに接続できるのは、同じバージョンの AsyncOS を実行しているマシンだけです。

## 設定ファイル コマンド

設定情報は、クラスタ内の個々のシステムに保存されます。([システム管理 (System Administration)] > [設定ファイル (Configuration File)] ページまたは `exportconfig` コマンドを使って) マシンモードで設定ファイルをエクスポートすると、現在設定中のマシンのローカルディスクにファイルがエクスポートされます。クラスタモードまたはグループモードでは、現在ログインしているマシンにファイルが保存されます。ファイルのエクスポート先となるマシンは、ユーザに通知されます。



(注) [システム管理 (System Administration)] > [設定ファイル (Configuration File)] ページまたは `loadconfig` コマンドを使ってクラスタ全体 (またはクラスタ化されたマシン) の設定をあらかじめ保存しておき、後でその設定を一連の (同じまたは異なる) マシンに復元する方法はサポートされていません。

## 設定のリセット

クラスタに含まれるマシン上で (ローカル マシン モード限定で)、([システム管理 (System Administration)] > [設定ファイル (Configuration File)] ページまたは `resetconfig` コマンドを使って) 設定をリセットすると、そのマシンは工場出荷時のデフォルト設定に戻ります。そのマシンがそれまでクラスタに含まれていた場合は、設定をリセットすることで、その設定がクラスタからも自動的に削除されます。

## CLI コマンドのサポート

### すべてのコマンドがクラスタに対応

AsyncOS のすべての CLI コマンドがクラスタ対応になりました。一部のコマンドは、クラスタモードで実行したときの動作がやや異なります。たとえば、次のコマンドをクラスタに含まれるマシン上で実行すると、コマンドの動作が変更されます。

### commit および clearchanges コマンド

#### commit

`commit` コマンドは、現在のモードに関係なく、すべての変更をクラスタの 3 つのレベルのすべてで確定します。



## commitdetail

commitdetail コマンドは、クラスタ内のすべてのマシンに反映された設定変更の詳細を表示します。

## clearchanges

clearchanges (clear) コマンドは、現在のモードに関係なく、すべての変更をクラスタの 3 つのレベルのすべてでクリアします。

## 新たに追加された操作

### CLUSTERSHOW

各コマンドに、コマンド設定時のモードを表示する CLUSTERSHOW 操作が追加されました。

下位レベルの既存の設定で上書きされる操作を実行する CLI コマンドを入力すると、通知メッセージが表示されます。たとえば、クラスタ モードでコマンドを入力すると、次のような通知メッセージが表示されることがあります。

Note: Changes to these settings will not affect the following groups and machines because they are overriding the cluster-wide settings:

East\_Coast, West\_Coast

facilities\_A, facilities\_B, receiving\_A

グループ モードの設定を編集した場合も、同じようなメッセージが表示されます。

## 制限コマンド

ほとんどの CLI コマンドとそれに対応する GUI ページは、任意のモード（クラスタ、グループ、マシン）で実行できます。しかし、一部のコマンドとページは 1 つのモードだけに制限されています。

システム インターフェイスには（GUI と CLI のどちらにも）、コマンドが制限されること、およびどのように制限されるかが必ず明示されます。コマンドを設定するための適切なモードに簡単に切り替えることができます。

- GUI では、[モードを変更 (Change Mode)] メニューまたは [この機能の設定は現在、次で定義されています: (Settings for this features are currently defined at:)] リンクを使ってモードを切り替えます。
- CLI では、clustermode コマンドを使ってモードを切り替えます。

**表 35-2 クラスタ モードに制限されるコマンド**

clusterconfig	sshconfig
clustercheck	userconfig
passwd	

上記のコマンドをグループ モードまたはマシン モードで実行しようとする、警告メッセージが表示され、適切なモードに切り替えることができます。



(注)

passwd コマンドは、ゲストユーザが使用できるようにするための特例です。ゲストユーザがクラスタ内のマシン上で passwd コマンドを実行すると、警告メッセージは表示されず、ユーザのモードを変更せずにクラスタレベルのデータに対して操作が行われます。他のすべてのユーザに対しては、上記の（他の制限されるコンフィギュレーションコマンドと同じ）動作が行われます。

次のコマンドは、マシンモードに制限されます。

antispamstatus	etherconfig	resume	suspenddel
antispamupdate	featurekey	resumedel	suspendlistener
antivirusstatus	hostrate	resumelister	techsupport
antivirusupdate	hoststatus	rollovernow	tophosts
bouncerecipients	interfaceconfig	routeconfig	topin
deleterecipients	ldapflush	sbstatus	trace
delivernow	ldaptest	setgateway	version
diagnostic	nslookup	sethostname	vofflush
dnsflush	quarantineconfig	settime	vofstatus
dnslistflush	rate	shutdown	workqueue
dnslisttest	reboot	status	
dnsstatus	resetcounters	suspend	

上記のコマンドをクラスタモードまたはグループモードで実行しようとする、警告メッセージが表示され、適切なモードに切り替えることができます。

次のコマンドは、さらにログインホスト（ユーザがログインしているマシン）に制限されます。これらのコマンドを使用するには、ローカルファイルシステムにアクセスする必要があります。

表 35-3 ログインホストモードに制限されるコマンド

last	resetconfig	tail	upgrade
ping	supportrequest	telnet	who

## GUI でのクラスタの管理

GUI では、クラスタの作成、クラスタへの参加、およびクラスタ固有の設定の管理（clusterconfig コマンドと同等の操作）を行うことはできませんが、クラスタ内のマシンの参照、設定の作成や削除、およびクラスタ間、グループ間、マシン間での設定のコピーや移動（つまり、clustermode および clusterset と同等の操作）を行うことができます。

GUI に最初にログインすると、[受信メールの概要 (Incoming Mail Overview)] ページが表示されます。現在のマシンがクラスタのメンバとして設定されている場合は、中央集中型管理機能が GUI でイネーブルになっていることも通知されます。

[受信メールの概要 (Incoming Mail Overview)] ページは、表示しているメールフローモニタリングのデータがローカルマシンに格納されるため、ログインホストに制限されるコマンドの例です。別のマシンの [受信メールの概要 (Incoming Mail Overview)] レポートを表示するには、そのマシンの GUI にログインする必要があります。

アプライアンス上でクラスタリングがイネーブルになっている場合は、ブラウザのアドレス フィールドの URL に注意してください。この URL には、必要に応じて machine、group、または cluster という単語が含まれています。たとえば、最初にログインしたときの [受信メールの概要 (Incoming Mail Overview)] ページの URL は次のように表示されます。

https:// ホスト名/**machine**/ 連番/monitor/incoming\_mail\_overview



(注) [モニタ (Monitor)] メニューの [受信メールの概要 (Incoming Mail Overview)] ページと [受信メールの詳細 (Incoming Mail Details)] ページは、ログインマシンに制限されます。

[メール ポリシー (Mail Policies)]、[セキュリティ サービス (Security Services)]、[ネットワーク (Network)]、[システム管理 (System Administration)] の各タブには、ローカルマシンに制限されないページが表示されます。[メール ポリシー (Mail Policies)] タブをクリックすると、GUI 内の中央集中型管理情報が変更されます。

図 35-2 GUI の中央集中型管理機能：設定が規定されていない場合

モードインジケータ

Mode — Machine: example.com Change Mode...

Centralized Management Options

Inheriting settings from Cluster: americas

> Override Settings

Settings for this feature are currently defined at:

- Cluster: americas

Find Policies

Email Address:  Recipient  Sender  Find Policies

Policies

Add Policy...

Order	Policy Name	Anti-Spam	Anti-Virus	Virus Outbreak Filters	Content Filters	Delete
	Default Policy	IronPort Positive: Deliver Suspected: Disabled	Repaired: Deliver Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	Enabled	Disabled	

Key: Default Custom Disabled

中央集中型管理ボックス

継承された設定プレビュー表示

図 35-2 では、このマシンの現在の機能に関する設定がクラスタモードから継承されています。継承された設定は薄いグレーで表示 (プレビュー) されます。これらの設定を保持することも、クラスタレベルの設定をこのマシン用に上書きして変更することも可能です。



(注) 継承された設定 (プレビュー表示) には、常にクラスタから継承した設定が表示されます。グループレベルとクラスタレベルの間で依存するサービスをイネーブルまたはディセーブルにするときは注意してください。詳細については、「設定のコピーと移動」(P.35-12) を参照してください。

[設定を上書き (Override Settings)] リンクをクリックすると、この機能に対応する新しいページが表示されます。このページでは、マシンモードの新しい設定を作成できます。デフォルト設定をそのまま使用することもできますが、別のモードですでに設定している場合は、それらの設定をこのマシンにコピーすることもできます。

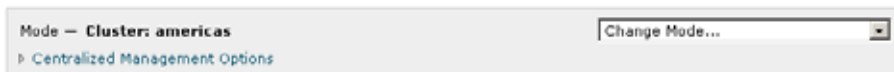
図 35-3 GUI の中央集中型管理機能：新しい設定の作成



または、図 35-2 に示すように、この設定がすでに規定されているモードに移動することもできます。これらのモードは、中央集中型管理ボックスの下部にある [この機能の設定は現在、次で定義されています：(Settings for this feature are currently defined at:)] に表示されます。ここでは、設定が実際に規定されているモードだけが表示されます。別のモードで規定された（別のモードから継承された）設定のページを表示すると、ページ上にそれらの設定が表示されます。

表示されたいずれかのモード（たとえば、図 35-2 に示す [クラスタ：南/北/中央アメリカ（Cluster: Americas）] リンク）をクリックすると、そのモードの設定を表示して管理できる新しいページが表示されます。

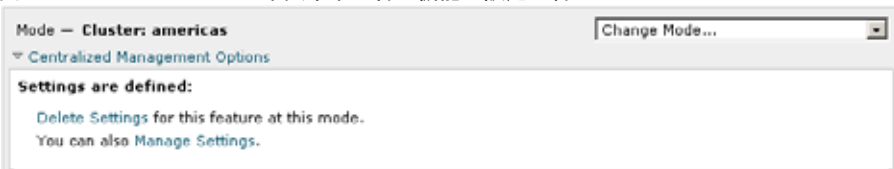
図 35-4 GUI の中央集中型管理機能：定義された設定



特定のモードで設定を規定すると、中央集中型管理ボックスがすべてのページに最小化された状態で表示されます。[集約管理オプション（Centralized Management Options）] リンクをクリックすると、ボックスが展開され、現在のモードで現在のページに関して設定できるオプションのリストが表示されます。[設定を管理（Manage Settings）] ボタンをクリックすると、現在の設定を別のモードにコピーまたは移動したり、設定を完全に削除したりできます。

たとえば、図 35-5 では、[集約管理オプション（Centralized Management Options）] リンクがクリックされ、設定可能なオプションが表示されています。

図 35-5 GUI の中央集中型管理機能：設定の管理



ボックスの右側には [モードを変更（Change Mode）] メニューが表示されます。このメニューには現在のモードが表示され、このメニューを使っていつでも他のモード（クラスタ、グループ、またはマシン）に移動できます。

図 35-6 [モードを変更（Change Mode）] メニュー  
Incoming Mail Policies

別のモードを表すページに移動すると、中央集中型管理ボックスの左側にある「モード —」というテキストが一時的に黄色で点滅し、モードが変更されたことを知らせます。

特定のタブに含まれる一部のページは、マシン モードに制限されています。ただし、(現在のログインホストに制限される) [受信メールの概要 (Incoming Mail Overview)] ページとは異なり、これらのページはクラスタ内のどのマシンでも使用できます。

図 35-7 中央集中型管理機能：マシンに制限される機能



[モードを変更 (Change Mode)] メニューから管理するマシンを選択します。テキストが一時的に点滅し、モードが変更されたことを知らせます。

## クラスタ通信

クラスタ内のマシンは、メッシュ ネットワークを使って相互に通信します。デフォルトでは、すべてのマシンが他のすべてのマシンに接続します。1 つのリンクが切断されても、他のマシンが更新を受信できなくなることはありません。

デフォルトでは、クラスタ内のすべての通信が SSH を使って保護されます。各マシンは、ルート テーブルのコピーをメモリ内に保持し、リンクの切断と確立に応じてメモリ内のテーブルを変更します。また、クラスタに含まれる他のすべてのマシンに対して定期的に (1 分間隔で) 「ping」を実行します。これにより、リンクの最新状態を確認し、ルータや NAT がタイムアウトした場合でも接続を維持します。



(注)

クラスタ内の 2 台のアプライアンス間の接続は、1 台のアプライアンスが許可される最大 SSH 接続数を超えて開こうとする場合、ドロップされる可能性があります。アプライアンスは数秒以内に自動的にクラスタを再接続するため、手動の設定は必要ありません。

## DNS とホスト名の解決

マシンをクラスタに接続するには、DNS が必要です。クラスタの通信は、通常、(マシン上のインターフェイスのホスト名ではなく) マシンの DNS ホスト名を使って開始されます。ホスト名を解決できないマシンは、形式的にはクラスタに含まれていても、実際にはクラスタ内の他のマシンと通信できません。

ホスト名がアプライアンス上の SSH または CCS をイネーブルにした正しい IP インターフェイスを指すように、DNS を設定する必要があります。これは非常に重要です。DNS が SSH または CCS をイネーブルにしていない別の IP アドレスを参照すると、ホストが見つかりません。中央集中型管理では、インターフェイスごとのホスト名ではなく、sethostname コマンドで設定した「メイン ホスト名」が使用されます。

IP アドレスを使ってクラスタ内の他のマシンに接続する場合は、接続先のマシンが接続元の IP アドレスの逆ルックアップを実行できる必要があります。DNS 内にその IP アドレスがないために逆ルックアップがタイムアウトすると、そのマシンはクラスタに接続できません。

## クラスタリング、完全修飾ドメイン名、およびアップグレード

AsyncOS をアップグレードすると、DNS の変更によって接続が失われることがあります。(クラスタ内のマシン上のインターフェイスのホスト名ではなく) クラスタ内のマシンの完全修飾ドメイン名を変更する必要がある場合は、AsyncOS をアップグレードする前に、sethostname を使ってホスト名の設定を変更し、そのマシンの DNS レコードを更新する必要があることに注意してください。

## クラスタ通信のセキュリティ

Cluster Communication Security (CCS) は、標準の SSH サービスに似たセキュア シェル サービスです。シスコが CCS を実装したのは、クラスタ通信に標準の SSH を使用することに対する懸念に応えるためです。マシン間の SSH 通信では、同じポートで (管理者などの) 通常のログインを開きます。多くの管理者は、クラスタ化されたマシン上で通常のログインを開くことを好みません。

ヒント: CCS はデフォルトですが、クラスタ化されたマシン間のポート 22 の通信がファイアウォールによってブロックされない場合は、CCS をイネーブルにしないでください。クラスタリングでは、すべてのマシン間でフル メッシュの SSH トンネル (ポート 22 上) が使用されます。いずれかのマシンですでに CCS をイネーブルにした場合は、クラスタからすべてのマシンを削除し、最初からやり直してください。クラスタ内の最後のマシンを削除すると、クラスタが削除されます。

CCS は、管理者が CLI へのログインではなく、クラスタ通信を開始できるように強化されています。デフォルトでは、このサービスはディセーブルです。アプライアンスの中央集中型管理機能をイネーブルにすると、interfaceconfig コマンドで他のサービスをイネーブルにするためのプロンプトが表示されたときに、CCS をイネーブルにするかどうかの選択を求められます。次の例を参考にしてください。

```
Do you want to enable SSH on this interface? [Y]>
```

```
Which port do you want to use for SSH?
```

```
[22]>
```

```
Do you want to enable Cluster Communication Service on this interface?
```

```
[N]> y
```

```
Which port do you want to use for Cluster Communication Service?
```

```
[2222]>
```

CCS のデフォルトのポート番号は 2222 です。必要な場合は、これを別の開いている未使用のポート番号に変更できます。マシンの参加が完了し、参加したマシンにクラスタのすべての設定データが適用されると、次の質問が表示されます。

```
Do you want to enable Cluster Communication Service on this interface? [N]> y
```

```
Which port do you want to use for Cluster Communication Service?
```

```
[2222]>
```

## クラスタの整合性

中央集中型管理をイネーブルにすると、「クラスタ対応」のマシンはクラスタ内の他のマシンへのネットワーク接続を継続的に確認します。この確認は、クラスタ内の他のマシンに対する定期的な「ping」によって行われます。

特定のマシンとの通信の試行がすべて失敗すると、通信を試行したマシンはリモートホストが切断されたことを示すメッセージをログに記録します。システムはリモートホストがダウンしたことを示すアラートを管理者に送信します。

マシンがダウンしても、確認用の ping は引き続き送信されます。マシンがクラスタのネットワークに再び参加すると、それまでオフラインだったマシンが更新をダウンロードできるように、同期コマンドが実行されます。この同期コマンドは、一方のマシンに含まれる変更がもう一方のマシンに含まれるかどうかを判定します。含まれない場合は、それまでダウンしていたマシンが更新をサイレントでダウンロードします。

## 切断/再接続

マシンは、クラスタから切断できます。ときには、たとえばマシンをアップグレードするために、マシンを意図的に切断することがあります。切断は、たとえば停電やソフトウェアまたはハードウェアのエラーのために突発的に起きることもあります。1台のアプライアンスがセッションで許可されている SSH 接続の最大数を超過して開こうとする場合も、切断が起きることがあります。クラスタから切断されたマシンに直接アクセスしてマシンを設定することはできますが、切断されたマシンを再接続するまでは、クラスタ内の他のマシンに変更が反映されません。

マシンをクラスタに再接続すると、そのマシンはただちにすべてのマシンに再接続しようとします。

理論的には、クラスタから2台のマシンを切断した場合、同じような変更が各マシンのローカルデータベースに同時に確定される可能性があります。これらのマシンをクラスタに再接続すると、これらの変更の同期が試行されます。競合がある場合は、最新の変更が記録されます（他の変更はすべて破棄されます）。

アプライアンスは、変更されるすべての変数を確定時にチェックします。確定データには、バージョン情報、連番 ID、その他の比較可能な情報が含まれます。変更しようとしているデータが以前の変更と競合することがわかった場合は、変更を破棄するオプションが表示されます。たとえば、次のようなメッセージが表示されます。

```
(Machine mail3.example.com)> clustercheck
```

```
This command is restricted to "cluster" mode. Would you like to switch to "cluster" mode? [Y]> y
```

```
Checking Listeners (including HAT, RAT, bounce profiles)...
```

```
Inconsistency found!
```

Listeners (including HAT, RAT, bounce profiles) at Cluster enterprise:

```
mail3.example.com was updated Mon Sep 12 10:59:17 2005 PDT by 'admin' on
mail3.example.com
```

```
test.example.com was updated Mon Sep 12 10:59:17 2005 PDT by 'admin' on
mail3.example.com
```

How do you want to resolve this inconsistency?

1. Force entire cluster to use test.example.com version.
2. Force entire cluster to use mail3.example.com version.
3. Ignore.

[1]>

変更を破棄しなかった場合、変更は（確定されませんが）保持されます。変更を現在の設定に照らして確認し、その後の処理方法を決めることができます。

また、いつでも `clustercheck` コマンドを使ってクラスタが正常に動作していることを確認できます。

```
losangeles> clustercheck
```

```
Do you want to check the config consistency across all machines in the cluster? [Y]> y
```

```
Checking losangeles...
```

```
Checking newyork...
```

```
No inconsistencies found.
```

## 互いに依存する設定

中央集中型管理環境では、互いに依存する設定が異なるモードで設定されることがあります。設定モデルの高い柔軟性によって複数のモードで設定できるため、個々のマシンでどの設定が使用されるかは継承の法則に基づいて決まります。しかし、一部の設定は他の設定に依存しており、依存する設定の適用範囲は同じモードの設定に制限されません。したがって、あるレベルで特定のマシン用に設定された設定を参照する設定を別のレベルで設定することも可能です。

互いに依存する設定の最も一般的な例は、ページ上の別のクラスタ セクションからデータを取得する選択フィールドに関するものです。たとえば、次の機能をそれぞれ異なるモードで設定できます。

- LDAP クエリーの使用
- デictionaryまたはテキスト リソースの使用
- バウンス プロファイルまたは SMTP 認証プロファイルの使用。



中央集中型管理には、制限コマンドと非制限コマンドがあります。「[制限コマンド](#)」(P.35-15)を参照。非制限コマンドは、通常、クラスタ全体で共有できるコンフィギュレーション コマンドです。

listenerconfig コマンドは、クラスタ内のすべてのマシンに設定できるコマンドの例です。非制限コマンドは、クラスタ内のすべてのマシンに反映できるため、マシンごとにデータを変更する必要がないコマンドです。

一方、制限コマンドは特定のモードだけに適用されるコマンドです。たとえば、ユーザを特定のマシン用に設定することはできません。ユーザはクラスタ全体に 1 セットしか設定できません（そうしないと、同じログイン名でリモートマシンにログインできなくなります）。同じように、メールフローモニタのデータ、システム概要のカウンタ、およびログファイルは、マシン単位でしか保持されないため、これらのコマンドやページはマシンだけに制限する必要があります。

定期レポートはクラスタ全体で同じに設定できますが、レポートの表示はマシン別に行われます。したがって、GUI の [定期レポート (Scheduled Reports)] ページは 1 つでも、設定はクラスタモードで行い、レポートの表示はマシンモードで行う必要があります。

[システム時刻 (System Time)] のページには、settz、ntpconfig、settime の各コマンドが含まれ、制限コマンドと非制限コマンドが混在しています。この場合、settime は（時間の設定がマシンに固有のものであるため）マシンモードだけに制限する必要がありますが、settz と ntpconfig はクラスタモードまたはグループモードで設定できます。

図 35-8 互いに依存する設定の例  
Edit Listener

この図では、リスナー「IncomingMail」がマシンレベルでのみ設定された「disclaimer」という名前のフッターを参照しています。使用可能なフッター リソースのドロップダウンリストには、クラスタでは使用できるのにマシン「buttercup.run」では使用できないフッターが表示されています。このジレンマを解消するには、次の 2 つの方法があります。

- フッター「disclaimer」をマシンレベルからクラスタレベルに格上げする
- リスナーをマシンレベルに格下げして、相互依存を解消する

中央集中型管理されたシステムの特長を最大限に活かすためには、1 つめの方法を推奨します。クラスタ化されたマシンの設定を調整するときは、設定間の相互依存に注意してください。

# ベスト プラクティスとよくあるご質問

## ベスト プラクティス

クラスタを作成すると、現在ログインしているマシンが自動的に最初の実機としてクラスタに追加され、Main\_Group にも追加されます。マシンのマシン レベルの設定は、できる限りクラスタ レベルに移動されます。グループ レベルの設定は存在せず、マシン レベルに残された設定は、クラスタ レベルでは意味を成さないためクラスタ化できません。例として、IP アドレスやライセンス キーなどがあります。

設定はできる限りクラスタ レベルに残します。クラスタ内の 1 つの実機にだけ異なる設定が必要な場合は、そのクラスタ設定をその実機のマシン レベルにコピーします。この場合は、設定を移動しないでください。工場出荷時のデフォルト値がない設定 (HAT テーブル、SMTPROUTES テーブル、LDAP サーバプロファイルなど) を移動すると、クラスタ設定を継承するシステムに空のテーブルが作成され、電子メールが処理されなくなるおそれがあります。

マシンにクラスタ設定を再度継承させるには、CM の設定を管理し、マシンの設定を削除します。マシンがクラスタ設定を上書きするかどうかは、次のメッセージが表示されたときにわかります。

Settings are defined:

```
To inherit settings from a higher level: Delete Settings for this feature at this mode.
You can also Manage Settings.
```

Settings for this feature are also defined at:

```
Cluster: xxx
```

または、次のメッセージが表示されます。

Delete settings from:

```
Cluster: xxx
Machine: yyyy.domain.com
```

## コピーと 移動

コピーする必要がある場合：クラスタに設定を作成し、グループまたはマシンには設定を作成しないか、別の設定を作成する場合。

移動する必要がある場合：クラスタには設定を作成せず、グループまたはマシンに設定を作成する場合。

## 適切な CM の設計方法

LIST 操作で CM マシンのリストを出力すると、次のように表示されます。

```
cluster = CompanyName
Group Main_Group:
 Machine lab1.example.com (Serial #: XXXXXXXXXXXX-XXXXXXX)
 Machine lab2.example.com (Serial #: XXXXXXXXXXXX-XXXXXXX)
Group Paris:
 Machine lab3.example.com (Serial #: XXXXXXXXXXXX-XXXXXXX)
 Machine lab4.example.com (Serial #: XXXXXXXXXXXX-XXXXXXX)
```

```
Group Rome:
 Machine lab5.example.com (Serial #: XXXXXXXXXXXX-XXXXXXX)
 Machine lab6.example.com (Serial #: XXXXXXXXXXXX-XXXXXXX)
現在変更しているレベルを忘れないように注意してください。たとえば、(RENAMEGROUP を使っ
て) Main_Group の名前を変更した場合は、次のように表示されます。
cluster = CompanyName
Group London:
 Machine lab1.cable.nu (Serial #: 000F1FF7B3F0-CF2SX51)
 ...
```

しかし、最初にグループレベルで London のシステムを変更すると、クラスタレベルを基本的な設定を行うための通常の設定レベルとして使用しなくなるため、このような設定は管理者にとって混乱の元です。

**ヒント：**グループにクラスタと同じ名前を付けること（クラスタ「London」とグループ「London」など）は推奨しません。グループ名としてサイト名を使用する場合、クラスタに場所を表す名前を付けることは推奨しません。

正しい方法は、前述のように、できるだけ多くの設定をクラスタレベルに残すことです。ほとんどの場合、プライマリサイトや主要なマシン群を Main\_Group に残し、グループを追加のサイト用に使用してください。これは、両方のサイトを「同等」に扱う場合にも当てはまります。CMにはプライマリ/セカンダリサーバやマスター/スレーブサーバがなく、クラスタ化されたすべてのマシンがピアになることを思い出してください。

**ヒント：**追加のグループを使用する場合は、マシンをクラスタに追加する前にグループを簡単に準備できます。

## 手順：サンプルクラスタの設定

このサンプルクラスタを設定するには、clusterconfig を実行する前に、すべてのマシン上ですべての GUI からログアウトします。プライマリサイトのいずれかのマシン上で clusterconfig を実行します。次に、他のローカルマシンとリモートマシンのうち、(IP アドレスなどのマシン専用の設定を除いて) できるだけ多くの設定を共有する必要があるマシンだけをこのクラスタに追加します。clusterconfig コマンドを使ってリモートマシンをクラスタに追加できません。リモートマシン上の CLI を使って clusterconfig (既存のクラスタへの参加) を実行する必要があります。

前述の例では、lab1 にログインし、clusterconfig を実行して CompanyName という名前のクラスタを作成しています。同じ要件のマシンは 1 つしかないため、lab2 にログインし、saveconfig で既存の設定を保存します (この設定は lab1 の設定のほとんどを継承して大幅に変更されます)。次に、lab2 上で clusterconfig を使って既存のクラスタに参加します。他にも同じようなポリシーと設定を必要とするマシンがこのサイトにある場合は、上記の手順を繰り返します。

CONNSTATUS を実行して、DNS でホスト名が正しく解決されることを確認します。マシンがクラスタに追加されると、新しいマシンのほとんどの設定は lab1 から継承され、古い設定は消失します。追加されたマシンが運用マシンである場合は、これまでの設定の代わりに新しい設定を使ってメールが引き続き処理されるかどうかを予測する必要があります。マシンをクラスタから削除しても、そのマシンが古い専用の設定に戻ることはありません。

次に、例外となるマシンの数を数えます。例外が 1 台しかない場合は、マシンレベルの設定をいくつか追加すればよく、そのマシン用に追加のグループを作成する必要はありません。そのマシンをクラスタに追加し、設定をマシンレベルにコピーする作業を始めます。このマシンが既存の運用マシンである場合は、設定をバックアップし、前述のように電子メール処理の変更を検討する必要があります。

前述の例のように、例外が 2 台以上ある場合は、それらのマシンがクラスタで共有されない設定を共有するかどうかを判断します。共有する場合は、これらのマシン用のグループを 1 つ以上作成します。共有しない場合は、各マシンでマシン レベルの設定を作成すればよく、追加のグループを作成する必要はありません。

前述の例では、クラスタにすでに含まれているいずれかのマシン上で CLI の `clusterconfig` を実行し、`ADDGROUP` を選択する必要があります。この作業を 2 回行います（Paris に対して 1 回、Rome に対して 1 回）。

これで、GUI と CLI を使ってクラスタ用の設定とすべてのグループ（まだマシンがないグループも含む）用の設定を作成できます。各マシンのマシン固有の設定を作成できるようになるのは、マシンをクラスタに追加した後です。

上書き（例外）用の設定を作成する最適な方法は、上位レベル（クラスタなど）から下位レベル（グループなど）に設定をコピーすることです。

たとえば、クラスタを作成した後の `dnsconfig` の初期設定は次のようになりました。

```
Configured at mode:
Cluster: Yes
Group Main_Group: No
Group Paris: No
Group Rome: No
Machine lab2.cable.nu: No
```

この DNS の設定を「グループにコピー」すると、次のようになります。

```
Configured at mode:
Cluster: Yes
Group Main_Group: No
Group Paris: Yes
Group Rome: No
Machine lab2.cable.nu: No
```

ここで、Paris グループ レベルの DNS の設定を編集すると、Paris グループの他のマシンはその設定を継承します。Paris グループ以外のマシンは、マシン固有の設定がない限り、クラスタの設定を継承します。DNS の設定に加えて、SMTPROUTES の設定もグループ レベルで作成するのが一般的です。

ヒント：CLI のさまざまなメニューで `CLUSTERSET` 機能を使用するときは、設定をすべてのグループにコピーする特別なオプションを使用できます。このオプションは GUI では使用できません。

ヒント：完成されたリスナーは、グループまたはクラスタから自動的に継承されるため、通常はクラスタ内の最初のシステム上でのみリスナーを作成します。これによって管理作業が大幅に軽減されます。ただし、そのためにはグループまたはクラスタ全体でインターフェイスに同じ名前を付ける必要があります。

設定をグループ レベルで正しく規定した後は、マシンをクラスタに追加し、このグループに含めることができます。これには次の 2 つの手順が必要です。

まず、残りの 4 つのシステムをクラスタに追加するため、各システム上で `clusterconfig` を実行します。大きく複雑なクラスタほど、追加処理にかかる時間も長くなり、数分かかることもあります。LIST および `CONNSTATUS` サブコマンドを使って追加処理の進行状況をモニタできます。追加処理が完了したら、`SETGROUP` を使ってマシンを Main\_Group から Paris および Rome に移動します。クラ

スタに追加されたすべてのマシンが最初に Paris や Rome の設定ではなく Main\_Group の設定を継承することは避けられません。これは、新しいシステムがすでに稼働中である場合、メールフローのトラフィックに影響する可能性があります。

ヒント：試験用マシンを運用マシンと同じクラスタに含めないでください。試験用システムには新しいクラスタ名を使用してください。これによって、予期しない変更（たとえば、誰かが試験用システムを変更し、誤って運用メールを消失するなど）に対する防御層が追加されます。

## GUI でクラスタのデフォルト以外の CM 設定を使用する場合のオプションの要約

設定の上書き（デフォルトの設定から開始）。たとえば、SMTPROUTES 設定のデフォルトの設定は空のテーブルであり、テーブルを最初から作成できます。

設定の上書き（ただし、クラスタ「xxx」またはグループ「yyy」から現在継承している設定のコピーから開始）。たとえば、SMTPROUTES テーブルの新しいコピーをグループ レベルで使用できます。このテーブルは、初期状態ではクラスタのテーブルとまったく同じです。（SETGROUP で）同じグループに追加されたすべての Cisco アプライアンスにこのテーブルが適用されます。このグループに含まれないマシンでは、引き続きクラスタ レベルの設定が使用されます。この独立したテーブルで SMTPROUTES を変更しても、他のグループ、クラスタの設定を継承するマシン、および個々のマシン レベルで設定が規定されているマシンには影響しません。これが最も一般的な選択です。

中央集中型管理オプションのサブメニューである [設定を管理 (Manage Settings)]。このメニューでは、上記のように設定をコピーできますが、設定を移動または削除することもできます。SMTPROUTES をグループまたはマシン レベルに移動すると、ルート テーブルはクラスタ レベルでは空になり、より具体的なレベルに存在することになります。

[設定を管理 (Manage Settings)]。同じ SMTPROUTES の例で削除オプションを使用した場合も、クラスタの SMTPROUTES テーブルが空になります。SMTPROUTES をグループ レベルまたはマシン レベルですでに設定している場合は、これで問題ありません。クラスタ レベルの設定を削除し、グループまたはマシンの設定だけに依存することは推奨しません。クラスタ全体の設定は、新しく追加したマシンに対するデフォルトとして有用であり、これを保持することによって、管理する必要があるグループまたはサイトの設定の数が 1 つ減ります。

## セットアップと設定に関する質問

Q. 中央集中型管理のライセンス キーを受け取るにはどうすればよいですか。

A. Cisco アプライアンスをクラスタに追加する前に、すべてのアプライアンスに中央集中型管理用の一意のライセンス キーをインストールする必要があります。キーを入手するには、Cisco のカスタマー サポートに連絡してください。個々のキーをインストールするには、[システム管理 (System Administration)] > [ライセンス キー (Feature Keys)] ページ (GUI) または `featurekey` コマンド (CLI) を使用します。

Q. 設定が完了し、リスナーやユーザからメールを受信しているスタンドアロンのアプライアンスがあります。中央集中型管理のライセンス キーを適用し、新しいクラスタを作成すると、これまでの設定はどうなりますか。

A. アプライアンスがすでに「スタンドアロン」モードで設定されている場合は、クラスタを作成したときにそのスタンドアロンの設定が使用されます。つまり、`clusterconfig -> create cluster` コマンドを使って新しいクラスタを作成すると、最初にすべての設定がクラスタ レベルで設定されます。次にクラスタに参加したマシンは、これらの設定をすべて受け取ります。

Q. これまでスタンドアロンとして設定されていたマシンがあり、既存のクラスタに参加しました。これまでの設定はどうなりますか。

A. マシンがクラスタに参加すると、そのマシンのすべてのクラスタ化可能な設定がクラスタ レベルから継承されます。クラスタに参加した時点で、ローカルで設定されたネットワーク以外の設定は消失し、クラスタや関連するグループの設定で上書きされます。(これにはユーザ/パスワードのテーブルも含まれ、パスワードとユーザはクラスタ内で共有されます)。

Q. クラスタ化されたマシンがあり、それをクラスタから (永続的に) 削除しました。これまでの設定はどうなりますか。

A. マシンをクラスタから永続的に削除すると、その設定階層は「平板化」され、そのマシンは引き続きクラスタに含まれていたときと同じように動作します。マシンに継承されたすべての設定が、スタンドアロンとして設定されたマシンに適用されます。

たとえば、クラスタ モードのグローバル配信停止テーブルしかない場合にマシンをクラスタから削除すると、そのグローバル配信停止テーブルのデータがマシンのローカル設定にコピーされます。

## 一般的な質問

Q. 中央集中型管理されるマシン間でログ ファイルは集約されますか。

A. いいえ。ログ ファイルは引き続き個々のマシンごとに保持されます。セキュリティ管理アプリケーションを使って複数のマシンのメール ログを集約し、トラッキングやレポート作成に利用できます。

Q. ユーザ アクセスはどうなりますか。

A. Cisco アプライアンスはクラスタ全体で 1 つのデータベースを共有します。特に、admin アカウントはクラスタ全体で 1 つしかありません。

Q. データセンターをクラスタ化するにはどうすればよいですか。

A. データセンターは、それ自体をクラスタにせずに、クラスタ内の「グループ」にするのが理想的です。しかし、データセンター間で共有する設定が多くない場合は、各データセンターを別個のクラスタにした方がうまくいく場合があります。

Q. オフラインのシステムを再接続するとどうなりますか。

A. クラスタにシステムを再接続すると、システム間の同期が試行されます。

## ネットワークに関する質問

Q. 中央集中型管理機能は「ピアツーピア」アーキテクチャと「マスター/スレーブ」アーキテクチャのどちらですか。

A. すべてのマシンにすべてのマシン用のあらゆるデータ (使用されないマシン固有の設定を含む) があるため、中央集中型管理機能は「ピアツーピア」アーキテクチャと見なすことができます。

Q. ピアにならないようにアプライアンスをセットアップするにはどうすればよいですか。「スレーブ」システムを設定する必要があります。

A. このアーキテクチャでは、本物の「スレーブ」マシンは設定できません。しかし、マシン レベルで HTTP アクセス (GUI) と SSH/Telnet アクセス (CLI) をディセーブルにすることは可能です。このように GUI アクセスや CLI アクセスができないマシンは、clusterconfig コマンドでのみ設定可能です (つまり、ログイン ホストではなくなります)。これはスレーブを設定するのに似ていますが、ログイン アクセスを再度イネーブルにすると、この設定は無効になります。

Q. 複数のセグメント化されたクラスタを作成できますか。

A. クラスタを「島」のように分離することは可能です。実際、たとえばパフォーマンス上の理由などで、このようなクラスタを作成するのが有益な場合もあります。

Q. クラスタ化されたアプライアンスのうち、1 台の IP アドレスとホスト名を再設定したいのですが、再設定した場合、再起動コマンドを実行できるようになる前に GUI/CLI セッションが終了しませんか。

次の手順を実行します。

- a. 新しい IP アドレスを追加します。
- b. リスナーを新しいアドレスに移動します。
- c. クラスタを脱退します。
- d. ホスト名を変更します。
- e. どのマシンから表示した `clusterconfig` の接続リストにも、古いマシン名が表示されないことを確認します。
- f. すべての GUI セッションがログアウトしたことを確認します。
- g. (`interfaceconfig` または [ ネットワーク (Network) ] > [ リスナー (Listeners) ] を使って) どのインターフェイスでも CCS がイネーブルになっていないことを確認します。
- h. マシンを再びクラスタに追加します。

Q. 送信先コントロール機能をクラスタ レベルで適用できますか。それともこの機能はローカル マシン レベル専用ですか。

クラスタ レベルでも設定できますが、制限はマシン単位で適用されます。したがって、接続を 50 個に制限すると、クラスタ内のそれぞれのマシンにその制限が設定されます。

## 計画と設定

Q. クラスタをセットアップするときに、効率を最大限に高め、問題を最小限に抑えるにはどうすればよいですか。

### 1. 初期の計画

- できるだけ多くの項目をクラスタ レベルで設定します。
- 例外のみをマシン単位で管理します。
- データセンターが複数ある場合は、たとえば、グループを使ってクラスタ共通でもマシン固有でもない特性を共有します。
- 各アプライアンスのインターフェイスとリスナーに同じ名前を使用します。

### 2. 制限コマンドに注意してください。

### 3. 設定間の相互依存に注意してください。

たとえば、`listenerconfig` コマンドは、(クラスタ レベルでも) マシン レベルにしか存在しないインターフェイスに依存します。クラスタ内のどのマシンにもマシン レベルのインターフェイスが存在しない場合、そのリスナーはイネーブルになります。

インターフェイスの削除も `listenerconfig` に影響します。

### 4. 設定に注意してください。

すでに設定されているマシンがクラスタに参加すると、そのマシン単独の設定は消失します。前に設定した設定の一部を再び適用する場合は、クラスタに参加する前にすべての設定をメモしてください。

「切断された」マシンは、まだクラスタに含まれています。マシンを再接続すると、オフライン中に行った変更がクラスタの他のマシンと同期化されます。

マシンをクラスタから永続的に削除すると、そのマシンはクラスタのメンバとして持っていたすべての設定を保持します。しかし、考えを変えて再びそのマシンをクラスタに追加すると、そのマシンのスタンドアロンの設定はすべて消失します。この場合、設定を意図した状態に復元することはほぼ不可能です。

saveconfig コマンドを使って設定の記録を取ってください。





## CHAPTER 36

# テストとトラブルシューティング

- 「テスト メッセージを使用したメール フローのデバッグ : トレース」 (P.36-1)
- 「アプライアンスのテストにリスナーを使用」 (P.36-13)
- 「ネットワークのトラブルシューティング」 (P.36-17)
- 「リスナーのトラブルシューティング」 (P.36-23)
- 「アプライアンスからの電子メール配信のトラブルシューティング」 (P.36-25)
- 「パフォーマンスのトラブルシューティング」 (P.36-27)
- 「アプライアンスの電源のリモート リセット」 (P.36-28)
- 「テクニカル サポートの使用」 (P.36-29)



(注)

このセクションに記載されている機能またはコマンドには、ルーティングの優先順位に影響を与えるものや、影響を受けるものが含まれています。詳細については、「ネットワーク アドレスと IP アドレスの割り当て」を参照してください。

## テスト メッセージを使用したメール フローのデバッグ : トレース

[システム管理 (System Administration)] > [トレース (Trace)] ページを使用して (CLI の `trace` コマンドと同等)、テスト メッセージの送信をエミュレートすることにより、システムを介したメッセージフローをデバッグできます。[トレース (Trace)] ページ (および `trace CLI` コマンド) では、リスナーに受け入れられているようにメッセージをエミュレートし、現在のシステム設定 (コミットしていない変更を含む) によって「トリガー」される、または影響を受ける機能の概要を出力できます。テストメッセージは実際には送信されません。特に、Cisco アプライアンスで使用できる多数の高度な機能を組み合わせると、[トレース (Trace)] ページ (および `trace CLI` コマンド) は、強力なトラブルシューティングまたはデバッグ ツールとなります。

[トレース (Trace)] ページ (および trace CLI コマンド) では、表 36-1 に示されている入力パラメータのプロンプトが表示されます。

表 36-1 [トレース (Trace)] ページに対する入力

値	説明	例
ソース IP アドレス	リモートドメインの送信元を模倣するため、リモートクライアントの IP アドレスを入力します。これは、インターネットプロトコルバージョン 4 (IPv4) またはバージョン 6 (IPv6) アドレスを指定できます。  (注) trace コマンドを実行すると、IP アドレスと完全修飾ドメイン名の入力が求められます。完全修飾ドメイン名が一致するかどうかを確認するための IP アドレスの逆引きは行われません。trace コマンドでは、完全修飾ドメイン名フィールドを空白にすることができないので、DNS で適切に逆引きできない場合にはテストできません。	203.45.98.109 2001:0db8:85a3::8a2e:0370:7334
ソース IP アドレスの完全修飾ドメイン名	模倣する完全修飾リモートドメイン名を入力します。そのままにすると、送信元 IP アドレスに対してリバース DNS ルックアップが実行されます。	smtp.example.com
次の動作をトレースするリスナー	テストメッセージの送信をエミュレートするため、システムに設定されているリスナーのリストから選択します。	InboundMail
ネットワーク所有者の組織 ID	SenderBase ネットワークオーナーに固有の ID 番号を入力するか、送信元 IP アドレスに関連付けられたネットワークオーナー ID の検索を指示します。GUI を介して送信者グループにネットワークオーナーを追加した場合は、この情報を表示できます。	34
SenderBase レピュテーションスコア (SBRSS コア)	スプーフィングドメインに与える SBRSS スコアを入力するか、送信元 IP アドレスに関連付けられた SBRSS スコアの検索を指示します。このパラメータは、SBRSS スコアを使用するポリシーをテストするときに役立ちます。手動で入力した SBRSS スコアは、Context Adaptive Scanning Engine (CASE) に渡されないことに注意してください。詳細については、「リスナーのレピュテーションフィルタリングスコアのしきい値の編集」(P.6-5) を参照してください。	-7.5
エンベロープ送信者	テストメッセージのエンベロープ送信者を入力します。	admin@example.net

表 36-1 [トレース (Trace)] ページに対する入力 (続き)

値	説明	例
エンベロープ受信者	テストメッセージの受信者のリストを入力します。複数のエントリを指定する場合は、カンマで区切ります。	joe frank@example.com
メッセージ本文	ヘッダーを含む、テストメッセージのメッセージ本文を入力します。メッセージ本文の入力を終了するには、別の行にピリオドを入力します。「ヘッダー」は(空白行で区切られた)メッセージ本文の一部と見なされます。ヘッダーを省略したり、ヘッダーの形式に誤りがあったりすると、予期しないトレース結果を招くことがあります。	To: 1@example.com From: ralph Subject: Test  this is a test message .

