Cisco IronPort AsyncOS 7.6 for Email
コンフィギュレーション ガイド

2013 年 2 月 25 日

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
ミッド タウン・タワー
http://www.cisco.com/jp
Tel： 408 526-4000
0120-092-255（フリーコール、携帯・PHS含む）
Fax： 408 527-0883

Text Part Number: OL-26342-01-J

【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、米国シスコシステムズ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。

Cisco IronPort AsyncOS 7.6 for Email コンフィギュレーション ガイド

CONTENTS

CHAPTER 1

Cisco IronPort E メール セキュリティ アプライアンスをご使用の前に

このリリースの新機能

ここでは、AsyncOS for Email Security 7.6 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 IronPort 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。

新しい機能：IPv6 のサポート

AsyncOS 7.6 では、E メール セキュリティ アプライアンスにインターネット プロトコル バージョン 6（IPv6）アドレスの互換性が追加されています。アプライアンスの IP インターフェイスに IPv4 と IPv6 の両方のアドレスを使用することができます。IPv6 アドレスは、次の機能のオプションでもあります。

- ゲートウェイ（デフォルト ルータ）とスタティック ルート。
- SMTP ルート。
- SMTP コール アヘッド。
- トレース。
- ホスト アクセス テーブルの送信者。
- 受信者アクセス テーブルの受信者。
- コンテンツ フィルタのリモート IP 状態と代替送信ホストにメッセージを送信アクション。

- 宛先コントロールでは、IPv4 アドレスまたは IPv6 アドレスのどちらを優先するかを指定できます。
- アウトブレイク フィルタのバイパス ドメイン スキャン フィールド。
- レポート検索。

AsyncOS は、次の形式の IPv6 アドレスをサポートしています。

- `2620:101:2004:4202::0-2620:101:2004:4202::ff`
- `2620:101:2004:4202::`
- `2620:101:2004:4202::23`
- `2620:101:2004:4202::/64`

新しい機能：RSA Enterprise Manager の統合

AsyncOS 7.6 の RSA Enterprise Manager の統合を使用すると、組織は、E メール セキュリティ アプライアンスのデータ損失防止ポリシーを RSA セキュリティの Enterprise Manager ソフトウェアに移行し、それらのポリシーをすべてのベクターの強制に配布できます。RSA Enterprise Manager の統合を使用すると、企業全体で一貫性のある DLP ポリシーを確保でき、必要に応じてローカルの E メール セキュリティ アプライアンスでポリシーを管理するオプションも引き続き使用できます。RSA の DLP データセンターのユーザの場合は、RSA Enterprise Manager の統合によって、ソース コードとドキュメントを特定の DLP ポリシーにスキャンするためのフィンガープリント検出も提供されます。

Enterprise Manager は、RSA Security, Inc. が提供するサードパーティ製ソフトウェアであり、Cisco IronPort E メール セキュリティ アプライアンスの一部ではありません。

詳細については、第 11 章、データ損失の防止を参照してください。

RSA Enterprise Manager の統合の一環として、AsyncOS に LDAP プロファイル用のユーザ識別名 LDAP クエリが含まれるようになりました。このクエリでは、E メール セキュリティ アプライアンスのメッセージ送信者の識別名が返され、Enterprise Manager に送信される他のすべての DLP インシデント データが含まれています。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。

拡張機能：DLP メッセージ アクション

AsyncOS 7.6 以降、DLP ポリシーによって実行されるプライマリ アクションとセカンダリ アクションは、*メッセージ アクション*として定義されるようになりました。メッセージ アクションは、GUI の [メールポリシー（Mail Policies）] > [DLP メッセージアクション（DLP Message Actions）] ページを使用して作成し、次にそのアクションを DLP ポリシーに追加します。以前のバージョンの AsyncOS からアップデートする場合、システムは既存の DLP ポリシーで定義されているプライマリ アクションとセカンダリ アクションに基づいて新しいメッセージ アクションを自動的に生成します。

詳細については、第 11 章、データ損失の防止を参照してください。

拡張機能：ユーザ グループ別 DLP メッセージ トラッキング権限

AsyncOS 7.6 では、管理者以外のどのユーザが、ユーザ ロールによるメッセージ トラッキングで機密性の高い DLP 関連情報を表示できるかを選択できます。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。

拡張機能：RSA メール DLP の「コピーを隔離して配信（Quarantine a Copy and Deliver）」オプション

AsyncOS 7.6 には、RSA メール DLP ポリシーに違反するメッセージのコピーを隔離する一方で、元のメッセージを引き続き配信するオプションがあります。

詳細については、DLP ポリシー（11-11 ページ）を参照してください。

拡張機能：SenderBase レピュテーション サービスにはスパム対策機能キーが必要

AsyncOS 7.6 以降、E メール セキュリティ アプライアンスでは、SenderBase レピュテーション サービスを使用するにはスパム対策システム機能キーが必要です。

新しい機能：DKIM 検証プロファイル

AsyncOS 7.6 では、E 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 シグネチャの検証に使用するパラメータのリストである DKIM 検証プロファイルが追加されています。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 つ目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。

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

拡張機能：DKIM 署名プロファイルの新しいタグ

AsyncOS 7.6 では、DKIM メッセージ シグネチャに含めるタグの新しいリストが追加されています。DKIM 署名プロファイルを作成するときに、署名に含めるタグを選択します。次のタグを使用できます。

- **「i」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、メーリング リスト マネージャ）。
- **「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カンマ区切りリスト。
- **「t」タグ。**署名が作成されたときのタイムスタンプ。
- **「x」タグ。**秒による署名の有効期限。（AsyncOS 7.6 の以前のバージョンに存在していた「x」タグ情報のオプション）。
- **「z」タグ。**垂直バー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。

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

新しい機能:システム生成メッセージの DKIM 署名

AsyncOS 7.6 では、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。E メール セキュリティ アプライアンスが署名するシステム生成メッセージの種類には、次のものがあります。

- Cisco IronPort スパム隔離通知
- 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

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

拡張機能:DKIM 署名アクションのスキップ

AsyncOS 7.6 では、コンテンツ フィルタに DKIM 署名をスキップするアクションが追加されました。

詳細については、コンテンツ フィルタのアクション (6-15 ページ)を参照してください。

拡張機能: メール フロー ポリシーのエンベロープ送信者のレート制限と TLS 強制

AsyncOS 7.6 では、特定の期間に受信者数を制限するオプションを使用してメール フロー ポリシーを更新し、リスナーがメール送信元アドレスに基づいて一意のエンベロープ送信者から受信するようにします。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。

メール フロー ポリシーの設定が [TLS での暗号化を優先(Preferred for encryption over TLS)] の場合は、特定のドメインのエンベロープ送信者または特定の電子メール アドレスのエンベロープ送信者に対し TLS 接続を必須にすることもできます。

詳細については、メール フロー ポリシー:アクセス ルールとパラメータ (5-8 ページ)を参照してください。

これらのエンベロープ送信者のドメインと電子メール アドレスは、アドレス リストを使用して指定します。詳細については、アドレス リスト (5-42 ページ)を参照してください。

また、AsyncOS にはレート制限レポートが追加されており、多数のメッセージから個々の送信者をすばやく識別できます。このレポートを使用して、内部ユーザ アカウントから迷惑メールを制御し、侵害を受けたユーザ アカウントを特定し、電子メールを使用する制御不能なアプリケーションを制限し、このような状況に起因する組織のオンラインでの評判の損害および付随する混乱を避けることができます。

詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Using Email Security Monitor」を参照してください。

拡張機能：AsyncOS のアップグレードとその他のサービスのアップデート用のアップデート サーバの分離

AsyncOS 7.6 では、機能キーの更新、アウトブレイク フィルタ、タイム ゾーン ルールなど、他のサービスのアップデートに使用されているサーバとは異なる AsyncOS アップグレード用のアップデート サーバを指定することができます。たとえば、AsyncOS アップグレードのダウンロードにはローカル サーバを指定し、他のサービス アップデート用には Cisco IronPort アップデート サーバを使用することができます。

詳細については、サービスのアップデート（15-9 ページ）を参照してください。

拡張機能：Web ユーザ インターフェイスの保護

AsyncOS 7.6 for Email では、クロスサイト リクエスト フォージェリ（CSRF）および Web ユーザ インターフェイスへのその他の攻撃に対して追加の保護が導入されています。

電子メール セキュリティ アプライアンスの関連資料

電子メール セキュリティ アプライアンスの関連資料は、次のとおりです。

- 『*Cisco IronPort AsyncOS for Email Daily Management Guide*』。このマニュアルでは、Cisco IronPort アプライアンスの管理およびモニタリングを行うためにシステム管理者が使用する、一般的な日常業務（電子メール セキュリティ モニタを使用した電子メール トラフィックの表示、電子メール メッセージのトラッキング、システム検疫の管理、アプライアンスのトラブルシューティングなど）を実行する方法について説明します。また、電子メール セキュリティ モニタ ページ、AsyncOS ログ、CLI サポート コマンド、隔離など、システム管理者が定期的に使用する機能についての参考情報も含まれています。
- 『*Cisco IronPort AsyncOS for Email Configuration Guide*』。このマニュアルは、新しい Cisco IronPort アプライアンスを設定しており、そのアプライアンスの電子メール配信機能に関する知識を必要とするシステム管理者に推奨されます。このマニュアルでは、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し、電子メール ゲートウェイ アプライアンスとして設定する方法について説明します。また、電子メール パイプライン、アウトブレイク フィルタ、コンテンツ フィルタ、RSA メール DLP、電子メール暗号化、アンチウイルス スキャン、アンチスパム スキャンなど、電子メール配信機能の参考情報および設定手順についても説明します。
- 『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』。このマニュアルでは、Cisco IronPort アプライアンスの高度な機能を設定する方法について説明します。LDAP を使用するためのアプライアンスの設定、電子メール ポリシーを施行するためのメッセージ フィルタの作成、複数のアプライアンスのクラスタ化、アプライアンスでのリスナーのカスタマイズなどの項目が含まれています。設定に加えて、メッセージ フィルタ ルールおよびアクション、コンテンツ ディクショナリおよびメッセージ フィルタ ルールで使用される正規表現、LDAP クエリー構文および属性などの高度な機能に関する参考資料も紹介します。
- 『*Cisco IronPort AsyncOS CLI Reference Guide*』このマニュアルでは、AsyncOS コマンドライン インターフェイス（CLI）のコマンドの詳細なリストおよびコマンドの使用例を示します。システム管理者は、Cisco IronPort アプライアンスで CLI を使用する際の参考資料としてこのマニュアルを使用できます。

このマニュアルでは、内容に関する追加情報を得るために他のマニュアルを参照することがあります。これらのマニュアルは、Cisco IronPort アプライアンスに同梱の Documentation CD および Cisco IronPort Customer Support Portal で入手できます。詳細については、Cisco IronPort サポート コミュニティ（1-11 ページ）を参照してください。

このマニュアルの使い方

このマニュアルを情報源として使用し、Cisco IronPort アプライアンスの機能について学習します。項目は、論理的な順序に整理されています。必ずしもマニュアルのすべての章を通読する必要はありません。目次およびこのマニュアルの構成（1-6 ページ）を参照して、お使いのシステムに関連する章を確認してください。

このマニュアルは、参考資料として使用することもできます。ネットワークおよびファイアウォールの構成設定など、アプライアンスの使用期間を通して参照する可能性のある重要な情報が含まれています。

このマニュアルは、印刷物として配布されます。また、PDF ファイル、HTML など電子的にも配布されます。このマニュアルの電子版は、Cisco IronPort Customer Support Portal で入手できます。また、右上の [ヘルプとサポート（Help and Support）] リンクをクリックすることにより、アプライアンスの GUI からマニュアルの HTML オンライン ヘルプ バージョンにアクセスできます。

はじめる前に

このマニュアルを読み始める前に、『*Cisco IronPort Quickstart Guide*』および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。このガイドでは、アプライアンスを梱包箱から取り出し、物理的にラックに取り付けて電源を投入済みであることを前提としています。

（注）　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 IronPort 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。（Cisco IronPort X1000/1000T/1050/1060/1070、C60/600/650/660/670、および C30/300/300D/350/350D/360/370 アプライアンスの）管理ポートまたは（Cisco IronPortC10/100/150/160 アプライアンスの）Data 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。

このマニュアルの構成

第 1 章、Cisco IronPort E メール セキュリティ アプライアンスをご使用の前には、Cisco IronPort アプライアンスの概要について説明し、エンタープライズ ネットワークにおける主な機能および役割を明示します。最新リリースの新機能について説明します。

第 2 章、概要では、Cisco IronPort AsyncOS for Email について、および Cisco IronPort アプライアンスの GUI および CLI を使用した管理について説明します。CLI を使用するための表記法について説明します。この章では、汎用的な CLI コマンドの概要についても説明します。

第 3 章、セットアップおよび設置では、ネットワーク計画、アプライアンスの初期システム設定と構成など、Cisco IronPort アプライアンスに接続するためのオプションについて説明します。

第 4 章、電子メール パイプラインについてでは、電子メール パイプライン（電子メールが Cisco IronPort アプライアンスによって処理されるときに電子メールが従うフロー）と、パイプラインを構成する機能の概要を示します。説明には、機能の詳細な説明を含むセクションへの相互参照が含まれています。

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では、電子メール ゲートウェイとしてアプライアンスを設定するプロセスについて説明します。この章では、着信電子メール トラフィックおよびメール フロー モニタをサポートする、インターフェイス、リスナー、およびホスト アクセス テーブル（HAT）の概念について説明します。

第 6 章、電子メール セキュリティ マネージャでは、Cisco IronPort 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 マネージャについて説明します。電子メール セキュリティ マネージャを使用すると、感染フィルタ機能、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、個別のインバウンドおよびアウトバウンド ポリシーを介して、受信者または送信者単位で管理できます。

第 7 章、レピュテーション フィルタリングでは、SenderBase レピュテーション サービスのスコアを使用して、メッセージ送信者の評判に基づいて受信メールを制御する方法の概要を示します。

第 9 章、アンチスパム では、Cisco IronPort アプライアンスに統合された SenderBase レピュテーション フィルタ、Cisco IronPort Anti-Spam、および Cisco IronPort Intelligent Multi-Scan 機能を使用して、スパムと戦うための固有のアプローチについて説明します。

第 8 章、アンチウイルスでは、Cisco IronPort アプライアンスに統合された Sophos および McAfee Anti-Virus スキャン機能について説明します。

第 10 章、アウトブレイク フィルタでは、アウトブレイク フィルタが新しいウイルス、詐欺、フィッシングの発生に対して重要な最初のレイヤによる防御をプロアクティブに提供する方法を説明します。アウトブレイク フィルタは、新しい発生をリアルタイムで検出し、疑わしいトラフィックがネットワークに侵入しないように動的に応答することにより、新しいシグネチャの更新が導入されるまで保護します。

第 11 章、データ損失の防止では、RSA Security, Inc. のデータ損失防止機能を使用して組織の情報および知的財産を保護する方法、およびユーザが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規制および組織のコンプライアンスを実施する方法について説明します。

第 12 章、Cisco IronPort 電子メール暗号化では、Cisco IronPort 暗号化アプライアンスまたはホステッド キー サービスを使用して、電子メールの暗号化に使用するプロセスについて説明します。

第 13 章、SenderBase Network Participation では、アプライアンスのデータを SenderBase ネットワークと共有する方法について説明します。

第 14 章、テキスト リソースでは、AsyncOS のさまざまなコンポーネントで使用するコンテンツ ディクショナリ、通知テンプレート、免責事項などのテキスト リソースの作成について説明します。

第 15 章、システム管理では、機能キーの操作、AsyncOS のアップグレード、AsyncOS の復帰、ルーチンのシステム メンテナンスの実行など、Cisco IronPort アプライアンスの管理と監視のための一般的な管理コマンドについて説明します。メンテナンス タスクには、システム時刻の設定、管理者パスワードの変更、およびシステムのオフライン化が含まれます。この章では、DNS、インターフェイス、ルーティング、ホスト名の設定など、Cisco IronPort アプライアンスのネットワーク操作を設定する方法についても説明します。

第 16 章、C350D アプライアンスのイネーブル化では、Cisco IronPort C300D、C350D、および C360D アプライアンスについて説明します。

第 17 章、Cisco IronPort M-Series セキュリティ管理アプライアンスでは、Cisco IronPort M-Series アプライアンスについて説明します。このアプライアンスは、重要なポリシーおよびランタイム データを集中管理および統合するために設計されており、管理者やエンド ユーザにレポート作成の管理および情報の監査のための単一のインターフェイスを提供します。

付録 A、メアプライアンスへのアクセスモでは、ファイルをアップロードおよびダウンロードするために Cisco IronPort アプライアンスにアクセスする方法について説明します。

付録 B、メネットワーク アドレスと IP アドレスの割り当てモでは、ネットワークおよび IP アドレスの割り当て関する全般的なルールについて説明し、企業ネットワーク インフラストラクチャ内で Cisco IronPort アプライアンスに接続する手段を示します。

付録 C、メファイアウォール情報モでは、セキュリティ ファイアウォールの背後にある Cisco IronPort アプライアンスを適切に動作させるために、開く必要性が生じることがあるポートについて説明します。

付録 D、メエンド ユーザ ライセンス契約書モには、Cisco IronPort E メール セキュリティ アプライアンスのソフトウェア使用許諾契約が含まれています。

『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』で説明されているトピック

『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』では、次のトピックについて説明しています。

第 1 章「Customizing Listeners」では、企業の電子メール ゲートウェイの設定を調整するためのプロセスについて説明します。この章では、ゲートウェイを通って受信する電子メールを処理するために、インターフェイスおよびリスナーを設定する際に使用できる高度な機能を詳細に説明します。

第 2 章「Configuring Routing and Delivery Features」では、Cisco IronPort アプライアンスを通過する電子メールのルーティングと配信に影響を与える機能について説明します。

第 3 章「LDAP Queries」では、Cisco IronPort アプライアンスが社内の Lightweight Directory Access Protocol（LDAP）サーバに接続し、承認する受信者の確認（グループ メンバーシップなど）を目的としたクエリーの実行方法、メールのルーティングとアドレスの書き換え、ヘッダーのマスカレード、および SMTP 認証のサポートについて説明します。

第 4 章「Email Authentication」では、Cisco IronPort アプライアンスで電子メール認証を設定してイネーブルにするプロセスについて詳しく説明します。Cisco IronPort AsyncOS は、複数のタイプの電子メール認証をサポートしています。これには、着信メールの Sender Policy Framework（SPF）検証、Sender ID Framework（SIDF）検証、DomainKeys Identified Mail（DKIM）検証、および発信メールの DomainKeys 署名と DKIM 署名が含まれます。

第 5 章「Using Message Filters to Enforce Email Policies」では、メッセージ フィルタを使用して、電子メールを処理するためのルールを定義する方法について説明します。また、添付ファイル フィルタリング、イメージ分析、およびコンテンツ ディクショナリの機能を使用してメッセージの内容を修正する機能についても説明します。

第 7 章「Advanced Network Configuration」には、NIC ペアリング、仮想 LAN などの情報が含まれています。

第 8 章「Centralized Management」では、複数のアプライアンスを管理および設定できる集中管理機能について説明します。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。

付録 A「AsyncOS Quick Reference Guide」では、CLI のほとんどのコマンドのクイック リファレンスについて説明します。

付録 B「Accessing the Appliance」では、Cisco IronPort アプライアンスからファイルを送信および取得するために Cisco IronPort アプライアンスにアクセスする方法について説明します。

『*Cisco IronPort AsyncOS for Email Daily Management Guide*』では、次のトピックについて説明しています

第 1 章「Managing the Cisco IronPort Email Appliance」では、Cisco IronPort アプライアンスの概要について説明し、企業ネットワークにおけるその主な機能および役割を定義します。

第 2 章「Using Email Security Monitor」では、企業のすべての着信電子メール トラフィックを完全に可視化する、強力な Web ベースのコンソールであるメール フロー モニタ機能について説明します。

第 3 章「Tracking Email Messages」では、ローカル メッセージ トラッキングについて説明します。メッセージ トラッキングを使用すると、特定のメッセージが配信されたか、ウイルスを含むことが検出されたか、スパム検疫エリアに配置されたかを確認できます。

第 4 章「Quarantines」では、メッセージの保留および処理に使用される特別なキューまたはリポジトリについて説明します。検疫エリア内のメッセージは、検疫の設定方法に基づいて、配信するか削除することができます。これには、Cisco IronPort スパム検疫が含まれます。

第 5 章「Logging」では、Cisco IronPort アプライアンスのロギングおよびログ サブスクリプション機能について説明します。

第 6 章「Managing and Monitoring via the CLI」では、ゲートウェイを通過するメール フローのモニタ時に使用できる CLI のコマンドについて説明します。

第 7 章「Other Tasks in the GUI」では、GUI を使用して Cisco IronPort アプライアンスを管理およびモニタするための代表的な管理タスクについて説明します。

第 8 章「Common Administrative Tasks」では、ユーザの追加、設定ファイルの管理、SSH キーの管理など、Cisco IronPort アプライアンスの管理と監視のための一般的な管理コマンドについて説明します。この章では、テクニカル サポートの依頼方法、Cisco IronPort カスタマー サポートによるアプライアンスへのリモート アクセスを許可する方法、および機能キーの使用方法についても説明します。

第 9 章「Testing and Troubleshooting」では、システムのパフォーマンスをテストし設定の問題をトラブルシューティングするための、いわゆる*ブラックホール リスナー*を作成するプロセスについて説明します。

付録 A「Accessing the Appliance」では、ファイルをアップロードおよびダウンロードするために Cisco IronPort アプライアンスにアクセスする方法について説明します。

印刷時の表記法

書体	意味	例
AaBbCc123	コマンド、ファイル、およびディレクトリの名前、画面に表示されるコンピュータの出力。	`Please choose an IP interface for this Listener.` `sethostname` コマンドは、Cisco IronPort アプライアンスの名前を設定します。
AaBbCc123	画面に表示されるコンピュータの出力ではなく、ユーザによる入力。	`mail3.example.com>` **`commit`** `Please enter some comments describing your changes:` `[]>` **`Changed the system hostname`**
AaBbCc123	書名、新規用語、強調表示される用語、およびコマンド ライン変数。コマンド ライン変数の場合、イタリック体のテキストは、実際の名前または値のプレースホルダです。	『*Cisco IronPort Quickstart Guide*』をお読みください。 Cisco IronPort アプライアンスは、発信パケットを送信するためのインターフェイスを一意に選択できる*必要があります*。 `Before you begin, please reset your password to a new value.` `Old password:` **`ironport`** `New password:` *`your_new_password`* `Retype new password:` **`your_new_password`**

詳細情報の入手先

シスコは、Cisco IronPort 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。

Cisco IronPort 技術トレーニング

Cisco IronPort システム技術トレーニング サービスは、Cisco IronPort セキュリティ製品およびソリューションの評価、統合、デプロイ、保守、およびサポートを正しく行うために必要な知識と技術の習得を支援します。

次のいずれかの方法で、Cisco IronPort 技術トレーニング サービスまでお問い合わせください。

トレーニング。登録およびトレーニング全般に関するご質問の場合:

- http://training.ironport.com
- training@ironport.com

認定。認定および認定試験に関するご質問の場合:

- http://training.ironport.com/certification.html
- certification@ironport.com

ナレッジ ベース

Customer Support Portal の Cisco IronPort 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次のリンク先で登録できます。https://tools.cisco.com/RPF/register/register.do

Knowledge Base には、Cisco IronPort 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 IronPort 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 IronPort 製品の使用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、Problem-and-Solution の記事では、製品の新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。**参考資料の記事は、通常、特定のハードウェアに関連するエラー コードなど情報のリストを提供します。
- **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 IronPort 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 番号がついています。

Cisco IronPort サポート コミュニティ

Cisco IronPort サポート コミュニティは、Cisco IronPort 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 IronPort 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 IronPort ユーザと情報を共有したりできます。

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

https://supportforums.cisco.com

Cisco IronPortカスタマー サポート

Cisco IronPort 製品のサポートは、年中無休の 24 時間体制で、電話、電子メール、またはオンラインでご依頼いただけます。

カスタマー サポートの営業時間（月曜から金曜までの 1 日 24 時間、ただし米国の祝日を除く）中は、依頼を受けてから 1 時間以内にエンジニアがご連絡します。

営業時間外に緊急の援助を必要とする重大な問題を報告するには、Cisco IronPort 以下の方法のいずれかを使用して連絡してください。

米国フリーダイヤル：1(877) 641- 4766

海外：http://cisco.com/web/ironport/contacts.html

ポート サイト：http://cisco.com/web/ironport/index.html

リセラーまたは他のサプライヤからサポートを購入した場合、製品に関するサポートについては、直接そのリセラーもしくはサプライヤにお問い合わせください。

サード パーティ コントリビュータ

Cisco IronPort 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 IronPort 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 IronPort 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。

Cisco IronPort へのコメントの送付

Cisco IronPort Technical Publications チームでは、より充実した製品マニュアルを提供すべく努めています。コメントや提案がございましたら、ぜひ以下の電子メールまでお知らせください。

contentsecuritydocs@cisco.com

メッセージの件名に次の部品番号を含めてください。OL-26342-01

Cisco IronPort E メール セキュリティ アプライアンスの概要

Cisco IronPort 電子メール セキュリティ アプライアンスは、要求水準が最も高い企業ネットワークの電子メール インフラストラクチャのニーズを満たすために設計された高性能機器です。電子メール セキュリティ アプライアンスは、スパムおよびウイルスを排除し、社内ポリシーを順守させます。また、ネットワーク境界をセキュアに保ち、企業の電子メール インフラストラクチャの Total Cost of Ownership（TCO; 総所有コスト）を削減します。

Cisco IronPort システムは、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します。

Cisco IronPort AsyncOS™ オペレーティング システムは、複数のインテリジェントな機能を Cisco IronPort アプライアンスに統合します。

- SenderBase レピュテーション フィルタと Cisco IronPort 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 IronPort の独自保護機能である **Outbreak Filters™**。

- 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 IronPort 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 IronPort 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、E 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 IronPort 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**アクセス制御**。
- 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なります。
- **Virtual Gateway**™ テクノロジーにより、Cisco IronPort 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、インターネット メッセージングのタスク用に高度に最適化された専用のオペレーティング システムです。AsyncOS は、「強化された」オペレーティング システムです。不要なすべてのサービスは取り除かれ、セキュリティの向上とシステム パフォーマンスの最適化が図れています。Cisco IronPort のスタックレスなスレッディング テクノロジーにより、各タスクに対する専用メモリ スタックの割り当ては行われず、MTA の同時並行性と安定性が向上します。従来のオペレーティング システムでの CPU の割り込み型タイム スライシングと比べ、カスタム I/O 駆動型スケジューラは、電子メール ゲートウェイで要求される大量の並列 I/O イベントに対して最適化されています。AsyncOS の基礎となるファイル システムの AsyncFS は、何百万もの小さいファイルを扱うために最適化され、システム障害が発生した場合のデータの復元性を確保します。

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。Cisco IronPort アプライアンスは、設定と管理を簡易化するように設計されています。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。Cisco IronPort アプライアンスには、確実なロギング機能もあり、システム全体の機能にわたるログ サブスクリプションを設定して、必要な情報を見つけるために費やす時間を削減します。

メール フローおよび Cisco IronPort M-Series アプライアンス

M-Series アプライアンスが構成に含まれている場合は、他の Cisco IronPort（C-Series および X-Series）アプライアンスから Cisco IronPort M-Series アプライアンスにメールが送信されます。Cisco IronPort M-Series 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 IronPort アプライアンスは、その M-Series 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、Cisco IronPort M-Series 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。Cisco IronPort M-Series 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。Cisco IronPort M-Series 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。

Cisco IronPort M-Series アプライアンスでは、Cisco IronPort スパム検疫設定で指定されている IP アドレスから検疫対象のメールを受け入れます。Cisco IronPort M-Series アプライアンスでローカル検疫を設定するには、『*Cisco IronPort AsyncOS for Security Management User Guide*』を参照してください。Cisco IronPort M-Series アプライアンスのローカル検疫は、M-Series アプライアンスにメールを送信する他の Cisco IronPort アプライアンスからは、*外部*の検疫と見なされることに注意してください。

Cisco IronPort M-Series アプライアンスによって解放されたメールは、スパム検疫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 IronPort 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 IronPort AsyncOS for Security Management User Guide*』を参照）。したがって、Cisco IronPort M-Series アプライアンスにメールを配信する Cisco IronPort 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 IronPort アプライアンス）に送信されます。Cisco IronPort M-Series 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。

CHAPTER 2

概要

この章では、Cisco IronPort AsyncOS オペレーティング システム、および 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）の両方を使用した Cisco IronPort アプライアンスの管理について説明します。各インターフェイスを使用する場合の表記法について説明します。この章では、汎用的な CLI コマンドについても説明します。

Web ベースのグラフィカル ユーザ インターフェイス（GUI）

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のためのコマンドライン インターフェイス（CLI）に代わる Web ベースの方法です。GUI を使用することにより、Cisco IronPort 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。

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。このマニュアルで説明しているタスクの多くは、最初に GUI（可能な場合）からタスクを実行する方法を示し、続いて CLI コマンドから同じタスクを実行する方法を示しています。

以降の章で、GUI を使用して次の処理を実行する方法について学習します。

- System Setup Wizard にアクセスして、Cisco IronPort アプライアンスの初期インストールおよび設定を実行します。
- 電子メール セキュリティ マネージャにアクセスして、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します。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 IronPort 評価フィルタ、感染フィルタ、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 フィルタリング ポリシーを管理できます。
- リスナーのホスト アクセス テーブル（HAT）を編集し、SenderBase Reputation Score（SBRS; SenderBase 評価スコア）などの送信者の評価を照合することにより、独自の送信者グループのカスタマイズ（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）し、メール フロー ポリシーを調整します。
- ディクショナリ、免責事項などのテキスト リソースを作成および管理します。
- Cisco IronPort 電子メール暗号化を使用してアウトバウンドの電子メールを暗号化するように、暗号化プロファイルを設定します。

- Cisco IronPort Anti-Spam、Sophos Anti-Virus、感染フィルタ、および SenderBase Network Participation のグローバル設定を行います。
- XML ページを使用してステータスを表示するか、プログラムで XML ステータス情報にアクセスします。

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、さらに、Cascading Style Sheet（CSS）を含む HTML ページをレンダリングできる必要があります。

（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 IronPort 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 IronPort 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 IronPort 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 IronPort 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、Enabling the GUI on an Interface（-442 ページ）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、必ず、「`https://`」というプレフィックスを使用して GUI にアクセスしてください。

ログイン

GUI にアクセスしているすべてのユーザがログインする必要があります。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（2-2 ページ）を参照）。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、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Common Administrative Tasks」の章の「Adding Users」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 IronPort 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用します。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 IronPort 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。

中央集中型の管理

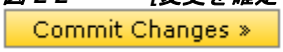
集中管理機能を使用し、クラスタをイネーブルにしている場合は、クラスタ内のマシンを参照し、クラスタ、グループ、マシン間での設定の作成、削除、コピー、および移動（つまり、`clustermode` コマンドおよび `clusterset` コマンドと同等の内容）を GUI 内から実行できます。

詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Administering a Cluster from the GUI」を参照してください。

[変更を確定（Commit Changes）] ボタン

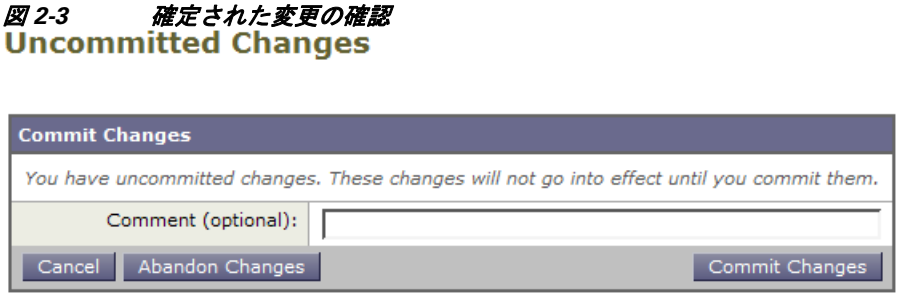
GUI の確定モデルは、CLI で使用されている「明示的な確定」モデルと同じです（詳細については、設定変更の確定（2-10 ページ）を参照してください）。GUI で設定を変更する際は、[変更を確定（Commit Changes）] ボタンをクリックして、それらの変更を明示的に確定する必要があります。このボタンは、保存する必要のある未確定の変更がある場合に表示されます。

図 2-2　　[変更を確定（Commit Changes）] ボタン



[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（2-10 ページ）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



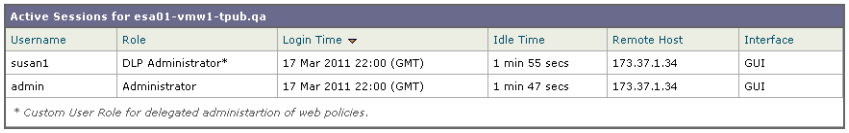
アクティブなセッションの表示

GUI から、現在 E 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 セッション（Active Sessions）



コマンドライン インターフェイス（CLI）

Cisco IronPort AsyncOS のコマンドライン インターフェイスは、Cisco IronPort 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。コマンドは、引数の有無を問わず、コマンド名を入力すると起動されます。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、電子メールを受信するためのゲートウェイの設定（5-1 ページ）に説明されている `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 IronPort 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 のプロンプトが現在のモードを示すように変更されます。次に例を示します。

```
(Cluster Americas) >
```

または

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

詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Centralized Management」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)
```

コマンドの構文

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 キーを組み合わせて使用します。

```
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 IronPort 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。入力した文字が複数のコマンドに該当する場合、CLI はそのセットをさらに「絞り込み」ます。次に例を示します。

```
mail3.example.com> set (type the Tab key)
setgateway, sethostname, settime, 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 IronPort 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 IronPort AsyncOS for Email Advanced Configuration Guide*』の付録 A「AsyncOS Quick Reference Guide」を参照するか、『*Cisco IronPort AsyncOS CLI Reference Guide*』を確認してください。

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

このセクションでは、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 IronPort 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。詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の付録 A「AsyncOS Quick Reference Guide」を参照してください。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 IronPort 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、タイムスタンプと共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 IronPort 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 の入力は、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

この章では、System Setup Wizard を使用して、電子メール配信用に Cisco IronPort C-Series または X-Series アプライアンスを設定するプロセスについて説明します。Cisco IronPort M-Series アプライアンスを設定する場合は、第 17 章、Cisco IronPort M-Series セキュリティ管理アプライアンスを参照してください。この章を終了すると、Cisco IronPort アプライアンスによって、インターネット越しまたはネットワーク内で SMTP 電子メールを送信できるようになっています。

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。

設置計画

はじめる前に

Cisco IronPort 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。ここでは、設置を計画するときに採用可能な複数のオプションについて説明します。

ネットワーク境界に Cisco IronPort アプライアンスを配置する

Cisco IronPort アプライアンスは、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ることに注意してください。インターネット メッセージング専用に機能強化されたオペレーティング システムに加え、AsyncOS オペレーティング システムの最新機能の多くは、電子メールの送受信のためにインターネット（つまり外部 IP アドレス）に直接アクセスできる IP アドレスを持つ、最初のマシンとしてアプライアンスを設置した場合に、最適な性能を発揮します。次に例を示します。

- 受信者ごとのレピュテーション フィルタリング、スパム対策、ウイルス対策、およびウイルス アウトブレイク フィルタの機能（評価フィルタリング（7-1 ページ）、Cisco IronPort スパム対策フィルタリング（9-4 ページ）、Sophos アンチウイルス フィルタリング（8-2 ページ）、およびアウトブレイク フィルタ（10-1 ページ）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（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（5-7 ページ））のために Cisco IronPort アプライアンスを設定できます。

Cisco IronPort 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必ず満たす必要があります。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、Cisco IronPort 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 IronPort Anti-Spam 機能やアウトブレイク 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*のマシンとしてアプライアンスを設定できない場合でも、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（9-21 ページ）を参照してください。

Cisco IronPort 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（『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Using Email Security Monitor」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 トラフィックに対する徹底的な可視性が提供されます。
- 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（『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「LDAP Queries」）では、ディレクトリ インフラストラクチャを統合でき、更新の単純化につながります。
- エイリアス テーブル（『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Creating Alias Tables」）、ドメイン ベースのルーティング（『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「The Domain Map Feature」）、およびマスカレード（『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Masquerading」）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 IronPort 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 IronPort 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場合は、Cisco IronPort アプライアンスが DNS に登録されていることを確認する必要があります。Cisco IronPort 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 IronPort 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 IronPort 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 IronPort アプライアンスを DNS に登録するということは、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 IronPort 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。

インストールのシナリオ

アプライアンスを設置する前に、すべての機能を検討しなければならない場合があります。第 4 章、電子メール パイプラインについてでは、インフラストラクチャへの Cisco IronPort アプライアンスの配置に影響する可能性のある、アプライアンスの全機能の概要を提供しています。

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 IronPort カスタマー サポートにお問い合わせください（Cisco IronPort サポート コミュニティ（1-11 ページ）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 IronPort アプライアンスの一般的な設置方法を示します。

図 3-1　　エンタープライズ ネットワーク環境

いくつかのシナリオでは、Cisco IronPort 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 IronPort 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。

- ファイアウォール内（図 3-2（3-8 ページ）を参照）

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、セットアップの準備（3-9 ページ）に進んでください。

着信（Incoming）

- 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（を参照）。
- 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 IronPort アプライアンスに直接接続し、Cisco IronPort 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。（『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Routing Email for Local Domains」を参照してください）。

発信（Outgoing）

- 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 IronPort アプライアンスにルーティングされます。
- Cisco IronPort 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、リスナーによる電子メールの受信（5-1 ページ）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 IronPort 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、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Using Virtual Gateway™ Technology」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 IronPort X1000/1050/1060/1070、C60/600/650/660/670、および C30/300/350/360/370 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 IronPort C10/100/150/160 E 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 3-2 および図 3-3 に示すこの設定に加え、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 IronPort アプライアンス。
- Cisco IronPort 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 ペアリング機能によって「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

これらの機能については、いずれも『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』を参照してください。

ファイアウォール設定値（NAT、ポート）

ネットワークの設定によっては、次のポートでアクセスを許可するように、ファイアウォールを設定することが必要になる場合があります。

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できる必要があります。他のシステム機能では、次のサービスが必要な場合があります。

表 3-1　ファイアウォール ポート

• SMTP：ポート 25 • DNS：ポート 53 • HTTP：ポート 80 • HTTPS：ポート 443 • SSH：ポート 22 • Telnet：ポート 23	• LDAP：ポート 389 または 3268 • NTP：ポート 123 • LDAP over SSL：ポート 636 • グローバル カタログ クエリー用の SSL を使用した LDAP：ポート 3269 • FTP：ポート 21、データ ポート TCP 1024 以上 • Cisco IronPort スパム検疫：ポート 6025

Cisco IronPort アプライアンスを適切に運用するために開けなければならない可能性のあるポートに関するすべての情報については、付録 C、ファイアウォール情報を参照してください。たとえば、次の接続のためにファイアウォールでポートを開けなければならない場合があります。

- 外部クライアント（MTA）からの Cisco IronPort アプライアンスに対する接続
- グループウェア サーバとの間の接続
- インターネット ルート DNS サーバまたは内部 DNS サーバへの接続
- Cisco IronPort ダウンロード サーバへの接続（McAfee および Sophos Anti-Virus のアップデート、感染フィルタ ルール、および AsyncOS のアップデートのため）
- NTP サーバへの接続
- LDAP サーバへの接続

サポート言語

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（中国と台湾）
- ロシア語

物理寸法

Cisco IronPort X1050/1060、C650/660 および **C350/360** E メール セキュリティ アプライアンスには、次の物理寸法が適用されます。

- 高さ：8.656 cm（3.40 インチ）
- 幅：レールを取り付けて 48.26 cm（19.0 インチ）（レールを取り付けない場合は 17.5 インチ）
- 奥行：75.68 cm（29.79 インチ）
- 重量：最大 26.76 kg（59 ポンド）

Cisco IronPort X1070、C670 および C370 E メール セキュリティ アプライアンスには、次の物理寸法が適用されます。

- 高さ：8.64 cm（3.40 インチ）
- 幅：レールの取り付け有無によらず 48.24 cm（18.99 インチ）
- 奥行：72.06 cm（28.40 インチ）
- 重量：最大 23.59 kg（52 ポンド）

Cisco IronPort C150 および C160 E メール セキュリティ アプライアンスには、次の物理寸法が適用されます。

- 高さ：4.2 cm（1.68 インチ）
- 幅：レールを取り付けて 48.26 cm（19.0 インチ）（レールを取り付けない場合は 17.5 インチ）
- 奥行：57.6 cm（22.7 インチ）
- 重量：最大 11.8 kg（26 ポンド）

ネットワークへの Cisco IronPort アプライアンスの物理的な接続

設定シナリオ

Cisco IronPort 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。

- **インターフェイス**：大部分のネットワーク環境では、Cisco IronPort 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。
  - 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。
  - 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 IronPort 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 IronPort 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。

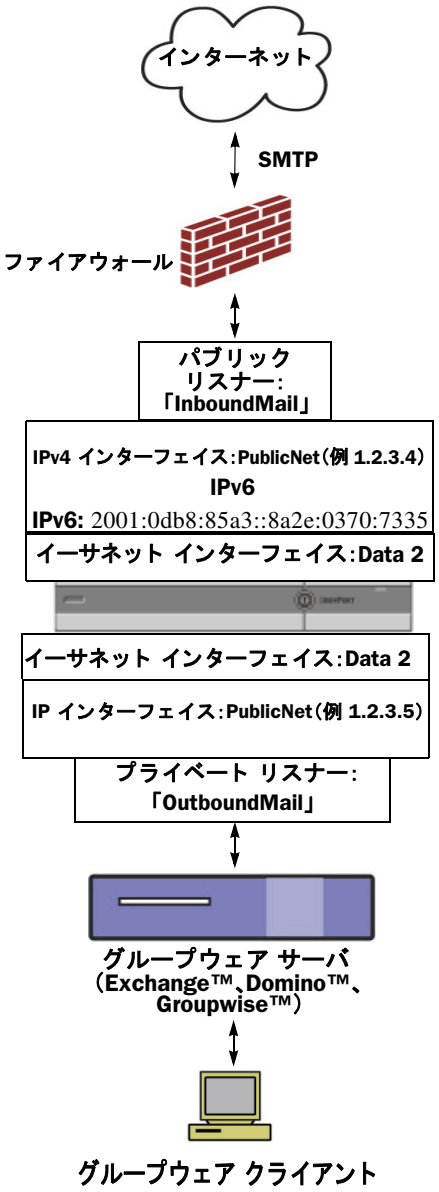
着信メールと発信メールの分離

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設定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（3-12 ページ）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 3-2　　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)

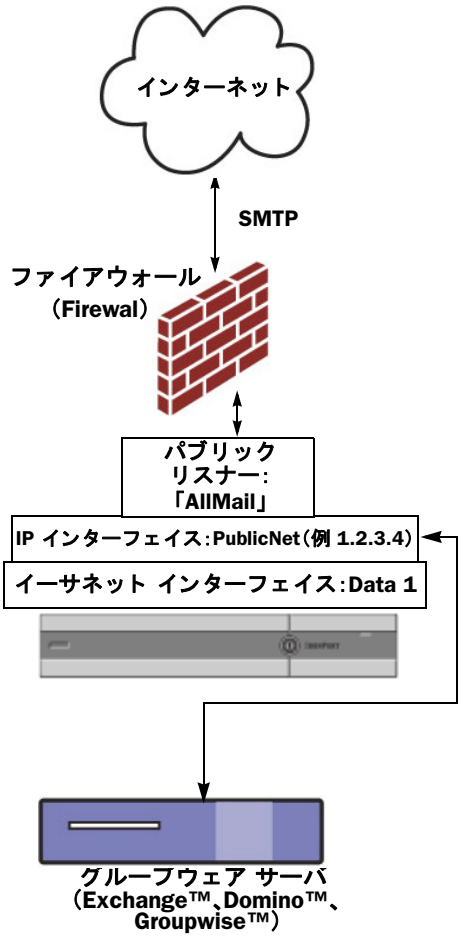
- IP address: 1.2.3.5
- IPv6 アドレス:
  2001:0db8:85a3::8a2e:0370:7335
- Data 2 インターフェイスのリスナーで ポート 25 をリッスン
- HAT(ローカル ドメイン宛てをリレー、その他すべてを拒否)

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 IronPort 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 3-3　　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 address: 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 IronPort 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

セットアップの準備

ステップ 1　アプライアンスへの接続方法を決定します。

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。IPv4 アドレスと IPv6 アドレスの両方を使用できます。

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。

ステップ 4　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（3-28 ページ）で説明されているコマンドライン インターフェイス（CLI）を使用することもできます）。

ステップ 5　システム セットアップ ウィザードを実行してシステムを設定します。

アプライアンスへの接続方式の決定

Cisco IronPort 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 IronPort 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 3-2　　アプライアンスに接続するオプション

Ethernet	PC とネットワークの間およびネットワークと Cisco IronPort 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 IronPort 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アクセス（A-7 ページ）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。 **ビット/秒**：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、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Adding Users」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

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 IronPort 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。

E 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を受け入れます。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 IronPort 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 IronPort 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は、Cisco IronPort 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 C、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 IronPort M-Series アプライアンスを設定する場合は、第 17 章、Cisco IronPort M-Series セキュリティ管理アプライアンスを参照してください。

表 3-3　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（Enable/Disable）	
オートサポート:（AutoSupport:）	イネーブル/ディセーブル（Enable/Disable）	
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）		
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）]**	**Destination**
外部への送信メールを中継:（Relay Outgoing Mail:）	**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）]**	**Destination**
外部への送信メールを中継:（Relay Outgoing Mail:）	**System**	

表 3-3　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（続き）

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）]**	**Destination**
外部への送信メールを中継:（Relay Outgoing Mail:）	**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 3-4　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:）	
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（Enable/Disable）
オートサポート:（AutoSupport:）	イネーブル/ディセーブル（Enable/Disable）
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:）	

表 3-4　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）

受信メールの受け入れ:（Accept Incoming Mail:）	[ドメイン（Domain）]	**Destination**
外部への送信メールを中継:（Relay Outgoing Mail:）	**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 ウィザードの使用方法

Cisco IronPort AsyncOS オペレーティング システムには、システム コンフィギュレーションの 5 つの手順を実行するための、ブラウザベースの System Setup Wizard が用意されています。コマンドライン インターフェイス（CLI）バージョンの System Setup Wizard も含まれています。詳細については、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（3-28 ページ）を参照してください。System Setup Wizard では使用できないカスタム コンフィギュレーション オプションを利用するユーザもいます。ただし、初期セットアップでは System Setup Wizard 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。セットアップの準備（3-9 ページ）で必要な情報を収集済みであれば、コンフィギュレーション プロセスを完了するための時間はわずかです。

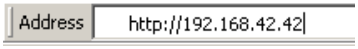
警告　システム セットアップ ウィザードでは、システムを完全に再設定します。システム セットアップ ウィザードは、アプライアンスをまったく初めて設置する場合か、既存の設定を上書きする場合に限り使用してください。

警告　C650/660/670、C350/360/370、および X1050/1060/1070 システムの Management ポートおよび C150/160 システムの Data 1 ポートの出荷時設定による Cisco IronPort アプライアンスのデフォルト IP アドレスは、`192.168.42.42` です。Cisco IronPort 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 IronPort M-Series アプライアンスを設定する場合は、Cisco IronPort M-Series セキュリティ管理アプライアンス（17-1 ページ）を参照してください。

複数の工場出荷時の設定を持つ Cisco IronPort アプライアンスをネットワークに接続する場合は、1 つずつ追加して、各 Cisco IronPort 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。

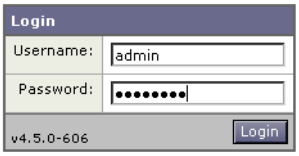
Web ベースのグラフィカル ユーザ インターフェイス（GUI）の利用

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 3-4　アプライアンスへのログイン



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求められます。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 System Setup Wizard の実行

System Setup Wizard を起動するには、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（3-15 ページ）の説明に従って、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。[System Administration] タブで、左方のリンク リストから [System Setup Wizard] をクリックします。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。

System Setup Wizard では、5 つのカテゴリに分割された、次のコンフィギュレーション タスクが順に示されます。

ステップ 1　開始

- ライセンス契約書の参照と受諾

ステップ 2　システム

- アプライアンスのホスト名の設定
- アラート、レポート配信、および AutoSupport の設定

- システム時刻と 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 3　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 4　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
- スパム対策サービスのイネーブル化
- Cisco IronPort スパム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 5　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

各手順を完了して [次へ（Next）] をクリックしながら、System Setup Wizard を進めてください。[前へ（Previous）] をクリックすると、前の手順に戻ることができます。プロセスの最後に、変更を確定するようプロンプトが表示されます。確定するまで、変更は有効になりません。[次へ（Next）] をクリックしたときに必須フィールドをブランクにした場合（または正しくない情報を入力した場合）は、そのフィールドの外枠が赤で表示されます。修正し、もう一度 [次へ（Next）] をクリックしてください。

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。

図 3-5　System Setup Wizard：手順 1：Start

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 IronPort 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 IronPort 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（15-15 ページ）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。この値をブランクにしても、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 IronPort 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（15-49 ページ）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 IronPort 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 IronPort 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 IronPort 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 IronPort 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（13-2 ページ）を参照）。

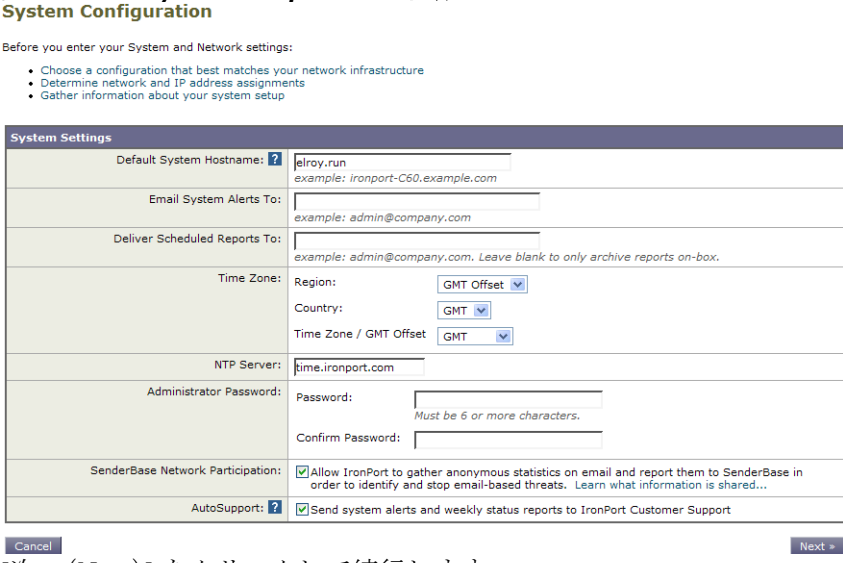
SenderBase ネットワークに参加する場合は、[メールをベースとする脅威の特定、排除を目的として、IronPort がメールの匿名統計を収集および SenderBase に対しレポートすることを許可（Allow IronPort to gather anonymous statistics on email and report them to SenderBase in order to identify and stop email-based threats）] の横のボックスをオンにし、[承認（Accept）] をクリックします。

詳細については、第 13 章、SenderBase Network Participation を参照してください。

AutoSupport のイネーブル化

Cisco IronPort AutoSupport 機能（デフォルトでイネーブル）では、ご使用の Cisco IronPort アプライアンスに関する問題を Cisco IronPort 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 IronPort AutoSupport（15-17 ページ）を参照してください）。

図 3-6　System Setup Wizard：手順 2：システム



[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）を設定します。Cisco IronPort 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（15-40 ページ）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 サーバを利用できる必要があります。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動中の 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 IronPort 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、C650/660/670、C350/360/370、および X1050/1060/1070 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。C150/160 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。C150 アプライアンスおよび C160 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。

C650/660/670、C350/360/370、および X1050/1060/1070 をご利用のお客様：シスコでは、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。

C150/160 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、System Setup Wizard 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（3-11 ページ）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 形式のネットマスク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（詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Routing Email for Local Domains」を参照してください）。

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、受信者の定義（5-55 ページ）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（5-21 ページ）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、X1050/1060/1070、C650/660/670、および C350/360/370 アプライアンスに該当します。C150/160 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（C150/160 の設置（3-22 ページ）を参照）。

図 3-7　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）

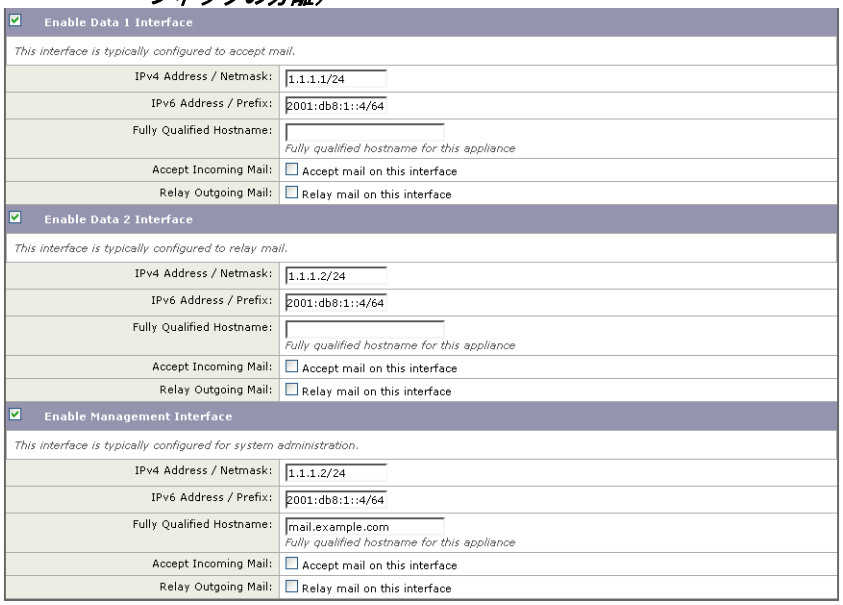


図 3-2（3-8 ページ）のようなネットワークを構築する場合に、この設定を使用します。

C150/160 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 3-8　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

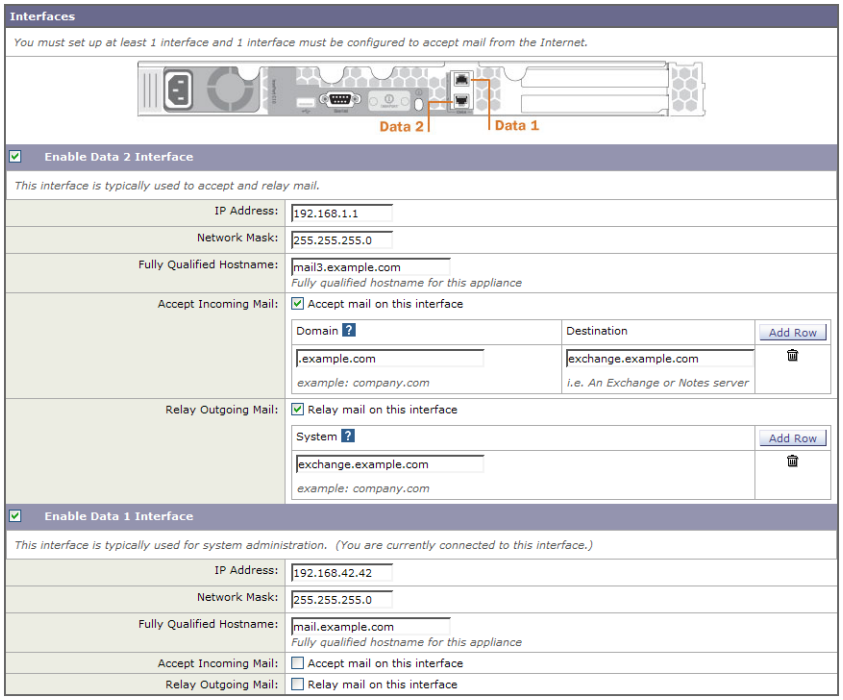


図 3-3（3-9 ページ）のようなネットワークを構築する場合に、この設定を使用します。

[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 IronPort 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 IronPort アプライアンスには、Cisco IronPort 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 IronPort 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。スパム対策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 IronPort スパム隔離エリアに送信するように、AsyncOS を設定できます。Cisco IronPort スパム隔離は、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うちは、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 IronPort Anti-Spam 設定オプションについては、第 9 章、アンチスパム を参照してください。Cisco IronPort スパム隔離の詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Quarantines」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 IronPort 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、アプライアンスでウイルス対策スキャン 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。

ウイルス対策スキャン 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 IronPort 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。

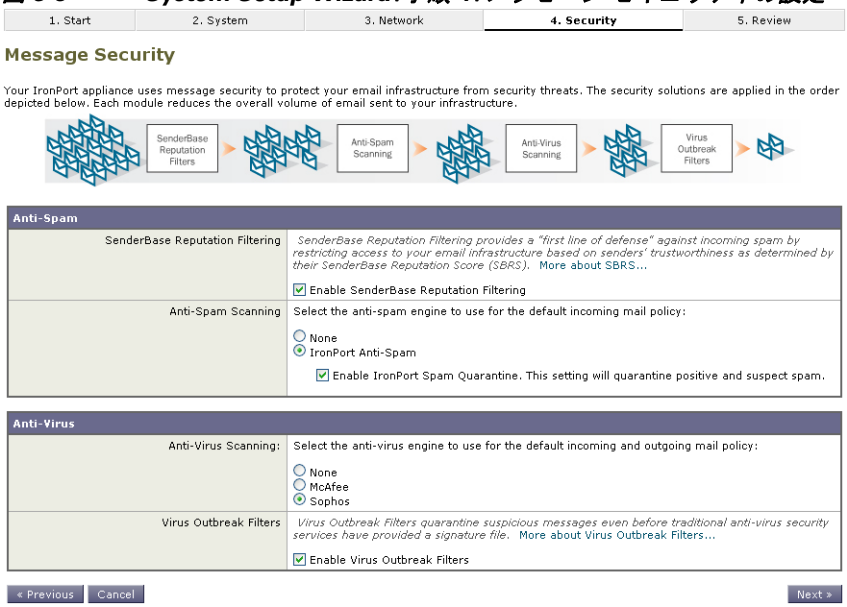
アプライアンスで使用可能なすべてのウイルス対策設定オプションについては、第 8 章、アンチウイルスを参照してください。

アウトブレイク フィルタのイネーブル化

Cisco IronPort 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、従来のウイルス対策セキュリティ 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 10 章、アウトブレイク フィルタを参照してください。

図 3-9　System Setup Wizard：手順 4：メッセージ セキュリティの設定

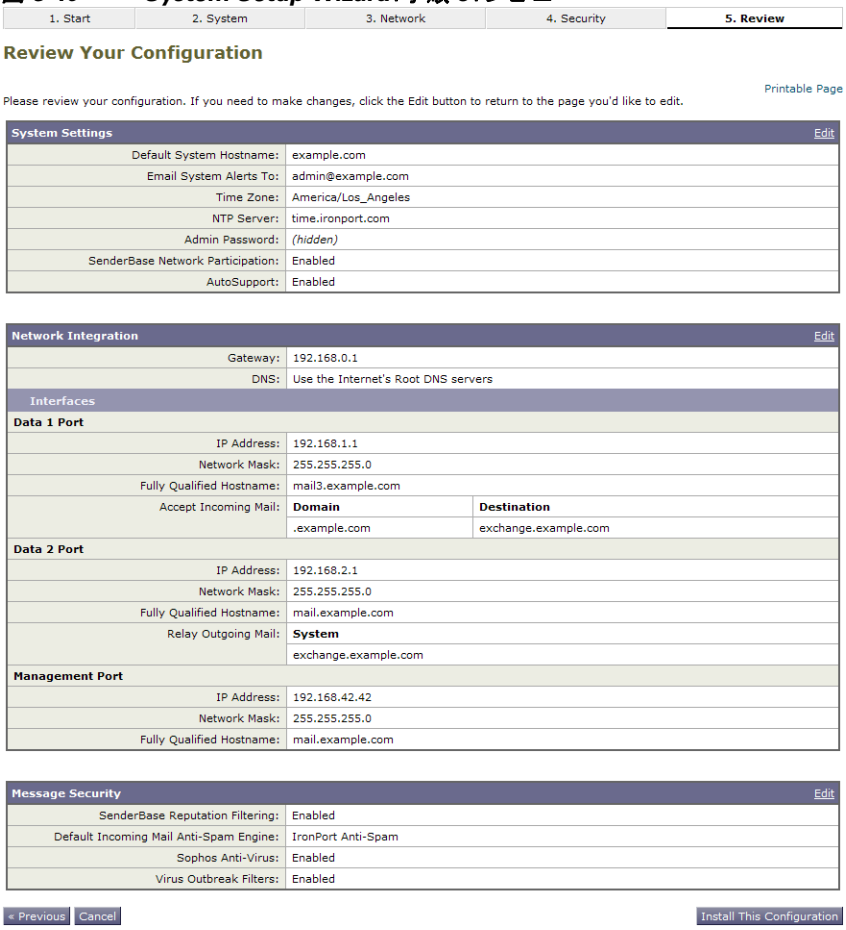


[次へ（Next）] をクリックして続行します。

手順 5：レビュー

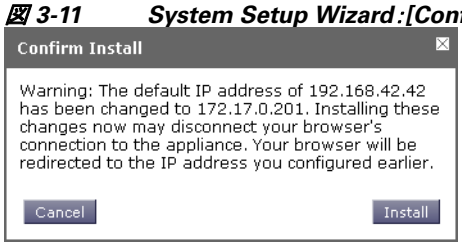
設定情報のサマリーが表示されます。[システム設定（System Settings）]、[ネットワークインテグレーション（Network Integration）]、および [メッセージセキュリティ（Message Security）] の情報は、[前へ（Previous）] ボタンをクリックするか、各セクションの右上にある対応する [編集（Edit）] リンクをクリックすることによって編集できます。変更を加える手順まで戻った場合は、再度このレビュー ページに至るまで、残りの手順を進める必要があります。以前に入力した設定は、すべて残っています。

図 3-10　System Setup Wizard：手順 5：レビュー



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。

図 3-11　System Setup Wizard：[Confirm Install]



これで、Cisco IronPort 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（X1050/1060/1070、C650/660/670、および C350/360/370 システムの Management インターフェイスまたは C150/160 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（3-41 ページ）を参照してください。

Active Directory の設定

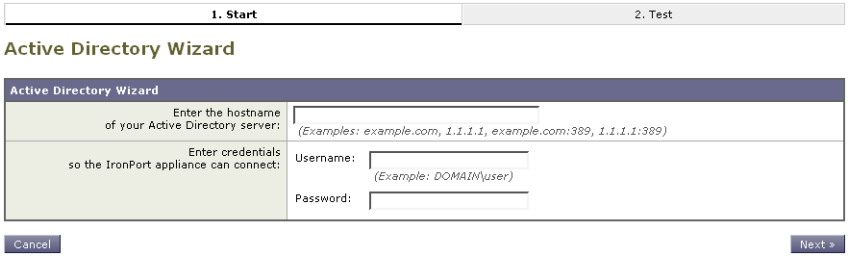
システム セットアップ ウィザードによって E メール セキュリティ アプライアンスに設定が正しくインストールされると、Active Directory Wizard が表示されます。ネットワークで Active Directory サーバを稼動している場合は、Active Directory Wizard を使用して、Active Directory サーバ用の LDAP サーバ プロファイルの設定と、受信者検証用リスナーの割り当てを行う必要があります。Active Directory を使用していないか、後で設定する場合は、[このステップをスキップ（Skip this Step）] をクリ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

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。

図 3-12　Active Directory Wizard：手順 1：Start



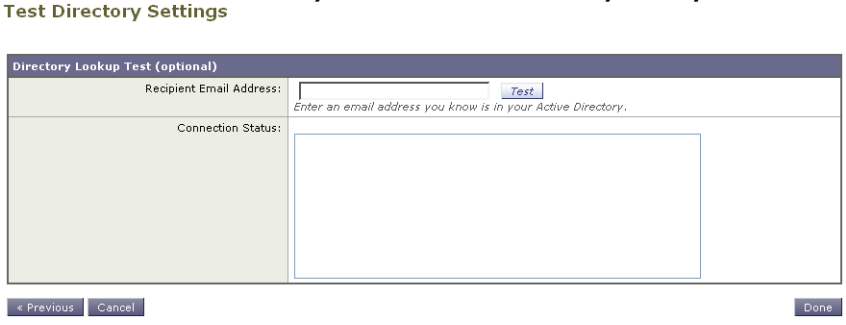
ステップ 2　Active Directory サーバのホスト名を入力します。

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。

図 3-13　Active Directory Wizard：手順 2：[Directory Lookup Test]



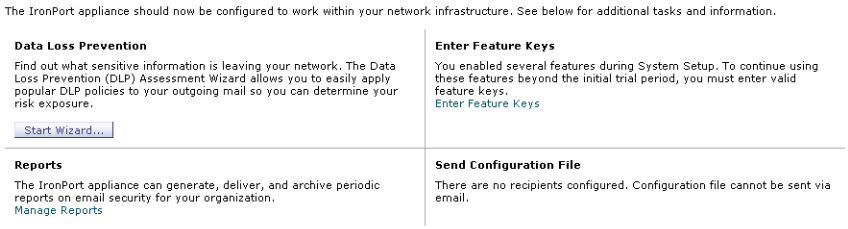
ステップ 5　Active Directory に存在すると判明している電子メール アドレスを入力し、[テスト（Test）] をクリックすることによって、ディレクトリ設定値をテストします。結果が [接続ステータス（Connection Status）] フィールドに表示されます。

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。

図 3-14　　システム セットアップの完了



[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 IronPort 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（3-10 ページ）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（ユーザの追加に関する詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Common Administrative Tasks」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（3-10 ページ）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**

次に例を示します。

```
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、グローバルなウイルス対策セキュリティとアウトブレイク フィルタ セキュリティ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、次の質問に「はい（Y）」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 System Setup Wizard の実行（3-15 ページ）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 ライセンス契約書を参照して受諾します。

ホスト名の設定

次に、Cisco IronPort 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。

X1050/1060/1070、C650/660/670、および C350/360/370 をご利用のお客様: シスコでは、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。

C150/160 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 アドレスの設定の詳細については、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、独自の証明書をアップロードするまで、デモ証明書が使用されます。詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Enabling a Certificate for HTTPS」を参照してください。

DNS 設定値の設定

次に、Domain Name Service（DNS）を設定します。Cisco IronPort 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、着信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 IronPort 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 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、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）。

X1050/1060/1070、C650/660/670、および C350/360/370 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(5-1 ページ)を参照してください)。

C150/160 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(3-35 ページ)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。詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Routing Email for Local Domains」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、[コンサーバティブ(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)、あるい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(5-21 ページ)およびパブリック リスナー(RAT)上でのローカル ドメインまたは特定のユーザの電子メールの受け入れ(5-54 ページ)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、X1050/1060/1070、C650/660/670、および C350/360/370 をご利用のお客様だけに適用されます。Cisco IronPortC150/160 をご利用のお客様は、次の項 C10/100/150/160 のリスナーの例(3-35 ページ)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が、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 IronPort 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、企業への着信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（5-21 ページ）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"):

[]> 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、パブリック リスナーとプライベート リスナー（5-4 ページ）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 addressed 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、C150/160 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が、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 IronPort 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、企業への着信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（5-21 ページ）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"):

[]> 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。詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Using the Email Security Monitor」を参照してください。

Cisco IronPort アンチスパムのイネーブル化

Cisco IronPort アプライアンスには、Cisco IronPort 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。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 IronPort Anti-Spam をイネーブルにすることができます。

Cisco IronPort 次に、着信メール ポリシーに対する 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 IronPort 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 IronPort Anti-Spam 設定オプションについては、第 9 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 IronPort スパム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 IronPort スパム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 IronPort スパム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。

Cisco IronPort スパム隔離の詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Quarantines」を参照してください。

ウイルス対策スキャンのイネーブル化

Cisco IronPort 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、アプライアンスでウイルス対策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ウイルス対策スキャン エンジンごとにライセンス契約書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 IronPort 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ウイルス対策設定オプションについては、第 8 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 IronPort 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、従来のウイルス対策セキュリティ 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（10-1 ページ）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 IronPort 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 13 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 IronPort AsyncOS 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、後でアラート設定を詳細化できます。詳細については、アラート（15-15 ページ）を参照してください。

Cisco IronPort AutoSupport 機能では、ご使用の Cisco IronPort アプライアンスに関する問題を Cisco IronPort 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。サポート アラートと週ごとのステータス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 IronPort AutoSupport（15-17 ページ）を参照してください）。

