AsyncOS 9.2 for Cisco Web Security Appliances ユーザ ガイド

発行日:2016 年 1 月 27 日
改訂日:2019 年 3 月 27 日

Cisco Systems, Inc.
www.cisco.com

【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。

AsyncOS 9.2 for Cisco Web Security Appliances ユーザ ガイド

CONTENTS

製品およびリリースの概要

Web セキュリティ アプライアンスの概要

Cisco Web セキュリティ アプライアンスはインターネット トラフィックを代行受信してモニタし、ポリシーを適用することによって、マルウェア、機密データの漏洩、生産性の低下などのインターネット ベースの脅威から内部ネットワークを保護します。

最新情報

Cisco AsyncOS 9.2 の新機能

（注） このリリースは主に、ハイブリッド Web セキュリティを一度も設定したことがないデバイスにインストールする場合を対象にしています。ハイブリッド モードでアプライアンスを稼働する予定がない場合は、このバージョンのインストール、またはこのバージョンへのアップグレードをしないでください。

Cisco AsyncOS 9.2.0-809（GD）の新機能

これはアップグレード リリースです。新しい機能の追加はありません。

Cisco AsyncOS 9.2.0-796 の新機能

- デフォルトおよびユーザ定義の両方の CWS ポリシーから WSA ポリシーへの変換が展開されて最適化されています。変換されていない CWS ルールはごくわずかです。
- AsyncOS ソフトウェアへのアップグレードは、使用可能な場合は自動的にダウンロードされます。ダウンロードされたアップグレードは、[アップグレードとアップデートの設定（Upgrade and Update Settings）] ページで指定された時間帯にインストールされます。

Cisco AsyncOS 9.2.0-083（GD）の新機能

これはアップグレード リリースです。新しい機能の追加はありません。

Cisco AsyncOS 9.2.0-075 の新機能

ハイブリッド Web セキュリティ モードは、Cisco ScanCenter（Web セキュリティ アプライアンスに自動的にダウンロードされるクラウド Web セキュリティの管理ポータル）で定義されているポリシーを使用して、クラウドとオンプレミスが統合されたポリシー適用および脅威防御を提供します。

- 関連項目（1-2 ページ）

関連項目

- 製品リリース ノート：
  http://www.cisco.com/en/US/partner/products/ps10164/prod_release_notes_list.html

アプライアンス Web インターフェイスの使用

Web インターフェイスのブラウザ要件

Web インターフェイスにアクセスするには、ブラウザが JavaScript および Cookie をサポートし、受け入れがイネーブルになっている必要があります。また、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。

Cisco Web セキュリティ アプライアンスは YUI（http://yuilibrary.com/yui/environments/）で設定されたターゲット環境に準拠しています。

セッションは、非アクティブな状態が 30 分続くと自動的にタイムアウトします。

Web インターフェイス内の一部のボタンとリンクを使用すると、さらにウィンドウが開きます。そのため、Web インターフェイスを使用するには、ブラウザのポップアップ ブロックを設定する必要があります。

（注）　アプライアンスの設定を編集する場合は、一度に 1 つのブラウザ ウィンドウまたはタブを使用します。また、Web インターフェイスおよび CLI を同時に使用してアプライアンスを編集しないでください。複数の場所からアプライアンスを編集すると、予期しない動作が発生するので、サポートされません。

仮想アプライアンスでの Web インターフェイスへのアクセスのイネーブル化

デフォルトでは、HTTP および HTTPS インターフェイスは仮想アプライアンスで有効化されません。これらのプロトコルを有効にするには、コマンドライン インターフェイスを使用する必要があります。

ステップ 1　コマンドライン インターフェイスにアクセスします。コマンドライン インターフェイスへのアクセス（B-1 ページ）を参照してください。

ステップ 2　`interfaceconfig` コマンドを実行します。

プロンプトで Enter キーを押すと、デフォルト値が受け入れられます。

HTTP および HTTPS のプロンプトを検索し、使用するプロトコルをイネーブルにします。

アプライアンス Web インターフェイスへのアクセス

はじめる前に

仮想アプライアンスを使用している場合は、仮想アプライアンスでの Web インターフェイスへのアクセスのイネーブル化（1-3 ページ）を参照してください。

ステップ 1　ブラウザを開き、Web セキュリティ アプライアンスの IP アドレス（またはホスト名）を入力します。アプライアンスが事前に設定されていない場合は、デフォルト設定を使用します。

```
https://192.168.42.42:8443
```

または

```
http://192.168.42.42:8080
```

ここで、`192.168.42.42` はデフォルト IP アドレス、`8080` は、HTTP のデフォルトの管理ポートの設定、`8443` は HTTPS のデフォルトの管理ポートです。

アプライアンスが現在設定されている場合は、M1 ポートの IP アドレス（またはホスト名）を使用します。

（注） アプライアンスに接続するときはポート番号を使用する必要があります（デフォルトはポート 8080）。Web インターフェイスにアクセスするときにポート番号を指定しないと、デフォルト ポート 80 になり、[ライセンスなしプロキシ（Proxy Unlicensed）] エラー ページが表示されます。

ステップ 2　アプライアンスのログイン画面が表示されたら、アプライアンスにアクセスするためのユーザ名とパスフレーズを入力します。

デフォルトで、アプライアンスには以下のユーザ名とパスフレーズが付属します。

- ユーザ名：**admin**
- パスフレーズ：**ironport**

admin のユーザ名でログインするのが初めての場合は、パスフレーズをすぐに変更するよう求められます。

ステップ 3　ユーザ名による最近のアプライアンスへのアクセス試行（成功と失敗の両方）の一覧を表示するには、アプリケーション ウィンドウ右上の [次のユーザとしてログイン（Logged in as）] エントリの前にある [最近のアクティビティ（recent-activity）] アイコン（**i** または **!**）をクリックします。

Web インターフェイスでの変更の送信

（注） すべてをコミットする前に、複数の設定変更を行うことができます。

ステップ 1　[変更を確定（Commit Changes）] ボタンをクリックします。

ステップ 2　選択する場合、[コメント（Comment）] フィールドにコメントを入力します。

ステップ 3　[変更を確定（Commit Changes）] をクリックします。

Web インターフェイスでの変更内容のクリア

ステップ 1　[変更を確定（Commit Changes）] ボタンをクリックします。

ステップ 2　[変更を破棄（Abandon Changes）] をクリックします。

Cisco SensorBase ネットワーク

Cisco SensorBase ネットワークは、世界中の何百万ものドメインを追跡し、インターネット トラフィックのグローバル ウォッチ リストを維持する脅威の管理データベースです。SensorBase は、既知のインターネット ドメインの信頼性の評価をシスコに提供します。Web セキュリティ アプライアンスは、SensorBase データ フィードを使用して、Web レピュテーション スコアを向上させます。

SensorBase の利点とプライバシー

Cisco SensorBase ネットワークへの参加は、シスコがデータを収集して、SensorBase 脅威管理データベースとそのデータを共有することを意味します。このデータには要求属性に関する情報およびアプライアンスが要求を処理する方法が含まれます。

シスコはプライバシーを維持する重要性を理解しており、ユーザ名やパスフレーズなどの個人情報または機密情報も収集または使用しません。また、ファイル名とホスト名に続く URL 属性は、機密性を保証するために難読化されます。復号化された HTTPS トランザクションでは、SensorBase ネットワークは IP アドレス、Web レピュテーション スコア、および証明書内のサーバ名の URL カテゴリのみを受信します。

SensorBase ネットワークへの参加に同意する場合、アプライアンスから送信されたデータは HTTPS を使用して安全に転送されます。データを共有すると、Web ベースの脅威に対応して、悪意のあるアクティビティから企業環境を保護するシスコの機能が向上します。

Cisco SensorBase ネットワークへの参加の有効化

（注）　システムの設定時にデフォルトで [標準 SensorBase ネットワークに参加（Standard SensorBase Network Participation）] がイネーブルにされています。

ステップ 1　[セキュリティサービス（Security Services）] > [SensorBase] ページを選択します。

ステップ 2　[SensorBase ネットワークに参加（SensorBase Network Participation）] がイネーブルであることを確認します。

ディセーブルの場合、アプライアンスが収集するデータは SensorBase ネットワーク サーバには戻されません。

ステップ 3　[加入レベル（Participation Level）] セクションで、以下のレベルのいずれかを選択します。

- [制限（Limited）]。基本的な参加はサーバ名情報をまとめ、SensorBase ネットワーク サーバに MD5 ハッシュ パス セグメントを送信します。
- [標準（Standard）]。拡張された参加は、unobfuscated パス セグメントを使用した URL 全体を SensorBase ネットワーク サーバに送信します。このオプションは、より強力なデータベースの提供を支援し、継続的に Web レピュテーション スコアの整合性を向上させます。

ステップ 4　[AnyConnect ネットワークへの参加（AnyConnect Network Participation）] フィールドで、Cisco AnyConnect を使用して Web セキュリティ アプライアンスに接続するクライアントから収集された情報を含めるかどうかを選択します。

AnyConnect クライアントは、Secure Mobility 機能を使用してアプライアンスに Web トラフィックを送信します。

ステップ 5　[除外されたドメインと IP アドレス（Excluded Domains and IP Addresses）] フィールドで、任意でドメインまたは IP アドレスを入力して、SensorBase サーバに送信されたトラフィックを除外します。

ステップ 6　変更を送信し、保存します。

ハイブリッド Web セキュリティ モード

ハイブリッド Web セキュリティ モードの概要

ハイブリッド Web セキュリティ モードは、Cisco ScanCenter（Web Security Appliance に自動的にダウンロードされるクラウド Web セキュリティの管理ポータル）で定義されているポリシーを使用して、クラウドとオンプレミスが統合されたポリシー適用および脅威防御を提供します。

ハイブリッド Web セキュリティには、標準モードで提供される機能のサブセットが用意されています。これらの使用方法は、このマニュアルに記載されていることを除いて標準モードと同じです。詳細については、操作モードの比較（3-2 ページ）を参照してください。

この章は本書のさまざまな個所と関連しており、標準モードとハイブリッド Web セキュリティ モードの両方に共通する Web セキュリティ アプライアンスの主要機能の一部は、それらの個所に記載されています。この章には、標準モードでは適用できないハイブリッド Web セキュリティの設定に関する情報が記載されています。

本書には、Cisco Cloud Web Security および ScanCenter に関する情報は記載されていません。そのマニュアルについては、
http://www.cisco.com/c/en/us/support/security/cloud-web-security/tsd-products-support-series-home.html [英語] から入手してください。

クラウド Web セキュリティのポリシーアプリケーションについて

WSA ポリシーに対する CWS ポリシー/フィルタ/ルールのダウンロード、変換および適用について、次の点に注意してください。

- デフォルトおよびユーザ定義の両方の CWS ポリシーから WSA ポリシーに対するトランザクションは、一対一の変換ではありません。ただし、両方の環境で特定のポリシーを適用した場合に生じるアクションは同じです。つまり、拒否または許可の決定は、両方のケースで「実行されている」ルールの順序に関係なく常に一貫しています。そのため、プロキシでのルールの評価を最適化して、一貫性のある動作を妥協することなく、より良いパフォーマンスを実現することができます。
- サポートされるマルウェア対策スキャン サービスは、両方のプラットフォームで同じではありません。依存しない状態のままです。WSA にはスキャン サービスを選択するオプションがあり、少なくとも 1 つは有効にする必要があります。
- ハイブリッド モードで、WSA は次の項目をサポートしません。これらは、ダウンロードされません。
  - 認証アクションを割り当てるルール
  - 送信フィルタ。キーワード、送信ファイル タイプ、設定済み ID、または正規表現を含むフィルタを使用したルールです。着信内線番号もサポートされていません。
  - 一連のドメインと URL をホワイトリストに登録して、グローバル レベルでスパイウェア/Web レピュテーションのスキャンをバイパスすることはできません。
  - 匿名化。アクションが [匿名化（Anonymize）] に設定されている CWS ルールです。
  - SearchAhead
  - WSA には、委任管理の概念は含まれていません。CWS は、マージされたポリシー設定を送信します。

ハイブリッド モードで使用できない WSA 機能

次の WSA 機能は、ハイブリッド モードで使用できません。

- 時間およびボリューム クォータ
- 外部 DLP（External DLP）
- SaaS ポリシー
- L4TM
- アップストリーム プロキシのサポート
- ISE の統合
- 範囲要求
- ネイティブ FTP および SOCKS プロトコルのサポート
- SNMP
- ドロップ アクションが割り当てられた HTTPS ルール

事前設定の要件

- クラウド Web セキュリティ ポリシーとの互換性を実現するには、Web ハイブリッド モードで動作しているときに少なくとも 1 つのマルウェア対策スキャン エンジン（McAfee、Sophos、または Webroot）のライセンスを付与されていて使用可能である必要があります。Web ハイブリッド モードで設定を完了するには、有効なライセンスまたは機能キーが使用可能であることを確認します。
- CWS および WSA には、相互の通信を認証してセキュリティ保護するために、認証局の署名付き証明書が必要です。この証明書を外部で生成し、Cisco ScanCenter と Cisco WSA の両方に証明書とそのキーをアップロードする必要があります。証明書およびキーのアップロード（12-25 ページ）を参照してください。
- この Web Security Appliance を Cisco Cloud Web Security に登録して、承認トークンを取得します。このトークンの有効期限は 1 時間です。1 時間以内に WSA の設定に使用しなかった場合、別のトークンを生成する必要があります。への登録 Cisco Cloud Web Security（3-12 ページ）を参照してください。

次の作業

- ハイブリッド Web セキュリティ モードでアプライアンスの接続、インストール、および設定を行います。特定の情報については、接続、インストール、設定に関するタスクの概要（3-8 ページ）を参照してください。
- クラウド Web セキュリティのポリシーアプリケーションについて（2-2 ページ）で説明したように、ダウンロードする CWS ポリシーに HTTPS ルールまたは認証グループ ルールが含まれている場合、システム セットアップ ウィザード（SSW）でハイブリッド Web セキュリティ モードの設定を完了した直後に WSA で HTTPS プロキシ設定、認証レルム、および識別プロファイルを設定することが重要です。HTTPS ルールまたは認証グループ ルールを含んでいる CWS ポリシーの変換およびダウンロードは WSA ハイブリッド システム セットアップではスキップされ、HTTPS プロキシ、認証レルム、および識別プロファイルが設定されていて、WSA がハイブリッド モードで設定された後にのみ完了します（CWS から WSA へのポリシーの更新は 2 分ごとに行われるため、変換/ダウンロード プロセスは自動的に完了します）。

  CWS では、認証レルムは SAML および EasyID と呼ばれます。WSA ではサポートされるタイプは異なり、通常、NTLM と呼ばれます（SAML は WSA ではまだサポートされていません）。CWS のルールに認証ユーザ名または設定済みの認証グループのいずれかが含まれている場合、WSA で認証が有効になっている状態で認証レルムとカスタム識別プロファイルを設定する必要があります。

  - HTTPS プロキシ設定の構成：HTTPS プロキシのイネーブル化（7-4 ページ）を参照してください。
  - 認証レルムおよび識別プロファイルの設定：エンドユーザおよびクライアント ソフトウェアの分類（6-1 ページ）を参照してください。

- CWS の [アクセプタブル ユース ポリシー（Acceptable Use Policy）（AUP）] ページと WSA の [エンドユーザ確認応答（End-User Acknowledgment）（EUA）] ページは、基本的に同じものです。これはアクセス契約の説明が表示されるページで、クリックして確認してから続行する必要があります。

  CWS でこのオプションを使用している場合は、WSA（[セキュリティ サービス（Security Services）] > [ユーザ通知（End-User Notification）]）でローカルにこれを有効にして、すべてのエンド ユーザに必要な同一の動作を指定する必要があります。EUA の設定は CWS からはダウンロードされないため、WSA でローカルに設定する必要があります。WSA によってエンドユーザに提供された HTML を編集して、両方のページの「ルックアンドフィール」が同じになるようにします。

- Cisco ScanCenter で設定可能ないくつかの項目は、Web Security Appliance によるダウンロードではまだサポートされていません。次の項目は、アプライアンスで直接設定する必要があります。
  - 電子メール アラート設定。電子メール アラートを受信する頻度（電子メール アドレスはソフトウェア セットアップ ウィザードによる設定時に提供されます。その他は後で追加できます）。
  - ブロック ページおよびエンドユーザ アラート ページ向けにカスタマイズされたテキストおよびその他の設定。
  - SearchAhead、SafeSearch、動的分類エンジン、コンテンツ範囲ヘッダー、サンドボクシングなどのグローバル設定。
- WSA ハイブリッド ソフトウェアがインストールまたはアップグレードされるときに、AVC シグニチャのバージョンが CWS サービスのバージョンと一致しないことがあります。WSA では、不一致があるアプリケーションのルールは生成されませんが、すべての一致するシグニチャに対するルールは生成されます。適用できないシグニチャの不一致は記録されます（正しい AVC シグニチャ ファイルは、通常 10 分もしないうちにダウンロードされます）。
- ロギング：`hybridd` ログはハイブリッド モードの一部として有効になります。そのレベルはその他すべての WSA ログと同様に設定できます。ポリシーの変換時にエラーが発生した場合は、`hybridd` および `configdefragd` のログを参照します。

CHAPTER 3

接続、インストール、設定

接続、インストール、設定の概要

Web セキュリティ アプライアンスには、標準、クラウド Web セキュリティ コネクタ、ハイブリッド Web セキュリティ の 3 つの動作モードがあります。

Web セキュリティ アプライアンスの標準動作モードには、オンサイトの Web プロキシ サービス（クラウド Web セキュリティ コネクタ モードで不可）、およびレイヤ4 トラフィック モニタ（ハイブリッド Web セキュリティ、クラウド Web セキュリティ コネクタ の両モードで不可）が含まれます。

クラウド Web セキュリティ コネクタ モードでは、アプライアンスは、Web セキュリティ ポリシーが適用されている Cisco Cloud Web Security（CWS）プロキシに接続してトラフィックをルーティングします。

ハイブリッド Web セキュリティ モードは、Cisco ScanCenter（Web セキュリティ アプライアンスに自動的にダウンロードされるクラウド Web セキュリティの管理ポータル）で定義されているポリシーを使用して、クラウドとオンプレミスが統合されたポリシー適用および脅威防御を提供します。