値を入力したら、[トレースを開始 (Start Trace)] をクリックします。メッセージに影響する、システムに設定されたすべての機能の概要が出力されます。

メッセージ本文は、ローカルファイルシステムからアップロードできます (CLI では、/configuration ディレクトリにアップロードしたメッセージ本文を使用してテストできます。Cisco アプライアンスへのインポート用ファイルの準備に関する詳細については、「[アプライアンスへのアクセス](#)」を参照してください)。

概要が出力されると、生成されたメッセージの確認とテストメッセージの再実行を求められます。別のテストメッセージを入力する場合、[トレース (Trace)] ページおよび trace コマンドで、前に入力した表 36-1 の値が使用されます。



(注)

表 36-2 に示す、trace コマンドによってテストされる設定の各セクションは、*順番どおり*に実行されます。この順番は、ある機能の設定が他の機能にどのように影響するかを理解するうえで非常に役立ちます。たとえば、ドメインマップ機能によって変換される受信者アドレスは、RAT によって評価されるアドレスに影響します。また、RAT の影響を受ける受信者は、エイリアステーブルによって評価されるアドレスに影響する、というようになります。

表 36-2 トレースを実行したときの出力の表示

trace コマンド セクション	出力
ホスト アクセス テーブル (HAT) およびメールフローポリシーの処理	<p>指定したリスナーに対するホスト アクセス テーブルの設定が処理されます。システムからは、入力したリモート IP アドレスおよびリモート ドメイン名と一致した HAT 内のエントリが報告されます。デフォルトのメールフローポリシーと送信者グループ、およびどちらが所定のエントリに一致したかを確認できます。</p> <p>Cisco アプライアンスが (REJECT または TCPREFUSE アクセスルールを介して) 接続を拒否するように設定された場合、処理中の trace コマンドはその時点で終了します。</p> <p>HAT プロパティの設定の詳細については、「<a href="#">定義済みの送信者グループとメールフローポリシーの理解</a> (P.7-11) を参照してください。</p>

**エンベロープ送信者アドレスの処理**

これらのセクションには、指定したエンベロープ送信者に対してアプライアンスの設定がどのように影響するかが要約されます (つまり、MAIL FROM コマンドがアプライアンスの設定によってどのように解釈されるかがわかります)。trace コマンドは、このセクションの前に「Processing MAIL FROM:」を出力します。

デフォルト ドメイン	<p>リスナーで、受信するメッセージのデフォルトの送信者ドメインを変更するように指定した場合は、エンベロープ送信者に対するすべての変更がこのセクションに出力されます。</p> <p>詳細については、「<a href="#">電子メールを受信するためのゲートウェイの設定</a>」を参照してください。</p>
マスカレード	<p>メッセージのエンベロープ送信者を変換するように指定した場合、ここに変更が表示されます。listenerconfig -&gt; edit -&gt; masquerade -&gt; config サブコマンドを使用して、プライベートリスナーに対するエンベロープ送信者のマスカレードをイネーブルにします。</p> <p>詳細については、「<a href="#">ルーティングおよび配信機能の設定</a>」を参照してください。</p>

**エンベロープ受信者の処理**

これらのセクションでは、指定したエンベロープ受信者に対してアプライアンスがどのように影響するかの要約を示します (つまり、RCPT TO コマンドがアプライアンスの設定によってどのように解釈されるかがわかります)。trace コマンドは、このセクションの前に「Processing Recipient List:」を出力します。

デフォルト ドメイン	<p>リスナーで、受信するメッセージのデフォルトの送信者ドメインを変更するように指定した場合は、エンベロープ受信者に対するすべての変更がこのセクションに出力されます。</p> <p>詳細については、「<a href="#">電子メールを受信するためのゲートウェイの設定</a>」を参照してください。</p>
------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------

表 36-2 トレースを実行したときの出力の表示 (続き)

trace コマンド セクション	出力
ドメイン マップの変換	<p>ドメイン マップ機能によって、受信者アドレスが代替アドレスに変換されます。ドメイン マップの変更を指定しており、指定した受信者アドレスが一致した場合は、このセクションに変換が出力されます。</p> <p>詳細については、「<a href="#">ルーティングおよび配信機能の設定</a>」を参照してください。</p>
受信者アクセス テーブル (RAT)	<p>ポリシーとパラメータのほか、このセクションには、RAT 内のエントリに一致する各エンベロープ受信者が出力されます (たとえば、リスナーの RAT の制限をバイパスするように、受信者を指定した場合)。</p> <p>受け入れる受信者の指定の詳細については、「<a href="#">電子メールを受信するためのゲートウェイの設定</a>」を参照してください。</p>
エイリアス テーブル	<p>このセクションには、アプライアンスで設定されたエイリアス テーブル内のエントリに一致する各エンベロープ受信者 (および 1 つまたは複数の受信者アドレスへの後続の変換) が出力されます。</p> <p>詳細については、「<a href="#">ルーティングおよび配信機能の設定</a>」を参照してください。</p>

**Pre-Queue メッセージ操作**

ここでは、メッセージの内容を受信した後、ワーク キュー上でメッセージがキューから出る前に、各メッセージにアプライアンスがどのように影響するかを示します。この処理は、最後の 250 ok コマンドがリモート MTA に返される前に実行されます。

trace コマンドは、このセクションの前に「**Message Processing:**」を出力します。

仮想ゲートウェイ	<p>altsrchost コマンドを実行すると、エンベロープ送信者の完全アドレス、ドメイン、または名前、あるいは IP アドレスの一致に基づいて、特定のインターフェイスにメッセージが割り当てられます。エンベロープ送信者が altsrchost コマンドのエントリに一致すると、その情報がこのセクションに出力されます。</p> <p>この時点で割り当てられた仮想ゲートウェイ アドレスは、メッセージ フィルタの処理によって上書きされる可能性があることに注意してください。</p> <p>詳細については、「<a href="#">ルーティングおよび配信機能の設定</a>」を参照してください。</p>
----------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

表 36-2 トレースを実行したときの出力の表示 (続き)

trace コマンド セクション	出力
バウンス プロファイル	<p>バウンス プロファイルは、処理中の 3 つの時点で適用されます。ここが最初のポイントです。リスナーにバウンス プロファイルが割り当てられる場合は、プロセス内のこの時点で割り当てられます。その情報がこのセクションに出力されます。</p> <p>詳細については、「<a href="#">ルーティングおよび配信機能の設定</a>」を参照してください。</p>

表 36-2 トレースを実行したときの出力の表示 (続き)

trace コマンド セクション	出力
<b>ワーク キュー操作</b>	
	<p>次の一連の機能は、ワーク キュー内のメッセージに対して実行されます。機能が実行されるのは、クライアントからのメッセージが受け入れられた後、そのメッセージが配信用として宛先キューに入れられる前です。status コマンドおよび status detail コマンドによって「Messages in Work Queue」が報告されます。</p>
マスカレード	<p>メッセージの [宛先: (To:)]、[差出人: (From:)]、および [CC:] ヘッダーが (リスナーから入力されたスタティック テーブルまたは LDAP クエリーを通じて) マスクされるように指定した場合は、ここに変更が表示されます。listenerconfig -&gt; edit -&gt; masquerade -&gt; config サブコマンドを使用して、プライベート リスナーに対してメッセージ ヘッダーのマスカレードをイネーブルにします。</p> <p>詳細については、「<a href="#">ルーティングおよび配信機能の設定</a>」を参照してください。</p>
LDAP ルーティング	<p>リスナーに対して LDAP クエリーがイネーブルになっている場合は、このセクションに LDAP 許可、再ルーティング、マスカレード、およびグループ クエリーの結果が出力されます。</p> <p>詳細については、「<a href="#">LDAP クエリー</a>」を参照してください。</p>
メッセージ フィルタの処理	<p>システムでイネーブルになっているすべてのメッセージ フィルタは、この時点でテスト メッセージによって評価されます。フィルタごとにルールが評価され、最後の結果が「true」であれば、そのフィルタの各アクションが順次実行されます。フィルタには他のフィルタがアクションとして含まれている場合があり、フィルタは無制限にネスティングされます。ルールが「false」と評価された場合、アクションのリストが else 句に関連付けられていれば、それらのアクションが代わりに評価されます。このセクションには、順番に処理されたメッセージ フィルタの結果が出力されます。</p> <p>「<a href="#">メッセージ フィルタを使用した電子メール ポリシーの適用</a>」を参照してください。</p>
<b>メール ポリシーの処理</b>	
	<p>メール ポリシーの処理セクションには、アンチスパム、アンチウイルス、アウトブレイク フィルタ機能と、指定されたすべての受信者に対する免責事項スタンプ機能が表示されます。複数の受信者が電子メール セキュリティ マネージャの複数のポリシーに一致する場合は、一致する各ポリシーが次の各セクションに繰り返し表示されます。「Message going to」というストリングは、どの受信者がどのポリシーに一致したかを定義します。</p>

表 36-2 トレースを実行したときの出力の表示（続き）

trace コマンド セクション	出力
スパム対策	<p>このセクションには、アンチスパム スキャンの処理対象としてフラグが設定されていないメッセージが示されます。メッセージがリスナーに対するアンチスパム スキャンによって処理されることになっている場合、メッセージは処理され、返された判定が出力されます。Cisco アプライアンスが、その判定に基づいてメッセージをバウンスまたはドロップするように設定されている場合は、その情報が出力され、trace コマンドの処理は停止します。</p> <p>(注) システムでアンチスパム スキャンが使用できない場合、この手順は省略されます。アンチスパム スキャンを使用できても、ライセンス キーによってイネーブルになっていない場合は、その情報もこのセクションに出力されます。</p> <p>「アンチスパム」を参照してください。</p>
アンチウイルス	<p>このセクションには、アンチウイルス スキャンの処理対象としてフラグが設定されていないメッセージが示されます。メッセージがリスナーに対するアンチウイルス スキャンによって処理されることになっている場合、メッセージは処理され、返された判定が出力されます。Cisco アプライアンスが、感染メッセージを「クリーニング」するように設定されている場合は、その情報が表示されます。その判定に基づいてメッセージをバウンスまたはドロップするように設定されている場合は、その情報が出力され、trace コマンドの処理は停止します。</p> <p>(注) システムでアンチウイルス スキャンが使用できない場合、この手順は省略されます。アンチウイルス スキャンを使用できても、ライセンス キーによってイネーブルになっていない場合は、その情報もこのセクションに出力されます。</p> <p>「アンチウイルス」を参照してください。</p>
コンテンツ フィルタの処理	<p>システムでイネーブルになっているすべてのコンテンツ フィルタは、この時点でテスト メッセージによって評価されます。フィルタごとにルールが評価され、最後の結果が「true」であれば、そのフィルタの各アクションが順次実行されます。フィルタには他のフィルタがアクションとして含まれている場合があり、フィルタは無制限にネスタリングされます。このセクションには、順番に処理されたコンテンツ フィルタの結果が出力されます。</p> <p>「コンテンツ フィルタ」を参照してください。</p>



表 36-2 トレースを実行したときの出力の表示 (続き)

trace コマンド セクション	出力
アウトブレイク フィルタの処理	<p>このセクションには、アウトブレイク フィルタ機能をバイパスする添付ファイルのあるメッセージが示されます。メッセージが受信者に対するアウトブレイク フィルタによって処理されることになっている場合、メッセージは処理され、その評価が出力されます。アプリケーションが、判定に基づいてメッセージを隔離、バウンス、またはドロップするように設定されている場合、その情報が出力されて、処理が停止します。</p> <p>「<a href="#">アウトブレイク フィルタ</a>」を参照してください。</p>
フッター スタンプ	<p>このセクションには、メッセージにフッター テキスト リソースが付加されたかどうかを示されます。テキスト リソースの名前が表示されます。「<a href="#">テキスト リソース</a>」の「<a href="#">メッセージの免責事項スタンプ</a>」(P.18-2) を参照してください。</p>

表 36-2 トレースを実行したときの出力の表示 (続き)

trace コマンド セクション	出力
<b>配信操作</b>	
次の各セクションには、メッセージが配信されるときに発生する動作が示されます。trace コマンドは、このセクションの前に「Message Enqueued for Delivery」を出力します。	
ドメインおよびユーザごとのグローバル配信停止	<p>trace コマンドの入力として指定した受信者が、グローバル配信停止機能に示されている受信者、受信者ドメイン、または IP アドレスに一致すると、未登録の受信者アドレスがこのセクションに出力されます。</p> <p>「ルーティングおよび配信機能の設定」を参照してください。</p>
<b>最終結果</b>	
すべての処理が出力されると、最終結果が表示されます。CLI では、「Would you like to see the resulting message?」という問いに対して <b>y</b> と入力して、結果のメッセージを表示します。	

## [トレース (Trace)] ページの GUI の例

図 36-1 [トレース (Trace)] ページでの入力事項  
Trace

Message Definition	
Sender Information	
Source IP:	1.2.3.4
Fully Qualified Domain Name of the Source IP: ?	remotehost.example.com
Listener to Trace Behavior on:	Public (172.22.85.1:25) ▼
SenderBase Network Owner ID:	<input checked="" type="radio"/> Lookup network owner ID associated with source IP <input type="radio"/> Use: _____
SenderBase Reputation Score (SBR5):	<input checked="" type="radio"/> Lookup SBR5 associated with source IP <input type="radio"/> Use: _____
Envelope Information	
Envelope Sender:	pretend.sender@example.domain
Envelope Recipients (separated by commas):	admin@ironport.com
Message Body	
Upload Message Body:	<input type="text"/> <input type="button" value="Browse..."/>
Paste Message Body: <i>(If no file is uploaded.)</i>	Subject: hello This is a test message.
<input type="button" value="Clear"/> <span style="float: right;"><input type="button" value="Start Trace"/></span>	

図 36-2 [トレース (Trace) ] ページの出力 (1/2)  
Trace

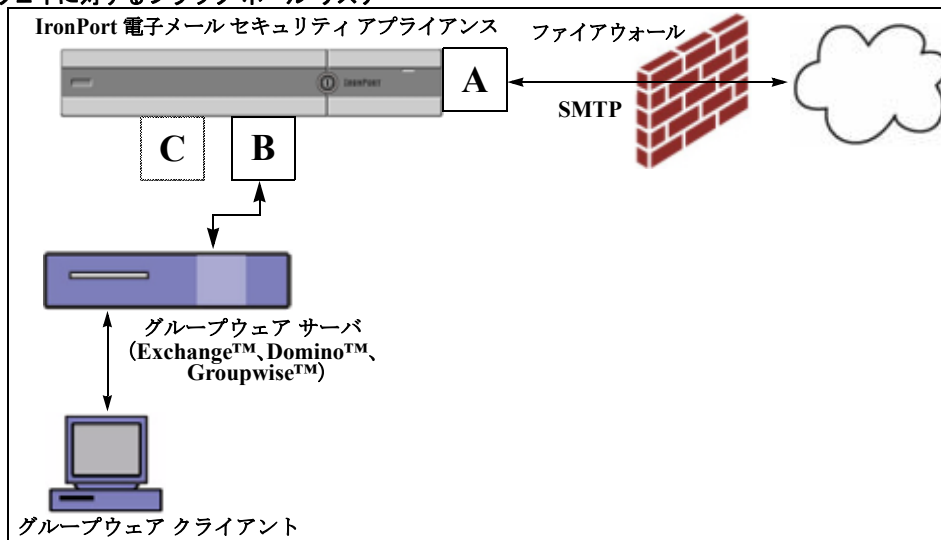
Trace Results			
Host Access Table Processing (Listener: Public)			
Matched On:	ALL Sender Group		
Named Policy:	ACCEPTED		
Connection Behavior:	ACCEPT		
Fully Qualified Domain Name:			
SenderBase Network Owner ID:	N/A		
SenderBase Reputation Score:	N/A		
Policy Parameters:	Max. Messages Per Connection:	1,000	Default
	Max. Recipients Per Message:	1,000	Default
	Max. Message Size:	100M	Default
	Max. Concurrent Connection From a Single IP:	1,000	Default
	Use TLS:	No	Default
	Max. Recipients Per Hour:	1000	
	Use SenderBase:	Yes	
	Use Spam Detection:	Yes	
	Use Virus Detection:	Yes	Default
Envelope Sender Processing			
Envelope Sender: pretend.sender@example.domain			
Default Domain Processing:	No Change		
Envelope Recipient Processing			
Envelope Recipient: admin@ironport.com			
Default Domain Processing:	No Change		
Domain Map Processing:	No Change		
Recipient Access Table Processing:	Behavior: ACCEPT Matched On: admin@ironport.com		
Alias Expansion:	No Change		
Message Processing			
Assigned Virtual Gateway:	None		
Assigned Bounce Profile:	None		



## ■ アプライアンスのテストにリスナーを使用

たとえば、図 36-4 では、ブラック ホール リスナー「C」を作成して、「B」というプライベートリスナーをミラーリングします。非キューイング版では、グループウェア クライアントからグループウェア サーバを経由してアプライアンスまでのシステムのパフォーマンス パスをテストします。キューイング版は、同じ方法およびメッセージをキューに入れて SMTP 経由で配信するためのアプライアンスの機能をテストします。

図 36-4 エンタープライズ ゲートウェイに対するブラック ホール リスナー



次の例では、`listenerconfig` コマンドを使用して、管理インターフェイス上で `BlackHole_1` という名前のブラック ホール キューイング リスナーを作成します。リスナーのためのこのホスト アクセス テーブル (HAT) は、次のホストからの接続を受け入れるように編集されています。

- `yoursystem.example.com`
- `10.1.2.29`
- `badmail.tst`
- `.tst`



(注)

最後のエン트리である `.tst` により、`.tst` ドメイン内にあるすべてのホストから `BlackHole_1` という名前のリスナーに電子メールを送信できるようになります。

## 例

```
mail3.example.com> listenerconfig
```

```
Currently configured listeners:
```

1. InboundMail (on PublicNet, 192.168.2.1) SMTP Port 25 Public
2. OutboundMail (on PrivateNet, 192.168.1.1) SMTP Port 25 Private

```
Choose the operation you want to perform:
```

- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.

[> **new**

Please select the type of listener you want to create.

1. Private
2. Public
3. Blackhole

[2]> **3**

Do you want messages to be queued onto disk? [N]> **y**

Please create a name for this listener (Ex: "OutboundMail"):

[> **BlackHole\_1**

Please choose an IP interface for this Listener.

1. Management (192.168.42.42/24: mail3.example.com)
2. PrivateNet (192.168.1.1/24: mail3.example.com)
3. PublicNet (192.168.2.1/24: mail3.example.com)

[1]> **1**

Choose a protocol.

1. SMTP
2. QMQP

[1]> **1**

Please enter the IP port for this listener.

[25]> 25

Please specify the systems allowed to relay email through the IronPort C60.

Hostnames such as "example.com" are allowed.

Partial hostnames such as ".example.com" are allowed.

IP addresses, IP address ranges, and partial IP addresses are allowed.

Separate multiple entries with commas.

[ ]> **yoursystem.example.com, 10.1.2.29, badmail.tst, .tst**

Do you want to enable rate limiting per host? (Rate limiting defines

the maximum number of recipients per hour you are willing to receive from a remote domain.) [N]> **n**

Default Policy Parameters

=====

Maximum Message Size: 100M

Maximum Number Of Connections From A Single IP: 600

Maximum Number Of Messages Per Connection: 10,000

Maximum Number Of Recipients Per Message: 100,000

Maximum Number Of Recipients Per Hour: Disabled

Use SenderBase for Flow Control: No

Spam Detection Enabled: No

Virus Detection Enabled: Yes

Allow TLS Connections: No

Allow SMTP Authentication: No

Require TLS To Offer SMTP authentication: No

Would you like to change the default host access policy? [N]> **n**

Listener BlackHole\_1 created.



```
Defaults have been set for a Black Hole Queuing listener.
```

```
Use the listenerconfig->EDIT command to customize the listener.
```

```
Currently configured listeners:
```

1. BlackHole\_1 (on Management, 192.168.42.42) SMTP Port 25 Black Hole Queuing
2. InboundMail (on PublicNet, 192.1681.1) SMTP Port 25 Public
3. OutboundMail (on PrivateNet, 192.168.1.1) SMTP Port 25 Private

```
Choose the operation you want to perform:
```

- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.

```
[]>
```

**(注)**

---

commit コマンドを実行して、これらの変更が有効になるようにしてください。

---

キューイング タイプのブラック ホール リスナーを設定して、HAT でインジェクション システムからの接続を受け入れるよう変更したら、インジェクション システムを使用して、アプライアンスへの電子メールの送信を開始します。status、status detail、および rate コマンドを使用して、システムのパフォーマンスをモニタします。また、グラフィカルユーザ インターフェイス (GUI) でシステムをモニタすることもできます。詳細については、以下を参照してください。

- 「[CLI を使用したモニタリング](#)」 (P.30-6)
- 「[GUI でのその他の作業](#)」 (P.32-7)

## ネットワークのトラブルシューティング

アプライアンスにネットワーク接続の問題があると思われる場合は、アプライアンスが適切に動作していることを確認します。

## アプライアンスのネットワーク接続テスト

### 手順

- ステップ 1** システムに接続し、管理者としてログインします。正常にログインできると、次のメッセージが表示されます。

```
Last login: day month date hh:mm:ss from IP address
```

```
Copyright (c) 2001-2003, IronPort Systems, Inc.
```

```
AsyncOS x.x for Cisco
```

```
Welcome to the Cisco Messaging Gateway Appliance(tm)
```

- ステップ 2** `status` コマンドまたは `status detail` コマンドを使用します。

```
mail3.example.com> status
```

または

```
mail3.example.com> status detail
```

`status` コマンドは、電子メール動作についてモニタされる情報のサブセットを返します。返される統計情報は、カウンタとゲージの 2 つのカテゴリにグループ化されます。レートなどの電子メールの動作についての全般的なモニタリング情報については、`status detail` コマンドを使用します。カウンタは、システム内の各種イベントの現在までの合計を示します。カウンタごとに、そのカウンタのリセット以降、最後のシステム再起動以降、およびシステムの存続期間に発生したイベントの合計数を表示できます。(詳細については、「[CLI を使用したモニタリング](#)」(P.30-6) を参照してください)。

- ステップ 3** `mailconfig` コマンドを使用して、機能している既知のアドレスに電子メールを送信します。

`mailconfig` コマンドによって、アプライアンスで有効な設定のすべてが含まれる、人が読み取ることのできるファイルが作成されます。このファイルのアプライアンスから機能する既知の電子メールアドレスに送信して、アプライアンスがネットワークで電子メールを送信できることを確認します。

```
mail3.example.com> mailconfig
```

```
Please enter the email address to which you want to send the
configuration file.
```

```
Separate multiple addresses with commas.
```

```
[]> user@example.com
```

```
Do you want to include passwords? Please be aware that a configuration without passwords
will fail when reloaded with loadconfig. [N]> y
```

```
The configuration file has been sent to user@example.com.
```

```
mail3.example.com>
```

## トラブルシューティング

アプライアンスがネットワーク上でアクティブであることが確認されたら、次のコマンドを使用して、ネットワークの問題をピンポイントで特定します。

- netstat コマンドを使用すると、次のようなネットワーク接続（着信と発信の両方）、ルーティングテーブル、ネットワーク インターフェイスのさまざまな統計情報が表示されます。
  - アクティブなソケットのリスト
  - ネットワーク インターフェイスの状態
  - ルーティング テーブルの内容
  - リッスン キューのサイズ
  - パケット トラフィック情報
- diagnostic -> network -> flush コマンドを使用すると、ネットワークに関連するすべてのキャッシュをフラッシュできます。
- diagnostic -> network -> arpshow コマンドを使用すると、システムの ARP キャッシュを表示できます。
- packetcapture コマンドを使用すると、コンピュータが接続されているネットワーク上で送受信されている TCP/IP や他のパケットを傍受して表示できます。

packetcapture を使用するには、ネットワーク インターフェイスとフィルタを設定します。このフィルタでは、UNIX の tcpdump コマンドと同じ形式を使用します。パケットの捕捉を開始するには start を、停止するには stop を使用します。捕捉を停止した後、SCP または FTP を使用して /pub/captures ディレクトリからファイルをダウンロードする必要があります。詳細については、「[パケット キャプチャの実行](#)」(P.36-33) を参照してください。
- アプライアンスでネットワーク上にアクティブな接続があり、ネットワーク上の特定のセグメントに到達できることを確認するには、動作している既知のホストに対して ping コマンドを使用します。

ping コマンドを使用すると、アプライアンスからネットワーク ホストへの接続をテストできます。

```
mail3.example.com> ping
```

```
Which interface do you want to send the pings from?
```

```
1. Auto
```

```
2. Management (192.168.42.42/24: mail3.example.com)
3. PrivateNet (192.168.1.1/24: mail3.example.com)
4. PublicNet (192.168.2.1/24: mail3.example.com)

[1]> 1

Please enter the host you wish to ping.

[>] anotherhost.example.com

Press Ctrl-C to stop.

PING anotherhost.example.com (x.x.x.x): 56 data bytes
64 bytes from 10.19.0.31: icmp_seq=9 ttl=64 time=0.133 ms
64 bytes from 10.19.0.31: icmp_seq=10 ttl=64 time=0.115 ms
^C
--- anotherhost.example.com ping statistics ---
11 packets transmitted, 11 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.115/0.242/1.421/0.373 ms
```



(注) ping コマンドを終了するには、Ctrl+C を使用します。

- traceroute コマンドを使用すると、アプライアンスからネットワーク ホストへの接続をテストして、ネットワークのホップに関するルーティングの問題をデバッグできます。

```
mail3.example.com> traceroute

Which interface do you want to trace from?

1. Auto
2. Management (192.168.42.42/24: mail3.example.com)
3. PrivateNet (192.168.1.1/24: mail3.example.com)
4. PublicNet (192.168.2.1/24: mail3.example.com)

[1]> 1
```

```
Please enter the host to which you want to trace the route.
```

```
[> 10.1.1.1
```

```
Press Ctrl-C to stop.
```

```
traceroute to 10.1.1.1 (10.1.1.1), 64 hops max, 44 byte packets
```

```
1 gateway (192.168.0.1) 0.202 ms 0.173 ms 0.161 ms
```

```
2 hostname (10.1.1.1) 0.298 ms 0.302 ms 0.291 ms
```

```
mail3.example.com>
```

- diagnostic -> network -> smtping コマンドを使用すると、リモートの SMTP サーバをテストできます。
- nslookup コマンドを使用すると、DNS の機能をテストできます。

nslookup コマンドでは、アプライアンスから動作している Domain Name Service (DNS; ドメインネーム サービス) サーバを使用してホスト名や IP アドレスを解決して到達できることを確認できます。

```
mail3.example.com> nslookup
```

```
Please enter the host or IP to resolve.
```

```
[> example.com
```

```
Choose the query type:
```

```
1. A
```

```
2. CNAME
```

```
3. MX
```

```
4. NS
```

```
5. PTR
```

```
6. SOA
```

```
7. TXT
```

```
[1]>
```

```
A=192.0.34.166 TTL=2d
```

表 36-3 DNS の機能の確認：クエリーのタイプ

クエリーのタイプ	説明
A	ホストのインターネット アドレス
CNAME	エイリアスの正規の名前
MX	メール エクスチェンジャ
NS	指定したゾーンのネーム サーバ
PTR	クエリーがインターネット アドレスの場合はホスト名、そうでない場合は他の情報に対するポインタ
SOA	ドメインの「start-of-authority (権威の開始)」情報
TXT	テキスト情報

- `tophosts` コマンドを CLI または GUI から使用して、「Active Recipients」の順にソートします。  
`tophosts` コマンドからは、キューにある上位 20 の受信者のリストが返されます。このコマンドは、ネットワーク接続の問題が、電子メールを送信しようとしている 1 台のホストまたは 1 つのホスト グループに限定されるかどうかを確認するのに役立ちます（詳細については、49 ページの「メール キューの構成の確認」を参照してください）。

```
mail3.example.com> tophosts
```

```
Sort results by:
```

1. Active Recipients
2. Connections Out
3. Delivered Recipients
4. Soft Bounced Events
5. Hard Bounced Recipients

```
[1]> 1
```

```
Status as of: Mon Nov 18 22:22:23 2003
```

```
ActiveConn.Deliv.SoftHard
```

```
Recipient HostRecipOutRecip.BouncedBounced
```

```
1 aol.com36510255218
```

```

2 hotmail.com29071982813
3 yahoo.com13461231119
4 excite.com9838494
5 msn.com8427633 29

```

^C

- `tophosts` コマンドの結果として得られたリストの最上位のドメインに対して `hoststatus` コマンドを実行し、詳しく調べます。

`hoststatus` コマンドは、特定の受信者ホストに関する電子メール動作のモニタリング情報を返します。AsyncOS キャッシュに格納されている DNS 情報と、受信者ホストから最後に返されたエラーも表示されます。返されるデータは、最後に実行した `resetcounters` コマンドからの累積です。(詳細については、「メールホストのステータスのモニタリング」(P.30-12) を参照してください)。

最上位のドメインに対して `hoststatus` コマンドを実行すると、アプライアンスまたはインターネットのいずれかに対する DNS 解決のパフォーマンスの問題を切り分けることができます。たとえば、最上位のアクティブな受信ホストに対して `hoststatus` コマンドを実行したとき、発信側の多数の接続が保留状態で表示された場合は、特定のホストがダウン状態または到達不能でないかどうか、またアプライアンスがすべてのホストあるいは大半のホストに接続不可能でないかどうかを確認してください。

- ファイアウォールの権限を確認します。

アプライアンスが正しく機能するためには、ポート 20、21、22、23、25、53、80、123、443、および 628 を開く必要がある場合があります（「ファイアウォール情報」を参照）。

- ネットワーク上のアプライアンスから、`dnscheck@ironport.com` に対して電子メールを送信します。

システムの基本的な DNS チェックを実行するために、ネットワーク内から `dnscheck@ironport.com` に電子メールを送信します。オートレスポンドによる電子メールによって、次の 4 つのテストについての結果と詳細が返されます。

**DNS PTR レコード** : Envelope From の IP アドレスがドメインの PTR レコードと一致するか。

**DNS A レコード** : ドメインの PTR レコードが Envelope From の IP アドレスと一致するか。

**HELO マッチ** : SMTP HELO コマンドにリストされたドメインが、Envelope From の DNS ホスト名と一致するか。

**遅延バウンス メッセージを受け入れるメールサーバ** : SMTP HELO コマンドのリストにあるドメインに、そのドメインの IP アドレスを解決する MX レコードがあるか。

## リスナーのトラブルシューティング

電子メールのインジェクションに問題があると疑われる場合は、次の方法を使用します。

- インジェクションを行っている IP アドレスを確認し、`listenerconfig` コマンドを使用して許可されているホストを確認します。

作成したリスナーに接続できるような IP アドレスが許可されていますか。`listenerconfig` コマンドを使用して、リスナーのホスト アクセス テーブル (HAT) を確認します。次のコマンドを使用して、リスナーの HAT を出力します。

```
listenerconfig -> edit -> listener_number -> hostaccess -> print
```

HAT は、IP アドレス、IP アドレスのブロック、ホスト名、ドメインなどを使用して、接続を拒否するよう設定できます。詳細については、「接続が許可されているホストの指定」(P.107) を参照してください。

また、limits サブコマンドを使用して、リスナーに許可されている接続の最大数を確認することもできます。

```
listenerconfig -> edit -> listener_number -> limits
```

- インジェクションを行っているマシンから、Telnet または FTP を使用して、アプライアンスに手動で接続します。次に例を示します。

```
injection_machine% telnet appliance_name
```

アプライアンス内で telnet コマンドを使用して、リスナーから実際のアプライアンスに接続することもできます。

```
mail3.example.com> telnet
```

```
Please select which interface you want to telnet from.
```

```
1. Auto
```

```
2. Management (192.168.42.42/24: mail3.example.com)
```

```
3. PrivateNet (192.168.1.1/24: mail3.example.com)
```

```
4. PublicNet (192.168.2.1/24: mail3.example.com)
```

```
[1]> 3
```

```
Enter the remote hostname or IP.
```

```
[> 193.168.1.1
```

```
Enter the remote port.
```

```
[25]> 25
```

```
Trying 193.168.1.1...
```

```
Connected to 193.168.1.1.
```

```
Escape character is '^]'.