スケジュール済みレポートの設定

デフォルトの定期レポートの送信先にするアドレスを入力します。この値はブランクにすることができ、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 IronPort 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 IronPort 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 IronPort Systems タイム サーバを使用して Cisco IronPort 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 IronPort 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 IronPort 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設定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 IronPort 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 IronPort 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、あるいはアウトブレイク 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（3-17 ページ）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。次に例を示します。

```
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 IronPort 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、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Common Administrative Tasks」にある機能キーの使用に関する項を参照してください）。

次の手順：電子メール パイプラインの理解

systemsetup が完了したため、Cisco IronPort 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。ウイルス対策、スパム対策、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 パイプラインについてでは、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 パイプラインについて

電子メール パイプラインは、Cisco IronPort アプライアンスによる処理に伴う、電子メールのプロセスまたはフローです。Cisco IronPort アプライアンスから最高のパフォーマンスを引き出すには、電子メール パイプラインを理解することが不可欠です。

この章では、受信メールの電子メール パイプラインの概要と各機能の簡単な説明を示します。簡単な説明には、機能の詳細な説明が記載された章または書籍へのリンクも含まれています。

概要:電子メール パイプライン

表 4-1 および表 4-2 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。各機能は上から順に実行されます。ここでは簡単に説明します。各機能の詳細については、次の章を参照してください。一部の機能は『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』と『*Cisco IronPort AsyncOS for Email Daily Management Guide*』で説明します。

表 4-2 の陰付きの部分は、ワーク キュー内で発生する処理を表します(ワーク キューとルーティング(4-7 ページ)を参照)。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、Debugging Mail Flow Using Test Messages: Trace (-446 ページ)を参照してください。

表 4-1　Cisco IronPort 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（Host DNS Sender Verification）	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（Envelope Sender Verification）	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（Sender Verification Exception Table）	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（Mail Flow Policies）	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（Received Header）	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（Domain Map）	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（Alias tables）	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（LDAP Recipient Acceptance）	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。
SMTP コールアヘッド受信者検証	SMTP コールアヘッド受信者検証は、SMTP カンバセーションで行われます。E メール セキュリティ アプライアンスが外部 SMTP サーバをコールアヘッドする間、SMTP カンバセーションは一時停止します。SMTP サーバの応答に応じて、メッセージがドロップまたはバウンスされるか、メール送信アクションが許可されます。

表 4-2　Cisco IronPort 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 カンバセーション 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（Message Filters）*		メッセージ フィルタはメッセージの「分裂」よりも前に適用されます。* メッセージを隔離エリアに送信できます。
	セーフリスト/ブロックリスト スキャン		AsyncOS では、送信者アドレスをエンドユーザ セーフリスト/ブロックリスト データベースと照合します。送信者アドレスがセーフリストに登録されている場合、アンチスパム スキャンがスキップされます。受信者が複数の場合は、メッセージを分裂できます。* 送信者がブロックリストに登録されている場合は、メッセージを隔離エリアに送信できます。
	アンチスパム**	電子メール セキュリティ マネージャ スキャン（受信者 1 人あたり）	アンチスパム スキャン エンジンでは、メッセージを検査して、さらに処理するために判定を返します。
	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。適切なコンテンツ フィルタ条件が定義されている場合は、DKIM、SPF、および SIDF 検証が実行されます。* 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、新しい詐欺、フィッシング、およびマルウェア攻撃から保護できます。* メッセージを隔離エリアに送信できます。
	データ漏洩防止（発信メッセージのみ）		RSA メールデータ漏洩防止機能により、発信メッセージに機密データが含まれているかどうかが検査されます。RSA メール DLP は、発信メッセージ専用です。* メッセージを隔離エリアに送信できます。

表 4-2　Cisco IronPort 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

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（Delivery limits）	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（Domain-based Limits）	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（Domain-based routing）	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（Global unsubscribe）	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（Bounce profiles）	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。

** メッセージを Cisco IronPort スパム隔離に送信できます。

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 IronPort 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、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（5-7 ページ）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」の章にある「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」の章にある「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」の章にある「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 IronPort 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、パブリック リスナー（RAT）上でのローカル ドメインまたは特定のユーザの電子メールの受け入れ（5-54 ページ）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ープ受信者（Envelope To または RCPT TO とも呼ぶ）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ー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」の章にある「Accept Queries」を参照してください。これにより、Cisco IronPort 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 コールアヘッド受信者検証

E メール セキュリティ アプライアンスで SMTP コールアヘッド受信者検証を設定すると、E 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 IronPort 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 E メール セキュリティ アプライアンスに返されます。E 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 コールアヘッド 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）　データ漏洩防止（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（6-5 ページ）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」の章にある「Accept Queries」を参照してください。これにより、Cisco IronPort 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、管理者が作成するテーブルに従って、プライベート リスナーで処理される電子メールのエンベロープ送信者（Sender または MAIL FROM とも呼ぶ）と 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「ConfiguringMasquerading」を参照してください。

LDAP 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 IronPort 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。

Anti-Spam

スパム対策機能は、Cisco IronPort 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、ネットワークが蹂躙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 IronPort 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 IronPort スパム隔離からリリース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 9 章、アンチスパム を参照してください。

アンチウイルス

Cisco IronPort 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
- 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（4-10 ページ）を参照）から解放されると、ウイルスがスキャンされます。アンチウイルス スキャンの詳細については、第 8 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（6-8 ページ）を参照してください。

アウトブレイク フィルタ

Cisco IronPort シスコのアウトブレイク 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 IronPort 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。

Outbreak 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（4-10 ページ）を参照してください。

詳細については、第 10 章、アウトブレイク フィルタを参照してください。

隔離

Cisco IronPort 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 IronPort Virtual Gateway テクノロジーを使用すると、Cisco IronPort 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、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」の章にある「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」の章にある「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」の章にある「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」の章にある「Routing Email for Local Domains」を参照してください。

グローバル登録解除

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 IronPort 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*』「Configuring Routing and Delivery Features」の章にある「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バセーションのハード バウンスおよびソフト バウンスを Cisco IronPort 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 Routingand Delivery Features」の章にある「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

GUI のシステムセットアップ ウィザード（または CLI `systemsetup` コマンド）を使用して Cisco IronPort アプライアンスの基本設定を構成したら、Cisco IronPort E メール セキュリティ アプライアンスの設定を調整して電子メールを受信する準備が整っています。この章では、電子メールの受信を処理するためにアプライアンス上でリスナーを設定する際に使用できるすべての機能について詳しく説明します。

ホスト アクセス テーブル（HAT）の概念が導入されました。パブリック リスナーのホスト アクセス テーブル（HAT）と、その固有の送信者グループおよびメール フロー ポリシーは、メール フロー モニタ機能を可能にするための基礎となるフレームワークです（『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Using Email Security Monitor」では、メール フロー モニタ機能について詳しく説明します）。

リスナーによる電子メールの受信

Cisco IronPort AsyncOS オペレーティング システムを使用すると、Cisco IronPort アプライアンスは企業のインバウンド電子メールのゲートウェイとして機能することが可能になり、インターネットからの SMTP 接続の処理、メッセージの許可、および適切なシステムへのメッセージの中継を行うことができます。

この設定では、*リスナー*がこれらの接続を提供できるようにします。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、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 IronPort アプライアンスに入る電子メールだけに適用されます。Cisco 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（`systemsetup` コマンドで設定した初期アドレスを含みます）用に特定のポート上で動作する「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。

1 つの IP アドレス上の複数のポートにメールが配信されるようにメール配信ポリシーを設定することはできません（たとえば、通常の配信の場合はポート 25 へ、Cisco IronPort スパム隔離の場合はポート 6025 へなど）。各配信オプションを個別の IP アドレスまたはホスト上で実行することが推奨されます。さらに、通常の電子メール配信用と検疫配信用には同じホスト名を使用できません。

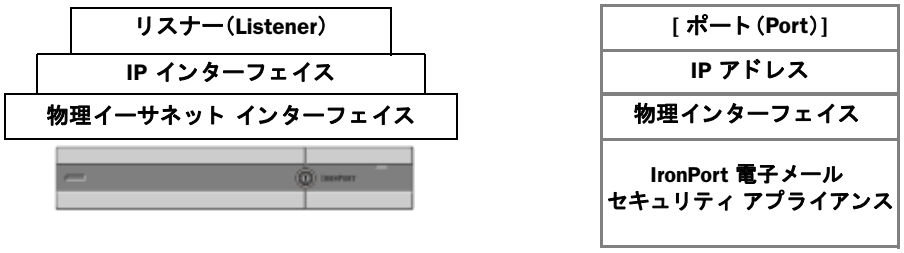
リスナーは、インターネット プロトコル バージョン 4（IPv4）およびバージョン 6（IPv6）アドレスの両方をサポートします。単一のリスナーでどちらかのプロトコル バージョンまたは両方を使用できます。リスナーは、接続ホストとしてメール配信に同じプロトコル バージョンを使用します。たとえば、リスナーが IPv4 と IPv6 の両方に設定され、IPv6 を使用してホストに接続する場合、リスナーは IPv6 を使用します。ただし、リスナーが IPv6 アドレスのみの使用を設定されている場合は、IPv4 アドレスのみを使用するホストに接続できません。

システム セットアップ ウィザードまたは `systemsetup` コマンド（CLI）は、Cisco IronPort アプライアンス上で使用可能な*イーサネット インターフェイス*上で実行する *IP インターフェイス*を最初に設定します。Cisco IronPort C150 および C160 アプライアンスでは、これらのイーサネット インターフェイスに Data1 および Data2 というラベルが付いています。その他のすべてのCisco IronPortData1、Data2、および管理という、アプライアンス、します。これらのインターフェイスは、後で [ネットワーク（Network）] メニューの [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編集できます。GUI のシステム セットアップ ウィザード（または `systemsetup` コマンド）を完了し、変更内容を確定した場合、すでに少なくとも 1 つのリスナーがアプライアンス上で構成されています。（手順 3: ネットワーク (3-18 ページ)で入力した設定を参照してください）。メールを受信するための特定のアドレスは、その時点と、最初の SMTP ルート（[ネットワーク（Network）] > [SMTP ルート（SMTP Routes）] または `smtproutes`）の入力時に入力します。

（注）　System Setup Wizard を使用して新しいリスナーを作成するとき、AsyncOS はデフォルト値でリスナーを作成します。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。

[リスナー（Listeners）] ページ（[ネットワーク（Network）] > [リスナー（Listeners）]）または `listenerconfig` コマンドを使用して、Cisco IronPort アプライアンス上の使用可能な IP インターフェイス上で実行されるリスナーを設定します。リスナーの作成と設定の詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Customizing Listeners」の章を参照してください。『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Using Virtual Gateway™ Technology」では、Cisco IronPort Virtual Gateway テクノロジーについて説明しています。このテクノロジーを使用すると、1 つ以上の IP アドレス（IP アドレス グループ）に対して IP インターフェイスをさらに定義してグループ化できます。

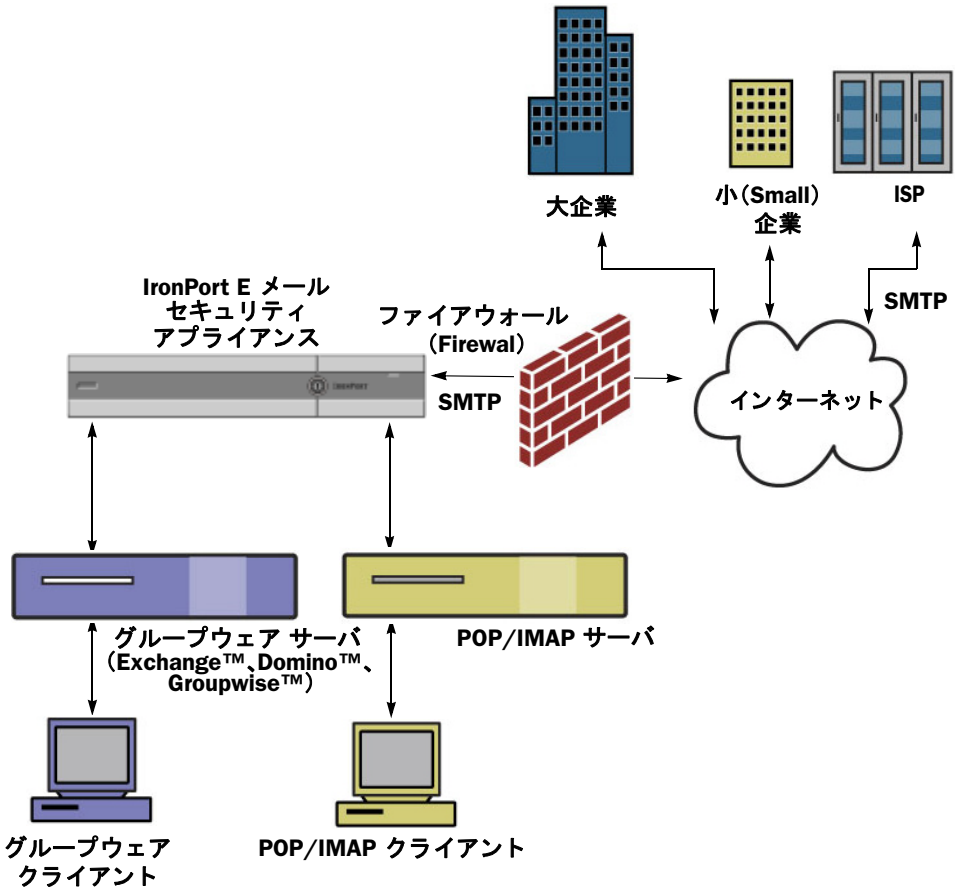
図 5-1　リスナー、IP インターフェイス、物理イーサネット インターフェイスの関係



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 5-2　エンタープライズ ゲートウェイとして Cisco IronPort アプライアンスを使用する



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

パブリック リスナーとプライベート リスナー

最初のリスナーを「パブリック」リスナー、2 番目のリスナーを「プライベート」リスナーと考えます。Cisco 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。パブリック リスナーとプライベート リスナーは、デフォルトでは使用できる機能とデフォルト設定が異なります。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、レポーティング、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、設定されたスパム対策エンジンおよびウイルス対策スキャン 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。リスナーがある同じ図を図 3-3 に示します。

図 5-3　エンタープライズ ゲートウェイのパブリック リスナーとプライベート リスナー

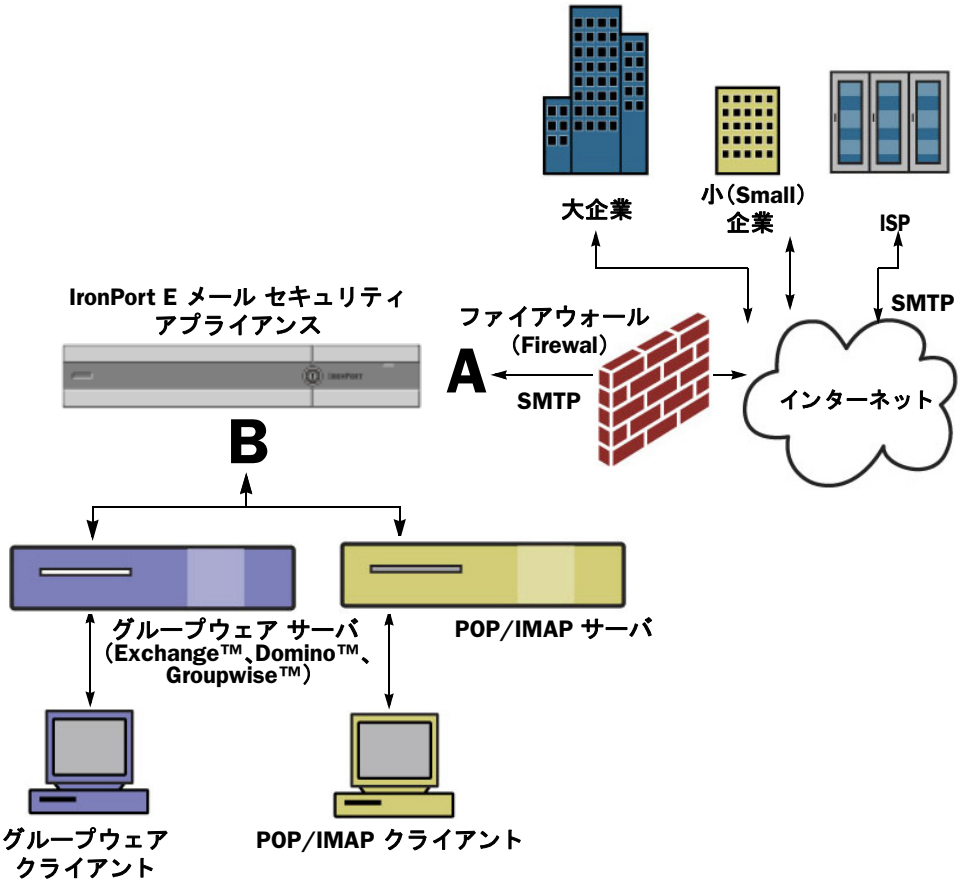


図 3-3 は、このエンタープライズ ゲートウェイ構成のアプライアンスで設定されたパブリック リスナー（A）1 つとプライベート リスナー（B）1 つを示しています。

さらに図 3-4 は、パブリック リスナーとプライベート リスナーのデフォルト設定の違いを示しています。パブリック リスナーは、インターネットからの電子メールを受信することを意図しています。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。これとは逆に、プライベート リスナーは、内部ネットワークからの電子メールを受信することを意図しています。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。

C10/100 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。

この章の後半では、これらの相違点を、各タイプのリスナーごとにホスト アクセス テーブルと受信者アクセス テーブルに示します。

図 5-4　　パブリック リスナーとプライベート リスナー

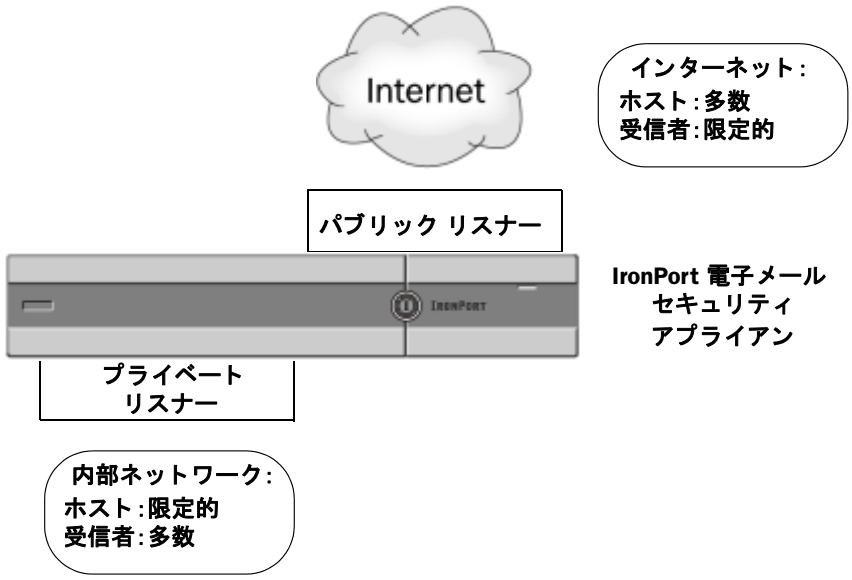
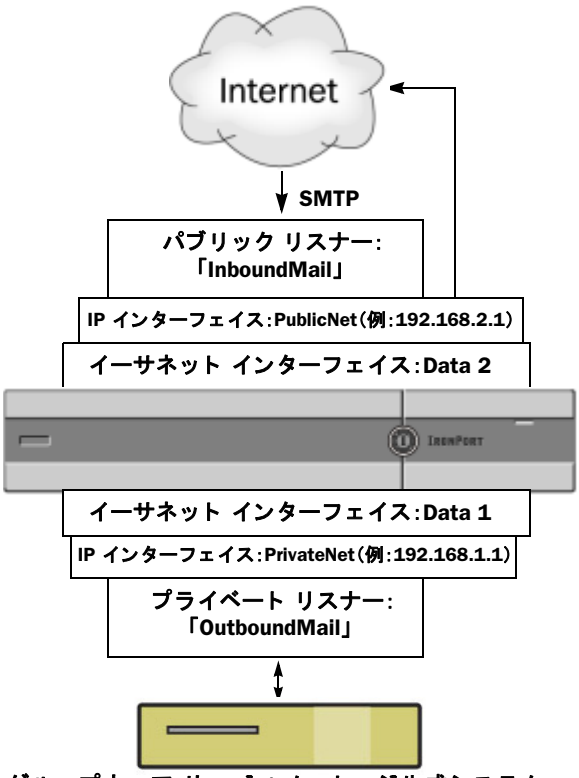


図 5-5 に、Cisco IronPort X1050/1060/1070、C650/660/670、および C350/360/370 アプライアンス上で System Setup Wizard（または CLI の `systemsetup` コマンド）によって作成される一般的な電子メール ゲートウェイ構成を示します。2 つのリスナーが作成されます。あるインターフェイス上でインバウンド接続を使用可能にするためのパブリック リスナーと、別の IP インターフェイス上でアウトバウンド接続を使用可能にするためのプライベート リスナーです。

図 5-6 に、Cisco IronPort C150/160 アプライアンス上で System Setup Wizard（または CLI の `systemsetup` コマンド）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 5-5　X1050/1060/1070、C650/660/670、C350/360/370 アプライアンス上のパブリック リスナーおよびプライベート リスナー

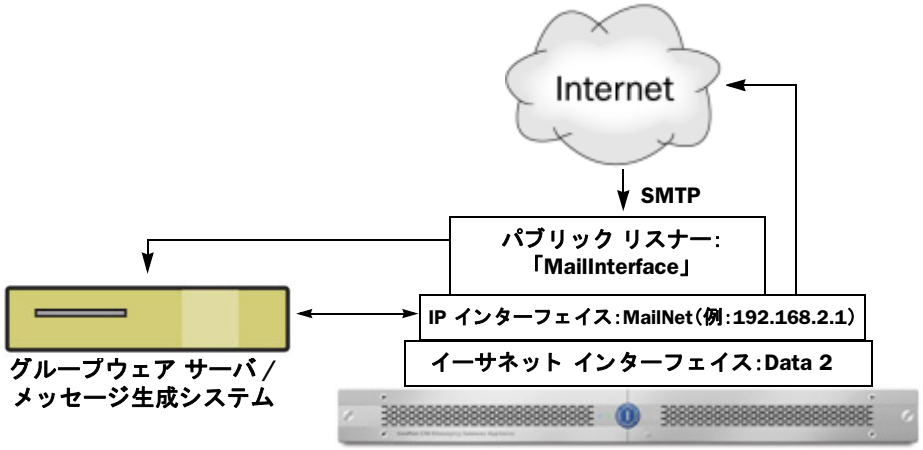


（注） このパブリック リスナーは、イーサネット インターフェイス Data2 上の IP インターフェイス PublicNet のポート 25 上で SMTP プロトコルを使用し、インターネットからのメッセージを受信します。IP インターフェイス PublicNet は、インターネット

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 5-6　　C150/160 アプライアンス上のパブリック リスナー



**IronPort C10 電子メール
セキュリティ アプライアンス**

（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。

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

アプライアンスに設定されている各リスナーには、受信するメッセージの動作を変更するために設定できるプロパティがあります。概要:電子メール パイプライン(4-1 ページ)で説明したように、リスナーの動作に影響を及ぼす最初の設定可能な機能の 1 つは、ホスト アクセス テーブル(HAT)です。

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。作成するすべてのリスナーに独自の HAT があります。HAT は、パブリック リスナーとプライベート リスナーに対して定義されます。

HAT 内のエントリは次の基本的な構文によって定義されます。

表 5-1　　HAT の基本的な構文

リモート ホストの定義	ルール

*リモート ホスト定義*は、リスナーに定義しようとするリモート ホストを(たとえば単一の IP アドレスで)定義する方法です。

*ルール*は、指定されたリモート ホストがリスナーに接続できるかどうかを定義します。

基本的な構文を拡張して、AsyncOS の HAT は、リモート ホスト定義の名前付きセットを作成する機能をサポートしています。これらは*送信者グループ*と呼ばれます。複数のアクセス ルールとパラメータ セットを組み合わせて名前を付けたものを、*メール フロー ポリシー*と呼びます。この拡張された構文を表 5-2 に示します。

表 5-2　　HAT 詳細構文

送信者グループ: (Sender Group:)	**メール フロー ポリシー:**
リモート ホスト (Remote Host)	**アクセス ルール + パラメータ**
リモート ホスト (Remote Host)	
リモート ホスト (Remote Host)	
...	

HAT 内でのルールの順序は重要な意味を持ちます。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。

HAT に配置された定義済みエントリとカスタム エントリは、最後の「ALL」ホスト エントリの上に入力されます。

デフォルト HAT エントリ

作成するすべてのパブリック リスナーについて、デフォルトでは、*すべてのホストからの電子メールを受け入れるように* HAT が設定されます。作成するすべてのプライベート リスナーについて、デフォルトでは、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* HAT が設定されます。

（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` および `systemsetup` コマンドは、ユーザがシステムをオープン リレーとして意図せずに設定するのを防ぎます。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。

メール フロー ポリシー:アクセス ルールとパラメータ

HAT のメール フロー ポリシーを使用すると、リスナーがリモート ホストからメールを受信する速度を制御または制限できます。また、SMTP カンバセーションの間でやりとりされる SMTP コードと応答も変更できます。

HAT には、リモート ホストからの接続時に動作するための 4 つの基本的なアクセス ルールがあります。

ステップ 1　`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。

ステップ 2　`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 グリーティングを取得します。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、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Customizing Listeners」を参照してください。

ステップ 3　`TCPREFUSE`

TCP レベルで接続は拒否されます。

ステップ 4　`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。

- `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、グラフィカル ユーザ インターフェイス（GUI）で HAT を容易に編集できるようにするために使用します。詳細については、新しい送信者グループの追加（5-33 ページ）を参照してください。

これらの基本的なアクセス コントロール パラメータに加え、作成するリスナーで次のパラメータを使用できます。アクセス ルール（ACCEPT または REJECT）と組み合わされたパラメータは、*メール フロー ポリシー*と呼ばれます。メール フロー ポリシーは、HAT パラメータ（アクセス ルール、その後に接続パラメータ、レート制限パラメータ、カスタム SMTP コードとレスポンス、スパム対策、ウイルス対策、暗号化、認証パラメータが続く）のグループを表現する方法です。

その後メール フロー ポリシーは、リスナーの HAT 内のエントリとして送信者グループにマッピングされます。

表 5-3　HAT 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。
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。

表 5-3　HAT メール フロー ポリシー パラメータ（続き）

パラメータ	説明
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。
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められます（たとえば、220-*hostname* ESMTP）。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。
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。

表 5-3　HAT メール フロー ポリシー パラメータ（続き）

パラメータ	説明
送信者のレート制限	
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。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、アドレス リスト（5-42 ページ）を参照してください。
フロー制御（Flow Control）	
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 IronPort 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 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。[SenderBase を使用（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 Routingand Delivery Features」の章の「HAT Significant Bits Feature」を参照してください。

表 5-3　HAT 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 時間あたりの最大不正受信者数（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 IronPort 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。
時間コードあたりの無効な受信者の最大数（Max. 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。
時間テキストあたりの無効な受信者の最大数（Max. 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。
時間コードあたりの無効な受信者の最大数（Max. 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。
時間テキストあたりの無効な受信者の最大数（Max. 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	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 5-3　HAT 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	
Allow TLS Connections	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）の拒否、推奨、必須を設定します。 [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由でメッセージを送信しようとすると、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。 アドレス リストの作成の詳細については、アドレス リスト（5-42 ページ）を参照してください。
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、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「LDAP Queries」の章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	
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 検証（DKIM Verification）	DKIM 検証をイネーブルにします。
SPF/SIDF 検証	
SPF/SIDF 検証のイネーブル化（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、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』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 互換（SIDF Compatible）] のいずれかを選択します。詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Email Authentication」の章を参照してください。
「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します：（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）。

表 5-3　HAT メール フロー ポリシー パラメータ（続き）

パラメータ	説明
タグなしバウンス	
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（『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「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	
	送信者検証（5-43 ページ）を参照してください。
例外テーブル	
例外テーブルを使用（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（5-46 ページ）を参照してください。

デフォルトでは、これらのパラメータは、アプライアンス上の各リスナーについて、表 5-5 および表 5-6 に示すデフォルト値に設定されます。

（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 IronPort 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 スキャンが無効にされた場合、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。

HAT 変数の構文

表 5-4 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で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 5-4　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 IronPort 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。

表 5-4　HAT 変数の構文（続き）

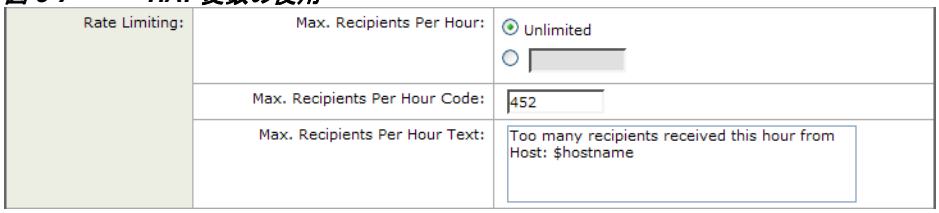
変数	定義
$OrgID	SenderBase 組織 ID（整数値）で置き換えられます。 Cisco IronPort アプライアンスが SenderBase 組織 ID を取得できないか、SenderBase レピュテーション サービスが値を返さなかった場合、「None」が表示されます。
$RemoteIP	リモート クライアントの IP アドレスで置き換えられます。
$HATEntry	リモート クライアントが一致した HAT のエントリで置き換えられます。

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 に示す高度な HAT パラメータ `smtp_banner_text` と `max_rcpts_per_hour_text` と併用できます。

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 5-7　HAT 変数の使用



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 IronPort 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 ESMTP

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.
```

デフォルト メール フロー ポリシーの参照

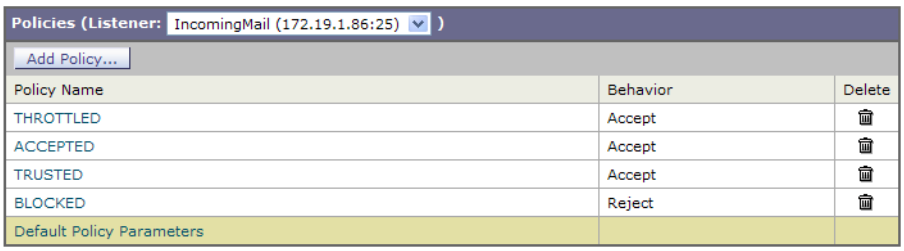
図 5-8 に、パブリック リスナーのデフォルト ポリシー パラメータを示します。

ステップ 1　GUI にアクセスします（GUI へのアクセス（2-2 ページ）を参照）。

ステップ 2　[Mail Policies] > [Mail Flow Policies] の順にクリックします。

[Mail Flow Policies] ページが表示されます。リスナーが設定されている場合、アルファベット順で最初のリスナーに対して定義されているメール フロー ポリシーが表示されます。

図 5-8　[Mail Flow Policies] ページ



ステップ 3　[Default Policy Parameters] リンクをクリックします。

[Default Policy Parameters] ページが表示されます。図 5-9 を参照してください。

図 5-9　　パブリック リスナーのデフォルト ポリシー パラメータ(1/2)

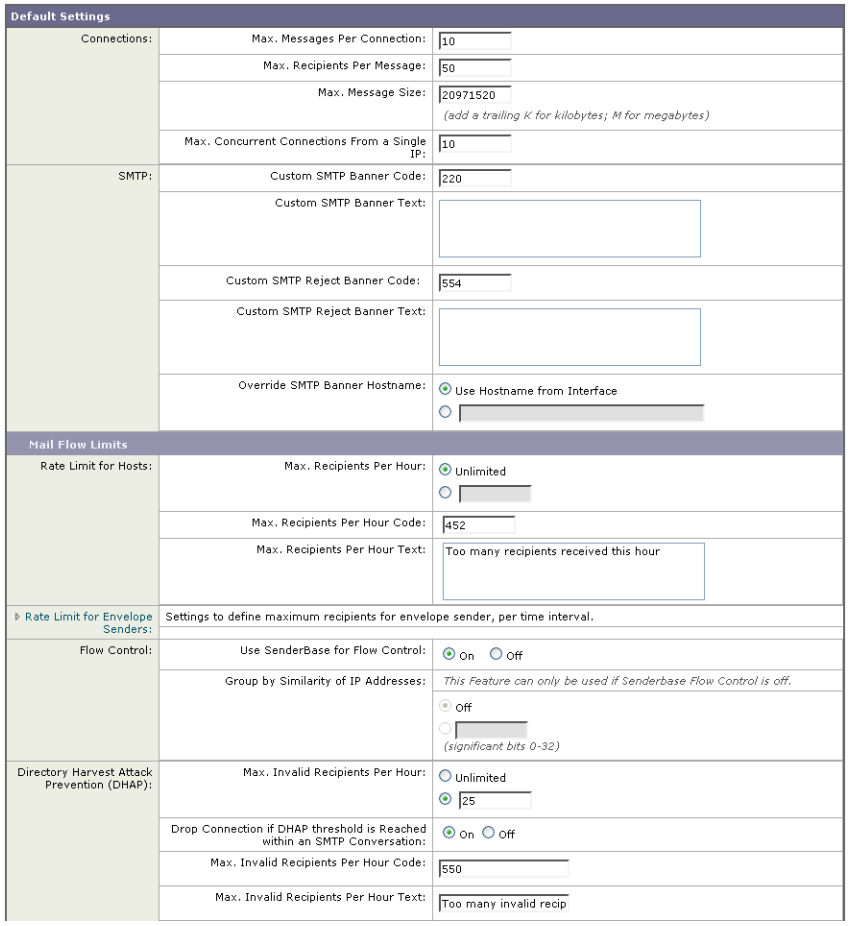
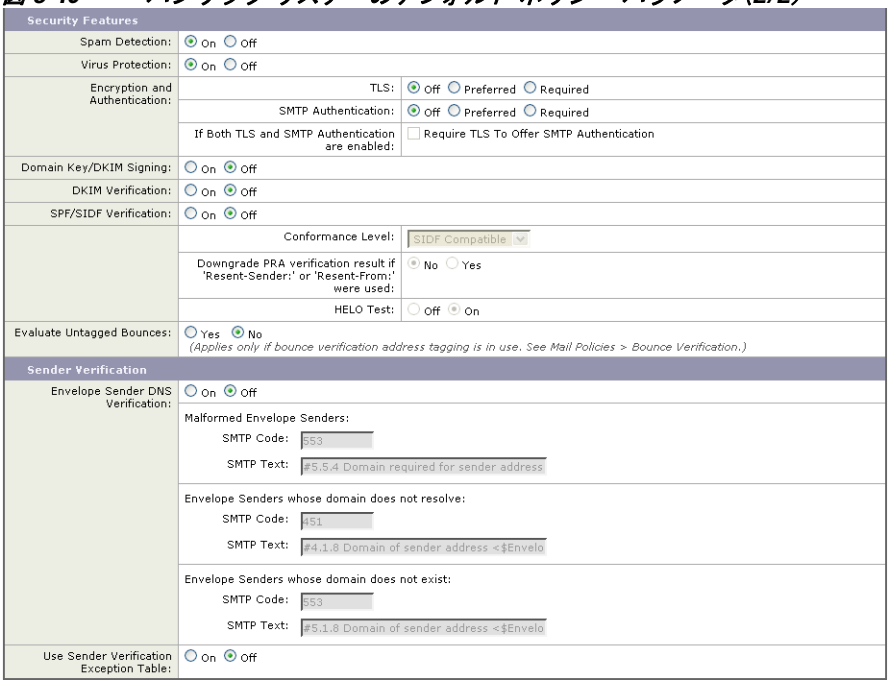


図 5-10　パブリック リスナーのデフォルト ポリシー パラメータ(2/2)



リスナーのデフォルト ポリシー パラメータ

次の表に、パブリック リスナーのデフォルト パラメータの一覧を示します。

表 5-5　パブリック リスナーの HAT デフォルト ポリシー パラメータ

パラメータ	デフォルト値
最大メッセージ サイズ: (Maximum message size:)	20 MB
このリスナーに許可された最大同時接続数: (Max. concurrent connections allowed to this listener:)	10 個の接続
接続あたりの最大メッセージ数: (Maximum messages per connection:)	10 メッセージ
メッセージあたりの最大受信者数: (Maximum recipients per message:)	50 の受信者
SMTP バナー コード : (SMTP Banner Code:)	220
SMTP バナー テキスト : (SMTP Banner Text:)	“*hostname* `ESMTP`”
SMTP 拒否バナー コード : (SMTP Reject Banner Code:)	554
SMTP 拒否バナー テキスト : (SMTP Reject Banner Text:)	“`Access Denied`”
SMTPバナーホスト名を上書き(Override SMTP Banner Hostname)	インターフェイスからのホスト名を使用
1 時間あたりの最大受信者数: (Maximum Recipients per Hour:)	デフォルトなし。ユーザ定義。
時間コードあたりの最大受信者数: (Maximum Recipients per Hour Code:)	452

表 5-5　パブリック リスナーの HAT デフォルト ポリシー パラメータ

パラメータ	デフォルト値
1 時間あたりのテキストの最大受信者数: (Maximum Recipients per Hour Text:)	"Too many recipients received this hour"
時間間隔あたりの最大受信者数: (Maximum Recipients Per Time Interval:)	Unlimited
送信者の最大レート制限エラーコード (Maximum Sender Rate Limit Error Code)	452
送信者のレート制限エラーテキスト (Sender Rate Limit Error Text)	"Too many recipients received from the sender"
例外 (Exceptions)	なし
ディレクトリ獲得攻撃防御 (Directory Harvest Attack Prevention)	OFF
SenderBase を使用: (Use SenderBase:)	ON
IP アドレスの類似性でグループ化: (Group by Similarity of IP address:)	DISABLED
スパム対策スキャンを使用: (Use anti-spam scanning:)	[オン (ON)] (スパム対策が有効な場合)
ウイルス対策スキャンを使用: (Use anti-virus scanning:)	ON (アンチウイルスがイネーブルな場合)
TLS 接続を許可: (Allow TLS Connections:)	NO
ホスト名を上書き (Override Hostname)	NO
SMTP 認証 (SMTP Auth)	OFF
Domainkey/DKIM 署名 (Domainkey/DKIM Signing)	OFF
DKIM 検証 (DKIM Verification)	OFF
SPF/SIDF 検証 (SPF/SIDF Verification)	OFF
エンベロープ送信者の DNS 検証 (Envelope Sender DNS Verification)	OFF
例外テーブルを使用 (Use Exception Table)	OFF

次の表に、プライベート リスナーのデフォルト パラメータの一覧を示します。

表 5-6　プライベート リスナーの HAT デフォルト ポリシー パラメータ

パラメータ	デフォルト値
接続あたりの最大メッセージ数: (Maximum messages per connection:)	10,000 メッセージ
メッセージあたりの最大受信者数: (Maximum recipients per message:)	100,000 の受信者
最大メッセージ サイズ: (Maximum message size:)	100 MB (104857600 バイト)
単一 IP からの最大同時接続数 (Max. concurrent connections from a single IP)	50 接続
SMTP バナー コード: (SMTP Banner Code:)	220

表 5-6　プライベート リスナーの HAT デフォルト ポリシー パラメータ

パラメータ	デフォルト値
SMTP バナー テキスト : (SMTP Banner Text:)	"*hostname* ESMTP"
SMTP 拒否バナー コード : (SMTP Reject Banner Code:)	554
SMTP 拒否バナー テキスト : (SMTP Reject Banner Text:)	"Access Denied"
SMTP バナーホスト名を上書き (Override SMTP Banner Hostname)	インターフェイスからのホスト名を使用
SenderBase を使用 (Use SenderBase:)	OFF
1 時間あたりの最大受信者数 : (Maximum Recipients per Hour:)	デフォルトなし。ユーザ定義。
時間コードあたりの最大受信者数 : (Maximum Recipients per Hour Code:)	452
1 時間あたりのテキストの最大受信者数 : (Maximum Recipients per Hour Text:)	"Too many recipients received this hour"
時間間隔あたりの最大受信者数 : (Maximum Recipients Per Time Interval:)	Unlimited
送信者の最大レート制限エラーコード (Maximum Sender Rate Limit Error Code)	452
送信者のレート制限エラーテキスト (Sender Rate Limit Error Text)	"Too many recipients received from the sender"
例外 (Exceptions)	なし
IP アドレスの類似性でグループ化 : (Group by Similarity of IP address:)	OFF
ディレクトリ獲得攻撃防御 (Directory Harvest Attack Prevention)	OFF
スパム対策スキャンを使用 : (Use anti-spam scanning:)	[オフ (OFF)] (スパム対策が有効な場合)
ウイルス対策スキャンを使用 : (Use anti-virus scanning:)	ON (アンチウイルスがイネーブルな場合)
TLS 接続を許可 : (Allow TLS Connections:)	NO
ホスト名を上書き (Override Hostname)	NO
SMTP 認証 (SMTP Auth)	OFF
Domainkey/DKIM 署名 (Domainkey/DKIM Signing)	OFF
DKIM 検証 (DKIM Verification)	OFF
SPF/SIDF 検証 (SPF/SIDF Verification)	OFF
タグなしバウンスを許可 (Accept Untagged Bounces)	NO
エンベロープ送信者の DNS 検証 (Envelope Sender DNS Verification)	OFF
例外テーブルを使用 (Use Exception Table)	OFF

送信者グループ

HAT パラメータをアクセス ルールと組み合わせることで、メール フロー ポリシーが作成されます（図 5-6 メール フロー ポリシー:アクセス ルールとパラメータ (5-8 ページ) を参照）。異なる HAT パラメータをグループ化して名前を割り当てる場合は、送信者のグループに適用できるメール フロー ポリシーを定義しています。

*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、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 レピュテーション スコア（SBRS）の範囲（またはスコアの欠如）
- DNS リスト クエリー応答

送信者グループを構成するリモート ホスト（送信者エントリ）を定義するための構文については、表 5-7 を参照してください。これらの送信者エントリは、リスナーの HAT 内でカンマで区切られます。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。

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。Cisco IronPort アプライアンスでは、デフォルトで、パブリック リスナー向けの定義済みのメール フロー ポリシーへのアクセス (5-26 ページ) に示すメール フロー ポリシーと送信者グループがあらかじめ定義されています。

第 6 章、電子メール セキュリティ マネージャでは、定義済みの送信者グループとメール フロー ポリシーを使用して、ゲートウェイを通過するメールをすばやく高性能に分類し、リスナーの HAT に対するリアルタイムな変更を行うことができます。

（注） ダブル 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。

送信者グループの構文

表 5-7　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: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: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

表 5-7　HAT 内でのリモート ホストの定義:送信者グループの構文(続き)

構文	意味
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 評価スコアによって定義された送信者グループ (5-24 ページ)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 評価スコアによって定義された送信者グループ (5-24 ページ)を参照してください。
dnslist[dnsserver.domain]	DNS リスト クエリー。詳細については、HAT 内の 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 (5-25 ページ)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 アドレスは、送信元メール ホストの IP アドレスとして定義します。E 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。

ドメインは、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。

ネットワーク オーナーは、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。

組織は、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。組織はネットワーク オーナー、ネットワーク オーナー内の部門、そのネットワーク オーナー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 5-8 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 5-8　　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 IronPort 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 3-7 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 IronPort アプライアンスは、Macromedia Inc.、Alloutdeals.com、*および* Greatoffers.com に対して最大 10 個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 個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 IronPort 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。

ステップ 1　**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。**

着信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。

ステップ 2　**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 モニタ機能の使用方法の詳細については、『*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 評価スコアによって定義された送信者グループ

Cisco IronPort アプライアンスは、Cisco IronPort SenderBase レピュテーション サービスに対してクエリを実行して、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 5-9 に示すように、-10.0 ～ +10.0 です。

表 5-9　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 IronPort アプライ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。SenderBase 評価スコアを使用した送信者グループの作成（5-37 ページ）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 5-10 を参照してください。『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Customizing Listeners」を参照してください。

表 5-10　　HAT 内の SenderBase 評価スコアの構文

`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、アプライアンスが 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。

HAT 内の 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、それに応じてメール 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 IronPort 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（積極的に供託金を拠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。

パブリック リスナー向けの定義済みのメール フロー ポリシーへのアクセス

アクセス ルール（ACCEPT または REJECT）と組み合わせた場合、表 5-3（5-9 ページ）に示すパラメータが、作成する各*パブリック*リスナーの次の 4 つのメール フロー ポリシーとして事前に定義されています。

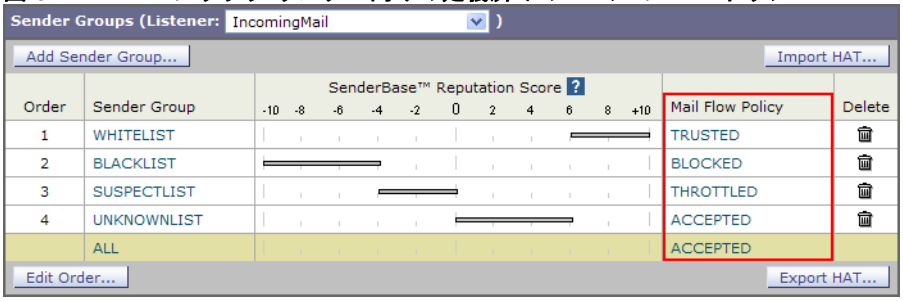
- $ACCEPTED
- $BLOCKED
- $THROTTLED
- $TRUSTED

ステップ 1　GUI にアクセスします（GUI へのアクセス（2-2 ページ）を参照）。

ステップ 2　[Mail Policies] > [HAT Overview] の順にクリックします。

[Overview] ページが表示されます。リスナーが設定されている場合、アルファベット順で最初のリスナーに対して定義されている [Host Access Table overview] ページが表示されます。[Listener] リストから目的のリスナーを選択します。

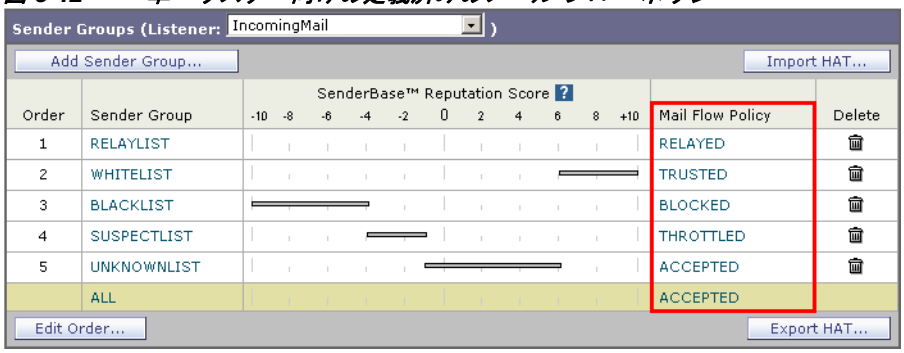
図 5-11　パブリック リスナー向けの定義済みのメール フロー ポリシー



ステップ 3　メール フロー ポリシーの名前をクリックして、そのポリシーの接続動作とパラメータを表示します。

（注）　デフォルトでは、C150/160 のユーザは、systemsetup コマンドの実行中に 1 つのパブリック リスナーのみを作成するように求められます。Cisco IronPort C150/160 アプライアンスで作成されたパブリック リスナーにも、内部システム用にメールを中継するために使用される $RELAYED メール フロー ポリシーが含まれています（図 5-12 を参照）。詳細については、RELAYLIST（5-31 ページ）を参照してください。$RELAYLIST ポリシーは、Cisco IronPort X1050/1060/1070、C650/660/670、および C350/360/370 アプライアンス上のプライベート リスナーのみで表示されます。

図 5-12　単一リスナー向けの定義済みのメール フロー ポリシー



この表で、「デフォルト」は、リスナーで定義されているデフォルト値が使用されることを意味します。

表 5-11　パブリック リスナー向けの定義済みのメール 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
$ACCEPTED （All で使用）	ACCEPT	Maximum messages / session: Maximum recipients / message: Maximum message size: Maximum concurrent connections: SMTP Banner Code: SMTP Banner Text: Override Hostname: Use TLS: Use McAfee virus scanning: Maximum recipients / hour: Maximum rcpt / hour Error Code: Max recipients / hour Text: Use SenderBase:	Default Default Default Default Default Default Default Default Default No default Default Default ON

（注）：$ACCEPTED ポリシーのすべてのパラメータは、CLI の systemsetup および listenerconfig コマンドでユーザが定義します。次の質問が表示されたら「**y**」を選択します。

```
Would you like to change the default host access policy?
```

これによりこれらの値を変更します。GUI を使用してこれらの値を変更するには、図 5-7 デフォルト メール フロー ポリシーの参照（5-16 ページ）の手順に従います。

表 5-11　パブリック リスナー向けの定義済みのメール フロー ポリシー（続き）

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	Maximum messages / session: Maximum recipients / message: Maximum message size: Maximum concurrent connections: SMTP Banner Code: SMTP Banner Text: Override Hostname: Use TLS: Use McAfee virus scanning: Maximum recipients / hour: Maximum rcpt / hour Error Code: Max recipients / hour Text: Use SenderBase:	N/A N/A N/A N/A Default Default Default N/A N/A N/A N/A N/A N/A
$THROTTLED	ACCEPT	Maximum messages / session: Maximum recipients / message: Maximum message size: Maximum concurrent connections: SMTP Banner Code: SMTP Banner Text: Override Hostname Use TLS: Use McAfee virus scanning: Maximum recipients / hour: Maximum rcpt / hour Error Code: Max recipients / hour Text: Use SenderBase: Envelope Sender DNS Ver:	1 25 10MB 1 Default Default Default Default Default* 20 Default Default ON ON
$TRUSTED	ACCEPT	Maximum messages / session: Maximum recipients / message: Maximum message size: Maximum concurrent connections: SMTP Banner Code: SMTP Banner Text: Override Hostname: Use TLS: Use McAfee virus scanning: Maximum recipients / hour: Maximum rcpt / hour Error Code: Max recipients / hour Text: Use SenderBase:	5,000 5,000 100 MB 600 Default Default Default Default OFF* -1(Disable) N/A N/A OFF

* イネーブルな場合

$ACCEPTED は名前付きポリシーであり、パブリック リスナーのデフォルトの HAT 設定と同じです。$ACCEPTED ポリシーは作成するどの送信者グループにも割り当てることができます（新しい送信者グループの追加（5-33 ページ）および接続（5-9 ページ）を参照してください。また、HAT の操作（5-41 ページ）も参照してください）。

パブリック リスナー用の HAT 内の最後の ALL エントリも、主な動作として $ACCEPTED ポリシーを使用します。

各パブリック リスナーには、表 5-12 に示す送信者グループと対応するメール フロー ポリシーがデフォルトで定義されています。

表 5-12　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

送信者グループ	使用するメール フロー ポリシー
WHITELIST	$TRUSTED
BLACKLIST	$BLOCKED
SUSPECTLIST	$THROTTLED
UNKNOWNLIST	$ACCEPTED

これら 4 つの基本的な送信者グループとメール フロー ポリシーを使用することで、パブリック リスナー上でゲートウェイに流れ込む電子メールの分類を開始するためのフレームワークが得られます。『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Using Email Security Monitor」では、ゲートウェイに流れ込む電子メールのリアルタイム フローを確認し、リスナーの HAT をリアルタイムで変更できます。（IP アドレス、ドメイン、または組織の既存の送信者グループへの追加、既存のポリシーまたは定義済みのポリシーの編集、新しいメール フロー ポリシーの作成）を行うことができます。

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。

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。

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。

- 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）。
- Cisco IronPort 送信者に関する詳細情報を得るために、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。

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 IronPort Anti-Spam ソフトウェア（システムでイネーブルになっている場合）、アンチウイルス スキャン エンジン、および Cisco IronPort 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ルになります。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（8-1 ページ）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、評価フィルタリング（7-1 ページ）を参照してください。

プライベート リスナー用の定義済みのメール フロー ポリシー

表 5-3 に定義されているパラメータを、アクセス ルール（RELAY または REJECT）と組み合わせた場合、作成する各プライベート リスナーの次の 2 つのメール フロー ポリシーとして事前に定義されます。

- $RELAYED
- $BLOCKED

これらのポリシーの要約を表 5-12 に示します。

図 5-13　　プライベート リスナー用の定義済みのメール フロー ポリシー

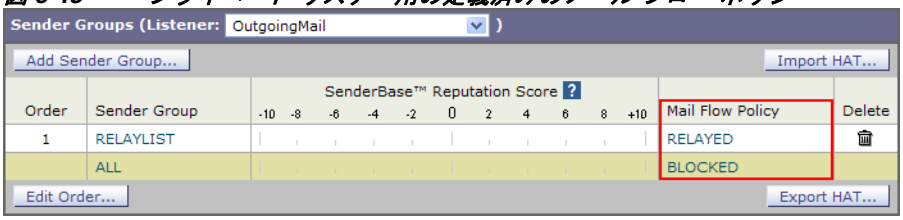


表 5-13　　プライベート リスナー用の定義済みのメール フロー ポリシー

ポリシー名	主要な動作（アクセス ルール）	パラメータ	値
$RELAYED	RELAY	Maximum messages / session:	Default
		Maximum recipients / message:	Default
		Maximum message size:	Default
		Maximum concurrent connections:	Default
		SMTP Banner Code:	Default
		SMTP Banner Text:	Default
		Override Hostname:	Default
		Use TLS:	Default
		Use Sophos virus scanning:	Off (if enabled)
		Maximum recipients / hour:	-1 (Disabled)
		Maximum rcpt / hour Error Code:	Not applicable
		Max recipients / hour Text:	Not applicable
		Use SenderBase:	Default

表 5-13　プライベート リスナー用の定義済みのメール フロー ポリシー（続き）

ポリシー名	主要な動作（アクセス ルール）	パラメータ	値
$BLOCKED（All で使用）	REJECT	Maximum messages / session: Maximum recipients / message: Maximum message size: Maximum concurrent connections: SMTP Banner Code: SMTP Banner Text: Override Hostname: Use TLS: Use Sophos virus scanning: Maximum recipients / hour: Maximum rcpt / hour Error Code: Max recipients / hour Text: Use SenderBase:	Not applicable Not applicable Not applicable Not applicable Default Default Default Not applicable Not applicable Not applicable Not applicable Not applicable Not applicable

$BLOCKED は名前付きポリシーであり、プライベート リスナーのデフォルトの HAT 設定と同じです。プライベート リスナー用の HAT 内の最後の ALL エントリも、デフォルトの動作として $BLOCKED ポリシーを使用します。

各プライベート リスナーには、表 5-14 に示す送信者グループと対応するメール フロー ポリシーがデフォルトで定義されています。

表 5-14　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

送信者グループ	使用するメール フロー ポリシー
RELAYLIST	$RELAYED
ALL	$BLOCKED

この基本的な送信者グループとメール フロー ポリシーを使用することで、プライベート リスナー上でゲートウェイから出て行く電子メールの分類を開始するためのフレームワークが得られます。

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） GUI の System Setup Wizard（または CLI の systemsetup コマンド）でアウトバウンド（プライベート）リスナーを作成するときに、Cisco IronPort アプライアンスを通じた電子メールの中継を許可したシステムは、送信者グループ RELAYLIST に自動的に追加されます。手順 3: ネットワーク (3-18 ページ) を参照してください。

（注）　デフォルトでは、C10/100 のユーザは、systemsetup コマンドの実行中に 1 つのパブリック リスナーのみを作成するように求められます。Cisco IronPort C10/100 アプライアンス上で作成されたパブリック リスナーにも、内部システム用にメールを中継するために使用される $RELAYED メール フロー ポリシーが含まれます。

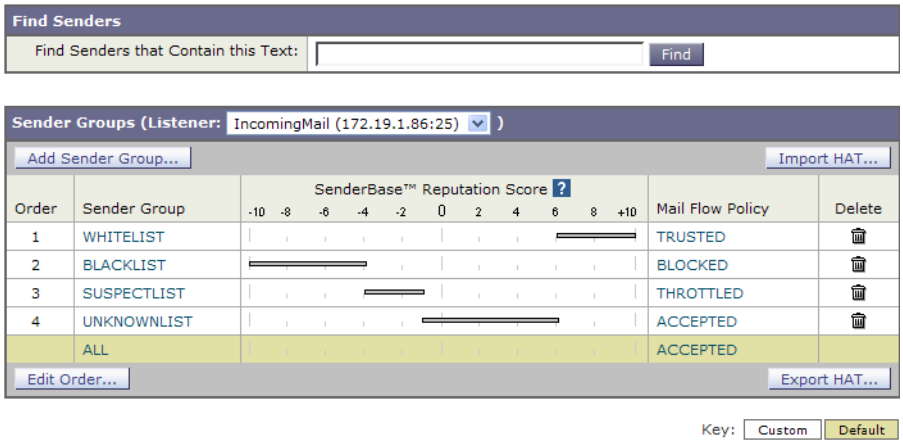
GUI による送信者グループとメール フロー ポリシーの管理

[Mail Policies] > [HAT Overview] ページと [Mail Flow Policy] ページでは、リスナーの HAT 設定を行うことができます。これらのページでは、次のことが可能です。

- 送信者グループからメール フロー ポリシーへのマッピングの参照
- 送信者グループの作成、編集、削除
- メール フロー ポリシーの作成、編集、削除
- リスナーの HAT エントリの順序変更

[Mail Policies] > [HAT Overview] リンクをクリックします。図 5-14 を参照してください。[Listener:] ドロップダウン リストから設定するリスナーを選択します。

図 5-14　[Host Access Table Overview] ページ

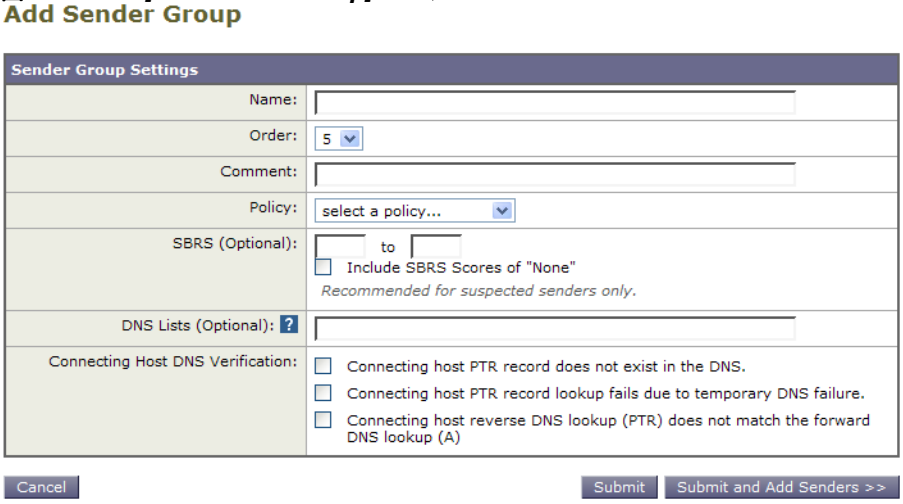


[HAT Overview] ページでは、送信者グループの追加やリスナーのメール フロー ポリシーの編集を行うことができます。

新しい送信者グループの追加

ステップ 1　[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 5-15　[Add Sender Group] ページ



ステップ 2　各フィールドに、送信者グループの名前を入力し、送信者グループのリストに配置する順序を選択し、コメントを入力します(任意)。

ステップ 3　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。そうでない場合は、ドロップダウン リストからメール フロー ポリシーを選択します。

ステップ 4　SBRS の範囲と DNS リストを選択します(任意)。また、SBRS に情報がない送信者を含めるためのチェックボックスをオンにすることもできます。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 5　ホストの DNS 検証の設定を行います(送信者検証の実装 — 設定例(5-46 ページ)を参照)。

ステップ 6　[送信(Submit)] をクリックして送信者グループを保存し [ホストアクセステーブル(Host Access Table)] ページに戻るか、[送信者を送信して追加(Submit and Add Senders)] をクリックしてグループを作成し、送信者のグループへの追加を開始します。

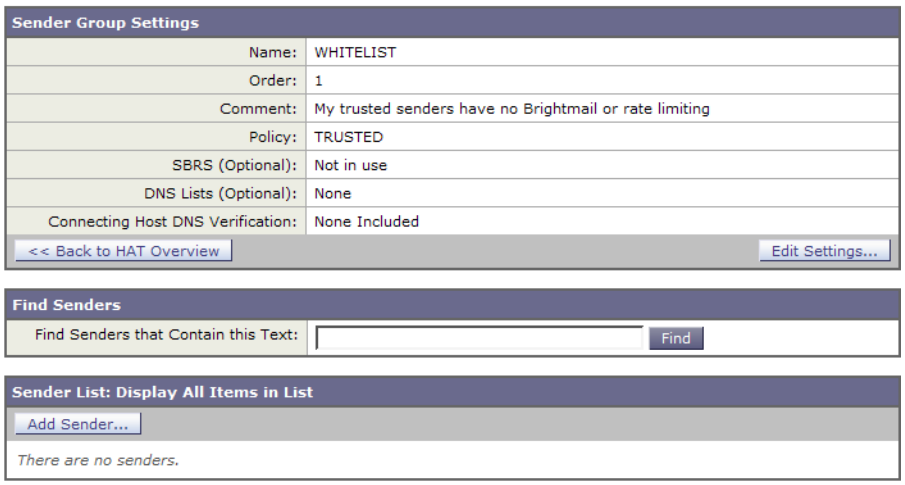
ステップ 7　変更を保存します。

(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。

送信者グループの編集

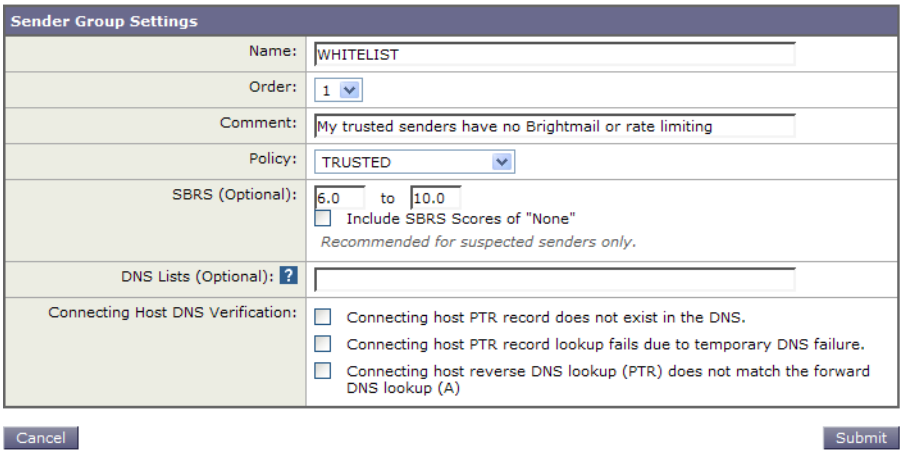
ステップ 1　[HAT Overview] ページで、既存の送信者グループの名前をクリックします。選択した送信者グループが表示されます。

図 5-16　[Sender Group Detail] ページ



ステップ 2　[設定を編集（Edit Settings）] をクリックします。[送信者グループを編集（Edit Sender Group）] ページが表示されます。

図 5-17　[Edit Sender Group] ページ



ステップ 3　送信者グループを変更し、[送信（Submit）] をクリックします。

ステップ 4　変更を保存します。

送信者グループの削除

ステップ 1　[HAT Overview] ページで、削除する送信者グループの [Delete] 列にあるゴミ箱のアイコンをクリックします。削除を確認するよう求められます。

ステップ 2　[はい（Yes）] をクリックして送信者グループを削除するか、[いいえ（No）] をクリックしてキャンセルします。

ステップ 3　変更を保存します。

新しいメール フロー ポリシーの追加

ステップ 1　[Mail Policies] > [Mail Flow Policies] リンクをクリックします。[Mail Flow Policies] ページが表示されます。

ステップ 2　[ポリシーを追加（Add Policy）] をクリックします。[Mail Flow Policies Add Policy] ページが表示されます。

ステップ 3　メール フロー ポリシーの情報を入力します。

ステップ 4　エンベロープ送信者の DNS 検証を設定します（送信者検証の実装 — 設定例（5-46 ページ）を参照）。

ステップ 5　変更を送信し、保存します。

（注）　[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、[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。

（注）　[Custom SMTP Banner Text] および [Max. Recipients Per Hour] テキスト文字列フィールドは、HAT 変数の構文（5-14 ページ）で説明した HAT 変数をサポートしています。

（注）　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 アクセプト クエリーを設定しておく必要があります）。

メール フロー ポリシーの編集

ステップ 1　[Mail Flow Policy overview] ページで、ポリシーの名前をクリックします。[Mail Flow Policy Edit Policy] ページが表示されます。

ステップ 2　ポリシーを変更します。

ステップ 3　変更を送信し、保存します。

メール フロー ポリシーの削除

ステップ 1　削除するメール フロー ポリシーの [Delete] 列にあるゴミ箱のアイコンをクリックします。削除を確認するよう求められます。

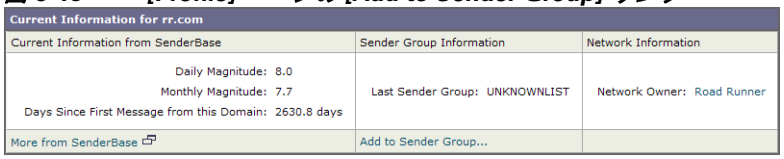
ステップ 2　[はい（Yes）] をクリックしてメール フロー ポリシーを削除するか、[いいえ（No）] をクリックしてキャンセルします。

ステップ 3　変更を保存します。

送信者グループへの送信者の追加

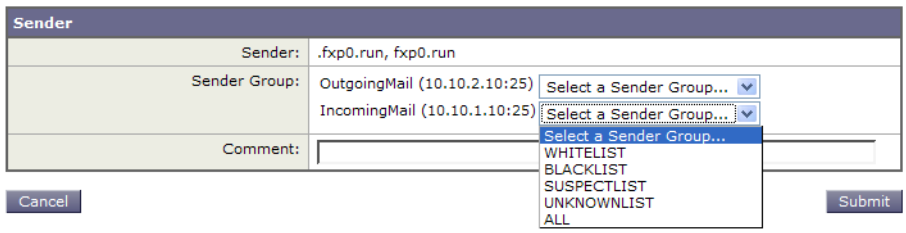
ステップ 1　ドメイン、IP、またはネットワーク オーナー プロファイル ページで、[送信者グループに追加（Add to Sender Group）] リンクをクリックします。

図 5-18　[Profile] ページの [Add to Sender Group] リンク



[Add to Sender Group] ページが表示されます。図 5-19 を参照してください。

図 5-19　[Add to Sender Group] ページ



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　[送信（Submit）] をクリックして選択した送信者グループにドメインを追加するか、[キャンセル（Cancel）] をクリックします。

ステップ 4　変更を保存します。

（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（5-21 ページ）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。

Success — Added sender(s) to sender group(s). Some duplicates existed and were not added.

ステップ 5　[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。

新しい送信者グループへの送信者の追加

ステップ 1　新しい送信者グループを作成する場合、[送信者を送信して追加（Submit and Add Senders）] をクリックします。[Add Sender] ページが表示されます。

ステップ 2　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。

ステップ 3　オプションで送信者のコメントを入力します。

ステップ 4　[送信（Submit）] をクリックして送信者グループにドメインを追加するか、[キャンセル（Cancel）] をクリックします。

ステップ 5　変更を保存します。

SenderBase 評価スコアを使用した送信者グループの作成

ステップ 1　[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。

ステップ 2　[Add Sender Group] ページで、送信者グループの名前とオプションのコメントを入力します。

ステップ 3　リストからメール フロー ポリシーを選択します。

ステップ 4　[送信者（Senders）] セクションで、ドロップダウン リストから [SBRS] を選択し、[送信者を追加（Add Sender）] をクリックします。

ページがリフレッシュされます。

ステップ 5　SBRS の [from:] フィールドと [to:] フィールドに範囲を入力し、オプションのコメントを入力します。

図 5-20 で、SenderBase 評価スコアが -7.5 未満の送信者は、BLOCKED メール フロー ポリシーを使用してブロックされます。

図 5-20　SenderBase 評価スコアを使用した送信者グループの作成（1）

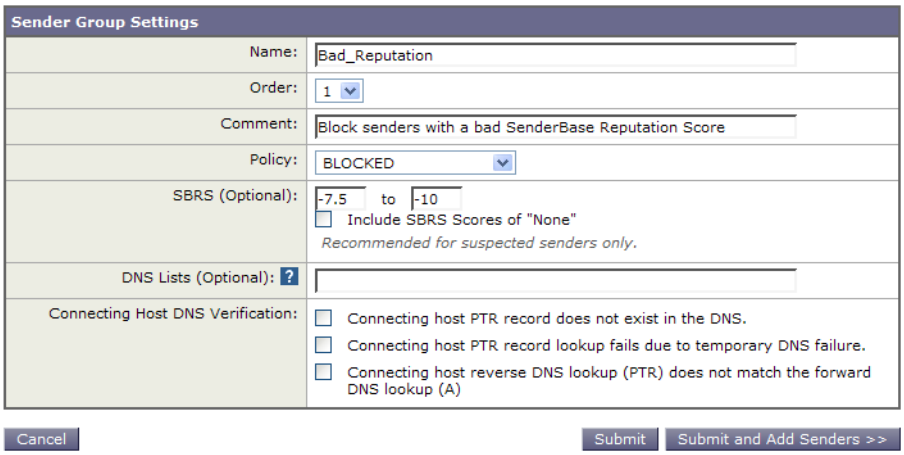
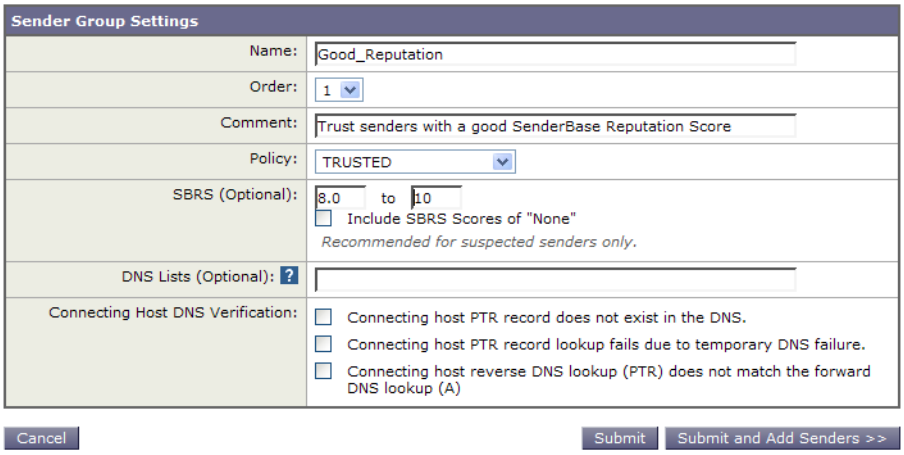


図 5-21 で、SenderBase 評価スコアが 8.0 を超えている送信者はリスナーのアンチスパム スキャンをバイパスします。

図 5-21　SenderBase 評価スコアを使用した送信者グループの作成（2）

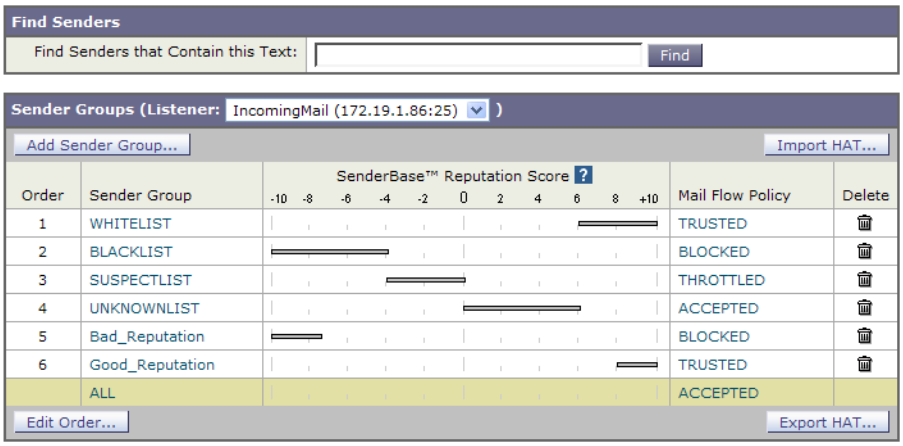


（注）　これらの同じパラメータを使用し、SenderBase 評価スコアに基づいて送信者を含めるように、TRUSTED および BLOCKED のデフォルト ポリシーを変更することもできます。詳細については、SenderBase 評価フィルタの実装（7-4 ページ）を参照してください。

ステップ 6　[送信（Submit）] をクリックし、SenderBase 評価スコアに基づいて送信者グループを作成します。

ステップ 7　変更を保存します。

図 5-22　SenderBase 評価スコアを使用したホスト アクセス テーブル



HAT の順序変更

HAT 内のエントリの順序は重要です。リスナーに接続しようとする各ホストについて、HAT が上から下に向かって読み込まれることを思い出してください。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。

たとえば、CIDR ブロックを送信者グループ A で指定し（ポリシー 1 を使用）、その CIDR ブロック内の IP アドレスに対して送信者グループ B を作成すると、送信者グループ B のポリシーは適用されません。

ステップ 1　[HAT 概要（HAT Overview）] ページで、[順番を編集（Edit Order）] をクリックします。[送信者グループの順番を編集（Edit Sender Group Order）] ページが表示されます。

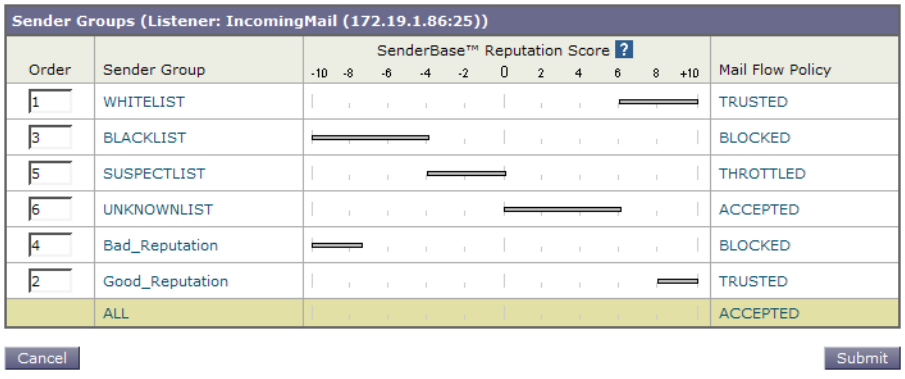
ステップ 2　HAT の既存の行の新しい順序を入力します。

ステップ 3　変更を送信し、保存します。

[HAT Overview] ページがリフレッシュされ、新しい順序で表示されます。

図 5-23 に示す次の例では、信頼できる送信者が最初に処理され、ブロックされる送信者が次に処理され、不明または疑いのある送信者が最後に処理されるように順序を変更しています。

図 5-23　HAT 内のエントリの順序の変更



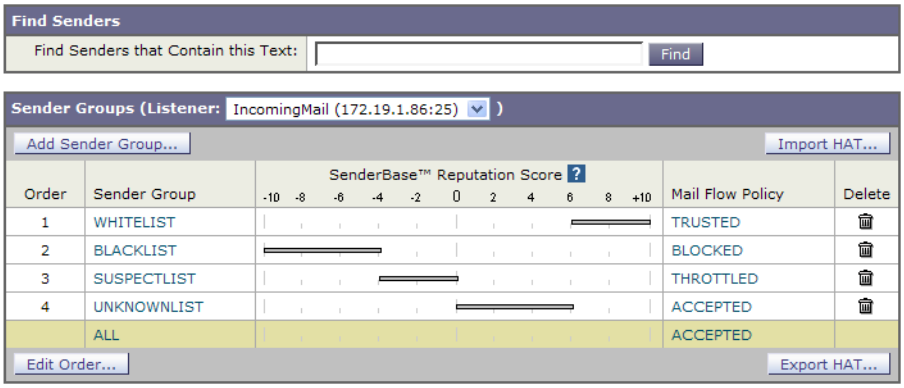
送信者の検索

[HA 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。

GUI によるリスナーの HAT の変更

グラフィカル ユーザ インターフェイス（GUI）にログインし、[Mail Policies] タブをクリックします（GUI へのアクセス方法の詳細については、GUI へのアクセス（2-2 ページ）を参照してください）。左側のメニューで [HAT 概要（HAT Overview）] リンクをクリックします。[Host Access Table Overview] ページが表示されます。

図 5-24　[Host Access Table Overview] ページ



[Host Access Table Overview] ページには、HAT 内の送信者グループが、順序、SenderBase 評価スコア範囲、関連付けられているメール フロー ポリシーとともに一覧表示されます。

[Host Access Table Overview] ページでは、次のことを行うことができます。

- 送信者グループの HAT への追加
- 送信者グループの HAT からの削除
- 既存の送信者グループの変更
- エントリの順序の変更
- ファイルからの HAT のインポート（既存のエントリの上書き）（HAT のインポートとエクスポートについては、HAT の操作（5-41 ページ）を参照してください）。
- HAT のファイルへのエクスポート
- 送信者の検索

送信者グループを編集すると、次のことが可能です。

- 送信者グループへの送信者の追加と削除
- 送信者グループの設定の編集

送信者グループの使用方法の詳細については、GUI による送信者グループとメール フロー ポリシーの管理（5-32 ページ）を参照してください。

HAT の操作

HAT のエクスポート

ステップ 1　[HAT をエクスポート（Export HAT）] をクリックします。[ホストアクセステーブルをエクスポート（Export Host Access Table）] ページが表示されます。

図 5-25　HAT のエクスポート

ステップ 2　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。

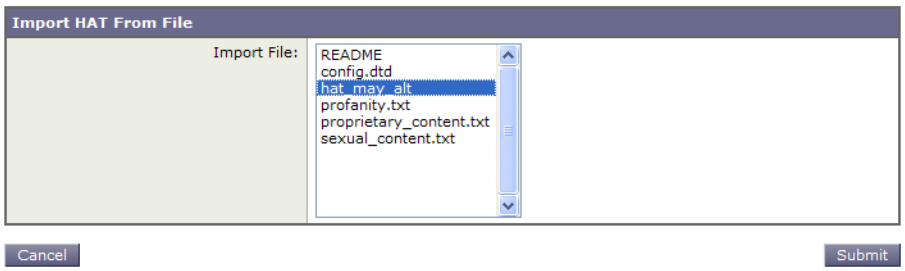
ステップ 3　変更を送信し、保存します。

HAT 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。

ステップ 1　[HAT をインポート（Import HAT）] をクリックします。[ホストアクセステーブルをインポート（Import Host Access Table）] ページが表示されます。

図 5-26　HAT のエクスポート



ステップ 2　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 3　[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 4　[インポート（Import）] をクリックします。