アプライアンスには複数のポートが搭載されており、各ポートは割り当てられた 1 つ以上の特定のデータ型を管理します。

アプライアンスは、ネットワーク ルート、DNS、VLAN、およびその他の設定とサービスを使用して、ネットワーク接続とトラフィック代行受信を管理します。システム セットアップ ウィザードでは基本的なサービスと設定項目をセットアップすることができ、アプライアンスの Web インターフェイスでは、設定の変更や追加オプションの設定を行うことができます。

仮想アプライアンスの展開

仮想 Web セキュリティ アプライアンスの展開については、『*Cisco Content Security Virtual Appliance Installation Guide*』を参照してください。このドキュメントは、http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html から入手できます。

物理アプライアンスから仮想アプライアンスへの移行

物理アプライアンスから仮想アプライアンスに展開を移行するには、前のトピックで言及した『Virtual Appliance Installation Guide』、および使用している AsyncOS のバージョンに応じたリリース ノートを参照してください。

操作モードの比較

Web セキュリティ アプライアンスの標準動作モードには、オンサイトの Web プロキシ サービス（クラウド Web セキュリティ コネクタ モードで不可）、およびレイヤ4 トラフィック モニタ（ハイブリッド Web セキュリティ、クラウド Web セキュリティ コネクタ の両モードで不可）が含まれます。

クラウド Web セキュリティ コネクタ モードでは、アプライアンスは、Web セキュリティ ポリシーが適用されている Cisco Cloud Web Security プロキシに接続してトラフィックをルートします。

ハイブリッド Web セキュリティ モードは、Cisco Cloud Web Security プロキシへの接続を取り入れることでクラウドとオンプレミス両方のポリシー適用と脅威防御を提供します。

次の表では、各モードで使用可能なさまざまなメニュー コマンドを示し、それにより各モードで使用可能なさまざまな機能について説明します。

メニュー	標準モードで使用可能	クラウド コネクタ モードで使用可能	ハイブリッド Web セキュリティ モードで使用可能
レポート	システム ステータス（System Status） 概要 Users Web サイト（Web Sites） URL カテゴリ（URL Categories） アプリケーションの表示（Application Visibility） マルウェア対策（Anti-Malware） 高度なマルウェア防御（Advanced Malware Protection） ファイル分析（File Analysis） AMP 判定のアップデート（AMP Verdict Updates） クライアント マルウェア リスク（Client Malware Risk） Web レピュテーション フィルタ（Web Reputation Filters） レイヤ 4 トラフィック モニタ（Layer-4 Traffic Monitor） ユーザの場所別レポート（Reports by User Location） Web トラッキング（Web Tracking） システム容量（System Capacity） システム ステータス スケジュール設定されたレポート（Scheduled Reports） アーカイブ レポート（Archived Reports）	システム ステータス（System Status）	システム容量（System Capacity） システム ステータス（System Status）

メニュー	標準モードで使用可能	クラウド コネクタ モードで使用可能	ハイブリッド Web セキュリティ モードで使用可能
Web セキュリティ マネージャ（Web Security Manager）	識別プロファイル（Identification Profiles） クラウド ルーティング ポリシー（Cloud Routing Policies） SaaS ポリシー 復号ポリシー（Decryption Policies） ルーティング ポリシー アクセス ポリシー 全体の帯域幅の制限（Overall Bandwidth Limits） Cisco データ セキュリティ 発信マルウェアスキャン（Outbound Malware Scanning） 外部データ消失防止 SOCKS ポリシー（SOCKS Policies） カスタム URL カテゴリ 時間範囲およびクォータの定義（Define Time Ranges and Quotas） バイパス設定（Bypass Settings） レイヤ 4 トラフィック モニタ（Layer-4 Traffic Monitor）	識別プロファイル（Identification Profiles） クラウド ルーティング ポリシー（Cloud Routing Policies） 外部データ消失防止（External Data Loss Prevention） カスタム URL カテゴリ（Custom URL Categories）	識別プロファイル（Identification Profiles） バイパス設定

メニュー	標準モードで使用可能	クラウド コネクタ モードで使用可能	ハイブリッド Web セキュリティ モードで使用可能
セキュリティ サービス	Web プロキシ（Web Proxy） FTP プロキシ（FTP Proxy） HTTPS プロキシ（HTTPS Proxy） SOCKS プロキシ（SOCKS Proxy） PAC ファイル ホスティング（PAC File Hosting） 使用許可コントロール（Acceptable Use Controls） マルウェア対策とレピュテーション（Anti-Malware and Reputation） データ転送フィルタ（Data Transfer Filters） AnyConnect セキュア モビリティ（AnyConnect Secure Mobility） ユーザ通知（End-User Notification） L4 トラフィック モニタ（L4 Traffic Monitor） SensorBase レポート	Web プロキシ（Web Proxy）	Web プロキシ（Web Proxy） HTTPS プロキシ マルウェア対策とレピュテーション（Anti-Malware and Reputation） ユーザ通知（End-User Notification） SensorBase

メニュー	標準モードで使用可能	クラウド コネクタ モードで使用可能	ハイブリッド Web セキュリティ モードで使用可能
ネットワーク（Network）	インターフェイス 透過リダイレクション（Transparent Redirection） ルート DNS 高可用性 内部 SMTP リレー（Internal SMTP Relay） 上位プロキシ（Upstream Proxy） 外部 DLP サーバ（External DLP Servers） 証明書の管理（Certificate Management） 認証 SaaS のアイデンティティ プロバイダー Identity Services Engine	インターフェイス 透過リダイレクション（Transparent Redirection） ルート DNS 高可用性 内部 SMTP リレー（Internal SMTP Relay） 外部 DLP サーバ（External DLP Servers） 証明書の管理（Certificate Management） 認証 マシン ID サービス（Machine ID Service） クラウド コネクタ（Cloud Connector）	インターフェイス 透過リダイレクション（Transparent Redirection） ルート DNS 高可用性 内部 SMTP リレー（Internal SMTP Relay） 証明書の管理（Certificate Management） 認証

メニュー	標準モードで使用可能	クラウド コネクタ モードで使用可能	ハイブリッド Web セキュリティ モードで使用可能
システム管理	ポリシー トレース（Policy Trace） アラート（Alerts） ログ サブスクリプション（Log Subscriptions） 返信先アドレス（Return Addresses） SSL の設定（SSL Configuration） Users Network Access タイム ゾーン 時刻設定（Time Settings） 設定の概要 設定ファイル（Configuration File） 機能キーの設定（Feature Key Settings） ライセンス キー（Feature Keys） アップグレードとアップデートの設定（Upgrade and Update Settings） システム アップグレード（System Upgrade） システム セットアップ ウィザード（System Setup Wizard） FIPS モード（FIPS Mode） 次の手順	アラート（Alerts） ログ サブスクリプション（Log Subscriptions） SSL の設定（SSL Configuration） Users Network Access タイム ゾーン 時刻設定（Time Settings） 設定の概要 設定ファイル（Configuration File） ライセンス キー（Feature Keys） アップグレードとアップデートの設定（Upgrade and Update Settings） システム アップグレード（System Upgrade） システム セットアップ ウィザード（System Setup Wizard）	アラート（Alerts） ログ サブスクリプション（Log Subscriptions） SSL の設定（SSL Configuration） Users Network Access タイム ゾーン 時刻設定（Time Settings） 設定の概要 設定ファイル（Configuration File） ライセンス キーの設定（Feature Key Settings） ライセンス キー（Feature Keys） アップグレードとアップデートの設定（Upgrade and Update Settings） システム セットアップ ウィザード 次の手順
Cisco CWS ポータル（ハイブリッド Web セキュリティ モードでのみ使用可能）	該当なし	該当なし	（ボタンをクリックして新しいウィンドウの ScanCenter ポータルにアクセス）

接続、インストール、設定に関するタスクの概要

タスク	詳細情報
1. アプライアンスをインターネット トラフィックに接続する。	アプライアンスの接続（3-8 ページ）
2. 設定情報を収集して記録する。	設定情報の収集（3-10 ページ）
3. システム セットアップ ウィザードを実行する。	システム セットアップ ウィザード（3-13 ページ）
4. HTTPS プロキシ設定、認証レルム、識別プロファイルを設定する。 **この手順は、ハイブリッド Web セキュリティ モードで完了する必要があります。**	HTTPS プロキシのイネーブル化（7-4 ページ） 認証レルム（5-11 ページ） 識別プロファイルと認証（6-8 ページ）
5. （任意）アップストリーム プロキシを接続する。	アップストリーム プロキシ（3-20 ページ）

アプライアンスの接続

はじめる前に

- アプライアンスを設置するには、管理用アプライアンスにケーブルを配線して電源に接続し、そのアプライアンスのハードウェア ガイドの手順に従います。ご使用のモデルのマニュアルの場所については、ドキュメント セット（C-2 ページ）を参照してください。
- 透過リダイレクションのためにアプライアンスを物理的に WCCP v2 ルータに接続する場合は、まず、WCCP ルータがレイヤ 2 リダイレクションに対応していることを確認します。
- 以下のシスコ推奨設定に注意してください。
  - パフォーマンスとセキュリティの向上のために、可能な場合はシンプレックス ケーブル（着信と発信トラフィック用の個別のケーブル）を使用します。

ステップ 1　管理インターフェイスを接続します（まだ接続していない場合）。

イーサネット ポート	注記
M1	接続可能な場所に M1 を接続します。 • 管理トラフィックを送受信します。 • （任意）Web プロキシ データ トラフィックを送受信します。 M1 にラップトップを直接接続して、アプライアンスを管理できます。 ホスト名（http://hostname:8080）を使用して管理インターフェイスに接続するには、アプライアンスのホスト名と IP アドレスを DNS サーバ データベースに追加します。

イーサネット ポート	注記
P1 および P2（任意）	• 発信方向の管理サービス トラフィックで使用可能ですが、管理には使用できません。 • [ポート M1 は管理目的でのみ使用（Use M1 port for management only）]（[ネットワーク（Network）] > [インターフェイス（Interfaces）] ページ）をイネーブルにします。 • データ インターフェイスを使用するように、サービスのルーティングを設定します。

ステップ 2　（任意）アプライアンスをデータ トラフィックに直接接続するか、透過リダイレクション デバイスを介して接続します。

イーサネット ポート	明示的な転送	透過リダイレクション
P1/P2	P1 のみ： • [ポート M1 は管理目的でのみ使用（Use M1 port for management only）] をイネーブルにします。 • P1 と M1 を異なるサブネットに接続します。 • 着信と発信の両方のトラフィックを受信できるように、デュプレックス ケーブルを使用して P1 を内部ネットワークとインターネットに接続します。 P1 および P2 • P1 をイネーブルにします。 • M1、P1、P2 を異なるサブネットに接続します。 • P2 をインターネットに接続し、着信インターネット トラフィックを受信します。 システム セットアップ ウィザードの実行後、P2 をイネーブルにします。	デバイス：WCCP v2 ルータ： • レイヤ 2 リダイレクションの場合は、ルータを物理的に P1/P2 に接続します。 • レイヤ 3 リダイレクションの場合は、総称ルーティング カプセル化（GRE）でパフォーマンス上の問題が発生する可能性があるので注意してください。 • アプライアンス上に WCCP サービスを作成します。 デバイス：レイヤ 4 スイッチ： • レイヤ 2 リダイレクションの場合は、スイッチを物理的に P1/P2 に接続します。 • レイヤ 3 リダイレクションの場合は、総称ルーティング カプセル化（GRE）でパフォーマンス上の問題が発生する可能性があるので注意してください。 **（注）** アプライアンスはインライン モードをサポートしていません。
M1（任意）	[ポート M1 は管理目的でのみ使用（Use M1 port for management only）] がディセーブルの場合は、M1 がデフォルトのデータ トラフィック用ポートになります。	該当なし

ステップ 3　外部プロキシをアプライアンスのアップストリームに接続し、外部プロキシがアプライアンスからデータを受信できるようにします。

次の作業

- 設定情報の収集（3-10 ページ）

関連項目

- ネットワーク インターフェイスのイネーブル化または変更（3-24 ページ）
- Web プロキシ データに対する P2 データ インターフェイスの使用（3-27 ページ）
- WCCP サービスの追加と編集（3-31 ページ）
- 透過リダイレクションの設定（3-30 ページ）
- アップストリーム プロキシ（3-20 ページ）

設定情報の収集

以下のワークシートを使用して、システム セットアップ ウィザードの実行時に必要な設定値を記録できます。各プロパティの詳細については、システム セットアップ ウィザードの参照情報（3-15 ページ）を参照してください。

システム セットアップ ウィザードのワークシート

プロパティ	値	プロパティ	値
アプライアンスの詳細（Appliance Details）		**ルート**	
デフォルト システム ホスト名（Default System Hostname）		**管理トラフィック（Management Traffic）**	
ローカル DNS サーバ（Local DNS Server(s)） **（インターネット ルート サーバを使用しない場合に必要）**		デフォルト ゲートウェイ（Default Gateway）	
DNS サーバ 1（DNS Server 1）		（任意）スタティック ルート テーブル名（Static Route Table Name）	
（任意）DNS サーバ 2（DNS Server 2）		（任意）スタティック ルート テーブルの宛先ネットワーク（Static Route Table Destination Network）	
（任意）DNS サーバ 3（DNS Server 2）		（任意）標準サービスのルータ アドレス（Standard Service Router Addresses）	
（任意）時間の設定（Time Settings）		**（任意）データ トラフィック（Data Traffic）**	

システム セットアップ ウィザードのワークシート			
ネットワーク タイム プロトコル サーバ（Network Time Protocol Server）		デフォルト ゲートウェイ（Default Gateway）	
（任意）外部プロキシの詳細（External Proxy Details）		スタティック ルート テーブル名（Static Route Table Name）	
プロキシ グループ名（Proxy Group Name）		スタティック ルート テーブルの宛先ネットワーク（Static Route Table Destination Network）	
プロキシ サーバのアドレス（Proxy Server Address）		（任意）**WCCP 設定（WCCP Settings）**	
プロキシ ポート番号（Proxy Port Number）		WCCP ルータ アドレス（WCCP Router Address）	
インターフェイスの詳細（Interface Details）		WCCP ルータ パスフレーズ（WCCP Router Passphrase）	
管理（M1）ポート（Management (M1) Port）		**管理設定（Administrative Settings）**	
IPv4 アドレス（IPv4 Address）（必須） IPv6 アドレス（IPv6 Address）（任意）		管理者パスフレーズ（Administrator Passphrase）	
ネットワーク マスク（Network Mask）		システム アラート メールの送信先（Email System Alerts To）	
ホスト ネーム		（任意）SMTP リレー ホスト（SMTP Relay Host）	
（任意）データ（P1）ポート（Data (P1) Port）			
IPv4（任意） IPv6 アドレス（IPv6 Address）（任意）			
ネットワーク マスク（Network Mask）			
ホスト ネーム			

への登録 Cisco Cloud Web Security

クラウドからセキュリティ ポリシーをダウンロードして定期的に更新するために、ハイブリッド Web セキュリティ モードで動作する Web セキュリティ アプライアンスを Cisco Cloud Web Security（CWS）に登録する必要があります。

登録が成功すると、セキュリティ アプライアンスは、Cisco ScanCenter から Cisco Cloud Web Security ポリシーをダウンロードします。

- Cisco ScanCenter の CWS ポリシーを変更するたびに、ポリシーの同期のためにすべてのポリシーがセキュリティ アプライアンスにダウンロードされます。
- デフォルトでは、アプライアンスは、更新されたポリシーがダウンロード可能かどうか 2 分ごとに確認します。
- [レポート（Reporting）] > [システム ステータス（System Status）] に、CWS へのハイブリッド モードの登録ステータスが表示されます。

次の手順に従って、CWS に登録し、WSA の接続トークンを生成します。

ステップ 1　Cisco ScanCenter アカウントにログインします。

ステップ 2　[管理者（Admin）] タブをクリックします。

ステップ 3　[管理（Management）] > [ハイブリッド Web セキュリティ（Hybrid Web Security）] を選択します。

ステップ 4　[トークンの生成（Generate Token）] をクリックします。

ステップ 5　新しいトークンが表示されたら、[クリップボードにトークンをコピー（Copy Token to Clipboard）] をクリックします。

次のステップ

Web セキュリティ アプライアンス の [システムソフトウェアウィザード（System Software Wizard）] の [Web ポリシーの接続性（Web Policy Connectivity）] ページで、[認証キーの入力（Enter Authorization Key）] ダイアログ ボックスにこのトークンを貼り付けます（システム セットアップ ウィザード (3-13 ページ)を参照）。

このトークンの有効期限は 1 時間です。1 時間以内に WSA の設定に使用しなかった場合、別のトークンを生成する必要があります。

関連項目

- http://www.cisco.com/c/en/us/td/docs/security/web_security/scancenter/administrator/guide/b_ScanCenter_Administrator_Guide.html

Web セキュリティ アプライアンスでの登録の変更

WSA で Cisco ScanCenter の登録を変更または更新するには、次の手順を実行します。

ステップ 1　[ネットワーク（Network）] > [Web ポリシーの接続性（Web Policy Connectivity）] を選択します。

ステップ 2　[登録の変更（Change Registration）] をクリックします。

ステップ 3　Cisco ScanCenter ポータルから受け取った新しい承認トークンを [認証キーの入力（Enter Authorization Key）] ダイアログボックスに入力し、[登録（Register）] をクリックします。

システム セットアップ ウィザード

はじめる前に:

- アプライアンスをネットワークとデバイスに接続します。アプライアンスの接続（3-8 ページ）を参照してください。
- システム セットアップ ウィザードのワークシートを完成させます。設定情報の収集（3-10 ページ）を参照してください。
- 仮想アプライアンスを設定する場合は、以下の手順に従います。
  - `loadlicense` コマンドを使用して、仮想アプライアンスのライセンスをロードします。詳細については、『*Cisco Content Security Virtual Appliance Installation Guide*』を参照してください。このドキュメントは、http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html から入手できます。
  - HTTP、および/または HTTPS インターフェイスを有効にします（コマンドライン インターフェイス（CLI）で、`interfaceconfig` コマンドを実行します）。
- Web ハイブリッド モードを設定するには、システム セットアップ ウィザードを実行して標準モードでアプライアンスを設定してから AsyncOS 9.2 にアップグレードし、システム セットアップ ウィザードを再実行してハイブリッド Web セキュリティ モードで設定する必要があります（これは、アップグレードされていない仮想イメージには適用されません）。
- クラウド Web セキュリティ ポリシーとの互換性を実現するには、Web ハイブリッド モードで動作しているときに少なくとも 1 つのマルウェア対策スキャン エンジン（McAfee、Sophos、または Webroot）のライセンスを付与されていて使用可能である必要があります。Web ハイブリッド モードで設定を完了するには、有効なライセンスまたは機能キーが使用可能であることを確認します。
- CWS および WSA には、相互の通信を認証してセキュリティ保護するために、認証局の署名付き証明書が必要です。この証明書を外部で生成し、Cisco ScanCenter と Cisco WSA の両方に証明書とそのキーをアップロードする必要があります。証明書およびキーのアップロード（12-25 ページ）を参照してください。
- この Web セキュリティ アプライアンスを Cisco Cloud Web Securityに登録して、承認トークンを取得します。このトークンの有効期限は 1 時間です。1 時間以内に WSA の設定に使用しなかった場合、別のトークンを生成する必要があります。への登録 Cisco Cloud Web Security（3-12 ページ）を参照してください。
- システム セットアップ ウィザードの参照情報（3-15 ページ）で使用される各設定項目の参照情報は、システム セットアップ ウィザード に記載されています。

警告　**初めてアプライアンスをインストールする場合、または既存の設定を完全に上書きする場合にのみ、システム セットアップ ウィザードを使用してください。完了前にシステム セットアップ ウィザードをキャンセルした場合でも、アプライアンスは工場出荷時の初期状態にリセットされます。**

ステップ 1　ブラウザを開き、Web セキュリティ アプライアンスの IP アドレスを入力します。初めてシステム セットアップ ウィザードを実行するときは、以下のデフォルトの IP アドレスを使用します。

```
https://192.168.42.42:8443
```

または

```
http://192.168.42.42:8080
```

ここで、192.168.42.42 はデフォルト IP アドレス、8080 は、HTTP のデフォルトの管理ポートの設定、8443 は HTTPS のデフォルトの管理ポートです。

あるいは、アプライアンスが現在設定されている場合は、M1 ポートの IP アドレスを使用します。

ステップ 2　アプライアンスのログイン画面が表示されたら、アプライアンスにアクセスするためのユーザ名とパスフレーズを入力します。デフォルトで、アプライアンスには以下のユーザ名とパスフレーズが付属します。

- ユーザ名：**admin**
- パスフレーズ：**ironport**

ステップ 3　パスフレーズをただちに変更する必要があります。

ステップ 4　[システム管理（System Administration）] > [システム セット アップウィザード（System Setup Wizard）] を選択します。

アプライアンスがすでに設定されている場合は、設定がリセットされるという警告が表示されます。システム セットアップ ウィザードを続行するには、[ネットワーク設定のリセット（Reset Network Settings）] をオンにしてから [構成のリセット（Reset Configuration）] ボタンをクリックします。アプライアンスがリセットされ、ブラウザが更新されてアプライアンスのホーム画面が表示されます。

ステップ 5　エンドユーザ ライセンス契約が表示されたら、内容を読んで同意します。

ステップ 6　続行するには、[セットアップの開始（Begin Setup）] をクリックします。

ステップ 7　必要に応じて、以下のセクションで提供されるリファレンス テーブルを使用して、すべての設定を行います。システム セットアップ ウィザードの参照情報（3-15 ページ）を参照してください。

ステップ 8　設定情報を確認してください。オプションを変更する必要がある場合は、そのセクションで [編集（Edit）] をクリックします。

ステップ 9　[この設定をインストール（Install This Configuration）] をクリックします。

ステップ 10　ハイブリッド Web セキュリティ ポリシー通信用の Cisco Cloud Web Security にアプライアンスを接続します。

a. [システムソフトウェアウィザード（System Software Wizard）] の [Web ポリシーの接続性（Web Policy Connectivity）] ページで [登録（Register）] をクリックします。

b. Cisco ScanCenter ポータルにコピーした承認トークンを [認証キーの入力（Enter Authorization Key）] ダイアログボックスに入力し、[登録（Register）] をクリックします。

承認トークンの取得の詳細については、への登録 Cisco Cloud Web Security（3-12 ページ）を参照してください。

この承認トークンの変更については、Web セキュリティ アプライアンスでの登録の変更（3-12 ページ）を参照してください。

登録に成功すると、使用可能なセキュリティ ポリシーが Cisco ScanCenter から Web セキュリティ アプライアンスにダウンロードされます。詳細については、クラウド Web セキュリティのポリシーアプリケーションについて（2-2 ページ）を参照してください。

設定がインストールされると、[次のステップ（Next Steps）] ページが表示されます。ただし、セットアップ中に設定した IP、ホスト名、DNS 設定によっては、この段階でアプライアンスへの接続が失われることがあります。「ページが見つかりません（Page Not Found）」というメッセージがブラウザに表示される場合は、新しいアドレス設定が反映されるように URL を変更し、ページをリロードします。その後、実行する必要があるポスト セットアップ タスクを続行します。

次の作業

ダウンロードされる CWS ポリシーに HTTPS ルールまたは認証グループ ルールが含まれる場合、システム セットアップ ウィザード（SSW）でハイブリッド Web セキュリティ モードの設定が完了した直後に WSA で HTTPS プロキシ設定、認証レルム、および識別プロファイルを設定することが重要です。HTTPS ルールまたは認証グループ ルールに含まれている CWS ポリシーの変換およびダウンロードは WSA ハイブリッド システムのセットアップではスキップされ、HTTPS プロキシ、認証レルム、および識別プロファイルが設定されていて、WSA がハイブリッド モードで設定された後にのみ完了します（CWS から WSA へのポリシーの更新は 2 分ごとに行われるため、変換/ダウンロード プロセスは自動的に完了します）。

CWS では、認証レルムは SAML および EasyID と呼ばれます。WSA ではサポートされるタイプは異なり、通常、NTLM と呼ばれます（SAML は WSA ではまだサポートされていません）。CWS のルールに認証ユーザ名または設定済みの認証グループのいずれかが含まれている場合、WSA で認証が有効になっている状態で認証レルムとカスタム識別プロファイルを設定する必要があります。

- HTTPS プロキシ設定の構成：HTTPS プロキシのイネーブル化（7-4 ページ）を参照してください。
- 認証レルムおよび識別プロファイルの設定：エンドユーザおよびクライアント ソフトウェアの分類（6-1 ページ）を参照してください。

Cisco ScanCenter で設定可能ないくつかの項目は、Cisco Web セキュリティ アプライアンスによるダウンロードではまだサポートされていません。次の項目は、アプライアンスで直接設定する必要があります。

- 電子メール アラート設定。電子メール アラートを受信する頻度（電子メール アドレスはソフトウェア セットアップ ウィザードによる設定時に提供されます）。
- カスタマイズされたアラート。[ブロック（Block）]、[警告（Warn）]、または [AUP] カスタム テキスト用のカスタム アラート ページ。
- グローバル設定（Global Settings）。[SearchAhead]、[SafeSearch]、[AUP]（WSA の場合は [EUA]）、[動的分類エンジン（Dynamic Classification Engine）]、[コンテンツ範囲ヘッダー（Content Range Headers）]、および [サンドボクシング（Sandboxing）] などの設定の有効化。

システム セットアップ ウィザードの参照情報

- ネットワーク/システムの設定（3-16 ページ）
- ネットワーク/ネットワーク インターフェイスおよび配線（3-17 ページ）
- 管理およびデータ トラフィックのネットワーク/ルートの設定（3-18 ページ）
- ネットワーク/透過的接続の設定（3-18 ページ）
- ネットワーク/管理の設定（3-19 ページ）
- セキュリティ/アップグレードのタイミング（3-20 ページ）

ネットワーク/システムの設定

プロパティ	説明
デフォルト システム ホスト名（Default System Hostname）	システム ホスト名は、以下の領域でアプライアンスの識別に使用される完全修飾ホスト名です。 • コマンドライン インターフェイス（CLI） • システム アラート • エンドユーザ通知ページおよび確認ページ • Web セキュリティ アプライアンスが Active Directory ドメインに参加するときに、マシンの NetBIOS 名を作成する場合 システム ホスト名はインターフェイスのホスト名と直接対応しておらず、クライアントがアプライアンスに接続するために使用されません。
DNS サーバ（DNS Server(s)）	• [インターネットのルート DNS サーバを使用（Use the Internet's Root DNS Servers）]：アプライアンスがネットワーク上の DNS サーバにアクセスできない場合に、ドメイン名サービス ルックアップにインターネットのルート DNS サーバを使用することを選択できます。 **（注）** インターネット ルート DNS サーバは、ローカル ホスト名を解決しません。アプライアンスでローカル ホスト名を解決する必要がある場合は、ローカル DNS サーバを使用して解決するか、CLI からローカル DNS に適切なスタティック エントリを追加する必要があります。 [以下の DNS サーバを使用（Use these DNS Servers）]：アプライアンスがホスト名の解決に使用できるローカル DNS サーバにアドレスを提供します。 これらの設定の詳細については、DNS の設定（3-38 ページ）を参照してください。
NTP サーバ（NTP Server）	システム クロックをネットワークまたはインターネット上の他のサーバと同期させるために使用する、Network Time Protocol（NTP）サーバ。 デフォルトは、time.sco.cisco.com です。
タイム ゾーン	アプライアンスの場所に応じたタイム ゾーン情報を提供します。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に影響します。
アプライアンスの動作モード（Appliance Mode of Operation）	• 標準：標準的なオンプレミス ポリシーの適用に使用します。 • クラウド Web セキュリティ コネクタ：主に、Cisco クラウド Web セキュリティ サービスにトラフィックをダイレクトし、ポリシーを適用して脅威から防御するために使用します。 • ハイブリッド Web セキュリティ：クラウドとオンプレミス ポリシーの適用および脅威に対する防御のために、Cisco クラウド Web セキュリティ サービスと併用されます。 これらの動作モードの詳細については、操作モードの比較（3-2 ページ）を参照してください。

ネットワーク/クラウド コネクタの設定

設定	説明
クラウド Web セキュリティ プロキシ サーバ（Cloud Web Security Proxy Servers）	クラウド プロキシ サーバ（CPS）のアドレス（例: `proxy1743.scansafe.net`）。
失敗のハンドリング（Failure Handling）	AsyncOS がクラウド Web セキュリティ プロキシへの接続に失敗した場合、インターネットに [直接接続（Connect directly）] するか、[要求をドロップ（Drop requests）] します。
Cloud Web Security 認証スキーム（Cloud Web Security Authorization Scheme）	トランザクションを認証する方式: • Web セキュリティ アプライアンスの公開されている IPv4 アドレス。 • 各トランザクションに含まれている認証キー。Cisco Cloud Web Security Portal 内で認証キーを生成できます。

ネットワーク/ネットワーク インターフェイスおよび配線

Web セキュリティ アプライアンスの管理および（デフォルトで）プロキシ（データ）トラフィック用に使用される IP アドレス、ネットワーク マスク、ホスト名。

アプライアンス管理インターフェイスに接続するときに（または、M1 がプロキシ データに使用される場合はブラウザ プロキシ設定で）、ここで指定したホスト名を使用できます。ただし、そのホスト名を組織の DNS に登録しておく必要があります。

設定	説明
イーサネット ポート（Ethernet Port）	（任意）データ トラフィック用に個別のポートを使用する場合は、[ポート M1 は管理目的でのみ使用（Use M1 Port For Management Only）] をオンにします。 M1 インターフェイスを管理トラフィック専用として設定する場合は、データ トラフィック用の P1 インターフェイスを設定する必要があります。また、管理トラフィックとデータ トラフィック用に異なるルートを定義する必要があります。ただし、管理トラフィックとデータ トラフィックの両方を M1 インターフェイスとして使用する場合でも、P1 インターフェイスを設定できます。 システム セットアップ ウィザードでは、P1 ポートのみをイネーブルにして設定できます。P2 インターフェイスをイネーブルにする場合は、システム セットアップ ウィザードを終了してから行う必要があります。
IP アドレス/ネットマスク（IP Address / Netmask）	このネットワーク インターフェイス上の Web セキュリティ アプライアンスを管理する際に使用する IP アドレスとネットワーク マスク。
ホスト ネーム	このネットワーク インターフェイス上の Web セキュリティ アプライアンスを管理する際に使用するホスト名。

管理およびデータ トラフィックのネットワーク/ルートの設定

（注）　[ポート M1 は管理目的でのみ使用（Use M1 port for management only）] をイネーブルにした場合、このセクションには、管理トラフィックとデータ トラフィック用の個別のセクションが表示されます。それ以外の場合は 1 つの結合されたセクションが表示されます。

プロパティ	説明
デフォルト ゲートウェイ（Default Gateway）	管理およびデータ インターフェイスを通過するトラフィックに使用するデフォルト ゲートウェイの IP アドレス。
スタティック ルート テーブル（Static Routes Table）	管理およびデータ トラフィック用のオプションのスタティック ルート。複数のルートを追加できます。 • [名前（Name）]: スタティック ルートの識別に使用する名前。 • [内部ネットワーク（Internal Network）]: このルートのネットワーク上の宛先の IPv4 アドレス。 • [内部ゲートウェイ（Internal Gateway）]: このルートのゲートウェイ IPv4 アドレス。ルート ゲートウェイは、それが設定されている管理インターフェイスまたはデータ インターフェイスと同じサブネット上に存在する必要があります。

ネットワーク/透過的接続の設定

（注）　デフォルトでは、クラウド コネクタはトランスペアレント モードで展開され、レイヤ 4 スイッチまたは WCCP バージョン 2 ルータと接続する必要があります。

プロパティ	説明
レイヤ 4 スイッチまたはデバイスなし（Layer-4 Switch or No Device）	Web セキュリティ アプライアンスが透過リダイレクション用にレイヤ 4 スイッチに接続されていること、または透過リダイレクション デバイスを使用せず、クライアントがアプライアンスに明示的に要求を転送することを指定します。

プロパティ	説明
WCCP v2 ルータ（WCCP v2 Router）	Web セキュリティ アプライアンスが WCCP バージョン 2 対応ルータに接続されていることを指定します。 アプライアンスを WCCP バージョン 2 ルータに接続する場合は、少なくとも 1 つの WCCP サービスを作成する必要があります。この画面で、またはシステム セットアップ ウィザードの終了後に、標準サービスをイネーブルにでき、複数のダイナミック サービスを作成することもできます。 標準サービスをイネーブルにすると、ルータ セキュリティをイネーブルにして、パスフレーズを入力することもできます。ここで使用されるパスフレーズは、同じサービス グループ内のすべてのアプライアンスと WCCP ルータで使用する必要があります。 標準サービス タイプ（別名「Web キャッシュ」サービス）には、固定 ID「ゼロ」、固定リダイレクト方式「宛先ポート別」、固定宛先ポート「80」が割り当てられます。 ダイナミック サービス タイプでは、カスタム ID、ポート番号、およびリダイレクト オプションとロード バランシング オプションを定義できます。

ネットワーク/管理の設定

プロパティ	説明
管理者パスフレーズ（Administrator Passphrase）	管理のために Web セキュリティ アプライアンスにアクセスするときに使用されるパスフレーズ。
システム アラート メールの送信先（Email System Alerts To）	アプライアンスがシステム アラートを送信する宛先の電子メール アドレス。
SMTP リレー ホスト経由で電子メールを送信（Send Email via SMTP Relay Host）（任意）	AsyncOS がシステムで生成された電子メール メッセージの送信に使用できる、SMTP リレー ホストのアドレスとポート。 SMTP リレー ホストが定義されていない場合、AsyncOS は MX レコードにリストされているメール サーバを使用します。
オートサポート（AutoSupport）	アプライアンスがシステム アラートと毎週のステータス レポートをシスコ カスタマー サポートに送信するかどうかを指定します。
SensorBase ネットワークに参加（SensorBase Network Participation）	Cisco SensorBase ネットワークに参加するかどうかを指定します。参加する場合、制限付き参加または標準（完全な）参加を設定できます。デフォルトは標準です。 SensorBase ネットワークは、世界中の何百万ものドメインを追跡し、インターネット トラフィックのグローバルな監視リストを保持する脅威管理データベースです。SensorBase ネットワーク参加をイネーブルにすると、Web セキュリティ アプライアンスは SensorBase ネットワーク データの価値を高めるために、HTTP 要求に関する匿名の統計情報をシスコに送信します。

セキュリティ/セキュリティ設定

オプション	説明
マルウェアとスパイウェアのスキャン（Malware and Spyware Scanning）	Webroot、McAfee、または Sophos によるマルウェアやスパイウェアのスキャンをイネーブルにするかどうかを指定します。クラウド ポリシーで通常使用可能なサービスに対応して、ほとんどのセキュリティ サービスは自動的に有効/無効になります。同様に、ポリシー関連のデフォルトは適用されません。少なくとも 1 つのスキャン オプションをイネーブルにする必要があります。 オプションをイネーブルにした場合は、検出されたマルウェアをモニタするかブロックするかも選択します。デフォルトの設定は、マルウェアのモニタです。 システム セットアップ ウィザードを完了後、マルウェア スキャンを追加設定することもできます。

セキュリティ/アップグレードのタイミング

オプション	説明
アップグレードの時間帯（Upgrade Timing Windows）	ハイブリッド モードでは、アップグレードは、使用可能な場合は自動的にダウンロードされ、指定された時間帯でインストールされます。必要なソフトウェアのアップデートを実行できるように、週ごとに少なくとも 2 つの時間帯を指定する必要があります。時間帯は、次の条件を満たしていなければなりません。 • 最低 2 時間。 • 4 日以上間隔を空けない（たとえば、初回の選択が月曜日の場合、 • 2 回目は木曜日か金曜日になります）。 各時間帯に対して、曜日、開始時刻、継続時間を選択します。 アップグレード/更新プログラムのインストールを開始する 2 時間の枠の始まりを定義します。インストールが完了するとアプライアンスが再起動するため、できるだけ影響の少ない時間を指定します。 **（注）** この WSA を CWS ポータルに登録して 30 分以内にアップグレードの時間帯を設定しないでください（つまり、システム セットアップ ウィザードの最後の手順を完了してから 30 分以上あけてください）。 時間帯の変更の詳細およびこの時間帯の一度限りの例外の設定については、AsyncOS for Web のアップグレードとアップデート（12-27 ページ）を参照してください。