```



あるインターフェイスから他のインターフェイスに接続できない場合は、アプライアンスの Management、Data1、Data2 インターフェイスからネットワークに接続している方法に問題がある可能性があります。telnet を使用して接続を試みている場合は、ターゲットとするインターフェイスで telnet サービスがイネーブルになっていることを確認してください。詳細については、付録 A 「アプライアンスへのアクセス」を参照してください。また、リスナーのポート 25 に対して telnet を実行して、SMTP コマンドを手動で入力することもできます（このプロトコルを熟知している場合）。

- IronPort のテキスト メール ログおよびインジェクション デバッグ ログを調べて、受信エラーがあるかどうかを確認します。

インジェクション デバッグ ログには、アプライアンスと、システムに接続している指定のホスト間の SMTP 会話が記録されます。インジェクション デバッグ ログは、インターネットから接続を開始するクライアントとアプライアンス間の通信に関する問題をトラブルシューティングするのに役立ちます。このログでは、2 つのシステム間で伝送されたすべてのバイトが記録され、接続ホストに「送信」または接続ホストから「受信」に分類されます。

詳細については、「IronPort テキスト メール ログの使用」(P.34-10) および「IronPort インジェクション デバッグ ログの使用」(P.34-24) を参照してください。

## アプライアンスからの電子メール配信のトラブルシューティング

アプライアンスからの電子メールの配信に問題があると疑われる場合は、次の方法を試してください。

- 問題がドメインに限定されたものであるかどうかを判断します。

tophosts コマンドを使用して、電子メール キューに関する直近の情報を入手して、特定の受信者のドメインに配信の問題が生じていないかを確認します。

「Active Recipients」の順にソートすると、問題のあるドメインが返されますか。

「Connections Out」の順にソートしたとき、リスナーに指定されている最大接続数に達しているドメインがありますか。リスナーに対するデフォルトの最大接続数は 600 です。システム全体でのデフォルトの最大接続数は 10,000 です (deliveryconfig コマンドで設定します)。リスナーに対する最大接続数は、次のコマンドで確認できます。

```
listenerconfig -> edit -> listener_number -> limits
```

リスナーに対する接続が、destconfig コマンドによってさらに制限されていませんか（システムの最大数または仮想ゲートウェイ アドレスによる）。destconfig による接続の制限を確認するには、次のコマンドを使用します。

```
destconfig -> list
```

- hoststatus コマンドを使用します。

tophosts コマンドの結果として得られたリストの最上位のドメインに対して hoststatus コマンドを実行し、詳しく調べます。

ホストが使用可能で、接続を受け入れていませんか。

指定したホストに対する特定の MX レコードのメール サーバに問題がありませんか。

hoststatus コマンドでは、特定のホストに対する 5XX エラー (Permanent Negative Completion Reply) がある場合に、ホストから返された直前の「5XX」のステータス コードと説明が表示されます。このホストに対する直前の発信 TLS 接続が失敗した場合は、hoststatus コマンドで失敗した理由が表示されます。

- ドメインのデバッグ、バウンス、およびテキストメールの各ログを設定および確認して、受信ホストが使用可能かどうかをチェックします。

**ドメイン デバッグ ログ**には、アプライアンスと指定の受信者ホスト間の SMTP 会話でのクライアントとサーバの通信が記録されます。このタイプのログ ファイルは、特定の受信ホストに関する問題のデバッグに使用できます。

詳細については、「[IronPort ドメイン デバッグ ログの使用](#)」(P.34-23) を参照してください。

**バウンス ログ**には、バウンスされた各受信者に関するすべての情報が記録されます。

詳細については、「[IronPort バウンス ログの使用](#)」(P.34-18) を参照してください。

**テキスト メール ログ**には、電子メールの受信、電子メールの配信、およびバウンスの詳細が記録されます。ステータス情報も、1 分ごとにメール ログに書き込まれます。これらのログは、特定のメッセージの配信を理解し、システム パフォーマンスを分析するうえで有益な情報源となります。

詳細については、「[IronPort テキスト メール ログの使用](#)」(P.34-10) を参照してください。

- telnet コマンドを使用して、アプライアンスから問題のあるドメインに接続します。

```
mail3.example.com> telnet

Please select which interface you want to telnet from.

1. Auto

2. Management (192.168.42.42/24: mail3.example.com)

3. PrivateNet (192.168.1.1/24: mail3.example.com)

4. PublicNet (192.168.2.1/24: mail3.example.com)

[1]> 1

Enter the remote hostname or IP.

[]> problemdomain.net

Enter the remote port.

[25]> 25
```

- 必要に応じて `tlsverify` コマンドを使用して発信 TLS 接続を確立し、宛先ドメインに関する TLS 接続の問題をデバッグすることができます。接続を確立するには、検証するドメインと宛先ホストを指定します。AsyncOS では、必要な (検証) TLS 設定に基づいて TLS 接続を確認します。

```
mail3.example.com> tlsverify

Enter the TLS domain to verify against:
```

```
[]> example.com
```

Enter the destination host to connect to. Append the port (example.com:26) if you are not connecting on port 25:

```
[example.com]> mxe.example.com:25
```

```
Connecting to 1.1.1.1 on port 25.
```

```
Connected to 1.1.1.1 from interface 10.10.10.10.
```

```
Checking TLS connection.
```

```
TLS connection established: protocol TLSv1, cipher RC4-SHA.
```

```
Verifying peer certificate.
```

```
Verifying certificate common name mxe.example.com.
```

```
TLS certificate match mxe.example.com
```

```
TLS certificate verified.
```

```
TLS connection to 1.1.1.1 succeeded.
```

```
TLS successfully connected to mxe.example.com.
```

```
TLS verification completed.
```

## パフォーマンスのトラブルシューティング

アプライアンスのパフォーマンスに関する問題があると疑われる場合は、次の方法を使用してください。

- `rate` コマンドと `hostrate` コマンドを使用して、現在のシステムのアクティビティを確認します。  
`rate` コマンドは、電子メール動作に関するリアルタイム モニタリング情報を返します。詳細については、「[リアルタイム アクティビティの表示](#)」(P.30-17) を参照してください。  
`hostrate` コマンドは、特定のメール ホストに関するリアルタイムのモニタリング情報を返します。
- `status` コマンドを使用して、これまでのレートを比較して、状態の悪化を確認します。
- `status detail` コマンドを使用して、メモリの使用率を確認します。  
`status detail` コマンドを使用すると、システムのメモリ、CPU、ディスク I/O の使用率を、素早く確認できます。



(注)

メモリの使用率は、常に 75 % 未満である必要があります。メモリの使用率が 75 % を超えると、アプライアンスは「リソース節約モード」に入ります。これによって「バックオフ」アルゴリズムが起動され、リソースのオーバーサブスクリプションが防止され、電子メールによる次のアラートが送信されません。

```
This system (hostname: hostname) has entered a 'resource conservation' mode in order to prevent the rapid depletion of critical system resources.
```

```
RAM utilization for this system has exceeded the resource conservation threshold of 75%. The allowed injection rate for this system will be gradually decreased as RAM utilization approaches 85%.
```

この状況は、配信機能が低下していて、大量のインジェクションが行われているときにのみ発生します。メモリの使用率が 75 % を超えたときには、キュー内のメッセージの数を調べて、特定のドメインがダウン状態または配信不可能になっていないかどうかを確認します (hoststatus コマンドまたは hostrate コマンドを使用します)。また、システムのステータスも確認して、配信が中断されないようにします。インジェクションが停止しても、依然としてメモリの使用率が高い場合は、Cisco カスタマー サポートにご連絡ください。「[シスコのテクニカルサポート](#)」(P.1-7) を参照してください。

- 問題が 1 つのドメインに限定されていますか。

tophosts コマンドを使用して、電子メール キューに関する直近の情報を入手して、特定の受信者のドメインに配信の問題が生じていないかを確認します。

キューのサイズを確認します。このサイズを制御したり、問題が生じている特定のドメインの受信者に対処するために、電子メール キューにあるメッセージを削除、バウンス、中断、またはリダイレクトすることができます。詳細については、「[電子メール キューの管理](#)」(P.30-24) を参照してください。以下のコマンドを使用します。

- deleterecipients
- bouncerecipients
- redirectrecipients
- suspenddel / resumedel
- suspendlistener / resumelister

tophosts コマンドを使用して、ソフトバウンスおよびハードバウンスの数を確認します。[Soft Bounced Events] (オプション 4) または [Hard Bounced Recipients] (オプション 5) でソートします。特定のドメインに対するパフォーマンスに問題があることが疑われる場合は、上記のコマンドを使用して、そのドメインへの配信を制御します。

## アプライアンスの電源のリモートリセット

アプライアンスのハードリセットが必要な場合は、サードパーティの Platform Management (IPMI) ツールを使用してアプライアンス シャーシをリモートからリブートできます。

### 制約事項

- リモート電源管理は、特定のハードウェアでのみ使用できます。

詳細については、「[リモート電源管理のイネーブル化](#)」(P.29-24) を参照してください。

- この機能を使用する場合は、使用が必要になる前に、あらかじめ有効にしておく必要があります。詳細は、「リモート電源管理のイネーブル化」(P.29-24) を参照してください。
- 次の IPMI コマンドのみがサポートされています。  
status、on、off、cycle、reset、diag、soft  
サポートされていないコマンドを発行すると、「権限不足」エラーが生成されます。

#### はじめる前に

- IPMI バージョン 2.0 を使用してデバイスを管理できるユーティリティを取得し、設定します。
- サポートされている IPMI コマンドの使用方法を理解します。IPMI ツールのマニュアルを参照してください。

#### 手順

- ステップ 1** IPMI を使用して、必要なクレデンシャルとともに、先に設定したリモート電源管理ポートに割り当てられた IP アドレスに、サポートされている電源の再投入コマンドを発行します。
- たとえば、IPMI をサポートする UNIX タイプのマシンからは、次のようなコマンドを発行します。
- ```
ipmitool -I lan -H 192.0.2.1 -U remoteresetuser -P password chassis power reset
```
- ここで、192.0.2.1 は、リモート電源管理ポートに割り当てられた IP アドレスで、remoteresetuser および password は、この機能を有効にしたときに入力したクレデンシャルです。
- ステップ 2** アプライアンスが再起動されるまで、少なくとも 5 分間待ちます。

テクニカル サポートの使用

- 「サポート事例を開くまたは更新する」(P.36-29)
- 「シスコのテクニカル サポート担当者のリモート アクセスのイネーブル化」(P.36-30)
- 「パケット キャプチャの実行」(P.36-33)

サポート事例を開くまたは更新する

はじめる前に



(注)

緊急のサポートが必要な場合は、この方法を使用しないでください。その場合、電話を使用します。詳細については、「シスコのテクニカル サポート」(P.1-7) を参照してください。

- 緊急の問題の場合、この方法は使用しないでください。代わりに、「シスコのテクニカル サポート」(P.1-7) に示されるその他の方法の 1 つを使用してサポートください。
次の手順は、情報が必要であるまたは回避策があるけれども代替策を使用したいといった問題に限り使用します。
- ヘルプに関しては別の選択肢を検討してみてください。
 - 「Knowledge Base」(P.1-6)

– 「Cisco サポート コミュニティ」 (P.1-7)

- この手順を使用してサポート事例を開くと、アプライアンスの設定ファイルがシスコ カスタマーサポートに送信されます。アプライアンスの設定を送信したくない場合、別の方法を使用してカスタマー サポートにお問い合わせください。
- アプライアンスがインターネットに接続され電子メールを送信する必要があります。
- 既存の事例に関する情報を送信する場合は、ケース番号を確認してください。

手順

- ステップ 1** アプライアンスにログインします。
- ステップ 2** [ヘルプとサポート (Help and Support)] > [テクニカル サポートに問い合わせる (Contact Technical Support)] を選択します。
- ステップ 3** サポート リクエストの受信者を設定します。

| | |
|------------------------|---|
| 要求をシスコのカスタマー サポートに送信する | [Cisco IronPort カスタマーサポート (Cisco IronPort Customer Support)] チェックボックスを選択します。 |
| 内部サポート デスクにだけ要求を送信する | <ul style="list-style-type: none"> • [Cisco IronPort カスタマーサポート (Cisco IronPort Customer Support)] チェックボックスをオフにします。 • サポート デスクの電子メール アドレスを入力します。 |
| (任意) 他の受信者を追加する | 電子メール アドレスを入力します。 |

- ステップ 4** フォームに入力します。
- ステップ 5** [送信 (Send)] をクリックします。

シスコのテクニカル サポート担当者のリモート アクセスのイネーブル化

シスコのカスタマー アシスタンスのみ、次の方法を使用してアプライアンスにアクセスできます。

- 「インターネット接続されたアプライアンスへのリモート アクセスのイネーブル化」 (P.36-30)
- 「インターネットに直接接続されていないアプライアンスへのリモート アクセスのイネーブル化」 (P.36-31)
- 「テクニカル サポートのトンネルのディセーブル化」 (P.36-32)
- 「リモート アクセスの無効化」 (P.36-32)
- 「サポートの接続状態の確認」 (P.36-33)

インターネット接続されたアプライアンスへのリモート アクセスのイネーブル化

サポートは、この手順でアプライアンスと `upgrades.ironport.com` のサーバ間で作成される SSH トンネル経由でアプライアンスにアクセスします。

はじめる前に

インターネットから到達可能なポートを識別します。デフォルトでは、ポート 25 です。システムは、電子メール メッセージを送信するために、このポートを介して一般的なアクセスを行う必要があるため、このポートは大部分の環境で機能します。このポート経由の接続は、ほとんどのファイアウォール設定で許可されます。

手順

-
- ステップ 1** アプライアンスへのログイン
- ステップ 2** GUI ウィンドウの右上にある、[ヘルプとサポート (Help and Support)] > [リモート アクセス (Remote Access)] を選択します。
- ステップ 3** [有効 (Enable)] をクリックします。
- ステップ 4** 情報を入力します。

| オプション | 説明 |
|--|---|
| カスタマー サポート パスワード (Customer Support Password) | この仮パスワードおよび (物理アプライアンスの場合) アプライアンスのシリアル番号または (仮想アプライアンスの場合) VLN は、サポートにアクセスするためのパスワードを生成するために使用されます。 |
| セキュア トンネル (Secure Tunnel) | リモート アクセス接続にセキュア トンネルを使用するために、このチェックボックスをオンにします。

接続ポートを入力します。

デフォルトでは、ポート 25 です。このポートは大部分の環境で機能します。 |

- ステップ 5** [送信 (Submit)] をクリックします。
-

次の作業

サポート担当者のリモート アクセスが必要なくなったときは、「[テクニカル サポートのトンネルのディセーブル化](#)」(P.36-32) を参照してください。

インターネットに直接接続されていないアプライアンスへのリモート アクセスのイネーブル化

インターネットに直接接続されていないアプライアンスの場合、インターネットに接続されている第 2 のアプライアンスを介してアクセスされます。

はじめる前に

- アプライアンスは、インターネットに接続されている第 2 のアプライアンスにポート 22 で接続する必要があります。
- インターネットに接続されているアプライアンスで該当のアプライアンスへのサポート トンネルを作成するには、「[インターネット接続されたアプライアンスへのリモート アクセスのイネーブル化](#)」(P.36-30) の手順を実行します。

手順

-
- ステップ 1** サポートが必要なアプライアンスのコマンドライン インターフェイスから、`techsupport` コマンドを入力します。
- ステップ 2** `sshaccess` と入力します。
- ステップ 3** プロンプトに従います。
-

次の作業

サポート担当者のリモート アクセスが必要なくなったときは、次のトピックを参照してください。

- 「リモート アクセスの無効化」(P.36-32)
- 「テクニカル サポートのトンネルのディセーブル化」(P.36-32)

テクニカル サポートのトンネルのディセーブル化

イネーブルにした `techsupport` トンネルは、`upgrades.ironport.com` に 7 日間接続されたままになります。その後、確立された接続は切断されませんが、いったん切断されるとトンネルに再接続できません。

トンネルを手動で無効にします。

手順

-
- ステップ 1** アプライアンスへのログイン
- ステップ 2** GUI ウィンドウの右上にある、[ヘルプとサポート (Help and Support)] > [リモート アクセス (Remote Access)] を選択します。
- ステップ 3** [無効 (Disable)] をクリックします。
-

リモート アクセスの無効化

`techsupport` コマンドを使用して作成したリモート アクセス アカウントは、非アクティブ化されるまでアクティブのままです。

手順

-
- ステップ 1** コマンドライン インターフェイスから、`techsupport` コマンドを入力します。
- ステップ 2** `sshaccess` と入力します。
- ステップ 3** `disable` と入力します。
-

サポートの接続状態の確認

手順

-
- ステップ 1** コマンドライン インターフェイスから、`techsupport` コマンドを入力します。
- ステップ 2** `status` と入力します。
-

パケット キャプチャの実行

パケット キャプチャは、サポート担当者が TCP/IP データおよびその他にアプライアンスから出入りするパケットを表示できるようにします。これはネットワーク設定をデバッグしたり、どのようなネットワークトラフィックがアプライアンスに到達または送出されているかを検出することができます。

手順

-
- ステップ 1** [ヘルプとサポート (Help and Support)] > [パケット キャプチャ (Packet Capture)] を選択します。
- ステップ 2** パケット キャプチャ設定の指定
- a. [パケット キャプチャ設定 (Packet Capture Settings)] セクションで、[設定を編集 (Edit Settings)] をクリックします。
 - b. (任意) パケット キャプチャの期間、制限およびフィルタを入力します。
サポート担当者が、これらの設定の方法を説明する場合があります。
時間の単位を指定しないでキャプチャ期間を入力すると、AsyncOS はデフォルトで秒を使用します。
[フィルタ (Filters)] セクションで次を実行します。
 - カスタム フィルタは、UNIX の `tcpdump` コマンドでサポートされた任意の構文 (`host 10.10.10.10 && port 80` など) を使用できます。
 - クライアント IP は、電子メールセキュリティ アプライアンスを介してメッセージを送信するメール クライアントなどのアプライアンスに接続しているマシンの IP アドレスです。
 - サーバ IP は、アプライアンスがメッセージを配信する Exchange サーバなどのアプライアンスが接続しているマシンの IP アドレスです。
クライアントとサーバの IP アドレスを使用して、中間に電子メールセキュリティ アプライアンスがある特定のクライアントと特定のサーバ間のトラフィックを追跡できます。
 - c. [送信 (Submit)] をクリックします。
- ステップ 3** [キャプチャを開始 (Start Capture)] をクリックします。
- キャプチャは一度に 1 つだけ実行できます。
 - パケット キャプチャが実行されている場合、[パケット キャプチャ (Packet Capture)] ページには、実行中のキャプチャのステータス (ファイル サイズや経過時間などの現在の統計情報) が表示されます。
 - GUI に表示されるのは GUI で開始されたパケット キャプチャだけで、CLI で開始されたパケット キャプチャは表示されません。同様に、CLI には CLI で開始された現在のパケット キャプチャのステータスだけが表示されます。

- パケット キャプチャ ファイルは 10 個の部分に分割されます。パケット キャプチャが終了する前にパケット キャプチャ ファイルが最大サイズ制限に到達した場合は、そのファイルの最も古い部分が削除され (データが破棄されます)、現在のパケット キャプチャ データで新しい部分が開始されます。パケット キャプチャ ファイルは一度に 1/10 だけ破棄されます。
- GUI で開始されたキャプチャはセッション間で維持されます。(CLI で実行したキャプチャは、セッションが終了したときに停止します)。

ステップ 4 キャプチャを指定した期間実行するようにします。またはキャプチャを無期限に実行する場合、[キャプチャを停止 (Stop Capture)] をクリックして停止します。

ステップ 5 パケット キャプチャ ファイルへアクセスします。

- [パケット キャプチャ ファイルの管理 (Manage Packet Capture Files)] リストでファイルをクリックして、[ファイルのダウンロード (Download File)] をクリックします。
- アプライアンスの captures サブ ディレクトリ内のファイルにアクセスするには、FTP または SCP を使用します。

次の作業

サポートでファイルを使用できるようにします。

- アプライアンスへのリモート アクセスを許可した場合、Technician が FTP または SCP を使用してパケット キャプチャ ファイルにアクセスできます。[「シスコのテクニカル サポート担当者のリモート アクセスのイネーブル化」 \(P.36-30\)](#) を参照してください。
- 電子メールでファイルをサポートに送信します。



CHAPTER 37

D-Mode を使用した発信メール配信アプライアンスの最適化

- 「機能の概要：最適化された発信配信の D-Mode」 (P.37-1)
- 「最適化された発信メール配信のアプライアンスの設定」 (P.37-3)
- 「IronPort Mail Merge (IPMM) を使用した大量のメールの送信」 (P.37-4)

機能の概要：最適化された発信配信の D-Mode

D-Mode は、特定の電子メール セキュリティ アプライアンスを発信メール配信向けに最適化する、キーでイネーブルにされる機能です。着信メール処理に特有の機能は、D-Mode ではディセーブルになっています。

- 「D-Mode-enabled アプライアンス特有の機能」 (P.37-1)
- 「D-Mode-enabled アプライアンスでディセーブルになっている標準機能」 (P.37-2)
- 「D-Mode-enabled アプライアンスに適用される標準機能」 (P.37-2)

D-Mode-enabled アプライアンス特有の機能

- 256 の仮想ゲートウェイ アドレス：Cisco Virtual Gateway テクノロジーを使用すると、個別の IP アドレス、ホスト名およびドメインを使用してホストするすべてのドメインのエンタープライズメール ゲートウェイを設定し、同じ物理アプライアンス内でホストしながら、これらのドメインの個別の企業電子メール ポリシー拡張およびアンチスパム方針を作成できます。第 5 章「電子メールを受信するためのゲートウェイの設定」にある「リスナーのカスタマイズ」に関する情報を参照してください。
- IronPort Mail Merge (IPMM)：IronPort Mail Merge (IPMM) を使用すると、個別の個人向けメッセージをカスタマー システムから生成する手間を省くことができます。ユーザは、数千の個別メッセージを生成し、メッセージ生成システムと電子メール ゲートウェイ間で送信する必要がなくなるため、システムにかかる負荷が軽減され、電子メール配信のスループットが向上します。詳細については、「IronPort Mail Merge (IPMM) を使用した大量のメールの送信」 (P.37-4) を参照してください。
- リソースを節約するバウンス設定：D-Mode-enabled アプライアンスを設定して、ブロックされている可能性のある宛先を検出し、その宛先へのすべてのメッセージをバウンスできます。詳細については、「リソースを節約するバウンス設定の指定」 (P.37-3) を参照してください。
- 発信配信のパフォーマンスの向上

D-Mode-enabled アプライアンスでディセーブルになっている標準機能

- IronPort Anti-Spam スキャンおよびオン/オフボックス スпам隔離：アンチスパム スキャンは、通常、着信メールに関係するため、IronPort Anti-Spam スキャン エンジンがディセーブルにされません。したがって、スパム対策の章は適用されません。
- アウトブレイク フィルタ：アウトブレイク フィルタは、着信メールの隔離に使用されるため、D-Mode-enabled アプライアンスではディセーブルになっています。したがって、アウトブレイク フィルタの章の情報は適用されません。
- SenderBase Network Participation 機能：SenderBase Network Participation は、着信メールに関する情報を報告するため、D-Mode-enabled アプライアンスではディセーブルになっています。したがって、SenderBase Network Participation に関する情報は適用されません。
- レポート：レポート機能は限定されます。一部のレポートは使用できません。発生するレポートも、パフォーマンス上の理由により、非常に限定的なレベルで実行するように設定されています。



(注) D-Mode-enabled アプライアンスの電子メールセキュリティ モニタ概要レポートに示される合計には、これらの機能が D-Mode-enabled アプライアンスでディセーブルにされている場合でも、スパム、および陽性と疑わしいスパムの数が、誤って含まれる可能性があります。

- RSA Data Loss Prevention：発信メッセージの RSA DLP スキャンは、D-Mode-enabled アプライアンスでディセーブルになっています。

D-Mode-enabled アプライアンスに適用される標準機能

表 37-1 D-Mode-enabled アプライアンスに含まれる AsyncOS 機能

| 機能 | 追加情報 |
|------------------------------------|--|
| アンチウイルス スキャン (Anti-virus scanning) | 第 12 章「アンチウイルス」を参照してください。 |
| DomainKeys 署名 | DKIM/DomainKeys は、送信者により使用される署名キーに基づいて電子メールの信頼性を確認する方式です。第 17 章「電子メール認証」を参照してください。 |
| 集中管理 | 第 35 章「クラスタを使用した中央集中型管理」を参照してください。 |
| 配信スロットリング | 各ドメインに対して、一定期間でシステムが超えることができない、接続および受信者の最大数を割り当てることができます。「グッド ネイバー」テーブルは、destconfig コマンドで定義されます。
詳細については、「送信先コントロールによる電子メール配信の管理」(P.21-43) を参照してください。 |
| バウンス検証 | バウンス メッセージの信頼性を検証します。「Cisco バウンス検証」(P.21-51) を参照してください。 |
| 委任管理 | 第 28 章「管理タスクの分散」を参照してください。 |

表 37-1 D-Mode-enabled アプライアンスに含まれる AsyncOS 機能 (続き)

| 機能 | 追加情報 |
|--------------------|---|
| トレース (デバッグ) | 「テストメッセージを使用したメールフローのデバッグ: トレース」(P.36-1) を参照してください。 |
| VLAN、NIC ペアリング | 第 33 章「高度なネットワーク構成」を参照してください。 |
| オプションのアンチウイルス エンジン | オプションのアンチウイルス スキャンを追加することで、アウトバウンドメッセージの完全性を保証できます。「アンチウイルス スキャンの概要」(P.12-1) を参照してください。 |

最適化された発信メール配信のアプライアンスの設定

手順

- ステップ 1** 提供されているライセンス キーを適用します。 *System Setup Wizard* を実行する前 (アプライアンスを設定する前) に、このキーを Cisco 電子メール セキュリティ アプライアンスに適用する必要があります。キーの適用は、[システム管理 (System Administration)] > [ライセンス キー (Feature Key)] ページを介して、または CLI の `featurekey` コマンドを入力して行います。



(注) 前述のライセンス キーには、サンプルの Sophos または McAfee Anti-Virus の 30 日間ライセンスが含まれています。これは、アウトバウンドメールでのアンチウイルス スキャンのテストに使用できます。

- ステップ 2** アプライアンスを再起動します。
- ステップ 3** システム セットアップ ウィザード (GUI または CLI) を実行して、アプライアンスを設定します。発信メール配信用に最適化されたアプライアンスには、アンチスパム スキャンもアウトブレイク フィルタも含まれないことに注意してください。(コンフィギュレーション ガイドのこれらの章は無視してください)。



(注) クラスタ環境では、D-Mode 機能キーで設定されたアプライアンスを、配信パフォーマンス パッケージで設定されていない AsyncOS アプライアンスと組み合わせることはできません。

リソースを節約するバウンス設定の指定

最適化された発信メール配信向けにアプライアンスを設定した後は、潜在的な配信問題を検出し、特定の宛先へのすべてのメッセージをバウンスするようにシステムを設定できます。



(注) この設定を使用すると、配信不能と見なされる宛先ドメインのキューのすべてのメッセージがバウンスされます。メッセージは、配信問題が解決された後で再送信する必要があります。

リソースを節約するバウンス設定をイネーブルにする例

```
mail3.example.com> bounceconfig
```

```
Choose the operation you want to perform:
```

- NEW - Create a new profile.
- EDIT - Modify a profile.
- DELETE - Remove a profile.
- SETUP - Configure global bounce settings.

```
[ ]> setup
```

```
Do you want to bounce all enqueued messages bound for a domain if the host is down? [N]>
y
```

この機能を使用する場合、最新の接続試行が 10 回連続で失敗すると、ホストは「ダウン」と見なされます。AsyncOS は、ダウン ホストを 15 分ごとにスキャンします。そのため、接続は、キューがクリアされる前に 11 回以上試行されます。

IronPort Mail Merge (IPMM) を使用した大量のメールの送信



(注) IronPort Mail Merge は、D-Mode-enabled アプライアンスでのみ使用可能です。

IronPort Mail Merge の概要

IronPort Mail Merge を使用すると、個別の個人向けメッセージをカスタマー システムから生成する手間を省くことができます。ユーザは、数千の個別メッセージを生成し、メッセージ生成システムと電子メール ゲートウェイ間で送信する必要がなくなるため、システムにかかる負荷が軽減され、電子メール配信のスループットが向上します。

IPMM では、個人向けに置換されるメッセージの場所を表す変数を使用して、各メッセージの本文が作成されます。各メッセージ受信者に対して、受信電子メール アドレスおよび変数置換だけを電子メール ゲートウェイに送信する必要があります。また、IPMM を使用して、受信者に応じて、送信するメッセージの本文の特定の「パーツ」を含めたり、除外したりできます (たとえば、2 つの異なる国の受信者に送信するメッセージの最後に異なる著作権宣言文を含めることができます)。

Mail Merge 機能の利点

- メール管理者にとって使いやすい。IPMM は、変数置換および一般的な多くの言語の抽象化インターフェイスを提供するため、各受信者の個人向けメッセージを簡単に作成できます。
- メッセージ生成システムの負荷を軽減する。メッセージ本文の 1 つのコピーと必須の置換のテーブルだけが必要であるため、ほとんどのメッセージ生成「作業」をメッセージ生成システムから、最適化された発信メール配信向けに設定されたアプライアンスに移行して、負荷を軽減できます。
- 配信スループットが改善される。数千の着信メッセージを受け取り、キューに入れるために必要なリソースを軽減することで、Cisco アプライアンスは、アウトバウンド配信パフォーマンスを大幅に改善できます。
- キューストレージの効率性が向上する。各メッセージ受信に保存する情報を減らすことで、ユーザは、D-Mode-enabled アプライアンスのキューストレージの使用効率を大幅に向上できます。

Mail Merge の使用

SMTP インジェクション

IPMM は、SMTP をトランスポート プロトコルとして拡張します。アプライアンスで行う特別な設定は必要ありません (デフォルトでは、IPMM は、プライベート リスナーでイネーブルにして、D-Mode-enabled アプライアンスのパブリック リスナーでディセーブルにできます)。ただし、現在、SMTP をインジェクション プロトコルとして使用していない場合は、D-Mode-enabled アプライアンス インターフェイスを介して SMTP を利用する新しいプライベート リスナーを作成する必要があります。

listenerconfig の setipmm サブコマンドを使用して、リスナーで IPMM をイネーブルにします。詳細については、第 5 章「電子メールを受信するためのゲートウェイの設定」を参照してください。

IPMM は、MAIL FROM と DATA の 2 つのコマンドを変更し、XDFN を追加することで、SMTP を変更します。MAIL FROM コマンドは XMRG FROM に、DATA コマンドは XPRT に置き換えられています。

Mail Merge メッセージを生成するには、メッセージの生成に使用されるコマンドを特定の順序で発行する必要があります。

1. 送信ホストを示す、初期 EHLO ステートメント。
2. 各メッセージは、送信者アドレスを示す、XMRG FROM: ステートメントで始まります。
3. 各受信者は、次のように定義されます。
 - 1 つ以上の XDFN 変数割り当てステートメントが含まれます。これには、パーツ定義 (XDFN *PART=1,2,3...) やその他の任意の受信者固有の変数が含まれます。
 - 受信者電子メールアドレスは、RCPT TO: ステートメントで定義されます。RCPT TO: の前にあり、前述の XMRG FROM または RCPT TO コマンドの後にある任意の変数割り当ては、この受信者電子メールアドレスにマッピングされます。
4. 各パーツは、XPRT n コマンドを使用して定義されます。各パーツは、DATA コマンドと同様にピリオド (.) 文字で終了します。最後のパーツは、XPRT n LAST コマンドで定義されます。

変数置換

メッセージ ヘッダーなど、メッセージ本文の任意のパーツに、置換用の変数を含めることができます。変数は、HTML メッセージにも表示できます。変数は、ユーザが定義し、アンパサンド (&) 文字で始まり、セミコロン (;) で終了する必要があります。アスタリスク (*) で始まる変数名は、予約されているため使用できません。

予約変数

IPMM には、事前に定義されている 5 つの特殊な「予約」変数が含まれます。

表 37-2 IPMM : 予約変数

| | |
|--------|--|
| *FROM | 予約変数 *FROM は、「Envelope From」パラメータから派生します。「Envelope From」パラメータは、「XMRG FROM:」コマンドにより設定されます。 |
| *TO | 予約変数 *TO は、「RCPT TO:」コマンドで設定される、エンベロープ受信者値から派生します。 |
| *PARTS | 予約変数 *PARTS は、パーツのカンマ区切りリストを含みます。これは、「RCPT TO:」で受信者を定義する前に設定され、特定のユーザが受信する「XPRT n」メッセージ本文ブロックを決定します。 |
| *DATE | 予約変数 *DATE は、現在の日付スタンプに置き換えられます。 |
| *DK | 予約変数 *DK は、DomainKeys 署名プロファイルの指定に使用されます（このプロファイルはすでに AsyncOS に存在している必要があります）。DomainKeys 署名プロファイルの作成の詳細については、第 17 章「電子メール認証」を参照してください。 |

メッセージの例 1

次の例のメッセージ本文（ヘッダーを含む）には、最後のメッセージで置換される、4 つの異なる変数と 5 つの置換用の場所が含まれます。同じ変数がメッセージ本文で複数回使用されることがあるため注意してください。また、予約変数 `&*TO;` が使用されます。これは、受信者の電子メールアドレスに置換されます。この予約変数は、個別の変数として渡す必要はありません。次の例の変数は太字で示されています。

```
From: Mr.Spaceley <spaceley@example.com>
To: &first_name;;&last_name;;&*TO;
Subject: Thanks for Being an Example.Com Customer
```

```
Dear &first_name;,
```

```
Thank you for purchasing a &color; sprocket.
```

このメッセージは、アプライアンスに一度だけインジェクトする必要があります。各受信者に対して、次の追加情報が必要です。

- 受信者の電子メールアドレス
- 変数置換の名前と値のペア

パーツ アセンブリ

SMTP は、各メッセージ本文に単一の DATA コマンドを使用し、IPMM は、1 つ以上の XPRN コマンドを使用してメッセージを作成します。パーツは、受信者ごとに指定される順序に従ってアセンブルされます。各受信者は、任意またはすべてのメッセージ パーツを受信できます。パーツは、任意の順序でアセンブルできます。

特殊な変数 *PARTS は、パーツのカンマ区切りリストを含みます。

たとえば、次の例のメッセージでは、2 つのパーツが含まれます。

最初のパーツには、メッセージ ヘッダーとメッセージ本文の一部が含まれます。2 番目のパーツには、特別なカスタマー向けに含めることができる割引価格が含まれます。

メッセージの例 2 (パーツ 1)

```
From: Mr. Spacely <spacely@example.com>

To: &first_name; &last_name; &*TO;

Subject: Thanks for Being an Example.Com Customer

Dear &first_name;,

Thank you for purchasing a &color; sprocket.
```

メッセージの例 2 (パーツ 2)

```
Please accept our offer for 10% off your next sprocket purchase.
```

メッセージ部分は、アプライアンスに一度だけインジェクトする必要があります。この場合、各受信者に、次の追加情報が必要です。

- 最後のメッセージに含まれる、パーツの順序付きリスト
- 受信者の電子メール アドレス
- 変数置換の名前と値のペア

IPMM および DomainKeys 署名

IPMM は、DomainKeys 署名をサポートします。DomainKeys プロファイルを指定するには、*DK 予約変数を使用します。次の例を参考にしてください。

```
XDFN first_name="Jane" last_name="User" color="red" *PARTS=1,2 *DK=mass_mailing_1
```

この例では、「mail_mailing_1」は、前に設定した DomainKeys プロファイルの名前です。

コマンドの説明

クライアントは、IPMM メッセージをリスナーにインジェクトするときに、次のキー コマンドで拡張 SMTP を使用します。

XMRG FROM

構文：

```
XMRG FROM: <sender email address>
```

このコマンドは、SMTP MAIL FROM: コマンドの代わりに使用されます。これは、次に IPMM メッセージがあることを示します。IPMM ジョブは、XMRG FROM: コマンドで開始されます。

XDFN

構文：

```
XDFN <KEY=VALUE> [KEY=VALUE]
```

XDFN コマンドは、受信者別のメタデータを設定します。キーと値のペアは、オプションでかぎカッコまたは角カッコで囲むことができます。

*PARTS は、XPRT コマンド（以下を参照）で定義されているように、インデックス番号を示す特殊な予約変数です。*PARTS 変数は、整数のカンマ区切りリストとして分割されます。整数は、XPRT コマンドにより定義されているように送信される本文パーツと一致します。その他の予約変数には、*FROM、*TO および *DATE があります。

XPRT

構文：

```
XPRT index_number LAST
```

Message

.

XPRT コマンドは、SMTP DATA コマンドの代わりに使用されます。このコマンドは、コマンド入力後にメッセージパーツの送信者を受け取ります。コマンドは、行の末尾に単一のピリオドを付けて完了します（これは、SMTP DATA コマンドを完了する方法と同じです）。

特殊キーワード **LAST** は、Mail Merge ジョブの最後を示します。これは、インジェクトされる最後のパーツを指定するときに使用する必要があります。

LAST キーワードが使用されると、メッセージがキューに入り、配信が始まります。

変数定義に関する注意事項

- XDFN コマンドで変数を定義する場合、実際のコマンドラインは、システムの物理的制限を超えることはできないため注意してください。D-Mode-enabled アプライアンスの場合、この制限は、1 行あたり 4 KB です。ホストシステムによっては、しきい値がこれより低くなる場合があります。非常に長いコマンドラインで複数の変数を定義する場合は注意してください。

- 変数キーと値のペアを定義する場合、スラッシュ「/」文字を使用して、特殊文字をエスケープできます。これは、メッセージ本文に、誤って変数定義と置換される可能性がある HTML 文字エンティティが含まれる場合に役に立ちます（たとえば、文字エンティティ `™` は、商標文字の HTML 文字エンティティを定義します）。コマンド `XDFN trade=foo` を作成して、HTML 文字エンティティ「`™`」を含む IPMM メッセージを作成した場合、アセンブルされるメッセージには、商標文字ではなく、変数置換（「`foo`」）が含まれます。これは、GET コマンドを含む URL で使用されることがあるアンパサンド文字「`&`」の場合も同じです。

IPMM カンバセーションの例

次に、メッセージの例 2（前述の例）での IPMM カンバセーションの例を示します。このメッセージは、この例の 2 人の受信者「Jane User」および「Joe User」に送信されます。

この例では、太字フォントは、D-Mode-enabled アプライアンスとの手動による SMTP カンバセーションで入力する内容です。また、モノスペース タイプのフォントは、SMTP サーバからの応答を表し、イタリック体フォントは、コメントまたは変数を表します。

接続が確立されます。

```
220 ESMTD
```

```
EHLO foo
```

```
250-ehlo responses from the listener enabled for IPMM
```

カンバセーションが開始されます。

```
XMRG FROM:<user@domain.com> [Note: This replaces the MAIL FROM: SMTP command.]
```

```
250 OK
```

変数およびパーツが各受信者に設定されます。

```
XDFN first_name="Jane" last_name="User" color="red" *PARTS=1,2
```

```
[Note: This line defines three variables (first_name, last_name, and color) and then uses the *PARTS reserved variable to define that the next recipient defined will receive message parts numbers 1 and 2.]
```

```
250 OK
```

```
RCPT TO:<jane@company.com>
```

```
250 recipient <jane@company.com> ok
```

```
XDFN first_name="Joe" last_name="User" color="black" *PARTS=1
```

```
[Note: This line defines three variables (first_name, last_name, and color) and then uses the *PARTS reserved variable to define that the next recipient defined will receive message parts numbers 1 only.]
```

IronPort Mail Merge (IPMM) を使用した大量のメールの送信

```
RCPT TO:<joe@company1.com>
```

```
250 recipient <joe@company1.com> ok
```

次に、パーツ 1 が送信されます。

```
XPRT 1 [Note: This replaces the DATA SMTP command.]
```

```
354 OK, send part
```

```
From: Mr. Spacely <spacely@example.com>
```

```
To: &first_name; &last_name; &*TO;
```

```
Subject: Thanks for Being an Example.Com Customer
```

```
&*DATE;
```

```
Dear &first_name; ,
```

```
Thank you for purchasing a &color; sprocket.
```

.

次に、パーツ 2 が送信されます。LAST キーワードは、パーツ 2 がアセンブルする最後のパーツであることを示すときに使用されます。

```
XPRT 2 LAST
```

```
Please accept our offer for 10% off your next sprocket purchase.
```

.

```
250 Ok, mailmerge message enqueued
```

「250 Ok, mailmerge message queued」は、メッセージが受け取られたことを示します。

この例に基づいて、受信者 Jane User は、このメッセージを受信します。

```
From: Mr. Spacely <spacely@example.com>
```

```
To: Jane User <jane@company.com>
```

```
Subject: Thanks for Being an Example.Com Customer
```

message date

Dear Jane,

Thank you for purchasing a red sprocket.

Please accept our offer for 10% off your next sprocket purchase.

受信者 Joe User は、このメッセージを受信します。

From: Mr. Spacely <spacely@example.com>

To: Joe User <joe@company1.com>

Subject: Thanks for Being an Example.Com Customer

message date

Dear Joe,

Thank you for purchasing a black sprocket.