ステップ 5　変更を保存します。

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 20060530T215438

$BLOCKED

    REJECT {}

[ ... ]
```

アドレス リスト

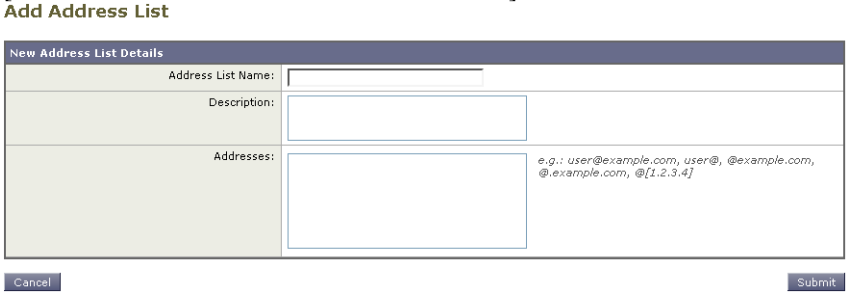
メール フロー ポリシーは、レート制限の除外、および必須 TLS 接続などのエンベロープ送信者グループに適用する特定の設定にアドレス リストを使用できます。アドレス リストは、電子メール アドレス、ドメイン、部分ドメインおよび IP アドレスで構成できます。GUI で [メールポリシー（Mail Policies）] > [アドレスリスト（Address Lists）] のページを使用するか、または CLI の `addresslistconfig` コマンドを使用し、アドレスリストを作成できます。[アドレスリスト（Address Lists）] のページには、アドレス リストを使用するメール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

アドレス リストの作成

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。

[アドレスリストの追加（Add Address List）] ページが表示されます。



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@`
- 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`
- 特定の IP アドレスを持つホストのすべてのユーザ：`@[1.2.3.4]`

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　変更を送信し、保存します。

アドレス リストの編集

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　編集するアドレス リストの名前をクリックします。

ステップ 3　アドレス リストを変更します。

ステップ 4　変更を送信し、保存します。

アドレス リストの削除

アドレス リストを削除するには、削除するメッセージ アクションの横にある [削除（Delete）] チェックボックスをオンにします。メール フロー ポリシーがアドレス リストを使用するかどうかを確認するメッセージが表示されます。リストを削除すると、そのリストを使用するメール フロー ポリシーからも削除されます。変更を保存します。

送信者検証

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 IronPort 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 IronPort アプライアンスを設定できます。

送信者検証機能は、SMTP カンバセーションの前に実行される接続元ホストの検証と、SMTP カンバセーションの最中に実行されるエンベロープ送信者のドメイン部分の検証の 2 つで構成されます。

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 IronPort 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。ダブル 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、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 3 つ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 に対するホスト送信者検証の実装（5-47 ページ）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ことは、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になります。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 検証を有効にすると、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）。ドメインは、DNS で確認試行がタイムアウトまたは DNS サーバの障害などの一時的なエラー状態が発生したかを解決できません。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 カンバセーションの中で実行されるのに対し、ホスト DNS 検証はカンバ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「存在しないドメインのエンベロープ送信者」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。

ただし DNS サーバが「SERVERFAIL」を返した場合、DNS サーバは「応答がないドメインのエンベロープ送信者」カテゴリに分類されます。SERVFAIL は、ドメインが存在しないが、DNS でレコードのルックアップ中に一時的な問題が発生していることを示します。

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 IronPort 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（5-46 ページ）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 カンバ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に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

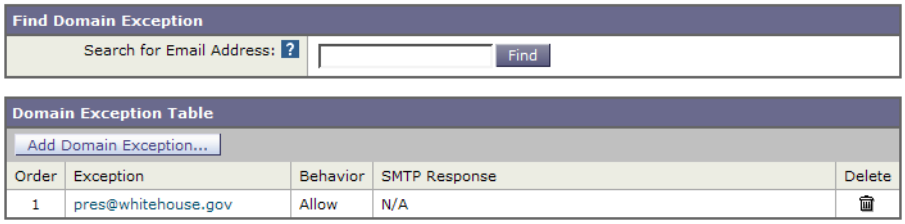
送信者検証例外テーブルは、SMTP カンバセーション中に自動的に許可または拒否されるドメインまたは電子メール アドレスのリストです。また、拒否されるドメインについて、オプションの SMTP コードと拒否応答を指定することもできます。Cisco IronPort アプライアンスあたりの送信者検証例外テーブルは 1 つのみであり、メール フロー ポリシーごとにイネーブルにされます。

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 に対する送信者検証の実装（5-50 ページ）を参照）または CLI（『*Cisco IronPort 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 5-27　例外テーブルのリスト



例外テーブルの変更についてはGUI での送信者検証例外テーブルの作成（5-50 ページ）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 カンバ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 5-15 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 5-15　送信者検証：推奨される設定

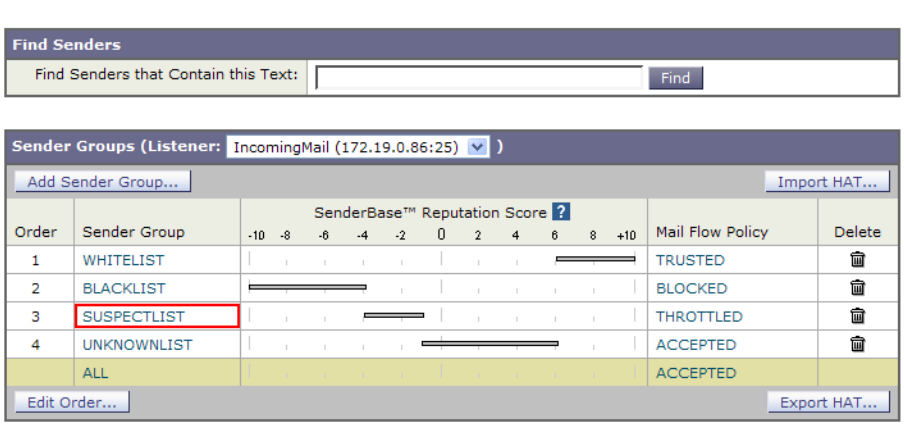
送信者グループ	ポリシー	含める
UNVERIFIED	THROTTLEMORE	SMTP カンバセーションの前。 接続元ホストの PTR レコードが DNS に存在しない。
SUSPECTLIST	THROTTLED	接続元ホストの逆引き DNS ルックアップ（PTR）が正引き DNS ルックアップ（A）に一致しない。
	ACCEPTED	SMTP カンバセーション中のエンベロープ送信者検証。 - 形式が不正な MAIL FROM:。 - エンベロープ送信者が DNS に存在しない。 - エンベロープ送信者が DNS で解決されない。

送信者グループ SUSPECTLIST に対するホスト送信者検証の実装

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。

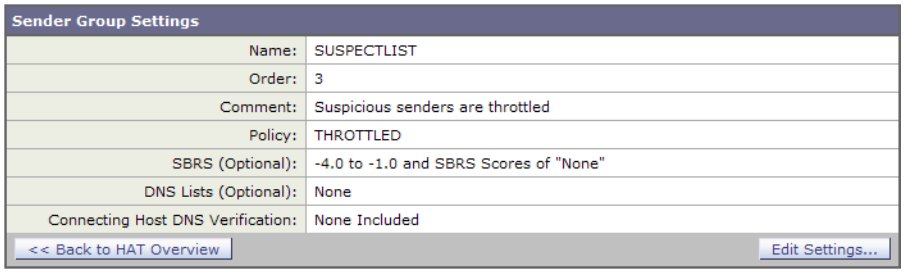
ステップ 2　送信者グループのリストで [SUSPECTLIST] をクリックします。

図 5-28　[HAT 概要（HAT Overview）] ページ



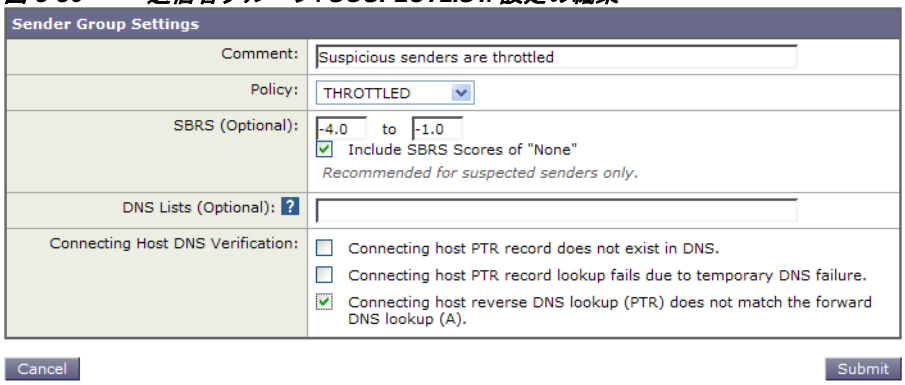
ステップ 3　[Sender Group: SUSPECTLIST] ページが表示されます。

図 5-29　Sender Group: SUSPECTLIST



ステップ 4　[設定を編集（Edit Settings）] をクリックします。[設定を編集（Edit Settings）] ダイアログが表示されます。

図 5-30　送信者グループ: SUSPECTLIST: 設定の編集



ステップ 5　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 6　[接続ホストの DNS 検証（Connecting Host DNS Verification）] の中の [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 7　変更を送信し、保存します。

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（5-54 ページ）を参照してください。

送信者検証の実装

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。

ステップ 1　[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。

ステップ 2　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。

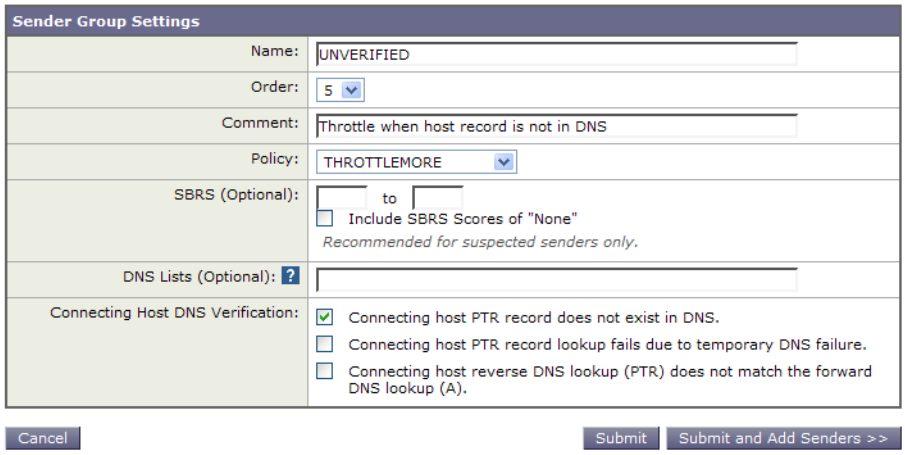
ステップ 3　メールをスロットリングするようにポリシーを設定します。

ステップ 4　変更を送信し、保存します。

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。

ステップ 1　[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 5-31　送信者グループの追加：THROTTLEMORE

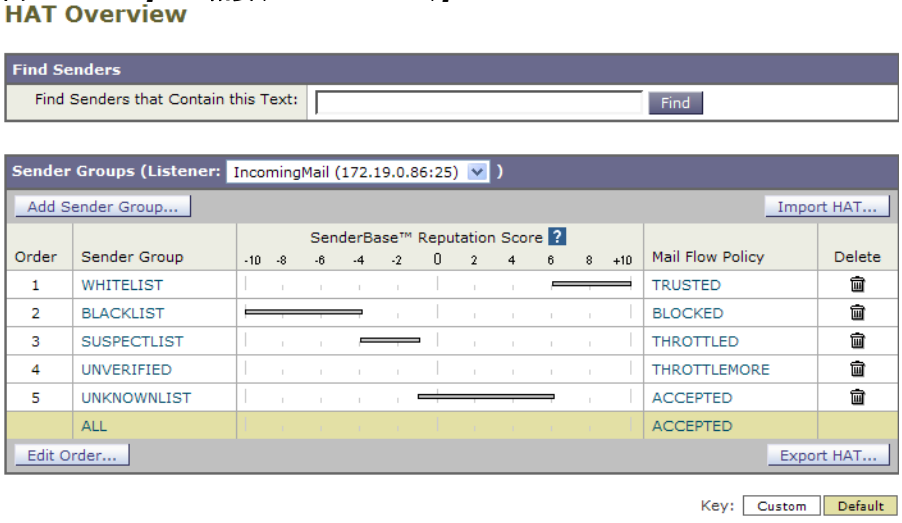


ステップ 2　リストから [THROTTLEMORE] ポリシーを選択します。

ステップ 3　[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。

ステップ 4　変更を送信し、保存します。これで [HAT Overview] ページは次のようになります。

図 5-32　[HAT 概要（HAT Overview）]



次の手順では、未検証の送信者を扱うようにメール フロー ポリシー ACCEPTED を設定します。

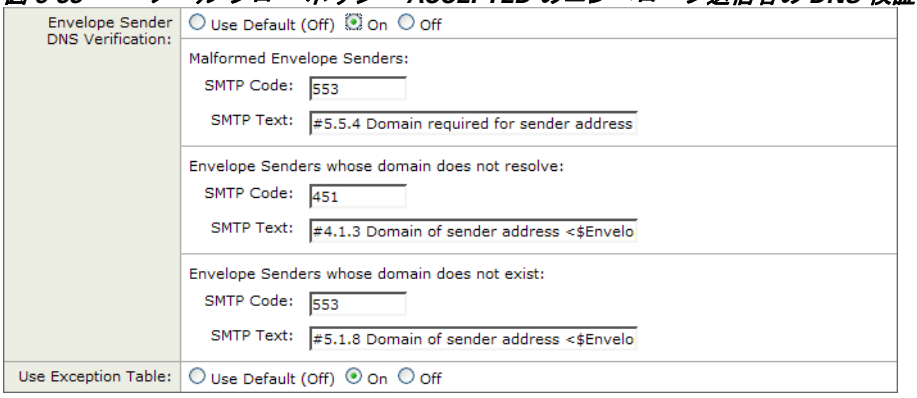
メール フロー ポリシー ACCEPTED に対する送信者検証の実装

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 5-33　メール フロー ポリシー ACCEPTED のエンベロープ送信者の DNS 検証の設定



ステップ 4　[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ープ送信者の 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 [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　変更を送信し、保存します。

最後の手順として、送信者検証例外テーブルを作成し、送信者検証設定に対する例外を列挙します。

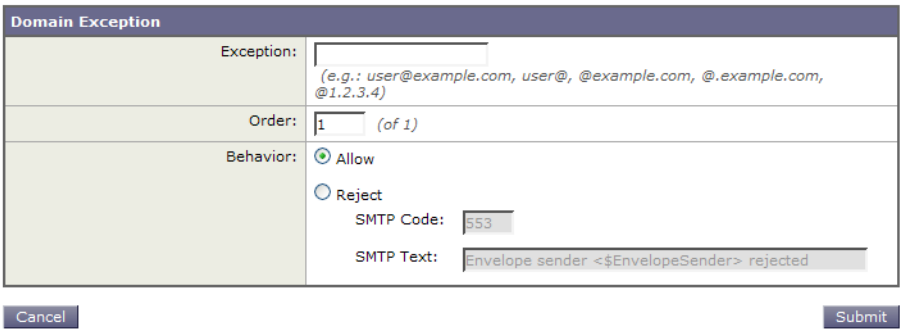
GUI での送信者検証例外テーブルの作成

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。[Add Domain Exception] ページが表示されます。

図 5-34　例外テーブルへのアドレスの追加



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。

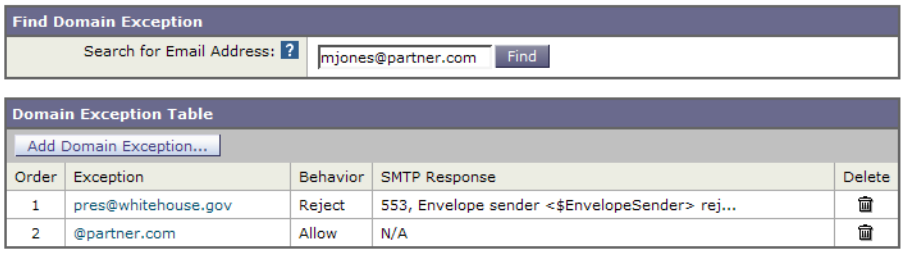
ステップ 4　そのアドレスからのメッセージを許可するか拒否するかを指定します。メールを拒否する場合、SMTP コードとカスタム応答を指定することもできます。

ステップ 5　変更を送信し、保存します。

送信者検証例外テーブル内でのアドレスの検索

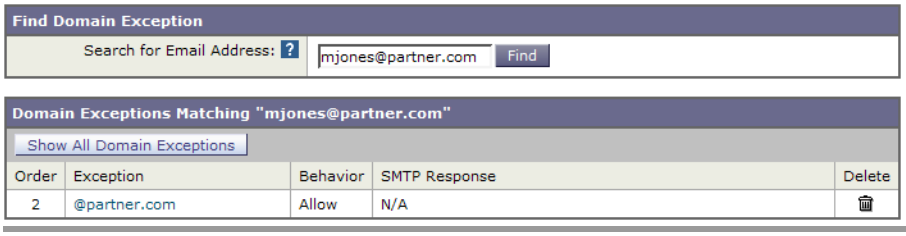
ステップ 1　[例外テーブル（Exception Table）] ページの [ドメイン例外の検索（Find Domain Exception）] セクションに電子メール アドレスを入力し、[検索（Find）] をクリックします。

図 5-35　例外テーブル中の一致エントリの検索



ステップ 2　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 5-36　例外テーブル中の一致エントリの一覧表示



送信者検証設定のテスト

これで送信者検証設定を完了したため、Cisco IronPort 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。

エンベロープ送信者検証の設定のテスト

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。

ステップ 1　Cisco IronPort 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 IronPort 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ルにした場合は（『*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 ESMTP

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。

送信者検証例外テーブルのテスト

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。

ステップ 1　アドレス admin@zzzaaazzz.com を、例外テーブルに動作「Allow」で追加します。

ステップ 2　変更を保存します。

ステップ 3　Cisco IronPort 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@zzzaaazzz.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@zzzaaazzz.com

250 sender <admin@zzzaaazzz.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 IronPort AsyncOS CLI Reference Guide*』を参照してください）。

表 5-16 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 5-16　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。	`nx.domain`
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。	`serv.fail`
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。	`not.double.verified`

パブリック リスナー（RAT）上でのローカル ドメインまたは特定のユーザの電子メールの受け入れ

パブリック リスナーを作成するとき、受信者アクセス テーブル（RAT）を使用して、アプライアンスがメッセージを受け付けるすべてのローカル ドメインを定義します。多くのエンタープライズ ゲートウェイは、複数のローカル ドメインのメッセージを受け付けるように設定されます。たとえば、会社名が変更されたとします。その場合、`currentcompanyname.com` および `oldcompanyname.com` 宛の電子メール メッセージを受信する必要があります。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 に含めることになります（注：ドメイン マップ機能によって、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」の章の「Domain Map feature」の項を参照してください）。

（注）　System Setup Wizard または `systemsetup` コマンドを完了し、`commit` コマンドを実行済みの場合、1 つのパブリック リスナーがアプライアンス上ですでに設定されています。（手順 3：ネットワーク（3-18 ページ）に入力した設定を参照してください）。そのときに入力した、メールを許可するデフォルト ローカル ドメインまたは具体的なアドレスは、そのパブリック リスナーの RAT の最初のエントリとして設定されます。

受信者アクセス テーブル（RAT）

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。このテーブルでは、アドレス（部分アドレス、ユーザ名、ドメイン、またはホスト名）と、それを許可するか拒否するかを指定します。オプションで、その受信者の RCPT TO コマンドに対する SMTP 応答を含めたり、特定のエントリでスロットリング制御をバイパスしたりできます。

RAT エントリは次の基本的な構文によって定義されます。

表 5-17　RAT の基本的な構文

受信者定義	ルール	（任意）カスタム SMTP 応答

ルール

RAT には、SMTP カンバセーションの中でやりとりするときに受信者に対して実行する、次の 2 つの基本的な動作があります。

ACCEPT	受信者は許可されます。
REJECT	受信者は拒否されます。

受信者の定義

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（3-18 ページ）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 も入力した方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て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て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）宛てのメールは許可*されません*。

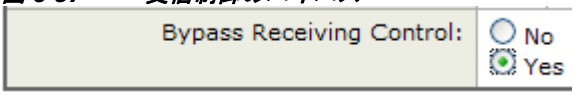
特別な受信者でのスロットリングのバイパス

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）] で [はい（Yes）] を選択します。

図 5-37　受信制御のバイパス



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「はい（yes）」と答えます。

```
Would you like to bypass receiving control for this entry?  [N]> y
```

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、customercare@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 customercare@example.com を bob@example.com および sue@example.com にマップします。customercare@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 アクセプト 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「y」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 宛て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。

デフォルト RAT エントリ

作成するすべてのパブリック リスナーについて、デフォルトでは、*すべての* 受信者からの電子メールを *拒否する* ように RAT が設定されます。

ALL	REJECT

[受信者アクセステーブルの概要（Recipient Access Table Overview）] リストでは、デフォルト エントリの名前は [その他の受信者（All Other Recipients）] になります。

（注）　デフォルトでは、RAT はすべての受信者を *拒否* し、誤ってインターネット上に *オープン リレー* が作成されないようにします。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。作成するパブリック リスナーの受信者アクセス テーブルのデフォルト値を変更するときには注意してください。

デフォルトの「ALL」エントリを RAT から削除してはなりません。

テキスト ファイルとしてのテキスト リソースのインポートおよびエクスポート

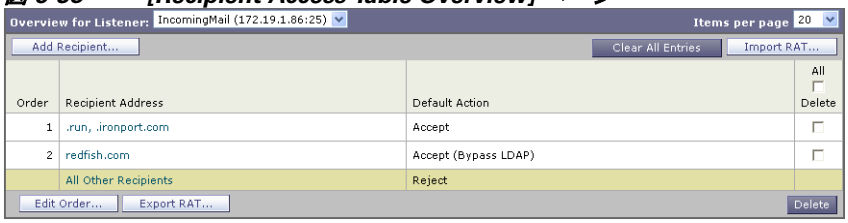
アプライアンスのコンフィギュレーション ディレクトリにアクセスする必要があります。インポートするテキスト ファイルは、アプライアンス上の configuration ディレクトリに存在する必要があります。エクスポートされたテキスト ファイルは、configuration ディレクトリに配置されます。

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。

GUI によるリスナーの RAT の変更

GUI から RAT を変更するには、[Mail Policies] > [Recipient Access Table (RAT)] をクリックします。[Recipient Access Table Overview] ページが表示されます。

図 5-38　[Recipient Access Table Overview] ページ



[Recipient Access Table Overview] 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。

[Recipient Access Table Overview] では、次のことを行うことができます。

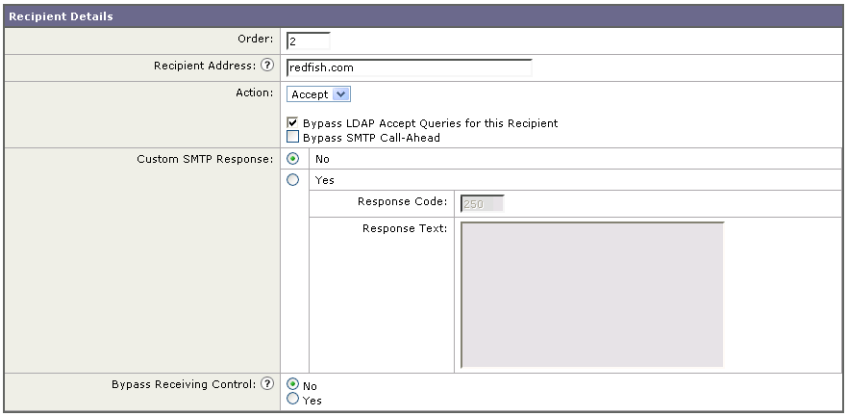
- RAT へのエントリの追加
- RAT からのエントリの削除
- 既存の RAT エントリの変更
- エントリの順序の変更
- ファイルからの RAT エントリのインポート（既存のエントリの上書き）
- RAT エントリのファイルへのエクスポート

RAT は、コマンドライン インターフェイス（CLI）を使って直接編集できます。定義したリスナーの RAT をカスタマイズするには、`listenerconfig` コマンドの `edit -> rcptaccess -> new` サブコマンドを使用して、設定する各パブリック リスナーについて、許可されるローカル ドメインを RAT に追加します。詳細については、『*Cisco IronPort AsyncOS CLI Reference Guide*』を参照してください。

新しい RAT エントリの追加

ステップ 1　[受信者の追加（Add Recipient）] をクリックします。[受信者アクセステーブルに追加（Add to Recipient Access Table）] ページが表示されます。

図 5-39　RAT エントリの追加



ステップ 2　エントリの順序を選択します。

ステップ 3　受信者アドレスを入力します（有効なエントリの詳細については、受信者の定義（5-55 ページ）を参照してください）。

ステップ 4　受信者を許可するか拒否するかを選択します。

ステップ 5　オプションで、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できます（特別な受信者での LDAP 許可のバイパス（5-56 ページ）を参照）。

ステップ 6　このエントリに対してカスタム SMTP 応答を使用する場合は、[Custom SMTP Response] で [Yes] を選択します。応答コードとテキストを入力します。

ステップ 7　オプションで、スロットリングをバイパスすることを設定できます（特別な受信者でのスロットリングのバイパス（5-56 ページ）を参照）。そのためには、[Bypass Receiving Control] で [Yes] を選択します。

ステップ 8　変更を送信し、保存します。

RAT エントリの削除

ステップ 1　削除する各エントリの [Delete] 列の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　チェックボックスをオンにしたエントリが RAT から削除されます。

ステップ 4　変更を保存します。

RAT エントリの変更

ステップ 1　[Recipient Access Table Overview] で RAT エントリをクリックします。[Edit Recipient Access Table] ページが表示されます。

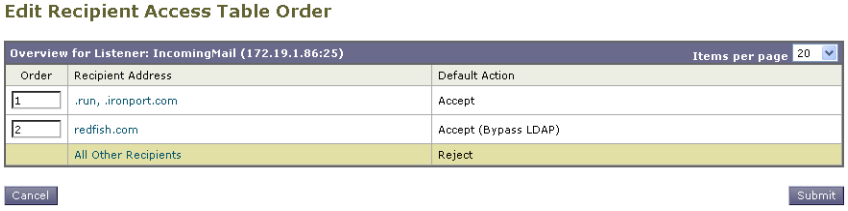
ステップ 2　エントリを変更します。

ステップ 3　変更を保存します。

RAT エントリの順序の変更

ステップ 1　[順番を編集（Edit Order）] をクリックします。[受信者アクセステーブルの順序を編集（Edit Recipient Access Table Order）] ページが表示されます。

図 5-40　RAT エントリの順序の変更



ステップ 2　[順番（Order）] 列の値を調整して順序を変更します。

ステップ 3　変更を保存します。

RAT エントリのエクスポート

ステップ 1　[RAT をエクスポート（Export RAT）] をクリックします。[受信者アクセステーブルのエクスポート（Export Recipient Access Table）] ページが表示されます。

図 5-41　RAT エントリのエクスポート

ステップ 2　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。

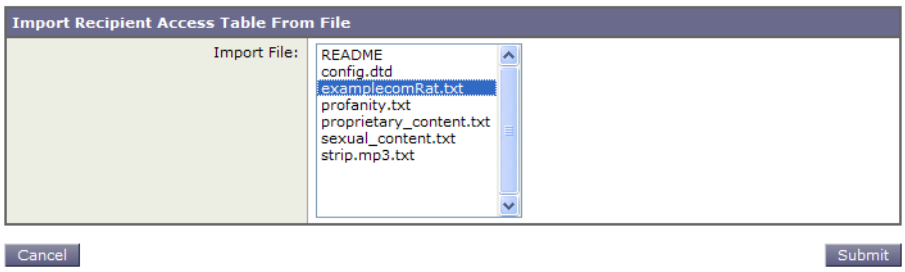
ステップ 3　変更を送信し、保存します。

RAT エントリのインポート

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

ステップ 1　[RAT をインポート（Import RAT）] をクリックします。[受信者アクセステーブルのインポート（Import Recipient Access Table）] ページが表示されます。

図 5-42　RAT エントリのエクスポート



ステップ 2　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 3　[送信（Submit）] をクリックします。既存の RAT 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 4　[インポート（Import）] をクリックします。

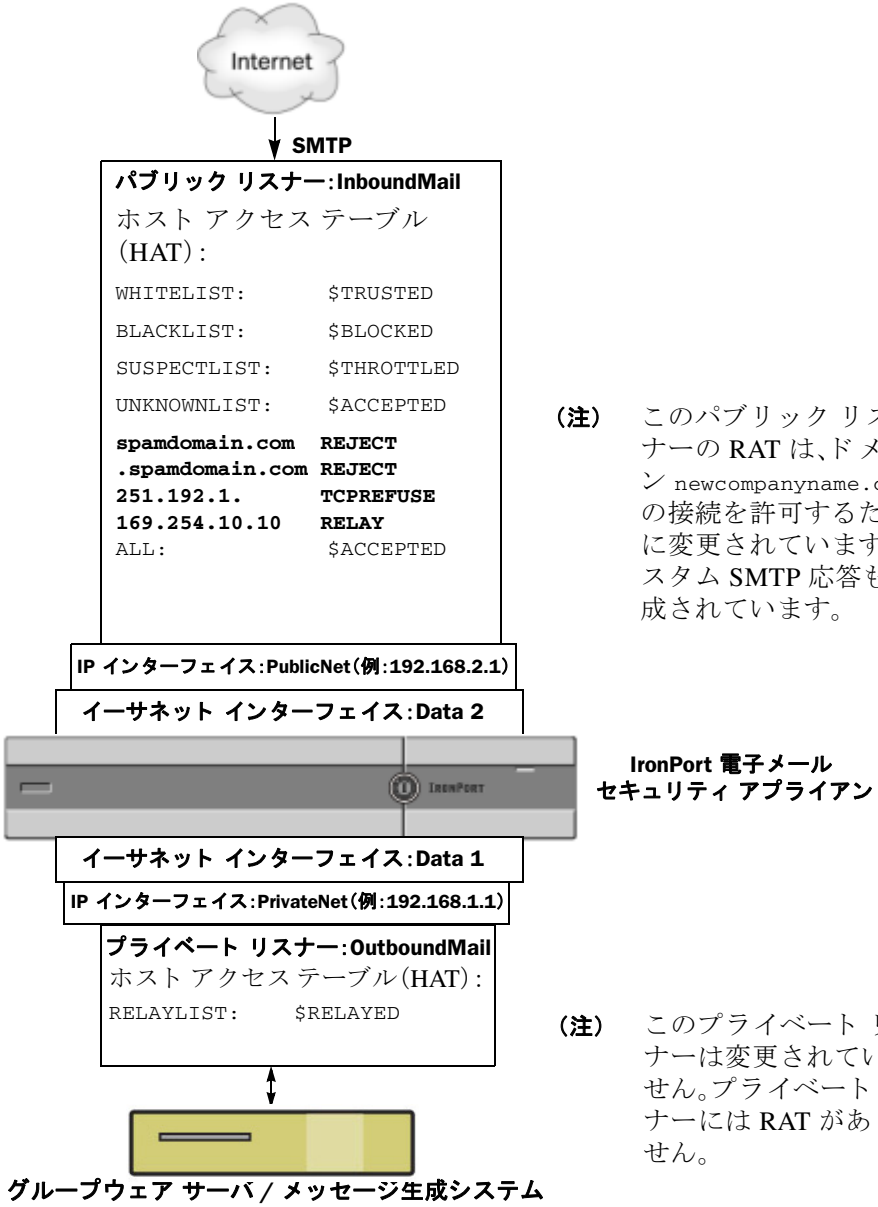
ステップ 5　変更を保存します。

ファイル内に「コメント」を配置できます。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
```

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 5-43　　パブリック リスナーの RAT の編集

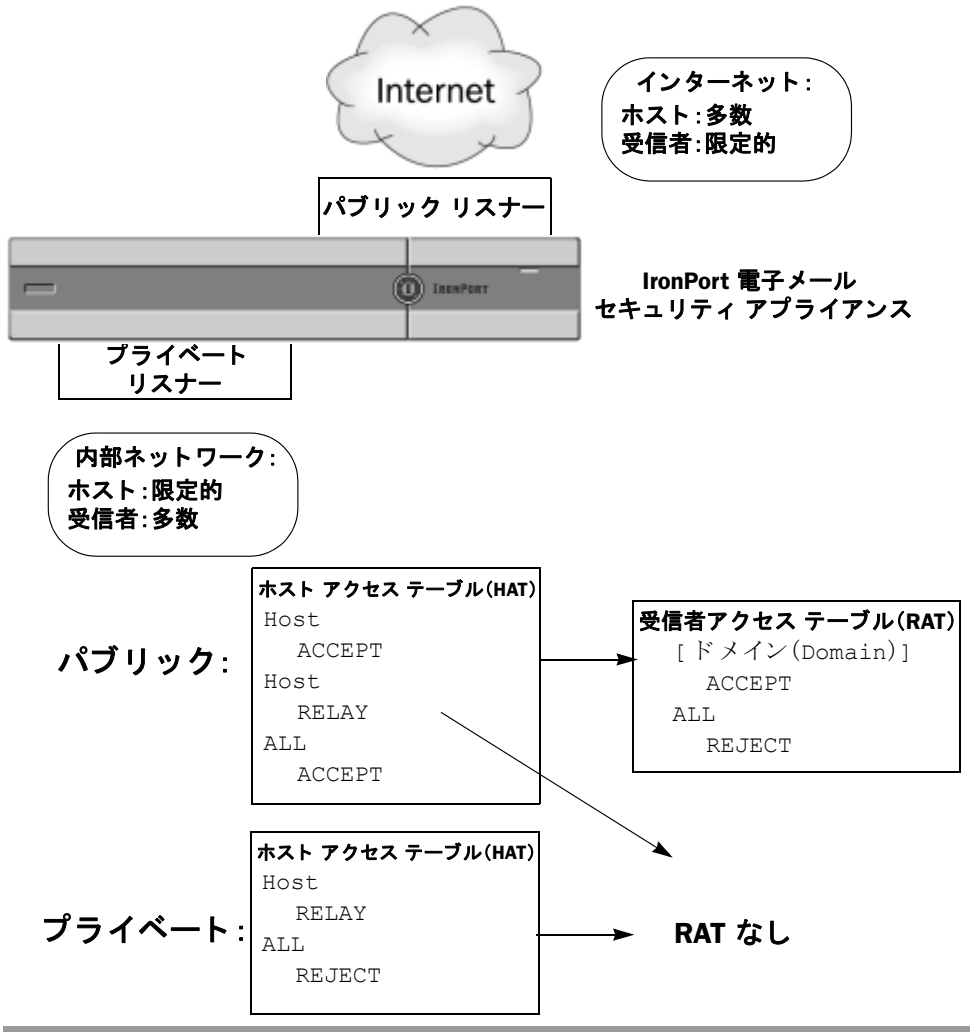


（注） このパブリック リスナーの RAT は、ドメイン `newcompanyname.com` の接続を許可するために変更されています。カスタム SMTP 応答も作成されています。

（注） このプライベート リスナーは変更されていません。プライベート リスナーには RAT がありません。

図 5-44 は、図 5-4 に示した図を展開したものであり、リスナーの HAT（該当する場合）と RAT の処理シーケンスと、それぞれのデフォルト値が含まれています。

図 5-44　　パブリック リスナーとプライベート リスナー



CHAPTER 6

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、Cisco IronPort アプライアンス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ための 1 つの包括的なダッシュボードです。本リリースよりも前のリリースでは、アンチスパムおよびアンチウイルス設定は、リスナー単位で行われていました。つまり、ポリシーは、メッセージの受信者または送信者に基づいてではなく、IP アドレスの受信リスナーに基づいて適用されていました。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、リスナーの作成および設定方法について説明します。

電子メール セキュリティ マネージャを使用すると、感染フィルタ機能、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、個別のインバウンドおよびアウトバウンド ポリシーを介して、受信者または送信者単位で管理できます。

GUI の [メールポリシー(Mail Policies)] メニュー(または CLI の `policyconfig` コマンド)を使用して、着信または発信メール ポリシーを作成および管理します。メール ポリシーは、次の機能の特定の設定にマッピングされるユーザの特定のセットとして定義されます(エンベロープ受信者、エンベロープ送信者、From: ヘッダーまたは Reply-To: ヘッダー)。

- アンチスパム スキャン
- アンチウイルス スキャン
- アウトブレイク フィルタ
- コンテンツ フィルタ
- RSA メール データ損失防止ポリシー (アウトバウンド メールのみ)

ユーザは、電子メール アドレス、電子メール ドメインまたは LDAP グループ クエリーにより定義できます。

ユーザベース ポリシーの概要

電子メール セキュリティ マネージャのユーザベース ポリシーを使用すると、組織内のすべてのユーザのさまざまな、また個別のセキュリティ ニーズを満たすポリシーを作成できます。

たとえば、この機能を使用すると、次の条件を適用するポリシーをすぐに作成できます。

- Cisco IronPort Anti-Spam スキャンを、販売部へのすべての電子メールでディセーブルにします。エンジニアリング部では、陽性と疑わしいスパム メッセージと問題のないマーケティング メッセージの件名にタグを付け、陽性と判定されたスパムをドロップする中程度のポリシーを適用してイネーブルにします。また、人事部では、陽性と疑わしいスパム メッセージと問題のないマーケティング メッセージを検疫して、陽性と判定されたスパムをドロップする、積極的なポリシーを適用してアンチスパム スキャンをイネーブルにします。
- 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。
- エンジニアリング部宛てのメッセージのウイルスをスキャンおよび修復しますが、アドレス jobs@example.com に送信されるすべてのメッセージの感染添付ファイルをドロップします。
- RSA メール データ損失防止（DLP）を使用してすべての発信メッセージをスキャンし、機密情報として扱う必要のある情報が含まれているかどうか確認します。条件と一致するメッセージは、検疫され、法務部にブラインド カーボン コピーで送信されます。

（注）　DLP に RSA Enterprise Manager を使用している場合、送信メール ポリシーは Enterprise Manager の DLP ポリシーに割り当てられます。詳細については、RSA Enterprise Manager（11-27 ページ）を参照してください。

- 着信メッセージに MP3 添付ファイルが含まれている場合は、メッセージを隔離し、ネットワーク オペレーション センターに電話をかけてメッセージを取得する手順を記載したメッセージを目的の受信者に送信します。このようなメッセージは 10 日後に有効期限が切れます。
- エグゼクティブ スタッフからのすべての発信メールへの免責事項を企業の最新のタグ ラインに含め、広報部からのすべての発信メールに異なる「将来の見込みに関する」免責事項を含めます。
- すべての着信メッセージの感染フィルタ機能をイネーブルにして、example.com へのリンクを含むメッセージまたはファイル拡張子が .dwg の添付ファイルを含むメッセージのスキャンをバイパスします。

（注）　コンテンツ ディクショナリ、免責事項、および通知テンプレートは、コンテンツ フィルタによって参照される前に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（14-1 ページ）を参照してください。

着信メッセージと発信メッセージ

電子メール セキュリティ マネージャでは、2 つのポリシー テーブルが定義されます。1 つは、HAT ポリシーにより「Accept」動作として規定される送信ホストからのメッセージ用のテーブルで、もう 1 つのテーブルは、HAT「Relay」動作と見なされる送信ホスト用のテーブルです。前者のテーブルは、*着信*ポリシー テーブルで、後者は、*発信*ポリシー テーブルです。

- *着信メッセージ*は、任意のリスナーの ACCEPT HAT ポリシーに一致する接続から受信されるメッセージです。
- *発信メッセージ*は、任意のリスナーの 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。

（注）　特定のインストールでは、Cisco IronPort 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 IronPort C10/100 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。

多くの構成では、着信テーブルはパブリック、発信テーブルはプライベートと考えることができますが、両方とも単一のリスナーで使用できます。特定のメッセージで使用されるポリシー テーブルは、メッセージの方向、つまり、送信者アドレスか受信者アドレスかどうか、またはインターネットへの発信かイントラネットへの着信かどうかに依存しません。

これらのテーブルを管理するには、GUI の [メールポリシー（Mail Policies）] > [受信メールポリシー（Incoming Mail Policies）] ページまたは [送信メールポリシー（Outgoing Mail Policies）] ページ、あるいは CLI の `policyconfig` コマンドを使用します。メール システムの管理などを担当する委任管理者に個々のメール ポリシーを割り当てることができます。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。

（注）　DLP スキャニングは、発信メッセージでのみ実行できます。

ポリシー マッチング

着信メッセージがシステムのリスナーにより受信されると、システムで設定されているリスナーの数に関係なく、各メッセージ受信者は、いずれか 1 つのテーブルのポリシーとマッチングされます。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マッチングされます。

  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、イネーブルにされている場合、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 マップおよびメッセージ フィルタ機能は、エンベロープ受信者アドレスを再作成できます。これにより、電子メール セキュリティ マネージャ（アンチスパム、アンチウイルス、コンテンツ フィルタおよび感染フィルタ）のポリシーとのメッセージのマッチングに影響を与えることがあります。

- 送信者アドレスは、次のアドレスとマッチングされます。
  - 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が有効

各受信者は、該当するテーブル（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。

メッセージの各受信者に対して、最初に一致したポリシーが適用されます。受信者がいずれのポリシーにも一致しない場合、その受信者には、自動的に、テーブルのデフォルト ポリシーが適用されます。

マッチングが送信者アドレス（またはアップグレードにより作成される特殊な「リスナー」ルール（以下を参照））に基づいて行われる場合、メッセージの残りの受信者全員に、そのポリシーが適用されます。（これは、メッセージごとに存在する送信者またはリスナーが 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 6-1 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照合されます。

表 6-1　　ポリシー マッチングの例

順序	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@
	Default Policy	（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 のメッセージには、ポリシー 3 で定義されているアンチスパム、アンチウイルス、ウイルス感染フィルタおよびコンテンツ フィルタが適用されますが、受信者 john@example.com のメッセージには、ポリシー 5 で定義されている設定が適用されます。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（6-5 ページ）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 には、ポリシー 1 で定義されているアンチスパム、アンチウイルス、感染フィルタおよびコンテンツ フィルタが適用され、受信者 larry@example.com には、ポリシー 2 で定義されているアンチスパム、アンチウイルス、感染フィルタおよびコンテンツ フィルタが定義されます。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（マッチング ポリシーによる）は、受信者が複数あるメッセージに、受信者に基づいた異なるポリシーを個別に適用できるメカニズムです。

各受信者は、該当する電子メール セキュリティ マネージャ 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。

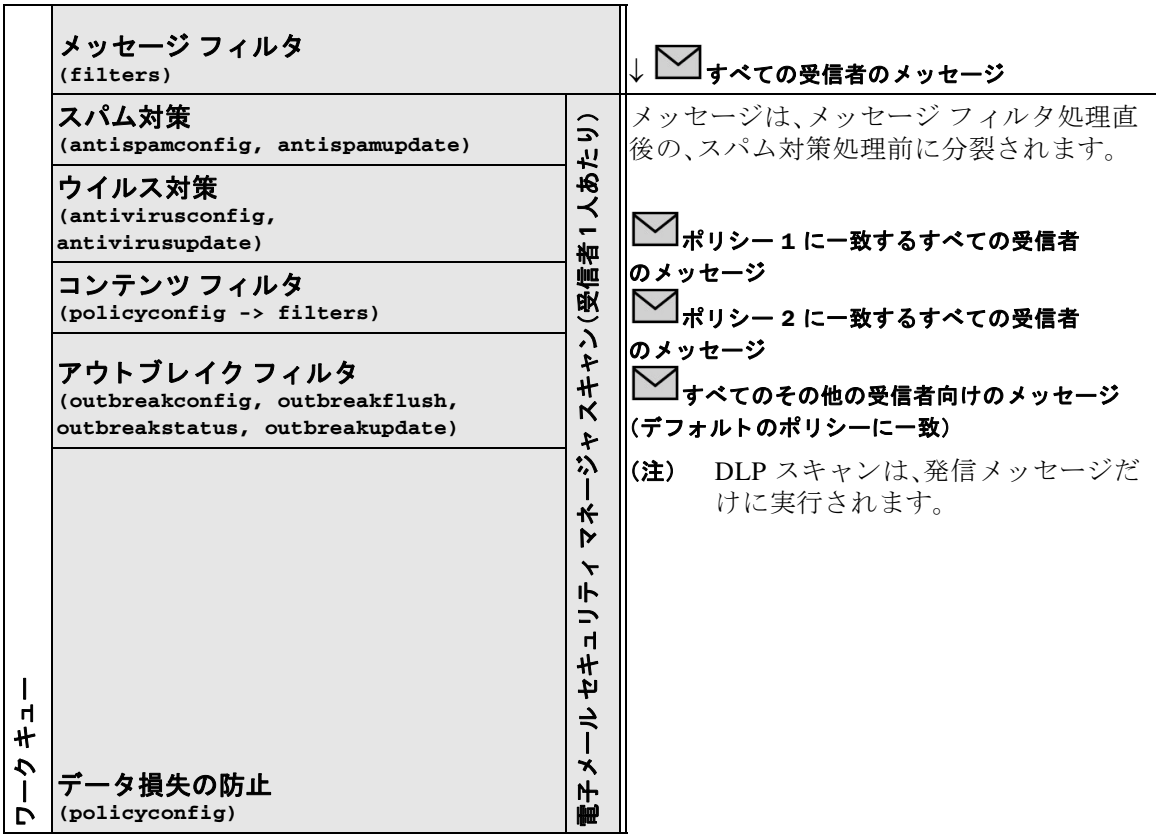
メッセージに一致する各ポリシーは、これらの受信者に新しいメッセージを作成します。このプロセスが、*「メッセージ分裂」*と定義されます。

- 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 6-2 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。

（注） Email DLP スキャンは、発信メッセージだけで使用できます。

表 6-2　　電子メール パイプラインでのメッセージ分裂



(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

分裂メッセージごとの反復処理はパフォーマンスに影響を与えるため、シスコは、電子メール セキュリティ マネージャの着信および発信メール ポリシー テーブルを使用して、*管理例外*単位でポリシー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。

ポリシーの内容

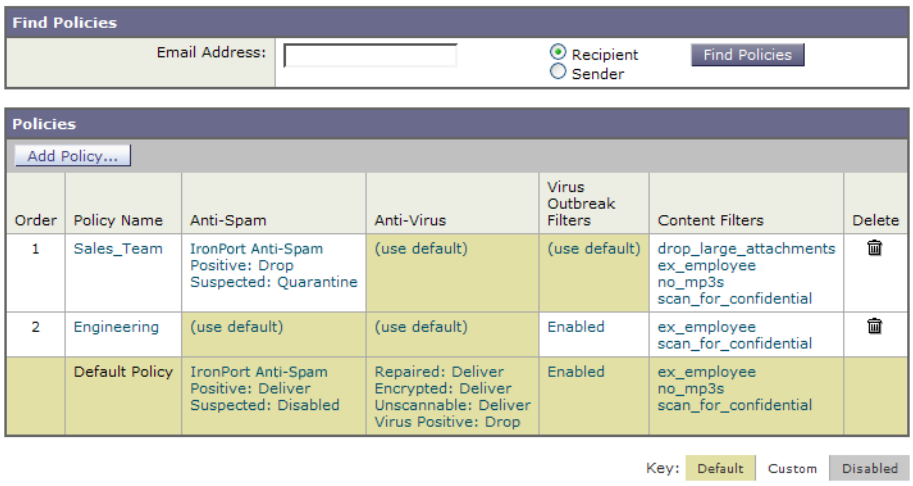
電子メール セキュリティ マネージャ テーブルは、ユーザの特定のグループ（エンベロープ受信者、エンベロープ送信者、From: ヘッダーまたは Reply-To: ヘッダー）に対して着信または発信メッセージをマッチングし、これらを次の機能の特定の設定にマッピングします。

- Anti-Spam スキャン：詳細については、アンチスパム（9-1 ページ）を参照してください。
- アンチウィルス スキャン：詳細については、アンチウイルス（8-1 ページ）を参照してください。
- コンテンツ フィルタ：詳細については、コンテンツ フィルタの概要（6-8 ページ）を参照してください。
- アウトブレイク フィルタ

  Cisco IronPort の感染フィルタ機能は、従来のアンチウイルスおよびアンチスパム セキュリティ サービスが更新されて検出できるまで、疑わしいメッセージを検疫することで、新種ウイルス、フィッシング、詐欺の発生に対する「第一の防衛ライン」を提供する予測セキュリティ サービスです。特定の受信者に対してアウトブレイク フィルタを有効または無効にすることができます。また、電子メール セキュリティ マネージャでアウトブレイク フィルタ機能をバイパスするファイル タイプを定義することもできます。詳細については、第 10 章、アウトブレイク フィルタを参照してください。
- データ消失防止：詳細については、第 11 章、データ損失の防止を参照してください。

図 6-1 に、ポリシーで定義されたユーザを特定のアンチスパム、アンチウイルス、感染フィルタ、DLP およびコンテンツ フィルタ設定にマッピングする GUI の電子メール セキュリティ マネージャを示します。

図 6-1　　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



コンテンツ フィルタの概要

電子メール セキュリティ マネージャ ポリシーでは、受信者または送信者単位でメッセージに適用されるコンテンツ 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。

通常のメッセージ フィルタと同様に、各コンテンツ フィルタに名前を定義します。この名前は、使用される着信または発信メール ポリシー テーブルで一意でなければなりません。各着信および発信メール ポリシー テーブルには、それぞれ独自のコンテンツ フィルタの「マスター リスト」があります。順序は、テーブル単位（着信または発信）で定義されます。ただし、各個別のポリシーは、実行される特定のフィルタを決定します。

通常のメッセージ フィルタ（アンチスパムおよびアンチウイルス スキャンの前に適用される）とは異なり、コンテンツ フィルタは、CLI および GUI の両方で設定できます。GUI には、「ルール ビルダ」ページがあります。このページでは、コンテンツ フィルタを構成する条件およびアクションを簡単に作成できます。電子メール セキュリティ マネージャの着信または発信メール ポリシー テーブルは、特定のポリシーに適用される順序で、イネーブルにされるコンテンツ フィルタを管理します。表 6-3 に、コンテンツ フィルタの作成に使用できる *条件* を示します。表 6-4 に、コンテンツ フィルタの定義に使用できる非最終および最終 *アクション* を示します。コンテンツ フィルタは、条件およびアクションにより構成されます。表 6-5 に、コンテンツ フィルタの作成に使用できるアクション変数を示します。

メール ポリシーでコンテンツ フィルタを編集してイネーブルにすることが可能な委任管理ユーザ ロールを指定できます。委任管理者のコンテンツ フィルタに関するアクセス権限の詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Common Administrative Tasks」の章を参照してください。

コンテンツ フィルタの条件

コンテンツ フィルタでの条件の指定はオプションです。

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 ディクショナリの用語に対して指定できます。

また、「スマート ID」を使用して、データのパターンを識別することもできます。スマート ID は、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
- 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

パターンが検出される回数の最小しきい値の指定、およびスマート 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。

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」）のいずれで結合するかを選択できます。

表 6-3　　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。
メッセージ本文または添付ファイル	[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。 [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。 [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、<*ディクショナリ名*> 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。 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（14-2 ページ）を参照してください。 [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。 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。

表 6-3　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	[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。 [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。 [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、<*ディクショナリ名*> 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。 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（14-2 ページ）を参照してください。 [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。 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。
メッセージ サイズ	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で、ヘッダーと添付ファイルも含みます。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。

表 6-3　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	[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 `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。 [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。 [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、<*ディクショナリ名*> 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（14-2 ページ）を参照してください。 [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 ディクショナリの一致回数に対して指定できます。
添付ファイルのファイル情報	[ファイル名（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。 [ファイルタイプ（File type）]：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）。 [MIME タイプ（MIME 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。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）。 [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含まれてい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。

表 6-3　コンテンツ フィルタの条件（続き）

条件	説明
添付ファイル保護	[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）]: （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）。 [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）]:
件名ヘッダー（Subject Header）	[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。 [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、<*ディクショナリ名*> 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（14-2 ページ）を参照してください。
その他のヘッダー	[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。 [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。 [ヘッダーの値がコンテント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、<*ディクショナリ名*> 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（14-2 ページ）を参照してください

表 6-3　コンテンツ フィルタの条件（続き）

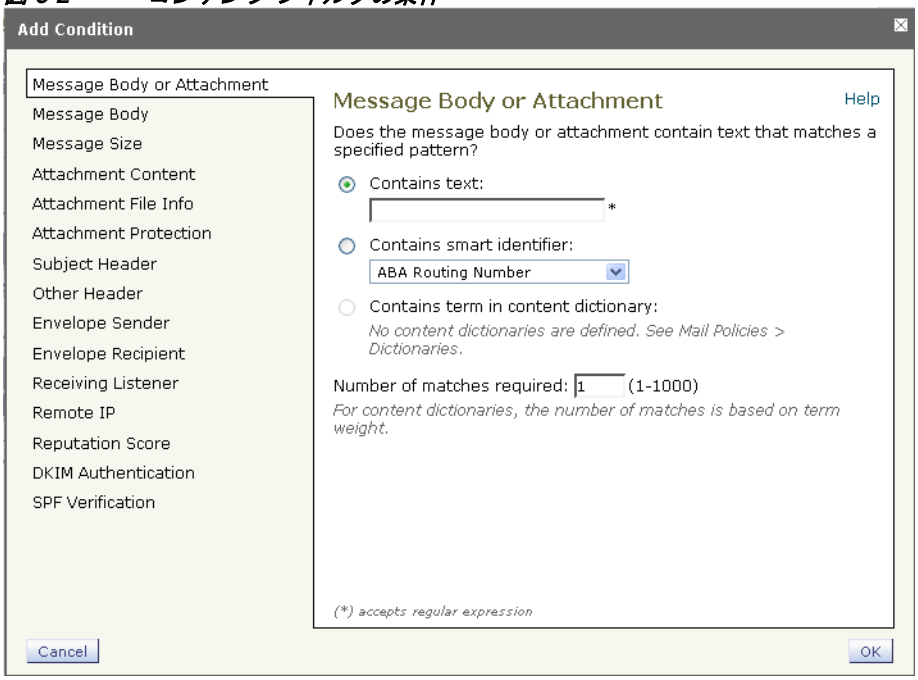
条件	説明
エンベロープ送信者	[エンベロープ送信者（Envelope Sender）]：エンベロープ送信者（Envelope From, <MAIL FROM>）が指定したパターンと一致しているか。 [LDAP グループに一致（Matches LDAP group）]：エンベロープ送信者（つまり、Envelope From、<MAIL FROM>）が、特定の LDAP グループに含まれるかどうかを判別します。 [コンテンツ辞書の単語を含む（Contains term in content dictionary）]：エンベロープ送信者に、*<ディクショナリ名>* という名前のコンテンツ ディク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（14-2 ページ）を参照してください。
グループ内エンベロープ（Envelope Recipient）	[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。 [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。 [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、*<ディクショナリ名>* 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（14-2 ページ）を参照してください。 **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 人でも検出されれば、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。 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。
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ある必要があります。

表 6-3　コンテンツ フィルタの条件（続き）

条件	説明
リモート 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（5-21 ページ）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	送信者の SenderBase レピュテーション スコアの値。[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。
DKIM 認証	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 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。

（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（14-2 ページ）を参照してください。

図 6-2　コンテンツ フィルタの条件



コンテンツ フィルタのアクション

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、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、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 6-4　　コンテンツ フィルタのアクション

アクション	説明
検疫	[隔離（Quarantine）]。いずれかのシステム検疫エリアに保持されるメッセージにフラグを付けます。 [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。
配信時の暗号化	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。 [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（12-8 ページ）を参照してください。 [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 IronPort 暗号化アプライアンスまたはホステッド キー サービスと併用します。 [件名（Subject）]: 暗号化されたメッセージの件名です。デフォルト値は `$Subject` です。

表 6-4　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	[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。 [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。 [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、<*ディクショナリ名*> 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。 [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 ディクショナリの一致回数に対して指定できます。 [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。

表 6-4　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	[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。 [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。 [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。 [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。 [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。 [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。
免責条項文の追加	[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）。 [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）。 **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。 詳細については、免責事項テンプレート（14-19 ページ）を参照してください。
アウトブレイク フィルタによるスキャンのスキップ	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。

表 6-4　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**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 6-4　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	**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。** [ヘッダー名（Header name）]：新規または既存のヘッダーの名前。 [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。 [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。 [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。 [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。
メッセージ タグの追加	RSA メール 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 メール 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、DLP ポリシー（11-11 ページ）を参照してください。
ログ エントリの追加	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。

表 6-4　コンテンツ フィルタのアクション（続き）

アクション	説明
暗号化して今すぐ配信（最終アクション）	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。 [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（12-8 ページ）を参照してください。 [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 IronPort 暗号化アプライアンスまたはホステッド キー サービスと併用します。 [件名（Subject）]：暗号化されたメッセージの件名です。デフォルト値は `$Subject` です。
バウンスする（最終アクション）	メッセージを送信者に戻します。
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。

図 6-3　GUI のコンテンツ フィルタのアクション

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は *アクション変数*と呼ばれます。Cisco IronPort 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 6-5　　アクション変数

変数	構文	説明
すべてのヘッダー（All Headers）	`$AllHeaders`	メッセージ ヘッダーに置き換えられます。
本文サイズ（Body Size）	`$BodySize`	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）	`$Date`	現在の日付（MM/DD/YYYY 形式）に置き換えられます。
ドロップされたファイル名（Dropped File Name）	`$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）	`$dropped_filenames`	`$filenames` 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）	`$dropped_filetypes`	`$filetypes` 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）	`$envelopefrom` or `$envelopesender`	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）	`$EnvelopeRecipients`	メッセージのエンベロープ受信者すべて（Envelope To、<RCPT TO>）に置き換えられます。
ファイル名（File Names）	`$filenames`	メッセージの添付ファイルのファイル名のカンマ区切リストに置き換えられます。
ファイルサイズ（File Sizes）	`$filesizes`	メッセージの添付ファイル サイズのカンマ区切りリストに置き換えられます。
ファイルタイプ（File Types）	`$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。
フィルタ名（Filter Name）	`$FilterName`	処理されるフィルタの名前に置き換えられます。
GMT 日時（GMTimeStamp）	`$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。
HAT グループ名（HAT Group Name）	`$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。

表 6-5　アクション変数（続き）

変数	構文	説明
メールフローポリシー（Mail Flow Policy）	`$Policy`	メッセージのインジェクト時に、送信者に適用した HAT ポリシーの名前に置き換えられます。事前に定義されているポリシー名が使用されていない場合、文字列「`>Unknown<`」が挿入されます。
一致した内容（Matched Content）	`$MatchedContent`	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。一致した内容は、コンテンツ ディクショナリ マッチ、スマート ID または正規表現との一致になります。
ヘッダー（Header）	`$Header['`*`string`*`']`	元のメッセージに一致するヘッダーが含まれる場合、引用符付きヘッダーの値に置き換えられます。二重引用符が使用される場合もあります。
ホストネーム	`$Hostname`	Cisco IronPort 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）	`$MID`	メッセージを内部で識別するために使用するメッセージ ID（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 $Header を使用します）。
受信リスナー（Receiving Listener）	`$RecvListener`	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）	`$RecvInt`	メッセージを受信したインターフェイスのニックネームに置き換えられます。
リモート IP アドレス（Remote IP Address）	`$RemoteIP`	メッセージを Cisco IronPort 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）	`$remotehost`	メッセージを Cisco IronPort アプライアンスに送信したシステムのホスト名に置き換えられます。
SenderBase レピュテーション スコア	`$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。
Subject	`$Subject`	メッセージの件名に置き換えられます。
時刻（Time）	`$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。

実際の例（GUI）

この例では、次のタスクを示し、電子メール セキュリティ マネージャの機能について説明します。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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電子メール セキュリティ マネージャのアンチスパム、アンチウイルス、感染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（9-1 ページ）
- アンチウイルス（8-1 ページ）
- アウトブレイク フィルタ（10-1 ページ）
- 一般的な管理タスク、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』

電子メール セキュリティ マネージャへのアクセス

新しくインストールされた、またはアップグレードされたシステムでは、[Mail Policies] タブをクリックして、電子メール セキュリティ マネージャにアクセスします。デフォルトでは、[Incoming Mail Policies] テーブルが表示されます。

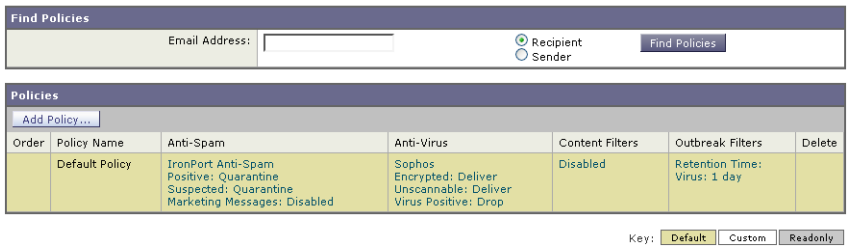
新規システムでは、システム セットアップ ウィザードのすべての手順を完了して、Cisco IronPort Anti-Spam、Sophos または McAfee Anti-Virus およびアウトブレイク フィルタをイネーブルにするように選択した場合、図 6-4 のような [着信メールポリシー（Incoming Mail Policies）] ページが表示されます。

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 IronPort スパム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
  - 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 IronPort スパム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 6-4　[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



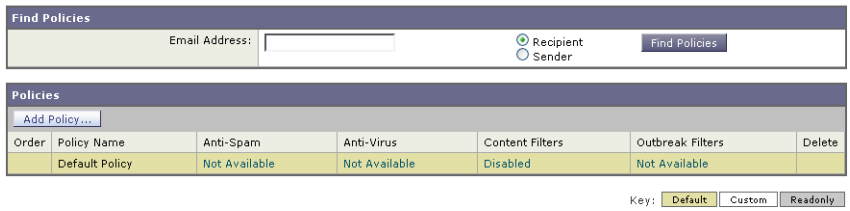
（注） この例では、着信メール ポリシーは、Cisco IronPort スパム隔離がイネーブルにされている場合のデフォルトのアンチスパム設定を使用します。

[有効(Enabled)]、[無効(Disabled)]、[利用不可(Not Available)]

[Email Security Manager] 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 6-5 を参照してください。

図 6-5　使用できないセキュリティ サービス



デフォルト ポリシーの編集：アンチスパム設定

電子メール セキュリティ マネージャの各行は、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、電子メール セキュリティ マネージャの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ます。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。

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。図 6-6 に示す [Anti-Spam Settings] ページが表示されます。

（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）] をクリックしてすべての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。

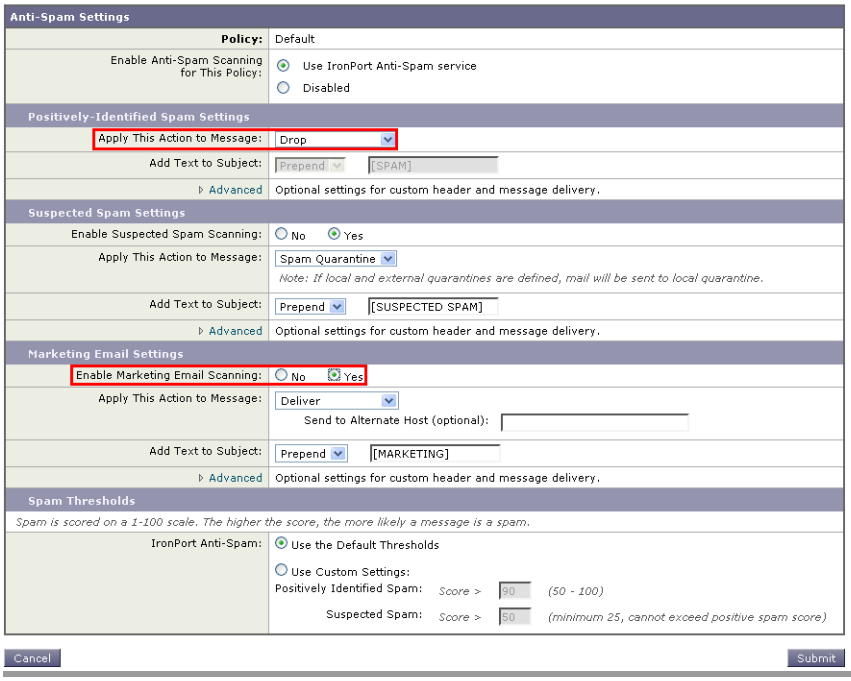
イネーブルにされている場合、デフォルト アクションでは、テキスト [MARKETING] が件名の前に追加され、問題のないマーケティング メッセージが配信されます。

[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。[Incoming Mail Policies table] ページが再表示されます。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 6-6　[スパム対策設定(Anti-Spam Settings)] ページ



新しいポリシーの作成

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。

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。

[Add Users] ページが表示されます。

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。詳細については、最初に一致したものが有効(6-4 ページ)を参照してください。

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、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Common Administrative Tasks」の章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（6-3 ページ）を参照してください）。図 6-7 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

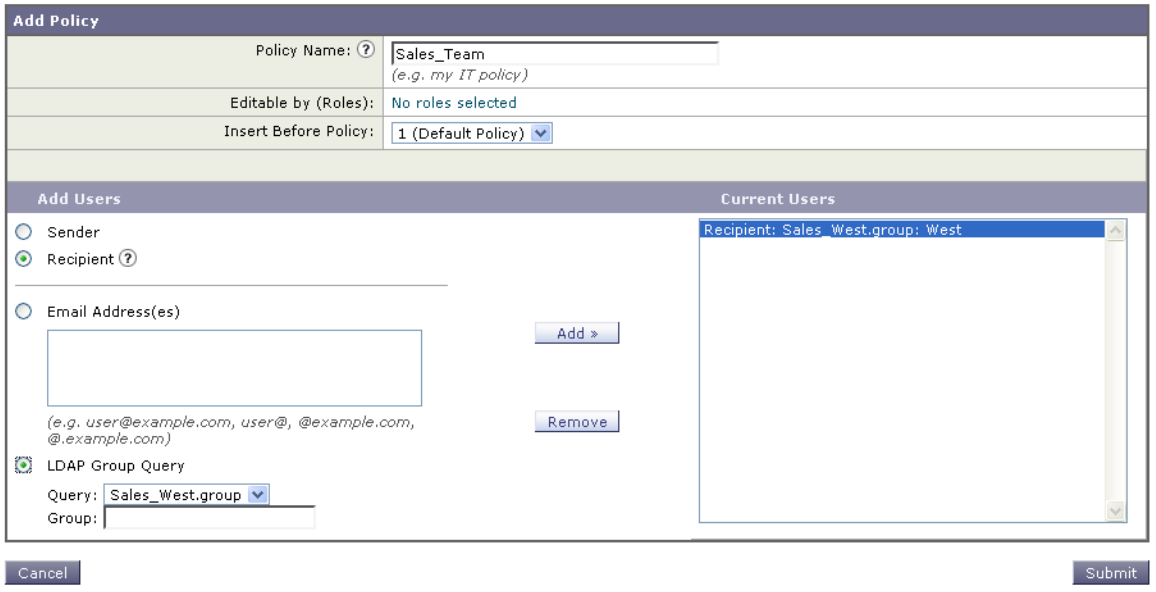
（注）　ユーザの入力は、AsyncOS の GUI および CLI の両方で、大文字と小文字が区別されます。たとえば、ユーザの受信者 `Joe@` を入力すると、`joe@example.com` に送信されるメッセージが一致します。

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 IronPort アプライアンスを設定して、LDAP サーバをクエリし、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、電子メール セキュリティ マネージャのメール ポリシーのユーザを定義できます。

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

図 6-7　　ポリシーのユーザの定義



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て含めることができます。

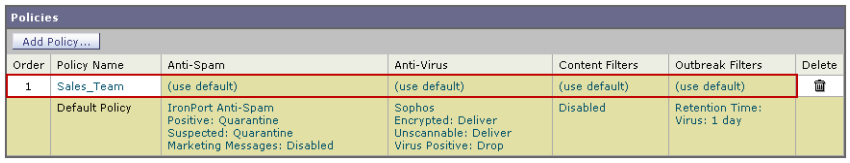
[削除(Remove)] ボタンを使用すると、定義されているユーザを現在のユーザのリストから削除できます。

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。

新しいポリシーが追加された状態で [Mail Policies] ページが表示されます。

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。

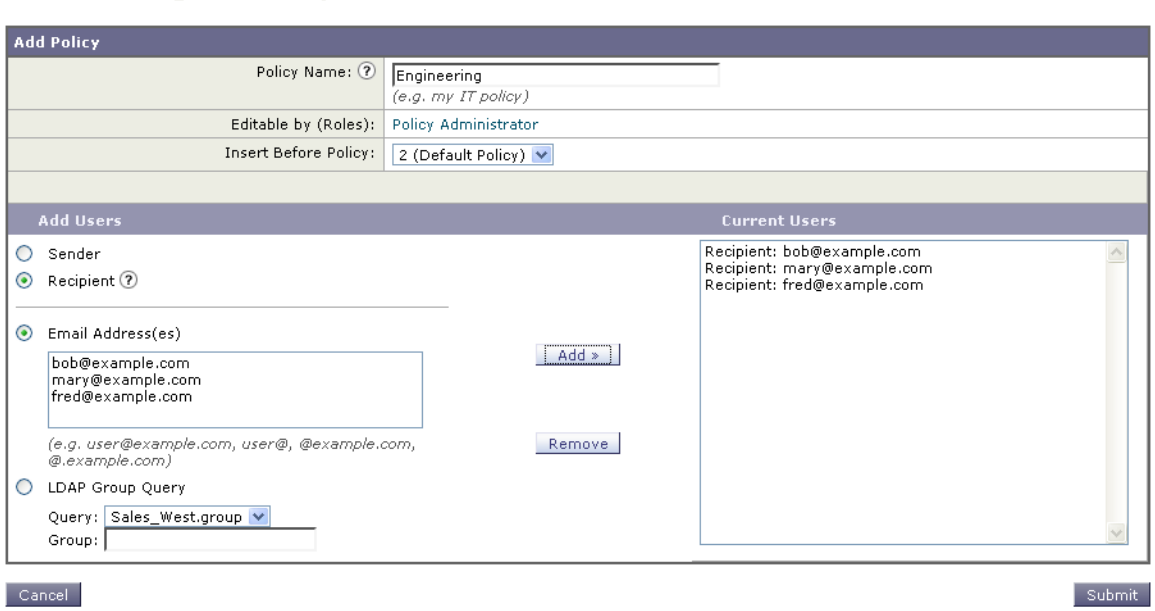
図 6-8　新しく追加されたポリシー:販売グループ



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 6-9　エンジニアリング チームのポリシーの作成

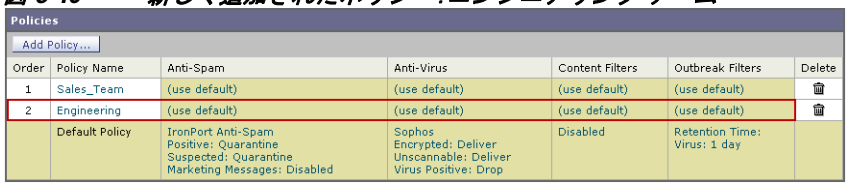


ステップ 8　エンジニアリング ポリシーのユーザの追加が完了したら、[送信(Submit)] をクリックします。

新しいポリシーが追加された状態で [Mail Policies] ページが表示されます。図 6-10 を参照してください。

ステップ 9　変更を保存します。

図 6-10　新しく追加されたポリシー：エンジニアリング チーム



（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。

カスタム 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（デフォルト ポリシーの編集：アンチスパム設定（6-25 ページ）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 IronPort スパム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（9-1 ページ）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。

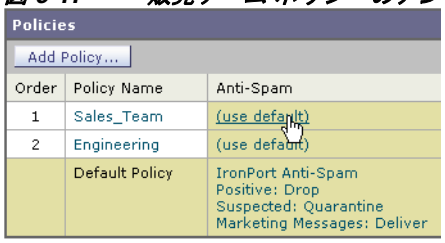
  アウトブレイク フィルタの設定の詳細については、アウトブレイク フィルタ（10-1 ページ）を参照してください。

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。

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（[スパム対策（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 6-11　販売チーム ポリシーのアンチスパム設定の編集



アンチスパムの設定ページが表示されます。

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 IronPortスパム対策を使用（Use Cisco IronPort Anti-Spam）] に変更します。

[Cisco IronPort スパム対策サービスを使用（Use Cisco IronPort 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　[スパム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 [スパム隔離（Spam Quarantine）] に変更します。

（注）　[Cisco IronPort スパム隔離（Cisco IronPort 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、[なし（None）] をクリックします。

Cisco IronPort スパム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。

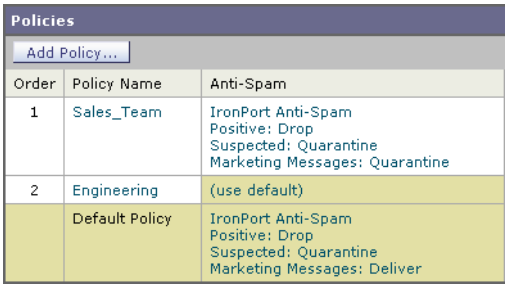
ステップ 7　[マーケティング メールの設定（Marketing Email Settings）] セクションで、[はい（Yes）] をクリックして、問題のない送信元からのマーケティング メールのスキャンをイネーブルにします。

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、[スパム隔離（Spam Quarantine）] を選択します。

ステップ 9　変更を送信し、保存します。

販売ポリシーの変更が反映された状態で、[Incoming Mail Policies] ページが表示されます。図 6-12 を参照してください。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 6-12　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



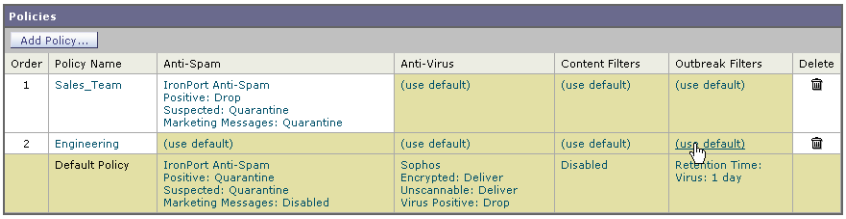
この時点では、スパムの疑いがあり、その受信者が販売チーム ポリシーで定義されている LDAP クエリーと一致するメッセージは、Cisco IronPort スパム隔離エリアに配信されます。

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。

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 6-13　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



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 IronPort 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と 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 を書き変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。

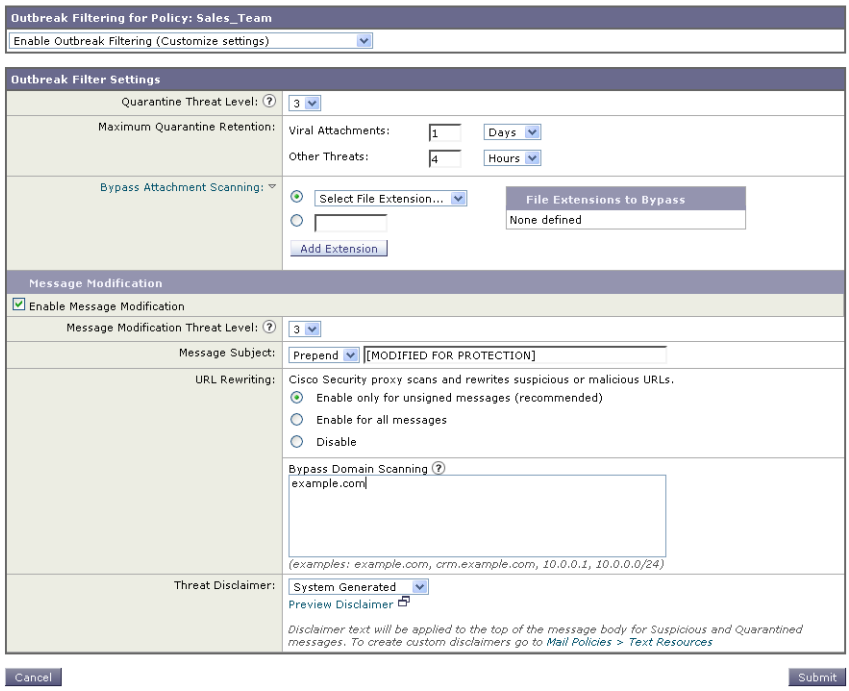
ステップ 7　[ドメインのスキャンをバイパス（Bypass Domain Scanning）] フィールドに example.com と入力します。

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。

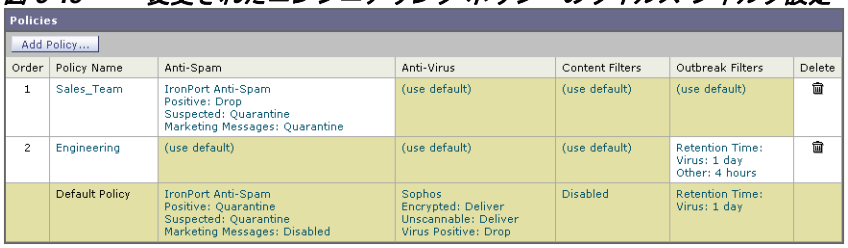
図 6-14　アウトブレイク フィルタの設定



ステップ 9　変更を送信し、保存します。

エンジニアリング ポリシーの変更が反映された状態で、[Incoming Mail Policies] ページが表示されます。図 6-15 を参照してください。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 6-15　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



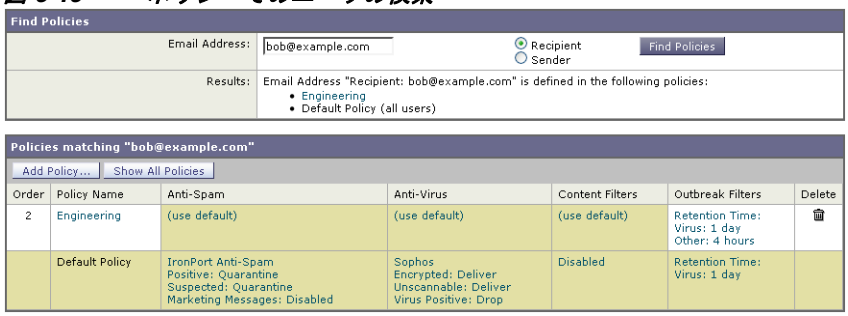
この時点では、ファイル拡張子が dwg である添付ファイルを含む任意のメッセージ、および受信者がエンジニアリング チーム ポリシーで定義されている受信者とマッチングする任意のメッセージは、アウトブレイク フィルタ スキャンをバイパスし、処理を続行します。example.com ドメインへのリンクを含むメッセージは、Cisco セキュリティ プロキシを介してリダイレクトするようにリンクを修正されることはなく、疑わしいと見なされません。

電子メール セキュリティ マネージャのポリシーのユーザの検索

[ポリシー検索（Find Policies）] ボタンを使用して、電子メール セキュリティ マネージャの [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 6-16　ポリシーでのユーザの検索



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。

電子メール セキュリティ マネージャ：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 6-6（6-34 ページ）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 6-6　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	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
ウイルス対策	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
ウィルス 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

新しいコンテンツ フィルタの作成

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。

ステップ 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。文字列が見つかると、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、メッセージがポリシー隔離エリアに送信されます。

ステップ 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。

ステップ 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。

Confidential のスキャン

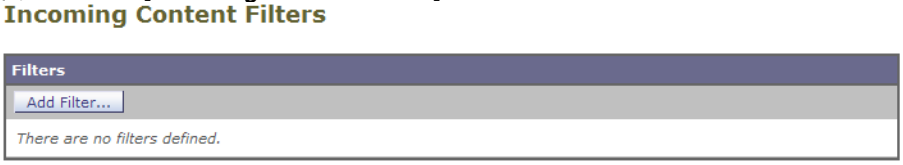
最初の例のコンテンツ フィルタには、1 つの条件と 2 つのアクションが含まれます。

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。

[Incoming Content Filters] ページが表示されます。新しくインストールされたシステムまたはアップグレードされたシステムの場合、デフォルトで、コンテンツ フィルタは定義されていません。

図 6-17　[Incoming Content Filters] ページ



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。

[Add Content Filter] ページが表示されます。

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 番めのアクションが表示されます。

ステップ 19　変更を送信し、保存します。

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、電子メール セキュリティ マネージャ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。

MP3 添付ファイルなし

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。

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。

[Add Content Filter] ページが表示されます。

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。

[Add Content] 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 11　変更を送信し、保存します。

（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

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。

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。

[Add Content Filter] ページが表示されます。

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択します。

（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（14-2 ページ）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))] を選択して、[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と、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　変更を送信し、保存します。

[Incoming Content Filters] ページが表示され、新しく追加されたコンテンツ フィルタが示されます。

個々のポリシーへのコンテンツ フィルタのイネーブル化および適用

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 6-18　[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

Filters

Add Filter...