アップストリーム プロキシ

Web プロキシは、Web トラフィックを宛先 Web サーバに直接転送することも、ルーティング ポリシーを使用して外部アップストリーム プロキシにリダイレクトすることもできます。

- アップストリーム プロキシのタスクの概要（3-21 ページ）
- アップストリーム プロキシのプロキシ グループの作成（3-21 ページ）

アップストリーム プロキシのタスクの概要

タスク	詳細情報
1. Cisco Web セキュリティ アプライアンス のアップストリームに外部プロキシに接続する。	アプライアンスの接続（3-8 ページ）。
2. アップストリーム プロキシのプロキシ グループを作成して設定する。	アップストリーム プロキシのプロキシ グループの作成（3-21 ページ）。
3. プロキシ グループのルーティング ポリシーを作成し、アップストリーム プロキシにルーティングするトラフィックを管理する。	Create Policies to Control Internet Requests

アップストリーム プロキシのプロキシ グループの作成

ステップ 1　[ネットワーク（Network）] > [アップストリームプロキシ（Upstream Proxies）] を選択します。

ステップ 2　[グループの追加（Add Group）] をクリックします。

ステップ 3　プロキシ グループの設定を完了させます。

プロパティ	説明
Name	ルーティング ポリシーなどでアプライアンス上のプロキシ グループの識別に使用される名前など。
プロキシ サーバ（Proxy Servers）	グループのプロキシ サーバのアドレス、ポート、再接続試行（プロキシが応答しない場合）。必要に応じて、各プロキシ サーバの行を追加または削除できます。 **（注）**　同じプロキシ サーバを複数回追加して、プロキシ グループのプロキシ間に不均衡に負荷を分散できます。

プロパティ	説明
ロード バランシング	複数のアップストリーム プロキシ間のロード バランス要求のために Web プロキシが使用する方法。次から選択します。 • [なし（フェールオーバー）（None (failover)）]。Web プロキシは、グループ内の 1 つの外部プロキシにトランザクションを送信します。一覧表示されている順序でプロキシへの接続を試みます。あるプロキシに到達できない場合、Web プロキシはリストの以下のプロキシに接続を試みます。 • [最少接続（Fewest connections）]。Web プロキシは、グループ内のざまざまなプロキシにおけるアクティブな要求の数を追跡し、その時点で接続数が最も少ないプロキシにトランザクションを送信します。 • [ハッシュベース（Hash based）]。[最も長い間使われていない（Least recently used）]。すべてのプロキシがアクティブである場合、Web プロキシは、最も長い間トランザクションを受信していないプロキシにトランザクションを送信します。この設定はラウンドロビンに似ています。異なる点は、Web プロキシが、異なるプロキシ グループのメンバーであるプロキシが受信したトランザクションも考慮するということです。つまり、あるプロキシが複数のプロキシ グループのリストに含まれている場合でも、[最も長い間使われていない（least recently used）] オプションによってそのプロキシが過負荷になることはほとんどありません。 • [ラウンドロビン（Round robin）]。Web プロキシは、リストに記載されている順序で、グループ内のすべてのプロキシにトランザクションを均等に割り当てます。 **（注）** 複数のプロキシを定義するまで、[ロードバランシング（Load Balancing）] オプションはグレー表示されます。
失敗のハンドリング（Failure Handling）	このグループのすべてのプロキシが失敗した場合のデフォルト アクションを指定します。次から選択します。 • [直接接続（Connect directly）]。宛先サーバに直接、要求を送信します。 • [要求をドロップ（Drop requests）]。要求を転送しないで、廃棄します。

ステップ 4　変更を送信し、保存します。

次の作業

- Creating a Policy（10-7 ページ）

ネットワーク インターフェイス

IP アドレスのバージョン

標準モードでは、Cisco Web セキュリティ アプライアンスは大部分の場合に IPv4 と IPv6 アドレスをサポートします。

（注）　クラウド コネクタ モードでは、Cisco Web セキュリティ アプライアンスは IPv4 のみをサポートします。

DNS サーバは、IPv4 と IPv6 の両方のアドレスと共に結果を返すことができます。DNS の設定項目には [IP アドレスバージョン設定（IP Address Version Preference）] が含まれているので、以下の場合における AsyncOS の動作を設定できます。

インターフェイス/サービス	IPv4	IPv6	注記
M1 インターフェイス	必須	オプション	IPv6 アドレスを使用するには、デフォルトの IPv6 ゲートウェイを定義する IPv6 ルーティング テーブルが必要です。ネットワークによっては、ルーティング テーブルで IPv6 スタティック ルートも指定する必要があります。
P1 インターフェイス	オプション	オプション	P1 インターフェイスに IPv6 アドレスが設定されており、アプライアンスが分割ルーティング（個別の管理ルートとデータ ルート）を使用している場合、P1 インターフェイスは管理ルート上に設定された IPv6 ゲートウェイを使用できません。代わりに、データ ルーティング テーブルに IPv6 ゲートウェイを指定します。
P2 インターフェイス	オプション	オプション	—
データ サービス	サポート対象	サポート対象	—
制御および管理サービス	サポート対象	一部サポートあり	イメージ（エンドユーザ通知ページのカスタム ロゴなど）には IPv4 が必要です。
AnyConnect セキュア モビリティ（MUS）	サポート対象	未サポート	—

関連項目

- ネットワーク インターフェイスのイネーブル化または変更（3-24 ページ）
- DNS の設定（3-38 ページ）

ネットワーク インターフェイスのイネーブル化または変更

- インターフェイス IP アドレスの追加または変更
- レイヤ 4 トラフィック モニタの配線タイプの変更
- 管理およびデータ トラフィックの分割ルーティングのイネーブル化

ステップ 1　[ネットワーク（Network）] > [インターフェイス（Interfaces）] 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。

ステップ 3　インターフェイスのオプションを設定します。

オプション	説明
インターフェイス	M1、P1、または P2 インターフェイスの新しい IPv4 または IPv6 アドレス、ネットマスク、ホスト名の詳細を追加するか、既存の詳細を変更します。 • **M1**：AsyncOS には M1（管理）ポートの IPv4 アドレスが必要です。IPv4 アドレスに加えて、IPv6 アドレスも指定できます。デフォルトで、管理インターフェイスはアプライアンスおよび Web プロキシ（データ）のモニタリングを管理するために使用されます。ただし、管理用途専用の M1 ポートを設定できます。 • **P1** および **P2**：データ ポートの IPv4 アドレス、IPv6 アドレス、または両方を使用します。データ インターフェイスは Web プロキシによるモニタリングとレイヤ 4 トラフィック モニタによるブロッキング（任意）で使用されます。これらのインターフェイスを設定して、DNS、ソフトウェア アップグレード、NTP、および traceroute データ トラフィックなどの発信サービスをサポートすることもできます。 **（注）** 管理およびデータ インターフェイスをすべて設定する場合、それぞれに異なるサブネット上の IP アドレスを割り当てる必要があります。
管理サービス用の分離ルーティング（Separate Routing for Management Services）	M1 を管理トラフィック専用に制限して、データ トラフィック用に別のポートを使用する必要がある場合は、[M1 ポートをアプライアンス管理サービスのみに限定する（Restrict M1 port to appliance management services only）] をオンにします。 **（注）** M1 を管理トラフィック専用にする場合は、別のサブネットにプロキシ トラフィック用のデータ インターフェイスを少なくとも 1 つ設定します。管理トラフィックとデータ トラフィック用に異なるルートを定義してください。
アプライアンス管理サービス（Appliance Management Services）	以下のネットワーク プロトコルの使用をイネーブルまたはディセーブルにして、そのデフォルトのポート番号を指定します。 • **FTP**：デフォルトでディセーブルになります。 • **SSH** • **HTTP** • **HTTPS** また、HTTP トラフィックの HTTPS へのリダイレクションをイネーブルまたはディセーブルにできます。

ステップ 4　変更を送信し、保存します。

次の作業

- IPv6 アドレスを追加する場合は、IPv6 ルーティング テーブルを追加します。

関連項目

- アプライアンスの接続（3-8 ページ）。
- IP アドレスのバージョン（3-23 ページ）
- TCP/IP トラフィック ルートの設定（3-28 ページ）

ハイ アベイラビリティを実現するためのフェールオーバー グループの設定

共通アドレス冗長プロトコル（CARP）を使用すると、WSA ではネットワーク上の複数のホストで IP アドレスを共有できるようになます。これにより IP 冗長性が実現され、それらのホストから提供されるサービスのハイ アベイラビリティを確保できます。CARP には、ホスト用の 3 種類のステータスがあります。

- master
- backup
- init

サービスを提供できる各フェールオーバー グループに対して 1 つのマスター ホストのみを配置できます。

フェールオーバー グループの追加

はじめる前に

- このフェールオーバー グループ専用に使用する仮想 IP アドレスを特定します。クライアントはこの IP アドレスを使用して、明示的な転送プロキシ モードでフェールオーバー グループに接続します。
- 以下のパラメータに対して、フェールオーバー グループ内のすべてのアプライアンスに同じ値を設定します。
  - フェールオーバー グループ ID（Failover Group ID）
  - ホストネーム
  - 仮想 IP アドレス（Virtual IP Address）
- 仮想アプライアンスにこの機能を設定する場合は、各アプライアンス固有の仮想スイッチと仮想インターフェイスが無差別モードを使用するように設定されていることを確認します。詳細については、各自の仮想ハイパーバイザのマニュアルを参照してください。

ステップ 1　[ネットワーク（Network）] > [ハイアベイラビリティ（High Availability）] を選択します。

ステップ 2　[フェールオーバーグループの追加（Add Failover Group）] をクリックします。

ステップ 3　[フェールオーバーグループ ID（Failover Group ID）] に 1 ～ 255 の値を入力します。

ステップ 4　（任意）[説明（Description）] に説明を入力します。

ステップ 5　[ホスト名（Hostname）] にホスト名を入力します（*www.example.com* など）。

ステップ 6　[仮想 IP アドレスとネットマスク（Virtual IP Address and Netmask）] に値を入力します。例: *10.0.0.3/24*（IPv4）または *2001:420:80:1::5/32*（IPv6）。

ステップ 7　[インターフェイス（Interface）] メニューからオプションを選択します。[インターフェイスの自動選択（Select Interface Automatically）] オプションを選択すると、指定した IP アドレスに基づいてインターフェイスが選択されます。

（注）　[インターフェイスの自動選択（Select Interface Automatically）] オプションを選択しない場合は、指定した仮想 IP アドレスと同じサブネット内のインターフェイスを選択する必要があります。

ステップ 8　優先順位を選択します。[マスター（Master）] をクリックし、優先順位を 255 に設定します。または、[バックアップ（Backup）] を選択し、[優先順位（Priority）] フィールドに 1（最下位）～ 254 の優先順位を入力します。

ステップ 9　（任意）。サービスに対してセキュリティをイネーブルにするには、[サービスのセキュリティ有効化（Enable Security Service）] チェックボックスをオンにし、共有シークレットとして使用する文字列を [共有シークレット（Shared Secret）] と [共有シークレットの再入力（Retype Shared Secret）] フィールドに入力します。

（注）　共有シークレット、仮想 IP、フェールオーバー グループ ID は、フェールオーバー グループ内のすべてのアプライアンスで同一でなければなりません。

ステップ 10　[アドバタイズメントの間隔（Advertisement Interval）] フィールドに、アベイラビリティをアドバタイズするホスト間の遅延を秒単位（1 ～ 255）で入力します。

ステップ 11　変更を送信し、保存します。

関連項目

- フェールオーバーに関する問題（A-4 ページ）

高可用性グローバル設定の編集

ステップ 1　[ネットワーク（Network）] > [ハイアベイラビリティ（High Availability）] を選択します。

ステップ 2　[高可用性グローバル設定（High Availability Global Settings）] 領域で、[設定を編集（Edit Settings）] をクリックします。

ステップ 3　[フェールオーバー処理（Failover Handling）] メニューからオプションを選択します。

- [プリエンプティブ（Preemptive）]: 使用可能な場合、優先順位が最も高いホストが制御を担います。
- [プリエンプティブでない（Non-preemptive）]: より優先順が高いホストが使用可能になった場合でも、現在制御を担っているホストが制御を続行します。

ステップ 4　[送信（Submit）] をクリックします。または、[キャンセル（Cancel）] をクリックして変更を破棄します。

フェールオーバー グループのステータスの表示

[ネットワーク（Network）] > [ハイアベイラビリティ（High Availability）] を選択します。[フェールオーバーグループ（Failover Groups）] 領域に現在のフェールオーバー グループが表示されます。[ステータスの更新（Refresh Status）] をクリックすると、表示を更新できます。また、[ネットワーク（Network）] > [インターフェイス（Interfaces）] または [レポート（Report）] > [システムステータス（System Status）] を選択すると、フェールオーバーの詳細を表示できます。

Web プロキシ データに対する P2 データ インターフェイスの使用

デフォルトでは、イネーブルになっている場合でも、Web プロキシは P2 で要求をリッスンしません。ただし、Web プロキシ データをリッスンするように P2 を設定できます。

（注）　`advancedproxyconfig > miscellaneous` CLI コマンドを使用して、クライアント要求をリッスンするために P2 をイネーブルにする場合、発信トラフィックに P1 を使用するか、P2 を使用するかを選択できます。発信トラフィックに P1 を使用するには、データ トラフィックのデフォルト ルートを変更して、P1 インターフェイスが接続されている以下の IP アドレスを指定します。

はじめる前に

- P2 をイネーブルにします（P1 がイネーブルになっていない場合は P1 もイネーブルにする必要があります）（ネットワーク インターフェイスのイネーブル化または変更（3-24 ページ）を参照）。

ステップ 1　CLI にアクセスします。

ステップ 2　`advancedproxyconfig ->miscellaneous` コマンドを使用して、必要なエリアにアクセスします。

```
example.com> advancedproxyconfig

    Choose a parameter group:
    - AUTHENTICATION - Authentication related parameters
    - CACHING - Proxy Caching related parameters
    - DNS - DNS related parameters
    - EUN - EUN related parameters
    - NATIVEFTP - Native FTP related parameters
    - FTPOVERHTTP - FTP Over HTTP related parameters
    - HTTPS - HTTPS related parameters
    - SCANNING - Scanning related parameters
    - PROXYCONN - Proxy connection header related parameters
    - CUSTOMHEADERS - Manage custom request headers for specific domains
    - MISCELLANEOUS - Miscellaneous proxy related parameters
    - SOCKS - SOCKS Proxy parameters
```

ステップ 3　**[]> miscellaneous**

ステップ 4　下記の質問が表示されるまで、Enter キーを押して各質問をパスします。

```
Do you want proxy to listen on P2?
```

この質問に対して「**y**」を入力します。

ステップ 5　**Enter** キーを押して、残りの質問をパスします。

ステップ 6　変更を保存します。

関連項目

- アプライアンスの接続（3-8 ページ）。
- TCP/IP トラフィック ルートの設定（3-28 ページ）。

TCP/IP トラフィック ルートの設定

ルートは、ネットワーク トラフィックの送信先（ルーティング先）を指定するために使用されます。Web セキュリティ アプライアンスは、以下の種類のトラフィックをルーティングします。

- **データ トラフィック。**Web を参照しているエンド ユーザからの Web プロキシが処理するトラフィック。
- **管理トラフィック。**Web インターフェイスを介してアプライアンスを管理することによって作成されるトラフィック、およびアプライアンスが管理サービス（AsyncOS のアップグレード、コンポーネントのアップデート、DNS、認証など）用に作成するトラフィック。

デフォルトでは、どちらのトラフィックも、すべての設定済みネットワーク インターフェイス用に定義されたルートを使用します。ただし、管理トラフィックが管理ルーティング テーブルを使用し、データ トラフィックがデータ ルーティング テーブルを使用するように、ルーティングを分割することを選択できます。これらのトラフィックはそれぞれ以下のように分割されます。

管理トラフィック	データ トラフィック
• WebUI • SSH • SNMP • NTLM 認証（ドメイン コントローラによる） • 外部 DLP サーバによる ICAP 要求 • Syslogs • FTP プッシュ • DNS（設定可能） • アップデート/アップグレード/機能キー（設定可能）	• HTTP • HTTPS • FTP • WCCP ネゴシエーション • DNS（設定可能） • アップデート/アップグレード/機能キー（設定可能）

[ネットワーク（Network）] > [ルート（Routes）] ページのセクションの数は、分割ルーティングがイネーブルかどうかに応じて決まります。

- **管理トラフィックとデータ トラフィック用の個別のルート設定セクション**（分割ルーティングがイネーブルの場合）。管理インターフェイスを管理トラフィック専用に使用する場合（[M1 ポートをアプライアンス管理サービスのみに限定する（Restrict M1 port to appliance management services only）] がイネーブルの場合）、このページには、ルートを入力する 2 つのセクション（管理トラフィック用とデータ トラフィック用）が表示されます。

- **すべてのトラフィックに対して 1 つのルート設定セクション**（分割ルーティングがディセーブルの場合）。管理トラフィックとデータ トラフィックの両方に管理インターフェイスを使用する場合（[M1 ポートをアプライアンス管理サービスのみに限定する（Restrict M1 port to appliance management services only）] がディセーブルの場合）、このページには、Web セキュリティ アプライアンスから送信されるすべてのトラフィック（管理トラフィックとデータ トラフィックの両方）のルートを入力する 1 つのセクションが表示されます。

（注） ルート ゲートウェイは、それが設定されている管理インターフェイスまたはデータ インターフェイスと同じサブネット上に存在する必要があります。複数のポートがイネーブルになっている場合、Web プロキシは、データ トラフィック用に設定されているデフォルト ゲートウェイと同じネットワーク上のデータ インターフェイスでトランザクションを送信します。

関連項目

- 管理トラフィックとデータ トラフィックの分割ルーティングをイネーブルにするには、ネットワーク インターフェイスのイネーブル化または変更（3-24 ページ）を参照してください。

デフォルト ルートの変更

ステップ 1 [ネットワーク（Network）] > [ルート（Routes）] を選択します。

ステップ 2 必要に応じて、[管理（Management）] テーブルまたは [データ（Data）] テーブルの [デフォルト ルート（Default Route）] をクリックします（分割ルーティングがイネーブルになっていない場合は、統合された [管理/データ（Management/Data）] テーブル）。