コード例

Cisco は、一般的なプログラミング言語でライブラリを作成して、IPMM メッセージを IPMM 対応の Cisco アプライアンス リスナーにインジェクトするタスクを抽象化します。IPMM ライブラリの使用例については、Cisco カスタマー サポートにお問い合わせください。コードは、構文説明のために広範囲にわたってコメント化されています。

■ IronPort Mail Merge (IPMM) を使用した大量のメールの送信



CHAPTER 38

Cisco コンテンツ セキュリティ管理アプライアンスの集中型サービス

- 「Cisco コンテンツ セキュリティ管理アプライアンス サービスの概要」 (P.38-1)
- 「ネットワーク プランニング」 (P.38-2)
- 「外部スパム隔離の設定」 (P.38-3)
- 「一元化されたポリシー、ウイルス、アウトブレイク隔離について」 (P.38-4)
- 「中央集中型レポートの設定」 (P.38-8)
- 「中央集中型メッセージ トラッキングの設定」 (P.38-9)
- 「中央集中型サービスの使用方法」 (P.38-10)

Cisco コンテンツ セキュリティ管理アプライアンス サービスの概要

シスコのコンテンツ セキュリティ管理アプライアンス (M-Series アプライアンス) は、複数の Cisco C-Series および X-Series 電子メール セキュリティ アプライアンス上の特定のサービスに対して一元化されたインターフェイスを提供する外部または「オフ ボックス」ロケーションです。

セキュリティ管理アプライアンス には、次の機能があります。

- 外部 Cisco スパム隔離。エンドユーザ向けのスパム メッセージおよび陽性と疑わしいスパム メッセージを保持しており、エンドユーザおよび管理者は、スパムとフラグ付けされたメッセージをレビューしてから最終的な決定を下すことができます。
- 一元化されたスパム、ポリシー、ウイルス、およびアウトブレイク隔離。アンチ ウイルス スキャン、アウトブレイク フィルタおよびポリシーにより隔離されたメッセージを保存し管理するために、ファイアウォールの内側の 1 つの場所を提供します。
- 中央集中型レポート。複数の電子メール セキュリティ アプライアンスから集約したデータに対してレポートを実行します。
- 中央集中型トラッキング。複数の電子メール セキュリティ アプライアンスを通過する電子メールを追跡します。

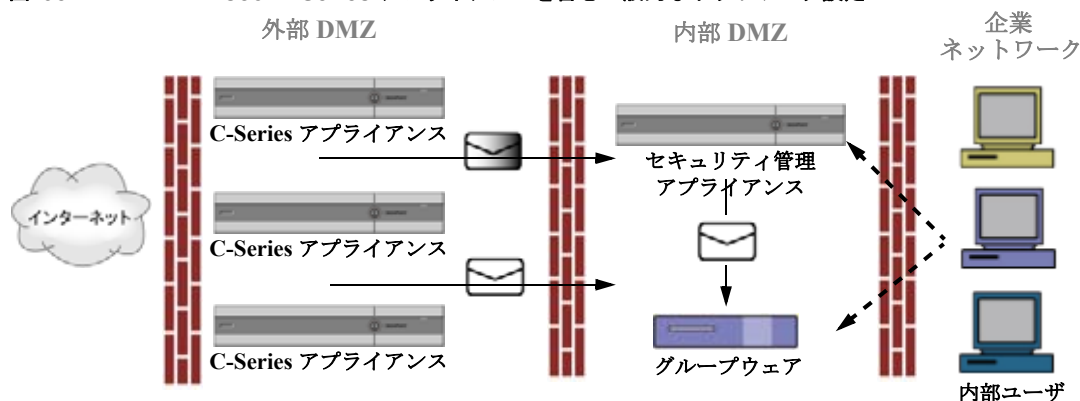
シスコのコンテンツ セキュリティ管理アプライアンスの設定および使用の詳細については、『Cisco Content Security Management Appliance User Guide』を参照してください。

ネットワーク プランニング

シスコのコンテンツセキュリティ管理アプライアンスを使用すると、エンドユーザ インターフェイス（メール アプリケーションなど）を、さまざまな DMZ 内のよりセキュアなゲートウェイ システムから切り離すことができます。2 層ファイアウォールの使用によって、ネットワーク プランニングの柔軟性が高まり、エンドユーザが外部 DMZ に直接接続することを防止できます。

図 38-1 に、セキュリティ管理アプライアンスと複数の DMZ を含む一般的なネットワーク設定を示します。

図 38-1 Cisco M-Series アプライアンスを含む一般的なネットワーク設定



大規模な企業データセンターでは、外部 Cisco スпам隔離として機能している 1 台のセキュリティ管理アプライアンスアプライアンスを、1 台または複数台の Cisco C-Series または X-Series アプライアンスで共有できます。さらに、ローカル使用のために独自のローカル Cisco アプライアンス隔離を保守するリモート オフィスをセットアップできます（C-Series または X-Series アプライアンス上でローカル Cisco スпам隔離を使用）。

メール フローおよび外部スпам隔離

ネットワークが図 38-1 の説明に従って設定される場合、インターネットからの着信メールは外部 DMZ の Cisco アプライアンスによって受信されます。正規のメールは、内部 DMZ のメール転送エージェント（MTA）（グループウェア）に従って、最終的に企業ネットワーク内のエンドユーザまで送信されます。

スпамおよび陽性と疑わしいスпам（メール フロー ポリシー設定値に基づく）は、セキュリティ管理アプライアンスのスпам隔離エリアに送信されます。次にエンドユーザが隔離エリアにアクセスして、スпамを削除し、自分宛に配信されるメッセージを解放することを選択できます。Cisco スпам隔離に残っているメッセージは、設定された期間後に自動的に削除されます（第 27 章「隔離」を参照）

メールは、他の Cisco（C-Series および X-Series）アプライアンスからセキュリティ管理アプライアンスアプライアンスに送信されます。セキュリティ管理アプライアンスにメールを送信するように設定された Cisco アプライアンスは、そのセキュリティ管理アプライアンスからリリースされるメールの受信を自動的に予測し、このようなメッセージを逆戻りして受信した場合は再処理を行いません。メッセージは、HAT などのポリシーやスキャン設定をバイパスして配信されます。これを機能させるために、セキュリティ管理アプライアンスの IP アドレスが変わらないようにしてください。セキュリティ管理アプライアンスの IP アドレスが変わると、受信側の C-Series または X-Series のアプライアンスは、メッセージを他の着信メッセージであるものとして処理します。セキュリティ管理アプライアンスの受信と配信では、常に同じ IP アドレスを使用する必要があります。

セキュリティ管理アプライアンスでは、Cisco スパム隔離設定で指定されている IP アドレスから隔離対象のメールを受け入れます。セキュリティ管理アプライアンスでローカル隔離を設定するには、『Cisco Content Security Management Appliance User Guide』を参照してください。セキュリティ管理アプライアンスのローカル隔離は、アプライアンスにメールを送信する他の Cisco アプライアンスからは、外部の隔離と見なされることに注意してください。

セキュリティ管理アプライアンスアプライアンスによって解放されたメールは、スパム隔離設定の定義に従って、プライマリ ホストおよびセカンダリ ホスト (Cisco アプライアンスまたは他のグループウェア ホスト) に配信されます (『Cisco Content Security Management Appliance User Guide』を参照)。したがって、セキュリティ管理アプライアンスにメールを配信する Cisco アプライアンスの数に関係なく、解放されるすべてのメール、通知、およびアラートが単一のホスト (グループウェアまたは Cisco アプライアンス) に送信されます。セキュリティ管理アプライアンスからの配信によって、プライマリ ホストが過負荷にならないように注意してください。

外部スパム隔離の設定

はじめる前に

- 「メールフローおよび外部スパム隔離」(P.38-2)を参照してください。
- 中央集中型スパム隔離およびエンドユーザのセーフリスト/ブロックリスト機能をサポートするようにセキュリティ管理アプライアンスを設定します。『Cisco Content Security Management Appliance User Guide』を参照してください。



(注)

外部スパム隔離を有効にすると、電子メールセキュリティアプライアンスはローカルスパム隔離へのメッセージの送信を停止します。サービスの空白を避けるため、ローカル隔離をディセーブルにする前にセキュリティ管理アプライアンスで中央集中型スパム隔離を設定します。

手順

- ステップ 1** [セキュリティ サービス (Security Services)] > [外部スパム隔離 (External Spam Quarantine)] を選択します。
- ステップ 2** [設定 (Configure)] をクリックします。
- ステップ 3** [外部スパム隔離 (External Spam Quarantine)] セクションで、[スパム外部隔離を有効にする (Enable External Spam Quarantine)] チェックボックスを選択します。
- ステップ 4** [名前 (Name)] フィールドに、セキュリティ管理アプライアンスの名前を入力します。
- ステップ 5** IP アドレスとポート番号を入力します。セキュリティ管理アプライアンスの IP アドレスおよびポート番号は、Cisco スパム隔離ページで設定します。
- ステップ 6** (任意) エンドユーザのセーフリスト/ブロックリスト機能をイネーブルにするチェックボックスをオンにして適切なブロックリストアクションを指定します。
- ステップ 7** 変更内容を送信し、確定します。

関連項目

- 第 13 章「アンチスパム」
- 「メッセージがスパムかどうかスキャンするためのアプライアンスの設定方法」(P.13-2)

一元化されたポリシー、ウイルス、アウトブレイク隔離について

- 「一元化されたポリシー、ウイルス、およびアウトブレイク隔離」 (P.38-4)
- 「ポリシー、ウイルス、アウトブレイク隔離の移行について」 (P.38-5)
- 「一元化されたポリシー、ウイルス、アウトブレイク隔離」 (P.38-5)
- 「一元化されたポリシー、ウイルス、アウトブレイク隔離のディセーブル化について」 (P.38-7)
- 「一元化されたポリシー、ウイルス、アウトブレイク隔離のトラブルシューティング」 (P.38-8)

一元化されたポリシー、ウイルス、およびアウトブレイク隔離

ポリシー、ウイルス、およびアウトブレイク隔離をセキュリティ管理アプライアンスで一元化できます。メッセージは、電子メールセキュリティアプライアンスで処理されますが、セキュリティ管理アプライアンスの隔離エリア内に保存されます。

ポリシー、ウイルス、およびアウトブレイク隔離を一元化する利点としては、次のものがあります。

- 管理者は複数の電子メールセキュリティアプライアンスで隔離されたメッセージを 1 か所で管理できます。
- 隔離されたメッセージは、セキュリティリスクを減らすために、DMZ の代わりに、ファイアウォールの内側に保存されます。
- 一元化された隔離は、セキュリティ管理アプライアンスの標準のバックアップ機能を使用して実行できます。

詳細については、お使いのセキュリティ管理アプライアンスのユーザマニュアルまたはオンラインヘルプを参照してください。

一元化されたポリシー、ウイルス、アウトブレイク隔離の制限事項

- 各電子メールセキュリティアプライアンスでは、すべてのポリシー、ウイルス、アウトブレイク隔離を一元化するか、またはすべてローカルに保存する必要があります。
- スキャンエンジンがセキュリティ管理アプライアンスでは使用できないため、ウイルスについてのポリシー、ウイルス、またはアウトブレイク隔離のテストメッセージを手動でテストできません。

クラスタ構成の一元化されたポリシー、ウイルス、アウトブレイク隔離の要件

一元化されたポリシー、ウイルス、およびアウトブレイク隔離を、クラスタ化されたアプライアンスの任意のレベルでイネーブルにできます。

要件

- 電子メールセキュリティアプライアンスの特定のレベル（マシン、グループ、またはクラスタ）で一元化されたポリシー、ウイルス、アウトブレイク隔離をイネーブルにする前に、同じレベルに属するすべてのアプライアンスを最初にセキュリティ管理アプライアンスに追加する必要があります。
- コンテンツ、メッセージフィルタおよび DLP メッセージアクションは同じレベルで設定され、そのレベル以下のすべてのレベルで上書きされない必要があります。

- 一元化されたポリシー、ウイルス、アウトブレイク隔離は同じレベルで設定され、設定したレベル以下のすべてのレベルで上書きされない必要があります。
- セキュリティ管理アプライアンスとの通信に使用するインターフェイスが、グループまたはクラスタ内のすべてのアプライアンスで同じ名前になっていることを確認します。

次に例を示します。

クラスタまたはグループ レベルで一元化されたポリシー、ウイルス、アウトブレイク隔離をイネーブルにしたい一方でクラスタに接続される電子メール セキュリティ アプライアンスがマシン レベルで設定されている場合、クラスタまたはグループ レベルでこの機能をイネーブルにする前に、マシン レベルでの集中型の隔離設定を削除する必要があります。

ポリシー、ウイルス、アウトブレイク隔離の移行について

ポリシー、ウイルス、アウトブレイク隔離を一元化すると、電子メール セキュリティ アプライアンスの既存のポリシー、ウイルス、アウトブレイク隔離はセキュリティ管理アプライアンスに移行します。

セキュリティ管理アプライアンスで移行を設定しますが、電子メール セキュリティ アプライアンスで一元化されたポリシー、ウイルス、およびアウトブレイク隔離のイネーブル化の変更を確定したときに移行が発生します。

この変更を確定すると、次が発生します。

- 電子メール セキュリティ アプライアンスのローカル ポリシー、ウイルス、アウトブレイク隔離がディセーブルになります。これらの隔離に入る新しいメッセージはすべてセキュリティ管理アプライアンスで隔離されます。
- セキュリティ管理アプライアンスへの既存の非スパム隔離の移行が開始されます。
- すべてのローカル ポリシー、ウイルス、アウトブレイク隔離が削除されます。カスタム移行を設定した場合は、移行しないように選択したローカル ポリシー隔離もすべて削除されます。ポリシー隔離の削除の影響については、「[ポリシー隔離の削除について](#)」(P.27-8) を参照してください。
- 移行前に複数の隔離に存在したメッセージは、移行後に該当の集中型隔離に存在します。
- 移行はバックグラウンドで実行されます。かかる時間は、隔離エリアのサイズとネットワークによって異なります。電子メール セキュリティ アプライアンスで中央集中型の隔離をイネーブルにすると、移行が完了したときに通知を受け取るための 1 つまたは複数の電子メール アドレスを入力できます。
- 送信元ローカル隔離ではなく中央集中型の隔離の設定が、それらのメッセージに適用されます。ただし、元の有効期限は各メッセージに適用されたままです。



(注) 移行時に自動的に作成されるすべての中央集中型の隔離は、デフォルトの隔離設定になります。

一元化されたポリシー、ウイルス、アウトブレイク隔離



(注) メンテナンス ウィンドウからまたはピーク時間帯以外に、この手順を実行してください。

はじめる前に

- 最初にセキュリティ管理アプライアンスに、一元化されたポリシー、ウイルス、アウトブレイク隔離の設定をします。オンラインヘルプの「Centralized Policy, Virus, and Outbreak Quarantines」の章の「Centralized Policy, Virus, and Outbreak Quarantines」の項にあるテーブル、またはセキュリティ管理アプライアンスのユーザ ガイドを参照してください。
- セキュリティ管理アプライアンスで中央集中型の隔離に割り当てられた容量が既存のローカル隔離が占める総容量よりも小さい場合は、メッセージはセキュリティ管理アプライアンスの隔離の設定に基づいて早期の期限切れとなります。移行の前に、隔離エリアのサイズを減らす手動の操作を行うことを検討してください。早期の期限切れの詳細については、「自動的に処理された隔離メッセージのデフォルト アクション」(P.27-5) を参照してください。
- 自動的な移行を選択する場合、または移行中に中央集中型の隔離を作成するためのカスタム移行を設定する場合は、中央集中型の隔離を設定するためのガイドラインとして使用する現在の電子メールセキュリティ アプライアンスの隔離設定がないことに注意してください。
- 電子メール セキュリティ アプライアンスをクラスタ コンフィギュレーションで展開している場合は、「クラスタ構成の一元化されたポリシー、ウイルス、アウトブレイク隔離の要件」(P.38-4) を参照してください。
- この手順で確定した変更は、すぐに発生することに注意してください。「ポリシー、ウイルス、アウトブレイク隔離の移行について」(P.38-5) を参照してください。

手順

-
- ステップ 1** [セキュリティ サービス (Security Services)] > [集約管理サービス (Centralized Services)] > [ポリシー、ウイルスおよびアウトブレイク隔離 (Policy, Virus, and Outbreak Quarantines)] を選択します。
- ステップ 2** [有効 (Enable)] をクリックします。
- ステップ 3** セキュリティ管理アプライアンスとの通信に使用するインターフェイスおよびポートを入力します。
セキュリティ管理アプライアンスからインターフェイスおよびポートに到達可能であることを確認します。
電子メール セキュリティ アプライアンスがクラスタ化されている場合、選択したインターフェイスがクラスタ内のすべてのマシンで使用できる必要があります。
- ステップ 4** 移行が完了したときに通知を受け取るには、1 つまたは複数の電子メールアドレスを入力します。
- ステップ 5** 想定どおりであるか確認するために、移行された隔離に関する情報を確認します。
- ステップ 6** カスタム移行を完了した場合は、この手順で変更を確定した際に削除される隔離に注意してください。
- ステップ 7** コンテンツおよびメッセージ フィルタ、およびアップデートするための DLP メッセージ アクションに関する情報が、想定どおりであることを確認します。



- (注)** クラスタ設定では、フィルタおよびメッセージ アクションが特定のレベルで定義され、そのレベル以下のすべてのレベルで上書きされていない場合に限り、メッセージ フィルタ アクションは特定のレベルで自動的にアップデートできます。移行後は、中央集中型の隔離名でフィルタおよびメッセージ アクションを手動で再設定する必要があります。

- ステップ 8** 移行のマッピングを再設定する必要がある場合、次を実行します。
- セキュリティ管理アプライアンスに戻ります。
 - 移行のマッピングを再設定します。
管理アプライアンスで、再マッピングする隔離を選択し、[集中型隔離から削除 (Remove from Centralized Quarantine)] をクリックします。その後、隔離を再マッピングできます。

- c. セキュリティ管理アプライアンスで新たに移行の設定を確定します。
- d. この手順を最初から繰り返します。

重要 [セキュリティ サービス (Security Services)] > [集約管理サービス (Centralized Services)] > [ポリシー、ウイルスおよびアウトブレイク隔離 (Policy, Virus, and Outbreak Quarantines)] ページを必ずリロードしてください。

ステップ 9 [送信 (Submit)] をクリックします。

ステップ 10 移行のマッピングを再設定する必要がある場合、**ステップ 8** の手順に従います。

ステップ 11 変更内容を確定します。



(注) 移行が進行中の間、電子メール セキュリティ アプライアンスまたはセキュリティ管理アプライアンスでの設定の変更は避けてください。

ステップ 12 ページの上部で移行ステータスを確認します。また、移行を設定するときに電子メールアドレスを入力した場合は、移行の完了を通知する電子メールを待ってください。

次の作業

オンラインヘルプの「Centralized Policy, Virus, and Outbreak Quarantines」の項目にあるテーブル、またはセキュリティ管理アプライアンスのユーザ ガイドに記載されるその他の作業を実行します。

関連項目

- 「[隔離にアクセスできるユーザ グループ](#)」 (P.27-10)

一元化されたポリシー、ウイルス、アウトブレイク隔離のディセーブル化について

電子メール セキュリティ アプライアンスで一元化されたポリシー、ウイルス、アウトブレイク隔離を無効にする場合、次が発生します。

- 電子メール セキュリティ アプライアンスでローカル隔離が自動的にイネーブルになります。
- システムに作成された隔離、およびメッセージフィルタ、コンテンツ フィルタ、DLP アクションから参照される隔離は、自動的に電子メール セキュリティ アプライアンスで作成されます。ウイルス、Outbreak および未分類の隔離は、割り当て済みユーザ ルールを含め、隔離が一元化される前と同じ設定で作成されます。その他すべての隔離は、デフォルト設定で作成されます。
- 新しく隔離されたメッセージは、すぐにローカル隔離に入ります。
- 中央集中型の隔離エリア内のメッセージは、ディセーブルにされたとき、次のいずれかが発生するまでそのままです。
 - 有効期限が切れたとき、メッセージは手動で削除するか自動的に削除されます。
 - メッセージは次のいずれかに該当する場合、手動または自動的にリリースされます。
 - * セキュリティ管理アプライアンスで代替のリリースのアプライアンスが設定されている。セキュリティ管理アプライアンスについては、オンライン ヘルプまたはマニュアルを参照してください。
 - * 中央集中型の隔離が電子メール セキュリティ アプライアンスで再度イネーブルになります。

中央集中型のポリシー、ウイルス、アウトブレイク隔離のディセーブル化

はじめる前に

- 中央集中型のポリシー、ウイルス、アウトブレイク隔離のディセーブル化の影響を理解します。
- 次のいずれかを実行します。
 - 現在中央集中型のポリシー、およびウイルス アウトブレイク隔離内にあるすべてのメッセージを処理します。
 - ディセーブルにした後で、中央集中型の隔離エリアから解放されるメッセージを処理する代替のリリースのアプライアンスが指定されていることを確認します。詳細については、セキュリティ管理アプライアンスのオンライン ヘルプまたはユーザ ガイドを参照してください。

手順

-
- ステップ 1** 電子メール セキュリティ アプライアンス で、[セキュリティ サービス (Security Services)] > [集約管理サービス (Centralized Services)] > [ポリシー、ウイルスおよびアウトブレイク隔離 (Policy, Virus, and Outbreak Quarantines)] を選択します。
- ステップ 2** 一元化されたスパム、ポリシー、ウイルス、およびアウトブレイク隔離をディセーブルにします。
- ステップ 3** 変更内容を送信し、確定します。
- ステップ 4** 新しく作成したローカル隔離の設定をカスタマイズします。
-

一元化されたポリシー、ウイルス、アウトブレイク隔離のトラブルシューティング

シスコのコンテンツのセキュリティ管理アプライアンスが使用できない場合

ポリシー、ウイルス、アウトブレイク隔離が使用できなくなったセキュリティ管理アプライアンスで一元化されている場合、電子メール セキュリティ アプライアンスでこれらの中央集中型の隔離をディセーブルにする必要があります。

代替のセキュリティ管理アプライアンスを配置している場合、セキュリティ管理アプライアンスおよび各電子メール セキュリティ アプライアンスで隔離の移行を再設定する必要があります。オンラインヘルプの「Centralized Policy, Virus, and Outbreak Quarantines」の章の「Centralized Policy, Virus, and Outbreak Quarantines」の項にあるテーブル、またはセキュリティ管理アプライアンスのユーザ ガイドを参照してください。

中央集中型レポーティングの設定

はじめる前に

- セキュリティ管理アプライアンスで中央集中型レポーティングのイネーブル化と設定を行います。前提条件と手順は、『Cisco Content Security Management Appliance User Guide』を参照してください。
- レポーティング サービスに十分なディスク領域が割り当てられていることをセキュリティ管理アプライアンスで確認します。

手順

-
- ステップ 1** [セキュリティ サービス (Security Services)]>[レポート (Reporting)] をクリックします。
- ステップ 2** [レポート サービス (Reporting Service)] セクションで [集約管理レポート (Centralized Reporting)] オプションを選択します。
- ステップ 3** 変更内容を送信し、確定します。
-

中央集中型レポートニングに変更後のレポート情報の可用性

中央集中型レポートニングが電子メールセキュリティアプライアンスでイネーブルになっている場合、次が発生します。

- 電子メールセキュリティアプライアンスにある月次レポート用の既存データは、セキュリティ管理アプライアンスに転送されません。
- 電子メールセキュリティアプライアンスのアーカイブ済みレポートは使用できません。
- 電子メールセキュリティアプライアンスは週次データのみ保存します。
- 月次レポートおよび年次レポート用の新規データはセキュリティ管理アプライアンスに保存されません。
- 電子メールセキュリティアプライアンスでスケジュール設定されたレポートは一時停止されます。
- 電子メールセキュリティアプライアンス上のスケジュール設定されたレポートの設定ページにはアクセスできなくなります。

中央集中型レポートニングのディセーブル化について

電子メールセキュリティアプライアンスで中央集中型レポートニングをディセーブルにした場合、電子メールセキュリティアプライアンスで新規月次レポートデータの保存が開始され、スケジュールされたレポートが再開し、アーカイブされたレポートにアクセスできます。中央集中型レポートニングをディセーブルにした場合に、電子メールセキュリティアプライアンスでは、過去の時間および日ごとのデータだけが表示され、過去の週ごとや月ごとのデータは表示されません。これは、一時的な変更です。十分なデータが蓄積されれば、過去の週および月のレポートが表示されます。電子メールセキュリティアプライアンスを中央集中型レポートニングモードに戻した場合、過去の週のデータはインタラクティブレポートに表示されます。

中央集中型メッセージトラッキングの設定



(注) 電子メールセキュリティアプライアンス中央集中型トラッキングおよびローカルトラッキングの両方をイネーブルにすることはできません。

手順

-
- ステップ 1** [セキュリティ サービス (Security Services)]>[メッセージトラッキング (Message Tracking)] をクリックします。

- ステップ 2** [メッセージトラッキング サービス (Message Tracking Service)] セクションで [設定を編集 (Edit Settings)] をクリックします。
- ステップ 3** [メッセージトラッキング サービスを有効にする (Enable Message Tracking Service)] チェックボックスを選択します。
- ステップ 4** [集約管理トラッキング (Centralized Tracking)] オプションを選択します。
- ステップ 5** (任意) 拒否された接続に関する情報を保存するチェックボックスをオンにします。



(注) 拒否された接続のトラッキング情報を保存すると、セキュリティ管理アプライアンスのパフォーマンスに悪影響を与えるおそれがあります。

- ステップ 6** 変更内容を送信し、確定します。

次の作業

中央集中型トラッキングを使用するには、電子メール セキュリティ アプライアンスおよびセキュリティ管理アプライアンスで機能をイネーブルにする必要があります。セキュリティ管理アプライアンスで中央集中型トラッキングをイネーブルにするには、『Cisco Content Security Management Appliance User Guide』を参照してください。

中央集中型サービスの使用方法

集約サービスの使用方法については、『Cisco Content Security Management Appliance User Guide』を参照してください。



APPENDIX A

アプライアンスへのアクセス

アプライアンスに作成したインターフェイスには、さまざまなサービスを通してアクセスできます。

表 A-1 インターフェイスに対してデフォルトでイネーブルになるサービス

| サービス | デフォルト ポート | デフォルトでイネーブルかどうか | |
|--------|-----------|-------------------------|-----------------|
| | | 管理インターフェイス ^a | 新規作成されたインターフェイス |
| FTP | 21 | いいえ | いいえ |
| Telnet | 23 | はい | いいえ |
| SSH | 22 | はい | いいえ |
| HTTP | 80 | はい | いいえ |
| HTTPS | 443 | はい | いいえ |

a. ここに示す「管理インターフェイス」は、Cisco C10 アプライアンスの Data 1 インターフェイスのデフォルト設定でもあります。

- Graphical User Interface (GUI; グラフィカル ユーザ インターフェイス) を使用してアプライアンスにアクセスする必要がある場合は、インターフェイスで HTTP、HTTPS、またはその両方をイネーブルにする必要があります。
- 設定ファイルのアップロードまたはダウンロードを目的としてアプライアンスにアクセスする必要がある場合は、インターフェイスで FTP または Telnet をイネーブルにする必要があります。
- Secure Copy (scp) を使用しても、ファイルをアップロードまたはダウンロードできます。

IP インターフェイス

IP インターフェイスには、ネットワークへの個別の接続に必要なネットワーク設定データが含まれています。1つの物理イーサネット インターフェイスに対して複数の IP インターフェイスを設定できます。IP インターフェイス経由でスパム隔離へのアクセスも設定できます。電子メール配信および仮想ゲートウェイでは、各 IP インターフェイスが特定の IP アドレスおよびホスト名を持つ1つの仮想ゲートウェイ アドレスとして動作します。IP インターフェイスまたは両方にインターネット プロトコルバージョン 4 (IPv4) または IP Version 6 (IPv6) を割り当てることができます。インターフェイスを独立したグループに (CLI を使用して) 「参加」させることもできます。システムは、電子メールの配信時にこれらのグループ間を循環します。

仮想ゲートウェイへの参加またはグループ化は、複数のインターフェイス間で大規模な電子メールキャンペーンを負荷分散するのに役立ちます。VLAN を作成し、他のインターフェイスを設定すると同様に（CLI を使用して）VLAN を設定することもできます。詳細については、[第 33 章「高度なネットワーク構成」](#)を参照してください。

電子メール セキュリティ アプライアンス への FTP アクセス設定

手順

- ステップ 1** [ネットワーク (Network)] > [IP インターフェイス (IP Interfaces)] ページまたは `interfaceconfig` コマンドを使用して、インターフェイスに対して FTP アクセスをイネーブルにします。

サービスを `interfaceconfig` コマンドでディセーブルにすると、CLI との接続が解除されることがあります。これは、アプライアンスにどのように接続しているかによって異なります。管理ポートで別のプロトコル、シリアルインターフェイス、またはデフォルト設定を使用してアプライアンスに再接続できない場合は、このコマンドでサービスをディセーブルにしないでください。

この例では、管理インターフェイスがポート 21（デフォルトポート）で FTP アクセスをイネーブルにするように編集されています。

図 A-1 [IP インターフェイスを編集 (Edit IP Interface)] ページ
Edit IP Interface

| IP Interface Settings | | |
|-----------------------|--|------|
| Name: | Management | |
| Ethernet Port: | Management | |
| IP Address: | 172.19.0.11 | |
| Netmask: | 255.255.255.0 | |
| Hostname: | elroy.run | |
| Services: | Service | Port |
| | <input checked="" type="checkbox"/> FTP | 21 |
| | <input checked="" type="checkbox"/> Telnet | 23 |
| | <input checked="" type="checkbox"/> SSH | 22 |



(注) 次の手順に進む前に、忘れずに変更を確定してください。

- ステップ 2** FTP 経由でインターフェイスにアクセスします。インターフェイスに対して正しい IP アドレスを使用していることを確認します。次の例を参考にしてください。

```
$ ftp 192.168.42.42
```



(注) ブラウザの多くは、FTP 経由でもインターフェイスにアクセスできます。

ステップ 3 実行しようとする特定のタスクのディレクトリを参照します。FTP 経由でインターフェイスにアクセスしたら、次のディレクトリを参照し、ファイルをコピーおよび追加（「GET」および「PUT」）できます。次の表を参照してください。

| ディレクトリ名 | 説明 |
|----------------|--|
| /configuration | <p>以下のコマンドからのデータがこのディレクトリにエクスポートされるか、このディレクトリからデータがインポート（保存）されます。</p> <ul style="list-style-type: none">仮想ゲートウェイ マッピング (altsrchoost)XML 形式の設定データ (saveconfig、loadconfig)ホストアクセス テーブル (HAT) (hostaccess)受信者アクセス テーブル (RAT) (rcptaccess)SMTP ルート エントリ (smtproutes)エイリアス テーブル (aliasconfig)マスカレード テーブル (masquerade)メッセージ フィルタ (filters)グローバル配信停止データ (unsubscribe)trace コマンドのテスト メッセージセーフリスト/ブロックリスト バックアップ ファイル (slbl<タイムスタンプ><シリアル番号>.csv 形式で保存) |

| ディレクトリ名 | 説明 |
|-------------------|--|
| /antivirus | Anti-Virus エンジンのログ ファイルが保存されるディレクトリです。このディレクトリにあるログ ファイルを検査して、ウイルス定義ファイル (scan.dat) の成功した最終ダウンロードを手動で確認できます。 |
| /configuration | logconfig コマンドと rollovernow コマンドを使用する ロギング 用に自動的に作成されます。各ログの詳細については、「 ロギング 」を参照してください。 |
| /system_logs | |
| /cli_logs | ログ ファイル タイプの違いについては、「ログ ファイル タイプの比較」を参照してください。 |
| /status | |
| /reportd_logs | |
| reportqueryd_logs | |
| /ftpd_logs | |
| /mail_logs | |
| /asarchive | |
| /bounces | |
| /error_logs | |
| /avarchive | |
| /gui_logs | |
| /sntpd_logs | |
| /RAID.output | |
| /euq_logs | |
| /scanning | |
| /antispam | |
| /antivirus | |
| /euqgui_logs | |
| /ipmitool.output | |

- ステップ 4** ご使用の FTP プログラムを使用して、適切なディレクトリに対するファイルのアップロードおよびダウンロードを行います。

secure copy (scp) アクセス

クライアント オペレーティング システムでセキュア コピー (scp) コマンドがサポートされている場合は、前述の表に示すディレクトリ間でファイルをコピーできます。たとえば、次の例では、ファイル /tmp/test.txt は、クライアント マシンからホスト名が mail3.example.com のアプライアンスの configuration ディレクトリにコピーされます。

コマンドを実行すると、ユーザ (admin) のパスワードを求めるプロンプトが表示されることに注意してください。この例を参考用としてだけ示します。特殊なオペレーティング システムの **secure copy** の実装方法によって異なる場合があります。

```
% scp /tmp/test.txt admin@mail3.example.com:configuration

The authenticity of host 'mail3.example.com (192.168.42.42)' can't be established.

DSA key fingerprint is 69:02:01:1d:9b:eb:eb:80:0c:a1:f5:a6:61:da:c8:db.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added 'mail3.example.com ' (DSA) to the list of known hosts.

admin@mail3.example.com's password: (type the password)

test.txt          100% |*****| 1007      00:00

%
```

この例では、同じファイルがアプライアンスからクライアント マシンにコピーされます。

```
% scp admin@mail3.example.com:configuration/text.txt .

admin@mail3.example.com's password: (type the password)

test.txt          100% |*****| 1007      00:00

%
```

Cisco アプライアンスに対するファイルの転送および取得には、**secure copy (scp)** を **FTP** に代わる方法として使用できます。



(注) operators グループおよび administrators グループのユーザだけが、アプライアンスへのアクセスに **secure copy (scp)** を使用できます。詳細については、「[ユーザの追加](#)」(P.28-4) を参照してください。

シリアル接続による電子メール セキュリティ アプライアンスへのアクセス

シリアル接続を使用してアプライアンスに接続している場合（「[アプライアンスへの接続](#)」(P.3-8) を参照）、[図 A-2](#) にシリアル ポート コネクタのピン番号を示し、[表 A-2](#) にシリアル ポート コネクタのピン割り当ておよびインターフェイス信号を定義します。

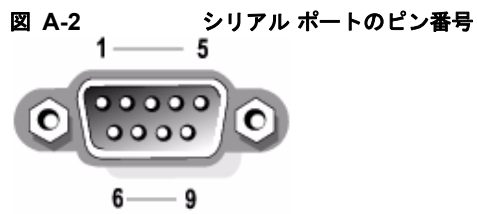


表 A-2 シリアル ポートのピン割り当て

| ピン | 信号 | I/O | 定義 |
|-----|------|-----|------------------|
| 1 | DCD | I | データ キャリア検出 |
| 2 | SIN | I | シリアル入力 |
| 3 | SOUT | O | シリアル出力 |
| 4 | DTR | O | データ ターミナル
レディ |
| 5 | GND | n/a | 信号用接地 |
| 6 | DSR | I | データ セット レ
ディ |
| 7 | RTS | I | 送信要求 |
| 8 | CTS | O | 送信可 |
| 9 | RI | I | リング インジケータ |
| シェル | n/a | n/a | シャーシグラウンド |



APPENDIX **B**

ネットワーク アドレスと IP アドレスの割り当て

この付録では、ネットワーク アドレスと IP アドレスの割り当てに関する一般的なルールについて説明し、ネットワークに Cisco アプライアンスを接続するための戦略の一部を示します。

- 「イーサネット インターフェイス」(P.B-1)
- 「IP アドレスとネットマスクの選択」(P.B-1)
- 「Cisco アプライアンスの接続時の戦略」(P.B-3)

イーサネット インターフェイス

Cisco X1050/1060/1070、C650/660/670、および C350/360/370 アプライアンスには、構成（オプションの光ネットワーク インターフェイスがあるかどうか）に応じて最大 4 個のイーサネット インターフェイスがシステムの背面パネルにあります。これらには次のようなラベルが付けられています。

- Management
- Data1
- Data2
- Data3
- Data4

Cisco C150/160 アプライアンスには、システムの背面パネルにイーサネット インターフェイスが 2 つ搭載されています。これらには次のようなラベルが付けられています。

- Data1
- Data2

IP アドレスとネットマスクの選択

ネットワークを設定する場合、Cisco アプライアンスが発信パケットを送信するインターフェイスを一意に選択する必要があります。この要件により、イーサネット インターフェイスの IP アドレスとネットマスクの選択に関する一部の内容が決定されます。単一のネットワークに配置できるインターフェイスは 1 つのみというのがルールです（ネットマスクがインターフェイスの IP アドレスに適用されることでそのように定められます）。

■ IP アドレスとネットマスクの選択

IP アドレスは、特定のネットワーク上の物理インターフェイスを識別します。物理イーサネットインターフェイスは、パケットを受け取る IP アドレスを複数持つことができます。複数の IP アドレスを持つイーサネットインターフェイスは、パケットの送信元アドレスとして任意の IP アドレスを 1 つ使用して、インターフェイスからパケットを送信できます。このプロパティは、Virtual Gateway テクノロジーの実装で使用されます。

ネットマスクの目的は、IP アドレスをネットワークアドレスとホストアドレスに分割することです。ネットワークアドレスは、IP アドレスのネットワーク部分（ネットマスクと一致するビット）と見なすことができます。ホストアドレスは IP アドレスの残りのビットです。4 オクテットアドレスの有効ビット数は、Classless Inter-Domain Routing (CIDR; クラスレス ドメイン間ルーティング) スタイルで表現されることがあります。すなわち、ビット数 (1 ~ 32) の先頭にスラッシュが付きます。

ネットマスクはこうした表現を、単純にバイナリ表記で 1 を数える形で行うことができます。したがって 255.255.255.0 は「/24」となり、255.255.240.0 は「/20」となります。

インターフェイスの設定例

ここでは、いくつかの代表的なネットワークに基づいたインターフェイスの設定例を示します。この例では、Int1 と Int2 の 2 つのインターフェイスを使用します。Cisco アプライアンスの場合、これらのインターフェイス名は、3 つの Cisco インターフェイス (Management、Data1、Data2) のうちのいずれか 2 つを表します。

ネットワーク 1:

インターフェイスはそれぞれ、別々のネットワークに配置する必要があります。

| インターフェイス | IP アドレス | ネットマスク | ネットアドレス |
|----------|--------------|---------------|----------------|
| Int1 | 192.168.1.10 | 255.255.255.0 | 192.168.1.0/24 |
| Int2 | 192.168.0.10 | 255.255.255.0 | 192.168.0.0/24 |

192.168.1.x にアドレス指定されたデータ (ここで X は自身のアドレスを除く 1 ~ 255 のいずれか。この場合は 10) は、Int1 に進みます。192.168.0.x にアドレス指定されたデータはすべて、Int2 に進みます。このような形式に該当しないその他のアドレス (WAN やインターネット上のアドレスである可能性が高い) が指定されているパケットはデフォルトのゲートウェイに送信されます。このゲートウェイは、これらのネットワークのいずれかに存在している必要があります。次に、デフォルトゲートウェイがパケットを転送します。

ネットワーク 2:

2 つの異なるインターフェイスのネットワークアドレス (IP アドレスのネットワーク部分) は同じにすることができません。

| イーサネットインターフェイス | IP アドレス | ネットマスク | ネットアドレス |
|----------------|--------------|-------------|----------------|
| Int1 | 192.168.1.10 | 255.255.0.0 | 192.168.0.0/16 |
| Int2 | 192.168.0.10 | 255.255.0.0 | 192.168.0.0/16 |

この場合、2 つの異なるイーサネットインターフェイスが同じネットワークアドレスを持つという矛盾した状態になっています。Cisco アプライアンスからのパケットを 192.168.1.11 に送信する場合に、どのイーサネットインターフェイスを使用してパケットを送信すべきかを決定する方法がありません。

2つのイーサネット インターフェイスが2つの物理ネットワークに別々に接続されている場合、パケットは誤ったネットワークに配信される可能性があり、そうするとそのパケットの送信先を見つけることはできません。Cisco アプライアンスを使用すると、矛盾を含むネットワークを設定できなくなります。

2つのイーサネット インターフェイスを同じ物理ネットワークに接続することはできますが、Cisco アプライアンスが一意の配信インターフェイスを選択できるように IP アドレスとネットマスクを設定する必要があります。

IP アドレス、インターフェイス、およびルーティング

GUI または CLI で、インターフェイスを選択可能なコマンドや関数を実行する際にインターフェイスを選択した場合（たとえば、AsyncOS のアップグレードや DNS の設定など）、ルーティング（デフォルトのゲートウェイ）が選択した内容より優先されます。

たとえば、3つのネットワーク インターフェイスがそれぞれ別のネットワーク セグメントに設定された次のような Cisco アプライアンスがあるとします（すべて /24 と仮定）。

| イーサネット | IP |
|------------|--------------|
| Management | 192.19.0.100 |
| data1 | 192.19.1.100 |
| data2 | 192.19.2.100 |

デフォルトのゲートウェイは 192.19.0.1 です。

AsyncOS のアップグレード（またはインターフェイスを選択できる他のコマンドや関数）を実行し、data1 (192.19.1.100) の IP を選択した場合、ユーザはすべての TCP トラフィックが data1 イーサネット インターフェイスを介して発生すると想定します。しかし、トラフィックはデフォルト ゲートウェイとして設定されているインターフェイス（この場合は Management）から発生し、data1 の IP の送信元アドレスのスタンプが付されます。

まとめ

Cisco アプライアンスは、配信するパケットが経由する一意のインターフェイスを常に識別できなければなりません。この決定を行うために、Cisco アプライアンスは、パケットの宛先 IP アドレスと、そのイーサネット インターフェイスのネットワークおよび IP アドレス設定を組み合わせ使用します。次の表に、ここまで説明してきた例をまとめます。

| | 同じネットワーク | 異なるネットワーク |
|---------------|----------|-----------|
| 同じ物理インターフェイス | 可 | 可 |
| 異なる物理インターフェイス | 不可 | 可 |

Cisco アプライアンスの接続時の戦略

Cisco アプライアンスを接続する際には、次の点に留意してください。

- 管理トラフィック（CLI、Web インターフェイス、ログ配信）は通常、電子メールのトラフィックに比べて小さいサイズになります。

- 2つのイーサネット インターフェイスが、同じネットワーク スイッチに接続されているが別のホスト ダウンストリーム上の単一のインターフェイスとのトークで終了する場合、またはすべてのデータがすべてのポートにエコーされるネットワーク ハブに接続されている場合、2つのインターフェイスを使用しても得られる利点はありません。
- 1000 Base-T で動作するインターフェイスを介した SMTP カンバセーションは、100 Base-T で動作する同じインターフェイスを介した場合より若干速くなりますが、これは理想的な条件下でのみです。
- 配信ネットワークのその他の部分にボトルネックがある場合、ネットワークへの接続を最適化しても意味がありません。ボトルネックは、インターネットへの接続や、接続プロバイダーによるアップストリームへの接続で最も頻繁に発生します。

接続する Cisco アプライアンス インターフェイスの数や、それらのアドレスを指定する方法は、基幹ネットワークの複雑さを考慮した上で決定する必要があります。ご使用のネットワーク トポロジやデータのボリュームから判断して不要であれば、複数のインターフェイスに接続する必要はありません。また、最初は単純な接続にしておき、ゲートウェイに慣れてきたら、ボリュームやネットワーク トポロジでの必要に応じて接続を増やすこともできます。



APPENDIX C

メール ポリシーとコンテンツ フィルタの例

受信メールポリシーの概要

この例では、次のタスクを示し、メール ポリシーの機能について説明します。

1. デフォルトの着信メール ポリシーのアンチスパム、アンチウイルス、アウトブレイク フィルタおよびコンテンツ フィルタを編集します。
2. 販売部とエンジニアリング部の異なるユーザのセットに 2 つの新しいポリシーを追加して、それぞれに異なる電子メール セキュリティ設定を指定します。
3. [着信メール ポリシーの概要 (Incoming Mail Overview policy)] テーブルで使用する 3 つの新しいコンテンツ フィルタを作成します。
4. ポリシーをもう一度編集して、コンテンツ フィルタをグループによってイネーブルまたはディセーブルにします。