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。
- 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。

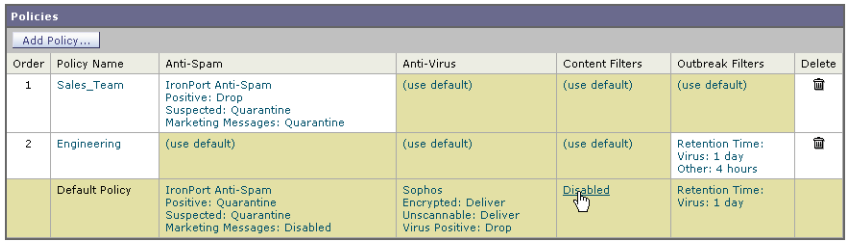
リンクをクリックして、個々のポリシーに対してコンテンツ フィルタをイネーブルにして選択します。

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 ポリシーおよび新しいポリシーの作成(6-26 ページ)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。

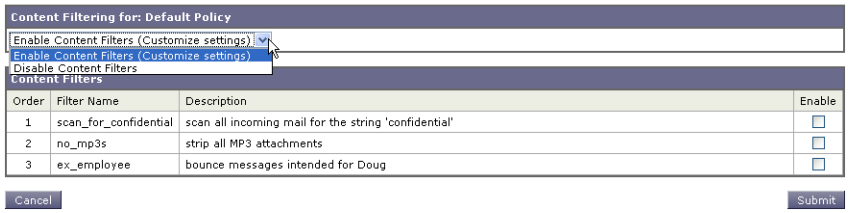
ステップ 2　デフォルト ポリシー行のコンテンツ フィルタ セキュリティ サービス([コンテンツフィルタ(Content Filters)] 列)のリンクをクリックします。図 6-19 を参照してください。

図 6-19　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



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 6-20　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



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(6-8 ページ)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。

[Incoming Mail Policies] ページが表示され、テーブルが更新され、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が示されます。

図 6-21　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

「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。

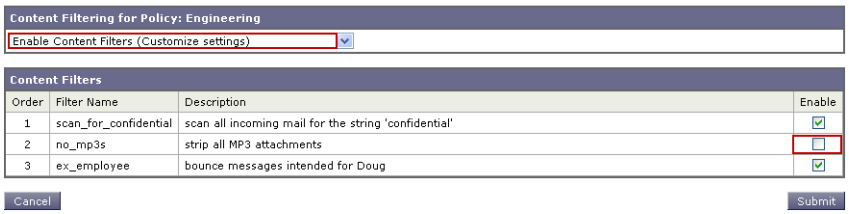
ステップ 1　エンジニアリング チーム ポリシー行の [コンテンツフィルタセキュリティサービス(Content Filters security service)]([コンテンツフィルタ(Content Filters)] 列)のリンクをクリックします。

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。

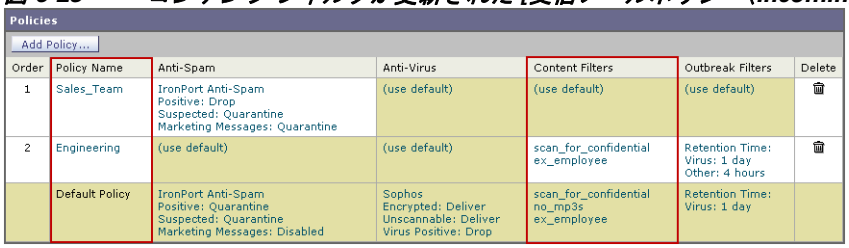
図 6-22　　コンテンツ フィルタの選択解除



ステップ 4　[送信（Submit）] をクリックします。

[Incoming Mail Policies] ページが表示され、テーブルが更新され、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が示されます。

図 6-23　　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）]



ステップ 5　変更を保存します。

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。

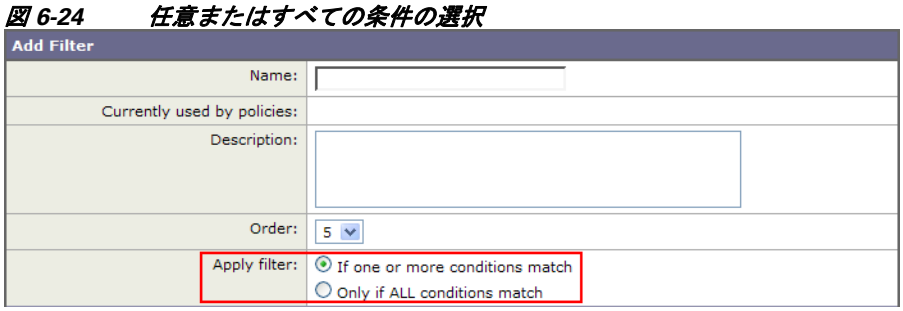
GUI でのコンテンツ フィルタの設定に関する注意事項

- 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（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。

- 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 6-24　任意またはすべての条件の選択

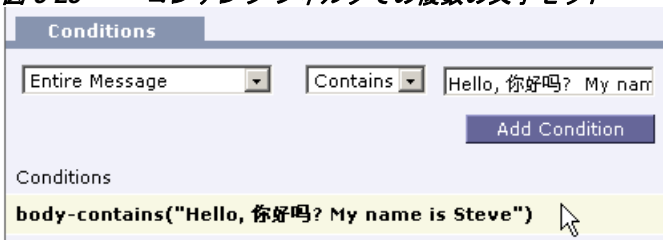


- 「benign」コンテンツ フィルタを作成して、メッセージ分裂およびコンテンツ フィルタをテストできます。たとえば、唯一のアクションが「配信」であるコンテンツ フィルタを作成できます。このコンテンツ フィルタは、メール処理に影響を与えませんが、このフィルタを使用して、電子メール セキュリティ マネージャ ポリシー処理が、システムの他の要素（たとえば、メール ログ）に影響を与えているかテストできます。
- 逆に、着信または発信コンテンツ フィルタの「マスター リスト」の概念を使用して、アプライアンスにより処理されるすべてのメールのメッセージ処理に即時に影響を与える、非常に優れた、広範囲に及ぶコンテンツ 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、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Quarantines」の章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）、システム隔離とのメール 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。「メッセージ全体（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 6-25　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 6-26　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

CHAPTER 7

レピュテーション フィルタリング

Cisco IronPort アプライアンスは、独自の階層化された方法により、電子メール ゲートウェイでスパムを阻止します。スパム制御の最初の階層である評価フィルタリングを使用すると、Cisco IronPort SenderBase™ 評価サービスにより決定される送信者の信頼性に基づいて、電子メールの送信者を分類し、ご使用の電子メール インフラストラクチャへのアクセスを制限できます。2 番めの防衛階層であるスキャン（次の章で説明します）では、Cisco IronPort Anti-Spam™ テクノロジーが使用されています。評価フィルタリングとアンチスパム スキャンを組み合わせることにより、現在使用可能なものの中では最高水準の効率と性能を持つアンチスパム ソリューションが実現されています。

Cisco IronPort アプライアンスを使用すると、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に対して、アンチスパム スキャンを一切実施しないでエンドユーザに直接配信するポリシーを非常に簡単に作成できます。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 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。

Cisco IronPort アプライアンスの提供する独自の二層スパム対策により、高性能で今までにない柔軟性を備えた、企業の電子メール ゲートウェイ管理および保護が可能になります。

（注） AsyncOS 7.6 以降、E メール セキュリティ アプライアンスでは、SenderBase レピュテーション サービスを使用するにはスパム対策システム機能キーが必要です。

評価フィルタリング

SenderBase 評価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、正確かつ柔軟に陽性と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。SenderBase 評価サービスは、特定の送信元からのメッセージがスパムである可能性に基づいてスコアを返し、メール フロー モニタ機能で客観的データを示すことで、電子メール管理者が電子メールの送信元をより詳しく知ることができるようにします（『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Using Email Security Monitor」を参照）。SenderBase レピュテーション サービスは、Cisco IronPort 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おり、これを使用するには、サービス上でアンチスパムを有効にする必要があります。

SenderBase 評価サービスを使用することで、次のことが実行できます。

- スパムの低減

SenderBase 評価サービスを使用することで、企業は接続 IP アドレスに基づいて既知のスパムを特定し、スパムがゲートウェイに到達した時点で、組織がそのスパムをブロックできるようにします。これにより、使用されているアンチスパム スキャン エンジンまたはその他すべてのコンテンツに基づいたフィルタの有効性が高まります。

- スパム フラッドに対する保護

SoBig などのウイルスまたは「当て逃げ」スパム攻撃により、メッセージ量が予期せず急激に増加する場合があります。特定の送信者が大量の送信を開始した場合、SenderBase 評価サービスはグローバルなアフィリエイト ネットワークを介してこれを検出し、陰性スコアを割り当てることができます。Cisco IronPort アプライアンスは、このスコアを使用して、送信者に対して許可する 1 時間あたりの受信者数をただちに制限できます（アウトブレイク フィルタ（10-1 ページ）も参照してください）。

- スループットの向上

Cisco IronPort アプライアンスは、ただちに既知のスパムを拒否し、既知の良好なメッセージをコンテンツ フィルタを通過するようにルーティングすることで、システム負荷を低減し、メッセージのスループットを増加できます。

評価フィルタリング：Cisco IronPort SenderBase 評価サービス

Cisco IronPort SenderBase 評価サービス（`http://www.senderbase.org` から入手可能）は、送信者の ID に関する客観的なデータを提供することにより、電子メール管理者が受信メールの流れをよりよく管理できるようにするサービスです。SenderBase 評価サービスは電子メールの信用レポート サービスに似ています。正当な送信者とスパム送信元を区別するために企業が使用できるデータが提供されます。SenderBase 評価サービスは、Cisco IronPort アプライアンスの GUI に直接組み込まれており、ここで提供される客観的データを使用して、Unsolicited Commercial Email（UCE）を送信している IP アドレスの信頼性を識別したり、その IP アドレスをブロックしたり、またはビジネス パートナー、顧客、またはその他すべての重要な送信元からの正規着信電子メールの信頼性を確認したりできます。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。

（注）　Cisco IronPort 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 ホストを識別する必要があります。詳細については、着信リレー（9-21 ページ）を参照してください。

SenderBase 評価サービスには、次のような主要な要素があります。

- スプーフが不可能

電子メール送信者の信頼性は、電子メールの送信者の IP アドレスに基づいています。SMTP は、TCP/IP を使用した双方向のカンバセーションであるため、IP アドレスを「スプーフ」することはほぼ不可能です。提示される IP アドレスは、メッセージを送信しているサーバにより、実際に制御されているものである必要があります。

- 包括

SenderBase 評価サービスは、慎重に選択された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だけでなく、クレーム率およびメッセージ量の統計情報などの SenderBase Affiliate ネットワークからのグローバル データも使用して、特定の送信元からのメッセージがスパムである可能性を決定します。

- 設定可能

SenderBase 評価サービスは、ブラックリストやホワイトリストのような単純な yes/no の決定を返す他の「ID ベースの」スパム対策技術とは異なり、その送信元からのメッセージがスパムである確率に基づいて段階的な応答を返します。これにより、スパムをブロックするしきい値を独自に設定したり、SenderBase 評価スコアに基づいて送信者を自動的にさまざまなグループに割り当てたりできます。

SenderBase レピュテーション スコア（SBRS）

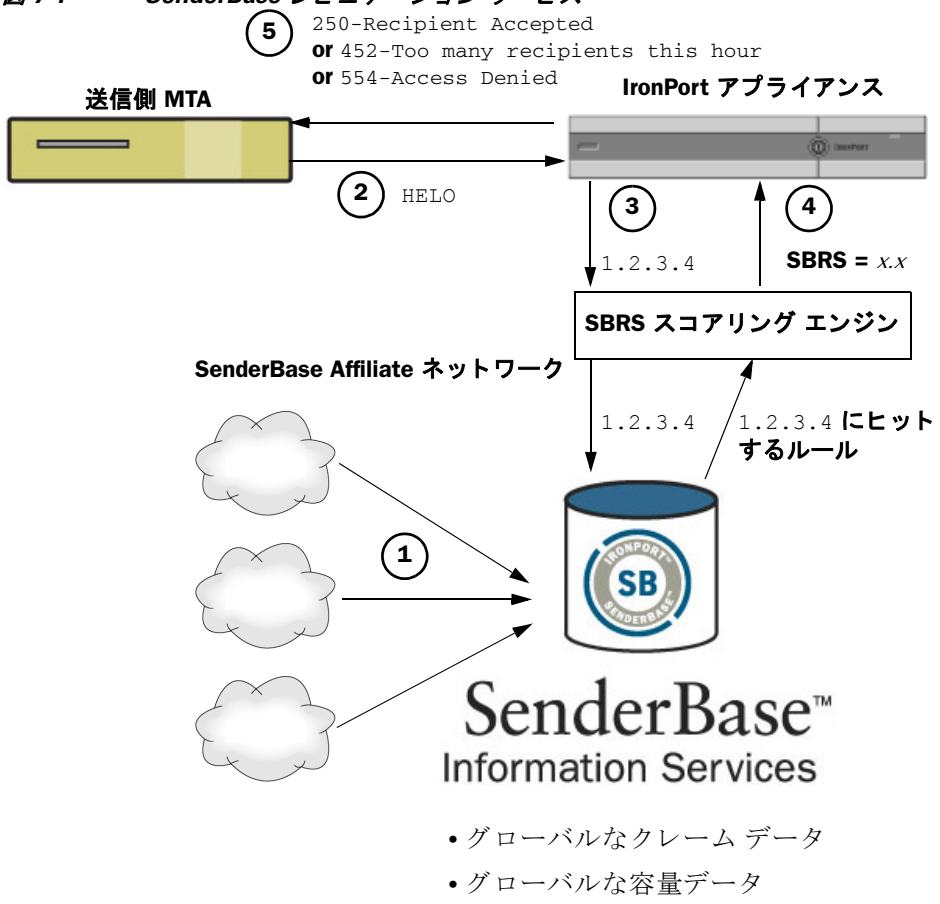
SenderBase レピュテーション スコア（SBRS）は、SenderBase レピュテーション サービスからの情報に基づいて、IP アドレスに割り当てられる数値です。SenderBase レピュテーション サービスは、25 個を超える公開ブラックリストおよびオープン プロキシ リストのデータを集約し、さらにこのデータを SenderBase のグローバル データと組み合わせて、次のように -10.0 ～ +10.0 のスコアを割り当てます。

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 IronPort 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、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Using Message Filters to Enforce Email Policies」の章の「SenderBase Reputation Rule」および「Bypass Anti-Spam System Action」を参照してください）。

図 7-1　SenderBase レピュテーション サービス



ステップ 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。

ステップ 2　送信 MTA により、Cisco IronPort アプライアンスとの接続が開始されます。

ステップ 3　Cisco IronPort 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。

ステップ 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。

ステップ 5　Cisco IronPort 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 評価フィルタの実装

Cisco IronPort レピュテーション フィルタ テクノロジーは、Cisco IronPort 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 パイプラインについて（4-1 ページ）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。世界中の 2000 社から送信された既知の良好なメールは自動的にスパム フィルタを避けてルーティングされるため、誤検出の可能性が低減されます。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 7-2　　レピュテーション フィルタリングの例

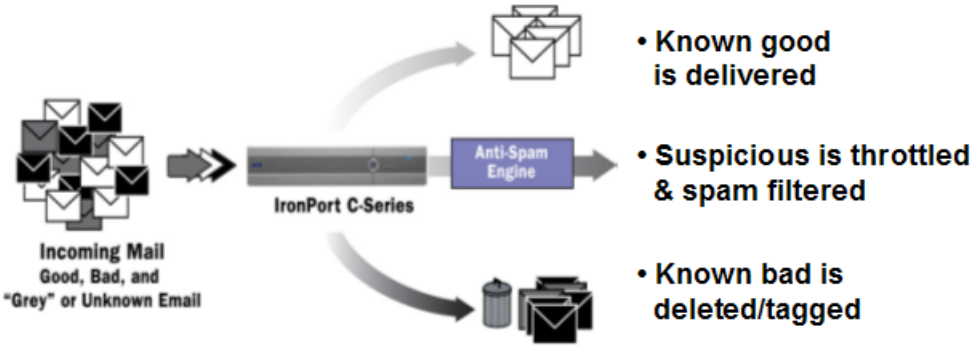


表 7-2 に、SenderBase 評価フィルタリングを実装する場合に推奨されるポリシー セットのリストを示します。企業の目的に応じて、Conservative、Moderate、Aggressive のいずれかの方法を選択できます。

（注） シスコではスロットリングが推奨ですが、SenderBase 評価サービスを実装するもう 1 つの方法として、スパムの疑いのあるメッセージの件名行を変更する方法があります。このようにするには、表 7-1 に示す次のメッセージ 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 評価スコアが -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 評価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）。

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。

表 7-1　　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\\}");

      }

 }

.
```

評価フィルタリングの設定

評価フィルタリングは、[Mail Policies] > [HAT Overview] ページで設定します。詳細については、SenderBase 評価フィルタの実装（7-4 ページ）を参照してください。

コンサーバティブ

Conservative 方式では、SenderBase 評価スコアが -4.0 未満のメッセージをブロックし、-4.0 ～ -2.0 のメッセージをスロットリングし、-2.0 ～ +6.0 のメッセージにデフォルト ポリシーを適用し、+6.0 を超えるスコアのメッセージに信頼されたポリシーを適用します。この方式を使用すると、false positive 率をほぼ 0 に抑えながら、良好なシステム パフォーマンスを実現できます。

適度

Moderate 方式では、SenderBase 評価スコアが -3.0 未満のメッセージをブロックし、-3.0 ～ 0 のメッセージをスロットリングし、0 ～ +6.0 のメッセージにデフォルト ポリシーを適用し、+6.0 を超えるスコアのメッセージに信頼されたポリシーを適用します。この方式を使用すると、false positive 率を非常に低くに抑えながら、良好なシステム パフォーマンスを実現できます（より多くのメールがアンチスパム処理から切り離されるため）。

アグレッシブ

Aggressive では、SenderBase 評価スコアが -2.0 未満のメッセージをブロックし、-2.0 ～ 0.5 のメッセージをスロットリングし、0 ～ +4.0 のメッセージにデフォルト ポリシーを適用し、+4.0 を超えるスコアのメッセージに信頼されたポリシーを適用します。この方式を使用すると、false positive 率がいくらか発生する可能性はありますが、ほとんどのメールをアンチスパム処理から切り離すことにより、システム パフォーマンスが最大化されます。

（注）　また、ユーザは SenderBase 評価スコアが 6.0 より大きいすべてのメッセージを、$TRUSTED ポリシーに割り当てることを推奨します。

表 7-2　SBRS を使用した評価フィルタリング実装の推奨段階的手法

ポリシー	ブラックリスト	[スロットル（Throttle）]	[デフォルト（Default）]	ホワイトリスト
コンサーバティブ	-10 ～ -4	-4 ～ -2	-2 ～ 7	7 ～ 10
適度	-10 ～ -3	-3 ～ -1	-1 ～ 6	6 ～ 10
アグレッシブ	-10 ～ -2	-2 ～ -0.5	-0.5 ～ 4	4 ～ 10

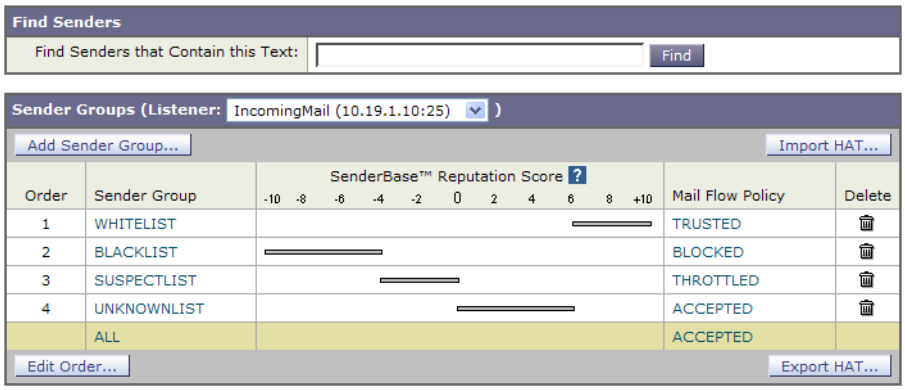
ポリシー：	特性：	適用するメール フロー ポリシー
コンサーバティブ：	誤検出はほぼ 0。良好なパフォーマンス。	**$BLOCKED**
適度：	誤検出は非常に少ない。高パフォーマンス。	**$THROTTLED**
アグレッシブ：	false positive はいくらか発生。パフォーマンスは最大。	**$DEFAULT**

次の手順では、評価フィルタリングを実装する段階的手法の概要を示します。

リスナーの HAT での評価フィルタリング実装

ステップ 1　[Mail Policies] タブで、[Host Access Table] > [HAT Overview] を選択します。[Sender Groups (Listener)] メニューからパブリック リスナーを選択します。[HAT Overview] ページに、各送信者グループの SenderBase 評価スコア設定が表示されます。

図 7-3　　送信者グループの SenderBase 評価スコア範囲リスト

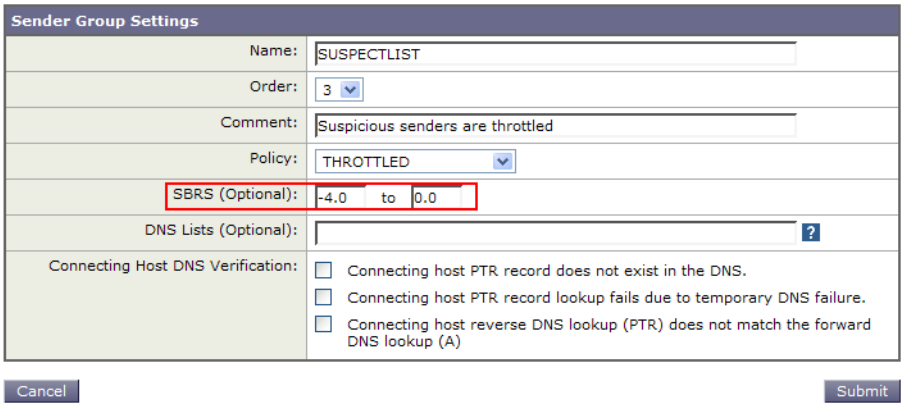


[HAT Overview] には、各送信者グループ（水平バー）に割り当てられた SenderBase 評価スコアの範囲および関連付けられたメール フロー ポリシーが表示されます。

ステップ 2　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。[Edit Sender Group] ページが表示されます。

図 7-4　　送信者グループの SBRS 範囲の変更



ステップ 3　SenderBase 評価スコアの範囲を入力して、送信者グループを定義します。任意でコメントを定義することもできます。

たとえば、「SUSPECTLIST」に -4.0 ～ 0 の範囲を入力します。構文については、SenderBase 評価スコアによって定義された送信者グループ（5-24 ページ）を参照してください。

ステップ 4　[送信（Submit）] をクリックします。

リスナーの HAT で、各グループについてステップ 2 ～ 5 を繰り返します。たとえば、*conservative* 方式の値を定義します。表 7-2 に示した Moderate または Aggressive 方式の値も定義できます。

送信者グループ	SBRS 範囲	メール フロー ポリシー
WHITELIST	6 ～ 10	TRUSTED
BLACKLIST	-10 ～ -7	BLOCKED
SUSPECTLIST	-7 ～ -2	THROTTLED
UNKOWNLIST	-2 ～ 6	ACCEPTED

（注）　リスナーの HAT で送信者グループを定義するときは、順序に注意してください（リスナーへの接続を試行する各ホストで、HAT は上から下へ順に読み込まれます。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）。シスコでは、リスナーの HAT であらかじめ定義されている送信者グループをデフォルトの順序で維持すること（つまり、RELAYLIST（C10/100 カスタマーのみ）、WHITELIST、BLACKLIST、SUSPECTLIST、UNKNOWNLIST の順）を推奨します。

ステップ 5　[変更を確定（Commit Changes）] ボタンをクリックし、必要に応じて任意のコメントを追加してから [変更を確定（Commit Changes）] をクリックして、リスナーの HAT での評価フィルタリングの実装を終了します。

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 7-3 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。

作成したポリシーは、任意の SBRS で trace コマンドを使用してテストします。Debugging Mail Flow Using Test Messages: Trace（-446 ページ）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 7-3　　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** *(recommended)* 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） $THROTTLED 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、パブリック リスナー向けの定義済みのメール フロー ポリシーへのアクセス（5-26 ページ）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 IronPort 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、および組織など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 7-5　[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 で `sbstatus` コマンドを使用しても、同じ情報を表示できます。

CHAPTER 8

アンチウイルス

Cisco IronPort アプライアンスには、Sophos, Plc 製および McAfee, Inc. 製のウイルス スキャン エンジンが統合されています。Cisco IronPort 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、メッセージのウイルスをスキャンできます。

(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 パイプラインについて (4-1 ページ) 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。

アンチウイルス スキャン

Cisco IronPort アプライアンスは、McAfee または Sophos 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。

評価キー

Cisco IronPort 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）有効にします。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 IronPort 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、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Common Administrative Tasks」にある機能キーの使用に関する項を参照してください）。

マルチレイヤ アンチウイルス 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 IronPort 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（8-5 ページ）および Sophos アンチウイルス フィルタリング（8-2 ページ）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 IronPort 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 IronPort 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 アンチウイルス フィルタリング

Cisco IronPort 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。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。

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 IronPort 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、E メール セキュリティ機能（[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（8-9 ページ）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:

- 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。
- 発見的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、E メール セキュリティ機能（[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（8-9 ページ）を参照してください。

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 スキャンを実行するには、最初に Cisco IronPort アプライアンスでウイルス スキャンをイネーブルにする必要があります。ウイルス スキャン エンジン（1 つまたは複数）をイネーブルにした後に、ウイルス スキャン エンジンを着信または発信メール ポリシーに適用できます。

概要

ウイルス スキャン エンジンは、System Setup Wizard を実行したときにイネーブルにできます。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（GUI）または `antivirusconfig` コマンド（CLI）を使用して、ウイルス スキャン エンジンのグローバル コンフィギュレーション設定をイネーブルにしたり、変更したりできます。次のグローバル設定を構成できます。

- システム全体に対してグローバルに McAfee または Sophos Anti-Virus スキャンをイネーブルにする。
- アンチウイルス スキャンのタイムアウト値を指定する。

グローバル設定ページの 2 つの値に加えて、[Service Updates] ページ（[Security Services] タブから使用できます）で、さらにアンチウイルス設定を構成できます。追加の設定には、次のようなものが含まれます。

- システムのアンチウイルス アップデートの取得方法（取得先 URL）。ウイルス定義は動的 URL からアップデートされます。厳格なファイアウォール ポリシーを適用している場合は、静的 URL からアップデートを取得するように Cisco IronPort アプライアンスを設定する必要がある場合があります。
- システムが新しいウイルス定義をチェックする頻度（チェックの間隔を何分にするか定義します）。
- 任意で、アンチウイルス アップデートを取得するプロキシ サーバをイネーブルにできます。

追加設定の構成に関する詳細については、サービスのアップデート（15-9 ページ）を参照してください。

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

ステップ 1　[Security Services] > [McAfee] を選択します。

または

[Security Services] > [Sophos] を選択します。

ステップ 2　[有効（Enable）] をクリックします。ライセンス契約書ページが表示されます。

（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　変更を送信し、保存します。

ステップ 7　これで、アンチウイルス設定を受信者ごとに構成できるようになりました。ユーザのウイルス スキャン アクションの設定(8-9 ページ)を参照してください。

(注)　アンチウイルス 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(4-7 ページ)を参照してください。

HTTP を使用した Anti-Virus アップデートの取得

デフォルトでは、Cisco IronPort 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。

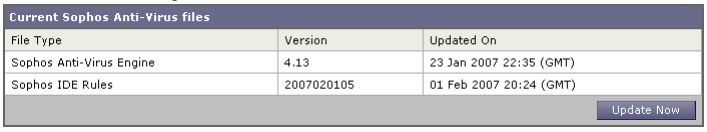
システムがタイムアウトせずに、アップデートが完了するまで待機する最大時間は、アンチウイルス アップデート間隔より 1 分短い値に定義された、動的な値です([セキュリティサービス(Security Services)] > [サービスのアップデート(Service Updates)] で定義されています)。この設定値は、接続速度の遅いアプライアンスが、完了まで 10 分を超える大きいアップデートをダウンロードする場合に役立ちます。

モニタリングおよび手動でのアップデート チェック

ライセンス契約書に同意し、グローバル設定を構成したら、[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(GUI)または `antivirusstatus` コマンド(CLI)を使用して、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。[Security Services] > [Sophos] または [McAfee Anti-Virus] ページの [Current McAfee/Sophos Anti-Virus Files] テーブルで、[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。

図 8-1　　Sophos アップデートの手動チェック



CLI では、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>
```

アップデータ 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。アップデータ 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。

ユーザのウイルス スキャン アクションの設定

Cisco IronPort 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、いったんグローバルにイネーブルにすると、電子メール セキュリティ マネージャ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 スキャンが実行されます。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。

- [ウイルスをスキャンして修復（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 スキャンが実行されます。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 スキャン エンジンにより、メッセージの添付ファイルがスキャ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（8-13 ページ）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 スキャン 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「スキャンできない」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 ヘッダーをスキャンされたメッセージに含めるかどうかは、切り替えできます。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 スキャン 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 8-2 に、ウイルス スキャン 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。GUI 設定については、図 8-3 および図 8-4 を参照してください。

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（8-11 ページ）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、ウイルス対策を設定できます。

修復されたメッセージの処理

メッセージが完全にスキャンされ、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、エンジンがスキャ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（『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Using Message Filters to Enforce Email Policies」の章の「Encryption Detection Rule」を参照）と、「暗号化された」メッセージに対するウイルス スキャン 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 スキャン 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 スキャ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」の項を設定する必要があります。

スキャンできないメッセージの処理

スキャン 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*スキャンできない*と見なされます。スキャ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、スキャ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、スキャ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（隔離およびウイルス対策スキャン（8-12 ページ）を参照））を選択します。検疫の詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Quarantines」の章を参照してください。

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（受信者宛てのみ）

（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（8-18 ページ）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。

隔離およびウイルス対策スキャン

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 8-1　アンチウイルス件名行変更のデフォルト件名行テキスト

判定	件名に追加されるデフォルトのテキスト
暗号化	[WARNING: MESSAGE ENCRYPTED]
感染している	[WARNING: VIRUS DETECTED]
修復されている	[WARNING: VIRUS REMOVED]
スキャン不可（Unscannable）	[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ャ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、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Logging」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 8-2　アンチウイルス通知のデフォルト通知

判定	通知（Notification）
修復されている	次のウイルスがメールメッセージで検出されました: <ウイルス名>（The following virus(es) was detected in a mail message: <virus name(s)>） 実行するアクション:感染している添付ファイルがドロップされました（または感染している添付ファイルが修復されました）。（Actions taken: Infected attachment dropped (or Infected attachment repaired).）
暗号化	暗号化されているため、次のメッセージをウイルス対策エンジンによって完全にスキャンできませんでした。（The following message could not be fully scanned by the anti-virus engine due to encryption.）

表 8-2　アンチウイルス通知のデフォルト通知（続き）

スキャン不可	次のメッセージをウイルス対策エンジンによって完全にスキャンできませんでした。（The following message could not be fully scanned by the anti-virus engine.）
感染している	次の修復不可能なウイルスがメールメッセージで検出されました: <ウイルス名>。（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 スキャン エンジンによってスキャ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 スキャンを回避するようにもできます。詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Using Message Filters to Enforce Email Policies」の章の「Bypass Anti-Virus System Action」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

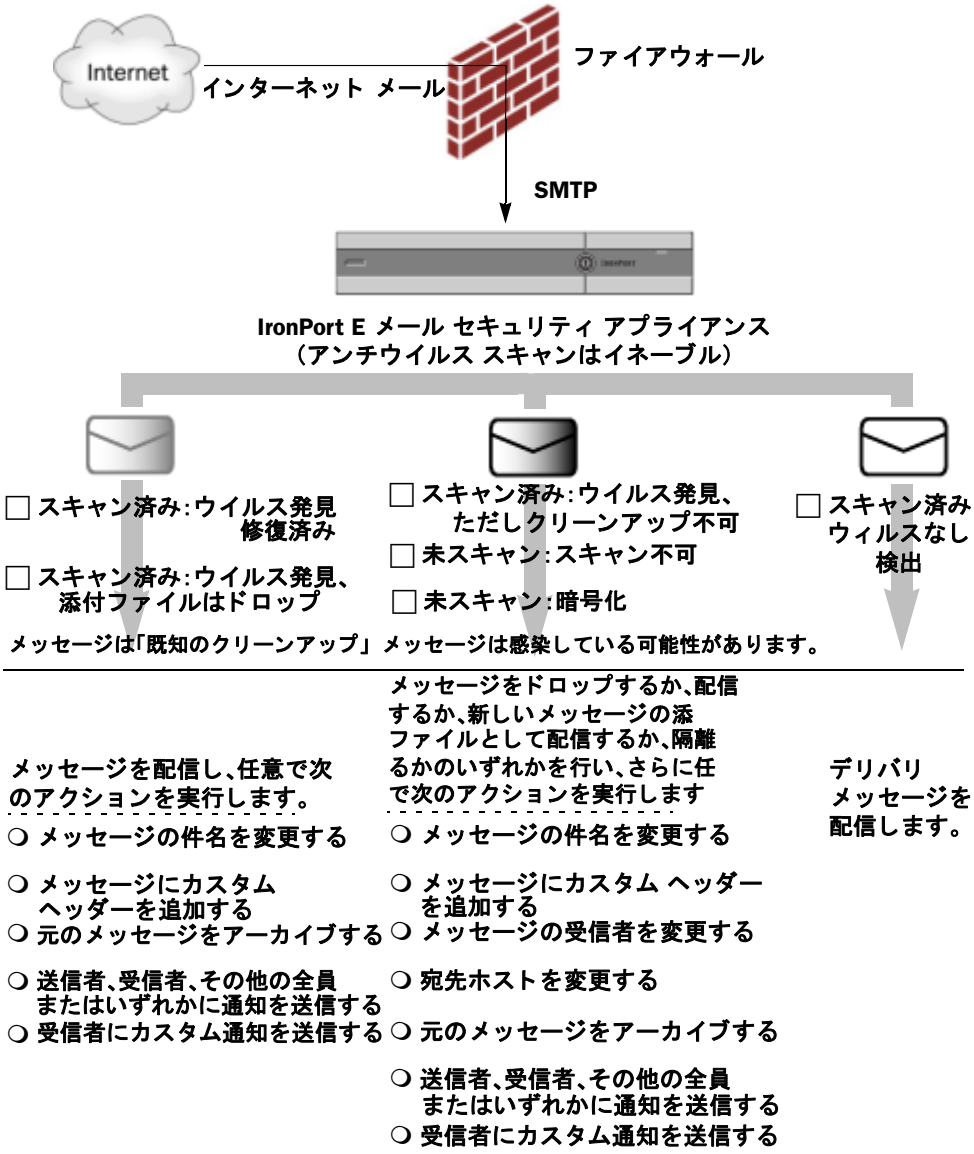
暗号化されたメッセージ、スキャンできないメッセージ、またはウイルスに感染したメッセージについて、異なる受信者または宛先ホストに通知を送信するように選択できます。[はい（Yes）] をクリックして代替アドレスまたはホストを入力します。

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（14-13 ページ）を参照してください。

図 8-2　　ウイルス スキャ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 スキャンは、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:アクセス ルールとパラメータ (5-8 ページ) を参照してください。

メール ポリシーのアンチウイルス設定の編集

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、[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。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。

ステップ 1　[Email Security Manager] の着信または発信メール ポリシー テーブルの任意の行で、アンチウイルス セキュリティ サービスへのリンクをクリックします。

図 8-3 および図 8-4 に示されている画面のような [Anti-Virus settings] ページが表示されます。

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。図 8-3 および図 8-4 に、個別のポリシー（デフォルト以外）の設定を示します。

ステップ 2　[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 3　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 4　[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（8-10 ページ）を参照してください。

ステップ 5　[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。

図 8-3 および図 8-4 に、「Engineering」という名前のこれから編集するメール ポリシーのアンチウイルス設定を示します。メッセージ処理設定（8-10 ページ）およびメッセージ処理アクションの設定の構成（8-11 ページ）を参照してください。

ステップ 6　[送信（Submit）] をクリックします。

[Mail Policies] > [Incoming Mail Policies] または [Outgoing Mail Policies] ページがリフレッシュされて、これまでの手順で選択した値が反映されます。

ステップ 7　変更を保存します。

図 8-3　　メール ポリシーのアンチウイルス設定（デフォルト以外）：1/2

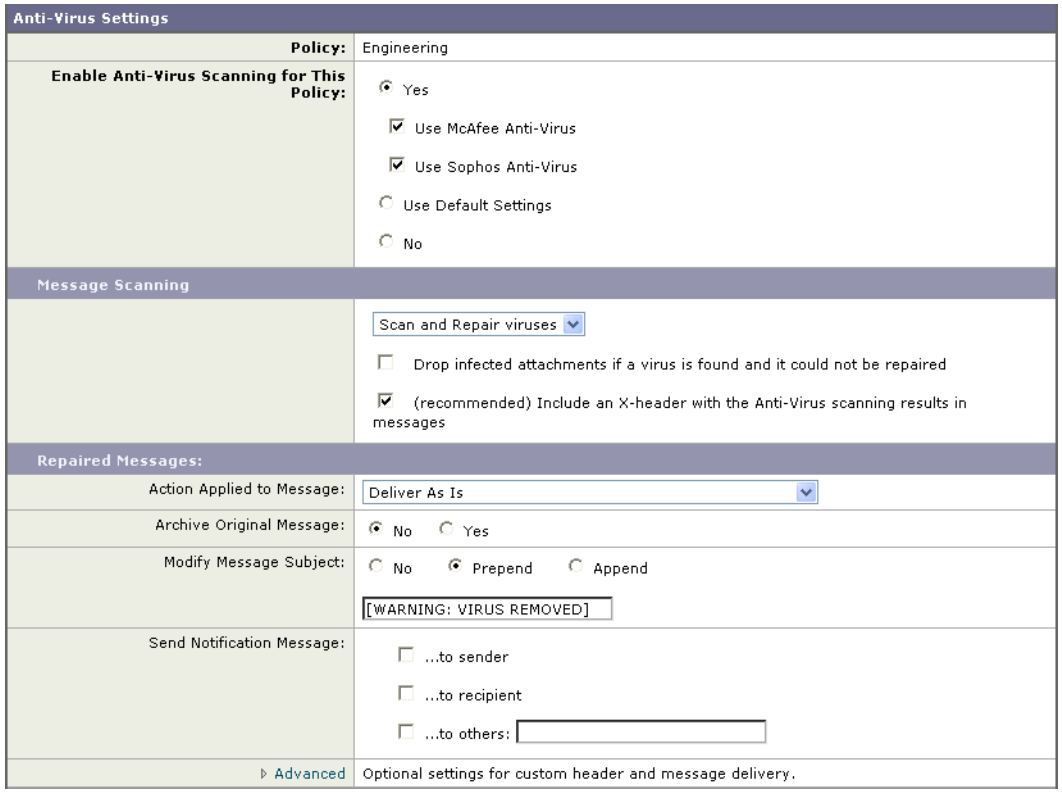
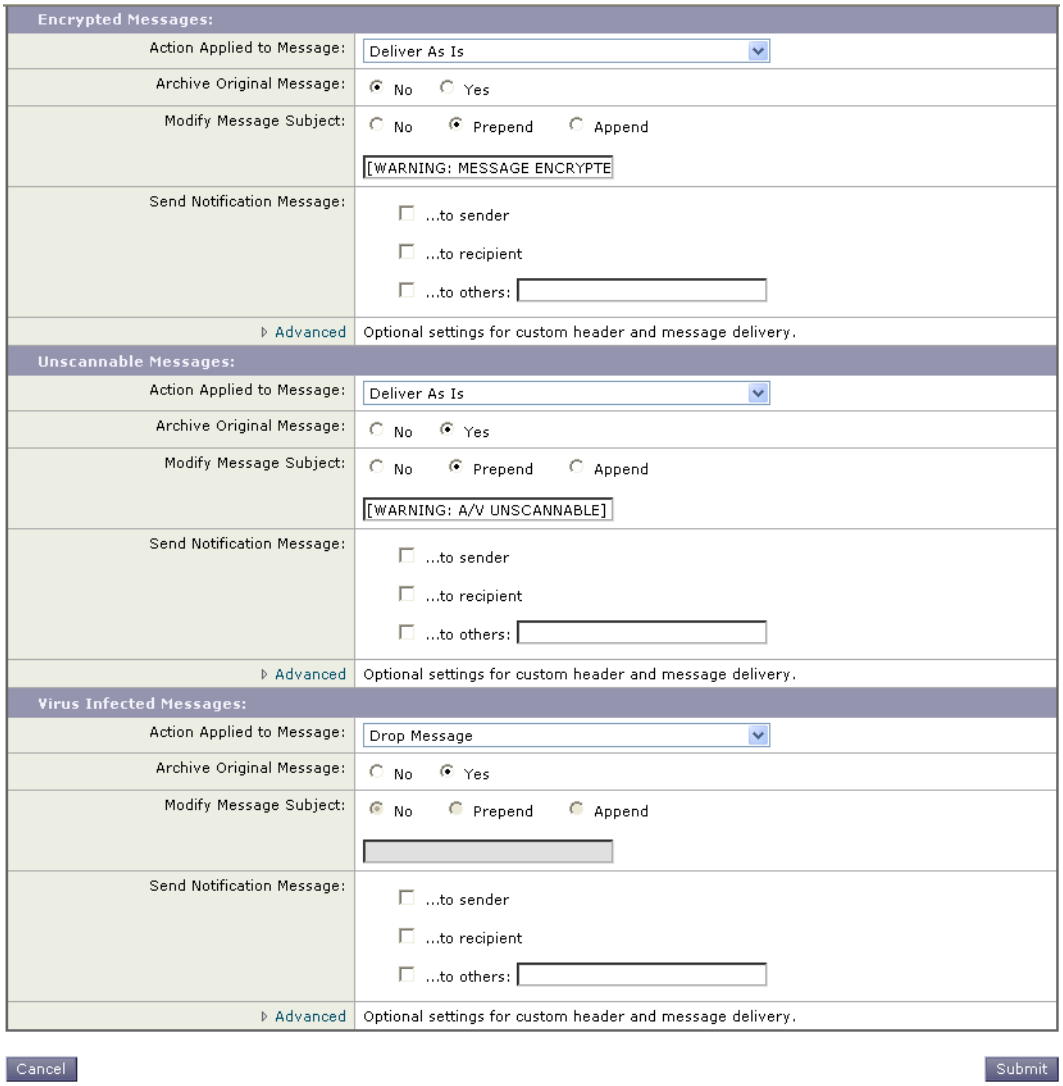


図 8-4　　メール ポリシーのアンチウイルス設定（デフォルト以外）:2/2



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。

[ウイルスのみスキャン（Scan for Viruses only）] 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、スキャ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 スキャンが [ウイルスのみスキャン（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、スキャ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 8-3 に、一般的なアンチウイルス設定オプションを示します。

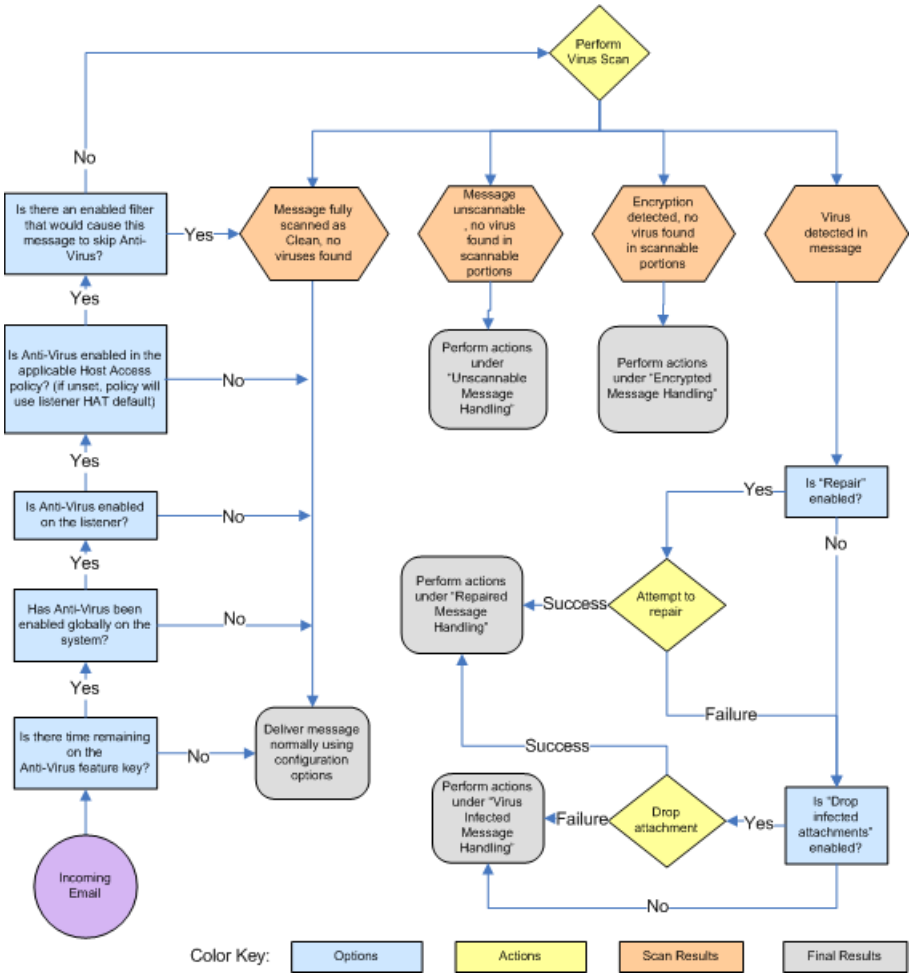
表 8-3　一般的なアンチウイルス設定オプション

状況	アンチウイルス設定
ウイルスが広範囲に発生 **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。**	**添付ファイルのドロップ:**しない。 **スキャン:**スキャンのみ。 **クリーンアップされたメッセージ:**配信する。 **スキャンできないメッセージ:**メッセージをドロップする。 **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。 **ウイルス性のメッセージ:**メッセージをドロップする。
リベラルなポリシー **できる限り多くのドキュメントを送信します。**	**添付ファイルのドロップ:**する。 **スキャン:**スキャンして修復。 **クリーンアップされたメッセージ:**[VIRUS REMOVED] として配信する **スキャンできないメッセージ:**添付ファイルとして転送する。 **暗号化されたメッセージ:**マークして転送する。 **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。
より保守的なポリシー	**添付ファイルのドロップ:**する。 **スキャン:**スキャンして修復。 **クリーンアップされたメッセージ:**[VIRUS REMOVED] として配信する (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)。 **スキャ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。 **暗号化されたメッセージ:**マークして転送する、またはスキャンできないメッセージとして処理する。 **ウイルス性のメッセージ:**アーカイブしてドロップする。
保守的なポリシーでレビューを実施する **ウイルス メッセージの可能性があるものは、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。**	**添付ファイルのドロップ:**しない。 **スキャン:**スキャンのみ。 **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)。 **スキャ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。 **暗号化されたメッセージ:**スキャンできないメッセージとして処理する。 **ウイルス性のメッセージ:**隔離するか管理者に転送する。

アンチウイルス アクションのフロー ダイアグラム

図 8-5（8-20 ページ）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 8-5　　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 IronPort 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 IronPort 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。

ウイルス スキャンのテスト

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。

[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、パブリック リスナー（RAT）上でのローカル ドメインまたは特定のユーザの電子メールの受け入れ（5-54 ページ）を参照してください）。

Cisco IronPort 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（8-11 ページ）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（8-11 ページ）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、ダウンロードする 4 つのファイルを提供します。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。

CHAPTER 9

アンチスパム

Cisco IronPort アプライアンスは、独自の階層化された方法により、電子メール ゲートウェイでスパムを阻止します。スパム制御の最初の階層である評価フィルタリング（第 7 章、レピュテーション フィルタリングで前述）を使用すると、Cisco IronPort SenderBase™ 評価サービスにより決定される送信者の信頼性に基づいて、電子メールの送信者を分類し、ご使用の電子メール インフラストラクチャへのアクセスを制限できます。2 番めの防衛階層であるスキャンでは、Cisco IronPort Anti-Spam™ テクノロジーと Cisco IronPort Intelligent Multi-Scan テクノロジーが使用されています。評価フィルタリングとアンチスパム スキャンを組み合わせることにより、現在使用可能なものの中では最高水準の効率と性能を持つアンチスパム ソリューションが実現されています。

Cisco IronPort アプライアンスを使用すると、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に対して、アンチスパム スキャンを一切実施しないでエンドユーザに直接配信するポリシーを非常に簡単に作成できます。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 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廃棄したりできます。

Cisco IronPort アプライアンスの提供する独自の二層スパム対策により、高性能で今までにない柔軟性を備えた、企業の電子メール ゲートウェイ管理および保護が可能になります。

Anti-Spam の概要

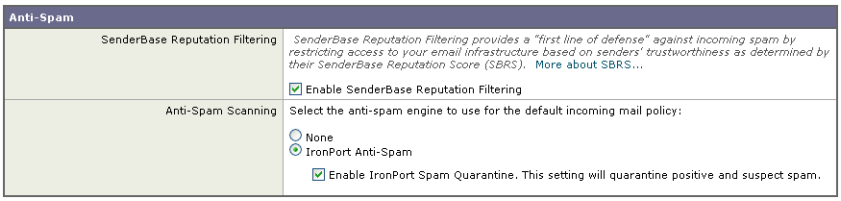
Cisco IronPort アプライアンスでは、Cisco IronPort Anti-Spam エンジンと Cisco IronPort Intelligent Multi-Scan の 2 つのアンチスパム ソリューションを提供しています。Cisco IronPort アプライアンスでこれらのソリューションのライセンスを取得して有効にすることはできますが、両方を同じポリシーで有効にすることはできません。電子メール セキュリティ マネージャを使用すると、異なるユーザのグループに対して異なるアンチスパム ソリューションをすばやく簡単に指定できます。

アンチスパム スキャンのイネーブル化

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 IronPort Intelligent Multi-Scan または Cisco IronPort 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 セットアップでは、陽性および陽性と疑わしいスパムに対処する Cisco IronPort スパム検疫を必要に応じてイネーブルにすることができます。

IronPort スパム検疫エンジンを初めてイネーブルにするときは（システム セットアップ時または後刻）、ライセンス契約書を読んで承諾してください。

図 9-1　アンチスパム エンジン：システム セットアップ時に選択

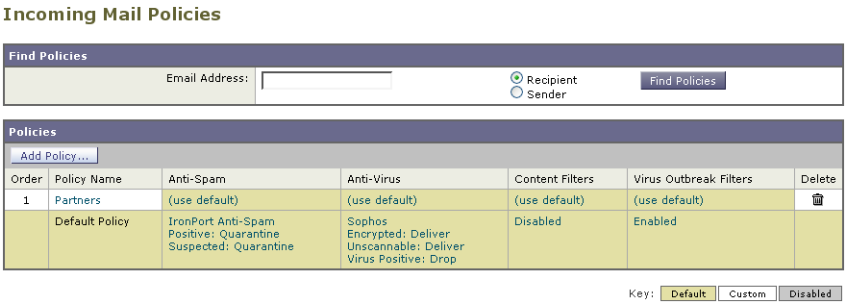


（注）　アンチスパム スキャンの適用方法および適用条件については、電子メール パイプラインとセキュリティ サービス（4-7 ページ）を参照してください。

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）] > [受信メールポリシー（Incoming Mail Policies）] ページから受信メール ポリシー用のスパム対策スキャン 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 ポリシーでは通常無効です）。ポリシーのスパム対策スキャンもディセーブルにできます。

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、陽性スパムおよび陽性と疑わしいスパムを隔離するために Cisco IronPort Anti-Spam スキャン エンジンを使用しています。

図 9-2　メール ポリシー：受信者ごとのスパム対策エンジン

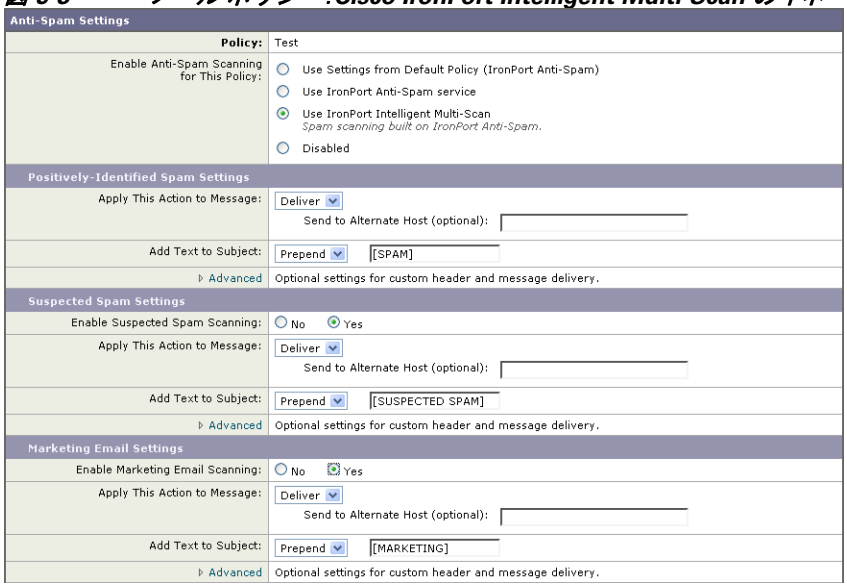


パートナーのポリシーを変更して、不要なマーケティング メッセージに対して Cisco IronPort Intelligent Multi-Scan とスキャンを使用するには、パートナーの行に対応する [スパム対策（Anti-Spam）] 列のエントリ（[デフォルトを使用（Use Default）]）をクリックします。

スキャン エンジンに Cisco IronPort 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イネーブルにする場合は [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。

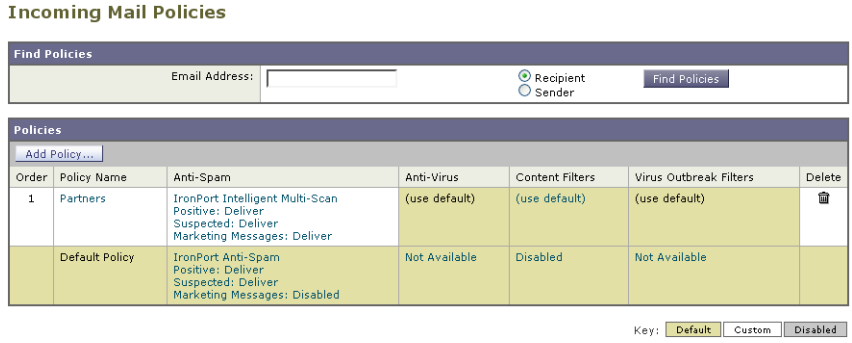
図 9-3 は、Cisco IronPort Intelligent Multi-Scan と不要なマーケティング メッセージの検出がポリシーでイネーブルに設定されていることを示します。

図 9-3　　メール ポリシー:Cisco IronPort 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 9-4　　メール ポリシー:Intelligent Multi-Scan がイネーブルにされたポリシー



Anti-Spam Scanning Engine の設定

各アンチスパム スパム ソリューションでは、それに関連付けられている構成時の設定グループがあります。これらの設定値は、対応するエンジンだけに適用される設定で、[セキュリティサービス(Security Services)] メニューの [Cisco IronPort Anti-Spam] ページと [Cisco IronPort インテリジェントマルチスキャン(Cisco IronPort Intelligent Multi-Scan)] ページおよび着信と発信のメール ポリシーのアンチスパム設定値ページで使用可能です。スキャン ソリューション固有の設定値については、対応する項で説明します。[Cisco IronPort Anti-Spam] ページおよび [Cisco IronPort インテリジェントマルチスキャン(Cisco IronPort Intelligent Multi-Scan)] ページには、最新のアップデート日時を持つアンチスパム ルールのリストも表示されます。

グローバル アンチスパム設定値を設定するときの詳細については、次の資料を参照してください。

- Cisco IronPort Anti-Spam のイネーブル化とグローバル設定の構成(9-6 ページ)および
- Cisco IronPort Intelligent Multi-Scan のイネーブル化とグローバル設定値の設定(9-10 ページ)。

受信者ごとにアンチスパム スキャンを構成する方法の詳細については、アンチスパムの受信者別ポリシーの設定（9-13 ページ）を参照してください。

Cisco IronPort アプライアンスで生成されるアンチスパム スキャンおよびメッセージ

シスコでは、Cisco IronPort アプライアンスから電子メール アラート、スケジュール済みレポート、およびその他の自動化されたメッセージを受信する受信者の場合は、アンチスパム スキャンをバイパスする着信メール ポリシーに入れるよう推奨しています。これらのメッセージは、企業のメール ストリームでは通常見つかることのない、スパム発信元と関連性のある URL やその他の情報を含むため、これらのメッセージには、スパムとマークされることがあります。または、Cisco IronPort アプライアンスに代わってメールを送信する IP アドレスを、ホスト アクセス テーブルの「ホワイトリスト」ポリシーに追加することもできます（送信者グループへの送信者の追加（5-36 ページ）を参照）。詳細については、認定されている Cisco IronPort アプライアンス サポート センターにお問い合わせください。

Cisco IronPort スパム対策フィルタリング

Cisco IronPort スパム対策機能は、従来の手法と革新的なコンテキスト認識型検出技術を使用して、既知および新種のさまざまな E メール脅威を排除します。

評価キー

Cisco IronPort アプライアンスには、Cisco IronPort 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 IronPort Anti-Spam がイネーブルになります。設定した管理者アドレス（手順 2：システム（3-17 ページ）を参照）に対して、Cisco IronPort 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 IronPort 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、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Common Administrative Tasks」にある機能キーの使用に関する項を参照してください）。

Cisco IronPort Anti-Spam と CASE：概要

Cisco IronPort Anti-Spam フィルタリングは、Context Adaptive Scanning Engine（CASE）™ に基づいており、次の目的のために電子メールと Web 評価情報を組み合わせる、1 層めのアンチスパム スキャン エンジンです。

- 広範囲の電子メール脅威を排除：スパム、「フィッシング」、ゾンビベースの攻撃、およびその他の「混在した」脅威を検出します。
- 最高の精度を提供：SenderBase レピュテーション サービスからの電子メールおよび web レピュテーションに基づいたスパム対策ルール。

- 使いやすさを提供:ハードウェア コストおよび管理コストを削減。
- 業界トップ クラスの性能の実現:CASE では、ダイナミックな初期終了基準およびオフボックス ネットワーク見積もりを使用して、きわめて優れた性能を実現できます。
- インターナショナル ユーザのニーズに対応:Cisco IronPort Anti-Spam は、世界的に業界トップ クラスの性能を発揮するように調整されています。

広範な脅威の防止

CASE では、コンテンツ分析、電子メール評価、および Web 評価を組み合わせて、最大限多様な脅威防止要因を収集します。

シスコは、広範な電子メールの脅威を検出することを目的に、Cisco IronPort Anti-Spam を徹底的に設計しました。Cisco 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、Cisco 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。

Cisco IronPort Anti-Spam では、これらの脅威を識別するために、業界随一の網羅性を持つ脅威検出方式を使用し、メッセージのコンテキスト全体、つまりメッセージの内容、メッセージの構築方式、送信者の評価、メッセージでアドバタイズされている Web サイトの評価などを調べます。Cisco IronPort Anti-Spam は世界最大の電子メールおよび Web トラフィック 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、開始と同時に新しい攻撃を検出します。

（注） Cisco IronPort 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 ホストを識別する必要があります。詳細については、着信リレー（9-21 ページ）を参照してください。

最も低い誤検出率

Cisco IronPort Anti-Spam および Cisco IronPort アウトブレイク フィルタには、Cisco IronPort が特許出願中のコンテキスト適応スキャン エンジン（CASE）が使用されています。CASE では、4 つの次元にまたがる 100,000 個以上のメッセージ属性を分析することにより、めざましい精度と性能の向上を実現しています。

ステップ 1　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*。

ステップ 2　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*。

ステップ 3　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。

ステップ 4　Web レピュテーション:遷移先は*どこか*。

CASE では、多次元的な関係を分析することにより、優れた精度を維持しながら、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。

業界トップ水準の性能

CASE は、以下の機能を組み合わせて、正確な判定を迅速に行います。

- 単一パスによる複数脅威のスキャン
- 動的な「初期終了」システム

  システムのパフォーマンスは、Cisco IronPort 独自の「初期終了」システムを使用して最適化されます。Cisco IronPort ルールの正確性と計算費用に基づいて、ルールの適用順序を決定する独自のアルゴリズムを開発しました。コストが低い一方で正確性の高いルールから実行していき、判定が出た時点でそれ以降のルールは不要になります。この方式によってシステムのスループットが向上されるため、大企業のニーズを満たす製品が実現されます。反対に、高効率なエンジンは低コスト ハードウェアへの実装を可能にしているため、Cisco IronPort のセキュリティ サービスはローエンドのお客様にとって魅力的です。
- オフボックス ネットワークの計算

インターナショナル ユーザ

Cisco IronPort Anti-Spam は、世界的に業界トップ クラスの性能を発揮するように調整されています。ロケール固有のコンテンツに対応した脅威(の)検出の技術だけでなく地域ルール プロファイルを使用して特定の領域のスパムをスキャンをさらに最適化できます。アンチスパム エンジンには、リージョナル ルール プロファイルが含まれています。リージョナル ルール プロファイルは、地域ごとのスパムを対象にしています。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、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。[セキュリティサービス(Security Services)] > [IronPort Anti-Spam] からリージョナル ルール プロファイルを有効にできます。

(注) リージョナル ルール プロファイル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。したがって、指定したリージョンから大量の電子メールを受信する場合に限り、この機能をイネーブルにすることを推奨します。

Cisco IronPort Anti-Spam では、南北アメリカ大陸、ヨーロッパ、およびアジアに散在している、125,000 を超える ISP、大学、および企業から提供された、地球規模において代表的な電子メールと Web のコンテンツ不可知データを活用しています。サンパウロ、北京、およびロンドンに中枢機能を置く Threat Operations Center が世界的活動のために設置されています。さらに、アナリストは、中国語、日本語、韓国語、ポルトガル語、スペイン語を含む 32 の言語を話します。

Cisco IronPort Anti-Spam のイネーブル化とグローバル設定の構成

概要

Cisco IronPort Anti-Spam のイネーブル化とグローバル設定値の変更には、[セキュリティサービス(Security Services)] > [IronPortAnti-Spam とセキュリティサービス(IronPortAnti-Spam and Security Services)] > [サービスのアップデート(Service Updates)] ページ(GUI)または `antispamconfig` コマンドと `updateconfig` コマンド(CLI)を使用します。次のグローバル設定値が設定されます。

- アプライアンス上の Cisco IronPort Anti-Spam をグローバル設定で有効にする。
- Cisco IronPort Anti-Spam によるメッセージ スキャンのしきい値を設定する。

スパム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、定義サイズより小さいメッセージがすべて CASE でスキャンされる *always scan* メッセージ サイズを定義でき、Cisco IronPort の業界トップレベルの性能を発揮しています。また、定義サイズより大きいメッセージが CASE でスキャンされない *never scan* メッセージ サイズを定義できます。*always scan* サイズより大きく、*never scan* サイズより小さいメッセージについては、CASE は限定的な高速スキャンを実行します。

（注） 感染フィルタの最大メッセージ サイズが Cisco IronPort Anti-Spam の *always scan* メッセージより大きい場合、CASE は感染フィルタの最大サイズより小さいメッセージをすべてスキャンします。

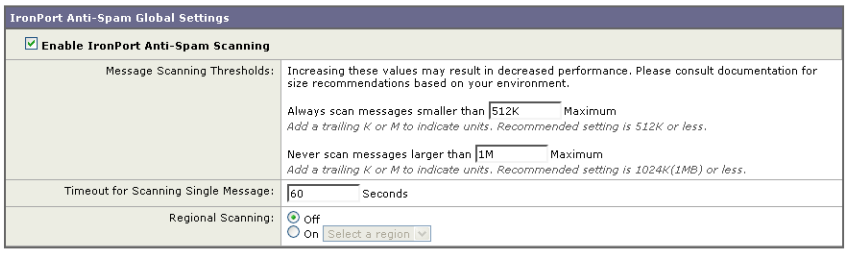
- メッセージをスキャンするときにタイムアウトを待機する時間の長さを入力します。
- Cisco IronPort Anti-Spam ルールのアップデートを取得するためのプロキシ サーバを定義し、必要に応じてイネーブルにします（[セキュリティサービス（Security Services）] > [サービスのアップデート（Service Updates）]）。ルールのアップデートを取得するためのプロキシ サーバを定義する場合は、必要に応じて、プロキシ サーバに接続するための認証済みユーザ名、パスワード、および特定のポートを設定できます。
- Cisco IronPort Anti-Spam ルールのアップデートを受信するダウンロード サーバを定義し、必要に応じてイネーブルにします（[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）]）。
- Cisco IronPort Anti-Spam ルールの自動アップデートの受信をイネーブルまたはディセーブルにし、アップデート間隔も指定します。

（注） プロキシ サーバのセットアップは、[Security Services] > [Service Updates] ページから行うことができます。プロキシ サーバの指定方法の詳細については、[Service Updates] ページ（15-9 ページ）を参照してください。これで、プロキシ サーバがグローバルになったため、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で同じプロキシ サーバが使用されます。

（注） GUI のシステム セットアップ ウィザード（または CLI の `systemsetup` コマンド）で Cisco IronPort Anti-Spam をイネーブルにすることを選択した場合は、グローバル設定値のデフォルト値を使用し、デフォルト着信メール ポリシーに対してイネーブルになります。

図 9-5 に、[セキュリティサービス（Security Services）] > [IronPort Anti-Spam] ページで設定するグローバル設定値を示します。

図 9-5　Cisco IronPort Anti-Spam グローバル設定：編集



ステップ 1　システム セットアップ ウィザードで Cisco IronPort Anti-Spam をイネーブルにしなかった場合は、[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　[有効（Enable）] をクリックします。

ライセンス契約書ページが表示されます。

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

ステップ 3　ページの下部までスクロールし、[承認（Accept）] をクリックしてライセンス契約に合意します。

図 9-6 とほぼ同じページが表示されます。

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　[IronPort Anti-Spam スキャニングを有効にする（Enable IronPort Anti-Spam Scanning）] の横にあるチェックボックスをオンにします。

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。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。詳細については、アンチスパムの受信者別ポリシーの設定（9-13 ページ）を参照してください。

ステップ 6　Cisco IronPort Anti-Spam の *always scan* メッセージ サイズの値を入力します。

推奨値は 512 Kb 以下です。「初期終了」の場合を除き、*always scan* 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、ステップ 7 で入力した *never scan* サイズより小さい場合、部分的にスキャンします。「初期終了」システムの詳細については、業界トップ水準の性能（9-6 ページ）を参照してください。

（注）　*always scan* 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。

ステップ 7　*never scan* メッセージ サイズの値を入力します。

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 IronPort Anti-Spam によってスキャンされず、`X-IronPort-Anti-Spam-Filtered: true` というヘッダーはメッセージに追加されません。

（注）　*never scan* 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。

ステップ 8　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。

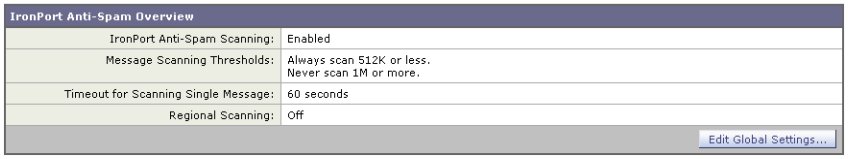
秒数を指定する場合は、1 ～ 120 の整数を入力します。デフォルト値は 60 秒です。

ステップ 9　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ます。リージョナル スキャンでは、特定のリージョン用に Cisco IronPort Anti-Spam スキャンが最適化されます。この機能では特定のリージョンに合わせてスパム対策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。したがって、指定したリージョンから大量の電子メールを受信する場合に限り、この機能をイネーブルにすることを推奨します。リージョナル スキャンの詳細については、インターナショナル ユーザ（9-6 ページ）を参照してください。

ステップ 10　変更を送信し、保存します。

[セキュリティサービス（Security Services）] > [IronPort Anti-Spam] ページがリフレッシュされて、前の手順で選択した値が表示されます。

図 9-6　Cisco IronPort Anti-Spam グローバル設定



この他の手順

Cisco IronPort Anti-Spam をイネーブルにすると、SenderBase 評価スコアに基づいて接続を拒否していない場合であっても、SenderBase 評価サービスのスコアリングがイネーブルになります。SBRS のイネーブル化の詳細については、SenderBase 評価フィルタの実装（7-4 ページ）を参照してください。

Cisco IronPort Intelligent Multi-Scan フィルタリング

Cisco IronPort Intelligent Multi-Scan では、Cisco IronPort 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、インテリジェントな多層スパム対策ソリューションを実現しています。この方式により、false positive 率を上昇させることなく、判定の精度が向上されて、検出されるスパムの量が増加します。

Cisco IronPort Intelligent Multi-Scan によってメッセージを処理する場合は、まず、サードパーティ製アンチスパム エンジンを使用してスキャンされます。Cisco IronPort 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 IronPort Anti-Spam に渡されて、最終判定が下されます。Cisco IronPort 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 IronPort スパム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 IronPort 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 IronPort 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 IronPort 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 IronPort Intelligent Multi-Scan がスキップすることはありません。

Cisco IronPort 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 IronPort サポート担当者にお問い合わせください。

この機能は、C100 アプライアンス以外のすべての C-Series アプライアンスおよび X-Series アプライアンスでサポートされています。

（注）　Intelligent Multi-Scan ライセンス キーによって、アプライアンスで Cisco IronPort 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 IronPort Intelligent Multi-Scan または Cisco IronPort 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 IronPort Intelligent Multi-Scan のイネーブル化とグローバル設定値の設定

概要

Cisco IronPort Intelligent Multi-Scan のイネーブル化とグローバル設定値の変更には、[セキュリティサービス（Security Services）] > [IronPort インテリジェントマルチスキャンとセキュリティサービス（IronPort Intelligent Multi-Scan and Security Services）] > [サービスのアップデート（Service Updates）] ページ（GUI）または `antispamconfig` コマンドと `updateconfig` コマンド（CLI）を使用します。次のグローバル設定値が設定されます。

- アプライアンスで Cisco IronPort Intelligent Multi-Scan をグローバルに有効にします。
- Cisco IronPort Intelligent Multi-Scan でスキャンするメッセージの最大サイズを設定します。
- 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時間の長さを入力します。

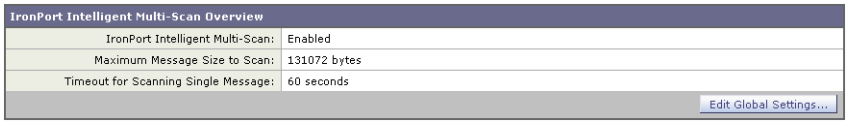
  大部分のユーザでは、スキャンする最大メッセージ サイズもタイムアウト値も変更する必要がありません。最大メッセージ サイズの設定を小さくして、アプライアンス スループットを最適化できる可能性があります。
- Cisco IronPort Intelligent Multi-Scan ルールのアップデートを取得するためのプロキシ サーバを定義し、必要に応じてイネーブルにします（[セキュリティサービス（Security Services）] > [サービスのアップデート（Service Updates）]）。ルールのアップデートを取得するためのプロキシ サーバを定義する場合は、必要に応じて、プロキシ サーバに接続するための認証済みユーザ名、パスワード、および特定のポートを設定できます。
- Cisco IronPort Intelligent Multi-Scan ルールのアップデートを受信するダウンロード サーバを定義し、必要に応じてイネーブルにします（[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）]）。
- Cisco IronPort Intelligent Multi-Scan ルールの自動アップデートの受信をイネーブルまたはディセーブルにし、アップデート間隔も指定します。

（注） プロキシ サーバのセットアップは、[Security Services] > [Service Updates] ページから行うことができます。プロキシ サーバの指定方法の詳細については、[Service Updates] ページ（15-9 ページ）を参照してください。これで、プロキシ サーバがグローバルになったため、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で同じプロキシ サーバが使用されます。

（注） GUI のシステム セットアップ ウィザード（または CLI の `systemsetup` コマンド）で Cisco IronPort Intelligent Multi-Scan をイネーブルにすることを選択した場合は、グローバル設定値のデフォルト値を使用し、デフォルト着信メール ポリシーに対してイネーブルになります。

図 9-7 に、[Security Services] > [IronPort Intelligent Multi-Scan] ページで設定するグローバル設定値を示します。

図 9-7　Cisco IronPort Intelligent Multi-Scan のグローバル設定値：編集



Cisco IronPort Intelligent Multi-Scan をイネーブルにするには、次の手順を実行します。

ステップ 1　システム セットアップ ウィザードで Cisco IronPort Intelligent Multi-Scan をイネーブルにしなかった場合は、[セキュリティサービス（Security Services）] > [IronPort インテリジェントマルチスキャン（IronPort Intelligent Multi-Scan）] を選択します。

ステップ 2　[有効（Enable）] をクリックします。

ライセンス契約書ページが表示されます。

（注）　ライセンス契約に合意しない場合、Cisco IronPort Intelligent Multi-Scan 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 3　ページの下部までスクロールし、[承認（Accept）] をクリックしてライセンス契約に合意します。

図 9-8 とほぼ同じページが表示されます。

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　[Enable IronPort Intelligent Multi-Scan] の横のボックスをオンにします。

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。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。詳細については、アンチスパムの受信者別ポリシーの設定（9-13 ページ）を参照してください。

ステップ 6　Cisco IronPort Intelligent Multi-Scan で [スキャンする最大メッセージ サイズ（maximum message size to scan）] 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 IronPort Intelligent Multi-Scan でスキャンされません。

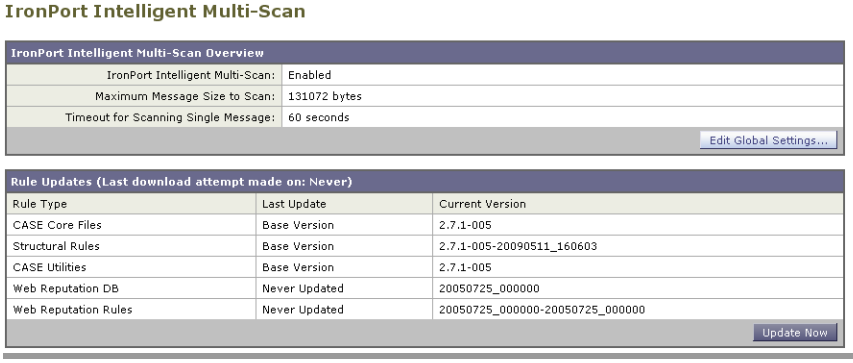
ステップ 7　メッセージをスキャンするときにタイムアウトを待機する秒数を入力します。

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。

ステップ 8　変更を送信し、保存します。

[Security Services] > [IronPort Intelligent Multi-Scan] ページがリフレッシュされて、前の手順で選択した値が表示されます。

図 9-8　Cisco IronPort Intelligent Multi-Scan のグローバル設定値



この他の手順

Cisco IronPort Intelligent Multi-Scan をイネーブルにすると、SenderBase 評価スコアに基づいて接続を拒否していない場合であっても、SenderBase 評価サービスのスコアリングがイネーブルになります。SBRS のイネーブル化の詳細については、SenderBase 評価フィルタの実装（7-4 ページ）を参照してください。

アンチスパム ルールのアップデートの設定

Cisco IronPort Anti-Spam および Cisco IronPort Intelligent Multi-Scan のルールは、デフォルトでは、Cisco IronPort のアップデート サーバから取得されます。アップデート用のローカル サーバ、アップデートの取得に使用するプロキシ サーバ、ルールのアップデートを確認するかどうかおよび確認する頻度を指定できます。アンチスパム ソリューションのアップデートを設定するには、[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）] ページの [アップデート設定を編集（Edit Update Settings）] をクリックします。

詳細については、サービスのアップデート（15-9 ページ）を参照してください。

Cisco IronPort Anti-Spam ルールのアップデートを取得するプロキシ サーバのイネーブル化

Cisco IronPort アプライアンスは、Cisco IronPort のアップデート サーバに直接接続して、アンチスパム ルールの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。

プロキシ サーバが定義されている場合、Cisco IronPort Anti-Spam および Cisco IronPort Intelligent Multi-Scan では、そのプロキシ サーバを*自動的に*使用します。他のすべてのサービス アップデート（感染フィルタ、Sophos Anti-Virus など）についてプロキシ サーバをディセーブルにしないで、アンチスパム ソリューションについてプロキシ サーバをオフにする方法はありません。

（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。

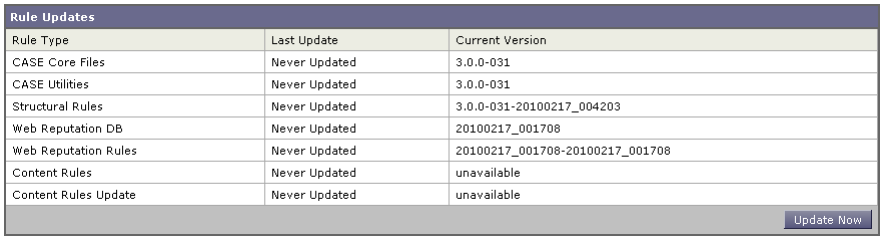
プロキシ サーバの定義の詳細については、HTTP プロキシ サーバの指定（任意）（15-14 ページ）を参照してください。

モニタリング ルールのアップデート

ライセンス契約に同意すると、最新の Cisco IronPort Anti-Spam および Cisco IronPort Intelligent Multi-Scan のルールのアップデートが、[セキュリティサービス（Security Services）] メニュー（GUI）および `antispamstatus` コマンド（CLI）の対応するページに一覧表示されます。

（注） 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。

図 9-9　[Security Services] > [IronPort Anti-Spam] ページの [Rules Updates] セクション：GUI



アンチスパムの受信者別ポリシーの設定

Cisco IronPort Anti-Spam ソリューションおよび Cisco IronPort Intelligent Multi-Scan ソリューションでは、電子メール セキュリティ マネージャ機能を使用して設定するポリシー（コンフィギュレーション オプション）に基づいて、着信（および発信）メール用の電子メールを処理します。Cisco IronPort Anti-Spam および Cisco IronPort Intelligent Multi-Scan では、フィルタリング モジュールによってメッセージをスキャンすることにより分類します。その後、分類または*判定*は、後続の配信アクション用に返されます。判定結果として得られる可能性があるのは、スパムでない、不要なマーケティング電子メール、陽性と判定されたスパム、または陽性と疑わしいスパムの 4 つです。スパム陽性と判定されたメッセージ、スパム陽性と疑わしいメッセージ、または不要なマーケティング メッセージであると識別されたメッセージに対するアクションには、次のアクションが含まれます。

- 陽性または陽性と疑わしいスパムのしきい値の指定。
- 不要なマーケティング メッセージ、陽性と判定されたスパム、または陽性と疑わしいスパム メッセージに対する全般的なアクションの選択：配信、ドロップ、バウンス、または検疫。
- mbox 形式のログ ファイルへのメッセージのアーカイブ。スパムであると識別されたメッセージのアーカイブをイネーブルにするには、ログを作成する必要があります。識別されたメッセージのアーカイブ（9-15 ページ）を参照してください。
- スパムまたはマーケティングであると識別されたメッセージの件名ヘッダーの変更。
- 代替宛先メールホストへのメッセージの送信。
- メッセージに対するカスタム X-Header の追加。
- 代替エンベロープ受信者アドレスへのメッセージの送信（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。