ステップ 3 [ゲートウェイ（Gateway）] カラムで、編集するネットワーク インターフェイスに接続されているネットワークのネクスト ホップ上のコンピュータ システムの IP アドレスを入力します。

ステップ 4 変更を送信し、保存します。

ルートの追加

ステップ 1 [ネットワーク（Network）] > [ルート（Routes）] を選択します。

ステップ 2 ルートを作成するインターフェイスに対応する [ルートを追加（Add Route）] ボタンをクリックします。

ステップ 3 名前、宛先ネットワーク、およびゲートウェイを入力します。

ステップ 4 変更を送信し、保存します。

ルーティング テーブルの保存およびロード

ステップ 1 [ネットワーク（Network）] > [ルート（Routes）] を選択します。

ルート テーブルを保存するには、[ルート テーブルを保存（Save Route Table）] をクリックし、ファイルの保存場所を指定します。

保存されているルート テーブルをロードするには、[ルート テーブルをロード（Load Route Table）] をクリックし、ファイルを探して開き、変更を送信して確定します。

（注）　宛先アドレスが物理ネットワーク インターフェイスの 1 つと同じサブネット上にある場合、AsyncOS は同じサブネット内のネットワーク インターフェイスを使用してデータを送信します。ルーティング テーブルは参照されません。

ルートの削除

ステップ 1　[ネットワーク（Network）] > [ルート（Routes）] を選択します。

ステップ 2　該当するルートの [削除（Delete）] 列のチェックボックスをオンにします。

ステップ 3　[削除（Delete）] をクリックして確認します。

ステップ 4　変更を送信し、保存します。

関連項目

- ネットワーク インターフェイスのイネーブル化または変更（3-24 ページ）。

透過リダイレクションの設定

透過リダイレクション デバイスの指定

はじめる前に

- レイヤ 4 スイッチまたは WCCP v2 ルータにアプライアンスを接続します。

ステップ 1　[ネットワーク（Network）] > [トランスペアレント リダイレクション（Transparent Redirection）] を選択します。

ステップ 2　[デバイスの編集（Edit Device）] をクリックします。

ステップ 3　[タイプ（Type）] ドロップダウン リストから、トラフィックを透過的にアプライアンスにリダイレクトするデバイスのタイプを選択します。

ステップ 4　変更を送信し、保存します。

ステップ 5　WCCP v2 デバイスの場合は、以下の追加手順を実行します。

a. デバイスのマニュアルを参照して、WCCP デバイスを設定します。

b. WCCP サービスを追加します。

c. アプライアンスで IP スプーフィングがイネーブルになっている場合は、セカンド WCCP サービスを作成します。

関連項目

- アプライアンスの接続（3-8 ページ）。
- WCCP サービスの設定（3-31 ページ）。

WCCP サービスの設定

WCCP サービスは、WCCP v2 ルータにサービス グループを定義するアプライアンスの設定です。使用するサービス ID やポートなどの情報が含まれます。サービス グループを使用して、Web プロキシは WCCP ルータとの接続を確立し、ルータからリダイレクトされたトラフィックを処理することができます。

（注） 1 つのアプライアンスに最大 15 個のサービス グループを設定できます。

WCCP サービスの追加と編集

はじめる前に

- WCCP v2 ルータを使用するようにアプライアンスを設定します（透過リダイレクション デバイスの指定（3-30 ページ）を参照）。

ステップ 1 [ネットワーク（Network）] > [透過リダイレクション（Transparent Redirection）] を選択します。

ステップ 2 [サービスの追加（Add Service）] をクリックします。または、WCCP サービスを編集するには、[サービスプロファイル名（Service Profile Name）] 列にある WCCP サービスの名前をクリックします。

ステップ 3 以下の手順に従って、WCCP のオプションを設定します。

WCCP サービス オプション	説明
サービス プロファイル名（Service Profile Name）	WCCP サービスの名前。 **（注）** このオプションを空のままにして、標準サービス（下記を参照）を選択すると、「web_cache」という名前が自動的に割り当てられます。

WCCP サービス オプション	説明
サービス	ルータのサービス グループのタイプ。次から選択します。 [標準サービス（Standard service）]。このサービス タイプには、固定 ID「ゼロ」、固定リダイレクト方式「*宛先ポート別*」、固定宛先ポート「80」が割り当てられます。1 つの標準サービスのみ作成できます。アプライアンスに標準サービスがすでに存在している場合、このオプションはグレー表示されます。 [ダイナミックサービス（Dynamic service）]。このサービス タイプでは、カスタム ID、ポート番号、およびリダイレクト オプションとロード バランシング オプションを定義できます。WCCP ルータでサービスを作成するときは、ダイナミック サービスで指定したパラメータと同じパラメータを入力します。 ダイナミック サービスを作成する場合は、以下の情報を入力します。 • [サービス ID（Service ID）]。[ダイナミックサービス ID（Dynamic Service ID）] フィールドに 0 ～ 255 の任意の数字を入力できます。ただし、このアプライアンスには 15 個以上のサービス グループを設定することはできません。 • [ポート番号（Port number(s)）]。[ポート番号（Port Numbers）] フィールドにリダイレクトするトラフィックに最大 8 つのポート番号を入力します。 • [リダイレクションの基礎（Redirection basis）]。送信元ポートまたは宛先ポートに基づいてトラフィックをリダイレクトするように選択します。デフォルトは宛先ポートです。 **（注）** 透過リダイレクションと IP スプーフィングを使用してネイティブ FTP を設定するには、[ソースポート（リターン パス）に基づいてリダイレクト（Redirect based on source port (return path)）] を選択し、送信元ポートを 13007 に設定します。 • [ロード バランシングの基礎（Load balancing basis）]。ネットワークで複数の Web セキュリティ アプライアンスを使用している場合は、アプライアンス間にパケットを分散する方法を選択できます。サーバまたはクライアント アドレスに基づいてパケットを配布できます。クライアント アドレスを選択した場合、クライアントからのパケットは常に同じアプライアンスに配布されます。デフォルトはサーバ アドレスです。
ルータ IP アドレス	1 つまたは複数の WCCP 対応ルータの IPv4 または IPv6 アドレスを入力します。各ルータ固有の IPを使用します。マルチキャスト アドレスは入力できません。1 つのサービス グループ内に IPv4 と IPv6アドレスを混在させることはできません。
ルータ セキュリティ	このサービス グループのパスフレーズを要求するかどうかを選択します。イネーブルにした場合、そのサービス グループを使用するアプライアンスと WCCP ルータは同じパスフレーズを使用する必要があります。

WCCP サービス オプション	説明
詳細設定（Advanced）	**ロード バランシング方式。**複数の Web セキュリティ アプライアンス間においてルータがパケットのロード バランシングを実行する方法を決定します。次から選択してください。 • [マスクのみ許可（Allow Mask Only）]。WCCP ルータは、ルータのハードウェアを使用して決定を行います。この方式は、ハッシュ方式よりもルータのパフォーマンスを向上させます。ただし、すべての WCCP ルータがマスク割り当てをサポートしているわけではありません。 • [ハッシュのみ許可（Allow Hash Only）]。この方式は、ハッシュ関数に依存して、リダイレクションに関する決定を下します。この方式はマスク方式ほど効率的ではありませんが、ルータがこのオプションしかサポートしていない場合もあります。 • [ハッシュもしくはマスクを許可（Allow Hash or Mask）]。AsyncOS がルータと方式をネゴシエートできるようになります。ルータがマスクをサポートしている場合、AsyncOS はマスクを使用します。サポートしていない場合は、ハッシュが使用されます。 [マスクのカスタマイズ（Mask Customization）]。[マスクのみ許可（Allow Mask Only）] または [ハッシュのみ許可（Allow Hash Only）] を選択する場合、マスクをカスタマイズしたり、ビット数を指定したりできます。 • [カスタム マスク（最大 5 ビット）]。マスクを指定できます。Web インターフェイスは、提供するマスクに関連付けられたビット数を表示します。 • [システム生成マスク（System generated mask）]。システムがマスクを生成するように設定できます。任意で、システムにより生成されたマスクにビット数（最大 5 ビット）を指定できます。 [転送方式（Forwarding method）]。この方式では、リダイレクトされたパケットがルータから Web プロキシに転送されます。 [リターン方式（Return Method）]。この方式では、リダイレクトされたパケットが Web プロキシからルータに転送されます。 転送方式およびリターン方式では、以下のいずれかのメソッド タイプが使用されます。 • [レイヤ 2（L2）（Layer 2 (L2)）]。パケットの宛先 MAC アドレスをターゲット Web プロキシの MAC アドレスに置き換えることで、レイヤ 2 のトラフィックをリダイレクトします。L2 メソッドはハードウェア レベルで動作し、通常、最高のパフォーマンスを実現します。ただし、すべての WCCP ルータが L2 転送をサポートしているわけではありません。また、WCCP ルータは、（物理的に）直接接続されている Web セキュリティ アプライアンスとの L2 ネゴシエーションのみを許可します。 • [総称ルーティングカプセル化（GRE）（Generic Routing Encapsulation (GRE)）]。この方式は、GRE ヘッダーとリダイレクト ヘッダーを含む IP パケットをカプセル化することで、レイヤ 3 でトラフィックをリダイレクトします。GRE はソフトウェア レベルで動作し、パフォーマンスに影響する可能性があります。 • [L2 またはGRE（L2 or GRE）]。このオプションを指定すると、アプライアンスはルータがサポートしている方式を使用します。ルータとアプライアンスの両方が L2 と GRE をサポートする場合、アプライアンスは L2 を使用します。 ルータが直接アプライアンスに接続されていない場合、GRE を選択する必要があります。

ステップ 4　変更を送信し、保存します。

IP スプーフィングの WCCP サービスの作成

ステップ 1　Web プロキシで IP スプーフィングがイネーブルになっている場合は、2 つの WCCP サービスを作成します。標準の WCCP サービスを作成するか、宛先ポートに基づいてトラフィックをリダイレクトするダイナミック WCCP サービスを作成します。

ステップ 2　宛先ポートに基づいてトラフィックをリダイレクトするダイナミック WCCP サービスを作成します。

ステップ 1 で作成したサービスで使用されるポート番号、ルータ IP アドレス、ルータ セキュリティの設定と同じ設定を使用します。

（注）　シスコでは、リターン パスに使用する（送信元ポートに基づく）WCCP サービスには 90 ～ 97 のサービス ID 番号を使用することを推奨します。

関連項目

- Web プロキシ キャッシュ（4-5 ページ）。

VLAN の使用によるインターフェイス能力の向上

1 つまたは複数の VLAN を設定することで、組み込まれている物理インターフェイスの数を超えて、Cisco Web セキュリティ アプライアンスが接続可能なネットワークの数を増加できます。

VLAN は、「VLAN DDDD」という形式の名前を持つ動的な「データ ポート」として表示されます。「DDDD」は最大 4 桁の ID です（たとえば、VLAN 2、VLAN 4094 など）。AsyncOS は、最大 30 の VLAN をサポートします。

物理ポートは、VLAN に配置するために IP アドレスを設定する必要がありません。VLAN を作成した物理ポートに VLAN 以外のトラフィックを受信する IP アドレスを設定できるため、VLAN のトラフィックと VLAN 以外のトラフィックの両方を同じインターフェイスで受信できます。

VLAN は、管理および P1 データ ポートでのみ作成できます。

VSAN の設定と管理

VLAN の作成、編集、および削除を行うには、`etherconfig` コマンドを使用します。作成した VLAN は、CLI の `interfaceconfig` コマンドを使用して設定できます。

例 1：新しい VLAN の作成

この例では、P1 1 ポート上に 2 つの VLAN（VLAN 31 と VLAN 34）を作成します。

（注）　T1 または T2 インターフェイス上で VLAN を作成しないでください。

ステップ 1　CLI にアクセスします。

ステップ 2　以下の手順を実行します。

```
example.com> etherconfig
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- VLAN - View and configure VLANs.
- MTU - View and configure MTU.
[]> vlan

VLAN interfaces:

Choose the operation you want to perform:
- NEW - Create a new VLAN.
[]> new

VLAN ID for the interface (Ex: "34"):
[]> 34

Enter the name or number of the ethernet interface you wish bind to:
1. Management
2. P1
3. T1
4. T2
[1]> 2

VLAN interfaces:
1. VLAN   34 (P1)

Choose the operation you want to perform:
- NEW - Create a new VLAN.
- EDIT - Edit a VLAN.
- DELETE - Delete a VLAN.
[]> new

VLAN ID for the interface (Ex: "34"):
[]> 31

Enter the name or number of the ethernet interface you wish bind to:
1. Management
2. P1
3. T1
4. T2
[1]> 2

VLAN interfaces:
1. VLAN   31 (P1)
2. VLAN   34 (P1)

Choose the operation you want to perform:
- NEW - Create a new VLAN.
- EDIT - Edit a VLAN.
- DELETE - Delete a VLAN.
[]>
```

ステップ 3　変更を保存します。

例 2：VLAN 上の IP インターフェイスの作成

この例では、VLAN 34 イーサネット インターフェイス上に新しい IP インターフェイスを作成します。

（注）　インターフェイスに変更を加えると、アプライアンスとの接続が閉じることがあります。

ステップ 1　CLI にアクセスします。

ステップ 2　以下の手順を実行します。

```
example.com> interfaceconfig

Currently configured interfaces:
1. Management (10.10.1.10/24 on Management: example.com)
2. P1 (10.10.0.10 on P1: example.com)

Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
[]> new

IP Address (Ex: 10.10.10.10):
[]> 10.10.31.10

Ethernet interface:
1. Management
2. P1
3. VLAN 31
4. VLAN   34
[1]> 4

Netmask (Ex: "255.255.255.0" or "0xffffff00"):
[255.255.255.0]>

Hostname:
[]> v.example.com


Currently configured interfaces:
1. Management (10.10.1.10/24 on Management: example.com)
2. P1 (10.10.0.10 on P1: example.com)
3. VLAN   34 (10.10.31.10 on VLAN  34: v.example.com)

Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
[]>

example.com> commit
```

ステップ 3　変更を保存します。

関連項目

- ネットワーク インターフェイスのイネーブル化または変更（3-24 ページ）。
- TCP/IP トラフィック ルートの設定（3-28 ページ）。

リダイレクト ホスト名とシステム ホスト名

システム セットアップ ウィザードを実行すると、システム ホスト名とリダイレクト ホスト名が同一になります。しかし、sethostname コマンドを使用してシステムのホスト名を変更しても、リダイレクト ホスト名は変更されません。そのため、複数の設定に異なる値が含まれることになります。

AsyncOS は、エンドユーザ通知と応答確認にリダイレクト ホスト名を使用します。

システム ホスト名は、以下の領域でアプライアンスの識別に使用される完全修飾ホスト名です。

- コマンドライン インターフェイス（CLI）
- システム アラート
- Web セキュリティ アプライアンスが Active Directory ドメインに参加するときに、マシンの NetBIOS 名を作成する場合

システム ホスト名はインターフェイスのホスト名と直接対応しておらず、クライアントがアプライアンスに接続するために使用されません。

リダイレクト ホスト名の変更

ステップ 1　Web ユーザ インターフェイスで、[ネットワーク（Network）] > [認証（Authentication）] に移動します。

ステップ 2　[グローバル設定を編集（Edit Global Settings）] をクリックします。

ステップ 3　[リダイレクトホスト名（Redirect Hostname）] に新しい値を入力します。

システム ホスト名の変更

ステップ 1　CLI にアクセスします。

ステップ 2　Web セキュリティ アプライアンスの名前を変更するには、sethostname コマンドを使用します。

```
example.com> sethostname
example.com> hostname.com
example.com> commit
…
hostname.com>
```

ステップ 3　変更を保存します。

SMTP リレー ホストの設定

AsyncOS は、通知、アラート、Cisco IronPort カスタマー サポート要求など、システムにより生成された電子メール メッセージを定期的に送信します。デフォルトでは、AsyncOS はドメインの MX レコードにリストされている情報を使用して電子メールを送信します。ただし、アプライアンスが MX レコードにリストされているメール サーバに直接到達できない場合、アプライアンス上に少なくとも 1 つの SMTP リレー ホストを設定します。

（注）　Web セキュリティ アプライアンス は、MX レコードにリストされているメール サーバまたは設定済み SMTP リレー ホストと通信できない場合、電子メール メッセージを送信できず、ログ ファイルにメッセージを書き込みます。

1 つまたは複数の SMTP リレー ホストを設定できます。複数の SMTP リレー ホストを設定する場合、AsyncOS は、使用可能な最上位の SMTP リレー ホストを使用します。SMTP リレー ホストが使用できない場合、AsyncOS は、そのリスト 1 つ下のリレー ホストの使用を試みます。

SMTP リレー ホストの設定

ステップ 1　[ネットワーク（Network）] > [内部 SMTP リレー（Internal SMTP Relay）] 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。

ステップ 3　[内部 SMTP リレー（Internal SMTP Relay）] の設定を完成させます。

プロパティ	説明
リレーのホスト名または IP アドレス（Relay Hostname or IP Address）	SMTP リレーに使用するホスト名または IP アドレス。
[ポート（Port）]	SMTP リレーに接続するためのポート。このプロパティを空欄にした場合、アプライアンスはポート 25 を使用します。
SMTP への接続に使用するルーティング テーブル（Routing Table to Use for SMTP）	SMTP リレーへの接続に使用するアプライアンスのネットワーク インターフェイス（管理またはデータのいずれか）に関連付けられているルーティング テーブル。リレー システムと同じネットワークにあるインターフェイスを選択します。

ステップ 4　（任意）[行を追加（Add Row）] をクリックして別の SMTP リレー ホストを追加します。

ステップ 5　変更を送信し、保存します。

DNS の設定

AsyncOS for Web では、インターネット ルート DNS サーバまたはユーザ独自の DNS サーバを使用できます。インターネット ルート サーバを使用する場合、特定のドメインに使用する代替サーバを指定できます。代替 DNS サーバは単一のドメインに適用されるため、当該ドメインの権威サーバ（最終的な DNS レコードを提供）である必要があります。

- スプリット DNS（3-39 ページ）
- DNS キャッシュのクリア（3-39 ページ）
- DNS 設定の編集（3-39 ページ）

スプリット DNS

AsyncOS は、内部サーバが特定のドメインに設定され、外部またはルート DNS サーバが他のドメインに設定されたスプリット DNS をサポートします。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。