この例では、受信者によって異なるメール ポリシーのアンチスパム、アンチウイルス、アウトブレイク フィルタおよびコンテンツ フィルタの設定を管理できる、機能と柔軟性を示しています。この例では、メール ポリシーおよびコンテンツ フィルタのアクセス権限を持つ「ポリシー管理者」と呼ばれるカスタム ユーザ ロールを割り当てます。アンチスパム、アンチウイルス、アウトブレイク フィルタ、および委任管理の機能の詳細については、次の章を参照してください。

- [「アンチスパム」 \(P.13-1\)](#)
- [「アンチウイルス」 \(P.12-1\)](#)
- [「アウトブレイク フィルタ」 \(P.14-1\)](#)
- [「管理タスクの分散」 \(P.28-1\)](#)

メール ポリシーへのアクセス

[メール ポリシー (Mail Policies)] メニューを使用して、着信および発信メール ポリシーにアクセスできます。

新規システムでは、システム セットアップ ウィザードのすべての手順を完了して、Cisco Anti-Spam、Sophos または McAfee Anti-Virus およびアウトブレイク フィルタをイネーブルにするように選択した場合、[図 C-1](#) のような [着信メールポリシー (Incoming Mail Policies)] ページが表示されます。

デフォルトでは、これらの設定は、デフォルトの着信メール ポリシーでイネーブルにされます。

- アンチスパム (Cisco スпам隔離がイネーブルの場合) : イネーブル
 - 陽性と判定されたスパム : 隔離、メッセージの件名が追加
 - 陽性と疑わしいスパム : 隔離、メッセージの件名が追加

受信メールポリシーの概要

- マーケティング電子メール：スキャンはイネーブルにされない
- アンチスパム（Cisco スпам隔離がイネーブルではない場合）：イネーブル
 - 陽性と判定されたスパム：配信、メッセージの件名が追加
 - 陽性と疑わしいスパム：配信、メッセージの件名が追加
 - マーケティング電子メール：スキャンはイネーブルにされない
- アンチウイルス：イネーブル、ウイルスのスキャンおよび修復、アンチウイルス スキャン結果が X-Header に追加
 - 修復されたメッセージ：配信、メッセージの件名が追加
 - 暗号化されたメッセージ：配信、メッセージの件名が追加
 - スキャンできないメッセージ：配信、メッセージの件名が追加
 - ウイルスに感染したメッセージ：ドロップ
- アウトブレイク フィルタ：イネーブル
 - ファイル拡張子は予測されない
 - 疑わしいウイルス添付ファイルのあるメッセージの保存期間は 1 日
 - メッセージの変更は有効ではない
- コンテンツ フィルタ：ディセーブル

図 C-1 [着信メールポリシー (Incoming Mail Policies)] ページ：新規アプライアンスのデフォルト Incoming Mail Policies

| Order | Policy Name | Anti-Spam | Anti-Virus | Content Filters | Outbreak Filters | Delete |
|-------|----------------|---|---|-----------------|---------------------------------|--------|
| | Default Policy | IronPort Anti-Spam
Positive: Quarantine
Suspected: Quarantine
Marketing Messages: Disabled | Sophos
Encrypted: Deliver
Uncannable: Deliver
Virus Positive: Drop | Disabled | Retention Time:
Virus: 1 day | |

Key: Default Custom ReadOnly



(注)

この例では、着信メールポリシーは、Cisco スпам隔離がイネーブルにされている場合のデフォルトのアンチスパム設定を使用します。

[有効 (Enabled)]、[無効 (Disabled)]、[利用不可 (Not Available)]

メールポリシーテーブル（着信または発信のいずれか）の列は、各ポリシー名のセキュリティサービスの状態のリンクを表示します。サービスがイネーブルの場合、[有効 (Enabled)] という語またはコンフィギュレーションの要約が表示されます。同様に、サービスがディセーブルの場合、[無効 (Disabled)] という語が表示されます。

サービスのライセンス契約書に同意していない場合、またはサービスの有効期限が切れている場合、リンクとして [利用不可 (Not Available)] が表示されます。この場合、[利用不可 (Not Available)] リンクをクリックすると、[セキュリティ サービス (Security Services)] タブ内に、サービスのポリシー単位の設定を指定できるページではなく、グローバル ページが表示されます。ページが別のタブに変わったことを示す警告が表示されます。図 C-2 を参照してください。

図 C-2 使用できないセキュリティ サービス
Incoming Mail Policies

| Order | Policy Name | Anti-Spam | Anti-Virus | Content Filters | Outbreak Filters | Delete |
|-------|----------------|---------------|---------------|-----------------|------------------|--------|
| | Default Policy | Not Available | Not Available | Disabled | Not Available | |

Key: Default Custom Readonly

着信メッセージのデフォルトのアンチスパムポリシーの設定

このメールポリシーテーブル内の各行は、異なるポリシーを表します。各列は、異なるセキュリティサービスを表します。

- デフォルトポリシーを編集するには、着信または発信メールポリシーテーブルの下部の行にあるセキュリティサービスの任意のリンクをクリックします。

この例では、着信メールのデフォルトポリシーのアンチスパム設定をより積極的に変更します。デフォルト値では、陽性と判定されたスパムメッセージおよび陽性と疑わしいスパムメッセージが隔離され、マーケティング電子メールのスキャンがディセーブルになります。次に、陽性と判定されたスパムがドロップされるように設定を変更する例を示します。陽性と疑わしいスパムは引き続き隔離されず。マーケティング電子メールのスキャンは、イネーブルにされ、マーケティングメッセージは目的の受信者に配信されます。マーケティングメッセージの件名には、テキスト [MARKETING] が前に追加されます。

手順

ステップ 1 アンチスパムセキュリティサービスのリンクをクリックします。



(注) デフォルトのセキュリティサービス設定の場合、このページの最初の設定では、ポリシーでサービスがイネーブルになるかどうかを定義します。[無効 (Disable)] をクリックして、サービスをディセーブルにできます。

ステップ 2 [陽性と判定されたスパムの設定 (Positively Identified Spam Settings)] セクションでは、[このメッセージに適用されるアクション (Action to apply to this message)] を [ドロップ (Drop)] に変更します。

ステップ 3 [マーケティングメールの設定 (Marketing Email Settings)] セクションでは、[はい (Yes)] をクリックして、マーケティング電子メールのスキャンをイネーブルにします。

イネーブルにされている場合、デフォルトアクションでは、テキスト [MARKETING] が件名の前に追加され、問題のないマーケティングメッセージが配信されます。

[メッセージにテキストを追加 (Add text to message)] フィールドでは、US-ASCII 文字だけを使用できます。

ステップ 4 [送信 (Submit)] をクリックします。着信メールポリシーテーブルのアンチスパムセキュリティサービスの要約リンクが変更され、新しい値が反映されているため注意してください。

前述の手順と同様、デフォルトポリシーのデフォルトアンチウイルスおよびウイルスアウトブレイクフィルタ設定を変更できます。

図 C-3 [スパム対策設定 (Anti-Spam Settings)] ページ
Mail Policies: Anti-Spam

送信者および受信者のグループのメールポリシーの作成

この例では、販売部（メンバーは LDAP 受け入れクエリーにより定義されます）用とエンジニアリング部用の 2 つの新しいポリシーを作成します。ポリシーは両方とも、これらのポリシーの管理を担当するロールに属する委任管理者を作成するためにポリシー管理者カスタム ユーザロールに割り当てられます。次に、それぞれに異なる電子メールセキュリティ設定を設定します。

手順

- ステップ 1** [ポリシーを追加 (Add Policy)] ボタンをクリックして、新しいポリシーの作成を開始します。
- ステップ 2** 一意な名前を定義して、(必要な場合) ポリシーの順序を調整します。
 ポリシーの名前は、定義されるメールポリシーテーブル（着信または発信のいずれか）で一意でなければなりません。
 各受信者は、適切なテーブル（着信または発信）の各ポリシーに対して上から順に評価されます。
- ステップ 3** [編集可能なユーザ (役割) (Editable By (Roles))] リンクをクリックし、メールポリシーの管理を担当する委任管理者にカスタム ユーザロールを選択します。
 リンクをクリックすると、AsyncOS は、メールポリシーの編集権限がある委任管理者のカスタムロールを表示します。委任管理者は、ポリシーのアンチスパム、アンチウイルス、アウトブレイクフィルタの設定を編集し、ポリシーのコンテンツフィルタを有効化または無効化できます。オペレータおよび管理者のみがメールポリシーの名前または送信者、受信者、またはグループを変更できます。メールポリシーへのフルアクセス権があるカスタム ユーザロールはメールポリシーに自動的に割り当てられます。
 委任管理の詳細については、「[管理タスクの分散](#)」を参照してください。
- ステップ 4** ポリシーのユーザを定義します。

ユーザが、送信者または受信者のいずれであるかを定義します（詳細については、「[ポリシー マッチングの例](#)」(P.10-4) を参照してください)。図 C-4 では、着信メールポリシーの受信者および発信メールポリシーの送信者というデフォルト形式を示しています。

ポリシーのユーザは、次の方法で定義できます。

- 完全な電子メールアドレス : user@example.com
- 電子メールアドレスの一部 : user@
- ドメインのすべてのユーザ : @example.com
- 部分ドメインのすべてのユーザ : @.example.com
- LDAP クエリーとのマッチング



(注) ユーザの入力は、AsyncOS の GUI および CLI の両方で、大文字と小文字が区別されます。たとえば、ユーザの受信者 Joe@ を入力すると、joe@example.com に送信されるメッセージが一致します。

ユーザ情報を、たとえば Microsoft Active Directory、SunONE Directory Server（以前の「iPlanet Directory Server」）または Open LDAP ディレクトリなど、ネットワーク インフラストラクチャの LDAP ディレクトリ内に保存する場合、Cisco アプライアンスを設定して、LDAP サーバをクエリーし、受信者アドレスの受け取り、代替アドレスまたはメール ホスト、あるいはその両方へのメッセージのリルーティング、ヘッダーのマスカレード、メッセージに特定のグループの受信者または送信者があるかどうかの判別を行うことができます。

アプライアンスをこのように設定した場合、設定したクエリーを使用してメールポリシーのユーザを定義できます。

詳細については、「[LDAP クエリー](#)」を参照してください。

図 C-4 ポリシーのユーザの定義
Add Incoming Mail Policy

ステップ 5 [追加 (Add)] ボタンをクリックして、[現在のユーザ (Current Users)] リストにユーザを追加します。

ポリシーには、送信者、受信者および LDAP クエリーを組み合わせる含めることができます。

[削除 (Remove)] ボタンを使用すると、定義されているユーザを現在のユーザのリストから削除できます。

ステップ 6 ユーザの追加が完了したら、[送信 (Submit)] をクリックします。

ポリシーを最初に追加する場合、すべてのセキュリティ サービス設定では、デフォルト値が使用されるため注意してください。

図 C-5 新しく追加されたポリシー：販売グループ

| Order | Policy Name | Anti-Spam | Anti-Virus | Content Filters | Outbreak Filters | Delete |
|-------|----------------|---|--|-----------------|---------------------------------|--------|
| 1 | Sales_Team | (use default) | (use default) | (use default) | (use default) | |
| | Default Policy | IronPort Anti-Spam
Positive: Quarantine
Suspected: Quarantine
Marketing Messages: Disabled | Sophos
Encrypted: Deliver
Unscannable: Deliver
Virus Positive: Drop | Disabled | Retention Time:
Virus: 1 day | |

ステップ 7 [ポリシーを追加 (Add Policy)] ボタンをもう一度クリックして、別の新しいポリシーを追加します。
このポリシーでは、エンジニアリング チームのメンバーの各電子メールアドレスが定義されます。

図 C-6 エンジニアリング チームのポリシーの作成
Add Incoming Mail Policy

Add Policy

Policy Name: (e.g. my IT policy)

Editable by (Roles): Policy Administrator

Insert Before Policy: 2 (Default Policy)

Add Users

Sender

Recipient

Email Address(es)

mary@example.com
fred@example.com

(e.g. user@example.com, user@, @example.com, @example.com)

LDAP Group Query

Query: Sales_West.group

Group:

Current Users

Recipient: bob@example.com
Recipient: mary@example.com
Recipient: fred@example.com

ステップ 8 エンジニアリング ポリシーのユーザの追加が完了したら、[送信 (Submit)] をクリックします。

ステップ 9 変更内容を確定します。

図 C-7 新しく追加されたポリシー：エンジニアリング チーム

| Order | Policy Name | Anti-Spam | Anti-Virus | Content Filters | Outbreak Filters | Delete |
|-------|----------------|---|--|-----------------|---------------------------------|--------|
| 1 | Sales_Team | (use default) | (use default) | (use default) | (use default) | |
| 2 | Engineering | (use default) | (use default) | (use default) | (use default) | |
| | Default Policy | IronPort Anti-Spam
Positive: Quarantine
Suspected: Quarantine
Marketing Messages: Disabled | Sophos
Encrypted: Deliver
Unscannable: Deliver
Virus Positive: Drop | Disabled | Retention Time:
Virus: 1 day | |



(注)

この時点では、新しく作成された両方のポリシーに、デフォルト ポリシーで使用される同じ設定が適用されています。いずれかのポリシーのユーザへのメッセージが一致しますが、メール処理設定は、デフォルト ポリシーと同じです。そのため、「Sales_Group」または「Engineering」ポリシーのユーザと一致するメッセージは、デフォルト ポリシーと同様に処理されます。

[デフォルト (Default)]、[カスタム (Custom)]、[無効 (Disabled)]

テーブル下部のキーは、特定のポリシーのセルのカラー コーディングが、デフォルト行に定義されているポリシーとどのように関係するかを示しています。

Key: Default Custom Disabled

- イエローのシェーディングは、ポリシーがデフォルト ポリシーと同じ設定を使用していることを示します。
- シェーディングなし（ホワイト）は、ポリシーがデフォルト ポリシーとは異なる設定を使用していることを示します。
- グレーのシェーディングは、セキュリティ サービスがポリシーでディセーブルにされていることを示します。

送信者および受信者のグループごとのメールポリシーの作成

この例では、前述の項で作成した 2 つのポリシーを編集します。

- 販売グループでは、アンチスパム設定をデフォルト ポリシーよりも積極的になるように変更します（「[着信メッセージのデフォルトのアンチスパムポリシーの設定](#)」(P.C-3) を参照）。陽性と識別されたスパム メッセージをドロップするデフォルト ポリシーが使用されます。ただし、この例では、Cisco スпам隔離エリアに送信されるように、マーケティング メッセージの設定を変更します。

この積極的なポリシーでは、販売チームの受信トレイに送信される不要なメッセージが最小限に押さえられます。

アンチスパム設定の詳細については、「[アンチスパム](#)」(P.13-1) を参照してください。

- エンジニアリング チームでは、example.com へのリンクを除く疑わしいメッセージの URL を変更するために、アウトブレイク フィルタ機能の設定をカスタマイズします。拡張子「dwg」の添付ファイルは、アウトブレイク フィルタのスキャンをバイパスします。

アウトブレイク フィルタの設定の詳細については、「[アウトブレイク フィルタ](#)」(P.14-1) を参照してください。

販売チーム ポリシーのアンチスパム設定を編集するには、次の手順を実行します。

手順

- ステップ 1** 販売ポリシー行のアンチスパム セキュリティ サービス ([スпам対策 (Anti-Spam)]) 列のリンクをクリックします。

このポリシーは新しく追加されたポリシーであるため、リンクの名前は [(デフォルトを使用) (use default)] です。

図 C-8 販売チーム ポリシーのアンチスパム設定の編集

| Policies | | |
|----------|----------------|--|
| Order | Policy Name | Anti-Spam |
| 1 | Sales_Team | (use default) |
| 2 | Engineering | (use default) |
| | Default Policy | IronPort Anti-Spam
Positive: Drop
Suspected: Quarantine
Marketing Messages: Deliver |

- ステップ 2** アンチスパム セキュリティ サービス ページで、[このポリシーのスパム対策スキャンを有効にする (Enable Anti-Spam Scanning for this Policy)] の値を [デフォルト設定を使用 (Use Default Settings)] から [Cisco スпам対策を使用 (Use Cisco Anti-Spam)] に変更します。

[Cisco スпам対策サービスを使用 (Use Cisco Anti-Spam service)] を選択すると、デフォルトポリシーで定義されている設定が無効になります。

- ステップ 3** [スпамと確定された場合の設定 (Positively-Identified Spam Settings)] セクションで、[このアクションをメッセージに適用する (Apply This Action to Message)] を [ドロップ (Drop)] に変更します。

- ステップ 4** [疑わしいスパムの設定 (Suspected Spam Settings)] セクションで、[はい (Yes)] をクリックして、陽性と疑わしいスパムのスキャンをイネーブルにします。

- ステップ 5** [疑わしいスパムの設定 (Suspected Spam Settings)] セクションで、[このアクションをメッセージに適用する (Apply This Action to Message)] を [スпам隔離 (Spam Quarantine)] に変更します。



(注) [Cisco スпам隔離 (Cisco Spam Quarantine)] を選択すると、『Cisco IronPort AsyncOS for Email Daily Management Guide』の「Quarantines」の章で定義されている設定に従って、メールが転送されます。

- ステップ 6** [件名へテキストを追加 (Add text to subject)] フィールドで、[None] をクリックします。

Cisco スпам隔離エリアに配信されるメッセージには、件名タギングが追加されません。

- ステップ 7** [マーケティングメールの設定 (Marketing Email Settings)] セクションで、[はい (Yes)] をクリックして、問題のない送信元からのマーケティングメールのスキャンをイネーブルにします。

- ステップ 8** [このアクションをメッセージに適用する (Apply This Action to Message)] セクションで、[スпам隔離 (Spam Quarantine)] を選択します。

- ステップ 9** 変更内容を送信し、確定します。

このシェーディングは、ポリシーがデフォルトポリシーとは異なる設定を使用していることを示します。

図 C-9 変更された販売グループのポリシーのアンチスパム設定

| Policies | | |
|----------|----------------|---|
| Order | Policy Name | Anti-Spam |
| 1 | Sales_Team | IronPort Anti-Spam
Positive: Drop
Suspected: Quarantine
Marketing Messages: Quarantine |
| 2 | Engineering | (use default) |
| | Default Policy | IronPort Anti-Spam
Positive: Drop
Suspected: Quarantine
Marketing Messages: Deliver |

この時点では、スパムの疑いがあり、その受信者が販売チーム ポリシーで定義されている LDAP クエリーと一致するメッセージは、Cisco スпам隔離エリアに配信されます。

エンジニアリング チーム ポリシーのアウトブレイク フィルタ設定を編集するには、次の手順を実行します。

手順

- ステップ 1** エンジニアリング ポリシー行のアウトブレイク フィルタ機能セキュリティ サービス ([アウトブレイク フィルタ (Outbreak Filters)] カラム) のリンクをクリックします。

このポリシーは新しく追加されたポリシーであるため、リンクの名前は [(デフォルトを使用) (use default)] です。

図 C-10 エンジニアリング チーム ポリシーのアウトブレイク フィルタ機能設定の編集

| Policies | | | | | | |
|----------|----------------|---|--|-----------------|---------------------------------|--------|
| Order | Policy Name | Anti-Spam | Anti-Virus | Content Filters | Outbreak Filters | Delete |
| 1 | Sales_Team | IronPort Anti-Spam
Positive: Drop
Suspected: Quarantine
Marketing Messages: Quarantine | (use default) | (use default) | (use default) | |
| 2 | Engineering | (use default) | (use default) | (use default) | (use default) | |
| | Default Policy | IronPort Anti-Spam
Positive: Quarantine
Suspected: Quarantine
Marketing Messages: Disabled | Sophos
Encrypted: Deliver
Unscannable: Deliver
Virus Positive: Drop | Disabled | Retention Time:
Virus: 1 day | |

- ステップ 2** [アウトブレイク フィルタ機能セキュリティ サービス (Outbreak Filters feature security service)] ページで、ポリシーのスキャン設定を [アウトブレイクフィルタを有効にする (設定をカスタマイズ) (Enable Outbreak Filtering (Customize settings))] に変更します。

[(設定をカスタマイズ) ((Customize settings))] を選択すると、デフォルト ポリシーで定義されている設定が無効になります。

また、別の設定を選択できるようにページの残りの部分のコンテンツがイネーブルになります。

- ステップ 3** ページの [添付ファイルのスキャンのバイパス (Bypass Attachment Scanning)] セクションで、ファイル拡張子フィールドに **dwg** と入力します。

ファイル拡張子「dwg」は、Cisco アプライアンスが添付ファイルのスキャン時にフィンガープリントにより認識できる既知のファイルタイプのリストにはありません。



(注) 3 文字のファイル拡張子の前にピリオド (.) を入力する必要はありません。

- ステップ 4** [拡張子を追加 (Add Extension)] をクリックして、.dwg ファイルをアウトブレイク フィルタ機能スキャンをバイパスするファイル拡張子のリストに追加します。

- ステップ 5** [メッセージの変更を有効にする (Enable Message Modification)] をクリックします。

メッセージの変更を有効にすると、アプライアンスはフィッシングおよび詐欺など脅威としてターゲットされるものや、疑わしいまたは不正な Web サイトへの URL がスキャンできるようになります。アプライアンスは、ユーザが Web サイトへアクセスしようとする Cisco セキュリティプロキシを介してリダイレクトするように、メッセージ中のリンクを書き換えます。



(注) アウトブレイク フィルタが非ウイルス性の脅威をスキャンするために、メールポリシーでアンチスパム スキャンをイネーブルにする必要があります。

ステップ 6 [未署名のメッセージに対して有効にする (Enable for Unsigned Messages)] を選択します。

その結果、アプライアンスは署名されたメッセージの URL を書き換えることができます。他のメッセージの変更および非ウイルス性の脅威が検出されたメッセージが解放されるまで隔離にとどまる時間が設定ができるように URL の書き換えをイネーブルにする必要があります。この例では、デフォルトの保存期間は 4 時間です。

ステップ 7 [ドメインのスキャンをバイパス (Bypass Domain Scanning)] フィールドに example.com と入力します。

example.com へのリンクは変更されません。

ステップ 8 [脅威に関する免責事項 (Threat Disclaimer)] で [システムが生成 (System Generated)] を選択します。

アプライアンスは、メッセージの内容についてユーザに警告するためにメッセージ本文の上に免責事項を挿入できます。この例では、システムが生成した脅威に関する免責事項を使用します。

図 C-11 アウトブレイク フィルタの設定
Mail Policies: Outbreak Filters

Outbreak Filtering for Policy: Sales_Team
[Enable Outbreak Filtering (Customize settings)]

Outbreak Filter Settings

Quarantine Threat Level: 3

Maximum Quarantine Retention: Viral Attachments: 1 Days, Other Threats: 4 Hours

Bypass Attachment Scanning: Select File Extension... File Extensions to Bypass: None defined

Message Modification

Enable Message Modification

Message Modification Threat Level: 3

Message Subject: Prepend [MODIFIED FOR PROTECTION]

URL Rewriting: Cisco Security proxy scans and rewrites suspicious or malicious URLs.
 Enable only for unsigned messages (recommended)
 Enable for all messages
 Disable

Bypass Domain Scanning: example.com
(examples: example.com, crm.example.com, 10.0.0.1, 10.0.0.0/24)

Threat Disclaimer: System Generated
Preview Disclaimer

Disclaimer text will be applied to the top of the message body for Suspicious and Quarantined messages. To create custom disclaimers go to Mail Policies > Text Resources

Cancel Submit

ステップ 9 変更内容を送信し、確定します。

このシェーディングは、ポリシーがデフォルトポリシーとは異なる設定を使用していることを示します。

図 C-12 変更されたエンジニアリングポリシーのウイルスフィルタ設定

| Order | Policy Name | Anti-Spam | Anti-Virus | Content Filters | Outbreak Filters | Delete |
|-------|----------------|---|--|-----------------|---|--------|
| 1 | Sales_Team | IronPort Anti-Spam
Positive: Drop
Suspected: Quarantine
Marketing Messages: Quarantine | (use default) | (use default) | (use default) | |
| 2 | Engineering | (use default) | (use default) | (use default) | Retention Time:
Virus: 1 day
Other: 4 hours | |
| | Default Policy | IronPort Anti-Spam
Positive: Quarantine
Suspected: Quarantine
Marketing Messages: Disabled | Sophos
Encrypted: Deliver
Unscannable: Deliver
Virus Positive: Drop | Disabled | Retention Time:
Virus: 1 day | |

この時点では、ファイル拡張子が dwg である添付ファイルを含む任意のメッセージ、および受信者がエンジニアリング チーム ポリシーで定義されている受信者とマッチングする任意のメッセージは、アウトブレイク フィルタ スキャンをバイパスし、処理を続行します。example.com ドメインへのリンクを含むメッセージは、Cisco セキュリティ プロキシを介してリダイレクトするようにリンクを修正されることはなく、疑わしいと見なされません。

メールポリシーでの送信者または受信者の検索

[ポリシー検索 (Find Policies)] ボタンを使用して、[受信メールポリシー (Incoming Mail Policies)] または [送信メールポリシー (Outgoing Mail Policies)] ページで定義されているポリシーですでに定義されているユーザを検索します。

たとえば、joe@example.com と入力して、[ポリシー検索 (Find Policies)] ボタンをクリックすると、ポリシーとマッチングする特定の定義済みユーザを含むポリシーを示す結果が表示されます。

図 C-13 ポリシーでのユーザの検索

Find Policies

Email Address:
 Recipient
 Sender
 Find Policies

Results: Email Address "Recipient: joe@example.com" is defined in the following policies:

- Engineering
- Default Policy (all users)

Policies matching "joe@example.com"

| Order | Policy Name | Anti-Spam | Anti-Virus | Content Filters | Outbreak Filters | Delete |
|-------|----------------|---|--|-----------------|---|--------|
| 2 | Engineering | (use default) | (use default) | (use default) | Retention Time:
Virus: 1 day
Other: 4 hours | |
| | Default Policy | IronPort Anti-Spam
Positive: Quarantine
Suspected: Quarantine
Marketing Messages: Disabled | Sophos
Encrypted: Deliver
Unscannable: Deliver
Virus Positive: Drop | Disabled | Retention Time:
Virus: 1 day | |

ポリシーの名前をクリックして、[ポリシー設定を編集 (Edit Policy)] ページに移動してそのポリシーのユーザを編集します。

ユーザを検索する場合、デフォルト ポリシーは常に表示されるため注意してください。これは、定義上、送信者または受信者が設定されているポリシーと一致しない場合、デフォルトのポリシーが必ず一致するためです。

管理例外

前述の 2 つの例で示されている手順を使用して、*管理例外*に基づいたポリシーの作成および設定を開始できます。つまり、組織のニーズを評価した後で、メッセージの大部分がデフォルト ポリシーで処理されるように、ポリシーを設定できます。また、必要に応じて、異なるポリシーを管理して、特定のユーザまたはユーザグループの追加「例外」ポリシーを作成できます。このようにすることで、メッセージ分裂が最小化され、ワークキューの各分裂メッセージの処理により受けるシステムパフォーマンスの影響が少なくなります。

スパム、ウイルスおよびポリシー実行に対する組織またはユーザの許容値に基づいて、ポリシーを定義できます。表 C-1 (P.C-12) に、ポリシーの例をいくつか示します。「積極的な」ポリシーでは、エンドユーザのメールボックスに到達するスパムおよびウイルスの量が最小限に抑えられます。「保守的な」ポリシーでは、偽陽性を回避し、ポリシーに関係なく、ユーザによるメッセージの見落としを防ぐことができます。

表 C-1 積極的および保守的なメールポリシーの設定

| | 積極的な設定 | 保守的な設定 |
|----------|--|---|
| スパム対策 | 陽性と判定されたスパム：ドロップ
陽性と疑わしいスパム：隔離
マーケティングメール：メッセージの件名の前に「[Marketing]」が追加されて配信 | 陽性と判定されたスパム：隔離
陽性と疑わしいスパム：メッセージの件名の前に「[Suspected Spam]」が追加されて配信
マーケティングメール：ディセーブル |
| アンチウイルス | 修復されたメッセージ：配信
暗号化されたメッセージ：ドロップ
スキャンできないメッセージ：ドロップ
感染メッセージ：ドロップ | 修復されたメッセージ：配信
暗号化されたメッセージ：隔離
スキャンできないメッセージ：隔離
感染メッセージ：ドロップ |
| ウイルスフィルタ | イネーブル、バイパスできる特定のファイル名拡張子またはドメインなし
すべてのメッセージのメッセージ変更の有効化 | バイパスできるファイル名拡張子またはドメインの有効化
未署名のメッセージのメッセージ変更の有効化 |

コンテンツに基づくメッセージのフィルタリング

この例では、[受信メールポリシー (Incoming Mail Policy)] テーブルで使用される新しいコンテンツフィルタを 3 つ作成します。これらのコンテンツフィルタは、ポリシー管理のカスタム ユーザロールに属す委任管理者が編集できます。次のフィルタを作成します。

1. 「scan_for_confidential」

このフィルタは、文字列「confidential」が含まれているかメッセージをスキャンします。文字列が見つかったら、メッセージのコピーが電子メールエイリアス hr@example.com に送信され、メッセージが Policy 隔離エリアに送信されます。

2. 「no_mp3s」

このフィルタは、MP3 添付ファイルを削除し、MP3 ファイルが削除されたことを受信者に通知します。

3. 「ex_employee」

このコンテンツフィルタは、特定のエンベロープ受信者アドレス (元受信者) に送信されるメッセージをスキャンします。メッセージが一致した場合、特定の通知メッセージがメッセージ送信者に送信され、メッセージがバウンスされます。

コンテンツフィルタを作成したら、各ポリシー (デフォルトポリシーを含む) を設定して、異なる組み合わせで特定のコンテンツフィルタをイネーブルにします。

件名に「Confidential」とあるメッセージの隔離

最初の例のコンテンツフィルタには、1つの条件と2つのアクションが含まれます。

手順

- ステップ 1** [メールポリシー (Mail Policies)] タブをクリックします。
- ステップ 2** [受信コンテンツフィルタ (Incoming Content Filters)] をクリックします。
- ステップ 3** [フィルタを追加 (Add Filter)] ボタンをクリックします。
- ステップ 4** [名前 (Name)] フィールドに、新しいフィルタの名前として `scan_for_confidential` と入力します。
フィルタ名には、ASCII 文字、数字、下線またはダッシュを含めることができます。コンテンツフィルタ名の最初の文字は、文字または下線でなければなりません。
- ステップ 5** [編集可能なユーザ (役割) (Editable By (Roles))] リンクをクリックし、[ポリシー管理者 (Policy Administrator)] を選択し、[OK] をクリックします。
ポリシー管理者ユーザ ロールに属する委任管理者はこのコンテンツフィルタを編集し、自身のメールポリシーで使用できます。
- ステップ 6** [説明 (Description)] フィールドに、説明を入力します。たとえば、`scan all incoming mail for the string 'confidential'` と入力します。
- ステップ 7** [条件を追加 (Add Condition)] をクリックします。
- ステップ 8** [メッセージ本文 (Message Body)] を選択します。
- ステップ 9** [テキストを含む: (Contains text:)] フィールドに `confidential` と入力して、[OK] をクリックします。
[コンテンツフィルタの追加 (Add Content Filter)] ページに、追加される条件が表示されます。
- ステップ 10** [アクションを追加 (Add Action)] をクリックします。
- ステップ 11** [コピーを送信 (Bcc:) (Send Copy To (Bcc:))] を選択します。
- ステップ 12** [メールアドレス (Email Addresses)] フィールドに、`hr@example.com` と入力します。
- ステップ 13** [件名 (Subject)] フィールドに、`[message matched confidential filter]` と入力します。
- ステップ 14** [OK] をクリックします。
[コンテンツフィルタの追加 (Add Content Filter)] ページに、追加されるアクションが表示されます。
- ステップ 15** [アクションを追加 (Add Action)] をクリックします。
- ステップ 16** [隔離 (Quarantine)] を選択します。
- ステップ 17** ドロップダウンメニューで、[ポリシー隔離領域 (Policy quarantine area)] を選択します。
- ステップ 18** [OK] をクリックします。
[コンテンツフィルタの追加 (Add Content Filter)] ページに、追加される2番目のアクションが表示されます。
- ステップ 19** 変更内容を送信し、確定します。
この時点では、コンテンツフィルタは、いずれの着信メールポリシーでもイネーブルになっていません。この例では、新しいコンテンツフィルタをマスターリストに追加しただけの状態です。このコンテンツフィルタはいずれのポリシーにも適用されていないため、アプライアンスによる電子メール処理は、このフィルタの影響を受けません。

メッセージから MP3 添付ファイルを除去

2 番めの例のコンテンツ フィルタには、条件はなく、アクションは 1 つ含まれます。

手順

-
- ステップ 1 [フィルタを追加 (Add Filter)] ボタンをクリックします。
 - ステップ 2 [名前 (Name)] フィールドに、新しいフィルタの名前として `no_mp3s` と入力します。
 - ステップ 3 [編集可能なユーザ (役割) (Editable By (Roles))] リンクをクリックし、[ポリシー管理者 (Policy Administrator)] を選択し、[OK] をクリックします。
 - ステップ 4 [説明 (Description)] フィールドに、説明を入力します。たとえば、`strip all MP3 attachments` と入力します。
 - ステップ 5 [アクションを追加 (Add Action)] をクリックします。
 - ステップ 6 [ファイル情報によって添付ファイルを除去 (Strip Attachment by File Info)] を選択します。
 - ステップ 7 [ファイルタイプが次の場合 (File type is)] を選択します。
 - ステップ 8 ドロップダウン フィールドで、[`-- mp3`] を選択します。
 - ステップ 9 必要な場合、置換メッセージを入力します。
 - ステップ 10 [OK] をクリックします。
 - ステップ 11 変更内容を送信し、確定します。



(注) コンテンツ フィルタを作成するときに条件を指定する必要はありません。条件が定義されていない場合、定義されるアクションは常にルールに適用されます (条件を指定しないことは、`true()` メッセージ フィルタ ルールを使用することと同じで、コンテンツ フィルタがポリシーに適用される場合、すべてのメッセージがマッチングされます)。

元従業員に送られたバウンス メッセージ

3 番めの例のコンテンツ フィルタには、1 つの条件と 2 つのアクションを使用します。

手順

-
- ステップ 1 [フィルタを追加 (Add Filter)] ボタンをクリックします。
 - ステップ 2 [名前: (Name:)] フィールドに、新しいフィルタの名前として `ex_employee` と入力します。
 - ステップ 3 [編集可能なユーザ (役割) (Editable By (Roles))] リンクをクリックし、[ポリシー管理者 (Policy Administrator)] を選択し、[OK] をクリックします。
 - ステップ 4 [説明 (Description)] フィールドに、説明を入力します。たとえば、`bounce messages intended for Doug` と入力します。
 - ステップ 5 [条件を追加 (Add Condition)] をクリックします。
 - ステップ 6 [エンベロープ受信者 (Envelope Recipient)] を選択します。
 - ステップ 7 エンベロープ受信者に対して、[次で始まる (Begins with)] を選択して、`doug@` と入力します。
 - ステップ 8 [OK] をクリックします。

[コンテンツ フィルタ (Content Filters)] ページがリフレッシュされ、追加された条件が表示されます。元従業員の電子メールアドレスを含む LDAP ディレクトリを作成できます。元従業員がそのディレクトリに追加されると、このコンテンツ フィルタは、動的に更新されます。

ステップ 9 [アクションを追加 (Add Action)] をクリックします。

ステップ 10 [通知 (Notify)] を選択します。

ステップ 11 [送信者 (Sender)] チェックボックスを選択して、[件名 (Subject)] フィールドに、message bounced for ex-employee of example.com と入力します。

ステップ 12 [テンプレート利用 (Use template)] セクションで、通知テンプレートを選擇します。



(注) リソースが事前に定義されていないため、コンテンツ フィルタ ルール ビルダのいくつかのセクションは、ユーザ インターフェイスに表示されません。たとえば、コンテンツ ディクショナリ、通知テンプレートおよびメッセージ免責事項は、[メール ポリシー (Mail Policies)] > [辞書 (Dictionaries)] ページ (または CLI の dictionaryconfig コマンド) から事前に設定されていない場合、オプションとして表示されません。ディクショナリの作成の詳細については、「[コンテンツ ディクショナリ](#)」(P.18-2) を参照してください。

ステップ 13 [OK] をクリックします。

[コンテンツ フィルタの追加 (Add Content Filters)] ページに、追加されるアクションが表示されます。

ステップ 14 [アクションを追加 (Add Action)] をクリックします。

ステップ 15 [バウンスする (最終アクション) (Bounce (Final Action))] を選擇して、[OK] をクリックします。

コンテンツ フィルタに指定できる最終アクションは 1 つだけです。複数の最終アクションを追加しようとする、GUI にエラーが表示されます。

このアクションを追加すると、この元従業員へのメッセージの送信者が、通知テンプレートとバウンス通知テンプレートの 2 つのメッセージを受け取る可能性があります。

ステップ 16 変更内容を送信し、確定します。

各受信者のグループごとのコンテンツ フィルタの適用

前述の例では、[受信メール ポリシー (Incoming Mail Policy)] ページを使用して、3 つのコンテンツ フィルタを作成しました。[受信メール ポリシー (Incoming Mail Policy)] および [送信コンテンツ フィルタ (Outgoing Content filters)] ページには、ポリシーに適用できるすべてのコンテンツ フィルタの「マスター リスト」が含まれます。

図 C-14 [受信コンテンツ フィルタ (Incoming Content Filters)]: 作成された 3 つのフィルタ
Incoming Content Filters

| Order | Filter Name | Description Rules Policies | Duplicate | Delete |
|-------|-----------------------|--|-----------|--------|
| 1 | scan_for_confidential | scan all incoming mail for the string 'confidential' | | |
| 2 | no_mp3s | strip all MP3 attachments | | |
| 3 | ex_employee | bounce messages intended for Doug | | |

この例では、[受信コンテンツ フィルタ (Incoming Content Filters)] テーブルで使用される新しいコンテンツ フィルタを 3 つ適用します。

- デフォルト ポリシーには、3 つすべてのコンテンツ フィルタが適用されます。

■ 受信メールポリシーの概要

- エンジニアリンググループには、no_mp3s フィルタは適用されません。
- 販売グループには、デフォルト着信メールポリシーとしてコンテンツフィルタが適用されます。

デフォルトでのすべての受信者のコンテンツフィルタのイネーブル化

リンクをクリックして、個々のポリシーに対してコンテンツフィルタをイネーブルにして選択します。

手順

- ステップ 1** [受信メールポリシー (Incoming Mail Policies)] をクリックして、[受信メールポリシー (Incoming Mail Policy)] テーブルに戻ります。
- ページがリフレッシュされ、デフォルトポリシーおよび「送信者および受信者のグループのメールポリシーの作成」(P.C-4) で追加した2つのポリシーが表示されます。コンテンツフィルタリングは、デフォルトでは、すべてのポリシーでディセーブルにされているため注意してください。
- ステップ 2** デフォルトポリシー行のコンテンツフィルタセキュリティサービス ([コンテンツフィルタ (Content Filters)] 列) のリンクをクリックします。図 C-15 を参照してください。

図 C-15 デフォルト着信メールポリシーのコンテンツフィルタ設定の編集

| Order | Policy Name | Anti-Spam | Anti-Virus | Content Filters | Outbreak Filters | Delete |
|-------|----------------|---|--|-----------------|---|--------|
| 1 | Sales_Team | IronPort Anti-Spam
Positive: Drop
Suspected: Quarantine
Marketing Messages: Quarantine | (use default) | (use default) | (use default) | |
| 2 | Engineering | (use default) | (use default) | (use default) | Retention Time:
Virus: 3 day
Other: 4 hours | |
| | Default Policy | IronPort Anti-Spam
Positive: Quarantine
Suspected: Quarantine
Marketing Messages: Disabled | Sophos
Encrypted: Deliver
Unscannable: Deliver
Virus Positive: Drop | Disabled | Retention Time:
Virus: 3 day | |

- ステップ 3** コンテンツフィルタセキュリティサービス ページで、[コンテンツフィルタリング: デフォルトポリシー (Content Filtering for Default Policy)] の値を [コンテンツフィルタを無効にする (Disable Content Filters)] から [コンテンツフィルタを有効にする (設定をカスタマイズ) (Enable Content Filters (Customize settings))] に変更します。

図 C-16 ポリシーでのコンテンツフィルタのイネーブル化および特定のコンテンツフィルタの選択

| Order | Filter Name | Description | Enable |
|-------|-----------------------|--|--------------------------|
| 1 | scan_for_confidential | scan all incoming mail for the string 'confidential' | <input type="checkbox"/> |
| 2 | no_mp3s | strip all MP3 attachments | <input type="checkbox"/> |
| 3 | ex_employee | bounce messages intended for Doug | <input type="checkbox"/> |