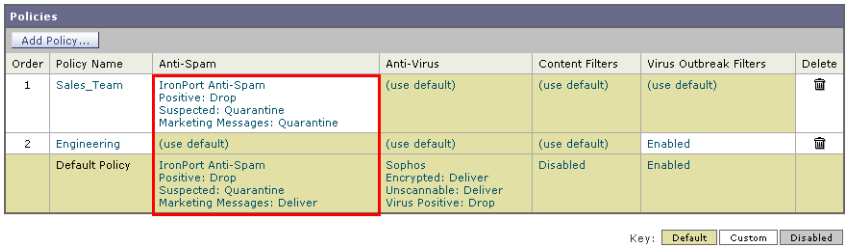
（注） これらのアクションは、相互に排他的ではありません。ユーザのグループのさまざまな処理ニーズに合わせて、さまざまな着信または発信ポリシーで、これらのアクションを数個またはすべてを、さまざまに組み合わせることができます。同じポリシーで、陽性と判定されたスパムと陽性と疑わしいスパムを別々に扱うことができます。たとえば、陽性と判定されたスパムであるメッセージをドロップする一方で、陽性と疑わしいスパム メッセージを隔離する必要がある場合があります。

Cisco IronPort Anti-Spam または Cisco IronPort Intelligent Multi-Scan のアクションは、電子メール セキュリティ マネージャ機能を使用して、[メールポリシー(Mail Policies)] > [受信メールポリシー(Incoming Mail Policies)] または [送信メールポリシー(Outgoing Mail Policies)] ページ(GUI)または `policyconfig -> antispam` コマンド(CLI)から、受信者単位を基本にイネーブルにします。アンチスパム ソリューションがグローバルでイネーブルになってから、作成したメール ポリシーごとに、これらのアクションを個別に設定します。異なるメール ポリシーに対して異なるアクションを設定できます。ポリシーごとにイネーブルにできるアンチスパム ソリューションは 1 つだけです。同じポリシーでは両方をイネーブルにできません。

(注) 発信メールのアンチスパム スキャンをイネーブルにするには、関連するホスト アクセス テーブルのアンチスパム設定値、特にプライベート リスナーも確認する必要があります。詳細については、メール フロー ポリシー:アクセス ルールとパラメータ(5-8 ページ)を参照してください。

電子メール セキュリティ マネージャの各行は、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。

図 9-10　メール ポリシー:アンチスパム エンジン



メール ポリシーのアンチスパム設定値の編集

メール ポリシーのアンチスパム設定値をユーザごとに編集する処理は、ポリシーが着信メール用であっても、発信メール用であっても、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。このフィールドを選択すると、デフォルト メール ポリシーのすべてのアンチスパム設定値がポリシーに導入されます。

詳細については、デフォルト ポリシーの編集:アンチスパム設定(6-25 ページ)も参照してください。

ステップ 1　電子メール セキュリティ マネージャの着信または発信メール ポリシー テーブルの任意の行にある、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。

図 9-11 に示すようなアンチスパム設定値ページが表示されます。

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。図 9-11 は、具体的なポリシー(デフォルト以外)の設定値を示します。この画面と図 6-6(6-26 ページ)を比較してください。[デフォルトを使用(Use Default)] オプションが個々のポリシーに付加されている状態に注意してください。

ステップ 2　ポリシーで使用するアンチスパム ソリューションを選択します。

[無効(Disabled)] をクリックすると、メール ポリシーのアンチスパム スキャン全体をディセーブルにできます。

ステップ 3　スパムであることが確実な電子メール、スパムだと疑われる電子メール、および不要なマーケティング メッセージの設定を行います。

図 9-11 に、編集直前のデフォルト メール ポリシーの Cisco IronPort Anti-Spam 設定値を示します。陽性と判定されたスパムと陽性と疑わしいスパム（9-17 ページ）および識別されたメッセージの設定値を設定する際の注意事項（9-15 ページ）を参照してください。

ステップ 4　変更を送信し、保存します。

[Mail Policies] > [Incoming Mail Policies] または [Outgoing Mail Policies] ページがリフレッシュされて、これまでの手順で選択した値が反映されます。

識別されたメッセージの設定値を設定する際の注意事項

陽性および陽性と疑わしいスパムのしきい値

陽性と判定されたスパムおよび陽性と疑わしいスパムのしきい値に対する値を入力します。スパムしきい値の詳細については、陽性および陽性と疑わしいスパムのしきい値（9-16 ページ）を参照してください。

適用するアクション

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配信、ドロップ、バウンス、または検疫から選択します。

識別されたメッセージのアーカイブ

識別されたメッセージを「スパム対策アーカイブ」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。詳細については、次の例との「ロギング」の章を参照してください『*Cisco IronPort AsyncOS for Email Daily Management Guide*』。

件名ヘッダーの変更

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ヘッダー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できます。

（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、前に追加する場合は、末尾に空白をいくつか付けて `[SPAM]` というテキストを追加します。

（注）　[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。

識別されたメッセージの代替宛先ホストへの送信

識別されたメッセージを代替宛先メールホストに送信できます。

カスタム X-Header の追加

識別されたメッセージにカスタム X-Header を追加できます。

[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。

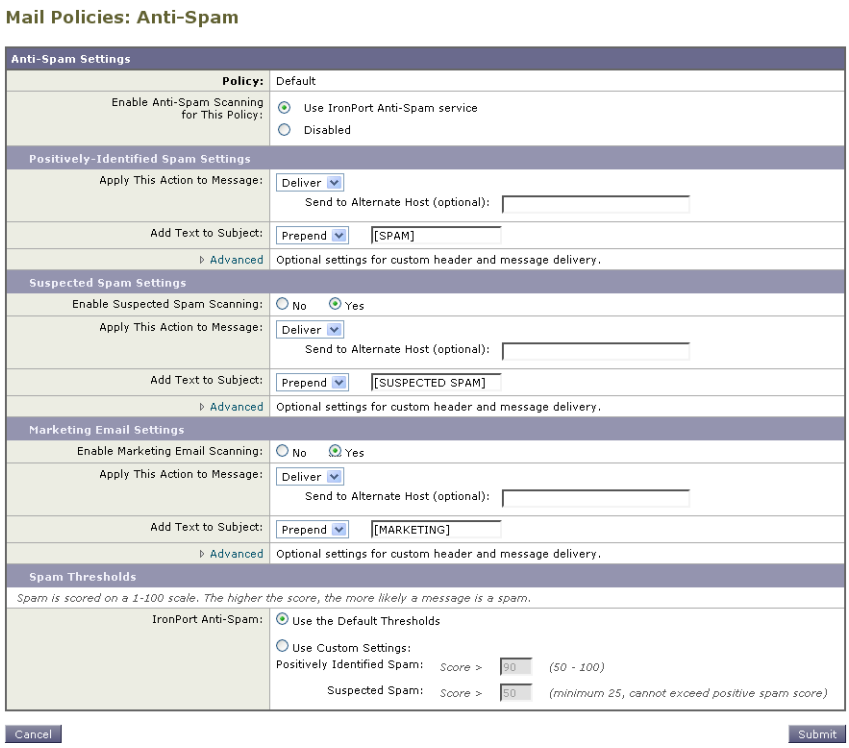
エンベロープ受信者アドレスの変更

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。

[はい（Yes）] をクリックし、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。

図 9-11　Cisco IronPort メール ポリシー用 Anti-Spam 設定値



陽性および陽性と疑わしいスパムのしきい値

メッセージがスパムであるかどうかを評価するときに、Cisco IronPort Anti-Spam および Cisco IronPort Intelligent Multi-Scan では、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。精度の高さを維持するために、この両方のアンチスパム ソリューションでは、デフォルトで高いしきい値に設定されています。90 ～ 100 の評点が返されるメッセージは、陽性と判定されたスパムであると見なされます。陽性と判定されたスパムのしきい値は、75（最も積極的）～ 99（最も保守的）で変更できます。アンチスパム ソリューションの設定に組織のスパム許容度を反映できます。Cisco IronPort Anti-Spam および Cisco IronPort Intelligent Multi-Scan の両方に、*メール ポリシー*単位で適用できる、設定可能な陽性スパムおよび陽性と疑わしいスパムのしきい値が用意されています。これを利用して、スパムとの類似が見られる一方で、正規のメッセージと共通する特徴も持つグレイゾーン メッセージを示す、「陽性と疑わしいスパム」という任意のカテゴリを作成できます。

この新しいカテゴリのしきい値設定を変更して異なる積極度に変更することにより、陽性と疑わしいスパム範囲に設定した評点未満のすべてのメッセージを、正規のメッセージであると見なし、陽性と疑わしいしきい値を超えており、陽性しきい値未満のすべてのメッセージを、陽性と疑わしいスパムと見なして、適宜処理するように設定できます。陽性と疑わしいスパムに対して実行する個別のアクションを定義することもできます。たとえば、「陽性と判定された」スパムをドロップする一方で、「陽性と疑わしい」スパムを検疫することができます。

入力する数値が大きいほど、メッセージを陽性と疑わしいスパムであると判定するために使用される Cisco IronPort Anti-Spam ルールのしきい値が高くなります。低いしきい値をイネーブルにして、その結果「スパムの可能性あり」とマークされるメッセージの数を増やすには（false positive 率が高くなる可能性あり）、小さい値を入力します。反対に、確実にスパム メッセージだけをフィルタリング対象にするには、大きい数値を入力します（一部のスパムを見逃す可能性あり）。デフォルト値は 50 です。この 2 つのカテゴリを使用する一般的な設定については、陽性と判定されたスパムと陽性と疑わしいスパム（9-17 ページ）を参照してください。

陽性と疑わしいスパムのしきい値は、Cisco IronPort Anti-Spam のメール ポリシーごとに設定されます。

陽性と判定されたスパムと陽性と疑わしいスパム

Cisco IronPort Anti-Spam および Cisco IronPort Intelligent Multi-Scan では、陽性と判定されたスパムと陽性と疑わしいスパムが区別されるため（陽性および陽性と疑わしいスパムのしきい値（9-16 ページ））、次のいずれかの方法でシステムを設定することが一般的です。

表 9-1　陽性と判定されたスパムおよび陽性と疑わしいスパムの一般的な設定の例

スパム	方式 1 のアクション（Aggressive）	方式 2 のアクション（Conservative）
陽性と判定された	削除	メッセージの件名に「`[Positive Spam]`」を追加して配信
陽性と疑わしい	メッセージの件名に「`[Suspected Spam]`」を追加して配信	メッセージの件名に「`[Suspected Spam]`」を追加して配信

1 番めの設定方式では、陽性と疑わしいスパム メッセージだけにタグを付け、陽性と判定されたメッセージはドロップされます。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、誤検出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。

2 番めの設定方式では、陽性と判定されたスパムおよび陽性と疑わしいスパムは、件名を変更して配信されます。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 番目の方式よりも保守的です。

電子メール セキュリティ マネージャ機能を使用する、受信者ごとを基本とした積極的なポリシーと保守的なポリシーの混合の詳細については、表 6-6（6-34 ページ）を参照してください。

不要なマーケティング メッセージの検出

Cisco IronPort Anti-Spam および Cisco IronPort Intelligent Multi-Scan では、スパムと正規送信元からの不要なマーケティング メッセージを区別できます。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、検疫、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。

Cisco IronPort Anti-Spam および Intelligent Multi-Scan によって追加されるヘッダー

メール ポリシーで Cisco IronPort Anti-Spam スキャンまたは Intelligent Multi-Scan がイネーブルにされている場合、そのポリシーを通過する各メッセージでは、次のヘッダーがメッセージに追加されます。

```
X-IronPort-Anti-Spam-Filtered: true
```

Cisco IronPort Anti-Spam または Intelligent Multi-Scan によってフィルタリングされた各メッセージについては、別のヘッダーも挿入されます。このヘッダーには、メッセージのスキャンに使用された CASE ルールとエンジンのバージョンを Cisco IronPort Support で識別できる情報が含まれています。

```
X-IronPort-Anti-Spam: result
```

Cisco IronPort 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。

また、電子メール セキュリティ マネージャ機能を使用すると、特定のポリシーに従って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 メールであると識別されたメッセージであるすべてのメッセージに対して、さらに追加するカスタム ヘッダーを定義することもできます（カスタム X-Header の追加（9-16 ページ）を参照）。

`skip-spamcheck` アクションを使用して、特定のメッセージの Cisco IronPort Anti-Spam スキャンをスキップさせるメッセージ フィルタも作成できます。詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Using Message Filters to Enforce Email Policies」にある「Bypass Anti-Spam System Action」を参照してください。

誤って分類されたメッセージの Cisco IronPort 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 IronPort 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：誤検出の報告用

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 IronPort ナレッジ ベースを参照するか、Cisco IronPort サポート プロバイダーにお問い合わせください。

Cisco IronPort スパム対策のテスト

ステップ 1　メール ポリシーに対して Cisco IronPort Anti-Spam をイネーブルにします（上記）。

ステップ 2　`X-Advertisement: spam` という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。

テストを目的として、Cisco IronPort 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 IronPort 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（アンチスパムの受信者別ポリシーの設定（9-13 ページ））が実行されることを確認できます。`trace` コマンドを使用してこのヘッダーを組み込むか、Telnet プログラムを使用して SMTP コマンドをアプライアンスに送信することができます。詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Testing and Troubleshooting」の章と付録 A、メアプライアンスへのアクセスモを参照してください。

（注）　アプライアンスの Cisco IronPort Anti-Spam の設定をテストする別の方法として、メッセージのヘッダーを調べて Cisco IronPort Anti-Spam によって追加された特定のヘッダーを確認する方法もあります。Cisco IronPort Anti-Spam および Intelligent Multi-Scan によって追加されるヘッダー（9-18 ページ）を参照してください。

アンチスパムの性能の評価

インターネットと直接接続した本物のメール ストリームを使用して製品を評価することを強く推奨しています。これは、Cisco IronPort Anti-Spam と Cisco IronPort 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、攻撃が終結するとすぐに期限切れになるためです。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。

「本物」を使用する場合は、スパムとみなされるメッセージが正しく処理されるシステム設定になっているのであれば、`X-Advertisement: spam` ヘッダーを使用するテスト方法が最適です。`trace` コマンドを使用するか（Debugging Mail Flow Using Test Messages: Trace（-446 ページ）を参照）、または次の例を参照してください。

評価時に陥りがちな落とし穴には、次のようなものがあります。

- 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。

- 別のアンチスパム 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

  CASE では、現行の脅威に基づいて、ルールがすぐに追加および削除されます。以前のメッセージのコレクションを使用してテストすると、結果は大幅に不正確になります。

例

SMTP コマンドを使用して、X-advertisement: spam ヘッダーを含むテスト メッセージを、アクセス権のあるアドレスに送信します。テスト アドレス宛てのメッセージを受信するようにメール ポリシーが設定されていること（パブリック リスナー（RAT）上でのローカル ドメインまたは特定のユーザの電子メールの受け入れ（5-54 ページ）を参照）および HAT で受け入れられるテスト接続であることを確認してください。

```
# 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
```

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。

着信リレー

着信リレー機能は、ネットワークのエッジにある 1 つまたは複数の Mail Exchange/Transfer エージェント（MX または MTA）、フィルタリング サーバなどを介して Cisco IronPort アプライアンスにメールを送信している外部マシンの IP アドレスを、Cisco IronPort アプライアンスで取得するために有用です。このタイプの設定では、Cisco IronPort アプライアンスで外部マシンの IP アドレスを自動的に認識しません。代わりに、外部マシンではなくローカル MX/MTA（着信リレー）から発信されたメールであると認識されます。Cisco IronPortAnti-Spam および Cisco IronPort Intelligent Multi-Scan では、外部送信者の正確な IP アドレスを必要としているため、Cisco IronPort アプライアンスにとってこの情報の取得は不可欠です。

（注）　この機能は、Cisco IronPort アプライアンスにメールをリレーするローカル MX/MTA がある場合に限りイネーブルにしてください。

図 9-12 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 IronPort 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 9-12　MX/MTA によるメール リレー：簡易

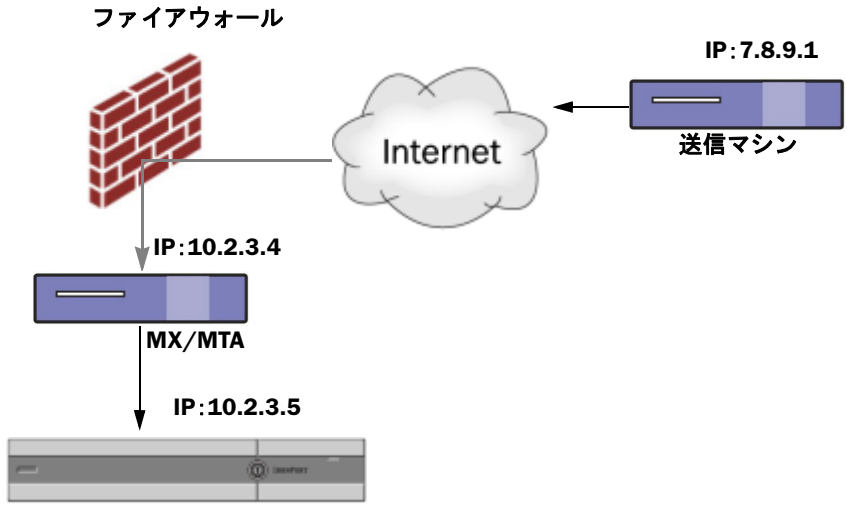
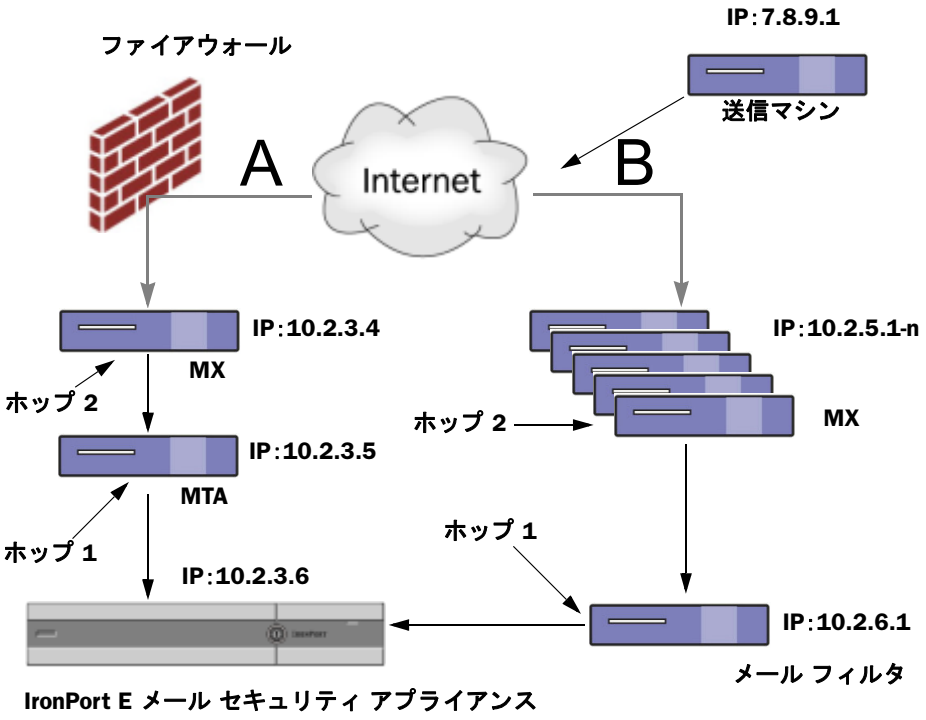


図 9-13 に別の 2 つの例を示します。この例は、少し複雑であり、ネットワーク内でのメールのリレー方法と、Cisco IronPort アプライアンスへの受け渡し前に実施できる、ネットワーク内の複数サーバにおけるメールの処理方法を示します。例 A では、7.8.9.1 からのメールがファイアウォールを通過し、MX および MTA で処理されてから、Cisco IronPort アプライアンスに配信されます。例 B では、7.8.9.1 からのメールがロード バランサまたは他のタイプのトラフィック シェーピング アプライアンスに送信され、一連の MX のいずれかに送信されてから、Cisco IronPort アプライアンスに配信されます。

図 9-13　MX/MTA によるメール リレー:拡張



着信リレー機能:概要

管理者は、インターネットからメールを直接受信する代わりに、ネットワークのエッジにある Mail Exchange（MX）または Mail Transfer Agent（MTA）の背後で Cisco IronPort アプライアンスを実行しなければならない場合があります。この設定を使用する場合、Cisco IronPort アプライアンスでは、残念ながらインターネットからメールを直接受信しないため、外部ネットワークからの直前の接続 IP アドレスが分かりません。受信メールは、代わりに、ローカル MX/MTA から受信されたと示されます。接続 IP アドレスが既知であり、Cisco IronPort Intelligent Multi-Scan および Cisco IronPort Anti-Spam のスキャンで SenderBase 評価サービスを使用できることは、Cisco IronPort アプライアンスの正常な動作にとって不可欠です。

これは、着信リレーを設定することによって解決されます。着信リレーを設定するときは、Cisco IronPort 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 アドレスおよび送信元 IP アドレスの格納に使用するヘッダーを指定します。内部 MX/MTA に対してインターネット プロトコル バージョン 4（IPv4）またはバージョン 6（IPv6）のアドレスを指定できます。ヘッダーを指定する方法は、カスタム ヘッダーと既存の Received ヘッダーの 2 通りあります。

着信リレーと電子メール セキュリティ モニタ

着信リレー機能を使用する場合、電子メール セキュリティ モニタによって準備されるデータには、外部 IP と MX/MTA の両方のデータが含まれています。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。

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 グループでは、着信リレーからの情報を現時点では使用していないことに注意してください。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。

着信リレーとレポート

着信リレーを使用している場合、電子メール セキュリティ モニタ レポートに示される SenderBase 評価スコアは正しくありません。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、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の SenderBase レピュテーション スコアが表示されます。

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、結果の着信リレーの SenderBase レピュテーション スコアを返します。

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、リレーからすべてのメッセージが、正規のメッセージも含め E 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。

IP アドレス

Cisco IronPort アプライアンスに接続するマシンの IP アドレス（着信リレー）を指定するときは、原則としてできるだけ個別に指定してください。つまり、IP アドレスは、標準 CIDR 形式または IP アドレスの範囲でも入力できます。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。MTA の IPv4 アドレスまたは IPv6 アドレスを使用できます。

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

メッセージ ヘッダーと着信リレー

カスタム ヘッダー

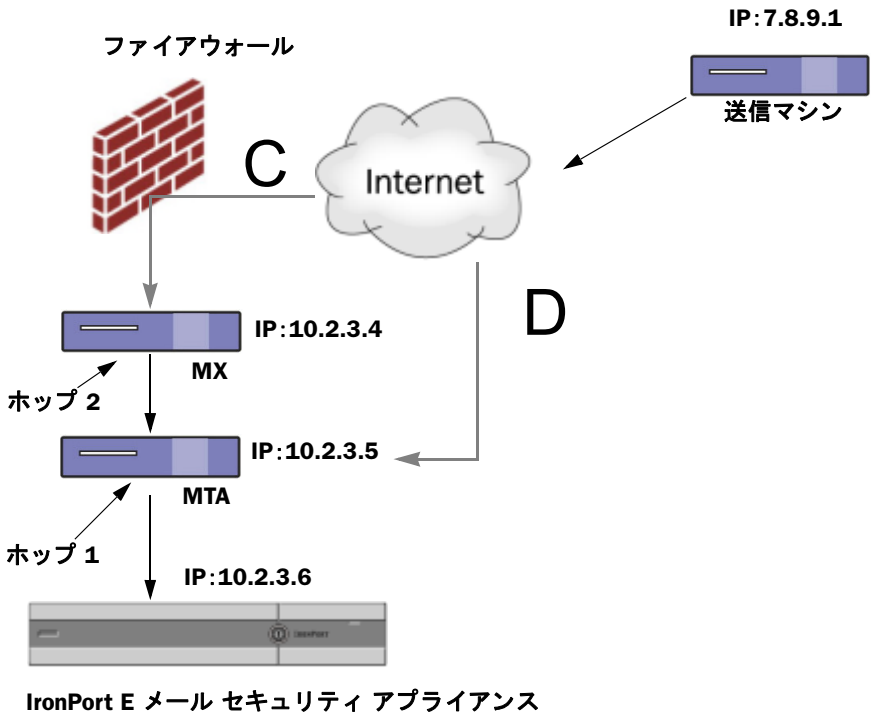
カスタム ヘッダーを指定する場合に、この方法を使用します。これは推奨される方法です。元の送信者に接続するマシンでは、このカスタム ヘッダーを追加する必要があります。このヘッダーの値は、外部の送信マシンの IP アドレスになることが予期されます。次に例を示します。

```
SenderIP: 7.8.9.1
X-CustomHeader: 7.8.9.1
```

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。

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 9-14 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 9-14　MX/MTA によるメール リレー:不定ホップ数



Received ヘッダー

MX/MTA を設定する際に、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らない場合、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」の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 9-13 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 IronPort 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 9-14 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（9-24 ページ）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 IronPort 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、使用されるヘッダーの特定（9-27 ページ）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 IronPort 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。解析対象の文字が見つからないか、有効な IP アドレスが見つからない場合、Cisco IronPort アプライアンスでは、接続元マシンの実際の IP アドレスを使用します。

次のメール ヘッダーの例で左角カッコ（[）と 2 ホップを指定した場合、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（]）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 9-13 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 9-2 に、図 9-13 同様、Cisco IronPort 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 IronPort 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 9-3 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 9-2　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 ESMTP; 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 ESMTP id j8LKkWu1008155 for <joefoo@customerdomain.org>`

表 9-2　一連の Received: ヘッダー(パス A 例 1)(続き)

4	Received: from sending-machine.spamham.com (sending-machine.spamham.com [7.8.9.1]) by mx.customerdomain.org (Postfix) with ESMTP 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 ESMTP; 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 9-2 についての注意事項は、次のとおりです。

ステップ 1　Cisco IronPort アプライアンスでは、これらのヘッダーを無視します。

ステップ 2　Cisco IronPort 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)。

ステップ 3　最初のホップ(着信リレー)。

ステップ 4　第 2 ホップ。これは、送信側 MTA です。IP アドレスは 7.8.9.1 です。

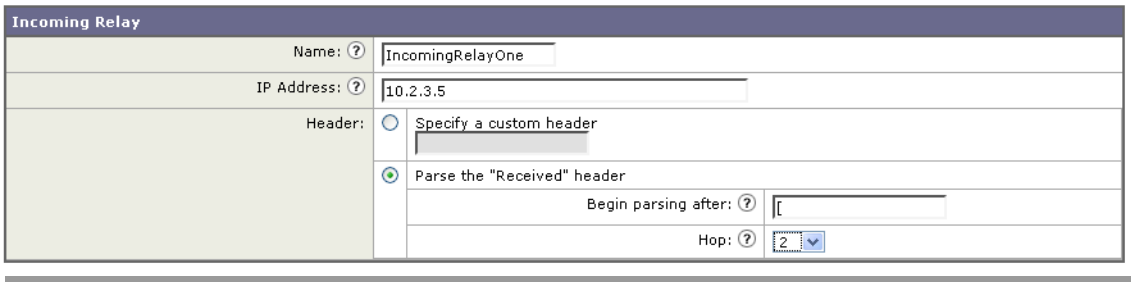
ステップ 5　Cisco IronPort アプライアンスでは、これらの Microsoft Exchange ヘッダーを無視します。

表 9-3　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 ESMTP; 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 ESMTP 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 ESMTP id 4F3DA15AC22 for <joefoo@customerdomain.org>;

図 9-15 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 9-15　設定された着信リレー



使用されるヘッダーの特定

Cisco IronPort 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 IronPort 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、`logconfig` CLI コマンドの `logheaders` サブコマンドを使用して、Received ヘッダーを AsyncOS ロギングに含めるよう設定することです。

```
mail3.example.com> logconfig


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.

- CLUSTERSET - Set how logs are configured in a cluster.

- CLUSTERSHOW - Display how logs are configured in a cluster.

[]> logheaders


Please enter the list of headers you wish to record in the log files.

Separate multiple headers with commas.

[]> Received
```

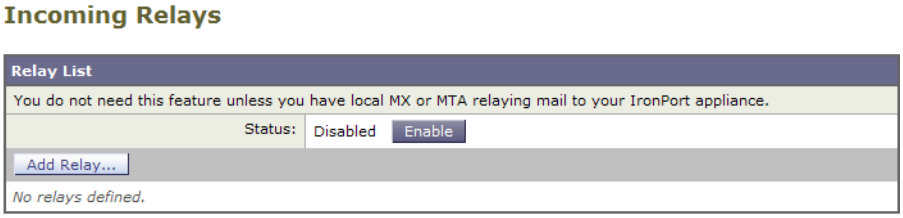
着信リレー機能の設定（GUI）

[着信リレー（Incoming Relays）] ページは [ネットワーク（Network）] タブ経由でアクセスできます。

着信リレー機能をグローバルに有効にする

ステップ 1　[Network] タブの [Incoming Relays] リンクをクリックします。[Incoming Relays] ページが表示されます。

図 9-16　[Incoming Relays] ページ



ステップ 2　[有効（Enable）] をクリックして、着信リレーをイネーブルにします。（イネーブルにした着信リレー機能は、[無効（Disable）] をクリックすることによって、ディセーブルにできます）。

ステップ 3　変更を保存します。

着信リレーとメール ログ

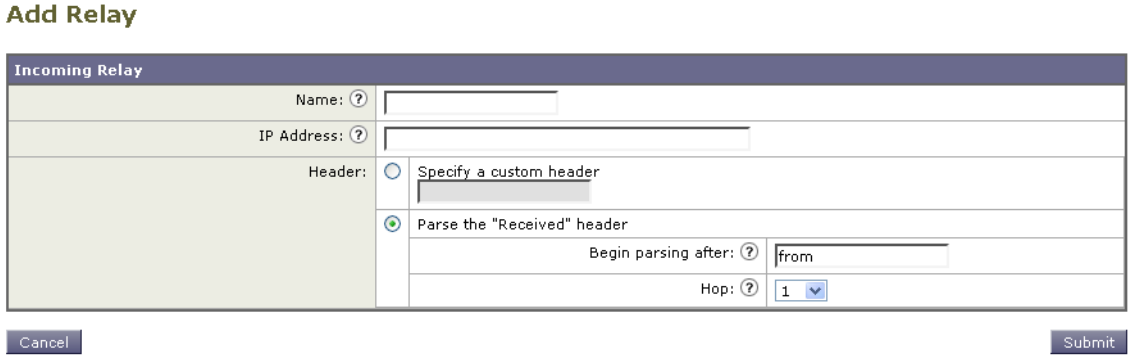
次の例は、着信リレー情報を含む、一般的なログ エントリを示します。

```
Wed Aug 17 11:20:41 2005 Info: MID 58298 IncomingRelay(myrelay): Header Received found,
IP 192.168.230.120 being used
```

リレーの追加

ステップ 1　[着信リレー（Incoming Relays）] ページの [リレーの追加（Add Relay）] ボタンをクリックします。[Add Relay] ページが表示されます。

図 9-17　[Add Relay] ページ



ステップ 2　リレーの名前を入力します。

ステップ 3　リレーの IP アドレスを入力します。有効な IP アドレス エントリの詳細（IPv6 アドレス形式）については、IP アドレス（9-23 ページ）を参照してください。

ステップ 4　ヘッダー タイプ（[Custom] または [Received]）を選択します。カスタム ヘッダーの詳細については、カスタム ヘッダー（9-24 ページ）を参照してください。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。

- カスタム ヘッダーの場合は、ヘッダー名を入力します。
- Received: ヘッダーの場合は、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。詳細については、Received ヘッダー（9-25 ページ）を参照してください。

ステップ 5　変更を保存します。

リレーの編集

ステップ 1　[着信リレー（Incoming Relay）] ページでリレーの名前をクリックします。[Edit Relay] ページが表示されます。

ステップ 2　リレーに変更を加えます。

ステップ 3　変更を保存します。

リレーの削除

ステップ 1　削除するリレーに対応する行のゴミ箱アイコンをクリックします。削除を確認するよう求められます。

ステップ 2　[削除（Delete）] をクリックします。

ステップ 3　変更を保存します。

着信リレーとロギング

次のログの例で、送信者の SenderBase 評価スコアは、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 行目に示されます。

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

CHAPTER 10

アウトブレイク フィルタ

添付ファイルを介したウイルスの蔓延が減少する一方で、フィッシング メッセージ、詐欺、およびマルウェア リンクなどの少量のターゲットを定めた電子メール攻撃は増加しています。非ウィルス性の攻撃に使用されるメッセージは複雑であり進化しています。プロフェッショナルなメッセージを装い、ソーシャル エンジニアリングのトリック（受信者の情報の利用など）を使って、フィッシング Web サイトやマルウェア Web サイトを指し示すカスタム URL を受信者がクリックするように仕向けます。これらの URL は、各受信者または少数の受信者のグループに対して一意にすることができ、これらの Web サイトは、短期間だけオンラインになる、Web セキュリティ サービスにとって未知のサイトです。これらの要因すべてによって、これら小規模の非ウイルス性のアウトブレイクを検出するのは、広範囲のウイルス アウトブレイクやスパム キャンペーンの検出よりもさらに難しくなります。Cisco IronPort アウトブレイク フィルタ機能は、新たなウィルスの発生に加えて、この拡大の一途をたどる標的型攻撃からユーザを保護します。

アウトブレイク フィルタ概要

ユーザから機密情報を盗んだり、マルウェアをコンピュータに配信したりするために設計されたメッセージは、進化し続けており、従来のウイルス対策およびスパム対策のスキャン ソフトウェアによって見逃される可能性があります。感染フィルタは、積極的にアクションを実行して、これらの新しいアウトブレイクに対する防御において、非常に重要な第 1 のレイヤを提供します。Cisco IronPort のアウトブレイク フィルタ機能は、新しい発生をリアルタイムで検出し、疑わしいトラフィックがネットワークに侵入しないように動的に応答することにより、新しいウイルス対策およびスパム対策の更新が導入されるまで保護します。アウトブレイク フィルタは、Cisco IronPort のアウトブレイク検出技術とインテリジェントな隔離システムを使用してユーザを保護します。

アウトブレイク フィルタ機能は、発生したアウトブレイクに関する情報を収集し、このデータを使用してこれらのアウトブレイクがユーザに広がらないようにすることで、ユーザとネットワークを保護します。アウトブレイク フィルタは、受信メッセージを Cisco Security Intelligence Operations（SIO）から公開されているアウトブレイク ルールと比較して、メッセージが大規模なウイルス アウトブレイクの一部であるか、またはより小さい非ウィルス攻撃であるかどうかを判断します。AsyncOS は、アウトブレイク ルールに一致するメッセージに、メッセージの脅威の重大度を示す脅威レベルを割り当て、その脅威レベルを、メール ポリシーに設定した隔離およびメッセージの変更しきい値と比較します。これらのしきい値の 1 つ以上を満たすメッセージは、受信者を保護するために隔離または変更されます。

アウトブレイクの検出とフィルタリングのプロセスは、SIO の一部である SenderBase から開始されます。SenderBase は世界最大の電子メールおよび Web トラフィック監視システムであり、世界の電子メール トラフィックの約 25% を監視しています。Cisco IronPort は、SenderBase の履歴データを使用して、正常なグローバル トラフィック パターンの統計的なビューを作成します。アウトブレイク フィルタは、このデータから作成されたルール セットに依存して、受信メッセージの脅威レベルを判断します。

アウトブレイク フィルタは、機能およびユーザビリティが大幅に拡張されています。大まかには、この拡張には次の内容が含まれます（ただし、これに限定されるものではありません）。

- Cisco Security Intelligence Operations（SIO）によって検出される脅威の種類の増加、およびウイルス アウトブレイクに加えてフィッシング詐欺やマルウェア配布などの非ウイルス攻撃を検出するアウトブレイク ルールを作成するのに使用。
- アダプティブ ルールからのコンテンツ分析と SIO からのアウトブレイク ルールを組み合わせてアウトブレイクを検出することに加えて、非ウイルス性の脅威を検出するために URL をスキャンする CASE（コンテキスト適応スキャンエンジン）スキャン。
- メッセージを定期的に再評価し、アウトブレイク ルールのアップデートに基づいて検疫を自動解除する動的検疫。
- Cisco 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し、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する URL 書き換え。

これらの機能拡張は、アウトブレイクに対するシステムのキャプチャ レートを向上させ、アウトブレイクの可視性を強化し、ユーザのコンピュータや機密情報を保護するように設計されています。

Cisco IronPort アプライアンスには、アウトブレイク フィルタ機能の 30 日間評価ライセンスが付属しています。

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 IronPort Anti-Spam または Cisco IronPort 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、E 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と 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。

アウトブレイク フィルタ：マルチレイヤ対象の保護

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 フィルタ機能は、メッセージを隔離することで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遅らせます。隔離の間、CASE はアップデートされたアウトブレイク ルールを受信し、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。CASE は、メッセージの脅威レベルに基づいて再スキャンの期間を決定します。詳細については、メッセージの遅延（10-5 ページ）を参照してください。

- **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と、感染フィルタは脅威レベルに基づき、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（10-5 ページ）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（10-6 ページ）を参照してください。

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。
- Dynamic Update。アウトブレイク発生時に、Cisco IronPort 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 IronPort E 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`

コンテキスト適応スキャン エンジン

アウトブレイク フィルタには、Cisco IronPort 独自のコンテキスト適応スキャン エンジン（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て、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ときに、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 IronPort Anti-Spam と CASE：概要（9-4 ページ）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 サイトを途中に置いて URL 短縮サービスを経由する 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（10-11 ページ）を参照してください。

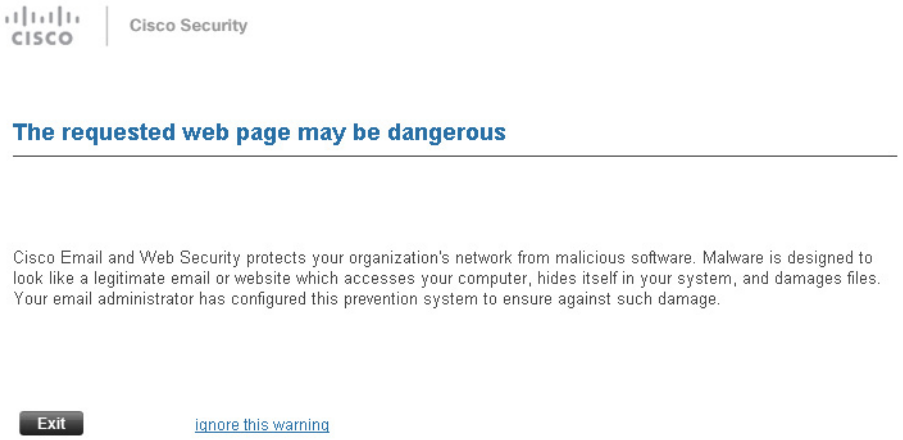
URL のリダイレクト

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（10-19 ページ）を参照してください。

E 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 10-1 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 サイトへ進むか、[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 10-1　　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（10-18 ページ）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 リソースの管理（GUI）（14-14 ページ）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

Cisco IronPort の業界をリードするアウトブレイク フィルタ テクノロジーは、いったんイネーブルにした後は管理者の操作を必要としない、「ファイア アンド フォーゲット」機能（標的を自動的に追尾する能力）を提供します。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。

アウトブレイクのルール

アウトブレイク ルールは、Cisco Security Intelligence Operations の一部である、Cisco IronPort 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 IronPort 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（10-8 ページ）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

適応ルール

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 IronPort 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 IronPort 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 IronPort 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（10-15 ページ）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 IronPort 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 10-1（10-8 ページ）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 10-1　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（Low）	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	最高	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。

脅威レベルとアウトブレイク 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（10-15 ページ）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（10-11 ページ）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 zip（.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を処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 番めのルール（.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 10-2　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 IronPort 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 パイプラインについて（4-1 ページ）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、そのメール ポリシーに対して有効になっている場合は、アンチスパムおよびアンチウイルス スキャン エンジンが実行されます。これらのスキャンを通過するメッセージのみ、感染フィルタ機能によりスキャンされます（感染フィルタ機能によりスキャンされるメッセージの決定に電子メール パイプラインがどのように影響を及ぼすかについての詳細は、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（10-24 ページ）を参照してください）。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。

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（10-7 ページ）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従って、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、E 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 IronPort 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 IronPort 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/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(10-12 ページ)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リリース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、E 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 E 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)

Outbreak 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。検疫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、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Quarantines」の章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 IronPort 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(10-20 ページ)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、より的を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）。

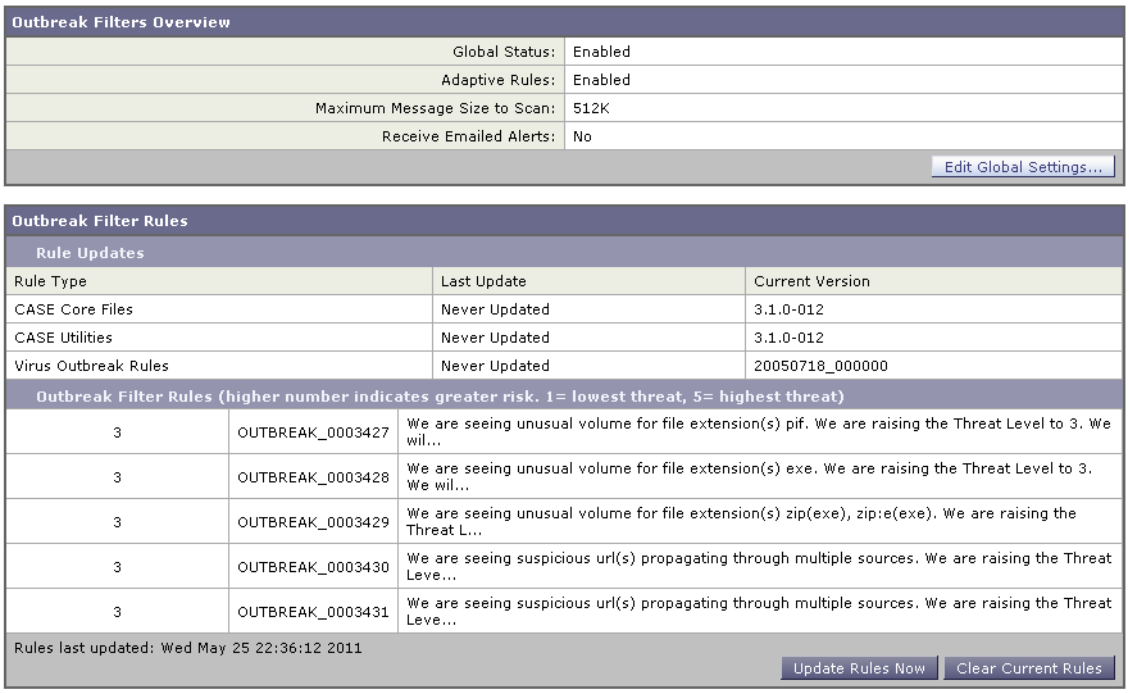
表 10-3　アウトブレイク ライフサイクルのルールの例

時間	ルール タイプ	ルールの説明	操作
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 10-2　[アウトブレイク フィルタ(Outbreak Filters)] メインページ



[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 10-2 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(10-13 ページ)を参照してください。

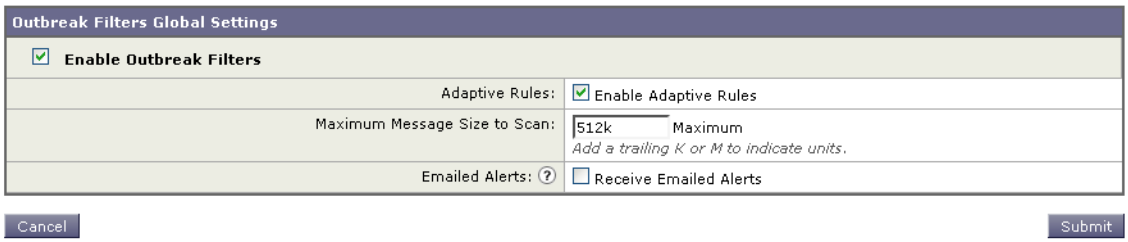
[アウトブレイクフィルタのルール(Outbreak Filter Rules)] セクションには、各種コンポーネント(ルール自体だけでなくルール エンジンも含む)の最新アップデートの時刻、日付、およびバージョンのリストと、脅威レベルと共にアウトブレイク フィルタ ルールのリストが示されます。

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(10-15 ページ)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

感染フィルタのグローバル設定を構成するには、[グローバル設定を編集(Edit Global Settings)] をクリックします。[アウトブレイクフィルタのグローバル設定(Outbreak Filters Global Settings)] ページが表示されます。

図 10-3　[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



このページは、次の目的で使用します。

- 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 コマンドからも使用できます(『*Cisco IronPort 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 フィルタ機能の有効化

アウトブレイク フィルタ機能をグローバルに有効にするには、[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(10-16 ページ)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 IronPort 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(3-22 ページ)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 を有効にするには、[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有効化

[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（10-23 ページ）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 IronPort Security Intelligence Operations から発行されます。Cisco IronPort 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、アップデート設定値の編集（15-9 ページ）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 IronPort アプライアンスが一定期間 Cisco IronPort 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。

[今すぐルールをアップデート（Update Rules Now）] をクリックすることによって、現在のアウトブレイク ルールを手動でアップデートできます。これは、CLI で `outbreakupdate` コマンドを発行することと同じです（『*Cisco IronPort AsyncOS CLI Reference Guide*』を参照）。

アウトブレイク フィルタ ルールのアップデート

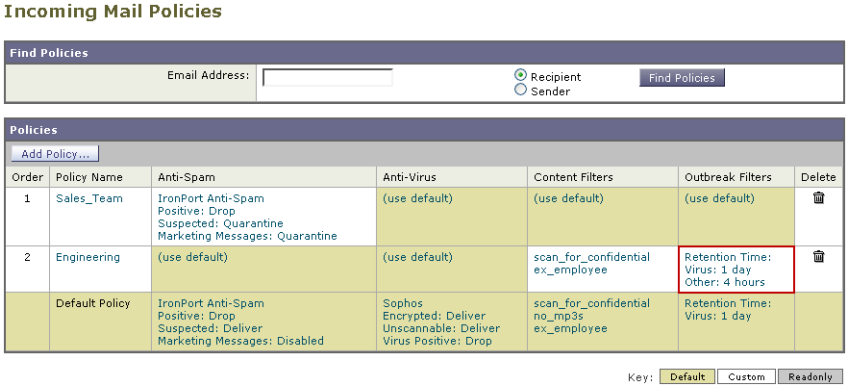
デフォルトでは、Cisco IronPort アプライアンスは 5 分ごとに新しいアウトブレイク フィルタ ルールのダウンロードを試行します。この間隔は、[セキュリティサービス（Security Services）] > [サービスのアップデート（Service Updates）] ページで変更できます。詳細については、サービスのアップデート（15-9 ページ）を参照してください。

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 コマンドからも使用できます（『*Cisco IronPort AsyncOS CLI Reference Guide*』を参照）。

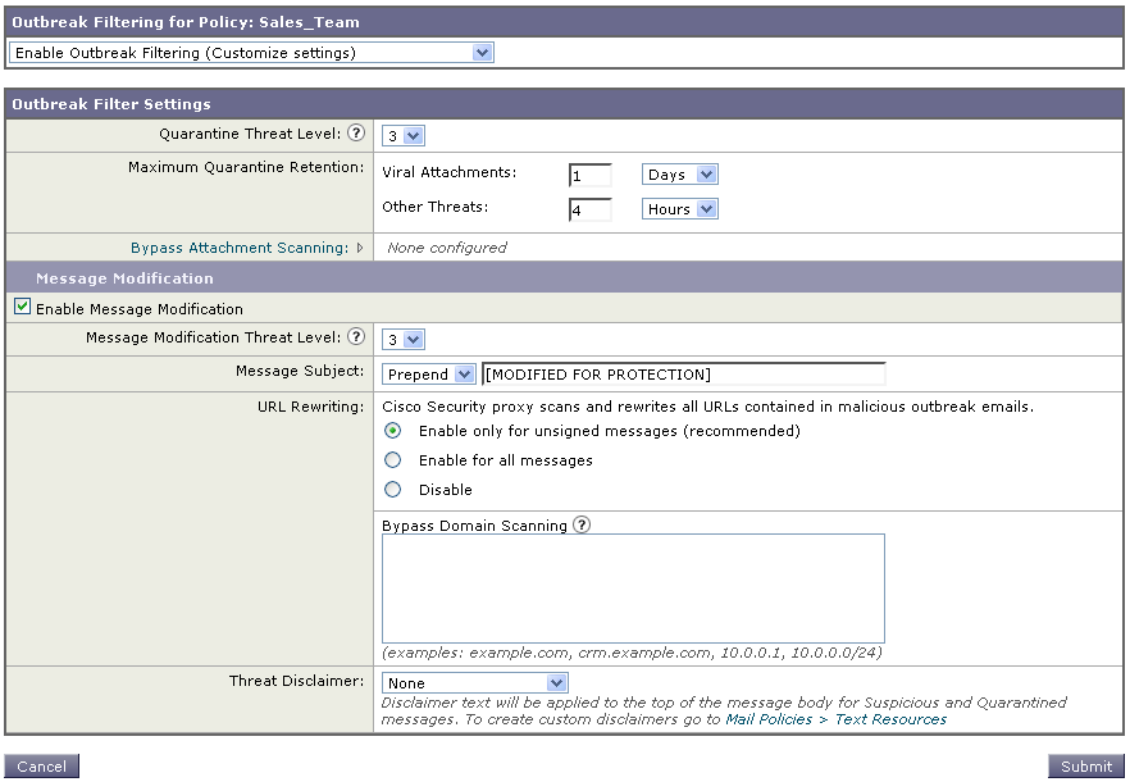
（注）　Cisco IronPort アウトブレイク フィルタ機能が非ウイルス性の脅威をスキャンするために、Anti-Spam または Intelligent Multi-Scan スキャンをアプライアンスでグローバルにイネーブルにする必要があります。

図 10-4　　メール ポリシーのリスト



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。[Outbreak Filter Settings] ページが表示されます。

図 10-5　　アウトブレイク フィルタ設定とメール ポリシー



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（10-8 ページ）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。E 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（10-5 ページ）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）　E 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、E 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

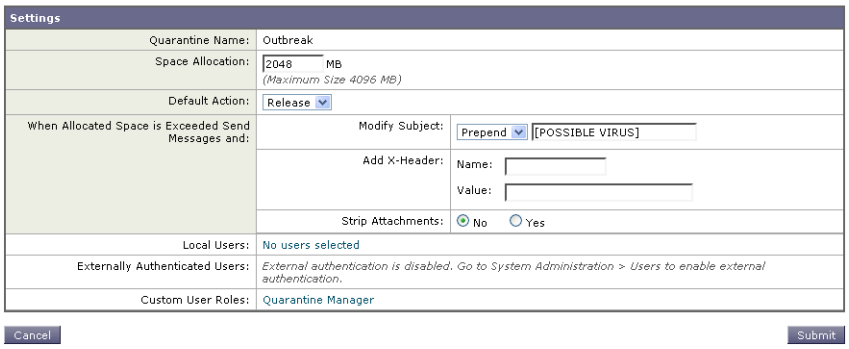
E メール セキュリティ アプライアンスは、疑わしいメッセージのヘッダーの上部に免責事項メッセージを追加して、ユーザにメッセージの内容を警告することができます。この免責事項には、メッセージのタイプに応じて HTML またはプレーン テキストが使用できます。

[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 リソースの管理（GUI）（14-14 ページ）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。この検疫エリアは、メッセージを検疫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、検疫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、その他のあらゆる検疫と同様に機能します（検疫の操作方法の詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Quarantines」の章を参照してください）。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（10-22 ページ）を参照してください。

図 10-6　　アウトブレイク隔離



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、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Quarantines」の章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エリア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。Outbreak 検疫エリアからのメッセージの解放、または Outbreak 検疫のデフォルト アクションの変更に関する詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Quarantines」の章を参照してください。

反対に、新しいルールの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。

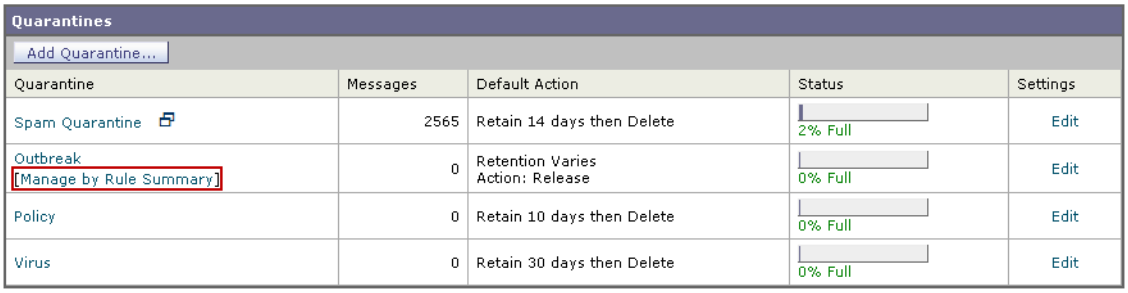
（注）　メッセージが アウトブレイク隔離エリアに留まっている間にアンチウイルス スキャンが（メール ポリシーごとではなく）グローバルにディセーブルにされた場合は、たとえメッセージが解放される前にもう一度アンチウイルス スキャンを再度イネーブルにしたとしても、そのメッセージが解放されたときのアンチウイルス スキャンは実行されません。

（注）　アウトブレイク フィルタ機能は、Cisco IronPort 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。

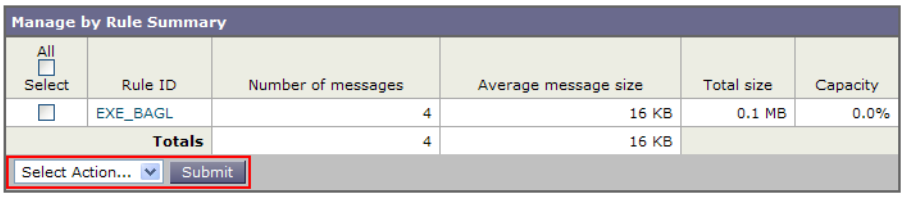
図 10-7　アウトブレイク隔離の [ルールサマリーによる管理（Manage by Rule Summary）] リンク



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 10-8　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



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 IronPort 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 IronPort 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 IronPort 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、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Quarantines」の章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（15-15 ページ）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、Outbreak 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 11

データ損失の防止

情報化時代では、組織のデータが組織の最も大切な財産の 1 つです。組織では多額の費用をかけ、従業員、顧客、パートナーが電子メールや Web 経由でデータを利用できるようにしています。このようにデータ アクセスが増加したため、インターネット上で機密情報や占有情報の悪意または過失による流出をどのように防止するかの答えを見つけ出すことは、情報セキュリティの専門家にとって難問となっています。

シスコでは、E メール セキュリティ アプライアンスを使用して、組織の情報および知的財産を保護し、州および連邦規制に準拠するための以下の方法を提供しています。

- **RSA メール DLP。**機密データの識別と保護を行う統合型データ漏洩防止（DLP）スキャン エンジンと RSA Security Inc. により設計された DLP ポリシー テンプレートを含む E メール セキュリティ アプライアンスにローカルなソリューション。
- **RSA Enterprise Manager。**RSA Enterprise Manager のユーザは、E メール セキュリティ アプライアンスと Enterprise Manager ソフトウェアを連携させ、RSA の DLP 技術を使用して送信メッセージをスキャンできます。RSA メール DLP は個々の E メール セキュリティ アプライアンスにローカルですが、RSA Enterprise Manager では、同じネットワーク上の複数の E メール セキュリティ アプライアンスを中央集中型のインターフェイスから管理できます。RSA の DLP データセンターのユーザは、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できます。Enterprise Manager は RSA のサードパーティ製ソフトウェアであり、シスコからは購入できません。

（注）この章では、E メール セキュリティ アプライアンスを Enterprise Manager に接続するための設定を構成する方法、およびアプライアンスが Enterprise Manager のパートナー デバイスとして動作する方法の概要について説明します。Enterprise Manager とその DLP ポリシーの構成については、オンライン ヘルプおよび技術文書「*Managing Partner Device DLP with Enterprise Manager*」を含め、Enterprise Manager に関する RSA のマニュアルを参照してください。

データ損失防止の概要

Cisco IronPort E メール セキュリティ アプライアンスのデータ損失防止機能により、ユーザが過失によってネットワークから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 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。

このドキュメントでは、*DLP 違反*としての DLP ポリシーに違反するすべてのメッセージ コンテンツ、および *DLP インシデント*としての違反を含むメッセージの発生について説明します。DLP インシデントが発生すると、アプライアンスはメッセージを隔離し、データ セキュリティを担当する組織の担当者に通知を送信するなど、メッセージで適切な処理を行い情報を保護します。

E メール セキュリティ アプライアンスには、統合された DLP スキャン エンジンと、RSA によって作成された一連の DLP ポリシーがあります。これは、このマニュアルおよびアプライアンスで RSA メール DLP と総称されています。DLP 違反がないかメッセージおよび添付ファイルをスキャンするように E メール セキュリティ アプライアンスの送信メール ポリシーを設定できます。RSA メール DLP には、RSA によって設計された 100 を超える DLP ポリシー テンプレートが含まれています。詳細については、RSA メール DLP（11-9 ページ）を参照してください。

RSA Enterprise Manager のユーザは、E 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 Enterprise Manager に接続し、アプライアンスが Enterprise Manager をネットワーク上の複数のアプライアンスの集中管理インターフェイスとして使用できるようにできます。Enterprise Manager では、ローカルの E メール セキュリティ アプライアンス上で RSP メール DLP よりも幅広い DLP テクノロジーが提供されます。

RSA メール DLP のポリシーはアプライアンス上でローカルに構成されますが、Enterprise Manager はクラスタ化されたアプライアンスを含む複数の E 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、送信メール ポリシーが DLP スキャンを実行するときにそれらのポリシーをアプライアンスにプッシュします。

DLP スキャンは、イネーブルになっていれば、感染フィルタの段階の直後にアプライアンスの「ワーク キュー」で発信メールに対して実行されます。詳細については、メッセージ分裂（6-5 ページ）を参照してください。

データ消失防止のグローバル設定

機密データがないか発信電子メールをスキャンするには、最初に [セキュリティサービス（Security Services）] > [RSA メール DLP（RSA Email DLP）] ページを使用してデータ損失防止機能をイネーブルにします。データ損失防止に RSA Enterprise Manager を使用するか、または RSA メール DLP を使用するかを選択できます。

ローカル E メール セキュリティ アプライアンスで DLP ポリシーを設定および管理する場合は、RSA メール DLP を選択します。DLP Assessment Wizard を実行して、アプライアンス上で最も一般的な DLP ポリシーを有効にするか、または DLP ポリシーを手動で設定するかを選択できます。DLP Assessment Wizard の起動方法については、DLP Assessment Wizard の使用（11-17 ページ）を参照してください。DLP ポリシーを手動で設定する方法については、DLP Policy Manager（11-11 ページ）を参照してください。

RSA メール DLP をイネーブルにすると、電子メール セキュリティ マネージャを使って発信メール ポリシーでそのポリシーをイネーブルにできます。詳細については、DLP の受信者ごとのポリシーの設定（11-32 ページ）を参照してください。すべてまたは選択した米国州で米国運転免許証分類子を有効にします。米国運転免許証分類子は、個人識別情報（PII）を保護する DLP ポリシーで一般的に使用されます。多くの米国の州では、PII を保護し、PII が悪用されている、または悪用されている可能性が高い場合に、個人および情報の所有者に通知するよう企業に求める法律があります。米国運転免許証分類子を使用する DLP ポリシーの例には、California SB-1386、Texas SB-122 および New York AB-4254 が含まれます。分類子の詳細については、コンテンツ照合分類子（11-20 ページ）を参照してください。

Enterprise Manager を使用してアプライアンスの DLP ポリシーを構成および管理する場合は、RSA Enterprise Manager を選択します。Enterprise Manager は、E メール セキュリティ アプライアンスから送信メール ポリシーおよびメッセージ アクション定義を受信し、DLP ポリシーを接続された E メール セキュリティ アプライアンスにプッシュします。管理者は、DLP インシデントを表示し、Enterprise Manager を使用して隔離領域からメッセージを削除または解放するコマンドを送信することもできます。

RSA メール DLP および RSA Enterprise Manager の両方で、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。アプライアンスでこの情報を記録しない場合は、このオプションを選択しないでください。

RSA メール DLP を使用して、必要に応じてローカル アプライアンスのデータ損失防止の管理に切り替えることができます。

イネーブル化 RSA メール DLP

（注） DLP Assessment Wizard を使って、アプライアンスの DLP ポリシーを設定するには、DLP Assessment Wizard の使用（11-17 ページ）を参照してください。

ステップ 1　[Security Services] > [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が表示されます。

（注） ライセンス契約に合意しない場合、RSA メール 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　ページの下部までスクロールし、[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 5　[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 6　[RSA メールデータ漏洩防止を有効にする（Enable RSA Email Data Loss Prevention）] チェックボックスをオンにします。

ステップ 7　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への記録をイネーブルにするかしないか選択します。これを選択すると、Cisco IronPort 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 8　変更を送信し、保存します。

RSA Enterprise Manager のイネーブル化

RSA Enterprise Manager を使用してアプライアンスのデータ損失防止を管理する場合は、E メール セキュリティ アプライアンスを Enterprise Manager のパートナー デバイスとして設定する必要があります。RSA Enterprise Manager の設定を構成した後、E 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。次に Enterprise Manager を開くと、アプライアンスはパートナー デバイスとして表示されます。

E メール セキュリティア プライアンスと Enterprise Manager 間の通信に SSL を使用する場合は、認証局の証明書ファイルとともに、サーバおよびクライアント証明書として使用する 1 つ以上の証明書をアプライアンスにインポートします。サーバ証明書とクライアント証明書は同じ証明書にすることができますが、E メール セキュリティ アプライアンスのホスト名を共通名にする必要があります。RSA が提供する証明書生成ツールを使用して証明書を作成できます（選択した場合）。詳細については、証明書（11-28 ページ）を参照してください。

E メール セキュリティ アプライアンスのデータを RSA Enterprise Manager モードに切り替えると、E 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。

（注） E メール セキュリティ アプライアンスの DLP ポリシーの管理については、Enterprise Manager に関する RSA の技術マニュアルを参照してください。

ステップ 1　[Security Services] > [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が表示されます。

（注） ライセンス契約に合意しない場合、RSA メール 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　ページの下部までスクロールし、[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 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 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　Enterprise Manager が接続する E メール セキュリティのサービス ポートを入力します。

ステップ 8　E メール セキュリティ アプライアンスと Enterprise Manager の接続で SSL を使用する場合は、[SSL 通信を有効にする（Enable SSL Communication）] チェックボックスをオンにし、Enterprise Manager のサーバ証明書と E メール セキュリティ アプライアンスのクライアント証明書を選択します。証明書では、アプライアンスのホスト名を共通名にする必要があります。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。

アプライアンスと Enterprise Manager 間の SSL 通信用の証明書の設定については、証明書（11-28 ページ）を参照してください。

ステップ 9　ソース コードとドキュメント検出のフィンガープリントを有効にするかどうかを選択します。このオプションを選択すると、Enterprise Manager はフィンガープリント検出コンテンツを E メール セキュリティ アプライアンスに送信します。フィンガープリントは、次の検出に使用できます。

- 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、完全バイナリ一致

ステップ 10　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への記録をイネーブルにするかしないか選択します。これを選択すると、Cisco IronPort 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 11　変更を送信し、保存します。

DLP 設定のエクスポート

既存の RSA メール DLP 構成内のアクティブ ポリシーを Enterprise Manager に使用する場合は、構成を .zip ファイルとしてエクスポートし、ポリシーを Enterprise Manager にインポートできます。

.zip ファイルを作成するには、[データ漏洩防止設定（Data Loss Prevention Settings）] ページで [DLP 設定のエクスポート（Export DLP Configuration）] をクリックします。.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。E メール セキュリティ アプライアンスには、送信メールに割り当てられたすべてのアクティブな DLP ポリシーが .zip ファイルに含まれています。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 は .zip ファイルに含まれていません。

E 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最も低い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。

アプライアンスが DLP に RSA Enterprise Manager を使用している場合は、これらの手順を使用して、Enterprise Manager がアプライアンスに送信したアクティブな DLP ポリシーをエクスポートできます。

ファイルを Enterprise Manager でインポートする準備ができました。構成を Enterprise Manager にインポートする手順については、RSA Enterprise Manager のヘルプを参照してください。

データ損失防止モードの切り替え

RSA Enterprise Manager を使用した後にデータ損失防止のために RSA メール DLP を使用する場合は、[グローバル設定（Global Settings）] ページを使用して、イネーブル化 RSA メール DLP（11-3 ページ）の手順に従って RSA メール DLP モードに戻ります。

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、事前定義されたテンプレートをもとにした Email DLP ポリシーの作成（11-13 ページ）を参照してください。

Enterprise Manager を使用したアプライアンスの DLP ポリシーの管理を停止する場合は、Enterprise Manager のパートナー デバイスとしての E メール セキュリティ アプライアンスを削除する方法について RSA Enterprise Manager のヘルプを参照してください。

メッセージ アクション

E メール セキュリティ アプライアンスは、発信メッセージ内に DLP 違反を検出すると、メッセージの処理方法を認識する必要があります。メッセージ アクションは、E メール セキュリティ アプライアンスがメッセージに対して取る *プライマリ アクション*（配信、廃棄、または隔離のいずれか）を定義します。メッセージに対して行う *セカンダリ アクション*を指定することもできます。セカンダリ アクションは次のとおりです。

- メッセージの配信を選択した場合は、システム隔離へのコピーの送信。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、以降の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。

Ignore を除くすべての DLP ポリシーの重大度レベルで、メッセージ アクションを実行できます。RSA メール DLP の重大度レベルの詳細については、重大度レベルの設定（11-16 ページ）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は検疫し、コンプライアンス責任者に通知を送信しますが、重大度レベルが低いメッセージは配信する、といったことです。

RSA メール DLP の場合は、DLP ポリシー マネージャを使用してポリシーを作成または編集するときに DLP ポリシーで使用するメッセージ アクションを指定します。詳細については、DLP Policy Manager（11-11 ページ）を参照してください。

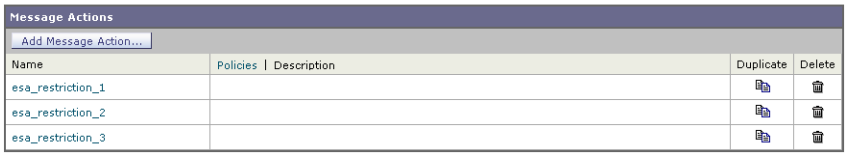
RSA Enterprise Manager の場合は、E メール セキュリティ アプライアンスで最初にメッセージ アクションを作成します。アプライアンスによってメッセージ アクションの名前とメタデータが Enterprise Manager に送信されるので、Enterprise Manager で作成および管理する DLP ポリシーでそのアクションを使用できます。詳細については、RSA Enterprise Manager の技術マニュアルを参照してください。

既存の DLP ポリシーを含むアプライアンスを AsyncOS 7.6 にアップグレードすると、オペレーティング システムは既存のポリシーで定義されたアクションをメッセージ アクションに自動的に変換し、それに従ってポリシーを更新します。AsyncOS によってメッセージ アクションの名前が生成されますが、GUI の [DLP メッセージアクション（DLP Message Actions）] ページを使用して名前を変更できます。アクションの名前を変更する方法については、メッセージ アクションの編集（11-8 ページ）を参照してください。

[DLP メッセージアクション（DLP Message Actions）] ページには、アプライアンス上のアクションのリストが表示されます。[メッセージアクション（Message Actions）] テーブルの [ポリシー（Policies）] リンクをクリックすると、各アクションが割り当てられているポリシーが表示されます。各アクションの説明を表示するには、[説明（Description）] リンクをクリックします。

図 11-1　　E メール セキュリティ アプライアンス上のアクションのリスト

DLP Policy Manager: Message Actions

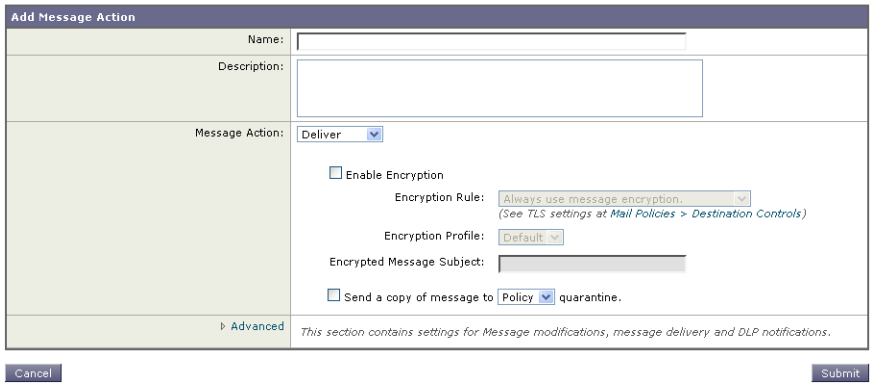


メッセージ アクションの作成

ステップ 1　[メールポリシー（Mail Policies）] > [DLP メッセージアクション（DLP Message Actions）] を選択します。

ステップ 2　[メッセージアクションの追加（Add Message Action）] をクリックします。[メッセージアクションの追加（Add Message Action）] ページが表示されます。

DLP Policy Manager: Add Message Action



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、システム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　配信時にメッセージを暗号化する場合や、隔離からメッセージを解放する場合は、[暗号化を有効にする（Enable Encryption）] チェックボックスをオンにして、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。

  DLP の通知については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Text Resources」の章を参照してください。

ステップ 9　変更を送信し、保存します。

メッセージ アクションの編集

ステップ 1　[セキュリティ設定（Security Settings）] > [DLP メッセージアクション（DLP Message Actions）] を選択します。

ステップ 2　編集するメッセージ アクションの名前をクリックします。

ステップ 3　メッセージ アクションを変更します。

ステップ 4　変更を送信し、保存します。

メッセージ アクションの削除

メッセージ アクションを削除するには、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。確認メッセージが 1 つ以上の DLP ポリシーで使用されているかを示します。メッセージ アクションを削除すると、これらの DLP ポリシーから削除されます。変更を送信し、保存します。

メッセージ アクションの複製

既存のメッセージ アクションとほぼ同じで設定が異なるアクションを作成する場合は、複製メッセージ アクションを作成することができます。

ステップ 1　[DLP メッセージアクション（DLP Message Actions）] ページで、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 2　新しいメッセージ アクションの名前を入力します。

ステップ 3　メッセージ アクションの設定に変更を加えます。

ステップ 4　変更を送信し、保存します。

RSA メール DLP

RSA メール DLP では、DLP ポリシーを個々の E メール セキュリティ アプライアンスにローカルで作成および管理できます。

RSA メール DLP の動作を理解する

RSA メール DLP 機能では、3 つのレベルのポリシー構造を使用して、送信メッセージ内の機密データを検出するための組織のデータ損失防止ルールを定義します。

- **検出ルール。**最も低いレベルの場合、DLP コンテンツ スキャンは、テキストのブロック内に特定のパターンがないかスキャンする*検出ルール*で構成されています。これらの検出ルールには、正規表現、単語やフレーズ、ディクショナリ、以前の AsyncOS で使用されていたスマート ID に似たエンティティなどがあります。
- **コンテンツ照合分類子。**次のレベルは*コンテンツ照合分類子*であり、発信メッセージと、添付ファイルおよびヘッダーにクレジット カード データや他の個人データなどの機密情報がないかスキャンします。分類子には、さらなる条件を適用する*コンテキスト ルール*を伴う検出ルールが多数あります。例として、RSA が開発したクレジット カード番号分類子を検討します。この分類子は、メッセージがクレジット カード番号のパターンに一致するテキスト文字列を含むだけではなく、有効期限、クレジット カード会社名（Visa、AMEX など）、使用者の名前および住所などの補足情報も含むように定めています。この追加情報を必須とすることで、メッセージ コンテンツの判断がより正確となり、誤検出も少なくなります。分類子が、メッセージ内に機密情報を検出すると、*DLP 違反*が発生します。
- **DLP ポリシー。**最も高いレベルは、*DLP ポリシー*で、条件のセットと、割り当てられたメッセージ アクションから成ります。条件には、送信者、受信者、添付ファイルのタイプなどの、メッセージのコンテンツに対する分類子とメッセージ メタデータのテストが含まれます。メッセージ アクションでは、メッセージに対する全体的なアクション（配信、ドロップ、または検疫）、およびメッセージの暗号化、ヘッダーの変更、組織のメンバーへの通知の送信といった二次的なアクションの両方を指定します。

DLP Policy Manager で組織の DLP ポリシーを定義し、発信メール ポリシーで DLP ポリシーをイネーブルにします。アプライアンスは、「ワークキュー」のアウトブレイク フィルタ ステージ後に、DLP ポリシー違反がないか送信メッセージをスキャンします。AsyncOS では DLP Assessment Wizard も提供され、それに沿って最も一般的な DLP ポリシーの設定を行うことができます。詳細については、DLP Assessment Wizard の使用（11-17 ページ）を参照してください。

RSA Email DLP スキャン エンジンは、発信メール ポリシーでイネーブルになっている DLP ポリシーの分類子をすべて使って、各メッセージとそのヘッダーおよび添付ファイルをスキャンします。メッセージ ヘッダーをスキャンするために、Cisco IronPort アプライアンスのコンテンツ スキャン エンジンは、ヘッダーをメッセージ本文またはコンテンツのすべての MIME 部分に付加し、RSA メール DLP スキャン エンジンは、コンテンツ照合分類子スキャンを実行します。添付ファイルをスキャンするために、アプライアンスのコンテンツ スキャン エンジンは添付ファイルを抽出し、RSA メール DLP スキャン エンジンが分析します。

スキャンが完了すると、RSA メール DLP エンジンが、イネーブルになっている DLP ポリシーのいずれかに対してメッセージが違反していないか確認します。違反が複数の DLP ポリシーに一致している場合、RSA メール DLP エンジンは、発信メール ポリシーのリストを上から順に調べ、最初に一致する DLP ポリシーを選択します。DLP Policy Manager で DLP ポリシーの順序を定義します。

RSA メール DLP エンジンは、最初に DLP 違反の *リスク要因*スコアを計算することで、メッセージの取り扱い方を決定します。リスク要因スコアは、DLP 違反の重大度を 0 ～ 100 の範囲で示します。RSA メール DLP エンジンは、リスク要因スコアを DLP ポリシー用に定義されている重大度基準と比較します。重大度基準は、想定される DLP 違反を次の重大度レベルの 1 つに区分します。

- [無視（Ignore）]
- 低
- 中
- 高（High）
- クリティカル（Critical）

重大度レベルにより、メッセージに適用されるアクション（設定されていれば）が決まります。

DLP インシデント レポートを使って、発信メールで検出された DLP 違反の情報を見ることができます。また、メッセージ トラッキングを使って、DLP 違反の重大度をもとにしたメッセージの検索もできます。

- DLP 電子メール ポリシーおよびコンテンツ照合分類子の詳細については、DLP ポリシー（11-11 ページ）を参照してください。
- コンテンツ照合分類子の詳細については、コンテンツ照合分類子（11-20 ページ）を参照してください。
- DLP インシデント レポートの詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Using Email Security Monitor」の章を参照してください。
- メッセージ トラッキングでの、DLP 違反があるメッセージの検索については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Tracking Email Messages」の章を参照してください。

（注） スキャン エンジンは、メッセージのスキャン時に分類子を 1 回だけ使用します。1 つの発信メール ポリシーに同じ分類子を使う 2 つ以上の DLP ポリシーがある場合、ポリシーは 1 つの分類子によるスキャンの結果を使用します。

ハードウェア要件

RSA Email DLP 機能は、すべての C-Series および X-Series アプライアンスでサポートされます。ただし、C10、C30、C60、C100、C300D、C350D、C360D、および C370D アプライアンスは除きます。

DLP ポリシー

DLP ポリシーは、発信メッセージが機密データとアクションを含んでいるか RSA メール DLP スキャン エンジンが判断するために使う条件と、メッセージにそのようなデータが含まれている場合 AsyncOS が講じるアクションとを組み合わせたものです。

DLP ポリシーには、RSA が開発したコンテンツ照合分類子が含まれます。分類子は、RSA メール DLP スキャン エンジンによって、メッセージおよび添付ファイル内の機密データ検出のため、使用されます。分類子は、クレジット カード番号や運転免許 ID のようなデータ パターンを探すだけでなく、パターンのコンテキストも検査するため誤検出が少なくなります。詳細については、コンテンツ照合分類子（11-20 ページ）を参照してください。

RSA メール DLP スキャンが行われる前に、AsyncOS のコンテンツ スキャン エンジンは送信元、送信先、CC、および件名のヘッダーをメッセージ本文またはコンテンツのタグが付けられたすべての MIME 部分に付加します。これにより、RSA メール DLP スキャン エンジンは、DLP ポリシーのコンテンツ照合分類子を使用してこれらのヘッダーをスキャンできるようになります。