DNS キャッシュのクリア

はじめる前に

- このコマンドを使用すると、キャッシュの再投入中に一時的にパフォーマンスが低下することがあるので注意してください。

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

ステップ 2　[DNS キャッシュを消去（Clear DNS Cache）] をクリックします。

DNS 設定の編集

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。

ステップ 3　必要に応じて、DNS 設定値を設定します。

プロパティ	説明
DNS サーバ（DNS Server(s)）	[これらの DNS サーバを使用（Use these DNS Servers）]。アプライアンスがホスト名の解決に使用できるローカル DNS サーバ。 [インターネットのルート DNS サーバを使用（Use the Internet's Root DNS Servers）]。アプライアンスがネットワーク上の DNS サーバにアクセスできない場合に、ドメイン名サービス ルックアップにインターネットのルート DNS サーバを使用することを選択できます。 **（注）** インターネット ルート DNS サーバは、ローカル ホスト名を解決しません。アプライアンスでローカル ホスト名を解決する必要がある場合は、ローカル DNS サーバを使用して解決するか、コマンドライン インターフェイスからローカル DNS に適切なスタティック エントリを追加する必要があります。 [優先代替 DNS サーバ（オプション）（Alternate DNS servers Overrides (Optional)）]。特定のドメイン用の権威 DNS サーバ
DNS トラフィック用ルーティング テーブル（Routing Table for DNS Traffic）	DNS サービスがルート トラフィックをルーティングする際に経由するインターフェイスを指定します。

プロパティ	説明
IP アドレス バージョン設定（IP Address Version Preference）	DNS サーバが IPv4 と IPv6 の両方のアドレスを提供する場合、AsyncOS はこの設定を使用して IP アドレスのバージョンを選択します。 （注）　AsyncOS は、透過的 FTP 要求のバージョン設定に従いません。
DNS 逆引きタイムアウト（Wait Before Timing out Reverse DNS Lookups）	無応答逆引き DNS ルックアップがタイムアウトするまでの待機時間（秒単位）。
ドメイン検索リスト（Domain Search List）	簡易ホスト名（「.」記号がないホスト名）宛てに要求を送信する際に使用される DNS ドメイン検索リスト。ドメイン名を加えたホスト名に一致する DNS が存在するどうかを調べるために、指定されたドメインが入力順に照合されます。

ステップ 4　変更を送信し、保存します。

関連項目

- TCP/IP トラフィック ルートの設定（3-28 ページ）
- IP アドレスのバージョン（3-23 ページ）

接続、インストール、設定に関するトラブルシューティング

- フェールオーバーに関する問題（A-4 ページ）
- アップストリーム プロキシが基本クレデンシャルを受け取らない（A-14 ページ）
- クライアント要求がアップストリーム プロキシで失敗する（A-15 ページ）
- 最大ポート エントリ数（A-16 ページ）

Web 要求の代行受信

Web 要求の代行受信の概要

Web Security Appliance は、ネットワーク上のクライアントまたは他のデバイスから転送された要求を代行受信します。

アプライアンスは他のネットワーク デバイスと連携してトラフィックを代行受信します。そのようなデバイスとして、一般的なスイッチ、トランスペアレント リダイレクション デバイス、、その他のプロキシ サーバまたは Web Security Appliance などがあげられます。

Web 要求の代行受信のためのタスク

手順	タスク	関連項目および手順へのリンク
1.	ベスト プラクティスを検討する。	• Web 要求の代行受信のベスト プラクティス（4-2 ページ）
2.	（任意）以下のネットワーク関連のフォローアップ タスクを実行します。 • アップストリーム プロキシを接続および設定する。 • ネットワーク インターフェイス ポリシーを設定する。 • 透過リダイレクション デバイスを設定する。 • TCP/IP ルートを設定する。 • VLAN の設定。	• アップストリーム プロキシ（3-20 ページ） • ネットワーク インターフェイス（3-23 ページ） • 透過リダイレクションの設定（3-30 ページ） • TCP/IP トラフィック ルートの設定（3-28 ページ） • VLAN の使用によるインターフェイス能力の向上（3-34 ページ）

手順	タスク	関連項目および手順へのリンク
3.	(任意)次の Web プロキシのフォローアップ タスクを実行する。 • 転送モードまたは透過モードで動作するように Web プロキシを設定する。 • 代行受信するプロトコル タイプに追加のサービスが必要かどうかを決定。 • Web プロキシ キャッシュの管理。 • カスタム Web 要求ヘッダーの使用。 • 一部の要求に対してプロキシをバイパス。	• Web 要求を代行受信するための Web プロキシ オプション(4-2 ページ) • Web プロキシの設定(4-3 ページ) • Web 要求を代行受信するための Web プロキシ オプション(4-2 ページ) • Web プロキシ キャッシュ(4-5 ページ) • Web プロキシのバイパス(4-9 ページ)
4.	以下のクライアント タスクを実行します。 • クライアントが Web プロキシに要求をリダイレクトする方法を決定。 • クライアントとクライアント リソースの設定。	• Web 要求をリダイレクトするためのクライアント オプション(4-10 ページ)

Web 要求の代行受信のベスト プラクティス

- 必要なプロキシ サービスのみをイネーブルにします。
- Web セキュリティ アプライアンスで定義されているすべての WCCP サービスに対して、同じ転送方式とリターン方式(L2 または GRE)を使用します。これによって、プロキシ バイパス リストが確実に機能します。
- ユーザが企業ネットワークの外部から PAC ファイルにアクセスできないことを確認します。これによって、モバイル ワーカーは、企業ネットワーク上にいるときは Web プロキシを使用し、それ以外の場合は Web サーバに直接接続できます。
- 信頼できるダウンストリーム プロキシまたはロード バランサからの X-Forwarded-For ヘッダーのみが Web プロキシで許可されるようにします。
- 当初は明示的な転送だけを使用していた場合でも、Web プロキシをデフォルトの透過モードのままにしておきます。透過モードでは、明示的な転送要求も許可されます。

Web 要求を代行受信するための Web プロキシ オプション

単独では、Web プロキシは HTTP(FTP over HTTP を含む)および HTTPS を使用する Web 要求を代行受信できます。プロトコル管理を向上させるために、さらに次のプロキシ モジュールを利用できます。

- **HTTPS プロキシ**。HTTPS プロキシは HTTPS トラフィックの復号化をサポートしているので、Web プロキシは、暗号化されていない HTTPS 要求をコンテンツ分析のためにポリシーに渡すことができます。

(注)　透過モードでは、HTTPS プロキシがイネーブルでない場合、Web プロキシは透過的にリダイレクトされたすべての HTTPS 要求をドロップします。透過的にリダイレクトされた HTTPS 要求がドロップされた場合、その要求のログ エントリは作成されません。

これらの追加プロキシのそれぞれを機能させるには、Web プロキシが必要です。Web プロキシをディセーブルにすると、これらをイネーブルにできなくなります。

（注）　Web プロキシはデフォルトでイネーブルになります。デフォルトでは、他のプロキシはすべてディセーブルになります。

Web プロキシの設定

はじめる前に

- Web プロキシをイネーブルにします。

ステップ 1　[セキュリティサービス（Security Services）] > [Web プロキシ（Web Proxy）] 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。

ステップ 3　必要に応じて基本的な Web プロキシ設定項目を設定します。

プロパティ	説明
プロキシを設定する HTTP ポート（HTTP Ports to Proxy）	Web プロキシが HTTP 接続をリッスンするポート
HTTP CONNECT ポート（HTTP CONNECT Ports）	ポート アプリケーションは、HTTP 経由で発信トラフィックをトンネリングする場合に使用が許可されます。
キャッシング（Caching）	Web プロキシによるキャッシングをイネーブルにするかディセーブルにするかを指定します。 Web プロキシは、パフォーマンスを向上させるためにデータをキャッシュします。
プロキシ モード（Proxy mode）	• [転送（Forward）]: クライアント ブラウザがインターネット ターゲットを指定できるようにします。Web プロキシを使用するように各 Web ブラウザを個々に設定する必要があります。このモードでは、Web プロキシは明示的に転送された Web 要求のみを代行受信できます。 • [透過（Transparent）]（推奨）: Web プロキシがインターネット ターゲットを指定できるようにします。このモードでは、Web プロキシは、透過的または明示的に転送された Web 要求を代行受信できます。

ステップ 4　必要に応じて Web プロキシの詳細設定を完了します。

プロパティ	説明
永続的接続のタイムアウト（Persistent Connection Timeout）	トランザクションが完了し、その他のアクティビティが検出されなかった後に、Web プロキシがクライアントまたはサーバとの接続を開いたままにしておく最大時間（秒単位）。 • [クライアント側（Client side）]。クライアントとの接続のタイムアウト値。 • [サーバ側（Server side）]。サーバとの接続のタイムアウト値。 これらの値を大きくすると、接続が開いたままになっている時間が延長され、接続の開閉に費やされるオーバーヘッドが低減します。ただし、永続的な同時接続の数が最大数に達した場合に Web Proxy が新しい接続を開く機能も低下します。 シスコは、デフォルト値を維持することを推奨します。
使用中接続タイムアウト（In-Use Connection Timeout）	現在のトランザクションが完了していないときに、Web プロキシがアイドル状態のクライアントまたはサーバからのデータをさらに待機する最大時間（秒単位）。 • [クライアント側（Client side）]。クライアントとの接続のタイムアウト値。 • [サーバ側（Server side）]。サーバとの接続のタイムアウト値。
同時永続的接続（サーバ最大数）（Simultaneous Persistent Connections (Server Maximum Number)）	Web プロキシ サーバがサーバに対して開いたままにする接続（ソケット）の最大数。
ヘッダーの生成（Generate Headers）	要求に関する情報をエンコードするヘッダーを生成して追加します。 • **X-Forwarded-For** ヘッダーは、HTTP 要求を発信したクライアントの IP アドレスをエンコードします。 **（注）** ヘッダーの転送をオン/オフするには、`advancedproxyconfig` CLI コマンドの Miscellaneous オプション「HTTP X-Forwarded-For ヘッダーを通過させますか?（Do you want to pass HTTP X-Forwarded-For headers?）」を使用します。 **（注）** 明示的な転送アップストリーム プロキシを使用して、プロキシ認証によりユーザ認証やアクセス制御を管理するには、これらのヘッダーを転送する必要があります。 • **Request Side VIA** ヘッダーは、クライアントからサーバへの要求が通過するプロキシをエンコードします。 • **Response Side VIA** ヘッダーは、サーバからクライアントへの要求が通過するプロキシをエンコードします。

Received ヘッダーの使用（Use Received Headers）	アップストリーム プロキシとして展開された Web プロキシが、ダウンストリームプロキシから送信された X-Forwarded-For ヘッダーを使用してクライアントを識別できるようにします。Web プロキシは、リストに含まれていない送信元からの X-Forwarded-For ヘッダーの IP アドレスを受け入れません。 これをイネーブルにする場合は、ダウンストリーム プロキシまたはロード バランサの IP アドレスが必要です（サブネットやホスト名は入力できません）。

ステップ 5　変更を送信し、保存します。

関連項目

- Web プロキシ キャッシュ（4-5 ページ）。
- 透過リダイレクションの設定（3-30 ページ）

Web プロキシ キャッシュ

Web プロキシは、パフォーマンスを向上させるためにデータをキャッシュします。AsyncOS には「セーフ」から「アグレッシブ」の範囲の定義済みキャッシュ モードがあり、またカスタマイズしたキャッシングも使用できます。キャッシュ対象から特定の URL を除外することもできます。これを行うには、その URL をキャッシュから削除するか、無視するようにキャッシュを設定します。

Web プロキシ キャッシュのクリア

ステップ 1　[セキュリティサービス（Security Services）] > [Web プロキシ（Web Proxy）] を選択します。

ステップ 2　[キャッシュを消去（Clear Cache）] をクリックしてアクションを確定します。

Web プロキシ キャッシュからの URL の削除

ステップ 1　CLI にアクセスします。

ステップ 2　`webcache > evict` コマンドを使用して、必要なキャッシング エリアにアクセスします。

```
example.com> webcache

Choose the operation you want to perform:
- EVICT - Remove URL from the cache
- DESCRIBE - Describe URL cache status
- IGNORE - Configure domains and URLs never to be cached
[]> evict

Enter the URL to be removed from the cache.
[]>
```

ステップ 3　キャッシュから削除する URL を入力します。

（注）　URL にプロトコルが含まれていない場合は、URL に http:// が追加されます（たとえば、www.cisco.com は http://www.cisco.com となります）。

Web プロキシによってキャッシュしないドメインまたは URL の指定

ステップ 1　CLI にアクセスします。

ステップ 2　webcache -> ignore コマンドを使用して、必要なサブメニューにアクセスします。

```
example.com> webcache

Choose the operation you want to perform:
- EVICT - Remove URL from the cache
- DESCRIBE - Describe URL cache status
- IGNORE - Configure domains and URLs never to be cached
[]> ignore

Choose the operation you want to perform:
- DOMAINS - Manage domains
- URLS - Manage urls
[]>
```

ステップ 3　管理するアドレス タイプを入力します（DOMAINS または URLS）。

```
[]> urls

Manage url entries:

Choose the operation you want to perform:
- DELETE - Delete entries
- ADD - Add new entries
- LIST - List entries
[]>
```

ステップ 4　**add** と入力して新しいエントリを追加します。

```
[]> add

Enter new url values; one on each line; an empty line to finish
[]>
```

ステップ 5　以下の例のように、1 行に 1 つずつ、ドメインまたは URL を入力します。

```
Enter new url values; one on each line; an empty line to finish
[]> www.example1.com

Enter new url values; one on each line; an empty line to finish
[]>
```

ドメインまたは URL を指定する際に、特定の正規表現（regex）文字を含めることができます。DOMAINS オプションでは、前にピリオドを付けることで、キャッシュ対象からドメインとそのサブドメイン全体を除外できます。たとえば、google.com ではなく、.google.com と入力すると、www.google.com、docs.google.com などを除外することができます。

URLS オプションでは、正規表現文字の全一式を使用できます。正規表現の使用方法については、Regular Expressions（9-21 ページ）を参照してください。

ステップ 6　値の入力を終了したら、メイン コマンドライン インターフェイスに戻るまで Enter キーを押します。

ステップ 7　変更を保存します。

Web プロキシのキャッシュ モードの選択

ステップ 1　CLI にアクセスします。

ステップ 2　advancedproxyconfig -> caching コマンドを使用して、必要なサブメニューにアクセスします。

```
example.com> advancedproxyconfig

Choose a parameter group:
- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters
[]> caching

Enter values for the caching options:

The following predefined choices exist for configuring advanced caching
options:
1. Safe Mode
2. Optimized Mode
3. Aggressive Mode
4. Customized Mode
Please select from one of the above choices:
[2]>
```

ステップ 3　必要な Web プロキシ キャッシュ設定に対応する番号を入力します。

入力	モード	説明
1	セーフ	他のモードと比較して、キャッシングが最も少なく、RFC #2616 には最大限準拠します。
2	最適化	キャッシングと RFC #2616 への準拠が適度です。セーフ モードと比較した場合、Last-Modified ヘッダーが存在するときにキャッシング時間が指定されていない場合に、最適化モードでは Web プロキシがオブジェクトをキャッシュします。Web プロキシは、ネガティブ応答をキャッシュします。

3	アグレッシブ	キャッシングが最も多く、RFC #2616 への準拠は最小限です。最適化モードと比較した場合、アグレッシブ モードでは、認証済みコンテンツ、ETag の不一致、および Last-Modified ヘッダーのないコンテンツがキャッシュされます。Web プロキシは非キャッシュ パラメータを無視します。
4	カスタマイズド モード	各パラメータを個々に設定します。

ステップ 4　オプション 4（カスタマイズ モード）を選択した場合は、各カスタム設定の値を入力します（または、デフォルト値のままにします）。

ステップ 5　メイン コマンド インターフェイスに戻るまで、**Enter** キーを押します。

ステップ 6　変更を保存します。

関連項目

- Web プロキシ キャッシュ（4-5 ページ）。

Web プロキシのカスタム ヘッダー

特定の発信トランザクションにカスタム ヘッダーを追加することにより、宛先サーバによる特別な処理を要求できます。たとえば、YouTube for Schools と関係がある場合、カスタム ヘッダーを使用して、YouTube.com へのトランザクション要求を自身のネットワークから発信された、特別な処理を必要とする要求として識別させることができます。

Web 要求へのカスタム ヘッダーの追加

ステップ 1　CLI にアクセスします。

ステップ 2　`advancedproxyconfig -> customheaders` コマンドを使用して、必要なサブメニューにアクセスします。

```
example.com> advancedproxyconfig

Choose a parameter group:
- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters
[]> customheaders

Currently defined custom headers:
```

```
Choose the operation you want to perform:
- DELETE - Delete entries
- NEW - Add new entries
- EDIT - Edit entries
[]>
```

ステップ 3　次のように、必要なサブコマンドを入力します。

オプション	説明
削除（Delete）	指定するカスタム ヘッダーを削除します。コマンドで返されたリストのヘッダーに関連付けられている番号を使用して削除するヘッダーを指定します。
新規作成（New）	指定するドメインの使用に提供するヘッダーを作成します。 ヘッダーの例： X-YouTube-Edu-Filter: ABCD1234567890abcdef （この場合の値は、YouTube で提供される固有キーです）。 ドメインの例： youtube.com
編集（Edit）	既存のヘッダーを指定したヘッダーと置き換えます。コマンドで返されたリストのヘッダーに関連付けられている番号を使用して削除するヘッダーを指定します。

ステップ 4　メイン コマンド インターフェイスに戻るまで、Enter キーを押します。

ステップ 5　変更を保存します。

Web プロキシのバイパス

Web プロキシのバイパス（Web 要求の場合）

特定のクライアントからの透過的要求や特定の宛先への透過的要求が Web プロキシをバイパスするように、Web Security Appliance を設定できます。

Web プロキシをバイパスすることによって、以下のことが可能になります。

- HTTP ポートを使用しているが、適切に機能しない HTTP 非対応の（または独自の）プロトコルが、プロキシ サーバに接続するときに干渉されないようにします。
- ネットワーク内の特定のマシンからのトラフィックが、マルウェアのテスト マシンなど、ネットワーク プロキシおよび組み込みのセキュリティ保護をすべてバイパスすることを確認します。