マスターリストで定義されているコンテンツフィルタ ([受信コンテンツフィルタ (Incoming Content Filters)] ページを使用して「コンテンツフィルタの概要」(P.11-1) で作成されたフィルタ) が、このページに表示されます。値を [コンテンツフィルタを有効にする (設定をカスタマイズ) (Enable Content Filters (Customize settings))] に変更すると、各フィルタのチェックボックスがディセーブル (グレー表示) からイネーブルに変わります。

- ステップ 4** 各コンテンツフィルタの [有効 (Enable)] チェックボックスをオンにします。
- ステップ 5** [送信 (Submit)] をクリックします。

[受信メールポリシー (Incoming Mail Policies)] ページのテーブルは、デフォルトポリシーでイネーブルにされているフィルタの名前を示します。

図 C-17 デフォルト着信メールポリシーでイネーブルにされた3つのコンテンツフィルタ

| | | | |
|----------------|---|--|---|
| Default Policy | IronPort Anti-Spam
Positive: Quarantine
Suspected: Quarantine
Marketing Messages: Disabled | Sophos
Encrypted: Deliver
Unscannable: Deliver
Virus Positive: Drop | scan_for_confidential
no_mp3s
ex_employee |
|----------------|---|--|---|

エンジニアリングの受信者への MP3 添付ファイルの許可

「エンジニアリング」ポリシーの「no_mp3s」コンテンツフィルタをディセーブルにするには、次の手順を実行します。

手順

- ステップ 1** エンジニアリング チーム ポリシー行の [コンテンツフィルタ セキュリティ サービス (Content Filters security service)] ([コンテンツフィルタ (Content Filters)] 列) のリンクをクリックします。
- ステップ 2** コンテンツフィルタ セキュリティ サービス ページで、[ポリシーのコンテンツフィルタリング: エンジニアリング (Content Filtering for Policy: Engineering)] の値を [コンテンツフィルタを有効にする (デフォルトのメールポリシー設定を継承) (Enable Content Filtering (Inherit default policy settings))] から [コンテンツフィルタを有効にする (設定をカスタマイズ) (Enable Content Filters (Customize settings))] に変更します。
- このポリシーはデフォルト値を使用していたため、値を [デフォルト設定を使用 (Use Default Settings)] から [はい (Yes)] に変更すると、各フィルタのチェックボックスがディセーブル (グレー表示) からイネーブルに変わります。
- ステップ 3** 「no_mp3s」フィルタのチェックボックスの選択を解除します。

図 C-18 コンテンツフィルタの選択解除
Mail Policies: Content Filters

| Order | Filter Name | Description | Enable |
|-------|-----------------------|--|-------------------------------------|
| 1 | scan_for_confidential | scan all incoming mail for the string 'confidential' | <input checked="" type="checkbox"/> |
| 2 | no_mp3s | strip all MP3 attachments | <input type="checkbox"/> |
| 3 | ex_employee | bounce messages intended for Doug | <input checked="" type="checkbox"/> |

- ステップ 4** [送信 (Submit)] をクリックします。
- [受信メールポリシー (Incoming Mail Policies)] ページのテーブルは、エンジニアリングポリシーでイネーブルにされているフィルタの名前を示します。

図 C-19 コンテンツフィルタが更新された [受信メールポリシー (Incoming Mail Policies)]

| Order | Policy Name | Anti-Spam | Anti-Virus | Content Filters | Outbreak Filters | Delete |
|-------|----------------|---|--|---|---|--------|
| 1 | Sales_Team | IronPort Anti-Spam
Positive: Drop
Suspected: Quarantine
Marketing Messages: Quarantine | (use default) | (use default) | (use default) | |
| 2 | Engineering | (use default) | (use default) | scan_for_confidential
ex_employee | Retention Time:
Virus: 1 day
Other: 4 hours | |
| | Default Policy | IronPort Anti-Spam
Positive: Quarantine
Suspected: Quarantine
Marketing Messages: Disabled | Sophos
Encrypted: Deliver
Unscannable: Deliver
Virus Positive: Drop | scan_for_confidential
no_mp3s
ex_employee | Retention Time:
Virus: 1 day | |

- ステップ 5** 変更内容を確定します。

この時点では、エンジニアリングポリシーのユーザリストと一致する着信メッセージで MP3 添付ファイルは削除されません。ただし、他のすべての着信メッセージでは、MP3 添付ファイルが削除されません。

GUI でのコンテンツフィルタの設定に関する注意事項

- コンテンツフィルタを作成するときに条件を指定する必要はありません。アクションが定義されていない場合、定義されるアクションは常にルールに適用されます（アクションを指定しないことは、true() メッセージフィルタルールを使用することと同じで、コンテンツフィルタがポリシーに適用される場合、すべてのメッセージが一致します）。
- カスタムユーザロールをコンテンツフィルタに割り当てていない場合、パブリックのコンテンツフィルタになり、メールポリシーの任意の委任管理者が使用できます。委任管理者とコンテンツフィルタの詳細については、「[管理タスクの分散](#)」を参照してください。
- 管理者とオペレータは、コンテンツフィルタがカスタムユーザロールに割り当てられていない場合でも、アプライアンスのすべてのコンテンツフィルタを表示および編集できます。
- フィルタルールおよびアクションのテキストを入力する場合、正規表現照合において、次のメタ文字に特殊な意味があります。^ \$ * + ? { [] \ | ()
正規表現を使用しない場合、「\」（バックスラッシュ）を使用して、これらの任意の文字をエスケープする必要があります。たとえば、「*Warning*」と入力します。
- コンテンツフィルタに複数の条件を定義する場合、コンテンツフィルタが一致したと見なされるために、定義されるアクションのすべて（論理 AND）、または定義されたいずれかのアクション（論理 OR）の適用が必要かどうかを定義できます。

図 C-20 任意またはすべての条件の選択

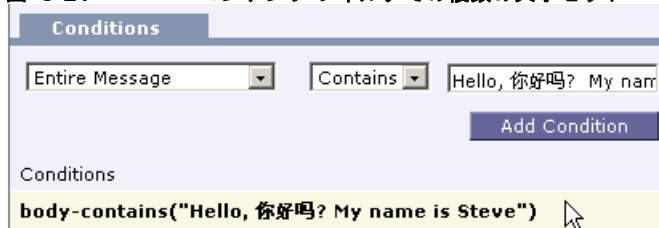
| Add Filter | |
|-----------------------------|--|
| Name: | <input type="text"/> |
| Currently used by policies: | |
| Description: | <input type="text"/> |
| Order: | 5 |
| Apply filter: | <input checked="" type="radio"/> If one or more conditions match
<input type="radio"/> Only if ALL conditions match |

- 「benign」コンテンツフィルタを作成して、メッセージ分裂およびコンテンツフィルタをテストできます。たとえば、唯一のアクションが「配信」であるコンテンツフィルタを作成できます。このコンテンツフィルタは、メール処理に影響を与えませんが、このフィルタを使用して、メールポリシー処理が、システムの他の要素（たとえば、メールログ）に影響を与えているかテストできます。
- 逆に、着信または発信コンテンツフィルタの「マスターリスト」の概念を使用して、アプライアンスにより処理されるすべてのメールのメッセージ処理に即時に影響を与える、非常に優れた、広範囲に及ぶコンテンツフィルタを作成できます。このコンテンツフィルタは次のように作成できます。
 - [受信コンテンツフィルタ (Incoming Content Filters)] または [送信コンテンツフィルタ (Outgoing Content filters)] ページを使用して、順序が 1 の新しいコンテンツフィルタを作成します。
 - [受信メールポリシー (Incoming Mail Policies)] または [送信メールポリシー (Outgoing Mail Policies)] ページを使用して、デフォルトポリシーの新しいコンテンツフィルタをイネーブルにします。

- 残りすべてのポリシーでこのコンテンツフィルタをイネーブルにします。
- コンテンツフィルタで使用できる [Bcc:] および [隔離 (Quarantine)] アクションは、作成する隔離エリアの保持設定に役に立ちます（詳細については、第 27 章「隔離」を参照してください）。メッセージがすぐにはシステムからリリースされないようにするため（つまり、隔離エリアの割り当てディスク領域がすぐにいっぱいにならないようにするため）、ポリシー隔離とのメールフローをシミュレートするフィルタを作成できます。
- scanconfig コマンドと同じ設定が使用されるため、「Entire Message」条件は、メッセージのヘッダーをスキャンしません。「Entire Message」を選択すると、メッセージ本文および添付ファイルだけがスキャンされます。特定のヘッダー情報を検索するには、「Subject」または「Header」条件を使用します。
- LDAP クエリーによるユーザの設定は、アプライアンスで LDAP サーバが設定されている場合（つまり、ldapconfig コマンドを使用して特定の文字列を含む特定の LDAP サーバをクエリーするようにアプライアンスが設定されている場合）だけ GUI に表示されます。
- リソースが事前に定義されていないため、コンテンツフィルタルールビルダのいくつかのセクションは、GUI に表示されません。たとえば、通知テンプレートおよびメッセージ免責事項は、[テキストリソース (Text Resources)] ページまたは CLI の textconfig コマンドを使用して事前に設定されていない場合、オプションとして表示されません。
- コンテンツフィルタ機能は、次の文字エンコーディングのテキストを認識し、これらを追加およびスキャンできます。
 - Unicode (UTF-8)
 - Unicode (UTF-16)
 - Western European/Latin-1 (ISO 8859-1)
 - Western European/Latin-1 (Windows CP1252)
 - 中国語 (繁体字) (Big 5)
 - 中国語 (簡体字) (GB 2312)
 - 中国語 (簡体字) (HZ GB 2312)
 - 韓国語 (ISO 2022-KR)
 - 韓国語 (KS-C-5601/EUC-KR)
 - 日本語 (Shift-JIS (X0123))
 - 日本語 (ISO-2022-JP)
 - 日本語 (EUC)

複数の文字セットを 1 つのコンテンツフィルタ内で組み合わせてマッチングできます。複数の文字エンコーディングでのテキストの表示および入力については、Web ブラウザのマニュアルを参照してください。ほとんどのブラウザでは、複数の文字セットを同時にレンダリングできます。

図 C-21 コンテンツフィルタでの複数の文字セット



- 着信または発信コンテンツフィルタの要約ページで、[説明 (Description)]、[ルール (Rules)] および [ポリシー (Policies)] のリンクを使用して、コンテンツフィルタに提供されているビューを変更します。
 - [説明 (Description)] ビューには、各コンテンツフィルタの説明フィールドに入力したテキストが表示されます (これはデフォルトビューです)。
 - [ルール (Rules)] ビューには、ルールビルダページにより構築されたルールおよび正規表現が表示されます。
 - [ポリシー (Policies)] ビューには、イネーブルにされている各コンテンツフィルタのポリシーが表示されます。

図 C-22 コンテンツフィルタの [説明 (Description)]、[ルール (Rules)] および [ポリシー (Policy)] を切り替えるリンクの使用
Incoming Content Filters

| Filters | | | | |
|---------------|------------------------|---|-----------|--------|
| Add Filter... | | | | |
| Order | Filter Name | Description Rules Policies | Duplicate | Delete |
| 1 | scan_for_confidential | scan_for_confidential: if (body-contains("confidential")) { quarantine ("Policy"); bcc ("hr@example.com", "[message matched confidential filter]"); } | | |
| 2 | no_mp3s | no_mp3s: if (true) { drop-attachments-by-filetype("mp3", "mp3 deleted"); } | | |
| 3 | ex_employee | ex_employee: if (rcpt-to == "^doug@") { notify-copy ("%EnvelopeSender", "message bounced for ex-employee of example.com"); bounce(); } | | |
| 4 | drop_large_attachments | drop_large_attachments: if (true) { drop-attachments-by-size(5242880, "This attachment was too big"); } | | |



APPENDIX **D**

ファイアウォール情報

次の表は、Cisco アプライアンスを正常に動作させるために開けなければならないことがあるポートのリストです（デフォルト値を示す）。

表 D-1 ファイアウォール ポート

| ポート | プロトコル | In/Out | ホスト名 | 説明 |
|-------|---------|------------|--------------------|--|
| 20/21 | TCP | In または Out | AsyncOS IP、FTP サーバ | ログ ファイルのアグリゲーションの FTP。
データ ポート TCP 1024 以上すべて開いておく必要があります。
詳細については、ナレッジ ベースの FTP ポート情報を検索してください。
「Knowledge Base」(P.1-6) を参照してください。 |
| 22 | TCP | In | AsyncOS IP | CLI への SSH アクセス、ログ ファイルのアグリゲーション。 |
| 22 | TCP | Out | SSH サーバ | ログ ファイルの SSH アグリゲーション。 |
| 22 | TCP | Out | SCP サーバ | ログ サーバへの SCP 配信。 |
| 23 | Telnet | In | AsyncOS IP | CLI への Telnet アクセス、ログ ファイルのアグリゲーション。 |
| 23 | Telnet | Out | Telnet サーバ | Telnet アップグレード、ログ ファイルのアグリゲーション（非推奨）。 |
| 25 | TCP | Out | Any | 電子メール送信用 SMTP。 |
| 25 | TCP | In | AsyncOS IP | バウンスされた電子メールを受信する SMTP または外部のファイアウォールから電子メールをインジェクトする場合。 |
| 53 | UDP/TCP | In および Out | DNS サーバ | インターネット ルート サーバまたはファイアウォール外部の DNS サーバを使用するように設定されている場合の DNS。また、SenderBase クエリーの場合。 |
| 80 | HTTP | In | AsyncOS IP | システム モニタリングのための GUI への HTTP アクセス。 |

表 D-1 ファイアウォールポート (続き)

| | | | | |
|-------------|---------|------------|---------------------------------|---|
| 80 | HTTP | Out | downloads.ironport.com | AsyncOS アップグレードおよび McAfee 定義を除くサービス更新。 |
| 80 | HTTP | Out | updates.ironport.com | AsyncOS アップグレードおよび McAfee ウイルス対策。 |
| 80 | HTTP | Out | cdn-microuupdates.cloudmark.com | Intelligent MultiScan 機能のサードパーティ スпам コンポーネントへの更新に使われます。アプライアンスは、サードパーティの phone home の更新の CIDR 範囲 208.83.136.0/22 に接続する必要があります。 |
| 82 | HTTP | In | AsyncOS IP | Cisco Anti-Spam 隔離の表示に使用します。 |
| 83 | HTTPS | In | AsyncOS IP | Cisco Anti-Spam 隔離の表示に使用します。 |
| 110 | TCP | Out | POP サーバ | Cisco スпам隔離のためのエンドユーザの POP 認証。 |
| 123 | UDP | In および Out | NTP サーバ | タイム サーバがファイアウォール外部の場合、NTP。 |
| 143 | TCP | Out | IMAP サーバ | Cisco スпам隔離のためのエンドユーザの IMAP 認証 |
| 161 | UDP | In | AsyncOS IP | SNMP クエリー |
| 162 | UDP | Out | 管理ステーション | SNMP トラップ |
| 389
3268 | LDAP | Out | LDAP サーバ | LDAP ディレクトリ サーバがファイアウォール外部の場合、LDAP。Cisco スпам隔離のための LDAP 認証 |
| 636
3269 | LDAPS | Out | LDAPS | LDAPS — ActiveDirectory のグローバルカタログ サーバ (SSL 使用) |
| 443 | TCP | In | AsyncOS IP | システム モニタリングのための GUI への HTTP (https) アクセス。 |
| 443 | TCP | Out | res.cisco.com | Cisco Registered Envelope Service |
| 443 | TCP | Out | updates-manifests.ironport.com | アップデート サーバの最新のファイルを確認します。 |
| 443 | TCP | Out | phonehome.senderbase.org | アウトブレイク フィルタの受信/送信 |
| 514 | UDP/TCP | Out | Syslog サーバ | Syslog ロギング |
| 628 | TCP | In | AsyncOS IP | 外部ファイアウォールから電子メールをインジェクトする場合の QMQP。 |
| 1024 以上 | — | — | — | ポート 21 (FTP) については、上記の情報を参照してください。 |
| 2222 | CCS | In および Out | AsyncOS IP | クラスタ通信サービス (中央集中管理用)。 |

表 D-1 ファイアウォール ポート (続き)

| | | | | |
|------|-----|---------------|------------|---|
| 6025 | TCP | Out | AsyncOS IP | Cisco スпам隔離 |
| 7025 | TCP | In および
Out | AsyncOS IP | この機能を集中化する場合、電子メールセキュリティアプライアンスと Cisco コンテンツセキュリティ管理アプライアンス間でポリシー、ウイルス、アウトブレイク隔離データを渡します。 |



APPENDIX **E**

End User License Agreement

Cisco Systems End User License Agreement

IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. IT IS VERY IMPORTANT THAT YOU CHECK THAT YOU ARE PURCHASING CISCO SOFTWARE OR EQUIPMENT FROM AN APPROVED SOURCE AND THAT YOU, OR THE ENTITY YOU REPRESENT (COLLECTIVELY, THE "CUSTOMER") HAVE BEEN REGISTERED AS THE END USER FOR THE PURPOSES OF THIS CISCO END USER LICENSE AGREEMENT. IF YOU ARE NOT REGISTERED AS THE END USER YOU HAVE NO LICENSE TO USE THE SOFTWARE AND THE LIMITED WARRANTY IN THIS END USER LICENSE AGREEMENT DOES NOT APPLY. ASSUMING YOU HAVE PURCHASED FROM AN APPROVED SOURCE, DOWNLOADING, INSTALLING OR USING CISCO OR CISCO-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.

CISCO SYSTEMS, INC. OR ITS SUBSIDIARY LICENSING THE SOFTWARE INSTEAD OF CISCO SYSTEMS, INC. ("CISCO") IS WILLING TO LICENSE THIS SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU PURCHASED THE SOFTWARE FROM AN APPROVED SOURCE AND THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS END USER LICENSE AGREEMENT PLUS ANY ADDITIONAL LIMITATIONS ON THE LICENSE SET FORTH IN A SUPPLEMENTAL LICENSE AGREEMENT ACCOMPANYING THE PRODUCT OR AVAILABLE AT THE TIME OF YOUR ORDER (COLLECTIVELY THE "AGREEMENT"). TO THE EXTENT OF ANY CONFLICT BETWEEN THE TERMS OF THIS END USER LICENSE AGREEMENT AND ANY SUPPLEMENTAL LICENSE AGREEMENT, THE SUPPLEMENTAL LICENSE AGREEMENT SHALL APPLY. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU ARE REPRESENTING THAT YOU PURCHASED THE SOFTWARE FROM AN APPROVED SOURCE AND BINDING YOURSELF TO THE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED CD PACKAGE AND ANY WRITTEN MATERIALS) FOR A FULL REFUND, OR, IF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM AN APPROVED SOURCE, AND APPLIES ONLY IF YOU ARE THE ORIGINAL AND REGISTERED END USER PURCHASER. FOR THE PURPOSES OF THIS END USER LICENSE AGREEMENT, AN "APPROVED SOURCE" MEANS (A) CISCO; OR (B) A DISTRIBUTOR OR SYSTEMS INTEGRATOR AUTHORIZED BY CISCO TO DISTRIBUTE / SELL CISCO EQUIPMENT, SOFTWARE AND SERVICES WITHIN YOUR TERRITORY TO END USERS; OR (C) A RESELLER AUTHORIZED BY ANY SUCH DISTRIBUTOR OR SYSTEMS INTEGRATOR

IN ACCORDANCE WITH THE TERMS OF THE DISTRIBUTOR'S AGREEMENT WITH CISCO TO DISTRIBUTE / SELL THE CISCO EQUIPMENT, SOFTWARE AND SERVICES WITHIN YOUR TERRITORY TO END USERS.

THE FOLLOWING TERMS OF THE AGREEMENT GOVERN CUSTOMER'S USE OF THE SOFTWARE (DEFINED BELOW), EXCEPT TO THE EXTENT: (A) THERE IS A SEPARATE SIGNED CONTRACT BETWEEN CUSTOMER AND CISCO GOVERNING CUSTOMER'S USE OF THE SOFTWARE, OR (B) THE SOFTWARE INCLUDES A SEPARATE "CLICK-ACCEPT" LICENSE AGREEMENT OR THIRD PARTY LICENSE AGREEMENT AS PART OF THE INSTALLATION OR DOWNLOAD PROCESS GOVERNING CUSTOMER'S USE OF THE SOFTWARE. TO THE EXTENT OF A CONFLICT BETWEEN THE PROVISIONS OF THE FOREGOING DOCUMENTS, THE ORDER OF PRECEDENCE SHALL BE (1) THE SIGNED CONTRACT, (2) THE CLICK-ACCEPT AGREEMENT OR THIRD PARTY LICENSE AGREEMENT, AND (3) THE AGREEMENT. FOR PURPOSES OF THE AGREEMENT, "SOFTWARE" SHALL MEAN COMPUTER PROGRAMS, INCLUDING FIRMWARE AND COMPUTER PROGRAMS EMBEDDED IN CISCO EQUIPMENT, AS PROVIDED TO CUSTOMER BY AN APPROVED SOURCE, AND ANY UPGRADES, UPDATES, BUG FIXES OR MODIFIED VERSIONS THERETO (COLLECTIVELY, "UPGRADES"), ANY OF THE SAME WHICH HAS BEEN RELICENSED UNDER THE CISCO SOFTWARE TRANSFER AND RE-LICENSING POLICY (AS MAY BE AMENDED BY CISCO FROM TIME TO TIME) OR BACKUP COPIES OF ANY OF THE FOREGOING.

License. Conditioned upon compliance with the terms and conditions of the Agreement, Cisco grants to Customer a nonexclusive and nontransferable license to use for Customer's internal business purposes the Software and the Documentation for which Customer has paid the required license fees to an Approved Source. "Documentation" means written information (whether contained in user or technical manuals, training materials, specifications or otherwise) pertaining to the Software and made available by an Approved Source with the Software in any manner (including on CD-Rom, or on-line). In order to use the Software, Customer may be required to input a registration number or product authorization key and register Customer's copy of the Software online at Cisco's website to obtain the necessary license key or license file.

Customer's license to use the Software shall be limited to, and Customer shall not use the Software in excess of, a single hardware chassis or card or such other limitations as are set forth in the applicable Supplemental License Agreement or in the applicable purchase order which has been accepted by an Approved Source and for which Customer has paid to an Approved Source the required license fee (the "Purchase Order").

Unless otherwise expressly provided in the Documentation or any applicable Supplemental License Agreement, Customer shall use the Software solely as embedded in, for execution on, or (where the applicable Documentation permits installation on non-Cisco equipment) for communication with Cisco equipment owned or leased by Customer and used for Customer's internal business purposes. No other licenses are granted by implication, estoppel or otherwise.

For evaluation or beta copies for which Cisco does not charge a license fee, the above requirement to pay license fees does not apply.

General Limitations. This is a license, not a transfer of title, to the Software and Documentation, and Cisco retains ownership of all copies of the Software and Documentation. Customer acknowledges that the Software and Documentation contain trade secrets of Cisco or its suppliers or licensors, including but not limited to the specific internal design and structure of individual programs and associated interface information. Except as otherwise expressly provided under the Agreement, Customer shall only use the Software in connection with the use of Cisco equipment purchased by the Customer from an Approved Source and Customer shall have no right, and Customer specifically agrees not to:

(i) transfer, assign or sublicense its license rights to any other person or entity (other than in compliance with any Cisco relicensing/transfer policy then in force), or use the Software on Cisco equipment not purchased by the Customer from an Approved Source or on secondhand Cisco equipment, and Customer acknowledges that any attempted transfer, assignment, sublicense or use shall be void;

- (ii) make error corrections to or otherwise modify or adapt the Software or create derivative works based upon the Software, or permit third parties to do the same;
- (iii) reverse engineer or decompile, decrypt, disassemble or otherwise reduce the Software to human-readable form, except to the extent otherwise expressly permitted under applicable law notwithstanding this restriction or except to the extent that Cisco is legally required to permit such specific activity pursuant to any applicable open source license;
- (iv) publish any results of benchmark tests run on the Software;
- (v) use or permit the Software to be used to perform services for third parties, whether on a service bureau or time sharing basis or otherwise, without the express written authorization of Cisco; or
- (vi) disclose, provide, or otherwise make available trade secrets contained within the Software and Documentation in any form to any third party without the prior written consent of Cisco. Customer shall implement reasonable security measures to protect such trade secrets.

To the extent required by applicable law, and at Customer's written request, Cisco shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of Cisco's applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Cisco makes such information available.

Software, Upgrades and Additional Copies. NOTWITHSTANDING ANY OTHER PROVISION OF THE AGREEMENT: (1) CUSTOMER HAS NO LICENSE OR RIGHT TO MAKE OR USE ANY ADDITIONAL COPIES OR UPGRADES UNLESS CUSTOMER, AT THE TIME OF MAKING OR ACQUIRING SUCH COPY OR UPGRADE, ALREADY HOLDS A VALID LICENSE TO THE ORIGINAL SOFTWARE AND HAS PAID THE APPLICABLE FEE TO AN APPROVED SOURCE FOR THE UPGRADE OR ADDITIONAL COPIES; (2) USE OF UPGRADES IS LIMITED TO CISCO EQUIPMENT SUPPLIED BY AN APPROVED SOURCE FOR WHICH CUSTOMER IS THE ORIGINAL END USER PURCHASER OR LESSEE OR OTHERWISE HOLDS A VALID LICENSE TO USE THE SOFTWARE WHICH IS BEING UPGRADED; AND (3) THE MAKING AND USE OF ADDITIONAL COPIES IS LIMITED TO NECESSARY BACKUP PURPOSES ONLY.

Proprietary Notices. Customer agrees to maintain and reproduce all copyright, proprietary, and other notices on all copies, in any form, of the Software in the same form and manner that such copyright and other proprietary notices are included on the Software. Except as expressly authorized in the Agreement, Customer shall not make any copies or duplicates of any Software without the prior written permission of Cisco.

Term and Termination. The Agreement and the license granted herein shall remain effective until terminated. Customer may terminate the Agreement and the license at any time by destroying all copies of Software and any Documentation. Customer's rights under the Agreement will terminate immediately without notice from Cisco if Customer fails to comply with any provision of the Agreement. Upon termination, Customer shall destroy all copies of Software and Documentation in its possession or control. All confidentiality obligations of Customer, all restrictions and limitations imposed on the Customer under the section titled "General Limitations" and all limitations of liability and disclaimers and restrictions of warranty shall survive termination of this Agreement. In addition, the provisions of the sections titled "U.S. Government End User Purchasers" and "General Terms Applicable to the Limited Warranty Statement and End User License Agreement" shall survive termination of the Agreement.

Customer Records. Customer grants to Cisco and its independent accountants the right to examine Customer's books, records and accounts during Customer's normal business hours to verify compliance with this Agreement. In the event such audit discloses non-compliance with this Agreement, Customer shall promptly pay to Cisco the appropriate license fees, plus the reasonable cost of conducting the audit.

Export, Re-Export, Transfer and Use Controls. The Software, Documentation and technology or direct products thereof (hereafter referred to as Software and Technology), supplied by Cisco under the Agreement are subject to export controls under the laws and regulations of the United States (U.S.) and any other applicable countries' laws and regulations. Customer shall comply with such laws and regulations governing export, re-export, transfer and use of Cisco Software and Technology and will obtain all required U.S. and local authorizations, permits, or licenses. Cisco and Customer each agree to provide the other information, support documents, and assistance as may reasonably be required by the other in connection with securing authorizations or licenses. Information regarding compliance with export, re-export, transfer and use may be located at the following URL:

http://www.cisco.com/web/about/doing_business/legal/global_export_trade/general_export_contract_compliance.html.

U.S. Government End User Purchasers. The Software and Documentation qualify as "commercial items," as that term is defined at Federal Acquisition Regulation ("FAR") (48 C.F.R.) 2.101, consisting of "commercial computer software" and "commercial computer software documentation" as such terms are used in FAR 12.212. Consistent with FAR 12.212 and DoD FAR Supp. 227.7202-1 through 227.7202-4, and notwithstanding any other FAR or other contractual clause to the contrary in any agreement into which the Agreement may be incorporated, Customer may provide to Government end user or, if the Agreement is direct, Government end user will acquire, the Software and Documentation with only those rights set forth in the Agreement. Use of either the Software or Documentation or both constitutes agreement by the Government that the Software and Documentation are "commercial computer software" and "commercial computer software documentation," and constitutes acceptance of the rights and restrictions herein.

Identified Components; Additional Terms. The Software may contain or be delivered with one or more components, which may include third-party components, identified by Cisco in the Documentation, readme.txt file, third-party click-accept or elsewhere (e.g. on www.cisco.com) (the "Identified Component(s)") as being subject to different license agreement terms, disclaimers of warranties, limited warranties or other terms and conditions (collectively, "Additional Terms") than those set forth herein. You agree to the applicable Additional Terms for any such Identified Component(s)."

Limited Warranty

Subject to the limitations and conditions set forth herein, Cisco warrants that commencing from the date of shipment to Customer (but in case of resale by an Approved Source other than Cisco, commencing not more than ninety (90) days after original shipment by Cisco), and continuing for a period of the longer of (a) ninety (90) days or (b) the warranty period (if any) expressly set forth as applicable specifically to software in the warranty card accompanying the product of which the Software is a part (the "Product") (if any): (a) the media on which the Software is furnished will be free of defects in materials and workmanship under normal use; and (b) the Software substantially conforms to the Documentation. The date of shipment of a Product by Cisco is set forth on the packaging material in which the Product is shipped. Except for the foregoing, the Software is provided "AS IS". This limited warranty extends only to the Software purchased from an Approved Source by a Customer who is the first registered end user. Customer's sole and exclusive remedy and the entire liability of Cisco and its suppliers under this limited warranty will be (i) replacement of defective media and/or (ii) at Cisco's option, repair, replacement, or refund of the purchase price of the Software, in both cases subject to the condition that any error or defect constituting a breach of this limited warranty is reported to the Approved Source supplying the Software to Customer, within the warranty period. Cisco or the Approved Source supplying the Software to Customer may, at its option, require return of the Software and/or Documentation as a condition to the remedy. In no event does Cisco warrant that the Software is error free or that Customer will be able to operate the Software without problems or interruptions. In addition, due to the continual development of new techniques for intruding upon and attacking networks, Cisco does not warrant that the Software or any equipment, system or network on which the Software is used will be free of vulnerability to intrusion or attack.

Restrictions. This warranty does not apply if the Software, Product or any other equipment upon which the Software is authorized to be used (a) has been altered, except by Cisco or its authorized representative, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Cisco, (c) has been subjected to abnormal physical or electrical stress, abnormal environmental conditions, misuse, negligence, or accident; or (d) is licensed for beta, evaluation, testing or demonstration purposes. The Software warranty also does not apply to (e) any temporary Software modules; (f) any Software not posted on Cisco's Software Center; (g) any Software that Cisco expressly provides on an "AS IS" basis on Cisco's Software Center; (h) any Software for which an Approved Source does not receive a license fee; and (i) Software supplied by any third party which is not an Approved Source.

DISCLAIMER OF WARRANTY

EXCEPT AS SPECIFIED IN THIS WARRANTY SECTION, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, SATISFACTORY QUALITY, NON-INTERFERENCE, ACCURACY OF INFORMATIONAL CONTENT, OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW AND ARE EXPRESSLY DISCLAIMED BY CISCO, ITS SUPPLIERS AND LICENSORS. TO THE EXTENT THAT ANY OF THE SAME CANNOT BE EXCLUDED, SUCH IMPLIED CONDITION, REPRESENTATION AND/OR WARRANTY IS LIMITED IN DURATION TO THE EXPRESS WARRANTY PERIOD REFERRED TO IN THE "LIMITED WARRANTY" SECTION ABOVE. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY IN SUCH STATES. THIS WARRANTY GIVES CUSTOMER SPECIFIC LEGAL RIGHTS, AND CUSTOMER MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. This disclaimer and exclusion shall apply even if the express warranty set forth above fails of its essential purpose.

Disclaimer of Liabilities - Limitation of Liability. IF YOU ACQUIRED THE SOFTWARE IN THE UNITED STATES, LATIN AMERICA, CANADA, JAPAN OR THE CARIBBEAN, NOTWITHSTANDING ANYTHING ELSE IN THE AGREEMENT TO THE CONTRARY, ALL LIABILITY OF CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS COLLECTIVELY, TO CUSTOMER, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), BREACH OF WARRANTY OR OTHERWISE, SHALL NOT EXCEED THE PRICE PAID BY CUSTOMER TO ANY APPROVED SOURCE FOR THE SOFTWARE THAT GAVE RISE TO THE CLAIM OR IF THE SOFTWARE IS PART OF ANOTHER PRODUCT, THE PRICE PAID FOR SUCH OTHER PRODUCT. THIS LIMITATION OF LIABILITY FOR SOFTWARE IS CUMULATIVE AND NOT PER INCIDENT (I.E. THE EXISTENCE OF TWO OR MORE CLAIMS WILL NOT ENLARGE THIS LIMIT).

IF YOU ACQUIRED THE SOFTWARE IN EUROPE, THE MIDDLE EAST, AFRICA, ASIA OR OCEANIA, NOTWITHSTANDING ANYTHING ELSE IN THE AGREEMENT TO THE CONTRARY, ALL LIABILITY OF CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS COLLECTIVELY, TO CUSTOMER, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), BREACH OF WARRANTY OR OTHERWISE, SHALL NOT EXCEED THE PRICE PAID BY CUSTOMER TO CISCO FOR THE SOFTWARE THAT GAVE RISE TO THE CLAIM OR IF THE SOFTWARE IS PART OF ANOTHER PRODUCT, THE PRICE PAID FOR SUCH OTHER PRODUCT. THIS LIMITATION OF LIABILITY FOR SOFTWARE IS CUMULATIVE AND NOT PER INCIDENT (I.E. THE EXISTENCE OF TWO OR MORE CLAIMS WILL NOT ENLARGE THIS LIMIT). NOTHING IN THE AGREEMENT SHALL LIMIT (I) THE LIABILITY OF CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND

LICENSORS TO CUSTOMER FOR PERSONAL INJURY OR DEATH CAUSED BY THEIR NEGLIGENCE, (II) CISCO'S LIABILITY FOR FRAUDULENT MISREPRESENTATION, OR (III) ANY LIABILITY OF CISCO WHICH CANNOT BE EXCLUDED UNDER APPLICABLE LAW.

Disclaimer of Liabilities - Waiver of Consequential Damages and Other Losses. IF YOU ACQUIRED THE SOFTWARE IN THE UNITED STATES, LATIN AMERICA, THE CARIBBEAN OR CANADA, REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE OR OTHERWISE, IN NO EVENT WILL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR LOST OR DAMAGED DATA, BUSINESS INTERRUPTION, LOSS OF CAPITAL, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY OR WHETHER ARISING OUT OF THE USE OF OR INABILITY TO USE SOFTWARE OR OTHERWISE AND EVEN IF CISCO OR ITS SUPPLIERS OR LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

IF YOU ACQUIRED THE SOFTWARE IN JAPAN, EXCEPT FOR LIABILITY ARISING OUT OF OR IN CONNECTION WITH DEATH OR PERSONAL INJURY, FRAUDULENT MISREPRESENTATION, AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE OR OTHERWISE, IN NO EVENT WILL CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR LOST OR DAMAGED DATA, BUSINESS INTERRUPTION, LOSS OF CAPITAL, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY OR WHETHER ARISING OUT OF THE USE OF OR INABILITY TO USE SOFTWARE OR OTHERWISE AND EVEN IF CISCO OR ANY APPROVED SOURCE OR THEIR SUPPLIERS OR LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IF YOU ACQUIRED THE SOFTWARE IN EUROPE, THE MIDDLE EAST, AFRICA, ASIA OR OCEANIA, IN NO EVENT WILL CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS, BE LIABLE FOR ANY LOST REVENUE, LOST PROFIT, OR LOST OR DAMAGED DATA, BUSINESS INTERRUPTION, LOSS OF CAPITAL, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES, HOWSOEVER ARISING, INCLUDING, WITHOUT LIMITATION, IN CONTRACT, TORT (INCLUDING NEGLIGENCE) OR WHETHER ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF, IN EACH CASE, CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS, HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT FULLY APPLY TO YOU. THE FOREGOING EXCLUSION SHALL NOT APPLY TO ANY LIABILITY ARISING OUT OF OR IN CONNECTION WITH: (I) DEATH OR PERSONAL INJURY, (II) FRAUDULENT MISREPRESENTATION, OR (III) CISCO'S LIABILITY IN CONNECTION WITH ANY TERMS THAT CANNOT BE EXCLUDED UNDER APPLICABLE LAW.

Customer acknowledges and agrees that Cisco has set its prices and entered into the Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the parties.

Controlling Law, Jurisdiction. If you acquired, by reference to the address on the purchase order accepted by the Approved Source, the Software in the United States, Latin America, or the Caribbean, the Agreement and warranties ("Warranties") are controlled by and construed under the laws of the State

of California, United States of America, notwithstanding any conflicts of law provisions; and the state and federal courts of California shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties. If you acquired the Software in Canada, unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of the Province of Ontario, Canada, notwithstanding any conflicts of law provisions; and the courts of the Province of Ontario shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties. If you acquired the Software in Europe, the Middle East, Africa, Asia or Oceania (excluding Australia), unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of England, notwithstanding any conflicts of law provisions; and the English courts shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties. In addition, if the Agreement is controlled by the laws of England, no person who is not a party to the Agreement shall be entitled to enforce or take the benefit of any of its terms under the Contracts (Rights of Third Parties) Act 1999. If you acquired the Software in Japan, unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of Japan, notwithstanding any conflicts of law provisions; and the Tokyo District Court of Japan shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties. If you acquired the Software in Australia, unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of the State of New South Wales, Australia, notwithstanding any conflicts of law provisions; and the State and federal courts of New South Wales shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties. If you acquired the Software in any other country, unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of the State of California, United States of America, notwithstanding any conflicts of law provisions; and the state and federal courts of California shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties.

For all countries referred to above, the parties specifically disclaim the application of the UN Convention on Contracts for the International Sale of Goods. Notwithstanding the foregoing, either party may seek interim injunctive relief in any court of appropriate jurisdiction with respect to any alleged breach of such party's intellectual property or proprietary rights. If any portion hereof is found to be void or unenforceable, the remaining provisions of the Agreement and Warranties shall remain in full force and effect. Except as expressly provided herein, the Agreement constitutes the entire agreement between the parties with respect to the license of the Software and Documentation and supersedes any conflicting or additional terms contained in any Purchase Order or elsewhere, all of which terms are excluded. The Agreement has been written in the English language, and the parties agree that the English version will govern.

Product warranty terms and other information applicable to Cisco products are available at the following URL:

<http://www.cisco.com/go/warranty>

Supplemental End User License Agreement for Cisco Systems Content Security Software

IMPORTANT: READ CAREFULLY

This Supplemental End User License Agreement ("SEULA") contains additional terms and conditions for the Software product licensed under the End User License Agreement ("EULA") between You ("You" as used herein means You and the business entity you represent or "Company") and Cisco (collectively, the "Agreement"). Capitalized terms used in this SEULA but not defined will have the meanings assigned to them in the EULA. To the extent that there is a conflict between the terms and conditions of the EULA and this SEULA, the terms and conditions of this SEULA will take precedence.

In addition to the limitations set forth in the EULA on your access and use of the Software, you agree to comply at all times with the terms and conditions provided in this SEULA.

DOWNLOADING, INSTALLING, OR USING THE SOFTWARE CONSTITUTES ACCEPTANCE OF THE AGREEMENT, AND YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT TO THE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED CD PACKAGE AND ANY WRITTEN MATERIALS) FOR A FULL REFUND, OR, IF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM CISCO OR AN AUTHORIZED CISCO RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL END USER PURCHASER.