DLP スキャン エンジンが、メッセージや添付ファイルで DLP 違反を検出すると、DLP スキャン エンジンは、違反のリスク要因を決定し、その結果をマッチング DLP ポリシーに返します。ポリシーは、独自の重大度基準を使ってリスク要因をもとに DLP 違反の重大度を評価し、メッセージに対して適切なアクションを適用します。その基準には、Ignore、Low、Medium、High、Critical の 5 つの重大度レベルがあります。Ignore を除き、各重大度ごとにメッセージ アクションを指定して、E メール セキュリティ アプライアンスによるメッセージの処理方法を決定します。メッセージ アクションの詳細については、メッセージ アクション（11-6 ページ）を参照してください。

ポリシーのコンテンツ

Email DLP ポリシーには次の情報が含まれます。

- ポリシーの名称と説明。
- コンテンツ照合分類子の一覧。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の場合があります。詳細については、コンテンツ照合分類子（11-20 ページ）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。詳細については、送信者および受信者のフィルタリング（11-15 ページ）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。詳細については、添付ファイルの種類に基づいたフィルタリング（11-15 ページ）を参照してください。
- 重大度の設定。設定に適用されるメッセージ アクションおよび重大度基準の調整を含みます。詳細については、重大度レベルの設定（11-16 ページ）を参照してください。

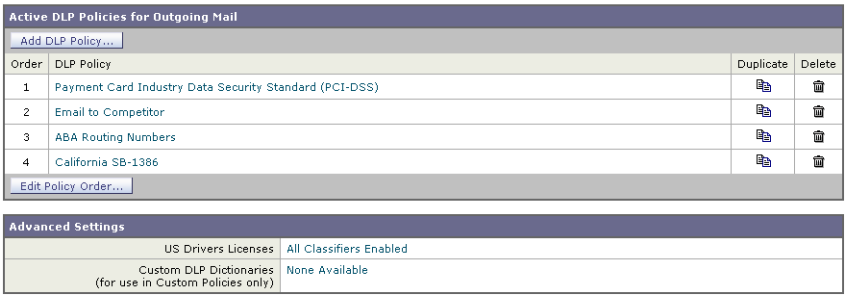
DLP Policy Manager

DLP Policy Manager は、Cisco IronPort アプライアンス上で DLP ポリシーをすべて管理する単一のダッシュボードです。DLP Policy Manager は [Mail Policies] メニューからアクセスします。DLP Policy Manager から、次のアクションを実行できます。

- 事前定義されたテンプレートをもとにした DLP ポリシーの作成および管理。詳細については、事前定義されたテンプレートをもとにした Email DLP ポリシーの作成（11-13 ページ）を参照してください。
- カスタム テンプレートをもとにした DLP ポリシーの作成および管理。詳細については、Custom Policy テンプレートを使用した DLP ポリシーの作成（11-26 ページ）を参照してください。

- カスタム DLP ディクショナリの作成、インポートおよび管理。詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Text Resources」の章を参照してください。
- 米国運転免許証分類子の管理。詳細については、米国運転免許証分類子（11-13 ページ）を参照してください。

図 11-2　アクティブな DLP ポリシーがある DLP Policy Manager

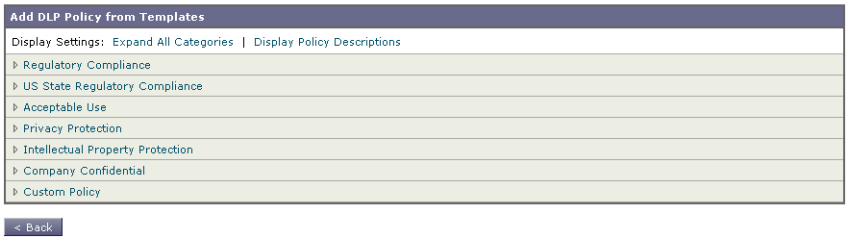


RSA メール DLP ポリシー テンプレート

AsyncOS には、組織の知的財産や極秘情報を保護する、RSA, Inc. の開発による事前定義されたポリシー テンプレートが多数あり、法や業界標準で規定されているルールや規制を強制的に適用します。DLP Policy Manager を使って DLP ポリシーを作成するときには、最初に使用するテンプレートを選択します。

図 11-3 は、使用可能な DLP ポリシー テンプレートのカテゴリを示しています。

図 11-3　テンプレートから DLP ポリシーを追加



DLP ポリシー テンプレートは次のカテゴリに整理されます。

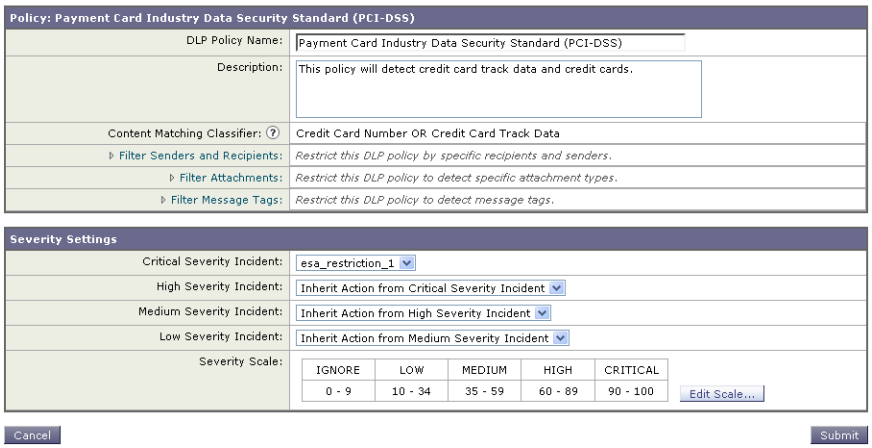
- [規制コンプライアンス（Regulatory Compliance）]。個人情報、クレジット情報、他の保護情報や非公開情報を含むメッセージおよび添付ファイルを識別します。
- [許可された使用（Acceptable Use）]。競合他社や制限された受信者に送信するメッセージで、組織に関する機密情報を含むものを識別します。
- [プライバシー保護（Privacy Protection）]。金融口座、税金記録、国民 ID の識別番号を含むメッセージおよび添付ファイルを識別します。
- [知的財産保護（Intellectual Property Protection）]。よく使われるパブリッシングおよびデザイン 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）]。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）]。AsyncOS では、RSA や組織で開発された分類子を使って、独自のポリシーをゼロから作成するオプションもあります。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。詳細については、高度な RSA メール DLP ポリシーのカスタマイズ（11-26 ページ）を参照してください。

カスタマイズが必要な DLP ポリシー テンプレートについては、DLP ポリシーに対する分類子のカスタマイズ（11-14 ページ）を参照してください。

図 11-4 に、PCI DSS（クレジット カード データ保護基準）違反を検出するための定義済みの RSA ポリシー テンプレートを示します。

図 11-4　事前定義された RSA メール DLP ポリシー テンプレート



米国運転免許証分類子

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証を検索します。誤検出またはアプライアンスのパフォーマンスが問題となるようであれば、DLP Policy Manager の [詳細設定（Advanced Settings）] の下の米国運転免許証用のリンクをクリックして、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。RSA スキャン エンジンが運転免許分類子をどのように使用するかについては、米国運転免許証（11-23 ページ）参照してください。

事前定義されたテンプレートをもとにした Email DLP ポリシーの作成

DLP ポリシーは、事前定義されたテンプレートまたはカスタム テンプレートのいずれかを使用して、作成可能です。カスタム テンプレートの使用方法については、Custom Policy テンプレートを使用した DLP ポリシーの作成（11-26 ページ）を参照してください。

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 メール DLP ポリシー テンプレートの一覧を表示します。

（注）　[ポリシーの説明を表示（Display Policy Descriptions）] をクリックして、使用可能なポリシー テンプレートの詳細な説明を表示することができます。

ステップ 4　使用する RSA メール DLP ポリシー テンプレートの [追加（Add）] をクリックします。

図 11-4（11-13 ページ）とほぼ同じページが開きます。事前定義されたテンプレートすべてに名前と説明がありますが、変更できます。テンプレートのほとんどには 1 つ以上の分類子があり、いくつかのテンプレートにはメッセージのフィルタリングに関する事前定義された添付ファイルのタイプがあります。

ステップ 5　ポリシーが、カスタマイズされた分類子を必要とする場合は、組織の識別番号付けシステムのパターンと、識別番号に関連する単語やフレーズの一覧を定義するための正規表現を入力します。詳細については、DLP ポリシーに対する分類子のカスタマイズ（11-14 ページ）を参照してください。

（注）　事前定義されたテンプレートをもとにしたポリシーでは、分類子の追加および削除はできません。

ステップ 6　任意で、DLP ポリシーの適用を、特定の受信者や送信者、添付ファイルのタイプやメッセージ タグを持つメッセージに限定することができます。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（11-15 ページ）を参照してください。

ステップ 7　[クリティカル重大度の設定（Critical Severity Settings）] セクションで、重大な DLP 違反を含むメッセージで実行するアクションを選択します。

ステップ 8　デフォルトでは、他の重大度レベルは、メッセージ アクションを 1 つ上のレベルから継承します。高、中、または低の重大度に一致するメッセージに異なる設定を定義する場合は、アプライアンスが実行するメッセージ アクションを選択します。

ステップ 9　ポリシーに対して DLP 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）] をクリックして設定を調整します。詳細については、重大度レベルの設定（11-16 ページ）を参照してください。

ステップ 10　変更を送信し、保存します。

ポリシーが DLP Policy Manager に追加されます。

DLP ポリシーに対する分類子のカスタマイズ

DLP ポリシー テンプレートには、より効果的にするためカスタマイズされた分類子を必要とするものもあります。このような分類子は、発信メッセージ内に患者や学生の識別番号など極秘の識別番号がないか検索しますが、組織の記録番号付けシステムのパターンを定義する正規表現を 1 つ以上必要とします。補足情報の記録識別番号に関連する単語およびフレーズの一覧を追加することもできます。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。これにより、false positive が少なくなります。

たとえば、HIPAA および HITECH テンプレートを使用して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。分類子の正規表現 `[0-9]{3}\-[A-Z]{2}[0-9]{6}` を入力します。この正規表現では、123-CL456789 というパターンの番号が検出されます。関連フレーズとして「Patient ID」と入力します。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。変更を送信し、保存します。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。

正規表現の作成方法については、コンテンツ照合分類子用の正規表現（11-24 ページ）を参照してください。コンテンツ照合分類子がどのようにして DLP 違反を検出するかの詳細については、コンテンツ照合分類子（11-20 ページ）参照してください。

DLP ポリシーのメッセージのフィルタリング

AsyncOS が検出した特定の情報に基づいて、DLP ポリシーの適用をメッセージのスキャンのみに限定できます。次の情報に従って、DLP ポリシー スキャンを制限できます。

- 送信者および受信者
- 添付タイプ
- メッセージ タグ

送信者および受信者のフィルタリング

次の方法の 1 つで、DLP ポリシーを特定の受信者または送信者のメッセージだけをスキャンするように限定できます。

- 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`

改行やカンマで、複数のエントリを分離できます。

発信メッセージに対して、AsyncOS は最初に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ます。受信者または送信者が一致したら、RSA メール DLP は、送信者または受信者がメール ポリシーでイネーブルとなっている DLP ポリシーと一致するか照合します。

添付ファイルの種類に基づいたフィルタリング

DLP ポリシーの適用を特定の添付ファイルのタイプを持つメッセージに限定することができます。最初に添付ファイルが AsyncOS のコンテンツ スキャン エンジンにより抽出され、次に添付ファイルの内容が RSA メール DLP スキャン エンジンによってスキャンされます。アプライアンスでは、多数の事前定義されたファイル タイプをスキャンで使用できますが、一覧にないファイル タイプを指定することもできます。事前定義されていないファイル タイプを指定した場合、AsyncOS は添付ファイルの拡張子に基づいてファイル タイプを検索します。RSA メール DLP のスキャンを、最小ファイル サイズ（バイト）以上の添付ファイルに限定することができます。

メッセージ タグによるフィルタリング

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。DLP ポリシー作成時に、発信メッセージのフィルタリングに使用するメッセージ タグを選択します。詳細については、コンテンツ フィルタのアクション（6-15 ページ）、および『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Using Message Filters to Enforce Mail Policies」を参照してください。

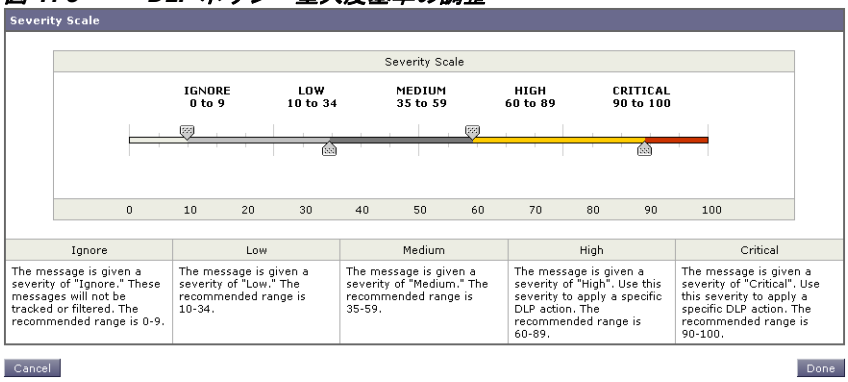
重大度レベルの設定

RSA メール DLPスキャン エンジンが DLP 違反を検出すると、違反の重大度を示すリスク要因スコア（0 ～ 100 の範囲）を計算します。ポリシーは、リスク要因スコアを重大度基準と比較します。重大度基準には、Ignore、Low、Medium、High、Critical の 5 つの重大度レベルがあります。重大度レベルで、メッセージに適用されるアクションが決まります。デフォルトで、すべての重大度レベル（Ignore を除く）で高位の重大度レベルの設定を継承するようになっています。High の重大度レベルは Critical から設定を継承し、Medium は High から、Low は Medium から継承します。レベルを編集し、異なる重大度に対して別々のアクションを指定することができます。

DLP スキャン エンジンのリスク要因の計算については、RSA メール DLP の動作を理解する（11-9 ページ）を参照してください。

重大度基準をポリシーに対して調整し、スキャン エンジンが返す DLP 違反の推定重大度を規定できます。図 11-5 は重大度基準を示します。スケールの矢印を使用して、重大度レベルのスコアを調整します。

図 11-5　DLP ポリシー重大度基準の調整



Email DLP ポリシーの順序の設定

DLP Policy Manager でのポリシーの順序は重要です。DLP 違反が発生した場合、RSA メール DLP は、その違反を発信メール ポリシーでイネーブルな DLP ポリシーと照合します。違反が複数の DLP ポリシーに一致する場合、RSA メール DLP は上から順に調べ、最初に一致した DLP ポリシーを選択します。

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。

Email DLP ポリシーの編集

ステップ 1　[DLP Policy Manager] ページに一覧表示されている RSA メール DLP ポリシーの名前をクリックします。[Mail Policies: DLP] ページが表示されます。

ステップ 2　DLP ポリシーを変更します。

ステップ 3　変更を送信し、保存します。

（注）　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。

Email DLP ポリシーの削除

DLP ポリシーを削除するには、一覧のポリシーの隣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。このメッセージは、DLP ポリシーが 1 つ以上の複数の発信メール ポリシーで使用されているかを示しています。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。変更を送信し、保存します。

メール DLP ポリシーの複製

既存のポリシーとほぼ同じで一部設定が異なる DLP ポリシーを作成する場合は、DLP Policy Manager で複製ポリシーを作成することができます。

ステップ 1　[DLP ポリシーマネージャ（DLP Policy Manager）] ページで、一覧の中から複製対象のポリシーの隣にある [重複（Duplicate）] アイコンをクリックします。

ステップ 2　ポリシーの名前を入力します。

ステップ 3　ポリシーの設定に変更を加えます。

ステップ 4　変更を送信し、保存します。

DLP Assessment Wizard の使用

AsyncOS のブラウザ ベース DLP Assessment Wizard を使うと、よく使われる RSA メール DLP ポリシーの設定と、そのポリシーを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する 3 つの手順のプロセスを簡単に行えます。

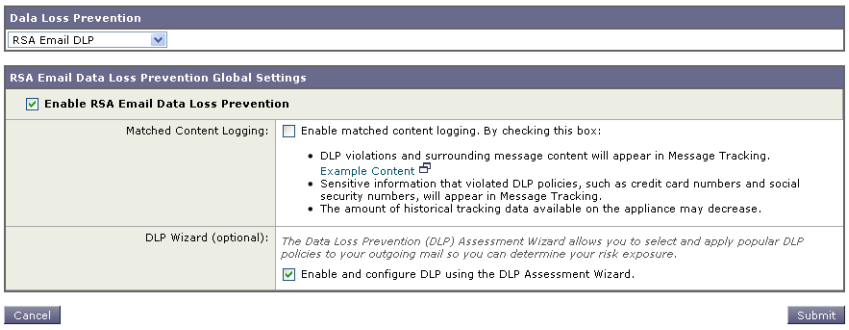
DLP Assessment Wizard を使って追加された DLP ポリシーでは、検出された DLP 違反の重大度にかかわらず、デフォルトですべてのメッセージが配信されます。DLP Policy Manager を使用して、メッセージの全体的なアクション、重大度レベルの設定、および必要なその他のポリシー設定を編集します。DLP ポリシーの編集の詳細については、DLP Policy Manager（11-11 ページ）参照してください。

アプライアンスが RSA メール DLP を使用している場合に DLP Assessment Wizard を起動するには、[セキュリティサービス（Security Services）] > [RSA メールDLP（RSA Email DLP）] ページを開きます。[設定の編集（Edit Settings）] をクリックします。[DLP 評価ウィザードを使用して DLP の有効化と設定を実行します（Enable and configure DLP using the DLP Assessment Wizard）] チェックボックスをオンにして、[有効（Enable）] をクリックします。

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。

図 11-6 は、DLP Assessment Wizard の実行オプションを示しています（[RSA Email Data Loss Prevention Settings] ページより）。

図 11-6　[RSA Email Data Loss Prevention Settings] ページ



DLP Assessment Wizard の実行

DLP Assessment Wizard を使用すると、次の DLP 設定作業が簡単にできます。作業は、3 つの手順に分けることができます。

ステップ 1　ポリシー

- ネットワーク上で保護する情報のタイプに合わせて DLP ポリシーを選択します。
- 機密データを検出するために追加情報を必要とする DLP ポリシーをカスタマイズします。

ステップ 2　レポート

- DLP Incident Summary レポート配信設定を設定します。

ステップ 3　レビュー

- DLP ポリシーをレビューしてイネーブルにします。

各手順を完了させたら、[次へ（Next）] をクリックして、DLP Assessment Wizard の手順を進めていきます。[前へ（Previous）] をクリックすると、前の手順に戻ることができます。プロセスの最後に、変更を確定するようプロンプトが表示されます。確定するまで、変更は有効になりません。

手順 1：ポリシー

DLP ポリシーの選択

アプライアンスが発信メッセージ内で検出対象とする機密情報のタイプ用の DLP ポリシーを選択します。

次のポリシーを使用できます。

- [FERPA (Family Educational Rights and Privacy Act)] は、生徒記録を検出し、生徒識別番号を検出するようにカスタマイズできます。
- [GLBA (Gramm-Leach Bliley Act)] は、クレジット カード番号、米国社会保障番号、米国運転免許証番号を検出し、カスタム アカウント番号を検出するようにカスタマイズできます。
- [California SB-1386] は、カルフォルニア SB-1386（民法 1798）で規制されている、米国社会保障番号、クレジット カード番号、米国運転免許証番号などの Personally Identifiable Information（PII; 個人情報）を含むドキュメントと送信を検出します。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 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、準拠することが必須となっています。
- [Restricted Files] は、.mdb、.exe、.bat および Oracle 実行ファイル（.fmx、.frm）など制限されているファイルを含む電子メールを検出します。このポリシーは付加的なファイル属性をポリシー違反ルールに追加してカスタマイズできます。

DLP Policy Manager を使って、DLP ポリシーの他のタイプを作成できます。

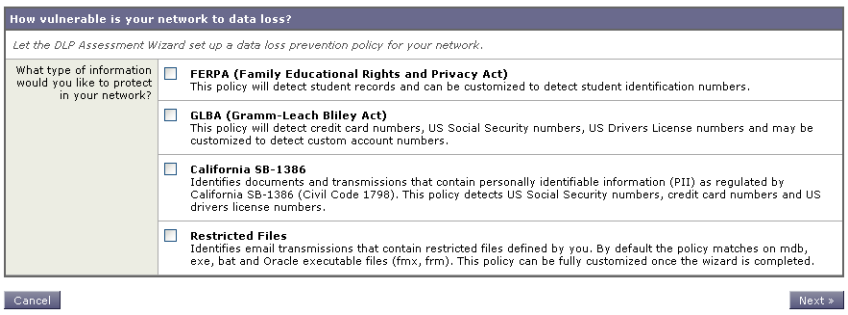
DLP ポリシーのカスタマイズ

DLP ポリシーには、発信メッセージ内の機密情報を検出するようにカスタマイズできるコンテンツ照合分類子を使うものがいくつかあります。FERPA および GLB 用のカスタマイズされた分類子、ポリシーは正規表現を使い、発信メッセージ内に識別番号パターンがないか検索します。Restricted Files ポリシーを選択した場合は、DLP ポリシーで検出する添付ファイル タイプを選択します。Restricted Files ポリシーはデフォルトで .exe および .mdb ファイルを検出しますが、これらのファイル タイプを削除できます。Restricted Files ポリシーを暗号化またはパスワードで保護されたファイルのみに適用するように設定できます。

これらの DLP ポリシー用のコンテンツ照合分類子のカスタマイズの詳細については、DLP ポリシーに対する分類子のカスタマイズ（11-14 ページ）参照してください。

[次へ（Next）] をクリックして続行します。

図 11-7　DLP Assessment Wizard：手順 1：ポリシー



手順 2: レポート

スケジュール済み DLP Incident Summary レポート用に電子メール アドレスを入力します。複数のアドレスを区切るには、カンマを使います。この値を空白のままにしておくと、スケジュール済みレポートは作成されません。DLP インシデント サマリー レポートの詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Using Email Security Monitor」の章を参照してください。

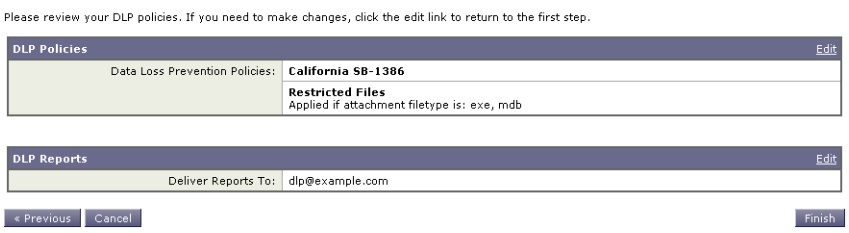
[次へ(Next)] をクリックして続行します。

図 11-8　DLP Assessment Wizard: 手順 2: レポート

手順 3: レビュー

DLP 設定情報の要約が表示されます。[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)] リンクをクリックして、ポリシーおよびレポートの情報を編集することができます。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。

図 11-9　DLP Assessment Wizard: 手順 3: レビュー



表示されている情報が十分であれば、[終了(Finish)] をクリックします。AsyncOS により、[Outgoing Mail Policies] ページに、デフォルトの発信メール ポリシーでイネーブルになっている DLP ポリシーが表示されます。DLP ポリシー設定の要約が、ページの上部に表示されます。変更を保存します。

DLP ポリシーの編集と追加作成については、DLP Policy Manager(11-11 ページ)を参照してください。DLP ポリシーを他の発信メール ポリシーに対してイネーブルにする方法については、DLP の受信者ごとのポリシーの設定(11-32 ページ)を参照にしてください。

コンテンツ照合分類子

コンテンツ照合分類子は、RSA メール DLP スキャン エンジンの検出コンポーネントです。クレジット カード番号や運転免許識別番号などのデータ パターン、およびそのパターンが出現するコンテキストがないか、メッセージ、メッセージ ヘッダー、および抽出した添付ファイルの内容を検索します。たとえば、クレジット カード番号を検出する分類子は、クレジット カード番号の形式に一致する数値のパターンだけではなく、有効期限やクレジット カード会社名などの補足データもないかスキャンします。データのコンテキストを評価することで、false positive が減少します。

RSA のポリシー テンプレートの多くは、分類子の事前定義されたセットを含みます。Custom Policy テンプレートをもとにしてポリシーを作成するときは、RSA 分類子を選択するか、独自の分類子を 1 つ追加できます。カスタム DLP ポリシーで使用する独自の分類子の作成については、コンテンツ照合分類子の作成（11-27 ページ）を参照してください。

多くのポリシー テンプレートでは、機密データ検出のために 1 つ以上の分類子をカスタマイズする必要があります。カスタマイズには、識別番号と、その識別番号とともに決まって出現する可能性がある単語とフレーズの一覧を検索するための正規表現を作成することが含まれます。たとえば、Family Educational Rights and Privacy Act（FERPA; 家族教育権とプライバシー法）テンプレートをもとにしたポリシーを追加するには、生徒識別番号に一致する正規表現を作成する必要があります。ID 番号が決まって「Student ID」というフレーズと共に出現するならば（「Student ID: 123-45-6789」など）、そのフレーズをポリシーに追加すればコンテンツ マッチングがより正確になります。DLP ポリシーで必須であるカスタマイズの詳細については、DLP ポリシーに対する分類子のカスタマイズ（11-14 ページ）参照してください。

（注）　分類子を持たないポリシーに対しては、メッセージがポリシーに違反した場合、スキャン エンジンは常に「75」のリスク要因値を返します。このようなポリシーには、発生する可能性のある DLP 違反のタイプによって重大度基準を調整します。詳細については、重大度レベルの設定（11-16 ページ）を参照してください。

分類子検出ルール

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。false positive 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、DLP 用の正規表現の例（11-25 ページ）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。RSA メール DLP には、RSA が作成したディクショナリがありますが、独自のディクショナリを作成できます。詳細については、第 14 章「テキスト リソース」を参照してください。
- **エンティティ（Entity）**. 以前のバージョンの AsyncOS のスマート識別子と同様に、エンティティはデータ内のパターン（ABA ルーティング番号、クレジット カード番号、住所、社会保障番号など）を識別します。

分類子は、メッセージ内で検出ルールと一致したものが見つかると数値を割り当て、メッセージのスコアを計算します。メッセージの DLP 違反の重大度の決定に使われるリスク要因は、分類子の最終的なスコアの範囲を 0 ～ 100 としたものです。分類子は、次の値を使ってパターンを検出し、リスク要因を計算します。

- **近接性**。有効と見なすには、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出現し、末尾の送信者の署名に住所が現れた場合、それらはおそらく関連がなく、分類子は一致と見なしません。
- **最小総合スコア**。分類子が結果を返すのに必要な最小スコア。メッセージの一致スコアが最小総合スコアに満たない場合、そのデータは機密データとして見なされません。

- **重み**。各ルールで、ルールの重要度を示す「重み」を指定します。分類子は、検出ルールに一致した数にルールの重みを乗算してメッセージのスコアを計算します。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えている場合、分類子では最大スコアの値が使用されます。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 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、表 11-1 リスク要因を算出します。

表 11-1　　リスク要因計算用の対数目盛り

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
1000	90
10000	100

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 false positive の数が減ります。

例：

- `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：

- 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：

- 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

DLP ポリシー テンプレートのいくつかは、米国運転免許証分類子を使用します。この分類子には、米国の各州およびコロンビア特別区用の検出ルールの一式が含まれています。DLP Policy Manager で [詳細設定（Advanced Settings）] の下の米国運転免許証用のリンクをクリックすることで、組織のポリシーにとって重要でない州を選択してイネーブルまたはディセーブルにすることができます。

（注） 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。

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：

- 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：

- `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て、特定の生徒 ID パターンを検出します。

例：

- `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：

`2009 Cisco net sales, net income, depreciation`（一致）

`FORM 10-Q 2009 I.R.S. Employer Identification No.`（一致）

コンテンツ照合分類子用の正規表現

多くのポリシー テンプレートで 1 つ以上の分類子をカスタマイズする必要があります。カスタマイズには、カスタム アカウント番号や患者識別番号など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。

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。

表 11-2　分類子での正規表現

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になります。 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。

表 11-2　分類子での正規表現

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。
Number of repetitions {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、式「\d{8}」は 12345678 および 11223344 と一致しますが、8 とは一致しません。
または (|)	代替、つまり「or」演算子に相当します。A および B という正規表現がある場合、式「A|B」は「A」または「B」のいずれかと一致する文字列と一致します。これは、正規表現で複数の数値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。

DLP 用の正規表現の例

コンテンツ照合分類子で正規表現を使用する主なケースは、特定の口座、患者や生徒の識別番号を検出することです。これらは、数や文字のパターンを記述する通常の単純な正規表現です。次に例を示します。

- 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

（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。

高度な RSA メール DLP ポリシーのカスタマイズ

使用可能な RSA メール DLP ポリシー テンプレートでは組織の独自の要件に適合しない場合、ゼロから独自の DLP ポリシーを作成するためのオプションがいくつかあります。オプションには次のものがあります。

- Custom Policy テンプレートを使って独自の DLP ポリシーを作成
- カスタム ポリシーで使用する独自の分類子を作成
- カスタム ポリシーで使用する独自の DLP ディクショナリを作成しインポート

（注）　これらのオプションは高度であり、事前定義された設定が組織のニーズに適合しない場合にのみ使用されることを想定しています。

Custom Policy テンプレートを使用した DLP ポリシーの作成

Custom Policy テンプレートを使用して、カスタム DLP ポリシーを作成し、定義された RSA 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。分類子の作成の手順については、コンテンツ照合分類子の作成（11-27 ページ）を参照してください。

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。false positive 防止のため、DLP ポリシーには、メッセージの内容と一致する場合、違反とは見なさなくなる分類子を含めることができます。分類子の [NOT] チェックボックスをオンにすると、その分類子に一致する内容を含むメッセージは、DLP 違反として報告されません。

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　ポリシー用に分類子を選択します。既存の分類子の使用または [分類子を作成（Create a Classifier）] オプションの選択が可能です。

ステップ 7　[追加（Add）] をクリックします。

[分類子を作成（Create a Classifier）] を選択すると、[コンテンツ照合分類子の追加（Add Content Matching Classifier）] ページが開きます。それ以外の場合は、事前定義された分類子がポリシーに追加されます。

ステップ 8　複数の分類子をポリシーに追加する場合は、ステップ 6 ～ 7 を繰り返します。

ステップ 9　任意で、DLP ポリシーの適用を、特定の受信者や送信者、添付ファイルのタイプを持つメッセージに限定することができます。改行やカンマで、複数のエントリを分離できます。詳細については、送信者および受信者のフィルタリング（11-15 ページ）および添付ファイルの種類に基づいたフィルタリング（11-15 ページ）を参照してください。

ステップ 10　[クリティカル違反の設定（Critical Violations Settings）] セクションで、重大な DLP 違反を含むメッセージで実行するアクションを選択します。

ステップ 11　一致する重大度レベルが High、Medium、Low のメッセージに、別々の設定を定義するときは、適切なセキュリティ レベルの [設定を継承（Inherit settings）] チェックボックスをオフにします。メッセージへの全体的なアクションや他の設定を編集します。

ステップ 12　ポリシーの DLP 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）] をクリックして、設定を調整します。詳細については、重大度レベルの設定（11-16 ページ）を参照してください。

ステップ 13　変更を送信し、保存します。

ポリシーが DLP Policy Manager に追加されます。

コンテンツ照合分類子の作成

カスタム ポリシー作成時は、[分類子を作成（Create a Classifier）] オプションを選択すると、カスタム分類子を作成できます。分類子の作成に必要なルールと値の詳細については、分類子検出ルール（11-21 ページ）を参照してください。

分類子を作成して送信すると、カスタム ポリシー作成時に使用可能な分類子の一覧に表示されます。

ステップ 1　分類子の名前と説明を入力します。

ステップ 2　近接性照合としてカウントするために、分類子のルールを検出する文字数を入力します。

ステップ 3　分類子の最小総合スコアを入力します。

ステップ 4　重みや最大スコアなど分類子のルールを定義します。

ステップ 5　[ルールの追加（Add Rule）] をクリックし、ルールを分類子に追加します。複数のルールを追加できます。

ステップ 6　分類子を送信し、カスタム ポリシーの作成を続けることができます。

RSA Enterprise Manager

AsyncOS 7.6 以降、シスコでは、RSA Enterprise Manager を使用してネットワーク上の E メール セキュリティ アプライアンスに DLP ポリシーを作成して管理するオプションを提供しています。RSA Enterprise Manager は、RSA Security, Inc. が提供するサードパーティ製ソフトウェアであり、Cisco IronPort E メール セキュリティ アプライアンスの一部ではありません。E メール セキュリティ アプライアンスを Enterprise Manager と連携させることで、DLP 機能の堅牢なセットがアプライアンスに開かれ、アプライアンスの DLP 機能の管理が Enterprise Manager に引き継がれます。また、RSA Enterprise Manager は、接続されているすべての E メール セキュリティ アプライアンス全体で DLP の集中管理機能を果たします。

（注）　このガイドでは、E メール セキュリティ アプライアンスを RSA Enterprise Manager と統合する方法の概要と、E メール セキュリティ アプライアンスの設定手順について説明します。E メール セキュリティ アプライアンスで動作するように Enterprise Manager を設定し、Enterprise Manager を使用して DLP ポリシーを管理する方法については、RSA Enterprise Manager のテクニカル ドキュメントを参照してください。このマニュアルでは、必要に応じて RSA Enterprise Manager のヘルプを参照します。

RSA Enterprise Manager DLP の動作

DLP に RSA Enterprise Manager を使用すると、Enterprise Manager は、ネットワーク上の E 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、DLP 違反を含むメッセージを処理するためのインターフェイスになります。DLP に RSA Enterprise Manager をセットアップするには、E メール セキュリティ アプライアンスと Enterprise Manager の両方が連動してデータを交換するように設定する必要があります。

まず、E メール セキュリティ アプライアンスで DLP の監視と適用に使用する発信メール ポリシーとメッセージ アクションを作成します。E メール セキュリティ アプライアンスを Enterprise Manager に接続すると、RSA Enterprise Manager のイネーブル化（11-4 ページ）に示すように、E メール セキュリティ アプライアンスはメール ポリシーとメッセージ アクションの名前とメタデータを Enterprise Manager に送信します。DLP ポリシーを作成する際はこの情報を使用します。Enterprise Manager で DLP ポリシーを作成して有効にすると、Enterprise Manager は DLP ポリシーをデータ パッケージの一部として E メール セキュリティ アプライアンスに送信します。E メール セキュリティ アプライアンスは、DLP ポリシーを格納し、それらを使用して Enterprise Manager DLP ポリシーに基づいて違反がないか送信メッセージをスキャンし、DLP 違反のインシデントに関する情報を Enterprise Manager に送信して、管理者が表示および管理できるようにします。RSA Enterprise Manager では、ユーザ識別名 LDAP クエリを使用してメッセージから送信者の名前を取得し、DLP 違反が検出されたときにアプライアンスから送信された DLP インシデント データの一部としてこの情報を含める必要があります。

Enterprise Manager で定義された DLP ポリシーの順序は重要です。DLP 違反が発生すると、E メール セキュリティ アプライアンスは DLP 違反をトップダウン方式で照合し、一致した最初のポリシーに基づいてメッセージに対して処理を行います。Enterprise Manager でポリシーの順序を設定します。この順序は、データ パッケージの一部として E メール セキュリティ アプライアンスに送信されます。

Enterprise Manager からの最新の DLP ポリシー アップデートに関する情報を確認するには、[セキュリティサービス（Security Services）] > [RSA メール DLP（RSA Email DLP）] ページを使用し、E メール セキュリティ アプライアンスの個々の DLP ポリシーを有効または無効にするには、[メールポリシー（Mail Policies）] > [DLP ポリシーマネージャ（DLP Policy Manager）] ページを使用します。

E 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 ポリシーを使用し続けます。

RSA Enterprise Manager DLP の E メール セキュリティ アプライアンスの設定

Enterprise Manager が E メール セキュリティ アプライアンスと連携するためには、E メール セキュリティ アプライアンスでいくつかの設定が必要です。

証明書

E 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。証明書の共通名は、アプライアンスのホスト名である必要があります。証明書を管理し、認証局をアプライアンスの認定済み認証局リストに追加するには、E メール セキュリティ アプライアンスの [ネットワーク（Networks）] > [証明書（Certificates）] ページを使用します。[DLP グローバル設定（DLP Global Settings）] を使用して SSL 接続を設定する場合、Enterprise Manager サーバがサーバで、E 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。

RSA Enterprise Manager 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 .p12 ファイルの生成に使用できる証明書の生成ツールが提供されます。このツールは、単一の証明書のみ生成できます。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。

.p12 証明書ファイルを含む Enterprise Manager サーバ上のディレクトリには、.pem 証明書ファイルもあります。.p12 ファイルを使用する場合は、認証局として E メール セキュリティ アプライアンスにこのファイルをインポートします。

ステップ 1　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>
```

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
```

これにより、`device-store.p12` ファイルが同じフォルダに出力されます。

ステップ 4　`<NAME OF DEVICE STORE>.p12` が目的のファイルです。E メール セキュリティ アプライアンスの証明書としてこれを使用してください。

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>
```

SSL 接続にクライアント証明書とサーバ証明書を使用するには、次の手順を実行します。

1. [ネットワーク（Networks）] > [証明書（Certificates）] ページを使用して、認証局をアプライアンスに追加します。RSA が提供するツールを使用してクライアント/サーバ証明書を生成した場合は、.pem ファイルをインポートします。
2. [ネットワーク（Networks）] > [証明書（Certificates）] ページを使用して、クライアント証明書およびサーバ証明書を E メール セキュリティ アプライアンスにアップロードします。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。クライアントとサーバに同じ証明書を使用できます。RSA ツールを使用して証明書を生成した場合は、.p12 証明書をインポートし、それをクライアント証明書とサーバ証明書の両方に使用します。
3. クライアント証明書とサーバ証明書の共通名は、E メール セキュリティ アプライアンスのホスト名でなければなりません。
4. DLP グローバル設定を使用して SSL 接続を設定する場合は、E メール セキュリティ アプライアンスにクライアント証明書を割り当て、Enterprise Manager にサーバ証明書を割り当てます。詳細については、データ消失防止のグローバル設定（11-2 ページ）を参照してください。

Enterprise Manager が接続された E メール セキュリティ アプライアンスをグループまたはクラスタ レベルで管理する場合、各アプライアンスにはアプライアンスのホスト名に一致する共通名を持つ独自の証明書が必要ですが、証明書の名前はすべて同じにする必要があります。アプライアンスの [ネットワーク（Networks）] > [証明書（Certificates）] ページを使用して、証明書名が一致することを確認します。E メール セキュリティ アプライアンスで証明書が見つからない場合、Enterprise Manager はアプライアンスを切断します。

LDAP ユーザ識別名クエリ

E メール セキュリティ アプライアンスは DLP インシデントについて Enterprise Manager にデータを送信する際、アプライアンス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を作成して、クエリを E 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。E 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、このクエリを使用します。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。

メッセージ アクション

E メール セキュリティ アプライアンスでメッセージ アクションを作成すると、アプライアンスはアクションの名前とそのアクションに関する読み取り専用メタデータの一部を、DLP ポリシーの Enterprise Manager に送信します。Enterprise Manager を使用してアクションを変更したり、新しいアクションを作成したりすることはできません。

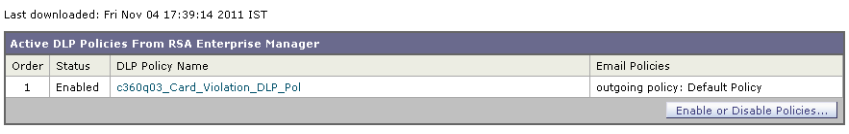
メッセージ アクションでは、DLP 違反が発生した場合に、DLP コンプライアンス責任者などのユーザに通知するよう E メール セキュリティ アプライアンスに指示できます。Enterprise Manager の DLP ポリシーは、DLP 違反通知をユーザに送信することもできます。通知の重複を防ぐために、Enterprise Manager または E メール セキュリティ アプライアンスの [メッセージアクション（Message Actions）] ページのいずれかを使用して通知を設定することをお勧めします。

詳細については、第 11 章「メッセージ アクション」を参照してください。

Enterprise Manager DLP ポリシーの DLP Policy Manager

DLP Policy Manager には、E メール セキュリティ アプライアンスで現在使用されている RSA Enterprise Manager DLP ポリシーが示されます。Manager を使用して、E メール セキュリティ アプライアンス上の個々の DLP ポリシーを有効または無効にすることができます。無効 DLP ポリシーに割り当てられた発信メール 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。

図 11-10　DLP Policy Manager での Enterprise Manager DLP ポリシー



E メール セキュリティ アプライアンスが Enterprise Manager から DLP ポリシーを受信していない場合、Enterprise Manager から新しいポリシーを含むデータ パッケージを受信するまで、既存の RSA メール DLP ポリシーが引き続き使用されます。

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、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。

隔離

DLP 違反を含むメッセージが、メッセージの隔離が必要な DLP ポリシーと一致する場合、E メール セキュリティ アプライアンスは DLP ポリシーのメッセージ アクションで指定された隔離領域にメッセージを送信します。DLP 違反の評価を担当するユーザは、Enterprise Manager を使用してインシデントを確認し、Enterprise Manager を使用して、アプライアンスに隔離からのメッセージの解放または削除を指示できます。メッセージ アクションでメッセージを解放時に暗号化する必要がある場合、これは Enterprise Manager ではなくメッセージを暗号化する E メール セキュリティ アプライアンスです。

ユーザは、Enterprise Manager で隔離されたメッセージを、E メール セキュリティ アプライアンスの GUI で[モニタ（Monitor）]> [隔離（Quarantines）] ページを使用して表示できます。シスコでは、ユーザは、ローカルの E メール セキュリティ アプライアンスの GUI ではなく、Enterprise Manager からのみ DLP 違反を含むメッセージを解放または削除することを推奨しています。

また、Enterprise Manager で検疫を使用する場合は、次の手順を実行することを推奨します。

- DLP 違反には、1 つ以上の専用検疫を使用します。
- 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。
- 検疫が割り当てられた領域を超えた場合、E メール セキュリティ アプライアンスは引き続き隔離メッセージを解放または削除することに留意してください。

E メール セキュリティ アプライアンスでの隔離の動作の詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Quarantines」の章を参照してください。

E メール セキュリティ アプライアンスと Enterprise Manager 間の接続

E 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られます。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。

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。
- E 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 レベルで使用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に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。

DLP の受信者ごとのポリシーの設定

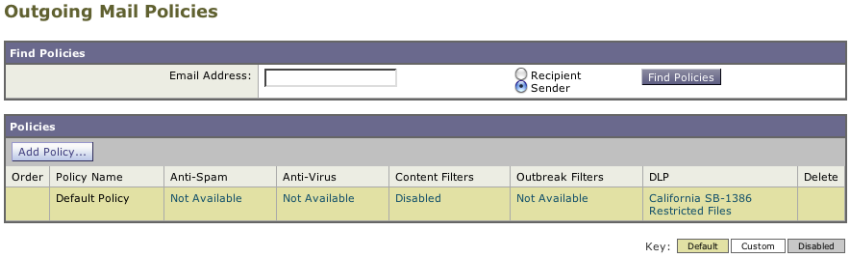
RSA メール DLP または RSA Enterprise Manager のどちらを使用しているかによって、DLP ポリシーを異なる方法で使用するように送信メール ポリシーを設定します。RSA メール DLP の場合は、E メール セキュリティ アプライアンスを使用して DLP ポリシーをメール ポリシーに割り当てます。RSA Enterprise Manager の場合は、Enterprise Manager を使用して E メール セキュリティ アプライアンスのメール ポリシーを DLP ポリシーに割り当てます。

RSA メール DLP

[メールポリシー（Mail Policies）] > [送信メールポリシー（Outgoing Mail Policies）] ページ（GUI）、または `policyconfig` コマンド（CLI）を使用して、受信者ごとの RSA メール DLP ポリシーをイネーブルにします。異なる発信メール ポリシーに対して別々の DLP ポリシーをイネーブルにすることができます。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。

DLP スキャンは、電子メールの「ワーク キュー」のアウトブレイク フィルタ段階の後に行われます。詳細については、第 6 章「電子メール セキュリティ マネージャ」を参照してください。

図 11-11　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

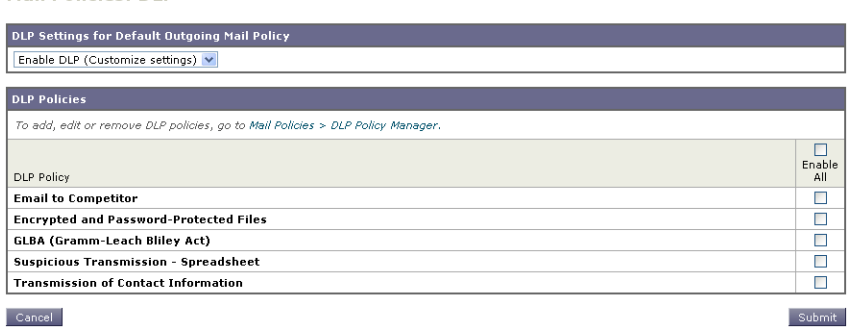


メール ポリシーの DLP 設定の編集

発信メール ポリシーに対するユーザごとの DLP 設定を編集するプロセスは、基本的にデフォルトのポリシーと個々のポリシーに対するものと同じです。個々のポリシー（デフォルトでない）には、DLP 設定を [DLP 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 DLP (Inherit default mail policy settings)）] にするという追加のオプションがあります。これを選択すると、ポリシーはデフォルトの発信メール ポリシーの DLP 設定をすべて採用します。

図 11-12 に、デフォルトの発信メール ポリシーでイネーブルな DLP ポリシーの一覧を示します。

図 11-12　デフォルトの発信メール ポリシーで DLP ポリシーをイネーブルにする



ステップ 1　電子メール セキュリティ マネージャの発信メール ポリシー テーブルの任意の行にある DLP セキュリティ サービスのリンクをクリックします。DLP 設定のページが表示されます。

ステップ 2　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　メール ポリシーの [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。

DLP Policy Manager で定義されているポリシーの一覧が表示されます。

ステップ 4　発信メール ポリシーで使用する RSA メール DLP ポリシーを選択します。

ステップ 5　変更を送信し、保存します。

RSA Enterprise Manager

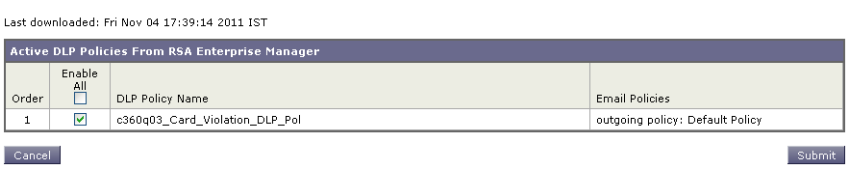
データ損失防止に RSA Enterprise Manager を使用する場合は、E メール セキュリティ アプライアンスを使用してメール ポリシーに DLP ポリシーを割り当てる代わりに、Enterprise Manager を使用して送信メール ポリシーを DLP ポリシーに割り当てます。Enterprise Manager で DLP ポリシーを設定する方法については、RSA Enterprise Manager のヘルプを参照してください。

RSA メール DLP とは異なり、発信メール ポリシーでは、Enterprise Manager がイネーブルにされている場合にはデフォルト ポリシーの DLP ポリシーを使用できません。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。

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と、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。継続してポリシーを削除すると、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 スキャンは引き続き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。

Enterprise Manager で複数の E メール セキュリティ アプライアンスを管理しており、アプライアンスの 1 つに特定の DLP ポリシーを使用させたくない場合は、DLP Policy Manager を使用して E メール セキュリティで DLP ポリシーを無効にできます。[メールポリシー（Mail Policies）] > [DLP ポリシーマネージャ（DLP Policy Manager）] に移動して、[ポリシーを有効または無効にする（Enable or Disable Policies）] をクリックします。E メール セキュリティ アプライアンスで使用しない DLP ポリシーのチェックボックスをオフにします。詳細については、Enterprise Manager DLP ポリシーの DLP Policy Manager（11-30 ページ）を参照してください。

図 11-13　DLP Policy Manager を使用した DLP ポリシーの有効化および無効化



CHAPTER 12

Cisco IronPort 電子メール暗号化

Cisco IronPort 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。

Cisco IronPort 電子メール暗号化：概要

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、Cisco Registered Envelope Service（管理対象サービス）または Cisco IronPort 暗号化アプライアンス（ローカル管理対象サーバ）のいずれかにできます。次に、メッセージを暗号化するか決めるコンテンツ フィルタまたはメッセージ フィルタ（または両方）を作成します。

フィルタ条件に合致する発信メッセージは、E 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。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。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。

E メール セキュリティ アプライアンスは、10 MB 未満のサイズのメッセージのみを暗号化します。アプライアンスは、自身のサイズより大きなメッセージをバウンスします。

（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（12-8 ページ）を参照してください。

ステップ 1 **ローカル キー サーバを使用する場合は、Cisco IronPort 暗号化アプライアンスを設定します。** キー サーバの設定手順については、『*IronPort Encryption Appliance Local Key Server User Guide*』を参照してください。

ステップ 2 **暗号化プロファイルを設定します。**暗号化プロファイルを設定する手順については、メール暗号化プロファイルの設定（12-3 ページ）を参照してください。

ステップ 3　**ホステッド キー サービスを使用する場合は、Cisco Registered Envelope Service の企業アカウントを作成します。暗号化プロファイルを設定した後、[Provision] ボタンをクリックしてアカウントを作成します。**

ステップ 4　**送信コンテンツ フィルタを設定します。**暗号化しなければならないアウトバウンド電子メールにタグをつけるように、コンテンツ フィルタを設定する必要があります。コンテンツ フィルタの作成方法については、暗号化コンテンツ フィルタの設定（12-8 ページ）を参照してください。

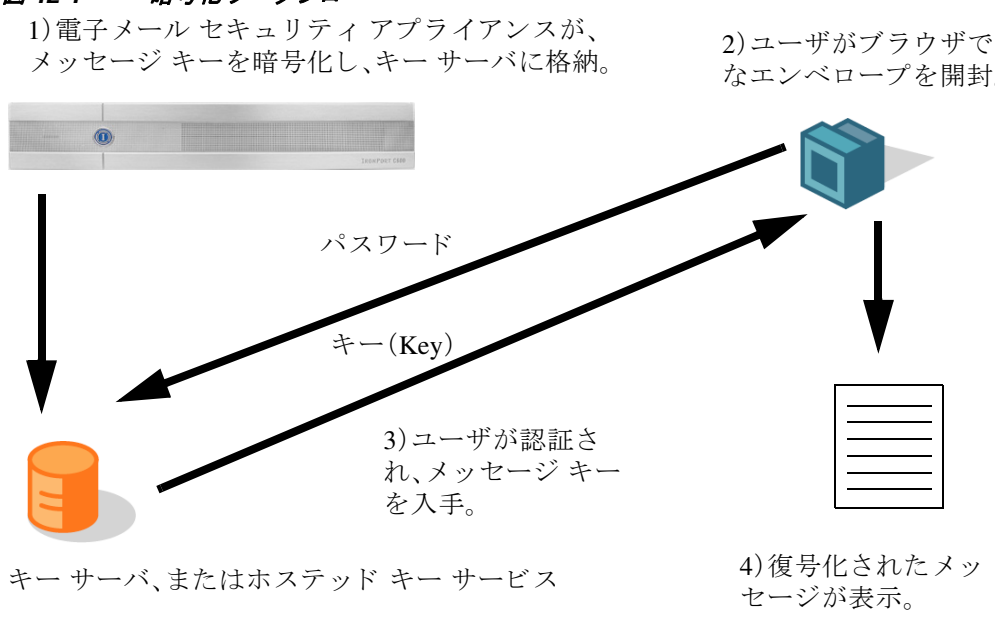
次の Web ブラウザがサポートされています。

- Microsoft® Internet Explorer 7（Windows XP および Vista）
- Microsoft® Internet Explorer 8（Windows XP および Vista）
- Firefox 3.0 および 3.5
- Safari 4.0（Mac OS X）

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 IronPort E 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 12-1　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。

ステップ 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 E 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。

ステップ 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。

ステップ 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。

ステップ 4　復号化したメッセージが表示されます。

メール暗号化プロファイルの設定

E 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。

メール暗号化グローバル設定の編集

ステップ 1　[Security Services] > [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　任意で、[設定を編集（Edit Settings）] をクリックし、プロキシ サーバを設定します。

図 12-2　　グローバル設定の構成

暗号化プロファイルの追加

ローカル 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。

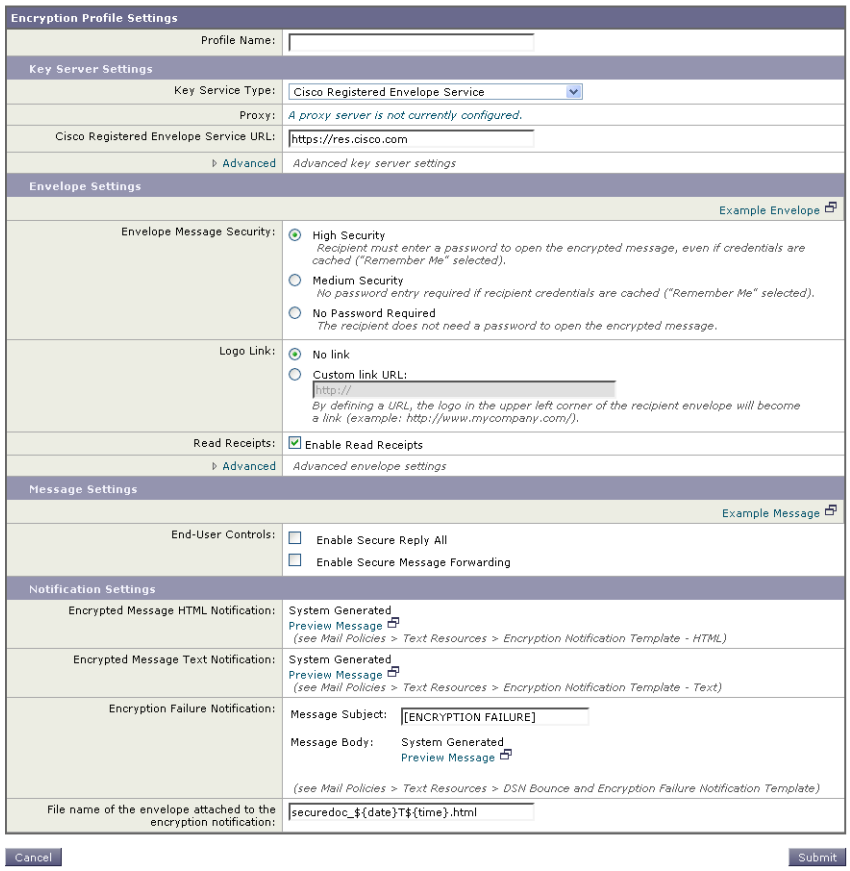
暗号化プロファイルをカスタム ユーザ ロールに割り当て、そのロールに割り当てられた委任管理者が DLP ポリシーとコンテンツ フィルタで暗号化プロファイルを使用できるようにします。DLP ポリシーとコンテンツ フィルタを設定する場合は、管理者、オペレータ、および委任ユーザだけが暗号化プロファイルを使用できます。カスタム ロールに割り当てられない暗号化プロファイルは、メールまたは DLP ポリシー権限を持つすべての委任管理者が使用できます。詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Common Administrative Tasks」の章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を作成および保存し、次の暗号化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（14-33 ページ）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（14-29 ページ）を参照してください。

図 12-3　暗号化エンベロープ プロファイルの追加



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（役割）（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 IronPort 暗号化アプライアンス（ネットワーク内）
- Cisco Registered Envelope Service（ホスト キー サービス）

ステップ 5　Cisco IronPort 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 IronPort E 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 IronPort 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 IronPort 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。次のいずれかを実行できます。

- [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。Cisco IronPort 暗号化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。

- [キーサービスを HTTPS で使用する（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。Cisco IronPort 暗号化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。

- [セキュリティ（高）（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。

- [セキュリティ（中）（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。受信者は暗号化されたメッセージを開くためにパスワードを入力する必要はありませんが、他の電子メール ユーザが元の受信者に代わってメッセージを送信するのを防ぐため、開封確認、セキュアな返信、全員にセキュアな返信、およびセキュアなメッセージ転送機能は利用できません。

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に、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）] をクリックします。

- 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　変更を送信し、保存します。

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 サービスと共に登録されます。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 [プロビジョニング（Provision）] ボタンをクリックします。

PXE エンジンの更新

[シスコ電子メール暗号化設定（Cisco IronPort 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。以前のバージョンの AsyncOS では、PXE エンジンを更新するためには AsyncOS を更新する必要がありました。[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 IronPort 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（15-9 ページ）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）を使用して、手動でエンジンを更新することもできます。

図 12-4　[IronPort Email Encryption Settings] ページの [PXE Engine Updates]

暗号化コンテンツ フィルタの設定

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決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 IronPort E 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。

（注）　E メール セキュリティ アプライアンスは、10 MB 未満のサイズのメッセージのみを暗号化します。アプライアンスは、自身のサイズより大きなメッセージをバウンスします。

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 IronPort 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 12-1 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、E 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 12-1　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	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 経由で送信します。	エンベロープを暗号化して送信します。
TLS 必須	TLS 経由で送信します。	リトライまたはメッセージのバウンス

宛先制御での TLS のイネーブル化の詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Customizing Listeners」の章を参照してください。

Encrypt and Deliver Now コンテンツ フィルタの作成

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。

条件の作成については、コンテンツ フィルタの概要（6-8 ページ）を参照してください。

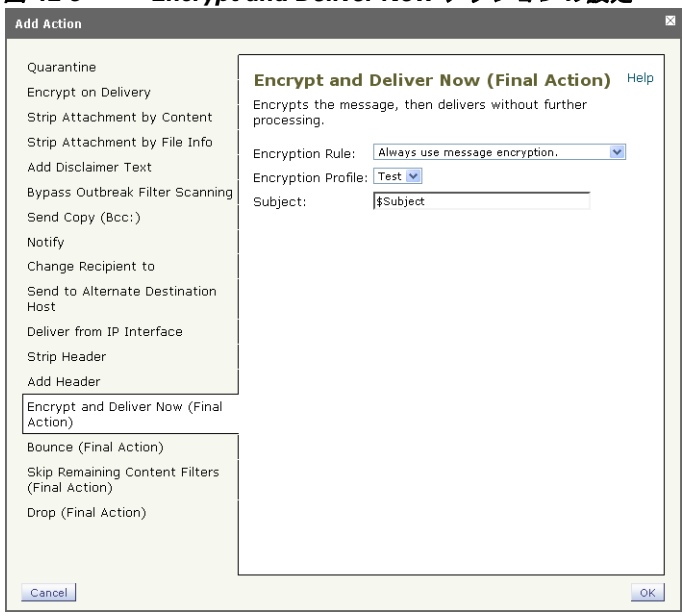
ステップ 6　任意で、[アクションを追加（Add Action）] をクリックし、[ヘッダーの追加（Add Header）] を選択し、追加の暗号化設定を指定する暗号化ヘッダーをメッセージに挿入します。

暗号化ヘッダーの詳細については、メッセージへの暗号化ヘッダーの追加（12-12 ページ）を参照してください。

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　[暗号化して今すぐ配信（最終アクション）（Encrypt and Deliver Now (Final Action)）] を選択します。

図 12-5　Encrypt and Deliver Now アクションの設定



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。

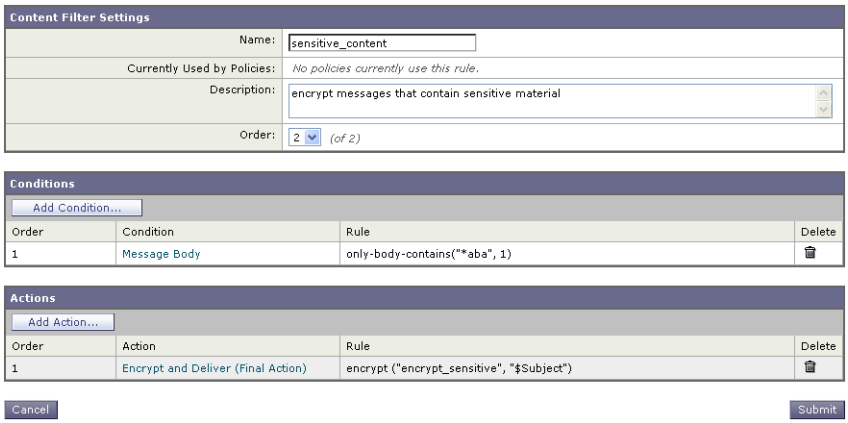
暗号化プロファイルは、使用するキー サーバ、セキュリティ レベル、およびメッセージ エンベロープのフォーマット化に関する設定、および他のメッセージ設定を指定します。暗号化プロファイルをコンテンツ フィルタに関連付けた場合、コンテンツ フィルタはこれらの格納された設定を暗号化メッセージに使用します。

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 12-6 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 12-6　　暗号化コンテンツ フィルタ



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　変更を保存します。

ステップ 15　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、ユーザベース ポリシーの概要（6-1 ページ）を参照してください。

Encrypt on Delivery コンテンツ フィルタの作成

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。

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。

条件の作成については、コンテンツ フィルタの概要（6-8 ページ）を参照してください。

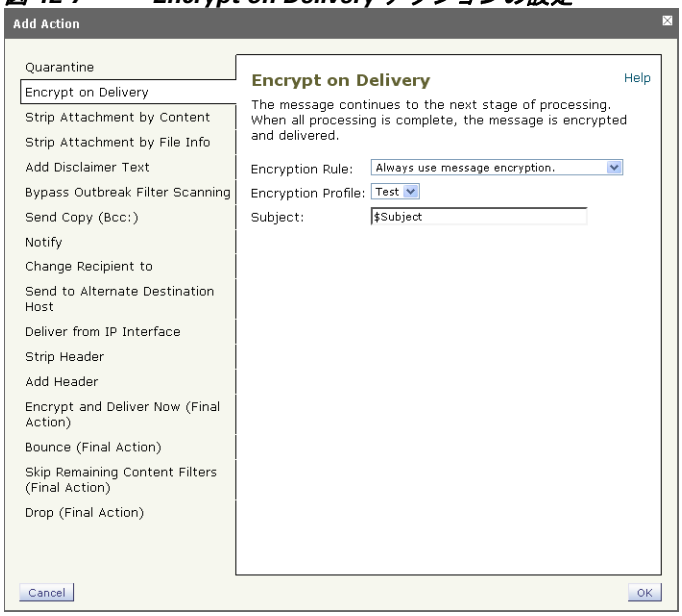
ステップ 6　任意で、[アクションを追加（Add Action）] をクリックし、[ヘッダーの追加（Add Header）] を選択し、追加の暗号化設定を指定する暗号化ヘッダーをメッセージに挿入します。

暗号化ヘッダーの詳細については、メッセージへの暗号化ヘッダーの追加（12-12 ページ）を参照してください。

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　[配信時に暗号化（Encrypt on Delivery）] を選択します。

図 12-7　Encrypt on Delivery アクションの設定



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　変更を保存します。

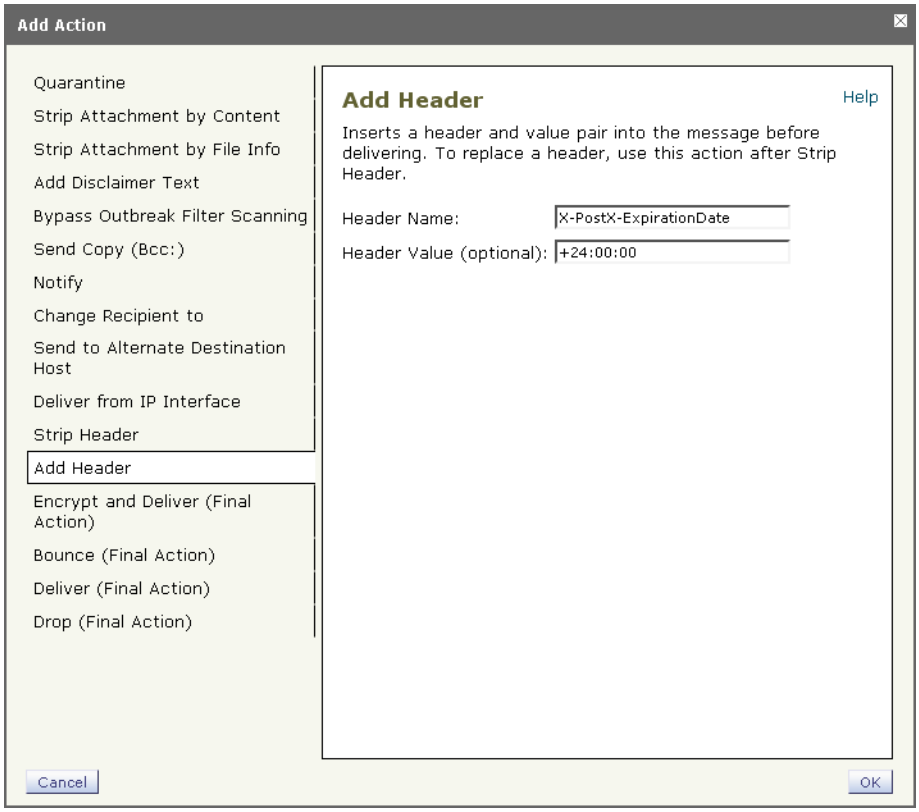
ステップ 15　コンテンツ フィルタを追加したら、フィルタを発信メール ポリシーに追加する必要があります。組織のニーズに応じて、デフォルト ポリシーでコンテンツ フィルタをイネーブルにする、またはフィルタを特定のメール ポリシーに適用することを選択します。メール ポリシーの操作については、ユーザベース ポリシーの概要（6-1 ページ）を参照してください。

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。

コンテンツ フィルタを使用してメッセージに暗号化ヘッダーを追加するには、ヘッダー フィルタの追加アクションをコンテンツ フィルタに追加し、暗号化ヘッダーとその値を入力します。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。

図 12-8　Add Header アクションの設定



暗号化コンテンツ フィルタの作成の詳細については、Encrypt and Deliver Now コンテンツ フィルタの作成（12-9 ページ）を参照してください。メッセージ フィルタを使用してヘッダーを挿入する方法の詳細については、『*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。

暗号化ヘッダー

表 12-2 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 12-2　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。
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しないかを示すブール値。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。

表 12-2　電子メール暗号化ヘッダー（続き）

MIME ヘッダー	説明	値
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しないかを示します。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しないかのブール値。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。
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。

表 12-2　電子メール暗号化ヘッダー（続き）

MIME ヘッダー	説明	値
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ュ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ュされます。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 キーのキャッシュ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 キーのキャッシュ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のイネーブル化

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 [オンラインで開く（Open Online）] リンクと共に表示され、[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のイネーブル化

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。

復号化アプレットの無効化

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 サーバで復号化するには、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 13

SenderBase Network Participation

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。

システム セットアップ ウィザード（GUI）および `systemsetup` コマンド（CLI）では、SenderBase ネットワークへの参加に同意することができます。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 IronPort 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。

SenderBase との統計の共有

ステップ 1 [セキュリティサービスにアクセス（Access the Security Services）] > [SenderBase] ページ。

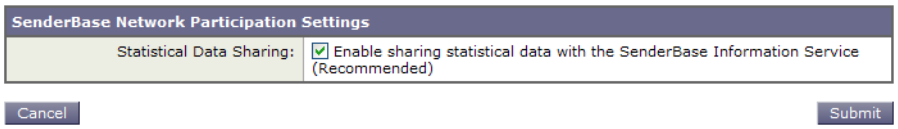
図 13-1　[セキュリティサービス（Security Services）] > [SenderBase] ページ

SenderBase

（注） システム セットアップ中にライセンス契約書に同意していない場合（手順 2：システム（3-17 ページ）を参照）は、このページの表示は異なります。[セキュリティサービス（Security Services）] > [SenderBase] ページで [有効（Enable）] をクリックしてから、グローバル設定を編集する前にライセンスを読んで同意する必要があります。

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。

図 13-2　[セキュリティサービス(Security Services)] > [SenderBase] ページ:編集



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 IronPort 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　オプションで、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できます。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(15-49 ページ)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 IronPort 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。(13-4 ページ)を参照してください)。

表 13-1 および表 13-2 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 13-1　Cisco IronPort 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
隔離サイズ（Quarantine Size）	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
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 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 13-2　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 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 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 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

表 13-2　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）
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 スパム陰性 10 件 スパムの疑い 5 件 ウイルス陽性 4 件 ウイルス陰性 16 件 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定によるメッセージ数	スパム 500 件、スパムなし 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	「.exe」添付ファイル 300 件
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」 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	50 ～ 55 K の範囲に「.exe」添付ファイルが 30 件

(a) ファイル名は一方向ハッシュ（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 IronPort 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 IronPort 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の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 IronPort 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 IronPort 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、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Using Message Filters to Enforce Email Policies」の章にある「Body Scanning Rule」を参照してください。

不明点は、Cisco IronPort カスタマー サポートまでお問い合わせください。Cisco IronPort サポート コミュニティ (1-11 ページ) 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、追加のデータの共有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 IronPort カスタマー サポートにお問い合わせください。

CHAPTER 14

テキスト リソース

概要

この章では、コンテンツ ディクショナリ、DLP 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。

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。

DLP ディクショナリ

Data Loss Prevention（DLP; データ消失防止）ディクショナリを使用して、発信メッセージに対して DLP ポリシーに従った機密情報のスキャンができます。コンテンツ ディクショナリと同様に、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。コンテンツ ディクショナリとは異なり、DLP ポリシー内の用語には「重み」はありません。AsyncOS には、RSA Security Inc. による事前定義されたディクショナリのセットが存在します。カスタム DLP ディクショナリを作成することもできます。

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。データ消失防止の詳細については、第 11 章、データ損失の防止を参照してください。

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

AsyncOS では、コンテンツ ディクショナリと DLP ディクショナリの 2 種類のディクショナリを提供しています。DLP ディクショナリの管理については、DLP ディクショナリ（14-10 ページ）を参照してください。

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 ディクショナリにスマート 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 文字を含むディクショナリ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 文字を含むディクショナリを表示および変更する最適な方法は、ディクショナリをテキスト 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（14-3 ページ）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

コンテンツ ディクショナリ機能には、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 ディクショナリ機能と組み合わせて使用することで、新規ディクショナリ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 ディクショナリ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） ディクショナリ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。

ユーザ独自のディクショナリ 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 文字をディクショナリ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 ファイルのディクショナリに単語を追加し、アプライアンス上にファイルを移動してから新しいディクショナリとしてファイルをインポートする方法です。ディクショナリのインポートの詳細については、ディクショナリのインポート（14-7 ページ）を参照してください。ディクショナリのエクスポートについては、ディクショナリのエクスポート（14-8 ページ）を参照してください。

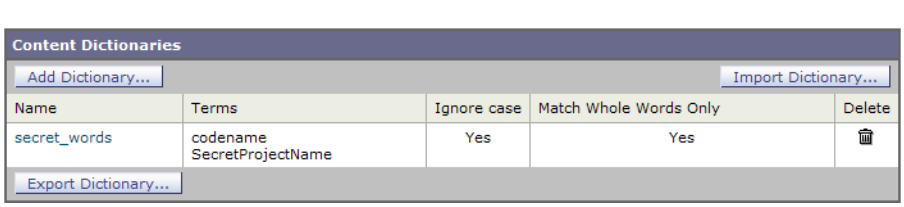
カスタム DLP ディクショナリをインポートおよびエクスポートすることもできます。詳細については、DLP ディクショナリのインポートおよびエクスポート（14-11 ページ）を参照してください。

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。**

コンテンツ ディクショナリの管理（GUI）

GUI にログインし、[Mail Policies] タブをクリックします。左側のメニューで [Dictionaries] リンクをクリックします。

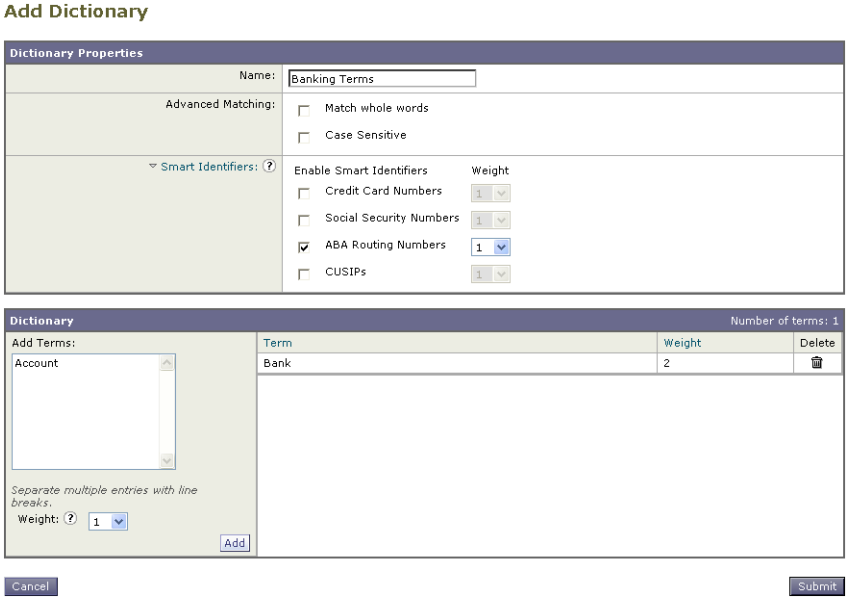
図 14-1　[Dictionaries] ページ



ディクショナリの追加

ステップ 1　[辞書（Dictionaries）] ページで [辞書を追加（Add Dictionary）] をクリックします。[Add Dictionary] ページが表示されます。

図 14-2　　[Dictionaries] ページ



ステップ 2　ディクショナリの名前を入力します。

ステップ 3　[Match Whole Words Only] の横にあるチェックボックスをオンにすることで、完全に一致する単語のみを検索するかどうかを指定します。詳細については、完全に一致する単語のみの検索（14-6 ページ）を参照してください。

ステップ 4　大文字と小文字を区別した検索を実行するかどうかを指定します。詳細については、大文字と小文字を区別した単語の一致（14-6 ページ）を参照してください。

（注）　AsyncOS は、設定ファイルに保存する際に、[単語全体の一致（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、これらの設定は保持されません。

ステップ 5　オプションで、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。サポートされているエントリの種類の詳細については、ディクショナリの内容（14-3 ページ）を参照してください。

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　変更を送信し、保存します。

[Dictionaries] ページには新しいディクショナリが、ディクショナリに含まれている単語およびディクショナリに設定した設定値とともに表示されています。

（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。

大文字と小文字を区別した単語の一致

このボックスをオンにすると、AsyncOS が照合の際に単語の大文字/小文字を考慮します。たとえば、単語「codename」では、「codename」というディクショナリ エントリに一致しますが、「CodeName」という単語は一致しません。

完全に一致する単語のみの検索

このボックスをオンにすると、エントリに完全に一致する単語のみを検索します。たとえば、単語「codename」はディクショナリのエントリ「codename」と一致しますが、単語「code」および「codenam」は一致しません。

単語のソート

カラムの見出しをクリックして、単語の順または重みの順にソートできます。カラムの見出しをもう一度クリックすると、ソート順が逆になります。

ディクショナリの編集

ステップ 1　[Dictionaries] ページで、リストにあるディクショナリの名前をクリックします。[ディクショナリの編集（Edit Dictionary）] が表示されます。

ステップ 2　ディクショナリのエントリまたは設定値を変更して、[送信（Submit）] をクリックします。

ステップ 3　変更を保存します。

ディクショナリの削除

ステップ 1　ディクショナリの横にあるゴミ箱アイコンをクリックして、ディクショナリのリストから削除します。確認メッセージが表示されます。

ステップ 2　確認メッセージには、ディ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　[削除（Delete）] をクリックして、ディクショナリを削除します。

ステップ 4　変更を保存します。

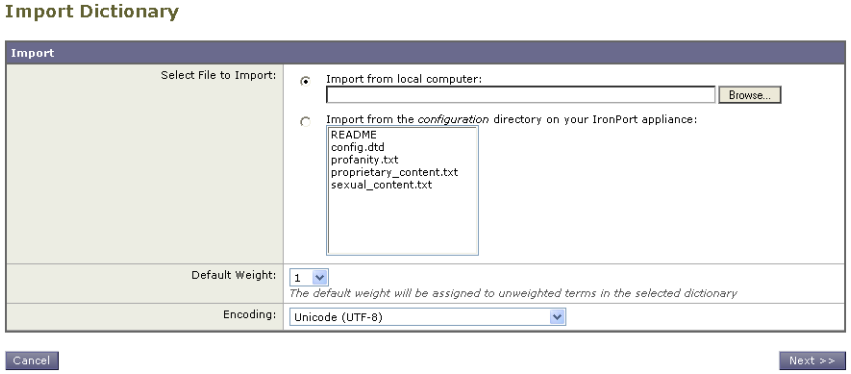
ステップ 5　削除されたディクショナリを参照しているすべてのメッセージ フィルタは、無効としてマークされます。

ステップ 6　削除されたディ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。

ディクショナリのインポート

ステップ 1　[辞書（Dictionaries）] ページで [辞書をインポート（Import Dictionary）] をクリックします。[Import Dictionary] ダイアログが表示されます。

図 14-3　[Import Dictionary] ページ



ステップ 2　インポート元の場所を選択します。

ステップ 3　インポートする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 4　ディ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 5　エンコード方式を選択します。

ステップ 6　[Next] をクリックします。

ステップ 7　インポートしたディクショナリは、[Add Dictionary] ページに表示されます。

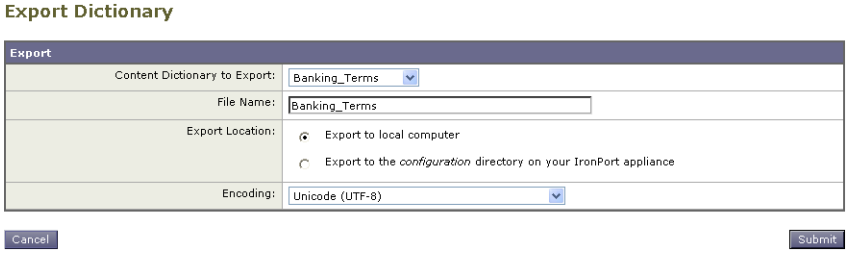
ステップ 8　ディクショナリを追加する前に、ディクショナリの名前の指定およびディクショナリの編集ができます。

ステップ 9　変更を送信し、保存します。

ディクショナリのエクスポート

ステップ 1　[辞書（Dictionaries）] ページで [辞書をエクスポート（Export Dictionary）] をクリックします。[Export Dictionary] ダイアログが表示されます。

図 14-4　[Export Dictionary] ページ



ステップ 2　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 3　ディクショナ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 4　エクスポート先の場所を選択します。

ステップ 5　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 6　変更を送信し、保存します。

コンテンツ ディクショナリの使用方法およびテスト方法

ディクショナリは、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。

ディクショナリの照合フィルタ ルール

`dictionary-match(<`*dictionary_name*`>)` という名前のメッセージ フィルタ ルール（および同様のルール）は、メッセージの本文にコンテンツ ディクショナリ（*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。該当のディクショナリ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）。ディクショナリ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 14-1　コンテンツ ディクショナリのメッセージ フィルタ ルール

ルール	構文	説明
ディクショナリ照合	`dictionary-match(<`*dictionary_name*`>)`	指定したディクショナリ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 IronPort 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、ポリシー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 14-2　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	末尾：foo $ 先頭：^ foo
電子メール アドレス（Email address） （ピリオドをエスケープしないこと）	**foo@example.com**, **@example.com** **example.com$**（最後で使用する場合） **@example.***
件名	**電子メールの件名** （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 関数を使用すると、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、Debugging Mail Flow Using Test Messages: Trace（-446 ページ）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。

DLP ディクショナリ

DLP ディクショナリは、アプライアンスの RSA DLP スキャン機能と連携して動作する単語または語句のグループであり、カスタム DLP ポリシーに利用できます。DLP 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および語句に対してメッセージ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。AsyncOS には、RSA Security Inc. による事前定義されたディクショナリのセットが存在します。カスタム DLP ディクショナリを作成することもできます。

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 Policy Manager を使用して、DLP ディクショナリを管理します。DLP Policy Manager を開くには、GUI で [Mail Policies] > [DLP Policy Manager] メニューを選択します。DLP Policy Manager の詳細については、第 11 章、データ損失の防止を参照してください。

カスタム ディクショナリの追加

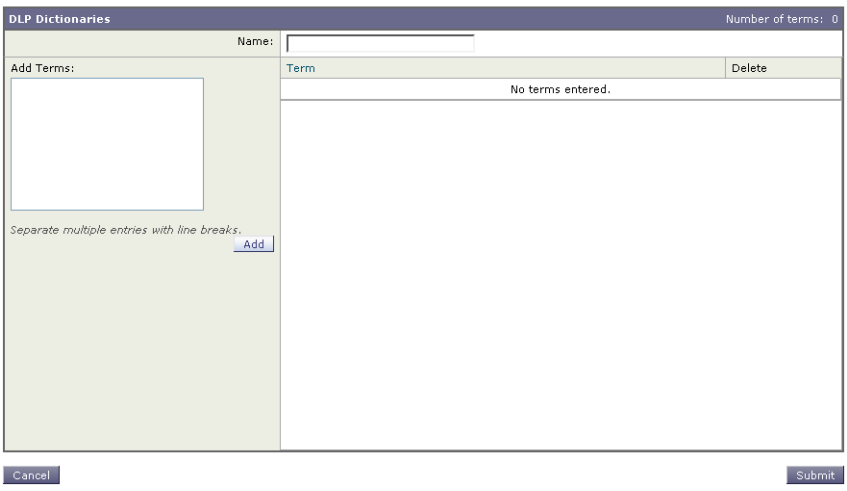
ステップ 1　DLP Policy Manager で [カスタム DLP 辞書(Custom DLP Dictionaries)] リンクをクリックします。

[DLP Dictionaries] ページが表示されます。

ステップ 2　[Add Dictionary] をクリックします。

[Add Dictionary] ページが表示されます。

図 14-5　　DLP ディクショナリの追加



ステップ 3　カスタム ディクショナリの名前を入力します。

ステップ 4　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。複数のエントリを一度に入力するには、強制改行を使用します。

ステップ 5　[追加(Add)] をクリックします。

ステップ 6　新規ディクショナリを送信し、確定します。

[Dictionaries] ページには新しいディクショナリが、ディクショナリに含まれている単語およびディクショナリに設定した設定値とともに表示されています。

カスタム DLP ディクショナリの編集

ステップ 1　[DLP Dictionaries] ページで、リストにあるディクショナリの名前をクリックします。

ステップ 2　エントリを変更します。

ステップ 3　変更を送信し、保存します。

カスタム DLP ディクショナリの削除

ステップ 1　ディクショナリの横にあるゴミ箱アイコンをクリックして、ディクショナリのリストから削除します。確認メッセージが表示され、ディ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 2　[削除(Delete)] をクリックして、ディクショナリを削除します。

ステップ 3　変更を保存します。

DLP ディクショナリのインポートおよびエクスポート

ユーザ独自の DLP 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、AsyncOS にインポートできます。また、同様に既存のカスタム ディクショナリをテキスト ファイルとしてエクスポートできます。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。

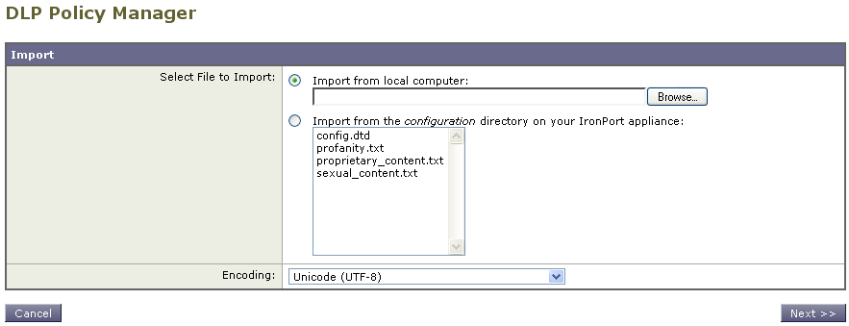
DLP ディクショナリ ファイルには、ディクショナリの単語として使用される単語および語句が強制改行で区切られたリストが含まれています。DLP ディクショナリとして使用するために既存のコンテンツ ディクショナリをエクスポートする場合は、DLP ディクショナリとしてテキスト ファイルをインポートする前に重み値を削除し、すべての正規表現を単語または語句に変換する必要があります。

テキスト ファイルとして DLP ディクショナリをインポートする方法

ステップ 1　[DLP Dictionaries] ページで [Import Dictionary] をクリックします。

[Import Dictionary] ダイアログが表示されます。

図 14-6　　ディクショナリのインポート



ステップ 2　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 3　エンコード方式を選択します。

ステップ 4　[Next] をクリックします。

ステップ 5　インポートしたディクショナリは、[Add Dictionary] ページに表示されます。

ステップ 6　ディクショナリを追加する前に、ディクショナリの名前の指定およびディクショナリの編集ができます。

ステップ 7　変更を送信し、保存します。

テキスト ファイルとして DLP ディクショナリをエクスポートする方法

ステップ 1　[Dictionaries] ページで [Export Dictionary] をクリックします。

[Export Dictionary] ダイアログが表示されます。

図 14-7　　ディクショナリのエクスポート

ステップ 2　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 3　ディクショナリのファイル名を入力します。

ステップ 4　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 5　ファイルのエンコード方式を選択します。

ステップ 6　変更を送信し、保存します。

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（14-19 ページ）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（14-26 ページ）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（14-27 ページ）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（14-29 ページ）を参照してください。
- **DLP 通知テンプレート**：電子メール 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情報が含まれる場合に送信されるメッセージ。詳細については、DLP 通知テンプレート（14-30 ページ）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 IronPort 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（14-33 ページ）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 リソースの管理（GUI）（14-14 ページ）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（14-13 ページ）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。

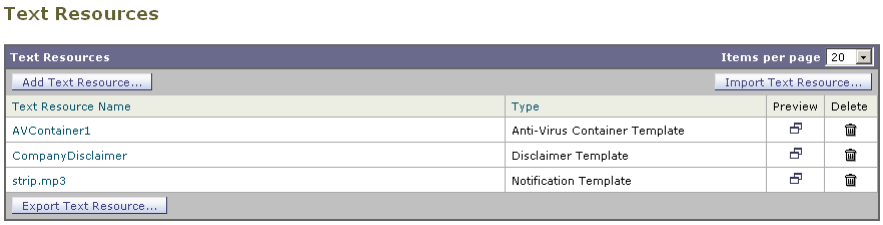
非 ASCII 文字をテキスト リソースに追加するには、アプライアンス以外の場所でテキスト ファイルのテキスト リソースに単語を追加し、アプライアンス上にファイルを移動し、新しいテキスト リソースとしてファイルをインポートします。テキスト リソースのインポートの詳細については、テキスト リソースのインポート（14-15 ページ）を参照してください。テキスト リソースのエクスポートについては、テキスト リソースのエクスポート（14-16 ページ）を参照してください。

テキスト リソースの管理（GUI）

GUI のテキスト リソースは、[メールポリシー（Mail Policies）] > [テキストリソース（Text Resources）] ページで管理できます。[テキストリソース（Text Resources）] ページでは、テキスト リソースの追加、編集、削除、エクスポート、およびインポートができます。

すべてのテキスト リソース タイプに対してプレーン テキスト メッセージを定義できます。また、一部のテキスト リソース タイプに対して HTML ベースのメッセージを定義することもできます。詳細については、HTML ベースのテキスト リソースの使用（14-17 ページ）を参照してください。

図 14-8　[Text Resources] ページ

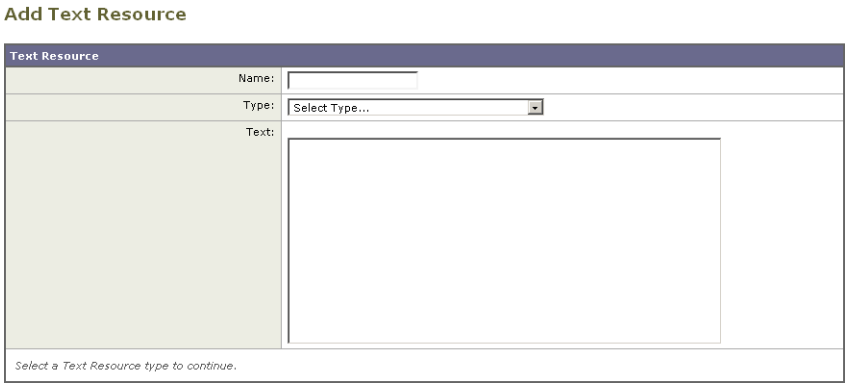


（注）　`textconfig` コマンドを使用して CLI からテキスト リソースを管理できます。

テキスト リソースの追加

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、[テキストリソースを追加（Add Text Resource）] をクリックします。[テキストリソースを追加（Add Text Resource）] ページが表示されます。

図 14-9　テキスト リソースの追加



ステップ 2　[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 3　[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 4　該当するフィールドに、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。詳細については、HTML ベースのテキスト リソースの使用(14-17 ページ)を参照してください。

ステップ 5　変更を送信し、保存します。

テキスト リソースの編集

ステップ 1　[Mail Policies] > [Text Resources] ページに移動し、編集するテキスト リソースの名前をクリックします。[テキストリソースの編集(Edit Text Resource)] ページが表示されます。

ステップ 2　テキスト リソースを変更します。

ステップ 3　変更を送信し、保存します。

テキスト リソースの削除

テキスト リソースは [Text Resources] ページから削除できます。ただし、次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。

ステップ 1　[Mail Policies] > [Text Resources] ページに移動し、削除するテキスト リソースの [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。

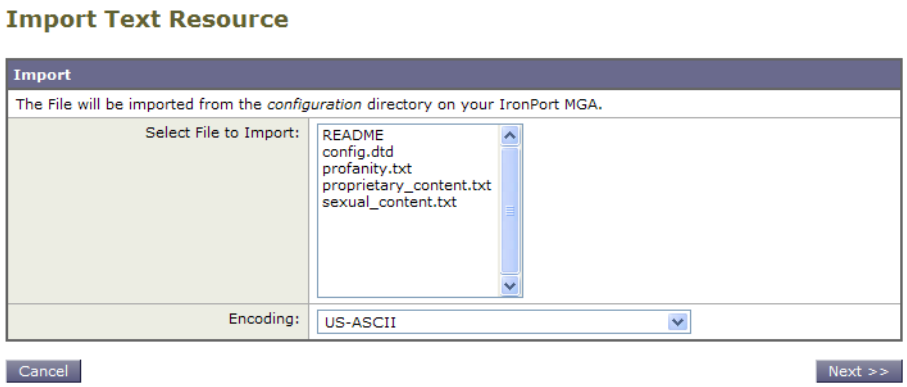
ステップ 2　[削除(Delete)] をクリックして、テキスト リソースを削除します。

ステップ 3　変更を保存します。

テキスト リソースのインポート

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。[テキストリソースのインポート(Import Text Resource)] ページが表示されます。

図 14-10　テキスト リソースのインポート



ステップ 2　インポートする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 3　エンコード方式を指定します。

ステップ 4　[Next] をクリックします。

インポートしたテキスト リソースは、[テキストリソースを追加（Add Text Resource）] ページの [テキスト（Text）] フィールドに表示されます。

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。

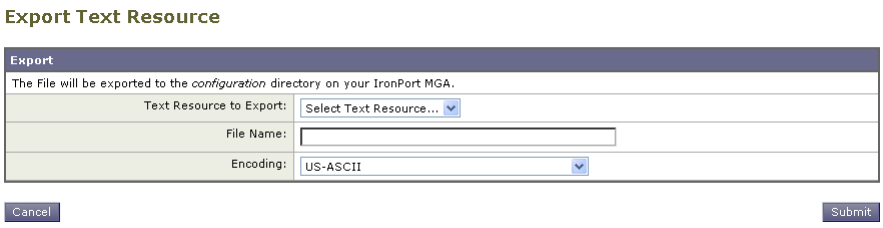
ステップ 6　変更を送信し、保存します。

テキスト リソースのエクスポート

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コンフィギュレーション ディレクトリに作成されます。

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。[Export Text Resource] ダイアログが表示されます。

図 14-11　テキスト リソースのエクスポート



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。

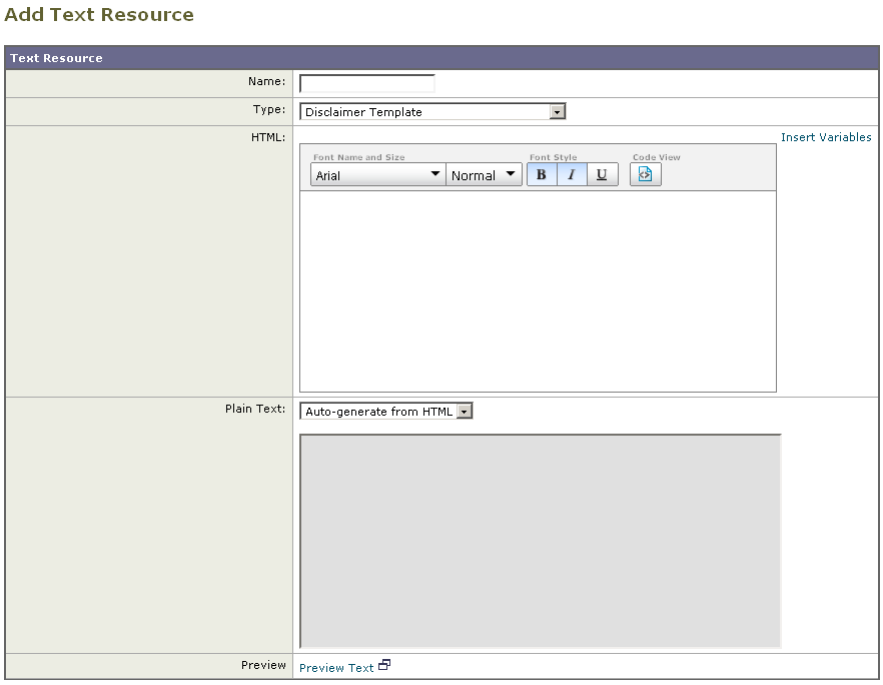
HTML ベースのテキスト リソースの使用

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。

図 14-12 に、HTML ベースのテキスト リソース向けのリッチ テキスト エディタを示します。

図 14-12　HTML ベースのテキスト リソースの作成



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、次のルールとガイドライン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、`<img src>` 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に行います。

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 IronPort 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 IronPort 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 IronPort 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（14-19 ページ）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（6-15 ページ）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（データ損失の防止（11-1 ページ）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（10-6 ページ）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（14-14 ページ）を参照）または `textconfig` コマンド（『*Cisco IronPort 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。

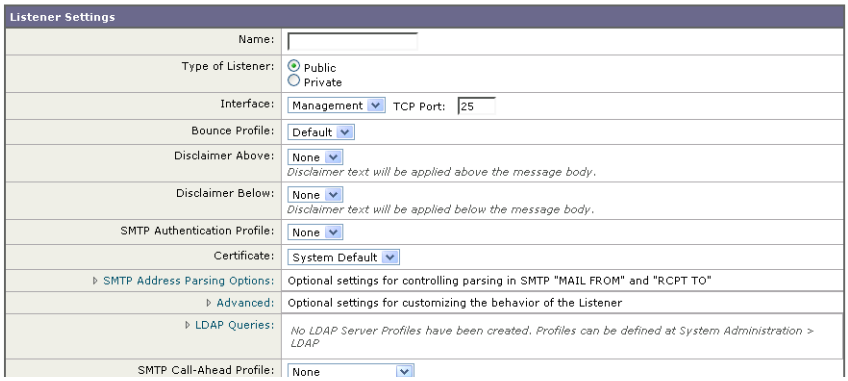
リスナーからの免責事項テキストの追加

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 IronPort 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`」という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」の章の「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 14-13　　リスナーに免責事項を含める編集



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「免責条項文の追加」を使用して、メッセージの免責事項に特定の定義済みテキスト文字列を付加することができます。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」に属する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 14-3　　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。

表 14-3　アンチウイルス通知変数（続き）

変数	置き換える値
$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	メッセージを内部で識別するために使用するメッセージ ID（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のカンマ区切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 サイズの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 IronPort 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 IronPort 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。
$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。

表 14-3　アンチウイルス通知変数（続き）

変数	置き換える値
$DLPSeverity	違反の重大度に置き換えられます。値は [低（Low）]、[中（Medium）]、[高（High）]、または [重大（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、UTF8 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 Subject: Hi!	ヘッダー
<空白行>	
Hello!	本文パート
このメッセージはスキャンされました。	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
このメッセージはスキャンされました。	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.
```