バイパスは、Web プロキシに透過的にリダイレクトされる要求に対してのみ機能します。Web プロキシは、透過モードでも転送モードでも、クライアントから明示的に転送されたすべての要求を処理します。

Web プロキシのバイパス設定（Web 要求の場合）

ステップ 1　[Web セキュリティマネージャ（Web Security Manager）] > [バイパス設定（Bypass Settings）] を選択します。

ステップ 2　[バイパス設定の編集（Edit Bypass Settings）] をクリックします。

ステップ 3　Web プロキシをバイパスするアドレスを入力します。

ステップ 4　変更を送信し、保存します。

Web プロキシのバイパス設定（アプリケーションの場合）

ステップ 1　[Web セキュリティマネージャ（Web Security Manager）] > [バイパス設定（Bypass Settings）] を選択します。

ステップ 2　[アプリケーションのスキップ設定を編集（Edit Application Bypass Settings）] をクリックします。

ステップ 3　スキャンをバイパスするアプリケーションを選択します。

ステップ 4　変更を送信し、保存します。

Web プロキシ使用規約

Web Security Appliance を設定して、Web アクティビティのフィルタリングとモニタリングが行われていることをユーザに通知できます。アプライアンスは、ユーザが初めてブラウザにアクセスしたときに、一定時間の経過後、エンド ユーザ確認ページを表示します。エンド ユーザ確認ページが表示されたら、ユーザはリンクをクリックして、要求した元のサイトまたは他の Web サイトにアクセスする必要があります。

関連項目

- エンドユーザへのプロキシ アクションの通知

Web 要求をリダイレクトするためのクライアント オプション

クライアントから Web プロキシに明示的に要求を転送することを選択した場合は、それを実行するためのクライアントの設定方法も指定する必要があります。以下の方法から選択します。

- **明示的な設定を使用してクライアントを設定する。**Web プロキシのホスト名とポート番号を使ってクライアントを設定します。設定方法の詳細については、個々のクライアントのマニュアルを参照してください。

（注）　デフォルトでは、Web プロキシ ポートはポート番号 80 と 3128 を使用します。クライアントはいずれかのポートを使用できます。

要求の代替受信に関するトラブルシューティング

エンドユーザ クレデンシャルの取得

エンドユーザ クレデンシャルの取得の概要

サーバ タイプ/レルム	認証方式	サポートされるネットワーク プロトコル	注記
Active Directory	Kerberos NTLMSSP 基本	HTTP、HTTPS ネイティブ FTP、FTP over HTTP SOCKS（基本認証）	Kerberos は標準モードでのみサポートされます。クラウド コネクタ モードではサポートされません。
LDAP	基本	HTTP、HTTPS ネイティブ FTP、FTP over HTTP SOCKS	—

認証タスクの概要

手順	タスク	関連項目および手順へのリンク
1.	認証レルムを作成する。	• Active Directory 認証レルムの作成（NTLMSSP および基本）（5-15 ページ） • LDAP 認証レルムの作成（5-18 ページ）
2.	グローバル認証を設定する。	• グローバル認証の設定（5-23 ページ）
3.	外部認証を設定する。 外部 LDAP または RADIUS サーバからユーザを認証できます。	• 外部認証（5-11 ページ）
4.	（任意）追加の認証レルムを作成して順序を決定する。 使用する予定の各認証プロトコルとスキームの組み合わせに対して、少なくとも 1 つの認証レルムを作成する。	• 認証シーケンスの作成（5-29 ページ）
5.	（任意）クレデンシャルの暗号化を設定する。	• クレデンシャル暗号化の設定（5-39 ページ）
6.	認証要件に基づいてユーザとクライアント ソフトウェアを分類する識別プロファイルを作成する。	• ユーザおよびクライアント ソフトウェアの分類（6-3 ページ）
7.	識別プロファイルの作成対象となったユーザとユーザ グループからの Web 要求を管理するポリシーを作成する。	• Managing Web Requests Through Policies Best Practices（10-3 ページ）

認証に関するベスト プラクティス

- できる限り少数の Active Directory レルムを作成します。多数の Active Directory レルムを作成すると、認証で追加のメモリが必要になります。
- NTLMSSP を使用する場合は、Web セキュリティ アプライアンス またはアップストリーム プロキシ サーバを使用してユーザを認証します（両方は使用できません）。（Web セキュリティ アプライアンスを推奨）
- Kerberos を使用する場合は、Web セキュリティ アプライアンスを使用して認証します。
- 最適なパフォーマンスを得るには、1 つのレルムを使用して同じサブネット上のクライアントを認証します。
- 一部のユーザ エージェントには、通常の動作に悪影響を及ぼすマシン クレデンシャルや認証失敗の問題があることが判明されています。これらのユーザ エージェントとの認証をバイパスする必要があります。問題のあるユーザ エージェントの認証のバイパス（5-31 ページ）を参照してください。

認証の計画

Active Directory/Kerberos

明示的な転送	透過、IP ベースのキャッシング	透過、Cookie ベースのキャッシング
利点： • NTLM と比べた場合、パフォーマンスと相互運用性が向上 • ドメインに参加している Windows クライアントと非 Windows クライアントの両方と連携 • すべてのブラウザ、および他のほとんどのアプリケーションでサポートされている • RFC ベース • 最小限のオーバーヘッド • HTTPS（CONNECT）要求で使用できる • パスフレーズが認証サーバに送信されないため、より安全である • ホストや IP アドレスではなく、接続が認証される • クライアント アプリケーションが Web セキュリティ アプライアンスを信頼するように設定されている場合に、Active Directory 環境で真のシングル サインオンを実現	利点： • NTLM と比べた場合、パフォーマンスと相互運用性が向上 • ドメインに参加している Windows クライアントと非 Windows クライアントの両方と連携 • すべての主要ブラウザで使用できる • 認証をサポートしていないユーザ エージェントを使用する場合、ユーザはサポートされるブラウザで最初に認証されるだけでよい • オーバーヘッドが比較的低い • ユーザが以前に HTTP 要求で認証されている場合は、HTTPS 要求で使用できる	利点： • NTLM と比べた場合、パフォーマンスと相互運用性が向上 • ドメインに参加している Windows クライアントと非 Windows クライアントの両方と連携 • すべての主要ブラウザで使用できる • 認証が、ホストや IP アドレスではなく、ユーザに関連付けられる 欠点： • Cookie はドメイン固有であるため、新規の各 Web ドメインで認証プロセス全体が必要 • Cookie をイネーブルにする必要がある • HTTPS 要求で使用できない

Active Directory/Basic

明示的な転送	透過、IP ベースのキャッシング	透過、Cookie ベースのキャッシング
利点: • すべてのブラウザ、および他のほとんどのアプリケーションでサポートされている • RFC ベース • 最小限のオーバーヘッド • HTTPS（CONNECT）要求で使用できる • パスフレーズが認証サーバに送信されないため、より安全である • ホストや IP アドレスではなく、接続が認証される • クライアント アプリケーションが Web セキュリティ アプライアンスを信頼するように設定されている場合に、Active Directory 環境で真のシングル サインオンを実現 欠点: • すべての要求でパスフレーズがクリア テキスト（Base64）として送信される • シングル サインオンなし • 中程度のオーバーヘッド：新規の接続ごとに再認証が必要 • 主に Windows および主要ブラウザでのみサポート	利点: • すべての主要ブラウザで使用できる • 認証をサポートしていないユーザ エージェントを使用する場合、ユーザはサポートされるブラウザで最初に認証されるだけでよい • オーバーヘッドが比較的低い • ユーザが以前に HTTP 要求で認証されている場合は、HTTPS 要求で使用できる 欠点: • 認証クレデンシャルが、ユーザではなく、IP アドレスに関連付けられる（Citrix および RDP 環境では使用できず、ユーザが IP アドレスを変更した場合も使用できない） • シングル サインオンなし • パスフレーズがクリア テキスト（Base64）として送信される	利点: • すべての主要ブラウザで使用できる • 認証が、ホストや IP アドレスではなく、ユーザに関連付けられる 欠点: • Cookie はドメイン固有であるため、新規の各 Web ドメインで認証プロセス全体が必要 • Cookie をイネーブルにする必要がある • HTTPS 要求で使用できない • シングル サインオンなし • パスフレーズがクリア テキスト（Base64）として送信される

Active Directory/NTLMSSP

明示的な転送	透過
利点: • パスフレーズが認証サーバに送信されないため、より安全である • ホストや IP アドレスではなく、接続が認証される • クライアント アプリケーションが Web セキュリティ アプライアンスを信頼するように設定されている場合に、Active Directory 環境で真のシングル サインオンを実現 欠点: • 中程度のオーバーヘッド:新規の接続ごとに再認証が必要 • 主に Windows および主要ブラウザでのみサポート	利点: • より柔軟性が高い 透過 NTLMSSP 認証は透過基本認証と似ています。ただし、Web プロキシはクライアントとの通信に、基本的なクリア テキストのユーザ名とパスフレーズではなく、チャレンジ/レスポンス認証を使用します。 透過 NTLM 認証を使用する利点と欠点は、透過基本認証を使用する場合と同様です。ただし、**透過 NTLM 認証には、パスフレーズが認証サーバに送信されないというさらなる利点があり、クライアント アプリケーションが Web セキュリティ アプライアンス を信頼するように設定されている場合はシングル サインオンを実現できます。**

LDAP/基本

明示的な転送	透過
利点: • RFC ベース • NTLM よりも多くのブラウザをサポート • 最小限のオーバーヘッド • HTTPS（CONNECT）要求で使用できる 欠点: • シングル サインオンなし • すべての要求でパスフレーズがクリア テキスト（Base64）として送信される 回避策: • 認証の失敗（5-31 ページ）	利点: • 明示的な転送よりも柔軟。 • NTLM よりも多くのブラウザをサポート • 認証をサポートしていないユーザ エージェントを使用する場合、ユーザはサポートされるブラウザで最初に認証されるだけでよい • オーバーヘッドが比較的低い • ユーザが以前に HTTP 要求で認証されている場合は、HTTPS 要求で使用できる 欠点: • シングル サインオンなし • パスフレーズがクリア テキスト（Base64）として送信される • 認証クレデンシャルが、ユーザではなく、IP アドレスに関連付けられる（Citrix および RDP 環境では使用できず、ユーザが IP アドレスを変更した場合も使用できない） 回避策: • 認証の失敗（5-31 ページ）

ユーザの透過的識別

従来、ユーザの識別および認証では、ユーザにユーザ名とパスフレーズの入力を求めていました。ユーザが入力したクレデンシャルは認証サーバによって認証され、その後、Web プロキシが、認証されたユーザ名に基づいてトランザクションに適切なポリシーを適用します。

しかし、Web セキュリティ アプライアンスは、ユーザを透過的に認証するように設定することができます。つまり、エンドユーザにクレデンシャルを要求しません。透過的な識別では、別の信頼できるソースによってユーザが認証済みであると想定し、そのソースから取得したクレデンシャルを使用してユーザを認証して、適切なポリシーを適用します。

ユーザを透過的に識別して以下を実行する場合があります。

- ユーザがネットワーク上のプロキシの存在を意識しないように、シングル サイン オン環境を構築する。
- エンド ユーザに認証プロンプトを表示できないクライアント アプリケーションからのトランザクションに、認証ベースのポリシーを適用する。

ユーザの透過的識別は、Web プロキシがユーザ名を取得して識別プロファイルを割り当てる方法にのみ影響を与えます。ユーザ名を取得して識別プロファイルを割り当てた後、Web プロキシは、識別プロファイルの割り当て方法に関係なく、通常どおり他のすべてのポリシーを適用します。

透過認証が失敗した場合、トランザクションを処理する方法を設定できます。ユーザにゲスト アクセスを許可するか、またはユーザに認証プロンプトを表示することができます。

透過的ユーザ ID の失敗によりエンド ユーザに認証プロンプトが表示され、ユーザが無効なクレデンシャルにより認証に失敗した場合、ユーザのゲスト アクセスを許可するかどうかを選択できます。

（注）　再認証をイネーブルにしたが、URL フィルタリングによってトランザクションがブロックされている場合、エンド ユーザ通知ページが表示され、別のユーザとしてログインするオプションが提供されます。ユーザがリンクをクリックすると、認証を求めるプロンプトが表示されます。詳細については、認証の失敗：異なるクレデンシャルによる再認証の許可（5-35 ページ）を参照してください。

透過的ユーザ識別について

透過的ユーザ識別は以下の方式で使用できます。

- [ISE によってユーザを透過的に識別（Transparently identify users with ISE）]：Identity Services Engine（ISE）サービスがイネーブルの場合に使用可能（[ネットワーク（Network）] > [Identity Services Engine]）。これらのトランザクションの場合、ユーザ名と関連するセキュリティ グループ タグは Identity Services Engine サーバから取得されます。Tasks for Certifying and Integrating the ISE Service（8-3 ページ）を参照してください。
- [ASA によってユーザを透過的に識別（Transparently identify users with ASA）]：ユーザは、Cisco 適応型セキュリティ アプライアンスから受信した現在の IP アドレス対ユーザ名のマッピングによって識別されます（リモート ユーザのみ）。このオプションは、AnyConnect Secure Mobility がイネーブルになっており、ASA と統合されている場合に使用できます。ユーザ名は ASA から取得され、関連するディレクトリ グループは Web セキュリティ アプライアンスで指定された認証レルムまたはシーケンスから取得されます。Remote Users（10-20 ページ）を参照してください。

- [認証レルムによってユーザを透過的に識別（Transparently identify users with authentication realms）]：このオプションは、1 つ以上の認証レルムが、以下のいずれかの認証サーバを使用して透過的識別をサポートするように設定されている場合に使用できます。
  - Active Directory：NTLM または Kerberos 認証レルムを作成し、透過的ユーザ識別をイネーブルにします。また、Cisco Context Directory Agent などの Active Directory エージェントを個別に展開する必要があります。詳細については、Active Directory による透過的ユーザ識別（5-7 ページ）を参照してください。
  - LDAP：eDirectory として設定した LDAP 認証レルムを作成し、透過的ユーザ識別をイネーブルにします。詳細については、LDAP による透過的ユーザ識別（5-8 ページ）を参照してください。

  AsyncOS for Web は eDirectory または Active Directory エージェントと定期的に通信して、認証されたユーザ名と現在の IP アドレスを照合するマッピングを保守します。

Active Directory による透過的ユーザ識別

Active Directory は、Web セキュリティ アプライアンス などの他のシステムから簡単に照会できる形式でユーザ ログイン情報を記録しません。Cisco Context Directory Agent（CDA）などの Active Directory エージェントは、認証済みユーザの情報を Active Directory セキュリティ イベント ログで照会する必要があります。

AsyncOS for Web は Active Directory エージェントと通信して、IP アドレス対ユーザ名のマッピングのローカル コピーを保守します。AsyncOS for Web は IP アドレスをユーザ名に関連付ける必要がある場合、最初にマッピングのローカル コピーをチェックします。一致が見つからない場合、Active Directory エージェントに照会して一致するものを見つけます。

Active Directory エージェントのインストールと設定の詳細については、Web セキュリティ アプライアンスに情報を提供する Active Directory エージェントの設定（5-8 ページ）を参照してください。

Active Directory を使用してユーザを透過的に識別する場合は、以下を考慮してください。

- Active Directory による透過的ユーザ識別は、NTLM または Kerberos 認証スキームでのみ機能します。Active Directory インスタンスに対応する LDAP 認証レルムでは使用できません。
- 透過的ユーザ ID は Active Directory エージェントがサポートする Active Directory のバージョンで動作します。
- 高可用性を実現するために、別のマシンに Active Directory エージェントの 2 番目のインスタンスをインストールできます。その場合、各 Active Directory エージェントは、他方のエージェントとは別個に、独自の IP アドレス対ユーザ名 マッピングを保持します。AsyncOS for Web は、プライマリ エージェントに対する ping の試行が 3 回失敗した後にバックアップとして Active Directory エージェントを使用します。
- Active Directory エージェントは、Web セキュリティ アプライアンスと通信する際にオンデマンド モードを使用します。
- Active Directory エージェントは、Web セキュリティ アプライアンス にユーザのログアウト情報をプッシュします。ただし、ユーザのログアウト情報が Active Directory セキュリティ ログに記録されないことがあります。これは、クライアント マシンがクラッシュしたり、ユーザがログアウトせずにマシンをシャット ダウンした場合に発生します。ユーザのログアウト情報がセキュリティ ログにないと、Active Directory エージェントは、IP アドレスがそのユーザに割り当てられていないことをアプライアンスに通知できません。これを回避するために、Active Directory エージェントからのアップデートがない場合に AsyncOS が IP アドレス対ユーザのマッピングをキャッシュしておく時間の長さを定義できます。詳細については、CLI を使用した透過的ユーザ識別の詳細設定（5-10 ページ）を参照してください。

- Active Directory エージェントは、ユーザ名の一意性を確保するために、特定の IP アドレスからログインする各ユーザの sAMAccountName を記録します。
- クライアント マシンが Active Directory サーバに提供するクライアントの IP アドレスと Web セキュリティ アプライアンスは同一である必要があります。
- AsyncOS for Web はユーザが属する上位の親グループだけを検索します。ネストされたグループは検索しません。

Web セキュリティ アプライアンスに情報を提供する Active Directory エージェントの設定

AsyncOS for Web OS は、Active Directory から直接クライアントの IP アドレスを取得できないので、Active Directory エージェントから IP アドレス対ユーザ名のマッピング情報を取得する必要があります。

Web セキュリティ アプライアンス にアクセスでき、表示されるすべての Windows ドメイン コントローラと通信できるネットワーク上のマシンに、Active Directory エージェントをインストールします。最高のパフォーマンスを実現するために、このエージェントは Web セキュリティ アプライアンス に物理的にできるだけ近いところに配置する必要があります。小規模なネットワーク環境では、Active Directory サーバに直接 Active Directory エージェントをインストールすることもできます。

（注）　Web セキュリティ アプライアンス との通信に使用される Active Directory エージェントのインスタンスは、シスコの適応型セキュリティ アプライアンスやその他の Web セキュリティ アプライアンス など、他のアプライアンスもサポートできます。