For purposes of this SEULA, the Product name and the Product description You have ordered is any of the following Cisco Systems Email Security Appliance ("ESA"), Cisco Systems Web Security Appliance ("WSA") and Cisco Systems Security Management Application ("SMA") (collectively, "Content Security") and their Virtual Appliance equivalent ("Software"):

Cisco AsyncOS for Email

Cisco AsyncOS for Web

Cisco AsyncOS for Management

Cisco Email Anti-Spam, Sophos Anti-Virus

Cisco Email Outbreak Filters

Cloudmark Anti-Spam

Cisco Image Analyzer

McAfee Anti-Virus

Cisco Intelligent Multi-Scan

Cisco RSA Data Loss Prevention

Cisco Email Encryption

Cisco Email Delivery Mode

Cisco Web Usage Controls

Cisco Web Reputation

Sophos Anti-Malware

Webroot Anti-Malware

McAfee Anti-Malware
Cisco Email Reporting
Cisco Email Message Tracking
Cisco Email Centralized Quarantine
Cisco Web Reporting
Cisco Web Policy and Configuration Management
Cisco Advanced Web Security Management with Splunk
Email Encryption for Encryption Appliances
Email Encryption for System Generated Bulk Email
Email Encryption and Public Key Encryption for Encryption Appliances
Large Attachment Handling for Encryption Appliances
Secure Mailbox License for Encryption Appliances

Definitions

For purposes of this SEULA, the following definitions apply:

"Company Service" means the Company's email, Internet, security management services provided to End Users for the purposes of conducting Company's internal business.

"End User" means: (1) for the WSA and SMA, the employee, contractor or other agent authorized by Company to access the Internet and the SMA via the Company Service; and (2) for the ESA, the email boxes of the employees, contractors, or other agent authorized by Company to access or use the email services via the Company Service.

"Ordering Document" means the purchase agreement, evaluation agreement, beta, pre-release agreement or similar agreement between the Company and Cisco or the Company and a Cisco reseller, or the valid terms of any purchase order accepted by Cisco in connection therewith, containing the purchase terms for the Software license granted by this Agreement.

"Personally Identifiable Information" means any information that can be used to identify an individual, including, but not limited to, an individual's name, user name, email address and any other personally identifiable information.

"Server" means a single physical computer or devices on a network that manages or provides network resources for multiple users.

"Services" means Cisco Software Subscription Services.

"Service Description" means the description of the Software Subscription Support Services at http://www.cisco.com/web/about/doing_business/legal/service_descriptions/index.html

"Telemetry Data" means samples of Company's email and web traffic, including data on email message and web request attributes and information on how different types of email messages and web requests were handled by Company's Cisco hardware products. Email message metadata and web requests included in Telemetry Data are anonymized and obfuscated to remove any Personally Identifiable Information.

"Term" means the length of the Software subscription You purchased, as indicated in your Ordering Document.

"Virtual Appliance" means the virtual version of Cisco's email security appliances, web security appliances, and security management appliances.

"Virtual Machine" means a software container that can run its own operating system and execute applications like a Server.

Additional License Terms and Conditions

LICENSE GRANTS AND CONSENT TO TERMS OF DATA COLLECTION

License of Software.

By using the Software and the Documentation, Company agrees to be bound by the terms of this Agreement, and so long as Company is in compliance with this Agreement, Cisco hereby grants to Company a nonexclusive, non-sublicensable, non-transferable, worldwide license during the Term to use the Software only on Cisco's hardware products, or in the case of the Virtual Appliances, on a Virtual Machine, solely in connection with the provision of the Company Service to End Users. The number of End Users licensed for the use of the Software is limited to the number of End Users specified in the Ordering Documents. In the event that the number of End Users in connection with the provision of the Company Service exceeds the number of End Users specified in the Ordering Documents, Company shall contact an Approved Source to purchase additional licenses for the Software. The duration and scope of this license(s) is further defined in the Ordering Document. The Ordering Document supersedes the EULA with respect to the term of the Software license. Except for the license rights granted herein, no right, title or interest in any Software is granted to the Company by Cisco, Cisco's resellers or their respective licensors. Your entitlement to Upgrades to the Software is subject to the Service Description. This Agreement and the Services are co-terminus.

Consent and License to Use Data.

Subject to the Cisco Privacy Statement at <http://www.cisco.com/web/siteassets/legal/privacy.html>, Company hereby consents and grants to Cisco a license to collect and use Telemetry Data from the Company. Cisco does not collect or use Personally Identifiable Information in the Telemetry Data. Cisco may share aggregated and anonymous Telemetry Data with third parties to assist us in improving your user experience and the Software and other Cisco security products and services. Company may terminate Cisco's right to collect Telemetry Data at any time by disabling SenderBase Network Participation in the Software. Instructions to enable or disable SenderBase Network Participation are available in the Software configuration guide.

Description of Other Rights and Obligations

Please refer to the Cisco Systems, Inc. End User License Agreement, Privacy Statement and Service Description of Software Subscription Support Services.



GLOSSARY

C

CIDR 表記 (CIDR Notation)

クラスレス ドメイン間ルーティング (Classless Inter-Domain Routing)。ビットの任意の番号を使用してネットワークのコンテキスト内の IP アドレスの範囲を定義するための簡略形。この表記法を使用して、ネットワーク部分に使用されるビット数が続くスラッシュ (/) を追加することで、アドレスのネットワークプレフィックス部分を書き留めます。そのため、クラス C ネットワークは 192.168.0.1/24 としてプレフィックス表記法で記述されます。CIDR 仕様による 206.13.1.48/25 は、アドレスの先頭 25 ビットが、206.13.1.48 の先頭 25 ビットと一致する任意のアドレスを含みます。

D

DLP

データ消失防止 RSA Security DLP スキャン エンジン は組織の情報と知的財産を保護し、ユーザが過失によって機密データに電子メールを送信することを防ぐことにより、規制や組織のコンプライアンスを確実に適用します。

DLP 違反 (DLP Violation)

一例として、メッセージ内で検出された、組織の DLP ルールに違反するデータ。

DLP インシデント (DLP Incident)

データ消失防止インシデントは、DLP ポリシーにより発信メッセージ内に留意すべき 1 つ以上の DLP 違反を検出すると発生します。

DLP ポリシー (DLP Policy)

データ消失防止ポリシーは、機密データとそのようなデータを含むメッセージに対して AsyncOS が実行するアクションを発信メッセージに含めるかどうかの決定に使用する一連の条件です。

DLP リスク要因 (DLP Risk Factor)

発信メッセージで検出される DLP 違反のセキュリティ リスクを表す 0 ~ 100 のスコア。リスク要因に基づいて、DLP ポリシーによってメッセージに対して実行するアクションが決まります。

DNS

ドメイン ネーム システム。「RFC 1045」および「RFC 1035」を参照してください。ネットワークの DNS サーバは IP アドレスをホスト名に、またはその逆に解決します。

DoS 攻撃 (DoS attack)

DoS 攻撃は、DDos (Distributed Denial of Service 攻撃) の形式にすることもできます。ネットワークまたはコンピュータ上での攻撃。特定のサービスへのアクセスを中断させることを主な目的とします。

DSN

配信ステータス通知 (Delivery Status Notification)、バウンスしたメッセージ。

H

HAT ホスト アクセス テーブル (Host Access Table) HAT は、リモート ホストからの着信接続を制御するリスナー用のルール セットを保持しています。いずれのリスナーにも独自の HAT があります。HAT は、パブリックおよびプライベートのリスナー用に定義され、メール フロー ポリシーおよび送信者グループを含みます。

I

IDE ファイル ウイルス定義ファイル。ウイルスを検出するためにウイルス対策ソフトウェアが使用するシグニチャまたは定義が含まれる IDE ファイル。

L

LDAP Lightweight Directory Access Protocol。プロトコルは、人 (電子メール アドレスを含む)、組織、およびインターネットのディレクトリまたはイントラネット ディレクトリにおける他のリソースに関する情報へのアクセスに使用されません。

M

MTA Mail Transfer Agent または Messaging Transfer Agent。電子メール メッセージの受け入れ、ルーティング、配信を担当するプログラム。Mail User Agent または他の MTA からのメッセージの受信時、MTA はメッセージを一時的にローカルに保存し、受信者を分析し、他の MTA にメッセージをルーティングします。メッセージ ヘッダーを編集したり、追加したりする場合があります。Cisco アプライアンスは、ハードウェア、セキュリティの強化されたオペレーティング システム、アプリケーション、およびサポート サービスを組み合わせ、目的に合わせて構築された、企業のメッセージング専用のラックマウント サーバ アプライアンスを提供する MTA です。

MUA メール ユーザ エージェント (Mail User Agent)。ユーザが電子メール メッセージを作成および読むことができるプログラム。MUA はユーザとメッセージ転送エージェント間のインターフェイスを提供します。送信メールはメール配信の MTA に最終的に渡されます。

MX レコード (MX Record) 特定のドメインのメールの受け入れを担当するインターネット上の MTA を指定します。Mail Exchange レコードは、ドメイン名のメール ルートを作成します。1 つのドメイン名には、複数のメール ルートを作成でき、それぞれにプライオリティ番号が割り当てられます。最も小さい番号のメール ルートは、そのドメインを担当するプライマリ サーバになります。リストされる他のメール サーバは、バックアップとして使用されます。

N

NTP ネットワーク タイム プロトコル (Network Time Protocol)。ntpconfig コマンドでは、ネットワーク タイム プロトコル (NTP) を使用してシステム クロックを他のコンピュータと同期するように、IronPort AsyncOS を設定します。

R

RAT 受信者アクセス テーブル (Recipient Access Table)。受信者アクセス テーブルは、パブリック リスナーが許可する受信者を定義します。テーブルは、アドレス (場合により、部分的なアドレスまたはホスト名) およびそのアドレスを受け入れるか拒否するかを指定します。その受信者に対する RCPT TO コマンドへの SMTP 応答を任意に含めることができます。RAT には通常、ローカル ドメインを含めます。

RCPT TO 「エンベロープ受信者」を参照してください。

S

STARTTLS Transport Layer Security (TLS; トランスポート レイヤ セキュリティ) は Secure Socket Layer (SSL; セキュア ソケット レイヤ) テクノロジーを改良したバージョンです。これは、インターネット上での SMTP カンパセーションの暗号化に広く使用されているメカニズムです。IronPort AsyncOS オペレーティング システムは FC 2487 に記述されている SMTP (セキュアな SMTP over TLS) への STARTTLS 拡張。

T

TOC Threat Operations Center。これは、ウイルス アウトブレイクの検出と応答に関わるすべてのスタッフ、ツール、データとその施設を指します。

あ

アウトブレイク フィルタ (Outbreak Filters) IronPort のアウトブレイク フィルタ機能は、ウイルスから保護するための追加の層を提供します。アウトブレイク フィルタ機能は疑わしい電子メール メッセージを隔離し、更新されたウイルス IDE が有効になるまでメッセージを保留します。あるいは、脅威ではないと判断します。

アンチウイルス (Anti-Virus) Sophos または McAfee のウイルス対策スキャン エンジン、プラットフォーム間のウイルス対策保護、検出、および除去を提供します。ウイルス検出エンジンで、トロイの木馬、ワームのウイルスをスキャンします。これらのプログラムは、「悪意のあるソフトウェア」を意味するマルウェアと総称されます。ウイルス対策スキャナは、すべてのタイプのマルウェアに共通する相似点を利用して、ウイルスだけでなく、すべてのタイプの悪意のあるソフトウェアを検出および削除します。

| | |
|---------------------------------------|---|
| エンベロープ受信者 (Envelope Recipient) | RCPT TO: SMTP コマンドで定義される電子メール メッセージの受信者。また「受信者 (Recipient To)」または「エンベロープ受信者 (Envelope To)」アドレスと呼ばれることがあります。 |
| エンベロープ送信者 (Envelope Sender) | MAIL FROM: SMTP コマンドで定義される電子メール メッセージの送信者。「送信者 (Mail From)」または「エンベロープ送信者 (Envelope From)」アドレスと呼ばれることもあります。 |
| オープン リレー (Open Relay) | オープンリレー（「セキュアでないリレー」または「サードパーティ リレー」とも呼びます）は、未確認のサードパーティ リレーによる電子メール メッセージを許可する SMTP 電子メール サーバです。ローカル ユーザへの送信または受信のいずれでもない電子メールを処理することにより、オープン リレーは、ゲートウェイを通じて不明な送信者を大量の電子メール（一般にスパム）にルーティングすることができます。listenerconfig および systemsetup コマンドは、無意識のうちにシステムをオープン リレーとして設定するのを防ぎます。 |

か

| | |
|--|--|
| 完全修飾ドメイン名 (FQDN) (Fully-Qualified Domain Name (FQDN)) | トップ レベル ドメイン ネームまでのすべての上位レベルのドメイン名を含むドメイン名。例: mail3.example.com は 192.168.42.42 がホストの完全修飾ドメイン名です。example.com は example.com ドメインの完全修飾ドメイン名です。完全修飾ドメイン名は、インターネット内で一意である必要があります。 |
| カンバセーション バウンス (Conversational Bounce) | SMTP カンバセーション内で発生するバウンス。カンバセーション型バウンスには、ハードバウンスとソフト バウンスの 2 種類があります。 |
| キュー (Queue) | アプライアンス Cisco では、電子メール キュー内のメッセージは、削除、バウンス、一時停止、またはリダイレクトすることができます。宛先ドメインへのメッセージのこの電子メール キューは、 <i>配信</i> キューとも呼ばれます。IronPort Anti-Spam またはメッセージフィルタ アクションによる処理を待機しているメッセージのキューは、 <i>ワーク</i> キューとも呼ばれます。status detail コマンドを使用して、両方のキューの状態を表示できます。 |
| キューの最大時間 (Maximum Time in Queue) | ハードバウンスされる前に、 <i>配信</i> 用の電子メール キューにソフトバウンスメッセージがとどまる最大時間。 |
| 許可ホスト (Allowed Hosts) | プライベート リスナー経由で Cisco アプライアンスを使用した電子メールのリレーが許可されたコンピュータ。許可ホストはホスト名または IP アドレスで定義されています。 |
| 検出漏れ (False Negative) | スパム メッセージまたはウイルスや DLP 違反またはウイルスを含むウイルスとしては検出されなかったメッセージ。 |
| 誤検出 (False Positive) | スパムとして、またはウイルスや DLP 違反を含むメッセージとして誤って分類されたメッセージ。 |

| | |
|---|--|
| コンテンツ照合分類子 (Content Matching Classifier) | RSA Data Loss Prevention (DLP) スキャン エンジン 検出 コンポーネント。分類子には、裏付けデータを検索するコンテキスト ルールとともに、機密データを検出するためのいくつかのルールが含まれます。たとえば、クレジットカードの分類子には、メッセージにクレジットカード番号と一致するストリングが含まれているだけでなく、期限データ、クレジットカード会社名、住所などの裏付け情報も含まれる必要があります。 |
| コンテンツ フィルタ (Content Filters) | 電子メール パイプラインのワーク キューの受信者単位のスキャン フェーズ中にメッセージを処理するために使用されるコンテンツ ベースのフィルタ。コンテンツ フィルタはメッセージ フィルタの後に呼び出され、個々の分裂されたメッセージに対して実行されます。 |

さ

| | |
|--|---|
| 最大再試行回数 (Maximum Number of Retries) | ハードバウンスされる前に、ソフト バウンスしたメッセージを配信し直す最大試行回数。 |
| 受信 (Receiving) | IP インターフェイスに設定されている特定のリスナーの電子メール メッセージの受信動作。Cisco アプライアンスは、インターネットからのインバウンドまたはイントラネット システムからのアウトバウンドの電子メール メッセージを受信するようにリスナーを設定します。 |
| スパム (Spam) | 不要な、商用の大量の迷惑電子メール (UCE/UBE)。スパム対策スキャンはフィルタリング ルールに従ってスパムであると思われる電子メール メッセージを特定します。 |
| 送信者 (MAIL FROM) | エンベロープ送信者を参照してください。 |
| 送信者グループ (Sender Group) | 送信者グループは、単に、複数の送信者からの電子メールを同じ方法で扱う (つまり、送信者のグループにメール フロー ポリシーを適用する) ために集められた送信者のリストです。送信者グループは、リスナーのホスト アクセス テーブル (HAT) でカンマ区切りの送信者 (IP アドレス、IP 範囲、ホスト/ドメイン、SenderBase レピュテーション サービスの分類、SenderBase レピュテーション スコア範囲、または DNS リスト クエリー応答により識別) のリストです。メール フロー ポリシーと同様に、送信者グループに名前を割り当てます。 |
| ソフト バウンス メッセージ (Soft Bounced Message) | 設定された最大再試行回数またはキューの最大時間に基づいて、後で配信が再試行されるメッセージ。 |

た

| | |
|--------------------------------|---|
| 遅延バウンス (Delayed Bounce) | SMTP カンパセーション内で発生するバウンス。受信者ホストは配信用にメッセージを許可し、後でのみバウンスします。 |
|--------------------------------|---|

- デバウンス タイムアウト (Debounce Timeout)** システムがユーザに同一のアラートの送信を控える時間 (秒単位)。
- 電子メール セキュリティ マネージャ (Email Security Manager)** IronPort アプライアンス上ですべての電子メール セキュリティ サービスおよびアプリケーションを管理するための、単一で包括的なダッシュボード。電子メール セキュリティ マネージャでは、アウトブレイク フィルタ、スパム対策、ウイルス対策、および電子メール内容のポリシーを、受信者単位または送信者単位で、インバウンドとアウトバウンドの独立したポリシーを使用して管理できます。「コンテンツ フィルタ」も参照してください。
-
- は**
- ハードバウンス メッセージ (Hard Bounced Message)** 永続的に配信できないメッセージ。SMTP カンパセーション中またはその後に生じることがあります。
- 配信 (Delivery)** 特定の IP インターフェイスから、受信者のドメインまたは Cisco アプライアンスの内部メール ホストに電子メール メッセージを配信する動作。Cisco アプライアンスは、Virtual Gateway テクノロジーを使用して、同じ物理マシン内の複数の IP インターフェイスからメッセージを配信できます。各仮想ゲートウェイには、独立した IP アドレス、ホスト名とドメイン、および電子メール キューがあり、それぞれに異なるメール フロー ポリシーおよびスキャンの方法を設定できます。
- リモート ホストへの最大同時接続数、ホストへの最大同時接続数毎の Virtual Gateway の制限、およびリモート ホストへの会話を暗号化するかしないかなどを含む、Cisco プライアンスが実行する配信設定を調整できます。
- 非カンパセーション型バウンス (Non-Conversational Bounce)** 受信者のホストがメッセージを受け入れて配信した後に、そのメッセージが返されたために発生するバウンス。ソフト (4XX) またはハード (5XX) のバウンスがあります。受信者メッセージの処理を決定するためにこれらのバウンス応答を分析できます (ソフト バウンスされた受信者メッセージを再送信して、データベースからハード バウンスされた受信者を削除するなど)。
- ブラックリスト (Blacklist)** 既知の不正な送信者のリストです。デフォルトでは、パブリック リスナーの BLACKLIST 送信者グループの送信者は \$BLOCKED メール フロー ポリシーで設定されたパラメータによって拒否されます。
- ホワイトリスト (Whitelist)** 既知の適切な送信者のリストです。信頼する送信者を WHITELIST の送信者グループに追加します。\$TRUSTED メール フロー ポリシーは、信頼する送信者からの電子メールはレート制限をイネーブルにせず、これらの送信者のコンテンツはスパム対策スキャンの対象にならないように設定されます。

ま

メールフローポリシー (Mail Flow Policies) メールフローポリシーは、リスナーのホストアクセステーブル (HAT) パラメータ (アクセスルールの後に *rate limiting* パラメータ、カスタム SMTP コード、および応答が続く) のグループを表す方法です。送信者グループおよびメールフローポリシーは合わせて、リスナーの HAT で定義されます。ご使用の Cisco アプライアンスは、リスナーの事前定義済みメールフローポリシーおよび送信者グループが設定された状態で出荷されます。

文字セット (2 バイト) (Character Set (Double-byte)) Double Byte Character Sets (DBCS) は各文字を表現するための情報を 1 バイト以上要求する外国語文字セットです。

ら

リスナー (Listener) リスナーは、特定の IP インターフェイスで設定される電子メール処理サービスを記述します。リスナーは、ネットワーク内にある内部システムまたはインターネットから Cisco アプライアンスに入る電子メールだけに適用されます。IronPort AsyncOS は、メッセージを受け入れて受信者のホストにリレーするために、リスナーを使用してメッセージが満たす必要のある基準を指定します。リスナーは、指定した各 IP アドレス上で動作する「電子メールインジェクタ」または「SMTP デーモン」と考えることができます。

IronPort AsyncOS では、デフォルトでインターネット経由の電子メールの受信のためのデフォルトの特性をもつパブリックリスナーと、内部 (グループウェア、POP/IMAP、および他のメッセージ生成) システムからのみ電子メールを受け入れるプライベートリスナーとを区別します。

レート制限 (Rate Limiting) レート制限は 1 セッションあたりの最大メッセージ数、メッセージあたりの最大受信者数、最大メッセージサイズ、1 時間あたりの最大メッセージサイズ、最大受信者、リモート ホストから受信を受け入れる同時接続の最大数を制限します。

レピュテーションフィルタ (Reputation Filter) レピュテーションに基づく疑わしい送信者をフィルタリングする方法。SenderBase レピュテーション サービスを使用すると、ユーザはリモート ホストの接続 IP アドレスに基づいて、正確かつ柔軟に疑わしいスパムを拒否またはスロットリングすることができます。

ログサブスクリプション (Log Subscription) Cisco アプライアンスのパフォーマンスをモニタするログファイルを作成します。ログファイルは、ローカルディスクに格納され、リモートシステムで転送され、保存できます。ログサブスクリプションの一般的な特性は次のとおりです: 監視する名前、コンポーネント (電子メールの処理、サーバ)、スタイル、転送方式。



INDEX

記号

- \$ACCEPTED メールフロー ポリシー [7-12](#)
- \$BLOCKED メールフロー ポリシー [7-11, 7-12](#)
- \$EnvelopeSender 変数 [7-30](#)
- \$RELAYED メールフロー ポリシー [7-12](#)
- \$THROTTLED メールフロー ポリシー [7-11](#)
- \$TRUSTED メールフロー ポリシー [7-11, 12-13](#)
- /dev/null、エイリアス テーブル内 [21-3, 21-8](#)
- /etc/mail/aliases [21-7](#)
- /etc/mail/genericstable [21-16](#)

数字

- 1 時間当たりの最大受信者数 [5-14](#)
- 4XX エラー コード [21-36](#)
- 5XX SMTP 応答 [7-11](#)
- 5XX エラー コード [21-36](#)

A

- Active Directory [22-21](#)
- Active Directory Wizard [3-22](#)
- Adaptive Scanning [14-13](#)
- admin パスワード
 - 変更 [3-15, 3-24](#)
- aliasconfig コマンド [21-8, 21-11](#)
- ALL エントリ
 - HAT 内の ALL エントリ [7-2, 7-4](#)
 - RAT 内の ALL エントリ [8-2](#)
- altsrchost コマンド [21-16, 21-60](#)
- antispam サブコマンド [12-14](#)
- antivirus サブコマンド [12-7](#)

- archivemessage コマンド [30-37](#)
- AsyncOS 更新サーバ [29-23](#)
- AsyncOS のアップグレード [29-15](#)
- AsyncOS 復元 [29-25](#)
- auto-select [21-56](#)
- AutoSupport 機能 [3-16, 3-35, 29-32](#)

B

- Base DN [22-13](#)
- BLACKLIST 送信者グループ [7-11](#)
- bounceconfig コマンド [21-40](#)
- bouncerecipients コマンド [30-26](#)

C

- Call-Ahead SMTP サーバ [19-1](#)
 - ルーティング [19-7](#)
- CIDR アドレス ブロック [7-4](#)
- Cisco Security Intelligence Operations [14-3](#)
- Cisco コンテンツ セキュリティ管理アプライアンス。「セキュリティ管理アプライアンス」を参照
- clear コマンド [2-10](#)
- CLI
 - 言語設定 [29-59](#)
 - コマンドライン インターフェイスを参照
- CLI 監査ログ [34-3](#)
- CLI の履歴 [2-8](#)
- commit コマンド [2-9](#)
- counters [30-2](#)
- CPU 使用率 [30-4](#)
- CRAM-MD5 [22-36](#)
- CSV データ [26-42](#)

D

deleterecipients コマンド [30-24](#)

delivernow コマンド [30-34](#)

deliveryconfig コマンド [21-57](#)

destconfig コマンド [20-12, 21-45](#)

DHAP

メールフローポリシー [7-18](#)

diagnostic -> network -> arpshow コマンド [36-19](#)

diagnostic -> network -> flush コマンド [36-19](#)

diagnostic -> network -> smtping コマンド [36-21](#)

Direct Server Return (DSR) [33-16](#)

DKIM

DNS TXT レコード [17-4](#)

署名 [17-2](#)

ドメインプロファイル [17-2](#)

メールフローポリシーでのイネーブル化 [17-2](#)

DKIM の検証 [17-19](#)

Authentication-Results ヘッダー [17-19](#)

DLP [15-1](#)

Assessment Wizard [15-7](#)

DLP ポリシーのエクスポート [15-31](#)

false positive、最小化 [15-2, 15-10, 15-11, 15-12, 15-14, 15-18](#)

RSA Email DLP [15-4](#)

RSA Enterprise Manager [15-23](#)

エンジンと分類子の更新 [15-39](#)

隔離 [15-42](#)

コンテンツ照合分類子 [15-14](#)

重要度スケール [15-21](#)

スイッチングモード [15-33](#)

正規表現 [15-14](#)

ディクショナリ [15-16](#)

トラブルシューティング [15-43](#)

ポリシーのカスタマイズ [15-33](#)

メッセージアクション [15-33](#)

メッセージトラッキングに重要なコンテンツを含む [15-38](#)

リスク要因スコア [15-18](#)

DLP のメッセージアクション [15-33](#)

DLP フィンガープリント [15-25](#)

DLP ポリシー

RSA Email DLP [15-6](#)

カスタムポリシー [15-9](#)

検出ルール [15-13, 15-14, 15-18](#)

コンテンツ照合分類子 [15-10](#)

重大度スケール [15-20](#)

順序の並べ替え [15-21](#)

正規表現 [15-14](#)

送信者および受信者のフィルタリング [15-20](#)

添付ファイルのフィルタリング [15-20](#)

テンプレート [15-6, 15-8](#)

DLP レポートティング [15-42](#)

D-Mode [15-4, 37-1](#)

DMODE。「D-Mode」を参照。

DNS [D-1](#)

A レコード [36-23](#)

PTR レコード [36-23](#)

逆引き DNS ルックアップのタイムアウト [29-54](#)

逆引き DNS ルックアップのタイムアウトのディセーブル化 [29-54](#)

キャッシュ [36-23](#)

権威サーバ [29-53](#)

サーバ [3-16, 3-26](#)

設定 [3-16, 3-26](#)

タイムアウト [29-53](#)

ダブルルックアップ [7-3, 7-28, 26-12](#)

テスト [36-21](#)

プライオリティ [29-53](#)

分割 [29-53](#)

DNSBL [9-32](#)

dnsconfig コマンド [29-53](#)

dnsflush コマンド [29-55](#)

dnsstatus コマンド [30-22](#)

DNS TXT レコード [17-2](#)

DNS キャッシュ [30-22](#)

DNS キャッシュ、フラッシュ [29-55](#)

DNS サーバ [29-53](#)

DNS 設定 [29-55](#)
 DNS ルックアップ [30-22](#)
 Document Type Definition (DTD) [29-9](#)
 DomainKeys
 メール フロー ポリシーを介して有効化 [7-19](#)
 DomainKey-Signature ヘッダー [17-3](#)
 drop-attachments-where-dictionary-match [9-77](#)
 DSN (遅延通知のメッセージ) [21-40](#)
 DSR [33-16](#)
 仮想 IP (VIP) [33-16](#)
 ループバック インターフェイス [33-16](#)
 ロード バランシング [33-16](#)

E

encryptionconfig CLI コマンド [16-3](#)
 Envelope To [21-7](#)
 Envelope To、エイリアス テーブルでの書き換え [21-7](#)
 exit コマンド [2-11](#)

F

featurekey コマンド [3-36, 12-2, 13-3](#)
 findevent [30-38](#)
 FIPS 管理
 概要 [24-1](#)
 証明書およびキーの管理 [24-2](#)
 説明 [24-1](#)
 FTP [A-1, D-1](#)
 FTP アクセス [A-2](#)
 FTP サーバ ログ [34-3](#)
 FTP プッシュ [34-7](#)

G

genericstable ファイル [21-18](#)
 global unsubscribe
 commenting [21-71](#)

GUI
 アクセス [2-2](#)
 移動 [2-3](#)
 イネーブル化 [32-7](#)
 概要 [32-7](#)
 言語設定 [29-59](#)
 ブラウザ要件 [2-1](#)
 ログイン [2-3](#)
 GUI セッションのタイムアウト [28-26](#)
 GUI による DNS 設定の編集 [29-55](#)
 GUI のメニュー [2-3](#)
 GUI へのログイン [2-3](#)
 GUI
 有効化 [3-26](#)
 GUI ログ。HTTP ログを参照
 GUI を使用したシステム モニタリング [32-7](#)

H

HAT [7-15](#)
 HAT 変数の使用 [7-9](#)
 HAT 変数の使用【ESCAPE_-32442】CLI の例 [7-10](#)
 HAT 変数の使用【ESCAPE_-32442】GUI の例 [7-10](#)
 HAT 変数のテスト [7-10](#)
 Significant Bits [7-17](#)
 インポート [7-21](#)
 エクスポート [7-21](#)
 遅延拒否 [5-7, 7-8](#)
 HAT 順序
 GUI を使用した編集 [7-14](#)
 HAT 遅延拒否 [5-7, 7-8](#)
 HAT 内の最終エントリ [7-2](#)
 HAT 変数の使用 [7-9](#)
 HAT 変数のテスト [7-10](#)
 help コマンド [2-11](#)
 hostrate コマンド [30-19](#)
 hoststatus コマンド [26-20, 30-14](#)

- HTTP
- GUI [32-7](#)
 - イネーブル化 [3-26](#)
- http [A-1, D-1](#)
- HTTPS [A-1](#)
- GUI [32-7](#)
 - イネーブル化 [3-26](#)
 - 証明書 [20-17](#)
- HTTPS プロキシ サーバ [29-24](#)
- HTTPS ログイン [2-3](#)
- HTTP 認証 [26-43](#)
- HTTP プロキシ サーバ [29-24](#)
- HTTP ログ [34-3](#)
- 解放されたメッセージと電子メール パイプライン [4-9](#)
- IronPort スпам隔離。「スパム隔離」を参照
- IronPort スпам対策ルール用プロキシ サーバ [29-22](#)
- IronPort テキスト メール ログ [34-2](#)
- IronPort 電子メール暗号化
- 暗号化プロファイル [16-3](#)
 - エンベロープ設定 [16-4](#)
 - キー サーバ設定 [16-4](#)
 - 設定 [16-1](#)
 - 通知設定 [16-5](#)
 - フィルタ アクションと使用 [16-7](#)
 - メッセージ設定 [16-5](#)
-
- I
- IMAP 認証 [27-25](#)
- implementsv [7-31](#)
- [Incoming Mail Reporting] ページ [26-9](#)
- interface コマンド [21-56](#)
- IPMI [30-40](#)
- IP アドレス [26-15](#)
- IP アドレス プロファイル ページ [26-14](#)
- IP インターフェイス
- リスナーの定義 [3-26](#)
 - 割り当て [3-17, 3-24](#)
- IP ポート
- listenerconfig コマンドでの定義 [5-8](#)
- IronPort Anti-Spam
- archivingY [13-10](#)
 - テスト [13-24](#)
 - 評価キー [3-21, 3-33, 13-3](#)
- IronPort Anti-Spam フィルタ [13-2](#)
- IronPort Anti-Spam 用評価キー [3-33, 13-3](#)
- IronPort Intelligent Multi-Scan
- イネーブル [13-7](#)
- IronPort スпам隔離
- LDAP クエリーの「SMTP:」の削除 [22-43](#)
-
- L
- last コマンド [28-6](#)
- LDAP [D-2](#)
- LDAPS 証明書 [22-14](#)
 - Microsoft Exchange 5.5 サポート [22-9](#)
 - OpenLDAP クエリー [22-19](#)
 - SSL [22-13](#)
 - SunONE クエリー [22-20](#)
 - エイリアス拡張 [22-20](#)
 - エイリアス統合クエリー [22-44](#)
 - エンドユーザ認証のクエリー [22-43](#)
 - および RSA Enterprise Manager [15-29](#)
 - 外部認証 [22-40, 28-21](#)
 - クエリー トークン [22-13](#)
 - クエリーのテスト [22-12, 22-17](#)
 - グループクエリー [9-23, 9-24](#)
 - サーバのテスト [22-7](#)
 - 再帰クエリー [22-14](#)
 - 承認クエリー [5-12](#)
 - 接続 [22-17](#)
 - 接続プール [22-34](#)
 - チェーンクエリー [22-28](#)
 - テスト サーバ [22-7](#)
 - 匿名クエリー [22-14](#)

ドメインベースのクエリー [22-26](#)
 フェールオーバー [22-46](#)
 複数サーバ [22-46](#)
 ベース DN [22-13](#)
 メール ポリシー [C-5](#)
 ユーザ識別名クエリー [22-45](#)
 ロードバランシング [22-46](#)
LDAPS [D-2](#)
 グローバル カタログ サーバ [D-2](#)
LDAPS 証明書 [22-14](#)
LDAP エラー [22-18](#)
LDAP 承認クエリー [5-12](#)
LDAP デバッグ ログ [34-3](#)
LDAP ルーティング クエリー
 SMTP Call-Ahead 受信者検証との使用 [19-6](#)
 listenerconfig コマンド [5-2](#)
 loadconfig コマンド [29-13](#)
 logheaders コマンド [34-43](#)

M

mailconfig コマンド [3-36, 29-12](#)
 mailertable 機能 [21-1](#)
MAIL FROM [9-9, 9-10, 11-8, 11-9, 21-16](#)
 通知用に設定 [29-29](#)
 masquerade サブコマンド [21-18](#)
 mbox 形式 [9-61](#)
 mbox 形式のログ ファイル [12-11, 13-10](#)
McAfee
 更新サーバ [29-23](#)
 評価キー [3-34](#)
McAfee Anti-Virus エンジン [12-5](#)
McAfee の評価キー [12-2](#)
Message ID (MID) [30-3](#)
MIB ファイル [30-40](#)
Microsoft Exchange、LDAP クエリー [22-21](#)
M-Series [38-1](#)
M-Series アプライアンス [38-1](#)
MTA [3-37, 5-1, 5-15, 20-1](#)

MX [3-1](#)
MX レコード [36-23](#)

N

netmask [3-17, 3-25](#)
 netstat コマンド [36-19](#)
NIC チーミング [33-3, 33-4](#)
NIC ペアリング [33-3, 33-4](#)
 アップグレード時の命名 [33-4](#)
 アラート [33-4](#)
No Subject [25-5](#)
 not.double.verified [7-29, 7-38](#)
 nslookup コマンド [36-21](#)
NTP [D-2](#)
NTP サーバ [29-57](#)
 削除 [29-58](#)
NTP ログ [34-3](#)
 nx.domain [7-38](#)
NXDOMAIN [7-29, 7-38](#)

O

offline コマンド [29-3](#)
 oldmessage コマンド [30-37](#)

P

PEM 形式、証明書用 [20-5](#)
pii [15-8](#)
 ping コマンド [36-19](#)
POP/IMAP サーバ [5-15](#)
POP 認証 [27-25](#)
Possible Delivery [21-56, 21-57](#)
PVO。「隔離、ポリシー、ウイルス、およびアウトブレイク」を参照

Q

qmail 形式配信ログ [34-2](#)QMQP [D-2](#)quit コマンド [2-11](#)

R

RADIUS 外部認証 [28-22](#)RAM [36-27](#)RAM 使用率 [30-4](#)

RAT

受信者のバイパス [8-5](#)受信者のバイパス (CLI) [8-5](#)受信者のバイパス (GUI) [8-5](#)rate コマンド [30-19](#)RBL [9-14](#)RCPT TO [9-10, 11-9](#)RCPT TO コマンド [8-3, 21-7](#)reboot コマンド [29-2](#)Received ヘッダー [5-11, 13-19](#)Received: ヘッダー、ディセーブル化 [5-11](#)

Recipient Access Table (RAT)

デフォルト エントリ [8-2](#)

Recipient Access Table (RAT)

CLI を使用した編集 [8-2](#)定義 [8-1](#)redirectrecipients [30-28](#)removemessage コマンド [30-37](#)resetconfig コマンド [29-3](#)resetcounters コマンド [26-42, 30-23](#)resumedel コマンド [30-32](#)resumelister コマンド [30-33](#)resume コマンド [29-3, 30-34](#)

RFC

1035 [21-7](#)1065 [30-39](#)1066 [30-39](#)1067 [30-39](#)1213 [30-39](#)1907 [30-39](#)2047 [27-6](#)2487 [20-1](#)2571 ~ 2575 [30-39](#)2821 [1-9, 5-9](#)821 [10-3](#)822 [10-3](#)rollovernow コマンド [34-8](#)RSA DLP Datacenter [15-25, 15-29](#)RSA Email DLP [15-4](#)RSA Enterprise Manager [15-23, 27-13](#)イネーブル [15-28](#)クラスタ化されたアプライアンス [15-32](#)証明書 [15-26](#)スイッチング モード [15-33](#)発信メール ポリシー [15-30](#)

S

saveconfig コマンド [29-12](#)

SBRs

none [7-7, 9-33](#)テスト [6-6](#)

SBRs。Senderbase レピュテーション サービス スコアを参照

SBRs スコア [25-6](#)SBRs のメッセージフィルタ [6-7](#)

scanconfig

添付ファイルの再帰レベルのスキャン [9-88](#)

scanconfig

スキャンされるファイルの最大サイズの設定 [9-88](#)添付ファイル タイプのスキップ [9-88](#)scp コマンド [A-4](#)SCP プッシュ [34-7](#)Secure LDAP [22-13](#)SenderBase [5-14, 7-11, 7-17, D-1](#)IP プロファイリングの使用 [5-11](#)接続ごとのタイムアウト [5-11](#)

- 送信者グループの SBO 7-7
- SenderBase Affiliate ネットワーク 6-1
- SenderBase、クエリー 7-7
- SenderBase ネットワーク オーナー識別番号 7-4
- SenderBase レピュテーション サービス 6-1, 26-1, 26-14
- SenderBase レピュテーション サービス スコア 7-6
- SenderBase レピュテーション スコア 6-2, 7-7, 7-13, 13-21, 25-6, 36-2
- SenderBase レピュテーション スコア、CLI の構文 7-7
- [Separate Window] アイコン 26-7
- serv.fail 7-38
- SERVFAIL 7-29, 7-38
- sethostname コマンド 29-52
- setup 3-1
- SGACL リスト (DNS list) 9-32
- showconfig コマンド 29-11
- showmessage コマンド 30-37
- showrecipients 30-29
- shutdown コマンド 29-2
- SIDF 検証
 - 準拠レベル 17-23
- SIDF の検証 9-11
 - イネーブル化 17-22
 - 結果 17-29
 - 設定 17-20
 - テスト 17-32
- SIDF レコード
 - テスト 17-21
 - 有効 17-21
- Significant Bits
 - メール フロー ポリシーを参照 7-17
- SMI ファイル 30-40
- SMTP D-1
 - HELO コマンド 7-11
 - IronPort Anti-Spam テスト 13-24
 - 応答 8-3
 - コード 7-8
 - バナー テキスト 7-8
 - バナー ホスト名 7-16
 - メッセージ 5-15
- SMTP Auth 22-2, 22-32
- SMTP Call-Ahead サーバ プロファイル
 - リスナーでのイネーブル化 19-6
- SMTP Call-Ahead サーバ プロファイル
 - 作成 19-3
- SMTP Call-Ahead 受信者検証 19-1
 - LDAP ルーティング クエリーとの使用 19-6
 - SMTP サーバ応答 19-5
 - 通信フロー 19-2
 - バイパス 19-8
- SMTP HELO コマンド 36-23
- SMTP アドレス解析
 - Loose モード 5-9
 - Strict モード 5-9
- SMTP クエリーのワークフロー 19-7
- SMTP 通信
 - SMTP Call-Ahead サーバ 19-2
- SMTP 通信中の LDAP 承認 5-12
- SMTP デーモン
 - インジェクタを参照
 - リスナーを参照
- SMTP 認証 25-5
 - DIGEST-MD5 22-36
 - HAT エントリ 7-19
 - MD5 22-33
 - SHA 22-33
 - TLS 22-37
 - サポートされる認証メカニズム 22-33
- SMTP 認証済みユーザの一致するフィルタ ルール 9-38
- SMTP 認証プロファイル 22-36
- SMTP ルート 21-1
 - USEDNS 21-3
 - 再帰的なエントリ 21-2
 - 制限 21-3
 - 複数ホストのエントリ 21-3
 - メール配信および分裂 21-4
- SMTP ルート、最大 21-2