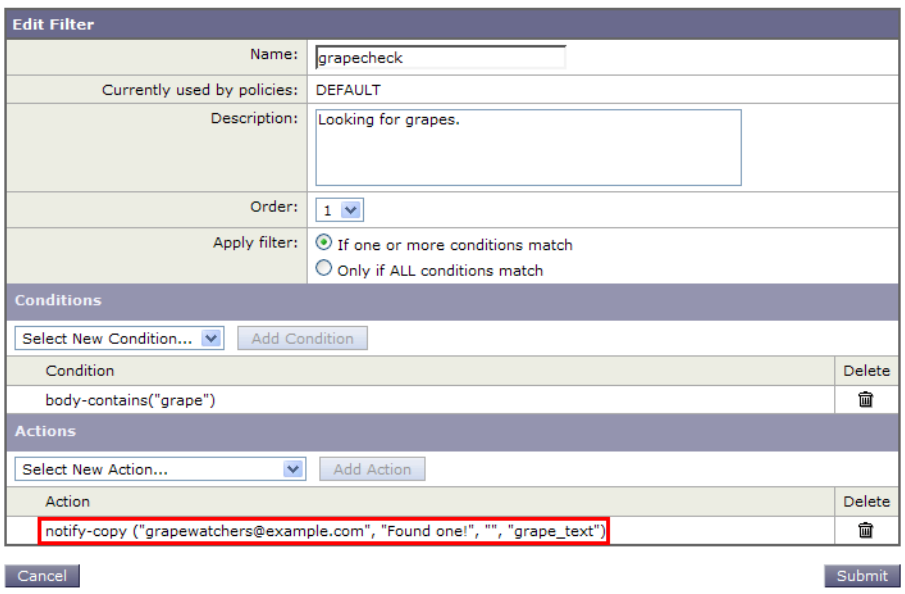
localeconfig コマンドの詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Customizing Listeners」の章を参照してください。

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。生成されるさまざまなメッセージに対する返信アドレスの設定（15-15 ページ）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 14-14 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 14-14　コンテンツ フィルタによる通知の例



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。

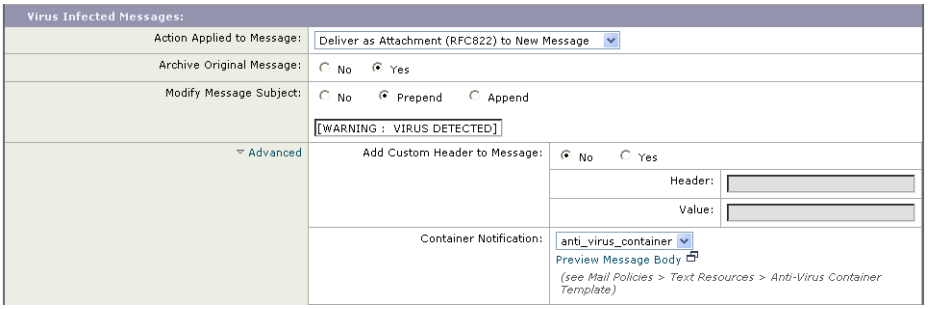
- **アンチウイルス通知テンプレート**。アンチウイルス通知テンプレートは、元のメッセージがウイルス通知に添付されていない場合に使用されます。
- **アンチウイルス コンテナ テンプレート**。コンテナ テンプレートは、元のメッセージが添付ファイルとして送信される際に使用されます。

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 ポリシーの編集中に送信するカスタム通知を指定できます。ウイルス対策通知用の From: アドレスを設定できます。詳細については、生成されるさまざまなメッセージに対する返信アドレスの設定（15-15 ページ）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 14-15 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 14-15　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 14-4 に記載されている通知変数を使用できます。

表 14-4　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。 例：“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。 例：“HELLO.SCR” : “W32/Bagel-F” <unnamed part of the message> : “Unix/Apache.Trojan”

表 14-4　アンチウイルス通知変数（続き）

変数	置き換える値
$AV_VERDICT	アンチウイルスの判定に置き換えられます。
$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。 例：“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。例：“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。 例：“HELLO.SCR”, “CheckThisOut.exe”
$AV_REPAIRED_PARTS	修復されたファイル名またはパート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ト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ト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	メッセージを内部で識別するために使用するメッセージ ID（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のカンマ区切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。

表 14-4　アンチウイルス通知変数（続き）

変数	置き換える値
$filesizes	メッセージの添付ファイル サイズの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 IronPort 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 IronPort 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。

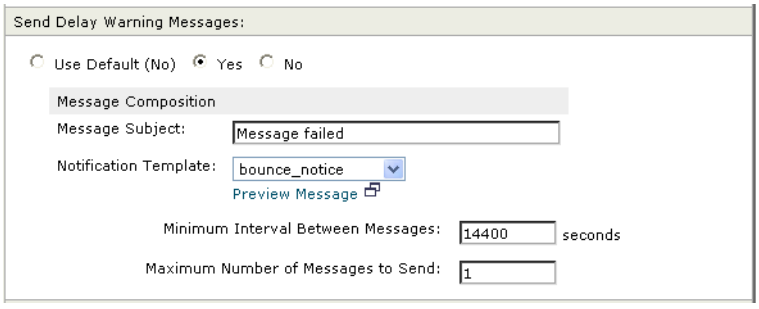
テキスト リソースを定義した後、[メールポリシー（Mail Policies）] > [送受信メールポリシー（Incoming/Outgoing Mail Policies）] > [ウイルス対策設定を編集（Edit Anti-Virus Settings）] ページまたは `policyconfig -> edit -> antivirus` コマンドを使用して、修復されたメッセージ、スキャンできなかったメッセージ、暗号化されたメッセージ、またはウイルスが陽性のメッセージに対して、元のメッセージが RFC 822 のアタッチメントとして含まれるように指定します。詳細については、カスタムのアラート通知の送信（受信者宛てのみ）（8-14 ページ）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中に、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 14-16 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。

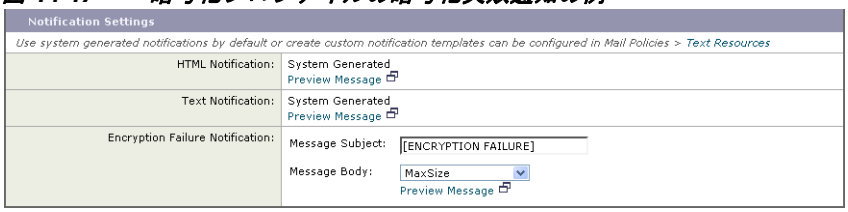
図 14-16　バウンス プロファイルのバウンス通知の例



（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 14-17 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 14-17　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 14-5 に記載されている通知変数を使用できます。

表 14-5　バウンス通知変数

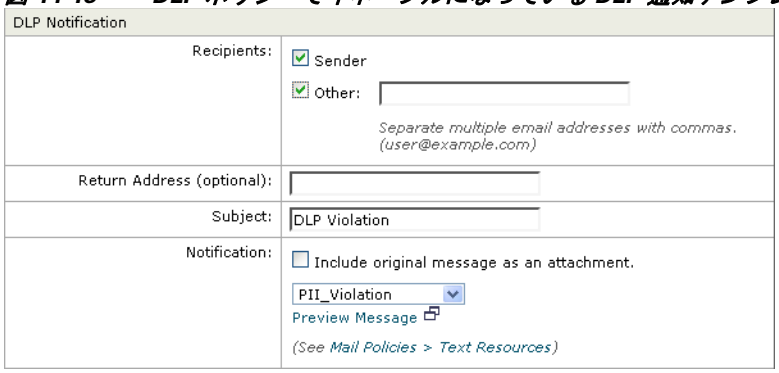
変数	置き換える値
$Subject	元のメッセージの件名。
$Date	現在の日付（MM/DD/YYYY 形式）に置き換えられます。
$Time	現在の時刻（ローカル時間帯）に置き換えられます。
$GMTimeStamp	現在の時刻および日付（GMT）に置き換えられます。電子メール メッセージの Received: 行で見られる形式と同様です。
$MID	メッセージを内部で識別するために使用するメッセージ ID（MID）に置き換えられます。RFC822「Message-Id」の値とは異なるため注意してください（「Message-Id」を取得するには $Header を使用します）。
$BouncedRecipient	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 IronPort 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。

DLP 通知テンプレート

DLP 通知テンプレートは、RSA Email DLP 機能を使用するようにアプライアンスを設定した際に使用されます。通知では、発信メッセージが企業のデータ消失防止ポリシーに違反した機密性の高いデータを含んでいる可能性があることを受信者に知らせます。DLP Policy Manager で DLP ポリシーを編集している間に、カスタム DLP 通知を指定できます。

図 14-18 は、DLP ポリシーで使用されている DLP 通知テンプレートの例を示しています。

図 14-18　DLP ポリシーでイネーブルになっている DLP 通知テンプレート



DLP 通知変数

DLP 通知テンプレートでは、次の変数を使用できます。

表 14-6　DLP 通知変数

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。値は [低（Low）]、[中（Medium）]、[高（High）]、または [重大（Critical）] のいずれかです。
$DLPRiskFactor	メッセージの機密内容のリスク要因スコアに置き換えられます（スコア 0 ～ 100）。
$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	メッセージを内部で識別するために使用するメッセージ ID（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のカンマ区切リストに置き換えられます。

表 14-6　DLP 通知変数

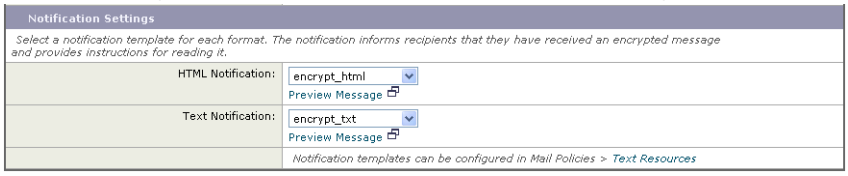
変数	置き換える値
$filetypes	メッセージの添付ファイルのファイル タイプを示すカンマ区切りリストに置き換えられます。
$filesizes	メッセージの添付ファイル サイズのカンマ区切りリストに置き換えられます。
$remotehost	メッセージを Cisco IronPort アプライアンスに送信したシステムのホスト名に置き換えられます。
$AllHeaders	メッセージ ヘッダーに置き換えられます。
$EnvelopeFrom	メッセージのエンベロープ送信者（Envelope From、<MAIL FROM>）に置き換えられます。
$Hostname	Cisco IronPort アプライアンスのホスト名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。
$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。
$remoteip	メッセージを Cisco IronPort 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。
$recvlistener	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。
$dropped_filenames	`$filenames` 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。
$dropped_filename	直近にドロップされたファイル名のみを返します。
$recvint	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。
$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。
$Time	現在の時刻（ローカル時間帯）に置き換えられます。
$orgid	SenderBase 組織 ID（整数値）で置き換えられます。
$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。
$dropped_filetypes	`$filetypes` 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。
$dropped_filetype	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。

暗号化通知テンプレート

暗号化通知テンプレートは、発信電子メールを暗号化するように Cisco IronPort 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 14-19 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 14-19　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 15

システム管理

一般的なシステム管理は、主にグラフィカル ユーザ インターフェイス（GUI）の [System Administration] メニューから実行します。一部のシステム管理機能は、コマンドライン インターフェイス（CLI）を介してのみアクセスできます。

さらに、Cisco IronPort のグラフィカル ユーザ インターフェイス（GUI）から、Cisco IronPort アプライアンスのシステム モニタリング機能にアクセスすることもできます（Other Tasks in the GUI（-441 ページ）を参照）。

（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（B-3 ページ）を参照してください。

AsyncOS のアップグレード

アップグレードする前に

AsyncOS をアップグレードするには、次の 2 つのステップ プロセスを使用します。

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 イメージなどをダウンロードする場所を選択できます。詳細については、GUI からのアップグレード設定値の設定（15-5 ページ）を参照してください。

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。詳細については、アップデート設定を構成した後の AsyncOS のアップグレード（15-2 ページ）と CLI からの AsyncOS のアップグレード（15-3 ページ）を参照してください。

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。

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。

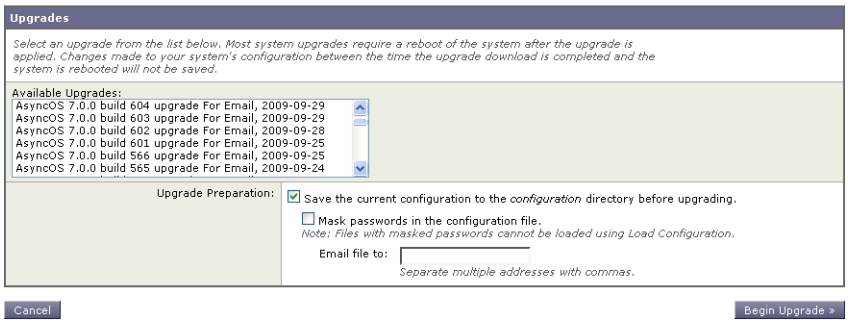
ステップ 4　キューが空になるまで待ちます。CLI の `workqueue` コマンドでワークキュー内のメッセージ数を表示するか、`rate` コマンドでアプライアンスのメッセージ スループットをモニタすることができます。

（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。

アップデート設定を構成した後の AsyncOS のアップグレード

ステップ 1　[システム管理（System Administration）] > [システムのアップグレード（System Upgrade）] ページで、[使用可能なアップグレード（Available Upgrades）] をクリックします。[使用可能なアップグレード（Available Upgrades）] ページが表示されます。

図 15-1　[Available Upgrades] ページ



ステップ 2　利用可能なアップグレードのリストから、アップグレードを選択します。

ステップ 3　現在の設定を `configuration` ディレクトリに保存するかどうかを選択します。

ステップ 4　コンフィギュレーション 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コンフィギュレーション 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。

ステップ 5　コンフィギュレーション 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　[アップグレード開始(Begin Upgrade)] をクリックします。ページの上部の近くに、経過表示バーが表示されます。変更の確定や新しいライセンス契約書への合意などを 1 回以上求められる場合があります。

ステップ 7　アップグレードが完了すると、アプライアンスをリブートするように求められます。

ステップ 8　[今すぐ再起動(Reboot Now)] をクリックします。

CLI からの AsyncOS のアップグレード

`upgrade` コマンドを発行して、利用可能なアップグレードのリストを表示します。リストから目的のアップグレードを選択して、インストールします。メッセージの確認や、使用許諾契約書を読み同意することを求められる場合があります。現在の設定を `configuration` ディレクトリに保存するかどうかを選択できます。その場合は、コンフィギュレーション ファイルでパスワードをマスクするかどうかを選択できます。また、設定ファイルのコピーを電子メールで送信することを選択することもできます。

（注）　マスクされたパスワードが記載されたコンフィギュレーション ファイルは、`loadconfig` コマンドからロードできません。

アップグレード時には、さまざまなプロンプトで長い時間作業を中断しないでください。TCP セッションがダウンロード中にタイムアウトしてしまった場合、アップグレードが失敗する可能性があります。

従来のアップグレード方式との違い

従来の方式と比較して、AsyncOS をローカル サーバからアップグレードする場合には、次の違いがあることに注意してください。

ステップ 1　*ダウンロード中に*、アップグレードによるインストールがすぐに実行されます。

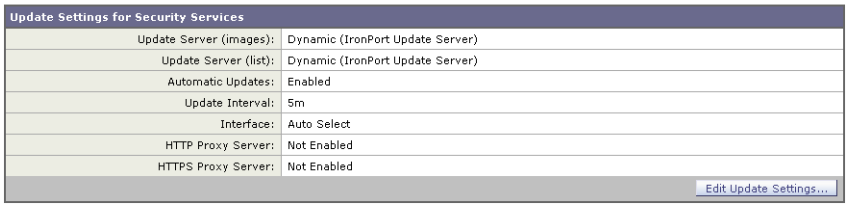
アップグレード プロセスの開始時に、バナーが 10 秒間表示されます。このバナーが表示されている間は、Ctrl を押した状態で C を押すと、ダウンロードの開始前にアップグレード プロセスを終了できます。

AsyncOS アップグレード設定の構成

Cisco IronPort アプライアンスは、Cisco IronPort アップデート サーバから AsyncOS アップグレードを直接ダウンロードします。各 Cisco IronPort アプライアンスは、個別にアップグレードをダウンロードします。詳細については、アップグレードの概要（15-4 ページ）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、アップグレードおよびプロキシ サーバの設定をダウンロードするために使用するインターフェイスを設定します。詳細については、GUI からのアップグレード設定値の設定（15-5 ページ）を参照してください。オプションで、CLI で `updateconfig` コマンドを使用します。

図 15-2　[Service Updates] ページ



（注） どちらのアップグレード方式を使用しても、アップグレードの完了後は、`saveconfig` コマンドを使用して設定を保存するかどうか判断する必要があります。詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Managing the Configuration File」を参照してください。

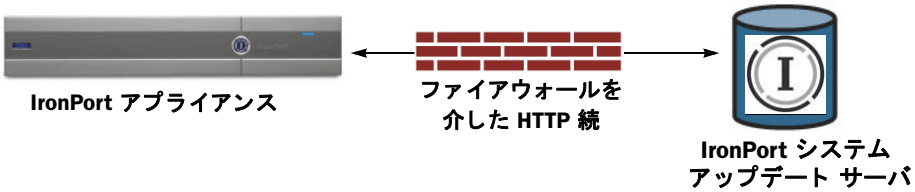
クラスタ化されたシステムのアップグレード

クラスタ化されたマシンをアップグレードする場合は、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Centralized Management」の章にある「Upgrading Machines in a Cluster」を参照してください。

アップグレードの概要

Cisco IronPort アプライアンスは、アップグレードを検索してダウンロードするために、Cisco IronPort アップデート サーバに直接接続します。

図 15-3　ストリーミング アップデートの方法



Cisco IronPort Systems では分散アップグレード 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 IronPort 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、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。詳細については、アップグレードのための静的アドレスの設定（15-5 ページ）を参照してください。

ポート 80 および 443 による Cisco IronPort 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。ポート 22、25、80、4766 などによる `upgrades.ironport.com` からのレガシー 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がすでに設定されている場合、そのルールを削除するか、修正したファイアウォールのルールで置き換えるか、もしくはこの両方の必要があります。詳細については、付録 C、ファイアウォール情報を参照してください。

アップグレードのための静的アドレスの設定

McAfee Anti-Virus および Cisco IronPort AsyncOS 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。

ステップ 1　Cisco IronPort カスタマー サポートに問い合わせて、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）] ページに移動して、[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 4　[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 5　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 6　変更を送信し、保存します。

GUI からのアップグレード設定値の設定

アップデート設定には、アップグレードおよびプロキシ サーバ設定のダウンロードに使用するインターフェイスが含まれています。AsyncOS のアップグレードに加えて、アンチスパム サービス、アンチウイルス サービス、および感染フィルタ サービスなどさまざまな Cisco IronPort サービスの設定値も編集できます。アップデート サービスの詳細については、サービスのアップデート（15-9 ページ）を参照してください。

ステップ 1　[Security Services] > [Service Updates] ページで、[Edit Update Settings] をクリックします。

[Edit Update Settings] ページが表示されます。

ステップ 2　アップグレードに使用するインターフェイスを選択します。

ステップ 3　必要に応じて、HTTP プロキシ サーバまたは HTTPS プロキシ サーバ情報を入力します。

ステップ 4　変更を送信し、保存します。

CLI からのアップグレード設定値の設定

AsyncOS アップグレードを取得する場所（ローカル サーバまたは Cisco IronPort サーバ）をアプライアンスに設定するには、`updateconfig` コマンドを実行します。アップグレードをインストールするには、`upgrade` コマンドを実行します。

updateconfig コマンド

updateconfig コマンドは、AsyncOS アップグレードを含むサービス アップデートを参照する場所を Cisco IronPort アプライアンスに設定するために使用されます。デフォルトでは、upgrade コマンドを入力すると、アプライアンスは Cisco IronPort アップグレード サーバに最新のアップデートを問い合わせます。

AsyncOS 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 IronPort Quality Assurance チームによる認定が必要です。Cisco IronPort 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 IronPort 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 IronPort 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 復元の実行

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 IronPort 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.


Do you want to continue?

Are you *really* sure you want to continue? yes


 Available version               Install date

 =================               ============

 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　アプライアンスは 2 回リブートします。

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　変更を保存します。

復元が完了した Cisco IronPort 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。

サービスのアップデート

Cisco IronPort アプライアンスがさまざまなサービス（アンチスパム、アンチウイルス、感染フィルタ サービスなど）をアップデートする方法の設定には、多くの設定値が使用されています。これらの設定値には、[セキュリティサービス（Security Services）] メニューの [サービスのアップデート（Service Updates）] ページ、または CLI の `updateconfig` コマンドからアクセスできます。

[Service Updates] ページ

[Service Updates] ページ（GUI の [Security Services] メニューから利用可能）では、Cisco IronPort アプライアンスのさまざまなサービスのアップデートに関する現在の設定値を表示します。アップデート設定には、アップデート サーバ（イメージ）、アップデート サーバ（リスト）、さまざまなコンポーネントのアップデート URL、自動アップデートのイネーブル化、自動アップデート間隔、HTTP プロキシ サーバおよび HTTPS プロキシ サーバが含まれます。

（注）　Cisco IronPort アップデート サーバでは、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、セキュリティ コンポーネント 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。アップデートおよびアップグレードに関して、ファイアウォール設定にスタティック IP アドレスが必要だと判断した場合、次の指示に従ってアップデート設定値を編集し、Cisco IronPort カスタマー サポートに必要な URL アドレスを問い合わせて取得します。

アップデート設定値の編集

Cisco IronPort アプライアンスのアップデート設定値を編集するには、[アップデート設定を編集（Edit Update Settings）] ボタンをクリックします。アップデート サーバ（イメージ）、アップデート サーバ（リスト）、自動更新、インターフェイス、およびプロキシ サーバの設定を構成できます。アップデート設定値の詳細については、表 15-1（15-12 ページ）を参照してください。

図 15-4 は、アップデート サーバの利用可能な設定値を示しています。

図 15-4　　イメージおよびリストに関するアップデート サーバの設定値

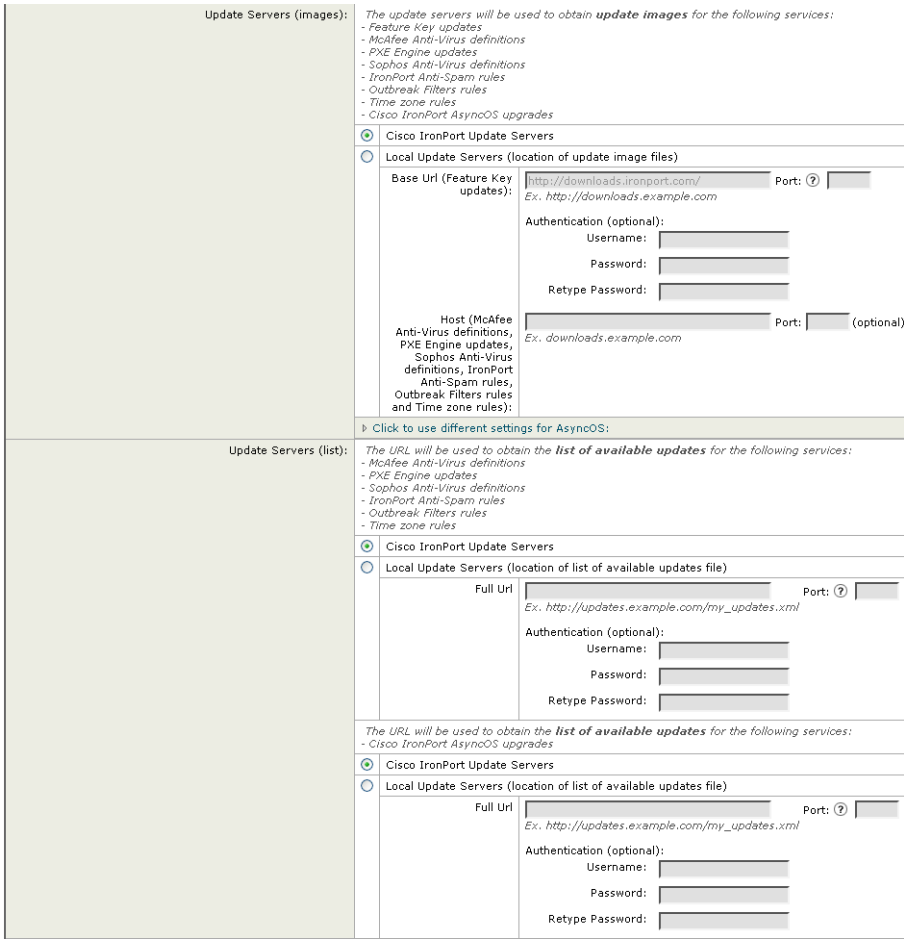


図 15-5 は、[Automatic Updates] および [Interface] で利用可能な設定値を示しています。

図 15-5　　自動更新設定およびインターフェイスの設定

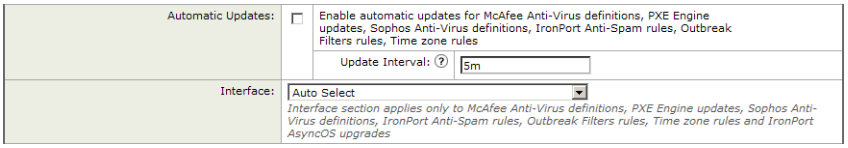


図 15-6 は、プロキシ サーバの利用可能な設定値を示しています。

図 15-6　　プロキシ サーバの設定値

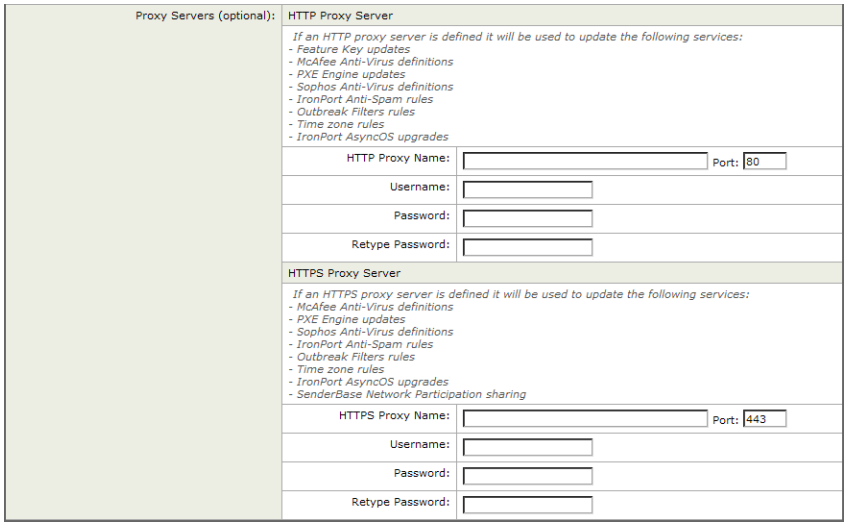


表 15-1 に、設定可能なアップデート設定値を示します。

表 15-1　　アップデート設定値

設定	説明
アップデート サーバ（イメージ）（Update Servers (images)）	Cisco IronPort AsyncOS アップグレード イメージおよびサービスのアップデートを、Cisco IronPort アップデート サーバまたはローカル Web 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。 これらのサーバは AsyncOS アップグレードのほかにも、Sophos および McAfee Anti-Virus 定義ファイル、Cisco IronPort Anti-Spam および Cisco IronPort Intelligent Multi-Scan ルール、感染フィルタ ルール、時間帯ルール、機能キーのアップデート、および PXE Engine のアップデートに関するアップデート イメージの取得に使用されます。 AsyncOS アップグレードの設定を表示するには、[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。 次のいずれかの場合、ローカル Web サーバを選択します。 • Cisco IronPort からアップグレードおよびアップデート イメージをダウンロードし、Cisco IronPort カスタマー サポートから提供されたスタティック アドレスを入力する必要がある場合。 • 任意のタイミングで Cisco IronPort AsyncOS アップグレード イメージをダウンロードする場合。（この場合でも、Cisco Ironport アップデート サーバからサービス アップデート イメージを動的にダウンロードできます）。 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。 **（注）** Cisco IronPort 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。

表 15-1　アップデート設定値（続き）

設定	説明
アップデート サーバ（リスト）（Update Servers (lists)）	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 サーバまたはローカル Web サーバのどちらからダウンロードするかを選択します。マニフェスト XML ファイルには、AsyncOS アップグレードのほかに McAfee Anti-Virus や PXE Engine などのさまざまなセキュリティ コンポーネントのアップデートが含まれます。 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。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。 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も入力します。 詳細については、Remote Upgrade Overview, page 15-5 を参照してください。
自動更新（Automatic Updates）	Sophos および McAfee Anti-Virus 定義ファイル、Cisco IronPort Anti-Spam ルール、Cisco IronPort 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。
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および Cisco IronPort AsyncOS アップグレードをアップデート 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す。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、これらのすべてのサービスで指定したプロキシ サーバが使用されることに注意してください。
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。

アップデート サーバの設定

ステップ 1　Cisco IronPort アップデート サーバまたはローカル アップデート サーバのいずれかから、サービスのアップデート イメージを取得するサーバを選択します。

（注）　アップグレードのソースとしてローカル サーバを選択した場合、Sophos および McAfee Anti-Virus 定義ファイルなど、複数のセキュリティ コンポーネントの自動アップデートが停止します。これらのセキュリティ コンポーネントのアップデートを継続するには、アップデート イメージまたはアップデートのリストをローカル サーバでホスティングします。

ステップ 2　アップデート イメージの取得先にローカル アップデート サーバを選択した場合、最初に AsyncOS アップグレードおよび McAfee Anti-Virus 定義ファイルを除く、すべてのサービス アップデートをホスティングするローカル サーバのベース URL、ポート番号、およびオプションの認証情報を入力します。

ステップ 3　AsyncOS アップグレードと McAfee Anti-Virus の定義を他のサービス アップデートとは異なる場所から取得する場合は、同じセクションの下部にある [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、次のオプションのいずれかを選択します。

- [Cisco IronPort アップデートサーバ（Cisco IronPort Update Server）]。
- [ローカルアップデートサーバ（Local Update Servers）]。AsyncOS アップグレードをホスティングするローカル サーバのベース URL とポート番号を入力します。

ステップ 4　利用可能なアップグレードのリストの取得先にローカル アップデート サーバを選択した場合、ファイル名、HTTP ポート番号およびオプションの認証情報を含む、リストの XML ファイルへの完全なパスを入力します。

自動アップデートの設定

ステップ 1　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 2　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。

HTTP プロキシ サーバの指定（任意）

ステップ 1　サーバの URL とポート番号を入力します。

ステップ 2　必要に応じて、サーバのアカウントのユーザ名とパスワードを入力します。

ステップ 3　変更を送信し、保存します。

HTTPS プロキシ サーバの指定（任意）

ステップ 1　サーバの URL とポート番号を入力します。

ステップ 2　必要に応じて、サーバのアカウントのユーザ名とパスワードを入力します。

ステップ 3　変更を送信し、保存します。

生成されるさまざまなメッセージに対する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。

GUI の [システム管理（System Administration）] メニューから利用できる [返信先アドレス（Return Addresses）] ページを使用するか、CLI で `addressconfig` コマンドを使用します。

図 15-7　[Return Addresses] ページ

Return Addresses

Return Addresses for System-Generated Email	
Anti-Virus Messages:	"Mail Delivery System" <MAILER-DAEMON@*hostname*>
Bounce Messages:	"Mail Delivery System" <MAILER-DAEMON@*hostname*>
Notifications:	"Mail Delivery System" <MAILER-DAEMON@*hostname*>
Quarantine Messages:	"Mail Delivery System" <MAILER-DAEMON@*hostname*>
Reports:	IronPort Reporting <reporting@*hostname*>
	Edit Settings...

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 で変更するには、[返信先アドレス（Return Addresses）] ページで [設定の編集（Edit Settings）] をクリックします。1 つまたは複数のアドレスを変更して [送信（Submit）] をクリックし、変更を保存します。

アラート

アラートとは、Cisco IronPort 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 IronPort 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 2 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。

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（15-20 ページ）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（15-21 ページ）を参照してください。

アラートの分類

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
- アンチウイルス
- スパム対策
- 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。

- Critical：すぐに対処が必要です。
- 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。
- 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。この増加は、待機する秒数に、直前の間隔の 2 倍を加えたものになります。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 メッセージを送信する前に待機する最大の秒数（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 IronPort 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 IronPort 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ルまたはディセーブルにするには、アラート設定値の設定（15-20 ページ）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 IronPort 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 IronPort 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す。

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

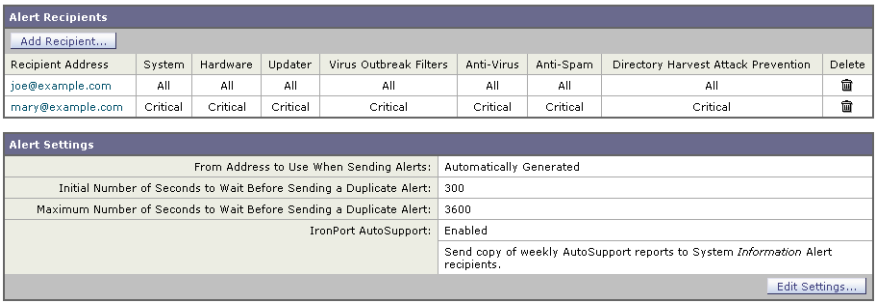
```
Date: 23 Mar 2005 21:10:19 +0000

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.
```

アラート受信者の管理

グラフィカル ユーザ インターフェイス（GUI）にログインして、[System Administration] タブをクリックします（GUI へのアクセス方法の詳細については、GUI へのアクセス（2-2 ページ）を参照してください）。左側のメニューで [アラート（Alerts）] リンクをクリックします。

図 15-8　[アラート（Alerts）] ページ



（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。

[アラート（Alerts）] ページは、既存のアラート受信者およびアラート設定のリストを表示します。

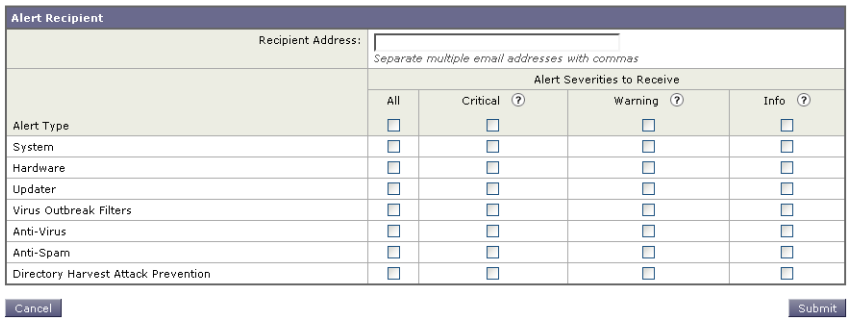
[アラート（Alerts）] ページからは、次の操作ができます。

- アラート受信者の追加、設定、または削除
- アラート設定値の変更

新規アラート受信者の追加

ステップ 1　[アラート（Alerts）] ページで [受信者を追加（Add Recipient）] をクリックします。[Add Alert Recipients] ページが表示されます。

図 15-9　新規アラート受信者の追加



ステップ 2　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 3　受信するアラートの重大度を選択します。

ステップ 4　変更を送信し、保存します。

既存のアラート受信者の設定

ステップ 1　[アラート受信者（Alert Recipients）] のリストからアラート受信者をクリックします。[Configure Alert Recipient] ページが表示されます。

ステップ 2　アラート受信者の設定を変更します。

ステップ 3　変更を送信し、保存します。

アラート受信者の削除

ステップ 1　[アラート受信者（Alert Recipient）] のリストから、アラート受信者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認します。

ステップ 3　変更を保存します。

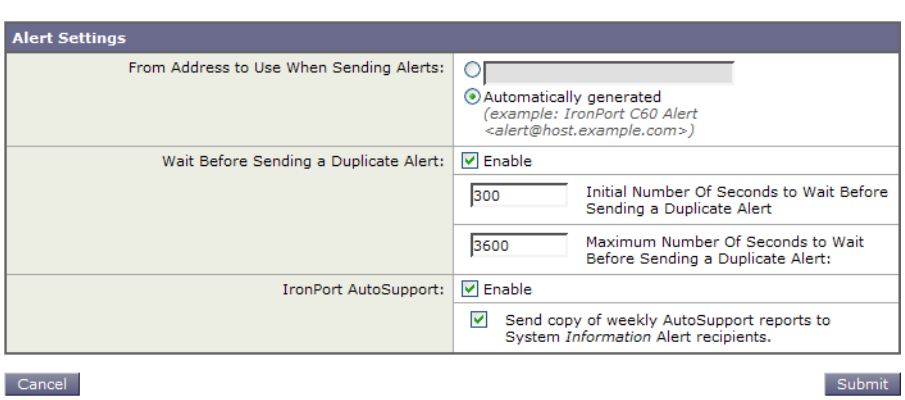
アラート設定値の設定

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。

アラート設定値の編集

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。[Edit Alert Settings] ページが表示されます。

図 15-10　アラート設定値の編集



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（15-17 ページ）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 IronPort AutoSupport（15-17 ページ）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　変更を送信し、保存します。

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 IronPort 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 15-2 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 15-2　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 クリティカル。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。 「**message**」: ログ メッセージ。 「**tb**」: イベントのトレースバック。
AS.TOOL.INFO_ALERT	Update - $engine - $message 情報。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す。	「**engine**」: アンチスパム エンジンの名前 「**message**」: メッセージ。
AS.TOOL.ALERT	Update - $engine - $message クリティカル。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 「**message**」: メッセージ。

アンチウイルス アラート

表 15-3 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 15-3　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/ AV.SERVER.CRITICAL	$engine antivirus - $message $tb クリティカル。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。	「**engine**」: アンチウイルス エンジンのタイプ。 「**message**」: ログ メッセージ。 「**tb**」: イベントのトレースバック。
AV.SERVER.ALERT.INFO	$engine antivirus - $message $tb 情報。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。	「**engine**」: アンチウイルス エンジンのタイプ。 「**message**」: ログ メッセージ。 「**tb**」: イベントのトレースバック。

表 15-3　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（続き）

アラート名	メッセージと説明	パラメータ
AV.SERVER.ALERT.WARN	$engine antivirus - $message $tb 警告。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。	「**engine**」：アンチウイルス エンジンのタイプ。 「**message**」：ログ メッセージ。 「**tb**」：イベントのトレースバック。
MAIL.ANTIVIRUS.ERROR_MESSAGE	MID $mid antivirus $what error $tag クリティカル。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。	「**mid**」：MID 「**what**」：発生したエラー。 「**tag**」：ウイルス アウトブレイク名（設定されている場合）。
MAIL.SCANNER.PROTOCOL_MAX_RETRY	MID $mid is malformed and cannot be scanned by $engine. クリティカル。メッセージが不正なため、スキャン エンジンは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。	「**mid**」：MID 「**engine**」：使用されているエンジン。

ディレクトリ獲得攻撃（DHAP）アラート

表 15-4 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 15-4　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. 警告。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 15-5 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 15-5　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. 警告。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。	「**port**」: インターフェイス名。 「**in_err**」: 最後のメッセージ以降の入力エラー数。 「**out_err**」: 最後のメッセージ以降の出力エラー数。 「**col**」: 最後のメッセージ以降のパケット衝突数。
MAIL.MEASUREMENTS_ FILESYSTEM	The $file_system partition is at $capacity% capacity 警告。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。	「**file_system**」: ファイルシステムの名前 「**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 クリティカル。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。	「**file_system**」: ファイルシステムの名前 「**capacity**」: ファイル システムの使用率(%)。
SYSTEM.RAID_EVENT_ ALERT	A RAID-event has occurred: $error 警告。重大な RAID-event が発生した場合に送信されます。	「**error**」: RAID エラーのテキスト。
SYSTEM.RAID_EVENT_ ALERT_INFO	A RAID-event has occurred: $error 情報。RAID-event が発生した場合に送信されます。	「**error**」: RAID エラーのテキスト。

Cisco IronPort スパム隔離アラート

表 15-6 に、AsyncOS で生成される可能性があるさまざまな Cisco IronPort スパム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 15-6　発生する可能性がある Cisco IronPort スパム隔離アラートのリスト

アラート名(Alert Name)	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 情報。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。	「**host**」: オフボックス隔離のアドレス。 「**port**」: オフボックス隔離に接続するポート。

表 15-6　発生する可能性がある Cisco IronPort スパム隔離アラートのリスト（続き）

アラート名（Alert Name）	メッセージと説明	パラメータ
ISQ.CRITICAL	ISQ: $msg	「**msg**」: 表示されるメッセージ
	クリティカル。Cisco IronPort スパム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	「**threshold**」: アラートを開始する使用率のしきい値
	警告。Cisco IronPort スパム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	
	クリティカル。Cisco IronPort スパム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	「**mid**」: MID 「**rcpt**」: 受信者または「all」 「**reason**」: メッセージが削除されない理由
	警告。Cisco IronPort スパム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	「**reason**」: 通知が送信されない理由
	警告。通知メッセージの送信に失敗した場合に送信されます。	
ISQ.MSG_QUAR_FAILED		
	警告。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	「**mid**」: MID 「**rcpt**」: 受信者または「all」 「**reason**」: メッセージが解放されない理由
	警告。メッセージの開放に失敗した場合に送信されます。	
ISQ.MSG_RLS_FAILED_UNK_RCPTS	ISQ: Failed to release MID $mid: $reason	「**mid**」: MID 「**reason**」: メッセージが解放されない理由
	警告。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。	
ISQ.NO_EU_PROPS	ISQ: Could not retrieve $user's properties. Setting defaults	「**user**」: エンドユーザ名
	情報。AsyncOS がユーザの情報を取得できない場合に送信されます。	

表 15-6　発生する可能性がある Cisco IronPort スパム隔離アラートのリスト（続き）

アラート名（Alert Name）	メッセージと説明	パラメータ
ISQ.NO_OFF_BOX_HOST_SET	ISQ: Setting up off-box ISQ without setting host	
	情報。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 15-7　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（Alert Name）	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**」：エラーの原因
	クリティカル。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） 「**limit**」：設定された制限使用量（MB）
	クリティカル。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。	

システム アラート

表 15-8 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 15-8　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（通常はトレースバック）
	警告。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。	

表 15-8　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
COMMON.KEY_EXPIRED_ALERT	Your "$feature" key has expired. Please contact your authorized Cisco IronPort sales representative.	「**feature**」: 有効期限が切れる機能の名前。
	警告。ライセンス キーの有効期限が切れた場合に送信されます。	
COMMON.KEY_EXPIRING_ALERT	Your "$feature" key will expire in under $days day(s). Please contact your authorized Cisco IronPort sales representative.	「**feature**」: 有効期限が切れる機能の名前。 「**days**」: 有効期限が切れるまでの日数。
	警告。ライセンス キーの有効期限が切れる場合に送信されます。	
COMMON.KEY_FINAL_ EXPIRING_ALERT	This is a final notice. Your "$feature" key will expire in under $days day(s). Please contact your authorized Cisco IronPort sales representative.	「**feature**」: 有効期限が切れる機能の名前。 「**days**」: 有効期限が切れるまでの日数。
	警告。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.	
	警告。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 「**pair_name**」: フェールオーバーのペア名。
	警告。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**」: 障害が発生したポート 「**pair_name**」: フェールオーバーのペア名。
	情報。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**」: 障害が発生したポート 「**port_other**」: 新しいポート 「**pair_name**」: フェールオーバーのペア名。
	クリティカル。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 15-8　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.FAILURE_DETECTED_NO_BACKUP	Port $port_other on $pair_name is down, can't switch to $port_other	「**port**」：障害が発生したポート 「**port_other**」：新しいポート 「**pair_name**」：フェールオーバーのペア名。
	クリティカル。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.FAILURE_RECOVERED	Recovered network on $pair_name using port $port	「**port**」：障害が発生したポート 「**pair_name**」：フェールオーバーのペア名。
	情報。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.MANUAL	Manual failover to port $port on $pair_name	「**port**」：新しいアクティブポート。 「**pair_name**」：フェールオーバーのペア名。
	情報。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」、「SimpleFilter」などのいずれか。 「**error**」：フィルタが無効な理由に関する追加の情報。
	警告。無効なフィルタが存在する場合に送信されます。	
LDAP.GROUP_QUERY_FAILED_ALERT	LDAP: Failed group query $name, comparison in filter will evaluate as false	「**name**」：クエリーの名前。
	クリティカル。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。 「**why**」：エラーが発生した理由。
	クリティカル。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.*	クリティカル。さまざまなロギング エラー。	
MAIL.PERRCPT.LDAP_GROUP_QUERY_FAILED	LDAP group query failure during per-recipient scanning, possible LDAP misconfiguration or unreachable server.	
	クリティカル。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.*	クリティカル。メール キューのさまざまなハード エラー。	

表 15-8　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%.	「**hostname**」: ホストの名前。 「**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。 「**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。
	クリティカル。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.	「**hostname**」: ホストの名前。
	クリティカル。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%.	「**hostname**」: ホストの名前。 「**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。 「**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。
	クリティカル。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 15-8　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。 「**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。 「**resume_threshold**」: リスナーが再開されるワーク キューの上限サイズ。
	情報。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。
	クリティカル。アプライアンスが「リソース節約」モードにな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。
	情報。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。 「**reason**」: ワーク キューが中断された理由。
	クリティカル。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。
	クリティカル。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	
	警告。Sent when the Cisco IronPort appliance is unable to adjust time because NTP is not running as root.	

表 15-8　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
	クリティカル。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。 「**target_version**」: 対象のスキーマ バージョン。
	クリティカル。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 $file_system partition.	「**file_system**」: ファイルシステムの名前
	クリティカル。隔離用のディスク領域がフルになった場合に送信されます。	
QUARANTINE.THRESHOLD_ALERT	Quarantine "$quarantine" is $full% full	「**quarantine**」: 隔離の名前。 「**full**」: 隔離エリアの容量使用率。
	警告。隔離エリアの容量使用率が 5 %、50 %、または 75 % に達した場合に送信されます。	
QUARANTINE.THRESHOLD_ALERT .SERIOUS	Quarantine "$quarantine" is $full% full	「**quarantine**」: 隔離の名前。 「**full**」: 隔離エリアの容量使用率。
	クリティカル。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
	クリティカル。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 15-8　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	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 $threshold percent, full processing of reporting data will be restarted automatically.	「**threshold**」: しきい値
	警告。システムのディスク領域が不足している場合に送信されます。ログ エントリに関するディスク使用率がログ使用率のしきい値を超過すると、reportd は集約をディセーブルにし、アラートを送信します。	
REPORTING.CLIENT.UPDATE_FAILED_ALERT	Reporting Client: The reporting system has not responded for an extended period of time ($duration).	「**duration**」: 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」）。
	警告。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。	
REPORTING.CLIENT.JOURNAL.FULL	Reporting Client: The reporting system is unable to maintain the rate of data being generated. Any new data generated will be lost.	
	クリティカル。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。	
REPORTING.CLIENT.JOURNAL.FREE	Reporting Client: The reporting system is now able to handle new data.	
	情報。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。	
PERIODIC_REPORTS.REPORT_TASK.BUILD_FAILURE	A failure occurred while building periodic report '$report_title'. This subscription has been removed from the scheduler.	「**report_title**」: レポートのタイトル
	クリティカル。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。	

表 15-8　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. REPORT_TASK.EMAIL_ FAILURE	A failure occurred while emailing periodic report '$report_title'. This subscription has been removed from the scheduler.	「**report_title**」: レポートのタイトル
	クリティカル。レポートを電子メールで送信できなかった場合に送信されます。	
PERIODIC_REPORTS. REPORT_TASK.ARCHIVE_FAILURE	A failure occurred while archiving periodic report '$report_title'. This subscription has been removed from the scheduler.	「**report_title**」: レポートのタイトル
	クリティカル。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。 「**response**」: 受信した応答の raw データ。
	情報。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_FAILED _ALERT	SMTP Auth: could not reach forwarding server $ip with reason: $why	「**ip**」: リモート サーバの IP。 「**why**」: エラーが発生した理由。
	警告。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_FAILED	SMTP Auth: LDAP query failed, see LDAP debug logs for details.	
	警告。LDAP クエリーが失敗した場合に送信されます。	
SYSTEM.HERMES_ SHUTDOWN_FAILURE. REBOOT	While preparing to ${what}, failed to stop mail server gracefully: ${error}$what:=reboot	「**error**」: 発生したエラー。
	警告。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_ SHUTDOWN_FAILURE. SHUTDOWN	While preparing to ${what}, failed to stop mail server gracefully: ${error}$what:=shut down	「**error**」: 発生したエラー。
	警告。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. RCPTVALIDATION.UPDATE_FAILE D	Error updating recipient validation data: $why	「why」: エラー メッセージ。
	クリティカル。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 15-8　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	
	情報。Cisco IronPort 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。
	情報。Cisco IronPort 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。	

アップデータ アラート

表 15-9 に、AsyncOS で生成される可能性があるさまざまなアップデータ アラートのリストを示します。

表 15-9　発生する可能性があるアップデータ 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
UPDATER.APP.UPDATE_ABANDONED	$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**」: アプリケーション名。 「**attempts**」: 試行した回数。
	警告。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。
	警告。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。 「**notification_subject**」: 通知するテキスト。
	警告。リリースの通知です。	
UPDATER.UPDATERD.UPDATE_FAILED	Unknown error occured: $traceback	「**traceback**」: トレースバック。
	クリティカル。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 15-10 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 15-10　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 IronPort Outbreak Filters Rule Update Alert:$text All rules last updated at: $time on $date.	「**text**」: アップデート アラートのテキスト。 「**time**」: 最終アップデートの時刻。 「**date**」: 最終アップデートの日付。
	情報。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	「**engine**」: アップデートに失敗したエンジン。 「**error**」: 発生したエラー。
	警告。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 15-10 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 15-11　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 - whyerror:=Machine does not appear to be in the cluster	「**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）。 「**ip**」: リモート ホストの IP。 「**why**」: エラーに関する詳細なテキスト。
	クリティカル。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 15-11　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 - whyerror:=Existing connection dropped 警告。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。	「**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）。 「**ip**」: リモート ホストの IP。 「**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 - whyerror:=Connection failure 警告。クラスタへの接続に失敗した場合に送信されます。	「**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）。 「**ip**」: リモート ホストの IP。 「**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 - whyerror:=Message forward failed, no upstream connection クリティカル。アプライアンス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。	「**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）。 「**ip**」: リモート ホストの IP。 「**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 - whyerror:=No route found クリティカル。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。	「**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）。 「**ip**」: リモート ホストの IP。 「**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 - whyerror:=Invalid host key クリティカル。無効な SSH ホスト キーがあった場合に送信されます。	「**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）。 「**ip**」: リモート ホストの IP。 「**why**」: エラーに関する詳細なテキスト。

表 15-11　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 - whyerror:=Operation timed out	「**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）。 「**ip**」: リモート ホストの IP。 「**why**」: エラーに関する詳細なテキスト。
	警告。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	「**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）。 「**why**」: エラーに関する詳細なテキスト。
	クリティカル。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 - whyerror:=Machine does not appear to be in the cluster	「**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）。 「**why**」: エラーに関する詳細なテキスト。
	クリティカル。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 - whyerror:=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）。 「**why**」: エラーに関する詳細なテキスト。
	警告。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 - whyerror:=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）。 「**why**」: エラーに関する詳細なテキスト。
	警告。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 15-11　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 - whyerror:=Message forward failed, no upstream connection クリティカル。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。	「**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）。 「**why**」：エラーに関する詳細なテキスト。
CLUSTER.CC_ERROR_ NOIP.NOROUTE	Error connecting to cluster machine $name - $error - whyerror:=No route found クリティカル。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。	「**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）。 「**why**」：エラーに関する詳細なテキスト。
CLUSTER.CC_ERROR_ NOIP.SSH_KEY	Error connecting to cluster machine $name - $error - whyerror:=Invalid host key クリティカル。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。	「**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）。 「**why**」：エラーに関する詳細なテキスト。
CLUSTER.CC_ERROR_ NOIP.TIMEOUT	Error connecting to cluster machine $name - $error - whyerror:=Operation timed out 警告。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。	「**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）。 「**why**」：エラーに関する詳細なテキスト。
CLUSTER.SYNC.PUSH_ALERT	Overwriting $sections on machine $name クリティカル。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。	「**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）。 「**sections**」：送信中のクラスタ セクションのリスト。

ネットワーク設定値の変更

この項では、Cisco IronPort 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（3-14 ページ）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 IronPort 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 IronPort 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 IronPort 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」を設定する場合は、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 15-12　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 IronPort 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 IronPort 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。結果が一致しないか、A レコードが存在しない場合ログ ファイルには、一致する受信者がドロ、システムはホスト アクセス テーブル（HAT）内のエントリと一致する IP アドレスのみを使用します）。この特別なタイムアウト時間はこのルックアップにのみ適用され、複数エントリとプライオリティ（15-40 ページ）で説明されている一般的な DNS タイムアウトには適用されません。

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無効にできます。

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、まれにメッセージ「DNS キャッシュのブートストラップに失敗しました（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

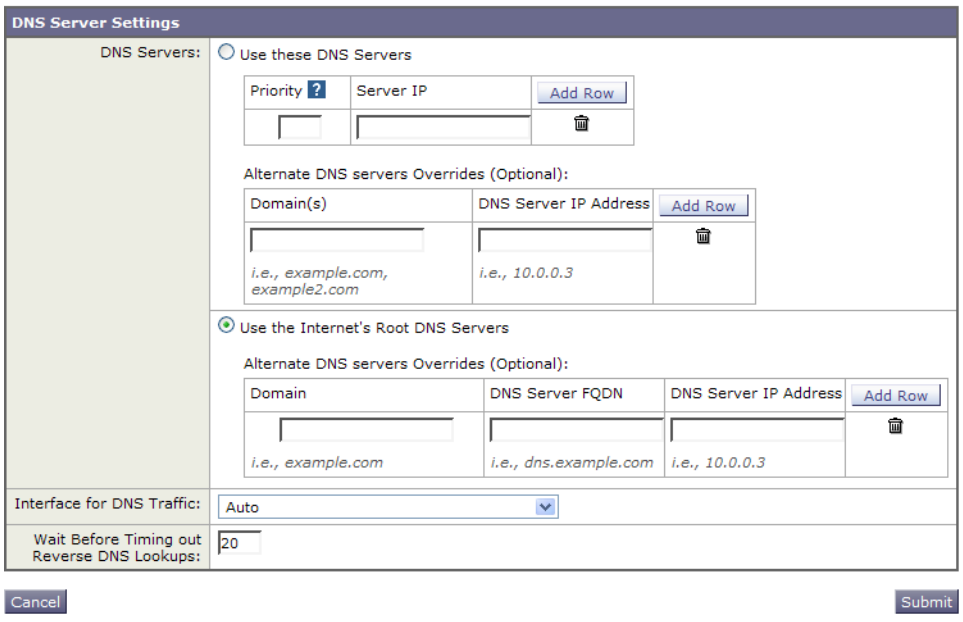
GUI の [キャッシュをクリア（Clear Cache）] ボタン、または dnsflush コマンドを使用して、DNS キャッシュのすべての情報をクリアします（dnsflush コマンドの詳細については、『*Cisco IronPort AsyncOS CLI Reference Guide*』を参照してください）。ローカル DNS システムが変更された際に、この機能を使用できます。コマンドはすぐに実行され、キャッシュの再投入中に一時的に性能が低下する可能性があります。

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

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

ステップ 2　[設定の編集（Edit Settings）] をクリックします。[Edit DNS] ページが表示されます。

図 15-11　[Edit DNS] ページ



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（15-40 ページ）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　変更を送信し、保存します。

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。

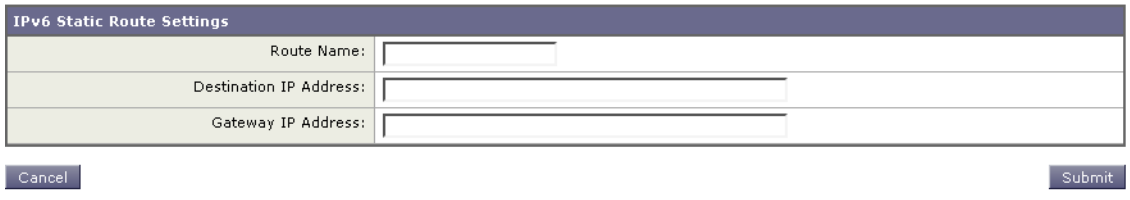
スタティック ルートの管理（GUI）

[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

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。次の図に、IPv6 スタティック ルートの設定を示します。

図 15-12　スタティック ルートの追加



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　変更を送信し、保存します。

スタティック ルートの削除

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認します。

ステップ 3　変更を保存します。

スタティック ルートの編集

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。[Edit Static Route] ページが表示されます。

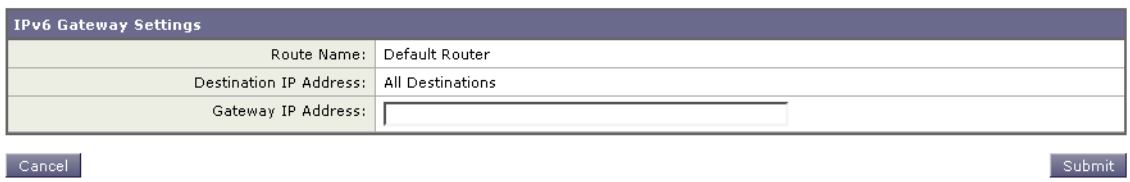
ステップ 2　ルートの設定を変更します。

ステップ 3　変更を保存します。

デフォルト ゲートウェイの変更

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。[デフォルトルートの編集（Edit Default Route）] ページが表示されます。次の図に、IPv6 デフォルト ゲートウェイの [デフォルトルートの編集（Edit Default Route）] ページを示します。