SMTP ルートと DNS 21-3

SNMP

IPMI 30-40

MIB ファイル 30-40

SMI ファイル 30-40

概要 30-39

コミュニティ スtring 30-40

トラップ 30-42

ハードウェア障害トラップの条件 30-41

複数のトラップ ターゲットの指定 30-42

SNMPv1 30-40

SNMPv2 30-40

SNMPv3 パスフレーズ 30-40

SNMP (簡易ネットワーク管理プロトコル) 30-39

Sophos

アップデート 12-20

評価キー 3-21, 3-34, 12-2

Sophos ウィルス スキャン

フィルタ 12-11

spf-passed フィルタ ルール 9-11, 17-31

spf-status フィルタ ルール 9-11, 17-30

SPF 検証 9-11

準拠レベル 17-23

SPF の検証

Received-SPF ヘッダー 17-28

イネーブル化 17-22

結果 17-29

設定 17-20

テスト 17-32

SPF レコード

テスト 17-21

有効 17-21

SSH 2-5, D-1

SSH1

ディセーブル化 28-28

sshconfig コマンド 28-27

SSH プロトコル 28-27

SSH1 のディセーブル化 28-28

SSL 22-13

STARTTLS

定義 20-1

status detail コマンド 30-9

status コマンド 30-8

strip-header フィルタ アクション 9-62

SUSPECTLIST 送信者グループ 7-11

suspenddel コマンド 30-31

suspendlistener コマンド 30-33

suspend コマンド 29-2

Syslog 34-7

systemsetup コマンド 3-24

T

tail コマンド 34-48

パラメータ 34-48

TCPREFUSE 7-8

TCP リッスン キュー 5-11

Telnet 2-5, A-1, D-1

Threat Operations Center (TOC) 14-6, 26-6

TLS

証明書 20-1

デフォルト 20-10

必須 20-10

優先 20-10

tlsverify コマンド 36-26

TLS (必須) 20-7

tophosts コマンド 30-17, 36-22

topin コマンド 30-21

trace 13-22

trace コマンド 6-6, 36-1

TTL 30-13

tzupdate

CLI コマンド 29-57

U

UNKNOWNLIST 送信者グループ 7-12

Unsolicited Commercial Email 6-1

uuencoded 添付ファイル 9-6

V

version 26-41

Virtual Gateway アドレス 9-60, 21-62

Virtual Gateway アドレスのモニタリング 21-67

Virtual Gateway キュー 21-59

Virtual Gateway™ テクノロジー 21-59

virususerstable。エイリアス テーブルを参照

VLAN

定義済み 33-9

ラベル 33-10

W

Web UI セッションのタイムアウト 28-26

Web インターフェイス

イネーブル化 3-26

WHITELIST 送信者グループ 7-11, 12-13

whoami コマンド 28-6

who コマンド 28-6

X

X.509 証明書 20-2

X-advertisement ヘッダー 13-24

X-Header、追加 27-6

X-IronPort-Anti-Spam ヘッダー 13-14

X-IronPort-AV ヘッダー 12-8

XML 29-7, 29-9, 29-12, 32-12, 34-2

XML ステータス機能 32-12

あ

アウトブレイク フィルタ

Adaptive Scanning 14-13

CASE 14-4

Context Adaptive Scanning Engine 14-4

SNMP トラップ 14-22

アラート 14-22

アラートのイネーブル化 14-14

アンチウイルス アップデート 14-10

アンチウイルス スキャンとの非併用 14-9

ウイルス感染 14-2

概要 14-1

隔離レベルのしきい値の設定 14-16

脅威カテゴリ 14-2

常時ルール 14-8

定義済みアウトブレイク ルール 14-6

定義済みアダプティブ ルール 14-6

非ウイルス性の脅威 14-3

評価キー 3-21, 3-34

ファイル拡張子のバイパス 14-16

複数のスコア 14-9

メッセージの再評価 14-9, 14-10

メッセージの遅延 14-4

メッセージの変更 14-5

メッセージ変更レベルのしきい値の設定 14-17

リンクのリダイレクト 14-4

ルール 14-7

ルールのアップデート 14-14

アウトブレイク フィルタの評価キー 3-21, 3-34

[アカウント権限 (Account Privileges)] ページ 28-8

アクセス ルール

HAT 内のアクセス ルール 7-8

アクティブなセッション 2-5

アップグレード

GUI を使用した取得 29-19

使用可能 29-16, 29-17

ストリーミング 29-19

リモート 29-20

アップグレード サーバ 29-20

アップデートの強制 12-20

宛先制御 21-45

および中央集中型管理 35-29

- コンフィギュレーションのインポートおよびエクスポート [21-47](#)
 - アドレス タギング キー
 - 削除 [21-55](#)
 - アドレス タギング キーの削除 [21-55](#)
 - アドレスの書き換え [21-7](#)
 - アドレス リスト [7-22](#)
 - 作成 [7-22](#)
 - 送信者のレート制限の例外 [7-17](#)
 - アドレス リテラル [5-10](#)
 - アラート
 - アウトブレイク フィルタでのイネーブル化 [14-14](#)
 - アラート分類 [29-31](#)
 - 重大度 [29-31](#)
 - 受信者 [29-30](#)
 - 設定 [29-30](#)
 - アラート設定 [3-15, 3-35, 29-30](#)
 - アラート メッセージ [3-15, 3-35](#)
 - アラートリスト [29-35](#)
 - 暗号化 [5-13, 20-1](#)
 - フィルタ アクションと使用 [16-7](#)
 - 暗号化プロファイル
 - 設定 [16-3](#)
 - 暗号化ヘッダー [16-11](#)
 - アンチウイルス [18-20](#)
 - Dropping Attachments [12-8](#)
 - Scan and Repair [12-8](#)
 - Scan Only [12-7](#)
 - アクション [12-9](#)
 - 暗号化 [12-8, 12-9](#)
 - ウイルスに感染 [12-9](#)
 - オリジナル メッセージのアーカイブ [12-11](#)
 - 拡張オプション [12-10](#)
 - カスタム ヘッダーの追加 [12-11](#)
 - グローバル オプション [12-7](#)
 - スキャン不可 [12-9](#)
 - 送信のカスタム アラート通知 [12-12](#)
 - 代替宛先ホストへの送信 [12-12](#)
 - デフォルト通知の送信 [12-11](#)
 - メール フロー ポリシー [7-18](#)
 - メッセージ件名の変更 [12-10](#)
 - メッセージ受信者の変更 [12-12](#)
 - アンチウイルス アーカイブ ログ [34-3](#)
 - アンチウイルス
 - 各リスナーのアクション [12-7](#)
 - アンチウイルス ログ [34-3](#)
 - アンチスパム
 - false positive および陰性のレポート [13-14](#)
 - HAT エントリ [7-18](#)
 - HAT パラメータ [5-14](#)
 - IronPort Anti-Spam [13-3](#)
 - X-IPASFiltered ヘッダー [13-6](#)
 - アプライアンス生成メッセージのスキャン [13-13](#)
 - 大きいメッセージのスキャン [13-5, 13-6](#)
 - テスト [13-24](#)
 - デフォルト スキャン エンジンの選択 [13-12](#)
 - 複数のスキャン エンジンの使用 [12-2](#)
 - 陽性スパムのしきい値 [13-9](#)
 - 陽性と疑わしいスパムのしきい値 [13-9](#)
 - アンチスパム アーカイブ ログ [34-3](#)
 - アンチスパム ログ [34-3](#)
-
- ## い
- イーサネット インターフェイス [B-1](#)
 - 一部のドメイン
 - マスカレード内 [21-17](#)
 - 一致した内容
 - 確認 [27-15](#)
 - 委任管理 [28-7](#)
 - イメージ スキャン [9-69](#)
 - イメージのスキャン [9-69](#)
 - イメージの判定 [9-69](#)
 - インジェクション カウンタのリセット期間 [5-6](#)
 - インジェクション制御期間 [7-25](#)
 - インジェクション制御のカウンタ リセット [7-25](#)
 - インジェクション接続 ID (ICID) [30-4](#)
 - インジェクション デバッグ ログ [34-2](#)

インジェクタ

リスナーを参照

インストール **3-1**復元 **29-25**陰性スコア **7-6**インターフェイスのサービス **A-1**

インポート

HTML テキスト リソース **18-11**テキスト リソース **18-10**

う

ウィザード

Active Directory **3-22**システム セットアップ **3-1, 3-12**

ウイルスアウトブレイク フィルタ

省略 **11-13**

ウイルス隔離。「隔離

ウイルス」を参照。

ウイルス対策隔離。「隔離、ウイルス」を参照。

[ウイルスタイプ (Virus Types)] ページ **26-28**

ウイルス定義

自動アップデート間隔 **29-24**ウイルス メッセージ **26-8**疑わしい送信者、スロットリング **7-11**

え

エイリアス テーブル

aliasconfig コマンド **21-8**CLI を使用した設定 **21-7**virtusertable **21-7**コメント **21-8**定義 **21-7**複数のエントリ **21-8**

エクスポート

HTML テキスト リソース **18-11**テキスト リソース **18-10**

エンコード

免責事項 **18-16**エンタープライズ ゲートウェイ **3-37**エンタープライズ ゲートウェイ構成 **5-15**エンベロープ受信者 **9-23, 21-7, 25-3**エンベロープ受信者、書き換え **21-7**エンベロープ送信者 **9-23, 25-3**エンベロープ送信者、書き換え **21-16**エンベロープ送信者の DNS 検証 **7-29**

お

大きいメッセージのスキャン **13-5, 13-6**オーバーフロー **14-10**オープン リレー、定義 **8-2**

大文字と小文字の区別

CLI **2-7**LDAP クエリー **22-13, 22-18**systemsetup コマンド **3-25**メッセージフィルタ内 **9-18**オフセットの指定 **29-58**オフライン状態 **29-3**オンライン ヘルプ **2-3, 2-11**

か

解析不可能なメッセージ **9-21**解析不可能なメッセージのフィルタリング **9-21**外部認証 **22-40**LDAP のイネーブル化 **28-21**RADIUS のイネーブル化 **28-22**[概要 (Overview)] ページ (セキュリティ モニタ) **26-5**隔離 **27-2**DLP **15-42**アウトブレイク **27-2**アウトブレイク、シスコへのメッセージの報告 **27-19**アウトブレイク専用フィルタ **27-18**ウイルス **27-2**

件名のタギング [27-6](#)
 件名の非 ASCII 文字の表示 [27-6](#)
 国際文字セット [27-12](#)
 スпам。「スパム隔離」を参照
 早期の期限切れ [27-4](#)
 タイプ [27-2](#)
 他の隔離 [27-14](#)
 中央集中型ポリシー、ウイルス、アウトブレイク隔離 [27-11](#)
 通常の期限切れ [27-4](#)
 デフォルト アクション [27-5, 27-8](#)
 添付の削除 [27-6](#)
 保持期間 [27-4](#)
 ポリシー [27-2](#)
 ポリシー、ウイルス、およびアウトブレイク管理 [27-3](#)
 中央集中型 [27-11, 38-4](#)
 未分類 [27-8](#)
 メッセージのウイルス テスト [27-17](#)
 メッセージへのアクションの適用 [27-13](#)
 隔離脅威レベルのしきい値
 推奨デフォルト [14-7](#)
 設定 [14-7](#)
 隔離されたメッセージ
 確認 [27-15](#)
 隔離のオーバーフロー [14-10](#)
 隔離レベルのしきい値 [14-16](#)
 カスタム DLP ディクショナリ [15-16](#)
 カスタム SMTP 応答
 変数 [7-30](#)
 カスタム ヘッダー [13-18](#)
 カスタム ユーザ ロール [28-7](#)
 カスタム ユーザ ロールのアクセス権限 [28-9](#)
 仮想 IP (VIP) [33-16](#)
 仮想テーブル [21-28](#)
 仮想電子メール セキュリティ アプライアンス
 ライセンスのロード [3-8](#)
 仮想ドメイン [21-16](#)
 画像分析 [9-69, 11-6, 11-13](#)

角カッコ [2-6](#)
 環境設定
 ユーザに対して定義 [29-59](#)
 完全修飾ドメイン名 [7-4](#)
 カンバセーションでないバウンス [21-36](#)
 カンバセーション バウンス [21-36](#)

き

キー
 FIPS 管理 [24-1, 24-2](#)
 キー サイズ [17-3](#)
 逆引き DNS ルックアップ
 タイムアウト [29-53](#)
 ディセーブル化 [29-54](#)
 キュー [5-3](#)
 脅威レベル
 定義 [14-6](#)
 拒否された接続 [25-3](#)

く

空白 [12-10, 13-9](#)
 空白ヘッダーの一致 [9-22](#)
 空白文字 [9-16](#)
 クエリー
 SMTP 認証 [22-33](#)
 受け入れ [22-19](#)
 外部認証 [22-40](#)
 グループ [22-23](#)
 スパム隔離のエイリアス統合 [22-44](#)
 スパム隔離へのエンドユーザ認証 [22-43](#)
 チェーン クエリー [22-28](#)
 ドメイン ベース [22-26](#)
 マスカレード [22-21](#)
 ルーティング [22-20](#)
 クエリー インターフェイス [29-57](#)
 グッド ネイバー テーブル [20-11](#)
 グラフ [26-6, 32-11](#)

グラフィカル ユーザ インターフェイス

GUI を参照

クリーン メッセージ [26-8](#)グローバル エイリアス [21-8](#)グローバル カウンタ [30-23](#)

グローバル配信停止

インポートおよびエクスポート [21-71](#)概要 [21-68](#)構文 [21-68](#)最大エントリ [21-68](#)追加 [21-69](#)

け

形式が不正なエントリ、エイリアス テーブル内 [21-8](#)ゲージ [30-4](#)ケース (コンテキスト Adaptive Scanning Engine [TM]) [13-23](#)ゲートウェイ設定 [5-1](#)

言語

スパム隔離のデフォルト言語の指定 [27-23](#)ユーザあたりのデフォルトの定義 [29-59](#)ユーザの環境設定 [29-59](#)検出ルール [15-13, 15-14, 15-18](#)

検証

SIDF [17-20](#)SPF [17-20](#)

件名

No Subject [25-5](#)

こ

工場出荷時の設定 [3-13](#)

更新

DLP エンジンと分類子 [15-39](#)更新サーバ [29-23](#)コマンドの補完 [2-8](#)コマンドライン インターフェイス (CLI) [2-5](#)大文字と小文字の区別 [2-7](#)空白文字 [2-7](#)コマンドの補完 [2-8](#)サブコマンド [2-7](#)終了 [2-8](#)デフォルト設定 [2-6](#)表記法 [2-6](#)履歴 [2-8](#)コミュニティ ストリング [30-40](#)コメント [7-22, 21-5](#)インポートしたファイル内のコメント [7-22, 21-5](#)コンテンツ照合分類子 [15-10, 15-14](#)コンテンツ ディクショナリ [18-1](#)コンテンツ フィルタ [27-2](#)アクション [11-10](#)条件 [11-2](#)電子メール パイプライン中に適用 [11-1](#)非 ASCII 文字セット [11-21, C-19](#)変数 [11-16](#)例 [C-13, C-14](#)コンテンツ フィルタによる阻止 [26-8](#)

さ

サードパーティ リレー [8-2](#)再帰クエリー、LDAP [22-14](#)再帰的 DNS クエリー [29-54](#)

再帰的なエントリ

SMTP ルート内 [21-2](#)エイリアス テーブル内 [21-8](#)再設定 [3-13](#)

最大値

1 時間あたりの受信者数、systemsetup [3-27, 3-31](#)HAT 内での 1 時間あたりの受信者数 [6-7, 7-16](#)HAT 内での 1 接続あたりのメッセージ数 [5-14, 7-16](#)HAT 内での 1 メッセージあたりの受信者数 [5-14, 7-16](#)HAT 内での時間間隔あたりの受信者数 [7-17](#)HAT 内での時間コードあたりの受信者数 [7-16](#)

- HAT 内での時間超過テキストあたりの受信者数 [7-16](#)
 - HAT 内でのメッセージ サイズ [5-14, 7-15](#)
 - HAT 内の同時接続 [7-15](#)
 - 最大同時接続数 [5-6](#)
 - サブドメインの削除 [21-16](#)
 - サブネット [3-17, 3-25](#)
 - サポート言語
 - デフォルト設定 [29-59](#)
-
- し**
- 時間帯、設定 [3-15, 3-35](#)
 - 時間帯ファイル
 - 更新 [29-57](#)
 - 時間の同期 [3-15, 3-35](#)
 - しきい値、SenderBase レピュテーション スコアの [7-7](#)
 - 時刻、システム [3-15, 3-35](#)
 - システム隔離。「隔離、ポリシー、ウイルス、およびアウトブレイク」を参照
 - システム クロック [3-15, 3-35](#)
 - システム時刻
 - 設定 [3-15, 3-35](#)
 - [システム ステータス (System Status)] ページ [26-40](#)
 - システム セットアップ [3-1](#)
 - システム セットアップ ウィザード [3-12](#)
 - システム セットアップの次の手順 [3-23](#)
 - [システム容量 (System Capacity)]
 - [システムの負荷 (System Load)] ページ [26-38](#)
 - [受信メール (Incoming Mail)] ページ [26-36](#)
 - [すべて (All)] ページ [26-40](#)
 - [送信メール (Incoming Mail)] ページ [26-37](#)
 - メモリ ページ スワッピング [26-39](#)
 - [ワーク キュー (WorkQueue)] ページ [26-35](#)
 - [システム容量 (System Capacity)] ページ [26-34](#)
 - システム ログ [34-3](#)
 - 失敗した着信接続または効果のない着信接続のクローズ [5-6](#)
 - 自動アップデート [29-24](#)
 - 間隔 [29-24](#)
 - 自動配信機能 [21-56](#)
 - 週ごとのステータス アップデート [3-35](#)
 - 重大度の設定 [15-20](#)
 - 重大度レベル [15-20](#)
 - 重要度スケール [15-20](#)
 - DLP [15-21](#)
 - 受信エラー [36-25](#)
 - 受信者検証 [19-1](#)
 - 受信者のバウンス
 - Envelope From [30-28](#)
 - すべて [30-28](#)
 - ホスト名 [30-28](#)
 - 受信者へのアラート [29-30](#)
 - 受信者、メッセージフィルタ内の数 [9-28](#)
 - 受信制御、バイパス [8-5](#)
 - 受信の一時停止 [30-32](#)
 - 受信の再開 [30-33](#)
 - 準拠レベル
 - SPF/SIDF 検証 [17-23](#)
 - 使用可能なアップグレード [29-15](#)
 - 常時ルール [14-8](#)
 - 使用する前に [3-1](#)
 - 証明書
 - FIPS 管理 [24-1, 24-2](#)
 - RSA Enterprise Manager を使用した DLP [15-26](#)
 - インポート [20-1](#)
 - エクスポート [20-5](#)
 - 中間証明書 [20-3](#)
 - 追加 [20-3](#)
 - デモ [3-26](#)
 - 独自の生成および署名 [20-2](#)
 - 認証局 [20-2](#)
 - 認証局リスト [20-15](#)
 - 要求の生成 [20-5](#)
 - 証明書署名要求 [20-2](#)
 - 署名
 - DKIM [17-2](#)
 - デュアル ドメイン キーおよび DKIM [17-2](#)
 - ドメイン キー [17-2](#)

署名キー

サイズ [17-3](#)指定キーの削除 [17-11](#)すべての既存のキーの削除 [17-11](#)署名キーのインポート [17-11](#)シリアル接続のピン割り当て [3-8, A-5](#)信頼性 [7-7](#)

すスキャン可能なアーカイブ ファイルのタイプ [9-29](#)スキャン ログ [34-4](#)スケジュール設定されたログ ロールオーバー [34-45](#)スタティック ルート [21-56](#)ステータス ログ [34-2](#)ステートレス ログ [34-16](#)ストリーミング アップグレード [29-19](#)

スパム

アーカイブ [13-10](#)カスタム ヘッダーを含む [13-10](#)スパムの件名行の変更 [13-9](#)代替アドレスへの送信 [13-10](#)代替メールホストへの送信 [13-9](#)テスト [13-24](#)

スパム隔離

IMAP/POP 認証 [27-30](#)LDAP 認証 [27-30](#)エンドユーザ認証 [27-25](#)外部 [38-3](#)解放されたメッセージと電子メール パイプライン [27-35](#)全メッセージの削除 [27-21, 27-35](#)通知 [27-19](#)通知のテスト [27-31](#)ディセーブル化 [27-21](#)デフォルト言語 [27-23](#)認証を受けないエンド ユーザ アクセス [27-25](#)複数 [27-20](#)複数通知の受信 [27-31](#)プライオリティ [27-20](#)満杯時の動作 [27-23](#)メッセージの詳細 [27-34](#)メッセージ変数 [27-26](#)スパム隔離内の全メッセージの削除 [27-35](#)スパム メッセージ [26-8](#)

すべてのエントリ

マスカレード内 [21-17](#)スロットリング [6-1, 7-11](#)

せ

正規表現

DLP [15-14](#)

制限

altsrchoost [21-63](#)SMTP ルート [21-3](#)セキュア HTTP (https) [20-1](#)セキュア コピー [A-4](#)セキュア ソケット レイヤ (SSL) [20-1](#)セキュアでないリレー [8-2](#)セキュリティ管理アプライアンス [38-1](#)接続の問題、トラブルシューティング [36-17](#)設定、テスト [3-36](#)設定ファイル [29-7](#)CLI [29-11](#)GUI [29-8](#)XML [29-7](#)説明済み [7-29](#)選択したインターフェイスよりも優先されるルーティン
グ [B-3](#)

そ

早期の期限切れ

隔離 [27-4](#)[送信先 (Outgoing Destinations)] ページ [26-17](#)

送信者

GUI を使用して送信者グループに送信者を追加 [7-14](#)

送信者グループ

BLACKLIST [7-11](#)

GUI を使用した追加 [7-13](#)

SUSPECTLIST [7-11](#)

UNKNOWNLIST [7-12](#)

WHITELIST [7-11](#)

概要 [7-3](#)

送信者検証

不正な形式の MAIL FROM およびデフォルト ドメイン [7-30](#)

例外テーブル [7-35](#)

送信者検証例外テーブル [7-30](#)

送信者の検索 [7-15](#)

送信者のレート制限

時間間隔あたりの最大受信者数 [7-17](#)

超過エラー コード [7-17](#)

超過エラー テキスト [7-17](#)

例外 [7-17](#)

[送信処理ステータス (Delivery Status)] ページ [26-19](#)

[送信処理ステータス詳細 (Delivery Status Details)] ページ [26-20](#)

[送信メッセージ送信者 (Outgoing Senders)] ページ [26-18](#)

送信元ルーティング [5-10](#)

そのままのアドレス [5-10](#)

た

代替 MX ホスト [21-2](#)

代替アドレス [12-1](#)

タイム サーバ [3-15, 3-35](#)

タイムゾーン [29-57, 29-58](#)

[(タイム ゾーン (Time Zone))] ページ [29-57](#)

ダブル DNS で検証済み [26-13](#)

ダミー アカウント [6-6](#)

単項形式、メッセージ フィルタ内 [9-28](#)

ち

チェーン、エイリアスの [21-8](#)

チェーン クエリー

LDAP [22-28](#)

作成 [22-29](#)

遅延バウンス [21-36](#)

着信接続

失敗した接続または効果のない接続のクローズ [5-6](#)

着信接続のタイムアウト [5-6](#)

着信メッセージ、定義済み [10-3](#)

着信リレー [13-14, 17-20](#)

Received ヘッダー [13-19](#)

カスタム ヘッダー [13-18](#)

ログ エントリの例 [13-23](#)

中央集中型管理

および宛先制御 [35-29](#)

および隔離 [27-11](#)

および中央集中型隔離 [38-4, 38-6](#)

つ

通常の期限切れ

隔離 [27-4](#)

通知の選択 [18-20](#)

て

定義

ユーザの環境設定 [29-59](#)

ディレクトリ ハーベスト攻撃 (DHA) [22-29](#)

データ消失防止 [27-2](#)

DLP を参照

テキスト リソース

HTML リソースのエクスポートおよび HTML リソースへのインポート [18-11](#)

インポート [18-10](#)

エクスポート [18-10](#)

概要 [18-8](#)

管理 **18-9**
 コード ビュー **18-11**
 コンテンツ ディクショナリ **18-1**
 非 ASCII 文字 **18-8**
 ポリシーおよび設定での使用 **18-12**
 免責条項 **18-12**
 テキスト リソースの
 HTML ベース **18-11**
 テスト
 IronPort Anti-Spam **13-24**
 Sophos ウイルス エンジン **12-17**
 システム セットアップ **3-36**
 デフォルト
 IP アドレス **3-13**
 送信者のドメイン **5-10**
 ホスト名 **3-15, 3-24**
 デフォルト DNS サーバ **29-54**
 デフォルト ゲートウェイ **3-16, 3-25**
 デフォルト ドメイン **8-1**
 デフォルト ルータ **3-16, 3-25**
 デモ証明書 **3-26, 20-3, 20-8**
 デュアル DKIM および DomainKey 署名 **17-7**
 電子メール
 アドレスの書き換え **21-7**
 クリーン メッセージ **26-8**
 電子メール アドレス
 送信元ルーティング **5-10**
 電子メール アドレスの書き換え **21-7**
 電子メール インジェクタ
 リスナーを参照
 電子メール ゲートウェイ **5-1**
 電子メール セキュリティ モニタ **26-1**
 サマリー テーブル **26-7**
 [時間範囲 (Time Range)] メニュー **26-7**
 自動レポート **26-42**
 受信された外部ドメイン リスト **26-12**
 [表示された項目 (Items Displayed)] メニュー **26-13**
 メール トレンド グラフ **26-7**

電子メールの受け付け **7-2**
 電子メールの受信、設定 **5-1**
 電子メールのリダイレクト **3-18, 21-2**
 電子メールのリレー **7-2**
 電子メール配信の一時停止 **30-31**
 電子メール配信の再開 **30-32**
 転送で使用する SMTP 認証
 定義 **22-35**

と

ドメイン **26-15**
 デフォルトのドメインの追加 **5-10**
 ドメイン キー **17-1**
 DNS TXT レコード **17-4**
 DNS テキスト レコード **17-12**
 検証 **17-1**
 署名 **17-2**
 署名キーのインポート **17-11**
 署名キーのサイズ **17-3**
 署名の検証 **17-2**
 セレクタ **17-4**
 ドメイン プロファイル **17-2**
 ドメイン プロファイルのインポート **17-13**
 ドメイン プロファイルのエクスポート **17-13**
 ドメイン プロファイルのテスト **17-12**
 標準化 **17-5**
 メール フロー ポリシーでのイネーブル化 **17-2**
 ドメイン コンテキスト
 エイリアス テーブル内 **21-7, 21-11**
 ドメイン テーブル **21-28**
 ドメイン デバッグ ログ **34-2**
 ドメイン ネーム サーバ (DNS)
 設定 **3-16, 3-26**
 ドメインの付加 **5-10**
 ドメインのマッピング **21-2**
 ドメイン プロファイル
 インポート **17-13**
 エクスポート **17-13**

すべての既存のプロファイルの削除 [17-14](#)
 テスト [17-12](#)
 ドメイン プロファイルの削除 [17-13](#)
 ドメイン プロファイルのインポート [17-13](#)
 ドメイン ページのプロファイル [26-14](#)
 ドメイン マップ
 インポートおよびエクスポート [21-34](#)
 概要 [21-28](#)
 コメント [21-34](#)
 制限 [21-28](#)
 不正なエントリのインポート [21-34](#)
 トラッキング
 「AND」検索 [25-2](#)
 トラブルシューティング
 DLP [15-43](#)
 トランスポート レイヤ セキュリティ (TLS) [7-19](#)
 [トレース] ページ [36-1](#)

に

二重設定、編集 [33-1](#)

ね

ネットマスク、選択 [B-1](#)
 ネットワーキング ワークシート [3-10](#)
 ネットワーク アクセス リスト [28-24](#)
 ネットワーク オーナー [26-15](#)
 ネットワーク オーナー プロファイル ページ [26-14](#)
 ネットワーク タイム プロトコル (NTP)
 設定 [3-15, 3-35](#)
 ネットワーク トポロジ [B-4](#)
 ネットワーク トポロジの隠蔽 [5-11, 21-16](#)
 ネットワークの問題、トラブルシューティング [36-19](#)

は

ハード電源リセット [29-24, 36-28](#)

配信

暗号化 [20-2](#)
 配信キュー [30-24](#)
 配信キューのモニタリング [30-16](#)
 配信接続 ID (DCID) [30-4](#)
 配信のトラブルシューティング [36-25](#)
 配信ログ [34-2](#)
 バイパス
 アンチスパム [9-65](#)
 スロットリング [8-5](#)
 バウンス
 カンパセーション [21-36](#)
 カンパセーションでない [21-36](#)
 バウンス検証 [21-51](#)
 バウンス プロファイル [21-40](#)
 バウンス ログ [34-2](#)
 パケット キャプチャ [36-33](#)
 パスワード [2-3](#)
 設定 [28-18](#)
 変更 [28-17](#)
 パスワードの変更 [28-17](#)
 [パスワードの変更 (Change Password)] リンク [28-17](#)
 パスワード、変更 [28-17](#)
 送信メッセージ、定義済み [10-3](#)
 パフォーマンス [36-27](#)
 パブリック ブラックリスト [9-32](#)
 パブリック リスナー [3-27](#)
 デフォルト エントリ [7-2](#)
 判定
 イメージ分析 [11-6, 11-13](#)

ひ

日単位マグニチュード [26-14](#)
 ひとかたまりにする [21-2](#)
 秘密キー [20-1](#)
 評価キー
 McAfee [3-34](#)
 Sophos [3-34](#)

標準化 17-5

ふ

- ファイアウォールの許可 36-23
- ファイアウォール ポート D-1
- フィルタ 9-1
 - 解析不可能なメッセージ 9-21
 - 空白ヘッダーの一致 9-22
 - コメント文字 9-3
 - 辞書用語の一致 9-14, 9-34
 - スキャン可能なアーカイブ ファイルのタイプ 9-29
 - 正規表現および Python 9-18
- フィンガープリント 15-25
- フォワード DNS ルックアップ 30-21
- 負荷 30-4
- 復元
 - インストール 29-25
 - 使用可能なバージョン 29-26
- 複数の IP インターフェイス 21-62
- 複数のアプライアンス 3-13
- 複数の受信者 10-5
- 部分的アドレス
 - HAT 内の部分的アドレス 7-4
 - RAT 内の部分的アドレス 8-4
- 部分ドメイン
 - エイリアス テーブル内 21-7
- プライベート インジェクタ 3-29
- プライベート リスナー
 - デフォルト エントリ 7-2
- ブラウザ
 - 複数のウィンドウまたはタブ 2-2
- ブラックホール リスナー 5-3, 36-13
- プロキシ サーバ 29-24
- プロトコル
 - 「メール プロトコル」を参照

へ

- 別個のウィンドウでリンクを開く 26-7
- ヘッダー 21-7, 21-16, 21-17
 - アンチスパム 13-14
- ヘッダー、挿入 16-11
- ヘッダーの削除 9-62
- ヘッダーの挿入 16-11
- ヘッダー、メッセージ フィルタでの削除 9-62
- ヘッダー、ロギング 13-23, 34-43

ほ

- 保持期間
 - 隔離 27-4
- ホスト DNS 検証、説明 7-28
- ホスト アクセス テーブル (HAT)
 - GUI での順序変更 7-14
 - HAT 内の順序 7-2
 - 構文 7-1
 - 定義 7-1
 - パラメータ 7-8
 - ルール 7-1
- ホスト名 3-15, 3-24
 - セットアップ中のホスト名の指定 3-15
- ホスト名、設定 29-52
- ポリシー、事前定義 7-2
- 本文スキャン 9-29

ま

- マーケティング メッセージ 26-8
- マスカレード
 - CLI を使用した設定 21-16
 - LDAP クエリー使用 21-16
 - インポートおよびエクスポート 21-18
 - および altsrchost コマンド 21-16
 - コメント 21-17
 - 制限 21-17

静的テーブル使用 [21-16](#)

定義 [21-16](#)

テーブルの構文 [21-17](#)

不正なエントリのインポート [21-18](#)

マルウェア

定義済み [12-2](#)

マルチレイヤ アンチウイルス スキャン [12-2](#)

み

未分類隔離。「隔離、未分類」を参照

む

無効な受信者 [26-8](#)

め

メーリングリスト

通知 [27-23](#)

メール転送エージェント。「MTA」を参照。 [38-2](#)

メールトレンド グラフ [26-6](#)

メールの配信 [21-43](#)

Possible Delivery [21-56](#)

宛先ドメインへのメールの制御 [21-43](#)

制御 [21-43](#)

メッセージのタイムアウト [21-56](#)

メールのループ、検出 [9-107](#)

メール フロー ポリシー

\$ACCEPTED [7-12](#)

\$BLOCKED [7-11, 7-12](#)

\$RELAYED [7-12](#)

\$THROTTLED [7-11](#)

\$TRUSTED [7-11](#)

GUI を使用した追加 [7-15](#)

GUI を使用した編集 [7-13](#)

HAT パラメータ [7-8](#)

事前定義済み [7-11](#)

定義 [7-8](#)

メール フロー ポリシーでの DomainKeys および DKIM のイネーブル化 [17-2](#)

メール プロトコル

listenerconfig コマンドでの定義 [5-2](#)

メール ポリシー

First Match Wins [10-3](#)

LDAP [C-5](#)

ユーザの削除 [10-9, C-6](#)

ユーザの追加 [10-9, C-5](#)

メールポリシー、発信

RSA Enterprise Manager [15-30](#)

DLP [15-22](#)

メッセージ アクション

作成 [15-34](#)

メッセージ トラッキング

および重要なコンテンツ [15-38](#)

着信リレー [13-22](#)

メッセージのエンコード [5-7](#)

ヘッダーおよびフッターの設定 [5-7](#)

変更 [5-7, 9-92](#)

メッセージのリレー [3-26, 5-1](#)

メッセージのレプリケーション [9-43, 9-56](#)

メッセージ配信の再試行 [26-20](#)

メッセージ フィルタ [27-2](#)

attachment-protected [9-12](#)

attachment-unprotected [9-13](#)

body-dictionary-match [9-34](#)

MIME タイプ [9-29](#)

SenderBase レピュテーション スコア [9-33](#)

アクティブ化 (非アクティブ化) [9-81](#)

暗号化 [9-30](#)

移動 [9-80](#)

インポート [9-84](#)

エクスポート [9-85](#)

概要 [9-1](#)

組み合わせ [9-3, 9-15](#)

構文 [9-3](#)

削除 [9-80](#)

時間および日付 [9-26](#)
 順番 [9-4](#)
 ステータス [9-81](#)
 追加 [9-80](#)
 フィルタ アクション [9-43](#)
 変数 [9-49](#)
 ランダムな番号 [9-28](#)
 ルール [9-2](#)
 メッセージ フィルタ アクションの変数
 免責事項の使用 [18-15](#)
 メッセージ分裂
 定義 [10-5](#)
 メッセージ ヘッダー [9-27, 34-43](#)
 メッセージ ヘッダー、メッセージ フィルタでの追加 [9-62](#)
 メッセージ変更レベルのしきい値 [14-17](#)
 メッセージ変数
 スパム隔離通知 [27-26](#)
 メッセージ本文のスキャン [9-29](#)
 メモリ [30-5](#)
 免責事項
 メッセージへの追加 [18-12](#)
 免責事項スタンプ [18-12, 18-13](#)
 複数のエンコード [18-16](#)
 免責条項
 HTML テキスト リソース [18-11](#)
 テキスト リソースの使用 [18-12](#)

も

元の状態への切り替え [33-4](#)
 モニタリング (Monitoring) [30-7](#)

ゆ

ユーザ アカウント [28-1](#)
 制限 [28-1](#)
 ロックとロック解除 [28-17](#)
 ユーザ グループ [28-1, 28-2](#)

ユーザ タイプ [28-2](#)
 ユーザの環境設定
 定義 [29-59](#)
 ユーザ パスワードの長さ [28-4](#)
 ユーザ名 [28-4](#)

よ

陽性スコア [7-6](#)

ら

ライセンス キー [29-5](#)
 ライセンス ロード [29-6](#)
 ラウンドロビン方式の Virtual Gateway [21-60](#)

り

リアルタイム モニタリング [30-17](#)
 リージョナル スキャン [13-6](#)
 リスク要因スコア [15-2](#)
 DLP [15-18](#)
 リスナー
 LDAP 承認クエリー [5-12](#)
 Received: ヘッダーの追加 [5-11](#)
 暗号化 [5-13, 20-2](#)
 インジェクション カウンタのリセット期間 [5-6](#)
 厳密な SMTP アドレス解析 [5-9](#)
 最大同時接続数 [5-6](#)
 失敗した着信接続のタイムアウト [5-6](#)
 すべての着信接続の合計時間の制限 [5-7](#)
 設定 [5-1](#)
 定義 [5-1](#)
 デフォルトのドメインの追加 [5-10](#)
 パブリック [5-1](#)
 不正な MAIL FROM およびデフォルト ドメイン [5-12](#)
 プライベート [5-1](#)
 免責事項の追加 [18-12](#)

- リスナーの追加 [5-8](#)
- ルーズな SMTP アドレス解析 [5-9](#)
- リスナーの最大接続数 [21-56](#)
- リセット [29-3](#)
- リソース節約モード [30-4, 36-28](#)
- リバース DNS [25-5](#)
- リバース DNS ルックアップ [7-9, 21-59, 30-21](#)
- リモートアップグレード [29-20](#)
- リンク集約 [33-3](#)

る

ルーティング

- SMTP Call-Ahead サーバ [19-7](#)
- ルートサーバ (DNS) [3-16, 3-26](#)
- ループバック インターフェイス [33-16](#)

ルックアップ

- DNS A [7-3, 7-28](#)
- DNS PTR [7-3, 7-28](#)

れ

例外テーブル

- エントリの追加 [7-35](#)
- レート [30-6](#)
- レート制限 [7-12](#)
- レピュテーションフィルタの推奨段階的手法 [6-4](#)
- レピュテーションフィルタリング [6-1](#)
- レピュテーションフィルタリングによる阻止 [26-8](#)
- レポート
 - アーカイブ [26-44](#)
 - 着信リレー [13-22](#)
- レポート DLP [15-42](#)
- レポートのアーカイブ [26-44](#)
- 連邦情報処理標準
 - FIPS 管理を参照

ろ

ロギング

- 概要 [34-1](#)
- ロギング オプション [34-43](#)
- ロギング、ヘッダー [13-23, 34-43](#)
- ログ
 - CLI 監査ログ [34-3](#)
 - FTP サーバログ [34-3](#)
 - HTTP ログ [34-3](#)
 - IronPort テキスト メール ログ [34-2](#)
 - LDAP デバッグ ログ [34-3](#)
 - NTP ログ [34-3](#)
 - qmail 形式配信ログ [34-2](#)
 - SCP プッシュ [34-7](#)
 - syslog プッシュ [34-7](#)
 - アンチウイルス [34-3](#)
 - アンチウイルス アーカイブ [34-3](#)
 - アンチスパム アーカイブ [34-3](#)
 - インジェクションデバッグ ログ [34-2, 34-3](#)
 - グローバル属性 [34-41](#)
 - 形式 [34-1](#)
 - コンフィギュレーション履歴ログ [34-38](#)
 - サブスクリプション [34-7](#)
 - スキャン [34-4](#)
 - ステータス ログ [34-2](#)
 - 定義 [34-1](#)
 - 定義されたログ サブスクリプション [34-1](#)
 - トラブルシューティング [36-25](#)
 - 配信ログ [34-2](#)
 - バウンス ログ [34-2](#)
 - ファイル名の拡張子 [34-44](#)
 - メッセージヘッダー [34-43](#)
 - レベル [34-40](#)
 - ロールオーバー [34-7](#)
- ログ サブスクリプション [34-1, 34-7](#)
 - IronPort Anti-Spam [13-10](#)
 - Sophos [12-11](#)
- ログ ファイルタイプ [34-2](#)

ログ ファイルのロールオーバー [34-44](#)

論理 IP インターフェイス [3-17](#), [3-24](#)

わ

ワーク キュー [30-5](#), [30-35](#)

ワーク キュー、一時停止 [30-35](#)

ワーク キューの一時停止 [30-35](#)

©2008 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0809R)

この資料の記載内容は2008年10月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先: シスコ コンタクトセンター

0120-092-255(フリーコール、携帯・PHS含む)

電話受付時間: 平日 10:00~12:00、13:00~17:00

<http://www.cisco.com/jp/go/contactcenter/>