図 15-13　デフォルト ゲートウェイの編集



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　変更を送信し、保存します。

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（15-44 ページ）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。

admin ユーザのパスワードの変更

admin ユーザのパスワードは GUI または CLI から変更できます。

パスワードを GUI から変更するには、[System Administration] タブから利用可能な [Users] ページを使用します。詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Common Administrative Tasks」にあるユーザ管理に関する項を参照してください。

`admin` ユーザのパスワードを CLI から変更するには、`password` コマンドを使用します。パスワードは 6 文字以上である必要があります。`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、`commit` コマンドの実行は不要です。

電子メール セキュリティ アプライアンスの設定

AsyncOS では E 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、E 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）

E 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のアクセスは拒否されます。

プロキシ経由の接続

リモート ユーザのマシンと E 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 Email Security Appliance 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 RFC 非準拠の HTTP ヘッダーであり、次の形式になります。

```
x-forwarded-for: client-ip, proxy1, proxy2,... CRLF.
```

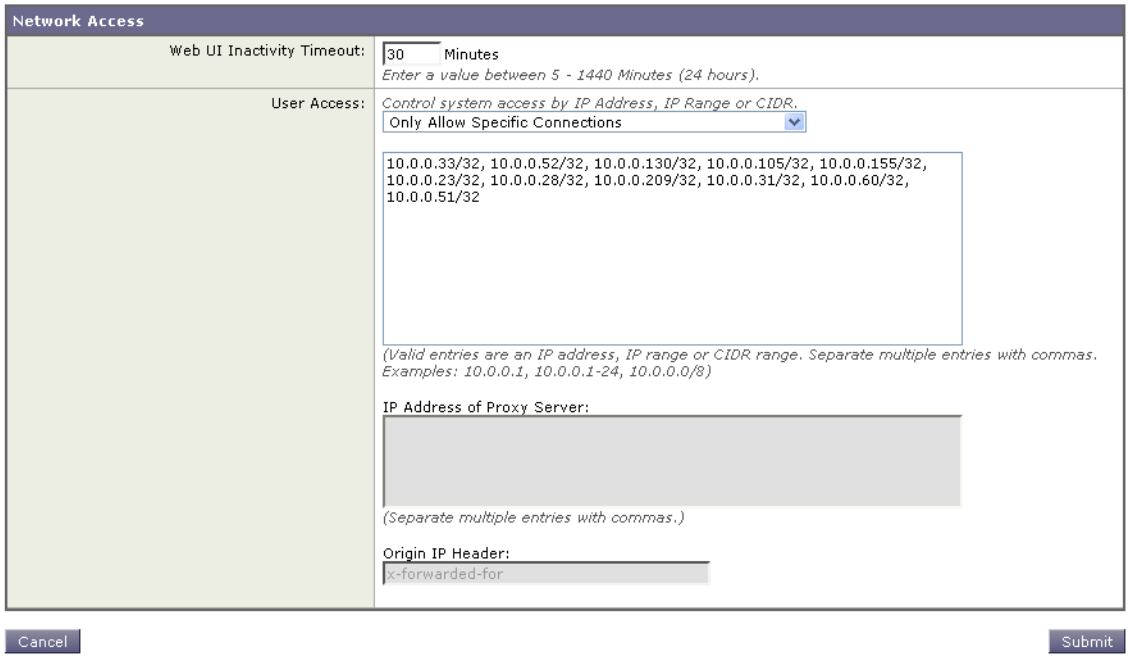
このヘッダーの値はカンマ区切りの IP アドレスのリストです。左端のアドレスがリモート ユーザ マシンのアドレスで、その後に、接続要求を転送した一連の各プロキシのアドレスが続きます（ヘッダー名は設定可能です）。E メール セキュリティ アプライアンスは、ヘッダーのリモート ユーザの IP アドレスおよび接続プロキシの IP アドレスを、アクセス リストで許可されたユーザ IP アドレスやプロキシ IP アドレスと照合します。

（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。図 15-14 は、電子メール セキュリティ アプライアンスへの直接接続が許可されているユーザ IP アドレスのリストが表示された [Network Access] ページを示しています。

図 15-14　[ネットワーク アクセス設定（Network Access Settings）]



AsyncOS はアクセス リストの制御で 4 種類のモードを用意しています。

- [すべて許可（Allow All）]。このモードはアプライアンスへの接続をすべて許可します。これが操作のデフォルト 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。

- [特定のプロキシ経由接続のみを許可（Only Allow Specific Connections Through Proxy）]。このモードは、次の条件を満たせば、逆プロキシ経由で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、アクセス リストの [プロキシサーバの IP アドレス（IP Address of Proxy Server）] フィールドに含まれている。
  - プロキシの接続要求に `x-forwarded-header` HTTP ヘッダーが記載されている。
  - `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 リスト内のユーザに対して定義された IP アドレス、IP 範囲、または CIDR 範囲と一致する。
- [特定の直接接続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、アクセス リストに含まれる IP アドレス、IP 範囲、CIDR 範囲のいずれかにユーザの IP アドレスが一致すれば、アプライアンスへの逆プロキシ経由接続または直接接続を許可します。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。
- [特定の直接接続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。

ステップ 1　[System Administration] > [Network Access] ページを使用します。

ステップ 2　[設定の編集（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　アプライアンスへの接続を許可するユーザの 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。複数のエントリを指定する場合は、カンマで区切ります。

ステップ 5　プロキシ経由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を許可するプロキシの IP アドレス。複数のエントリを指定する場合は、カンマで区切ります。
- 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。デフォルトのヘッダー名は `x-forwarded-for` です。

ステップ 6　変更を送信し、保存します。

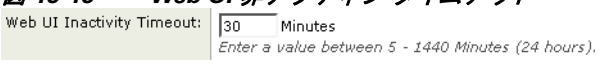
Web UI セッション タイムアウトの設定

非アクティブな状態によりログアウトになるまで、E 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 IronPort スパム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。

図 15-15　Web UI 非アクティブ タイムアウト



ステップ 1　[System Administration] > [Network Access] ページを使用します。

ステップ 2　[設定の編集（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　変更を送信し、保存します。

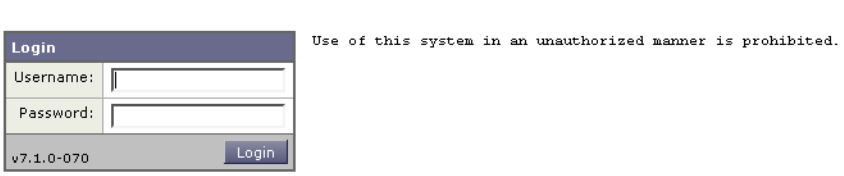
ログイン バナーの追加

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 E 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 15-16 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 15-16　バナーが表示された Web UI ログイン画面



システム時刻

Cisco IronPort 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 インターフェイスの選択を行うには、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 [時間の設定（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。

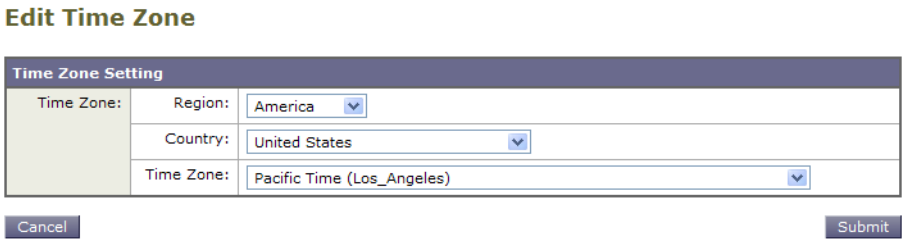
AsyncOS で使用される時間帯ファイルは、[システム管理（System Administration）] > [時間の設定（Time Settings）] ページ、または `tzupdate` CLI コマンドで確認することもできます。

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 IronPort 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。

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。[Edit Time Zone] ページが表示されます。

図 15-17　[Time Zone] ページ



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。

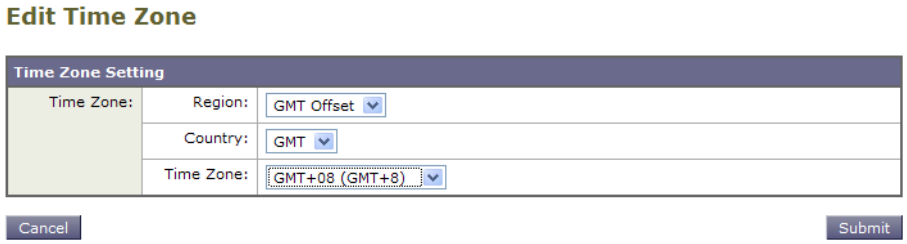
ステップ 3　変更を送信し、保存します。

GMT オフセットの選択

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。[Edit Time Zone] ページが表示されます。

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。[Time Zone Setting] ページが更新されます。

図 15-18　[Time Zone] ページ



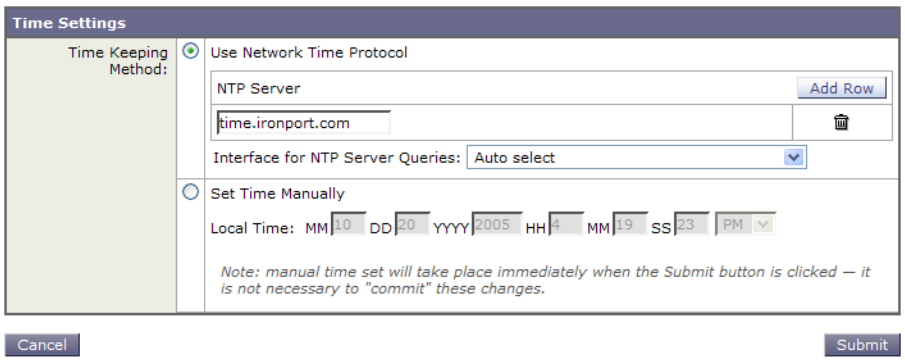
ステップ 3　[タイム ゾーン（Time Zone）] リストでオフセットを選択します。オフセットは、GMT（グリニッジ子午線）に達するために足し引きする必要がある時間を示しています。時間の前にマイナス記号（「-」）が付いている場合、グリニッジ子午線の東側にあたります。プラス記号（「+」）の場合、グリニッジ子午線の西側にあたります。

ステップ 4　変更を送信し、保存します。

時刻設定の編集

Cisco IronPort アプライアンスの時刻設定を編集するには、[システム管理（System Administration）] > [時間の設定（Time Settings）] ページの [設定を編集（Edit Settings）] ボタンをクリックします。[Edit Time Settings] ページが表示されます。

図 15-19　[Edit Time Settings] ページ



ネットワーク タイム プロトコル（NTP）設定の編集（Time Keeping Method）

ステップ 1　[システム管理（System Administration）] > [時間の設定（Time Settings）] ページで、[設定を編集（Edit Settings）] をクリックします。[Edit Time Settings] ページが表示されます。

ステップ 2　[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 3　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 4　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 5　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 6　変更を送信し、保存します。

システム時刻の設定（NTP サーバを使用しない方法）

ステップ 1　[システム管理（System Administration）] > [時間の設定（Time Settings）] ページで、[設定を編集（Edit Settings）] をクリックします。[Edit Time Settings] ページが表示されます。

ステップ 2　[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 3　月、日、年、時、分、および秒を入力します。

ステップ 4　[A.M.] または [P.M.] を選択します。

ステップ 5　変更を送信し、保存します。

CHAPTER 16

C350D アプライアンスのイネーブル化

C350D/C360D/C370D アプライアンスは、アウトバウンド電子メール配信を専用とした、Cisco IronPort アプライアンスの特殊なモデルです。この章では、C350D アプライアンスに固有な AsyncOS オペレーティング システムのさまざまな機能および変更点について説明します。この章では、C350D、C360D、および C370D アプライアンスは同じアプライアンスを意味します。この章の以降の箇所では、C350D だけが示されていますが、説明されている情報はすべて、C370D および C360D アプライアンスにも適用されます。

概要：C350D アプライアンス

C350D アプライアンスは、メールのアウトバウンド配信用に設計および最適化された AsyncOS 変更のライセンス キーがある、C350/360/370 アプライアンスです。C350D アプライアンスでは、アウトバウンド カスタマー メッセージングの特定のニーズを満たすように、パフォーマンスが劇的に改善されます。

C350D の追加機能

メッセージ配信を最適化するため、C350D アプライアンスには、標準の Cisco IronPort アプライアンスにはない追加機能がいくつかあります。

追加機能

- 256 の仮想ゲートウェイ アドレス：Cisco IronPort 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。詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Customizing Listeners」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）（16-4 ページ）を参照してください。

- リソースを節約するバウンス設定：C350D アプライアンスでは、ブロックされる可能性がある宛先を検出して、そ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。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（16-4 ページ）を参照してください。
- ソフトウェアに基づいたパフォーマンス拡張：C350D アプライアンスには、アウトバウンド配信パフォーマンスを大幅に拡張するソフトウェア モジュールが含まれています。

C350D でディセーブルにされる機能

C350D アプライアンスでは、AsyncOS オペレーティング システムの一部が変更されています。アウトバウンド電子メール配信やシステム パフォーマンスの改善に適さない、標準 C および X-Series アプライアンスのいくつかの機能は、ディセーブルにされています。次に、これらの変更点と相違点について説明します。

適していない機能

- Cisco IronPort Anti-Spam スキャンおよびオン/オフボックス スパム隔離：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、Cisco IronPort Anti-Spam スキャン エンジンではディセーブルにされています。そのため、第 9 章は適用されません。
- アウトブレイク フィルタ：Cisco IronPort のアウトブレイク フィルタ機能は、着信メールの隔離に使用されるため、この機能は C350D ではディセーブルにされています。そのため、第 11 章は適用されません。
- 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、この機能は、C350D アプライアンスではディセーブルにされています。そのため、第 8 章および第 12 章は適用されません。
- レポーティング：レポーティング機能は限定されます。一部のレポートは使用できません。発生するレポーティングも、パフォーマンス問題のため、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。
- RSA Data Loss Prevention：発信メッセージの RSA DLP スキャンは、C350D アプライアンスでディセーブルにされています。
- これらの機能が C350D アプライアンスでディセーブルにされている場合であっても、350D 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、スパムおよび疑わしいスパムの数が誤って含まれることがあります。

C350D に適用される AsyncOS 機能

C350D アプライアンスには、最新の AsyncOS 機能のほとんどが含まれています。これらの機能の多くは、C350D ユーザにとって魅力的な機能です。表 16-1 に、これらの機能の一部を示します。

表 16-1　C350D アプライアンスに含まれる AsyncOS 機能

機能	詳細情報
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。『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Email Authentication」の章を参照してください。
集中管理	『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Centralized Management」の章を参照してください。

表 16-1　C350D アプライアンスに含まれる AsyncOS 機能（続き）

機能	詳細情報
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、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Delivery Features」の章の「Controlling Email Delivery」の項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 IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Delivery Features」の章にある「Cisco IronPort Bounce Verification」の項を参照してください。
委任管理	ユーザの追加については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Common Administrative Tasks」の章を参照してください。
トレース（デバッグ）	Debugging Mail Flow Using Test Messages: Trace（-446 ページ）を参照してください。
VLAN、NIC ペアリング	『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Advanced Network Configuration」の章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（8-1 ページ）を参照してください。

C350D アプライアンスの設定

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。*システム セットアップ ウィザードを実行する前*（アプライアンスを設定する前）に、このキーを C350D Cisco IronPort E 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。

Cisco IronPort C350D アプライアンスには、アンチスパム スキャンまたはアウトブレイク フィルタ機能が含まれてい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）　クラスタ化された環境では、C350D アプライアンスを、配信パフォーマンス パッケージでは設定されない 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

C350D アプライアンスが設定されていると、潜在的な配信問題を検出して、宛先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）

（注）　IronPort Mail Merge は、IronPort C350D アプライアンスだけで使用できます。

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）。

利点

Cisco IronPort C350D アプライアンスの Mail Merge 機能を使用すると、次のような多くの利点があります。

- 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 Cisco IronPort C350D 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 IronPort 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、C350D 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。Cisco IronPort C350D 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、Cisco IronPort C350D E 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、Cisco IronPort C350D 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。

リスナーの設定の詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Customizing Listeners」の章を参照してください。`listenerconfig` の `setipmm` サブコマンドを使用して、インジェクタで IPMM をイネーブルにします。

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（.）文字で終端します。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（;）で終端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 16-2　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、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Email Authentication」の章を参照してください。

たとえば、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。

メッセージの例 1

```
From: Mr.Spacely <spacely@sprockets.com>

To: &first_name;&last_name;&*TO;

Subject: Thanks for Being a Spacely Sprockets Customer



Dear &first_name;,



Thank you for purchasing a &color; sprocket.
```

このメッセージは、Cisco IronPort C350D 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 XPRT 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 番めのパーツには、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@sprockets.com>

To: &first_name; &last_name; &*TO;

Subject: Thanks for Being a Spacely Sprockets 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、Cisco IronPort C350D 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。次に例を示します。

```
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。Cisco IronPort C350D 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ことがあります。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 `&trade;` 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「`&trade;`」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、Cisco IronPort C350D 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 ESMTP

EHLO foo

250-ehlo responses from the injector 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@example.com>

250 recipient <jane@example.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.]

RCPT TO:<joe@example.com>

250 recipient <joe@example.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@sprockets.com>

To: &first_name; &last_name; &*TO;

Subject: Thanks for Being a Spacely Sprockets 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@sprockets.com>

To: Jane User <jane@example.com>

Subject: Thanks for Being a Spacely Sprockets 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@sprockets.com>

To: Joe User <joe@example.com>

Subject: Thanks for Being a Spacely Sprockets Customer
```

```
message date

Dear Joe,



Thank you for purchasing a black sprocket.
```

コード例

Cisco IronPort 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 IronPort 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 IronPort 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。

CHAPTER 17

Cisco IronPort M-Series セキュリティ管理アプライアンス

Cisco IronPort M-Series アプライアンスは、Cisco IronPort アプライアンスの特別なモデルで、特に他の Cisco IronPort アプライアンスで使用するための外部または「オフボックス」のスパム隔離として機能するように設計されています。この章では、Cisco IronPort M-Series アプライアンスのネットワーク プランニング、システム セットアップ、および一般的な用途を説明します。

概要

Cisco IronPort M-Series セキュリティ管理アプライアンスを使用すると、Cisco IronPort E メール セキュリティ アプライアンスの機能を補完できます。Cisco IronPort M-Series セキュリティ管理アプライアンスは、企業ポリシーの設定および監査情報をモニタするための外部または「オフボックス」ロケーションとして機能するように設計されています。ハードウェア、オペレーティング システム（AsyncOS）、および補助サービスを組み合わせて重要なポリシーと実行時データの集中化と統合を行うことにより、Cisco IronPort C-Series と X-Series の E メール セキュリティ アプライアンスで使用するレポート情報および監査情報を管理者およびエンドユーザが管理するための単一インターフェイスになります。Cisco IronPort M-Series アプライアンスは、展開の柔軟性を高めることで、Cisco IronPort E メール セキュリティ アプライアンスから最上のパフォーマンスを確保し、企業ネットワークの整合性を保護します。1 台の Cisco IronPort M-Series アプライアンスからのセキュリティ操作を調整することも、複数のアプライアンス間に負荷を分散させることもできます。

セキュリティ管理アプライアンスの AsyncOS には次の機能が含まれています。

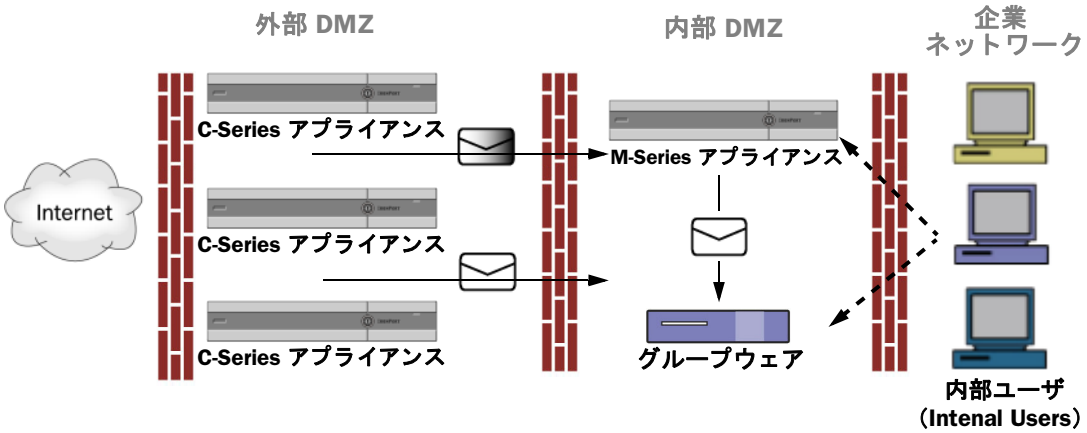
- 外部 Cisco IronPort スパム隔離。エンドユーザ向けのスパム メッセージおよび陽性と疑わしいスパム メッセージを保持しており、エンドユーザおよび管理者は、スパムとフラグ付けされたメッセージをレビューしてから最終的な決定を下すことができます。
- 中央集中型レポーティング。複数の E メール セキュリティ アプライアンスからの集計データに関するレポートを実行します。
- 中央集中型トラッキング。複数の E メール セキュリティ アプライアンスを通過する電子メール メッセージを追跡します。

Cisco IronPort セキュリティ管理アプライアンスの設定および使用については、『*Cisco IronPort AsyncOS for Security Management User Guide*』を参照してください。

ネットワーク プランニング

Cisco IronPort M-Series 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 17-1 を参照）。

図 17-1　Cisco IronPort 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 IronPort スパム検疫として機能している 1 台の Cisco IronPort M-Series アプライアンスを、1 台または複数台の Cisco IronPort 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 IronPort 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 IronPort スパム隔離を使用）。

図 17-1 に、Cisco IronPort M-Series 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。インターネットからの着信メールは外部 DMZ の Cisco IronPort 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 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。

スパムおよび陽性と疑わしいスパム（メール フロー ポリシー設定値に基づく）は、Cisco IronPort M-Series アプライアンスのスパム検疫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、スパムを削除し、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 IronPort スパム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（『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Quarantines」の章を参照）。

メール フローおよび Cisco IronPort M-Series アプライアンス

メールは、他の Cisco IronPort（C-Series および X-Series）アプライアンスからCisco IronPort M-Series アプライアンスに送信されます。Cisco IronPort M-Series 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 IronPort アプライアンスは、その M-Series 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、Cisco IronPort M-Series 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。Cisco IronPort M-Series 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。Cisco IronPort M-Series 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。

Cisco IronPort M-Series アプライアンスでは、Cisco IronPort スパム検疫設定で指定されている IP アドレスから検疫対象のメールを受け入れます。Cisco IronPort M-Series アプライアンスでローカル検疫を設定するには、『*Cisco IronPort AsyncOS for Security Management User Guide*』を参照してください。Cisco IronPort M-Series アプライアンスのローカル検疫は、M-Series アプライアンスにメールを送信する他の Cisco IronPort アプライアンスからは、*外部*の検疫と見なされることに注意してください。

Cisco IronPort M-Series アプライアンスによって解放されたメールは、スパム検疫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 IronPort 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 IronPort AsyncOS for Security Management User Guide*』を参照）。したがって、Cisco IronPort M-Series アプライアンスにメールを配信する Cisco IronPort 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 IronPort アプライアンス）に送信されます。Cisco IronPort M-Series 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。

モニタリング サービスの設定

中央集中型レポーティングまたは中央集中型トラッキングのためや、外部 Cisco IronPort スパム検疫としてセキュリティ管理アプライアンスを使用するには、まず、E メール セキュリティ アプライアンス上にモニタリング サービスを設定（構成）する必要があります。

電子メール セキュリティ アプライアンス上にモニタリング サービスを設定するときは、セキュリティ管理アプライアンス上でモニタリング サービスをイネーブルにする必要もあります。詳細については、『*Cisco IronPort AsyncOS for Security Management User Guide*』を参照してください。

モニタリング サービスを使用して、電子メール トラフィックのレポートを実行し、メッセージ ルーティングを追跡し、また疑わしいメッセージとスパム メッセージを外部 Cisco IronPort スパム検疫に配信することができます。次の 1 つまたは複数のサービスを設定できます。

- **中央集中型レポーティング。**詳細については、中央集中型レポーティングを使用するように E メール セキュリティ アプライアンスを設定する（17-3 ページ）を参照してください。
- **中央集中型トラッキング。**詳細については、中央集中型トラッキングを使用するように E メール セキュリティ アプライアンスを設定する（17-5 ページ）を参照してください。
- **Cisco IronPort スパム隔離。**詳細については、外部の Cisco IronPort スパム隔離を使用するように E メール セキュリティ アプライアンスを設定する（17-6 ページ）を参照してください。

中央集中型レポーティングを使用するように E メール セキュリティ アプライアンスを設定する

いつでも E 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ティングを設定できます。通常は、セキュリティ管理アプライアンスで機能を有効にした後で中央集中型レポーティングを設定します。

（注）　中央集中型レポーティングをイネーブルにする前に、十分なディスク領域がサービスに割り当てられていることを確認します。

ステップ 1　[Security Services] > [Reporting] をクリックします。

[レポートサービス設定（Reporting Service Settings）] ページが表示されます。

図 17-2　[Reporting Service Settings] ページ

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　変更を送信し、保存します。

（注）　中央集中型レポーティングを使用するには、E メール セキュリティ アプライアンスとセキュリティ管理アプライアンスの両方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上での中央集中型レポーティングのイネーブル化については、『*Cisco IronPort AsyncOS for Security Management User Guide*』を参照してください。

中央集中型レポーティング モード

E メール セキュリティ アプライアンスが中央集中型レポーティングを使用するように設定され、管理対象アプライアンスとしてセキュリティ管理アプライアンスに追加された後、E メール セキュリティ アプライアンスは中央集中型レポーティング モードで動作します。電子メール セキュリティ アプライアンスが中央集中型レポーティング モードになっている場合、そのアプライアンスのスケジュール済みレポートは中断され、そのアプライアンスのスケジュール済みレポートの設定ページやアーカイブされたレポートを利用できません。また、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す。E 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。中央集中型レポーティングをディセーブルにすると、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ます。

E 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ティングをディセーブルにすると、アーカイブされたレポートにアクセスできます。中央集中型レポーティングをディセーブルにした場合に、E 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。E 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ティング 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。

中央集中型トラッキングを使用するようにE メール セキュリティ アプライアンスを設定する

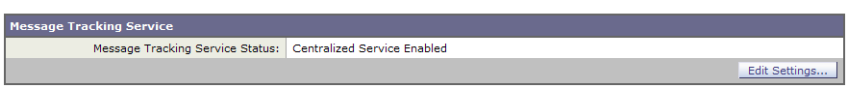
ローカル(オンボックス)トラッキングまたは中央集中型トラッキングのいずれかを使用するようにE メール セキュリティ アプライアンスを設定できます。

(注) E メール セキュリティ アプライアンスで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。

ステップ 1　[Security Services] > [Message Tracking] をクリックします。

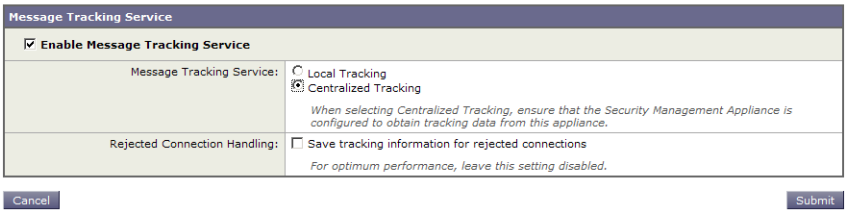
[メッセージトラッキングサービス(Message Tracking Service)] ページが表示されます。

図 17-3　[Message Tracking Service] ページ



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。

図 17-4　[Message Tracking Service Settings] ページ



ステップ 3　[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　必要に応じて、拒絶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　変更を送信し、保存します。

(注) 中央集中型トラッキングを使用するには、E メール セキュリティ アプライアンスとセキュリティ管理アプライアンスの両方で監視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上での中央集中型トラッキングのイネーブル化については、『*Cisco IronPort AsyncOS for Security Management User Guide*』を参照してください。

外部の Cisco IronPort スパム隔離を使用するように E メール セキュリティ アプライアンスを設定する

セキュリティ管理アプライアンスを Cisco IronPort スパム隔離として使用するには、E メール セキュリティ アプライアンスで外部スパム隔離機能を有効にする必要があります。また、e メール セキュリティ アプライアンスは、外部のスパム検疫への接続を使用して IP アドレスとポート番号を提供する必要があります。

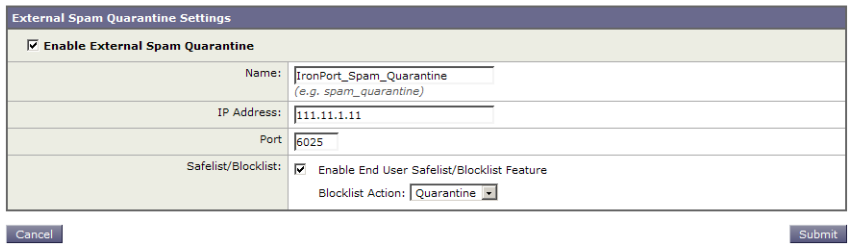
ステップ 1　[セキュリティサービス（Security Services）] > [外部スパム隔離（External Spam Quarantine）] をクリックします。

[External Spam Quarantine] ページが表示されます。

ステップ 2　[構成] をクリックします。

[Configure External Spam Quarantine] ページが表示されます。

図 17-5　[Configure External Spam Quarantine] ページ



ステップ 3　[External Spam Quarantine] セクションで、[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 アドレスとポート番号は、[Cisco IronPort スパム隔離（Cisco IronPort Spam Quarantine）] ページで設定します。

ステップ 6　任意で、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　変更を送信し、保存します。

Cisco IronPort スパム検疫およびエンドユーザ セーフリスト/ブロックリスト機能の詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Quarantines」の章を参照してください。M-Series アプライアンスで Cisco IronPort スパム検疫を使用する場合の詳細については、『*Cisco IronPort AsyncOS for Security Management 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

アプライアンスで作成する任意の IP 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。

デフォルトでは、各インターフェイスに対して次のサービスが有効または無効に設定されています。

表 A-1　IP インターフェイスに対してデフォルトで有効になるサービス

		デフォルトで有効かどうか	
サービス	**デフォルト ポート**	**管理インターフェイス**	**作成する新しい IP 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

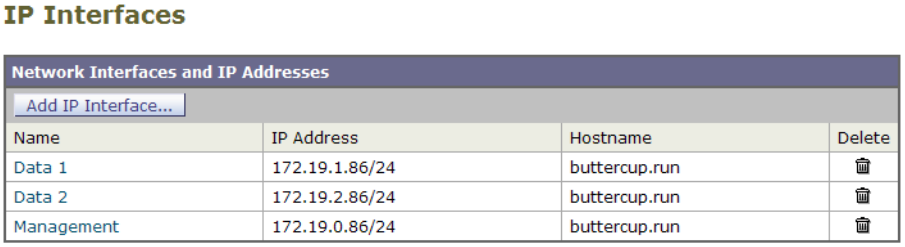
(a) ここに示す「管理インターフェイス」は、Cisco IronPort C10/100 アプライアンスの Data 1 インターフェイスのデフォルト設定でもあります。

- グラフィカル ユーザ インターフェイス(GUI)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。FTP アクセス(A-4 ページ)を参照してください。
- 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の Cisco IronPort 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の場合、各 IP インターフェイスは特定の 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 アドレスとして機能します。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を順番に使用します。仮想ゲートウェイの参加またはグループ化は、大規模な電子メール キャンペーンを複数のインターフェイス間でロード バランシングする際に役立ちます。VLAN を作成し、他のインターフェイスと同様に（CLI を介して）設定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「Advanced Networking」の章を参照してください。

図 A-1　　[IP インターフェイス（IP Interfaces）] ページ



IP インターフェイスの設定

[ネットワーク（Network）] > [IP インターフェイス（IP Interfaces）] ページ（および `interfaceconfig` コマンド）では、IP インターフェイスを追加、編集、または削除できます。

（注）　M シリーズ アプライアンス上の管理インターフェイスに関連付けられた名前またはイーサネット ポートを変更することはできません。さらに、Cisco IronPort M シリーズ アプライアンスは後述のすべての機能をサポートしているわけではありません（たとえば、仮想ゲートウェイ）。

IP インターフェイスを設定する場合は、次の情報が必要です。

表 A-2　　IP インターフェイス コンポーネント

名前	インターフェイスのニックネーム。
IPv4 アドレス/ネットマスク	同じサブネットに含まれる IPv4 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。CIDR 表記のプレフィックスとしてサブネットマスクを入力できます（たとえば、255.255.255.0 サブネットの場合は `/24`）。
IPv6 アドレス/プレフィックス	同じサブネットに含まれる IPv6 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。IPv6 アドレスは、先行ゼロを使用する必要があります（`2001:0db8:85a3::8a2e:0370:7334` など）。CIDR 表記のプレフィックスであるサブネットマスクを入力できます（例: `2001:0db8:85a3::8a2e:0370:7334/64`）

表 A-2　IP インターフェイス コンポーネント（続き）

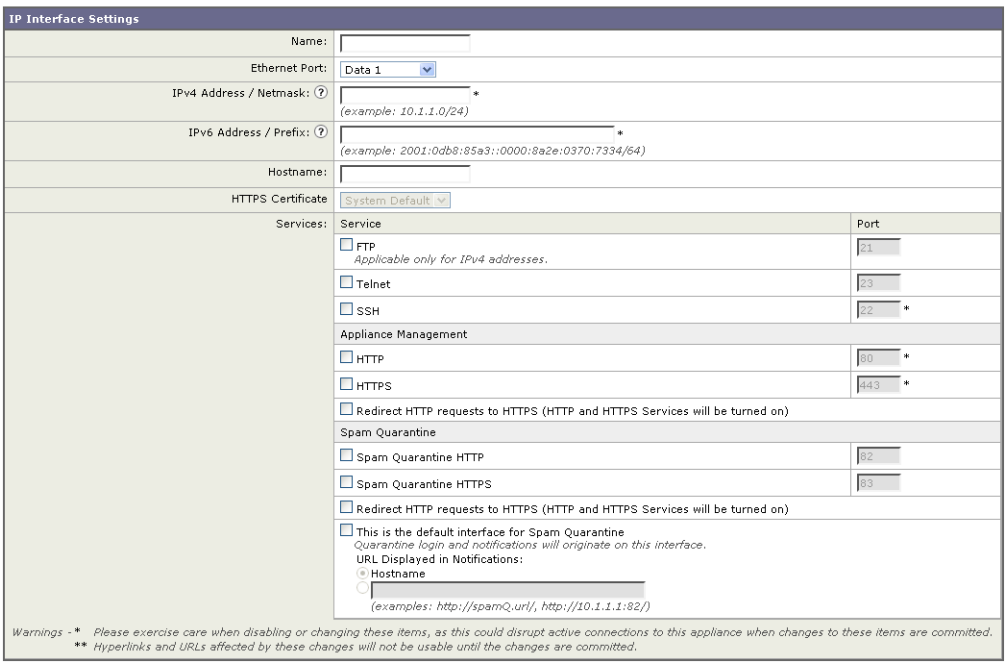
ブロードキャスト アドレス	Cisco IronPort AsyncOS はデフォルトのブロードキャスト アドレスを IP アドレスおよびネットマスクから自動的に計算します。
ホストネーム	インターフェイスに関連するホスト名。ホスト名は、SMTP カンバセーション中のサーバの特定に使用されます。各 IP アドレスに関連付けられた有効なホスト名を入力する必要があります。ソフトウェアは、DNS によってホスト名が一致する IP アドレスに正しく変換されたり、または逆引き DNS によって所定のホスト名が変換されることをチェックしません。
許可されるサービス	FTP、SSH、Telnet、Cisco IronPort スパム隔離、HTTP、および HTTPS はインターフェイス上で有効または無効にできます。サービスごとにポートを設定できます。Cisco IronPort スパム隔離の HTTP/HTTPS、ポート、および URL も設定できます。

（注） 第 3 章、セットアップおよび設置の説明に従って 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）を実行し、変更を確定していれば、アプライアンス上で 1 つまたは 2 つのインターフェイス設定が構成されているはずです。（「論理 IP インターフェイスの割り当てと設定」の項で入力した設定を参照してください）。さらに、管理インターフェイスが Cisco IronPort アプライアンスに設定されます。

GUI を使用した IP インターフェイスの作成

ステップ 1　[ネットワーク（Network）] > [IP インターフェイス（IP Interfaces）] ページ上で [IP インターフェイスの追加（Add IP Interface）] をクリックします。[Add IP Interface] ページが表示されます。

図 A-2　[IP インターフェイスの追加（Add IP Interface）] ページ



ステップ 2　インターフェイスの名前を入力します。

ステップ 3　イーサネット ポートを選択します。

ステップ 4　IP アドレスを入力します。IPv4 アドレス、IPv6 アドレス、またはその両方を入力することができます。IPv4 の場合は /24、IPv6 の場合は /64 など、CIDR 形式のプレフィックスを使用して、アドレスのサブネットマスクを入力できます。IPv4 アドレスと IPv6 アドレスの両方を入力すると、インターフェイスは各接続に適したバージョンを使用します。

ステップ 5　インターフェイスのホスト名を入力します。

ステップ 6　HTTPS サービスの TLS 証明書を選択します。

ステップ 7　この IP インターフェイスで有効にする各サービスの横にあるチェックボックスをオンにします。必要に応じて、対応するポートを変更します。

ステップ 8　アプライアンス管理用にインターフェイスで HTTP から HTTPS へのリダイレクトをイネーブルにするかどうかを選択します。

ステップ 9　Cisco IronPort スパム隔離を使用している場合は、HTTP、HTTPS、またはその両方を選択し、それぞれにポート番号を指定できます。HTTP 要求を HTTPS にリダイレクトするかどうかも選択できます。最後に、IP インターフェイスを Cisco IronPort スパム隔離のデフォルト インターフェイスにするかどうか、ホスト名を URL として使用するかどうか、およびカスタム URL を指定するかどうかを指定できます。

ステップ 10　[送信（Submit）] をクリックします。

ステップ 11　[変更を確定（Commit Changes）] ボタンをクリックし、必要に応じて任意のコメントを追加して、[変更を確定（Commit Changes）] をクリックし、IP インターフェイスの作成を終了します。

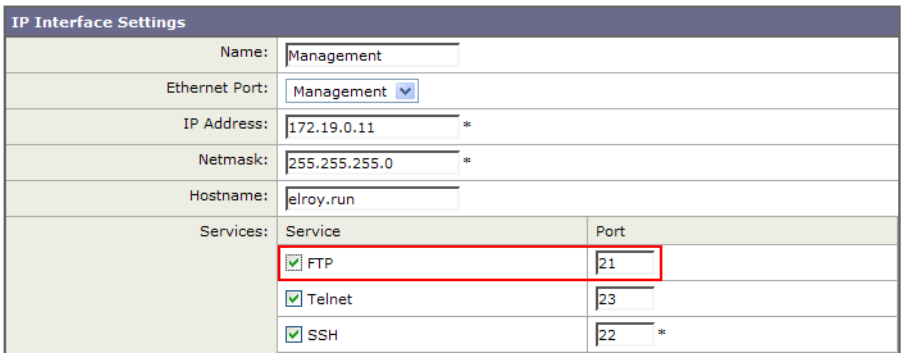
FTP アクセス

警告　**アプライアンスに接続している方法によっては、[Network] > [IP Interfaces] ページまたは interfaceconfig コマンドを使用してサービスをディセーブルにすることで、GUI または CLI から独自に切断できます。別のプロトコル、シリアル インターフェイス、または管理ポートの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。**

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。FTP を使用してアクセスするには、インターフェイスに IPv4 アドレスが必要です。

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-3　[IP インターフェイスを編集(Edit IP Interface)] ページ



(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。次に例を示します。

```
ftp 192.168.42.42
```

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。次に例を示します。

```
ftp://192.10.10.10
```

(注)　アプライアンス上の FTP サービスは、IPv6 アドレスではなく IPv4 アドレスのみを使用します。

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。表 A-2(A-5 ページ)を参照してください。

表 A-3　アクセスできるディレクトリ

ディレクトリ名	説明
/antivirus	Sophos Anti-Virus エンジンのログ ファイルが保持されるディレクトリ。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。
/avarchive **/bounces** **/cli_logs** **/delivery** **/error_logs** **/ftpd_logs** **/gui_logs** **/mail_logs** **/rptd_logs** **/sntpd.logs** **/status** **/system_logs**	[システム管理(System Administration)] > [ロギング(Logging)] ページまたは `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。各ログの詳しい説明については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Logging」の章を参照してください。 各ログ ファイル タイプ間の違いについては、「Logging」章の「Log File Type Comparison」を参照してください。

表 A-3　アクセスできるディレクトリ（続き）

ディレクトリ名	説明
/MFM	メール フロー モニタリング データベース ディレクトリには、GUI から使用できるメール フロー モニタ機能のデータが含まれます。各サブディレクトリには、各ファイルのレコード形式を文書化した README ファイルが含まれます。 記録を残すためにこれらのファイルを異なるマシンにコピーしたり、ファイルをデータベースにロードして独自の分析アプリケーションを作成したりできます。レコード形式は、すべてのディレクトリ内にあるすべてのファイルで同じです。この形式は今後のリリースで変更される場合があります。
/saved_reports	システムで設定されているすべてのアーカイブ済みレポートが保管されます。
/configuration	次のページおよびコマンドからのデータのエクスポート先ディレクトリ、またはインポート元（保存）ディレクトリ。 • 仮想ゲートウェイ マッピング（`altsrchost`） • XML 形式の設定データ（`saveconfig`、`loadconfig`） • [ホストアクセステーブル（HAT）（Host Access Table (HAT)）] ページ（`hostaccess`） • [受信者アクセステーブル（RAT）（Recipient Access Table (RAT)）] ページ（`rcptaccess`） • [SMTP ルート（SMTP Routes）] ページ（`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

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 secure copy（`scp`）コマンドをサポートしている場合は、表 A-2 に示されている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 IronPort 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、セキュア コピー（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、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Common Admistrative Tasks」でユーザを追加する方法について参照してください。

シリアル接続によるアクセス

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（3-10 ページ）を参照）、図 A-4 にシリアル ポート コネクタのピン番号を示し、表 A-4 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。

図 A-4　　シリアル ポートのピン番号

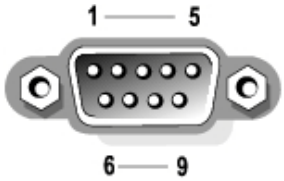


表 A-4　　シリアル ポートのピン割り当て

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	適用対象外	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	適用対象外	適用対象外	シャーシ アース

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 IronPort 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

Cisco IronPort 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。次のラベルが付いています。

- 管理
- Data1
- Data2
- Data3
- Data4

Cisco IronPort 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 IronPort 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できる必要があります。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 アドレスは、指定されたネットワーク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いずれか 1 つの IP アドレスを使用して、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、仮想ゲートウェイ 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、単純にバイナリの 1 を数える方法で表現できます。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 IronPort 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 IronPort 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:

個別のインターフェイスは別のネットワーク上に存在するように示す必要があります。

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 IronPort 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 IronPort 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 IronPort 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 IronPort 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
管理	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。

サマリー

Cisco IronPort 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 IronPort 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て使用します。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	許可	許可
異なる物理インターフェイス	不可	許可

Cisco IronPort アプライアンスの接続時の戦略

Cisco IronPort 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。
- 同じネットワーク スイッチに接続されている 2 つのイーサネット インターフェイスが、最終的に別のホスト ダウンストリーム上の単一のインターフェイスと通信する場合、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 IronPort 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

ファイアウォール情報

次の表は、Cisco IronPort 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 C-1　　ファイアウォール ポート

ポート	プロトコル	入力/出力	ホストネーム	説明
20/21	TCP	入力または出力	AsyncOS IP、FTP サーバ	ログ ファイルのアグリゲーション用 FTP。
22	TCP	入力	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	出力	SSH サーバ	ログ ファイルの SSH アグリゲーション。
22	TCP	出力	SCP サーバ	ログ サーバへの SCP 配信。
23	Telnet	入力	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	出力	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	出力	任意	電子メール送信用 SMTP。
25	TCP	入力	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。
80	HTTP	入力	AsyncOS IP	システム モニタリングのための GUI への HTTP アクセス。
80	HTTP	出力	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	出力	updates.ironport.com	AsyncOS アップグレードおよび McAfee Anti-Virus の定義。
80	HTTP	出力	cdn-microupdates.cloudmark.com	Intelligent MultiScan 機能のサードパーティ スパム 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。

表 C-1　ファイアウォール ポート（続き）

ポート	プロトコル	入力/出力	ホストネーム	説明
82	HTTP	入力	AsyncOS IP	Cisco IronPort Anti-Spam 隔離の表示に使用します。
83	HTTPS	入力	AsyncOS IP	Cisco IronPort Anti-Spam 隔離の表示に使用します。
53	UDP/TCP	入力および出力	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 クエリの場合。
110	TCP	出力	POP サーバ	Cisco IronPort スパム隔離のためのエンドユーザの POP 認証。
123	UDP	入力および出力	NTP サーバ	タイム サーバがファイアウォールの外側にある場合の NTP。
143	TCP	出力	IMAP サーバ	Cisco IronPort スパム隔離のためのエンド ユーザの IMAP 認証
161	UDP	入力	AsyncOS IP	SNMP クエリー
162	UDP	出力	管理ステーション	SNMP トラップ
389 3268	LDAP	出力	LDAP サーバ	LDAP ディレクトリ サーバがファイアウォールの外側にある場合の LDAP。Cisco IronPort スパム隔離のための LDAP 認証
636 3269	LDAPS	出力	LDAPS	LDAPS：ActiveDirectory のグローバル カタログ サーバ
443	TCP	入力	AsyncOS IP	システム モニタリングのための GUI への Secure HTTP（`https`）アクセス。
443	TCP	出力	res.cisco.com	Cisco Registered Envelope Service
443	TCP	出力	updates-static.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	出力	phonehome.senderbase.org	アウトブレイク フィルタの受信/送信
514	UDP/TCP	出力	Syslog サーバ	Syslog ロギング
628	TCP	入力	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。
2222	CCS	入力および出力	AsyncOS IP	クラスタ通信サービス（中央集中管理用）。
6025	TCP	出力	AsyncOS IP	Cisco IronPort スパム隔離

APPENDIX D

エンド ユーザ ライセンス契約書

Cisco Systems エンド ユーザ ライセンス契約書

重要:本エンド ユーザ ライセンス契約書をよくお読みください。お客様がシスコのソフトウェアまたは機器を認定販売元から購入したかどうか、また、お客様ご自身またはお客様が代表する法人(総称して「お客様」)がこのシスコ エンド ユーザ ライセンス契約におけるエンド ユーザとして登録済みかどうかを確認することは、非常に重要です。エンド ユーザとして登録されていないお客様は本ソフトウェアを使用するライセンスを有しておらず、このエンド ユーザ ライセンス契約の限定保証は適用されません。お客様が認定販売元から購入されたことを前提として、シスコのソフトウェア、またはシスコが提供するソフトウェアをダウンロード、インストールまたは使用することにより、お客様はこの契約に同意したものと見なされます。

Cisco Systems, Inc. Cisco Systems, Inc.、または同社に代わり本ソフトウェアのライセンスを許諾する同社の関連会社(以下、「シスコ」)は、お客様が本ソフトウェアを認定販売元から購入し、かつ本エンド ユーザ ライセンス契約書に含まれるすべての条件、および本製品に添付され、お客様の発注時に入手可能になる補遺ライセンス契約書に記載の、ライセンスに関する一切の追加制限条件(以下総称して「本契約」)に同意する場合に限り、お客様に対し本ソフトウェアのライセンスを許諾します。本エンド ユーザ ライセンス契約書内の各規定と補遺ライセンス契約書内の各規定が相反する場合、補遺ライセンス契約書内の各規定が優先します。本ソフトウェアをダウンロード、インストールまたは使用することにより、お客様は本ソフトウェアをご自身が認定販売元から購入したことを表明したこととなり、お客様に本契約の拘束力が及びます。お客様が本契約のすべての規定に同意しない場合、シスコは、お客様による本件ソフトウェアの使用を許諾しません。その場合、(A)お客様は、本件ソフトウェアをダウンロード、インストール、または使用できません、また、(B)お客様は、本件ソフトウェア(あらゆる未開封の CD パッケージや関連文書を含む)を返却して全額払い戻しを受けられます。または、本件ソフトウェアと関連文書が、別の製品の一部として提供されたものである場合には、当該製品全体を返却して全額払い戻しを受けられます。返却および代金払い戻しの有効期限は、認定販売元から本ソフトウェアを購入後 30 日間であり、お客様が最初の登録済みエンド ユーザ購入者である場合にのみ適用されます。本エンド ユーザ ライセンス契約において、「認定販売元」とは、(A)シスコ、(B)対象地域内でエンド ユーザにシスコの機器、ソフトウェアおよびサービスを配布および/もしくは販売することについてシスコより認定を受けたディストリビュータもしくはシステム インテグレータ、または(C)シスコの機器、ソフトウェアおよびサービスをお客様の地域内でエンド ユーザに配布および/もしくは販売することについて、ディストリビュータとシスコとの契約の条件に従い、ディストリビュータもしくはシステム インテグレータにより認定された再販業者を意味します。

本契約の以下の条件は、本ソフトウェア（後に定義）のお客様による使用に適用されます。ただし、(a)本ソフトウェアのお客様による使用に適用される、お客様とシスコとの間の別段の署名済み契約が存在する場合、または(b)本ソフトウェアに、導入もしくはダウンロードの手続きの一部として、本ソフトウェアのお客様による使用に適用される別段の「クリック同意」ライセンス契約もしくは第三者ライセンス契約が含まれている場合は、この限りではありません。上記各契約書内の各規定が矛盾する場合、その優先順位は、以下のとおりです。(1)署名済の契約、(2)クリック同意契約または第三者のライセンス契約、(3)本契約。本契約において、「本ソフトウェア」とは、認定販売元からお客様に提供されるシスコ機器に組み込まれたファームウェアおよびコンピュータ プログラムを含むコンピュータ プログラム、ならびに一切のアップグレード、更新、バグ修正またはこれらの修正バージョン（総称して「アップグレード」）であって、Cisco Software Transfer and Re-licensing Policy（随時シスコによりなされる修正を含む）に基づいて再許諾されたもの、またはこれらのいずれかのバックアップ コピーを意味します。

本件ライセンス本契約の各契約条件に従うことを条件として、シスコはお客様に対し、お客様が必要なライセンス料を認定販売元に支払った本ソフトウェアおよび本文書を社内業務目的で使用するための、非排他的かつ譲渡不能なライセンスを付与します。「本文書」とは、本ソフトウェアに関する情報を文書化したもの（当該情報がユーザ マニュアル、技術マニュアル、研修資料、仕様書その他のいずれに含まれているか否かは問わない）であって、認定販売元が何らかの形式（CD-ROM やオンラインを含む）により本ソフトウェアとともに提供するものを意味します。本ソフトウェアを使用するには、登録番号または製品認証キーを入力し、シスコの Web サイトにてお手持ちの本ソフトウェアをオンライン登録した上で、必要なライセンス キーまたはライセンス ファイルを入手する必要があります。

お客様が本ソフトウェアを使用するためのライセンスは、単一のハードウェア シャーシもしくはカード、または該当する補遺ライセンス契約書、もしくは認定販売元が同意済みで、お客様が必要なライセンス料を認定販売元に支払済みの該当する発注書（以下、「本発注書」）に記載されているその他の制限に限定され、お客様はこの制限を超えて本ソフトウェアを使用してはなりません。

本文書または該当する補遺ライセンス契約書に別途明記されていない限り、お客様は、以下のいずれかのみを目的として本ソフトウェアを使用する必要があります。お客様が所有または賃借しており、お客様の社内業務目的に使用されるシスコ機器に本ソフトウェアを組み込んで使用すること。当該シスコ機器上で本ソフトウェアを実行すること。（対応する本文書が、シスコ以外の機器に本ソフトウェアをインストールすることを許可している場合に）当該シスコ機器と通信すること。お客様には上記以外のいかなるライセンス（黙示のライセンス、禁反言の法理が適用されるライセンス、またはその他のライセンス）も付与されません。

シスコがライセンス料を徴収しない評価版またはベータ版については、上記のライセンス料の支払い要件は適用されません。

一般的な各種制限。本契約は、ソフトウェアおよび資料の使用許諾であり、所有権を譲渡するものではありません。すべてのソフトウェアおよび資料の所有権はシスコが保有しています。お客様は、本件ソフトウェアおよび本件文書に、シスコまたはそのサプライヤもしくはライセンサの営業秘密が含まれていることを認識しているものとします。この営業秘密には、各プログラムの固有の内部設計および構造ならびに関連インターフェイス情報が含まれますが、これらのみには限定されません。本契約に明示的に別段の規定がない限り、お客様は、お客様が認定販売元から購入したシスコ機器の使用に関連する場合にのみ本ソフトウェアを使用するものとし、以下のいずれについてもこれを行う権利を有しておらず、またこれを行わないことについて特に同意するものとします。

(i)他の個人もしくは法人に、ライセンス権を移転もしくは譲渡するか、本ライセンスのサブライセンスを付与すること（その時点で有効な、シスコのライセンスの再許諾および移転に関するポリシーに従って行う場合は除きます）、または、お客様が認定販売元から購入したものではないシスコ機器もしくは中古のシスコ機器上で本ソフトウェアを使用すること。なお、お客様は、計画された移転、譲渡、サブライセンスの付与または使用はいずれも無効となることを了解するものとします。

(ii)以下のいずれかを行うこと。(a)本件ソフトウェアのエラーを修正するか、本件ソフトウェアを変更または改変すること、(b)本件ソフトウェアをもとに派生物を作成するか、第三者による当該行為を許可すること。

(iii)本ソフトウェアを対象とするリバース エンジニアリング、逆コンパイル、復号化、逆アセンブルを行うか、その他の方法で本ソフトウェアを人間の可読形式に変換すること。なお、本制限事項にかかわらず、適用法に基づいて明示的に許可されている場合、または適用されるオープン ソース ライセンスに基づいて当該特定の行為を許容すべきことがシスコに義務づけられている場合は除きます。

(iv)本ソフトウェアで実行したベンチマーク テストの結果を公表すること。

(v)シスコの書面による許可なく、サービス ビューロ、タイム シェアリング、またはその他の方法により、第三者へのサービス提供を目的として本ソフトウェアを使用、または使用を許可すること。

(vi)シスコの書面による事前の同意なしに、本ソフトウェアおよび本文書に含まれる企業秘密を第三者に対して開示、提供、またはその他の何らかの方法により公開すること。お客様は、かかる営業秘密を保護するため、相当のセキュリティ対策を講じる必要があります。

シスコは、準拠法により求められている範囲内で、お客様からの書面による依頼に応じて、本ソフトウェアと独自に開発された他のプログラムとの互換性を実現するために必要なインターフェイス情報を、シスコが妥当とみなす料金が支払われた場合にお客様に提供するものとします。お客様は、上記情報について厳格な秘密保持義務を遵守すると共に、その提供条件としてシスコが提示した準拠規定に従って上記情報を使用する必要があります。

本件ソフトウェア、本件アップグレード版、および追加コピー版。本契約のその他の規定にかかわらず、以下の条件が適用されます。(1)お客様は、追加コピー版またはアップグレード版の作成または取得時に、オリジナルのソフトウェアの有効なライセンスを保有しており、アップグレードまたは追加コピー版の適用料金を認定販売元に支払っている場合を除き、かかる追加コピー版またはアップグレード版を作成または使用するライセンスまたは権利を有しません。(2)アップグレードの使用は、お客様が最初のエンド ユーザ購入者または賃借者であるか、またはアップグレードされるソフトウェアを使用するための有効なライセンスを保持しており、かつ認定販売元から供給されたシスコ機器に限定されます。(3)追加の複製物の作成および使用は、必要なバックアップ用途のみに限定されます。

所有権表示。お客様は、いかなる形式であれ、本ソフトウェアのすべての複製物について、あらゆる著作権、財産権およびその他の表示を、それらの著作権およびその他の所有権の表示が本ソフトウェアに含まれているのと同じ形式かつ方法で保持し、複製することに同意します。本契約に基づき明示的に許可される場合でなければ、お客様は、シスコから書面による事前の許可を得ることなく本件ソフトウェアのコピー版または複製物を作成してはなりません。

契約の期間および終了。本契約および本契約において供与されるライセンスは、終了時まで有効に存続します。お客様は、本件ソフトウェアおよび本件文書のすべてのコピーを破棄することにより、随時、本契約および本件ライセンスを終了させることができます。お客様が本契約のいずれかの規定に従わなかった場合、本契約に基づくお客様の権利は、シスコからの通知なしにただちに終了します。お客様は、上記終了時に、保有または管理している本件ソフトウェアおよび本件文書のすべてのコピーを破棄する必要があります。お客様のあらゆる守秘義務、「一般的な制限」と題する条項に基づいてお客様に課されたあらゆる制約および制限、あらゆる責任制限、および保証の否認と制限はすべて、本契約終了後も存続するものとします。また「米国政府がエンドユーザ購入者の場合」および「限定保証表明およびエンド ユーザ ライセンス契約書に適用される一般規定」と題された各条項の各規定の効力は、本契約の終了後も存続します。

お客様の記録の検査。お客様は、シスコとその独立会計士に対して、お客様の通常の営業時間中にお客様の帳簿、記録、財務諸表を査察し、本契約の条項に従っていることを確認する権利を認めるものとします。上記監査の結果、本契約に反する行為が発覚した場合、お客様は、相当のライセンス料に上記監査の実施に伴う相当の費用を加えた額を、速やかにシスコへ支払う必要があります。

輸出、再輸出、移転、および使用に関する規制本契約に基づいてシスコによって供給されるソフトウェア、本文書、および技術、またはそれらの直接的な製品（「本製品および技術」）は、アメリカ合衆国（「米国」）の法令およびその他関連国の法令に基づく輸出規制の対象となっています。お客様は、シスコの本件ソフトウェアと付帯技術の輸出、再輸出、移転、および使用に適用される各種法規に従う必要があると共に、必要となる米国および現地の各種許可、認可、または許諾をすべて取得するものとします。シスコとお客様の各々は、上記許認可または許諾の取得に関連して相手方当事者から相当の根拠に基づき請求を受けたその他の情報、裏付け文書、および各種支援を提供することに同意しているものとします。コンプライアンス、輸出、再輸出、移転、および使用についての法律に関する情報は、次の URL に掲載されています。

http://www.cisco.com/web/about/doing_business/legal/global_export_trade/general_export/contract_compliance.html.

米国政府機関がエンド ユーザ購入者である場合。本ソフトウェアおよび資料は、連邦調達規則（FAR）（以下「FAR」）(48 C.F.R.) 2.101 で定義される「商用品目」に分類されます。これは、「商用コンピュータ ソフトウェア」および「商用コンピュータ ソフトウェア関連資料」で構成されます（当該用語は FAR 12.212 で使用されています）。FAR 12.212 および DoD FAR 補則227.7202-1 から 227.7202-4 で定められているとおり、また、他の FAR 条項、または本契約の組み込み先である契約書内のこれと矛盾する他の契約条項にかかわらず、お客様は、連邦政府機関エンド ユーザに対して、本ソフトウェアおよび本文書とともに本契約に定める権利のみを提供することができ、または、本契約が直接契約である場合は、連邦政府機関エンド ユーザは、本ソフトウェアおよび本文書とともに本契約に定める権利のみを取得します。ソフトウェアと資料のいずれか、または両方を使用することにより、政府機関は、本ソフトウェアと資料が「商用コンピュータ ソフトウェア」および「商用コンピュータ ソフトウェア関連資料」であることに同意し、この契約書に規定されている権利および制限に同意したことになります。

指定コンポーネントおよび追加条件。本ソフトウェアは、本書に規定されたものとは異なるライセンス契約条件、保証の否認、制限付き保証または他の契約条件（総称して「追加条件」）が適用される、第三者のコンポーネントを含んでいる可能性のある単一または複数のコンポーネントであって、本文書、readme.txt_file、第三者のクリック同意またはその他（www.cisco.com 上など）においてシスコにより指定されたもの（「指定コンポーネント」）を含むこと、または指定コンポーネントと共に提供されることがあります。お客様は、かかる指定コンポーネントについて該当する追加条件に同意するものとします。

限定保証

本契約に規定の各種制限および条件を前提として、シスコは、お客様への出荷日（シスコ以外の認定販売元による再販の場合、シスコの初回出荷より 90 日以内の日）を始期として、(a) 90 日間、または (b) 本ソフトウェアを組み込んでいる製品（以下、「本製品」）に添付される保証カード（存在する場合）に明記されている、本ソフトウェアに固有の保証期間（設定されている場合）、のいずれか長い方の期間内で、(a) 通常の使用において、本ソフトウェアの提供媒体に材質上および製造上の欠陥がないこと、ならびに (b) 本ソフトウェアが本文書に実質的に適合していること、を保証します。シスコによる本件製品の出荷日は、本件製品の出荷に用いられる梱包材に記載されています。上記を除き、本ソフトウェアは「現状のまま」で提供されます。この限定保証は、最初の登録済みエンド ユーザたるお客様が認定販売元から購入した本ソフトウェアに対してのみ適用されます。この限定保証のもとでは、お客様の唯一の救済、かつシスコおよびそのサプライヤの全責任は、(i) 欠陥のある媒体の交換、および/または (ii) シスコの選択により、本ソフトウェアの修理、交換、もしくは代金の返金に限定されます。いずれの場合も、この限定保証に反するようなエラーまたは欠陥が、保証期間内に、お客様に本ソフトウェアを提供した認定販売元に報告されることを条件とします。シスコ、またはお客様に本ソフトウェアを提供した認定販売元は、救済の条件として、自らの判断で、本ソフトウェアおよび/または本文書の返却を請求できます。シスコはいかなる場合でも以下の 2 点について保証しません。(i) 本件ソフトウェアにエラーが生じないこと、(ii) お客様が、問題または障害なく本件ソフトウェアを使用できること。また、ネットワークへの侵入やネットワークの攻撃を目的とする新技術が日々開発されているため、シスコは、本件ソフトウェアまたは本件ソフトウェアが使用される各種機器、システムもしくはネットワークが、侵入または攻撃に耐えられることについても保証しません。

*制約事項。*この保証は、本件ソフトウェア、本件製品、または本件ソフトウェアの使用先として許可されているその他の機器が以下のいずれかに該当するものの場合には適用されません。(a)シスコまたはシスコ認定代理人以外によって改変されたもの、(b)シスコが提示した指示に従ってインストール、運用、メンテナンスされていないもの、(c)異常な物理的もしくは電気的負荷、異常な環境条件、誤使用、過失、事故による影響を受けたもの、(d)ベータ版、評価版、テスト版、実演版としてその使用が許諾されているもの。本ソフトウェアの保証は、以下のいずれかに該当するものには適用されません。(e)一時的に使用される本ソフトウェアの各種モジュール、(f)シスコのソフトウェア センターに掲載されていないあらゆる本ソフトウェア、(g)シスコがシスコのソフトウェア センターにて「現状のまま」で明示的に提供しているあらゆる本ソフトウェア、(h)認定販売元がライセンス料を受領していないあらゆる本ソフトウェア、および(i)認定販売元以外の第三者から供給された本ソフトウェア。

保証の放棄

保証に関する本条項に明記されているものを除き、あらゆる明示または黙示の条件、表明および保証は、適用法により許される範囲で除外され、シスコ、そのサプライヤおよびライセンサによって明示的に放棄されます。上記条件、表明および保証は、以下の(i)または(ii)を含みますが、これらに限定されません。(i)商品性、特定目的への適合性、非侵害、十分な品質、不干渉、情報内容の正確性に関する黙示の保証または条件、(ii)各種取引、法律、利用、または商慣行に起因する黙示の保証または条件。これらのいずれかが排除できない場合はその範囲において、かかる黙示の条件、表明および/または保証の存続期間は、上記の「限定保証」条項で言及されている明示的な保証期間に限定されます。州または司法管轄区域によっては、黙示保証の有効期間を限定することが許可されていないため、お客様に上記の制限が適用されない場合があります。この保証は、お客様に特定の法的権利を付与するものですが、お客様は、法域によってはその他の権利を有する場合もあります。この放棄および除外は、上記の明示保証がその本質的な目的を達成できない場合にも適用されるものとします。

*責任の否認 – 責任の制限。*本ソフトウェアの取得地が米国、ラテンアメリカ諸国、カナダ、日本またはカリブ海沿岸諸国の場合、本契約中の別段の規定にかかわらず、お客様に対するシスコ、その関連会社、役員、取締役、従業員、代理人、サプライヤおよびライセンサーの合算での全責任は、契約、不法行為(過失を含む)、保証違反またはその他の原因に基づくかを問わず、当該請求を生じさせた本ソフトウェアについてお客様が認定販売元に支払った価格、または本ソフトウェアが対象外製品の一部である場合には当該製品について支払われた価格を超えないものとします。ソフトウェアの当該責任の制限は累積的なものであり、一件毎のものではありません。(すなわち、複数の請求が行われた場合でも制限が拡大されることはありません)。

本ソフトウェアの取得地が欧州、中東、アフリカ、アジアまたはオセアニアの場合、本契約中の別段の規定にかかわらず、お客様に対するシスコ、その関連会社、役員、取締役、従業員、代理人、サプライヤおよびライセンサーの合算での全責任は、契約、不法行為(過失を含む)、保証違反またはその他の原因に基づくかを問わず、当該請求を生じさせた本ソフトウェアについてお客様がシスコに支払った価格、または本ソフトウェアが対象外製品の一部である場合には当該対象外製品について支払われた価格を超えないものとします。ソフトウェアの当該責任の制限は累積的なものであり、一件毎のものではありません。(すなわち、複数の請求が行われた場合でも制限が拡大されることはありません)。本契約のいかなる規定も、(i)シスコ、ならびにその関連会社、役員、取締役、従業員、代理人、サプライヤおよびライセンサーが、その過失に起因する身体障害または死亡に関してお客様に対して負う責任、(ii)詐欺的な不実表示に関するシスコの責任、または(iii)適用法のもとで排除できないシスコの責任を限定するものではありません。

*責任の否認 – 結果的損害および他の損失に関する免責。*本ソフトウェアの取得地が米国、ラテンアメリカ諸国、カリブ海沿岸諸国またはカナダの場合、本契約に定められている救済措置が、その本質的な目的を達成できないものであるかどうかにかかわらず、シスコまたはそのサプライヤは、いかなる場合でも、収益もしくは利益の損失、データの喪失もしくは破損、事業の中断、資本喪失、または特別、間接、結果的、偶発的もしくは懲罰的な損害について、発生原因を問わず、責任論の種類、または本ソフトウェアの使用もしくは使用不能によって発生したかどうかにかかわらず、上記損害が発生する可能性についてシスコまたはそのサプライヤもしくはライセンサーが事前に告知を受けていた場合であっても、一切責任を負いません。一部の州または法域では、結果的な損害または偶発的な損害の制限または除外が許可されていないため、上記制限がお客様に適用されない場合があります。

本ソフトウェアの取得地が日本の場合、死亡もしくは人身傷害または詐欺的な不実表示に起因または関連する責任を除き、本契約に定められている救済措置が、その本質的な目的を達成できないものであるかどうかにかかわらず、シスコ、その関連会社、役員、取締役、従業員、代理人、サプライヤおよびライセンサーは、いかなる場合でも、収益もしくは利益の損失、データの喪失もしくは破損、事業の中断、資本喪失、または特別、間接、結果的、偶発的もしくは懲罰的な損害について、発生原因を問わず、責任論の種類、または本ソフトウェアの使用もしくは使用不能によって発生したかどうかにかかわらず、上記損害が発生する可能性についてシスコもしくは認定販売元またはそれらのサプライヤもしくはライセンサーが事前に告知を受けていた場合であっても、一切責任を負いません。

本ソフトウェアの取得地が欧州、中東、アフリカ、アジアまたはオセアニアの場合、シスコ、その関連会社、役員、取締役、従業員、代理人、サプライヤおよびライセンサーは、収益もしくは利益の損失、データの喪失もしくは破損、事業の中断、資本喪失、または特別、間接、結果的、偶発的もしくは懲罰的な損害について、その発生原因（契約、不法行為（過失を含む）または本ソフトウェアの使用もしくは使用不能に起因するものを含むが、これらに限定されない）にかかわらず、それぞれの場合において、たとえ当該損害が発生する可能性についてシスコ、その関連会社、役員、取締役、従業員、代理人、サプライヤおよびライセンサーが事前に告知を受けていた場合であっても、一切責任を負いません。州または司法管轄区域によっては、結果的または偶発的な損害の制限または除外が許可されていないため、お客様に上記の制限が完全には適用されない場合があります。上記の排除は、(i) 死亡または人身傷害、(ii) 詐欺的な不実表示、または (iii) 適用法のもとで排除できない条件に関連するシスコの責任、に起因または関連する責任には適用されません。

お客様は以下の 3 点について認識および同意しているものとします。(i) シスコは、本契約内の保証の放棄および責任の制限に依拠して価格を決定し本契約を結んでいること、(ii) これは、両当事者間のリスク配分（契約上の救済措置が、その本質的な目的を達成できず、結果的に損失を被るというリスクを含む）にも反映されていること、(iii) これは、両当事者間での取引の基幹を成す事項であること。

*準拠法、管轄裁判所。*本ソフトウェアの取得地が、認定販売元により受諾された発注書上の住所の記載から判断して、米国、ラテンアメリカ諸国またはカリブ海沿岸諸国の場合、本契約および保証（「本保証」）に関する規定は、法の抵触に関する条文にかかわらず米国カリフォルニア州の各法に準拠し、同法に従って解釈されます。また、本契約または本保証に起因する各種申し立てについては、カリフォルニア州内の州裁判所および連邦裁判所が専属的に管轄します。本ソフトウェアの取得地がカナダの場合、現地法が明示的に禁止していない限り、本契約および本保証は、法の抵触に関する条文にかかわらず、カナダのオンタリオ州の各法に準拠し、同法に従って解釈されます。また、本契約または本保証に起因する各種申し立てについては、オンタリオ州内の各裁判所が専属的に管轄します。本ソフトウェアの取得地が欧州、中東、アフリカ、アジアまたはオセアニア（オーストラリアを除く）の場合、現地法が明示的に禁止していない限り、本契約および本保証は、法の抵触に関する条文にかかわらず英国の各法に準拠し、同法に従って解釈されます。本契約または本保証に起因する各種申し立てについては、英国内の各裁判所が専属的に管轄します。また、本契約が英国法に準拠する場合、本契約の当事者ではない者は、本契約のいずれの条項についても、Contracts (Rights of Third Parties) Act 1999（1999 年契約（第三者の権利）法）に基づいて権利行使を行ったり、利益を享受したりする権利を有しません。本ソフトウェアの取得地が日本の場合、現地法が明示的に禁止していない限り、本契約および本保証は、法の抵触に関

する条文にかかわらず日本国の各法に準拠し、同法に従って解釈されます。また、本契約または本保証に起因する各種申し立てについては、日本国内の東京地方裁判所が専属的に管轄します。本ソフトウェアの取得地がオーストラリアの場合、現地法が明示的に禁止していない限り、本契約および本保証に関する規定は、法の抵触に関する条文にかかわらずオーストラリア連邦ニュー サウス ウェールズ州の各法に準拠し、同法に従って解釈されます。また、本契約または本保証に起因する各種申し立てについては、ニュー サウス ウェールズ州内の州裁判所および連邦裁判所が専属的に管轄します。本ソフトウェアの取得地がその他の国の場合、現地法が明示的に禁止していない限り、本契約および本保証に関する規定は、法の抵触に関する条文にかかわらず米国カリフォルニア州の各法に準拠し、同法に従って解釈されます。また、本契約または本保証に起因する各種申し立てについては、カリフォルニア州内の州裁判所および連邦裁判所が専属的に管轄します。

上記のすべての国について、両当事者は、国際物品売買契約に関する国際連合条約の規定の適用を明示的に否定します。上記にかかわらず、いずれの当事者も、当事者の知的所有権または所有権の侵害の申し立てに対して、適切な司法管轄区域の裁判所において暫定的な差し止めによる救済を求めることができます。本契約のいずれかの規定が無効または施行不能なものとなった場合でも、本契約の残りの規定および本件保証書は有効に存続します。本契約内に別段の明示規定がない限り、本契約は、本件ソフトウェアおよび本件文書の使用許諾に関する両当事者の合意事項をまとめた唯一の文書となり、本件注文書またはその他の文書内の抵触規定または追加規定に優先し、これらの規定はすべて除外されます。本契約書は英語で記述されており、両当事者は、英語版が優先することに同意しているものとします。

製品保証条件およびシスコ製品に適用されるその他の情報は、次の URL に掲載されています。

http://www.cisco.com/go/warranty

Cisco コンテンツ セキュリティ ソフトウェア用エンド ユーザ ライセンス契約補則

重要（よくお読みください）

本エンド ユーザ ライセンス契約補則（以下「SEULA」）には、お客様とシスコとの間のエンド ユーザ ライセンス契約（以下「EULA」）に基づいてライセンスされているソフトウェア製品に対する追加条項（以下、総称して「契約」）が記載されています。この SEULA 内で定義されずに使用されている大文字の用語は、EULA で定義されたとおりの意味となります。この SEULA と EULA の条項に不一致がある場合は、この SEULA の条項が優先して適用されます。

お客様は、EULA により定められたお客様による本ソフトウェアへのアクセスおよび使用における制限事項の他に、本 SEULA に記載されている条項に同意したものと見なされます。

本ソフトウェアのダウンロード、インストール、または本ソフトウェアを内蔵する機器の使用により、お客様およびお客様が代表する企業体は本契約に法的に拘束されます。お客様が本契約のすべての規定に同意しない場合、シスコは、お客様による本件ソフトウェアの使用を許諾しません。その場合、（A）お客様は、本件ソフトウェアをダウンロード、インストール、または使用できません、また、（B）お客様は、本件ソフトウェア（あらゆる未開封の CD パッケージや関連文書を含む）を返却して全額払い戻しを受けられます。または、本件ソフトウェアと関連文書が、別の製品の一部として提供されたものである場合には、当該製品全体を返却して全額払い戻しを受けられます。返却および払い戻しに関するお客様の権利は、シスコまたはシスコ認定リセラーからの購入後 30 日で失効し、お客様が最初のエンド ユーザ購入者である場合にのみ適用されます。

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（Data loss prevention）。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 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 AyncOS 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。

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。

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）の形をとることもあります。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（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 の略。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す。

M

MAIL FROM[MAILFROM]

*エンベロープ送信者*を参照してください。

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。メール ユーザ エージェントまたは他の MTA からのメッセージの受信時に、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もあります。Cisco IronPort 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 Network Time Protocol（ネットワーク タイム プロトコル）。`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

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。

STARTTLS Transport Layer Security（TLS）はセキュア ソケット レイヤ（SSL）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 カンバ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 拡張をサポートしています。

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 メッセージを検疫し、更新されたウイルス IDE が使用可能になるまで、または脅威なしと判断されるまでの間、そのメッセージを保持します。

アンチウイルス（Anti-Virus）

Sophos および McAfee のウイルス対策スキャン エンジンは、プラットフォーム間のウイルス対策保護、検出、および保護を提供します。ウイルス検出エンジンは、ファイルをスキャンし、ウイルス、トロイの木馬、ワームを検出します。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。

え

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。

お

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、意図せず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。たとえば、`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。

き

キュー（Queue）
Cisco IronPort アプライアンスでは、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、*配信*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、*ワーク 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、*配信用* 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 IronPort 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。

け

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。

こ

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 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。

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 ルールと共に、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。

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。

し

受領（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 IronPort 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。

そ

送信者グループ 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。

ち

遅延バウンス（Delayed Bounce） SMTP カンバ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。

て

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 カンバ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 IronPort 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 IronPort 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ごとの 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 IronPort プライアンスが実行する配信設定を調整できます。

ひ

非カンバ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）。

ふ

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。

ほ

ホワイトリスト

既知の適切な送信者のリストです。信頼する送信者は、*送信者グループ* ホワイトリストに追加します。$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。

め

メール フロー ポリシー

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 IronPort 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。

も

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。

り

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 IronPort 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。

れ

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 評価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*スパム*の疑いがあるものを拒否またはスロットリングすることができます。

ろ

ログ サブスクリプション（Log Subscription）

Cisco IronPort 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

シンボル

数値

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

X

あ

い

う

え

お

か

き

く

け

こ

さ

し

す

せ

そ

た

ち

つ

て

と

ね

は

ひ

ふ

へ

ほ

ま

め

も

よ

り

る

れ

ろ