Cisco Context Directory Agent の取得、インストール、および設定

Cisco Context Directory Agent のダウンロード、インストール、および設定に関する詳細については、http://www.cisco.com/en/US/docs/security/ibf/cda_10/Install_Config_guide/cda10.html を参照してください。

（注）　Web セキュリティ アプライアンス と Active Directory エージェントは、RADIUS プロトコルを使用して相互に通信します。アプライアンスとエージェントは、ユーザのパスフレーズを難読化するために同じ共有秘密キーを使用して設定する必要があります。その他のユーザ属性は難読化されません。

LDAP による透過的ユーザ識別

AsyncOS for Web は、Lightweight Directory Access Protocol（LDAP）レルムとして設定されている eDirectory サーバと通信し、IP アドレス対ユーザ名のマッピングを保守できます。eDirectory クライアントを介してログインする場合、ユーザは eDirectory サーバに対して認証されます。認証に成功すると、ログインしたユーザの属性（NetworkAddress）としてクライアントの IP アドレスが eDirectory サーバに記録されます。

LDAP（eDirectory）を使用してユーザを透過的に識別する場合は、以下を考慮してください。

- eDirectory クライアントを各クライアント ワークステーションにインストールし、エンドユーザがそれを使用して eDirectory サーバによる認証を受けるようにする必要があります。
- eDirectory クライアントのログインで使用する LDAP ツリーは、認証レルムに設定されている LDAP ツリーと同一である必要があります。
- eDirectory クライアントが複数の LDAP ツリーを使用する場合は、ツリーごとに認証レルムを作成し、各 LDAP 認証レルムを使用する認証シーケンスを作成します。

- eDirectory として LDAP 認証レルムを設定する場合は、クエリー クレデンシャルのバインド DN を指定する必要があります。
- eDirectory サーバは、ユーザのログイン時にユーザ オブジェクトの `NetworkAddress` 属性を更新するように設定する必要があります。
- AsyncOS for Web はユーザが属する上位の親グループだけを検索します。ネストされたグループは検索しません。
- eDirectory ユーザの `NetworkAddress` 属性を使用して、ユーザの最新のログイン IP アドレスを特定できます。

透過的ユーザ識別のルールとガイドライン

任意の認証サーバで透過的ユーザ ID を使用する場合は、以下のルールとガイドラインを考慮してください。

- DHCP を使用してクライアント マシンに IP アドレスを割り当てる場合は、Web セキュリティ アプライアンス 上の IP アドレス対ユーザ名のマッピングが DHCP リースよりも頻繁に更新されるようにします。`tuiconfig` CLI コマンドを使用して、マッピングの更新間隔を更新します。詳細については、CLI を使用した透過的ユーザ識別の詳細設定（5-10 ページ）を参照してください。
- IP アドレス対ユーザ名のマッピングが Web セキュリティ アプライアンス上で更新される前に、ユーザがマシンからログアウトし、別のユーザが同じマシンにログインした場合、Web プロキシは前のユーザをクライアントとして記録します。
- 透過的ユーザ識別に失敗した場合に Web プロキシがトランザクションを処理する方法を設定できます。ユーザにゲスト アクセスを許可するか、または認証プロンプトをエンド ユーザに強制的に表示することができます。
- 透過的ユーザ ID の失敗によりユーザに認証プロンプトが表示され、ユーザが無効なクレデンシャルにより認証に失敗した場合、ユーザのゲスト アクセスを許可するかどうかを選択できます。
- 割り当てられた識別プロファイルが、ユーザが存在する複数のレルムを含む認証シーケンスを使用している場合、AsyncOS for Web はシーケンスで示される順序でレルムからユーザ グループを取得します。
- ユーザを透過的に識別するように識別プロファイルを設定する場合、認証サロゲートは IP アドレスでなければなりません。別のサロゲート タイプを選択することはできません。
- ユーザの詳細なトランザクションを表示すると、透過的に識別されたユーザが [Web トラッキング（Web Tracking）] ページに表示されます。
- `%m` および `x-auth-mechanism` カスタム フィールドを使用して、透過的に識別されたユーザをアクセス ログと WC3 ログに記録することができます。`SSO_TUI` のログ エントリは、ユーザ名が、透過的ユーザ識別により認証されたユーザ名をクライアント IP アドレスと照合することによって取得されたことを示しています。（同様に、`SSO_ASA` の値は、ユーザがリモート ユーザであり、ユーザ名が AnyConnect Secure Mobility を使用して Cisco ASA から取得されたことを示しています）。

透過的ユーザ識別の設定

透過的なユーザの識別と認証の設定については、エンドユーザ クレデンシャルの取得（5-1 ページ）に詳しく記載されています。基本的な手順は以下のとおりです。

- 認証レルムを作成して、順序付けます。
- 識別プロファイルを作成し、ユーザおよびクライアント ソフトウェアを分類します。
- 識別されたユーザとユーザ グループからの Web 要求を管理するポリシーを作成します。

CLI を使用した透過的ユーザ識別の詳細設定

AsyncOS for Web は以下の TUI 関連の CLI コマンドを備えています。

- **tuiconfig**：透過的ユーザ識別に関連する詳細設定を設定します。バッチ モードを使用して、複数のパラメータを同時に設定できます。
  - **Configure mapping timeout for Active Directory agent**：AD エージェントからのアップデートがない場合に、AD エージェントによって取得された IP アドレスに対して、IP アドレス対ユーザのマッピングをキャッシュしておく時間の長さ（分単位）。
  - **Configure proxy cache timeout for Active Directory agent**：プロキシ固有の IP アドレス対ユーザのマッピングをキャッシュしておく時間の長さ（秒単位）。有効な値は 5～1200 秒です。デフォルト値および推奨値は 120 秒です。より低い値を指定すると、プロキシのパフォーマンスに悪影響を及ぼします。
  - **Configure mapping timeout for Novell eDirectory**：サーバからのアップデートがない場合に、eDirectory サーバから取得された IP アドレスに対して、IP アドレス対ユーザのマッピングをキャッシュしておく時間の長さ（秒単位）。
  - **Configure query wait time for Active Directory agent**：Active Directory エージェントからの応答を待機する時間の長さ（秒単位）。クエリーに要する時間がこのタイムアウト値を上回った場合、透過的ユーザ識別は失敗したと見なされます。これにより、エンドユーザが体験する認証遅延が限定されます。
  - **Configure query wait time for Novell eDirectory**：eDirectory サーバからの応答を待機する時間の長さ（秒単位）。クエリーに要する時間がこのタイムアウト値を上回った場合、透過的ユーザ識別は失敗したと見なされます。これにより、エンド ユーザが体験する認証遅延が限定されます。

  Active Directory の設定は、透過的ユーザ識別に AD エージェントを使用するすべての AD レルムに適用されます。eDirectory の設定は、透過的ユーザ識別に eDirectory を使用するすべての LDAP レルムに適用されます。

  いずれかのパラメータの検証に失敗した場合は、どの値も変更されません。
- **tuistatus**：このコマンドには、以下のような AD 関連のサブコマンドがあります。
  - **adagentstatus**：すべての AD エージェントの現在のステータス、および Windows ドメイン コントローラとの接続に関する情報を表示します。
  - **listlocalmappings**：Web セキュリティ アプライアンス に保存されているすべての IP アドレス対ユーザ名のマッピングを、AD エージェントによって取得された順序で一覧表示します。このコマンドは、エージェントに保存されているエントリや、現在クエリーが進行中のマッピングを一覧表示しません。

シングル サインオンの設定

透過的にクレデンシャルを取得することにより、シングル サインオン環境を実現できます。透過的ユーザ識別は認証レルムの設定項目の 1 つです。

Internet Explorer の場合は、リダイレクト ホスト名として、完全修飾ドメイン名ではなく、(ドットを含まない)短縮形のホスト名または NetBIOS 名を必ず使用します。または、Internet Explorer の [ローカル イントラネット] ゾーンにアプライアンスのホスト名を追加することができます([ツール] > [インターネット オプション] > [セキュリティ] タブ)。ただし、この操作をすべてのクライアントで実行する必要があります。これに関する詳細については、『How do I properly set up NTLM with SSO (credentials sent transparently)?』を参照してください。

Firefox およびその他の Microsoft 以外のブラウザでは、パラメータ **network.negotiate-auth.delegation-uris**、**network.negotiate-auth.trusted-uris**、**network.automatic-ntlm-auth.trusted-uris** を透過モードのリダイレクト ホスト名に設定する必要があります。『Firefox is not sending authentication credentials transparently (SSO)』も参照してください。この記事には、Firefox パラメータの変更に関する一般情報が記載されています。

リダイレクト ホスト名については、グローバル認証の設定、または CLI コマンド sethostname を参照してください。

認証レルム

認証レルムによって、認証サーバに接続するために必要な詳細情報を定義し、クライアントと通信するときに使用する認証方式を指定します。AsyncOS は複数の認証レルムをサポートしています。レルムを認証シーケンスにグループ化することにより、認証要件が異なるユーザを同じポリシーで管理することができます。

- 外部認証(5-11 ページ)
- Kerberos 認証方式の Active Directory レルムの作成(5-12 ページ)
- Active Directory 認証レルムの作成(NTLMSSP および基本)(5-15 ページ)
- LDAP 認証レルムの作成(5-18 ページ)
- 認証レルムの削除について(5-23 ページ)
- グローバル認証の設定(5-23 ページ)

関連項目

- RADIUS ユーザ認証(12-9 ページ)
- 認証シーケンス(5-28 ページ)

外部認証

外部 LDAP または RADIUS サーバからユーザを認証できます。

LDAP サーバによる外部認証の設定

はじめる前に

- LDAP 認証レルムを作成し、それに 1 つ以上の外部認証クエリーを設定します。LDAP 認証レルムの作成（5-18 ページ）

ステップ 1　アプライアンスで外部認証を有効にします。

a. [システム管理（System Administration）] > [ユーザ（Users）] に移動します。

b. [外部認証（External Authentication）] セクションで [有効（Enable）] をオンにします。

c. 以下のオプションを設定します。

オプション	説明
外部認証を有効にする（Enable External Authentication）	—
認証タイプ（Authentication Type）	[LDAP] を選択します。
外部認証キャッシュタイムアウト（External Authentication Cache Timeout）	再認証のために LDAP サーバに再接続するまで、AsyncOS が外部認証クレデンシャルを保存する秒数。デフォルトはゼロ（0）です。
LDAP 外部認証クエリー（LDAP External Authentication Query）	LDAP レルムにより設定されたクエリー。
サーバからの有効なレスポンス待ちタイムアウト（Timeout to wait for valid response from server）	AsyncOS がサーバからのクエリーに対する応答を待機する秒数。
グループ マッピング（Group Mapping）	ディレクトリ内の各グループ名にロールを割り当てます。

ステップ 2　変更を送信し、保存します。

RADIUS 外部認証のイネーブル化

RADIUS を使用した外部認証のイネーブル化（12-9 ページ）を参照してください。

Kerberos 認証方式の Active Directory レルムの作成

はじめる前に

- アプライアンスが（クラウド コネクタ モードではなく）標準モードで設定されていることを確認します。
- Active Directory サーバを準備します。
  - 以下のサーバのいずれかに Active Directory をインストールします：Windows Server 2003、2008、2008R2、2012。
  - ドメイン管理者グループまたはアカウント オペレータ グループのメンバーであるユーザを Active Directory サーバ上に作成します。

    または

  - 次の権限を持つユーザ名を作成します。

    - Active Directory でのパスワード リセット権限

    - servicePrincipalName への検証済み書き込み

    - アカウント制限事項の書き込み

    - dNShost 名の書き込み

    - servicePrincipalName の書き込み

    以上は、アプライアンスをドメインに参加させてアプライアンスが完全機能していることを確認するために、ユーザ名に必要な最小限の Active Directory 権限です。
  - クライアントをドメインに参加させます。サポートされるクライアントは、Windows XP、Windows 7、Mac OS 10.5+ です。
  - Windows Resource Kit の kerbtray ツールを使用して、クライアントの Kerberos チケットを確認します（http://www.microsoft.com/en-us/download/details.aspx?id=17657）。
  - Mac クライアントでは、[メイン メニュー（Main Menu）] > [Keychain Access] で、Ticket Viewer アプリケーションを使用して Kerberos チケットを確認できます。
- 認証元となる Active Directory ドメインに Webセキュリティ アプライアンスを参加させるために必要な、権限とドメイン情報を取得済みであることを確認します。
- Web セキュリティ アプライアンスの現在の時刻と Active Directory サーバの現在時刻を比較して、その差が Active Directory サーバの [コンピュータ クロック同期の最大許容時間（Maximum tolerance for computer clock synchronization）] オプションで指定されている時間を超えていないことを確認します。
- Web セキュリティ アプライアンスがセキュリティ管理アプライアンスで管理されている場合は、異なる Web セキュリティ アプライアンス上の同名の認証レルムのプロパティが、各アプライアンスで定義されているプロパティと同一になるように設定しておきます。
- Web セキュリティ アプライアンス の設定
  - 明示的モードでは、WSA ホスト名（sethostname CLI コマンド）をブラウザで設定されているプロキシ名と同じにする必要があります。
  - 透過モードでは、WSA ホスト名をリダイレクト ホスト名と同じにする必要があります（グローバル認証の設定（5-23 ページ）を参照）。さらに、Kerberos レルムを作成する前に、WSA ホスト名とリダイレクト ホスト名を設定する必要があります。
- 新しいレルムを確定すると、レルムの認証プロトコルを変更できなくなるので注意してください。
- シングル サインオン（SSO）をクライアント ブラウザで設定する必要があります（シングル サインオンの設定（5-11 ページ）を参照）。
- ログの使用を簡素化するため、%m のカスタム フィールドのパラメータを使用してアクセス ログをカスタマイズします。アクセス ログのカスタマイズ（11-30 ページ）を参照してください。

ステップ 1　Cisco Web セキュリティ アプライアンス Web インターフェイスで、[ネットワーク（Network）] > [認証（Authentication）] を選択します。

ステップ 2　[レルムを追加（Add Realm）] をクリックします。

ステップ 3　英数字とスペース文字だけを使用して、認証レルムに一意の名前を割り当てます。

ステップ 4　[認証プロトコル（Authentication Protocol）] フィールドで [Active Directory] を選択します。

ステップ 5　Active Directory サーバの完全修飾ドメイン名または IP アドレスを 3 つまで入力します。

例：`ntlm.example.com`

IP アドレスが必要なのは、アプライアンスで設定されている DNS サーバが Active Directory サーバのホスト名を解決できない場合だけです。

レルムに複数の認証サーバを設定した場合、アプライアンスは、そのレルム内のトランザクションの認証に失敗するまでに最大 3 つの認証サーバで認証を試みます。

ステップ 6　アプライアンスをドメインに参加させます。

a.　Active Directory アカウントを設定します。

設定	説明
Active Directory ドメイン（Active Directory Domain）	Active Directory サーバのドメイン名。DNS ドメインまたはレルムとも呼ばれます。
NetBIOS ドメイン名（NetBIOS domain name）	ネットワークで NetBIOS を使用する場合は、ドメイン名を入力します。 **ヒント**　このオプションを使用できない場合は、setntlmsecuritymode CLI コマンドを使用して、NTLM セキュリティ モードが [ドメイン（domain）] に設定されていることを確認します。
コンピュータ アカウント（Computer Account）	ドメイン上のコンピュータを一意的に識別する Active Directory コンピュータ アカウント（別名「マシン信頼アカウント」）が作成される、Active Directory ドメイン内の場所を指定します。 Active Directory 環境で、コンピュータ オブジェクトが一定の間隔で自動的に削除される場合は、自動削除から保護されているコンテナ内にコンピュータ アカウントの場所を指定します。

b.　[ドメインに参加（Join Domain）] をクリックします。

（注）　すでに参加しているドメインに参加しようとすると（同じクレデンシャルを使用している場合でも）、Active Directory が新しいキー セットをこの WSA を含む全てのクライアントに送信するため、既存の接続は閉じられます。影響を受けるクライアントは、ログオフしてから再度ログインする必要があります。

c.　Active Directory 上のアカウントにログイン クレデンシャル（ユーザ名およびパスフレーズ）を指定し、[アカウントの作成（Create Account）] をクリックします。

ステップ 7　（任意）透過的ユーザ識別を設定します。

設定	説明
Active Directory を使用して透過ユーザ識別を有効にする（Enable Transparent User Identification using Active Directory agent）	プライマリ Context Directory エージェントがインストールされているマシンのサーバ名と、それにアクセスするために使用する共有秘密の両方を入力します。 （任意）バックアップ Context Directory エージェントがインストールされているマシンのサーバ名とその共有秘密を入力します。

ステップ 8　ネットワーク セキュリティを設定します。

設定	説明
クライアントの署名が必須（Client Signing Required）	クライアントの署名を要求するように Active Directory サーバが設定されている場合は、このオプションを選択します。 このオプションを選択した場合、AsyncOS は、Active Directory サーバとの通信時に Transport Layer Security を使用します。

ステップ 9　（任意）[テスト開始（Start Test）] をクリックします。これにより、ユーザが実際にそれらを使用して認証を受ける前に、入力した設定をテストして正しいかどうかを確認できます。テストの具体的な実行方法については、「 •既存の NTLM レルムが信頼していないドメインのユーザを認証するには、追加の NTLM レルムを作成します。（5-23 ページ）」を参照してください。

ステップ 10　テスト中に発生した問題をトラブルシューティングします。

ステップ 11　変更を送信し、保存します。

次の作業

- Kerberos 認証方式を使用する識別プロファイルを作成します。ユーザおよびクライアント ソフトウェアの分類（6-3 ページ）。

Active Directory 認証レルムの作成（NTLMSSP および基本）

Active Directory 認証レルムの作成の前提条件（NTLMSSP および基本）

- 認証元となる Active Directory ドメインに Webセキュリティ アプライアンスを参加させるために必要な、権限とドメイン情報を取得済みであることを確認します。
- NTLM セキュリティ モードとして「domain」を使用する場合は、ネストした Active Directory グループのみを使用します。Active Directory グループがネストされていない場合は、デフォルト値の「ads」を使用します。このマニュアルの付録「コマンドライン インターフェイス」で setntlmsecuritymode を参照してください。
- Web セキュリティ アプライアンスの現在の時刻と Active Directory サーバの現在時刻を比較して、その差が Active Directory サーバの [コンピュータ クロック同期の最大許容時間（Maximum tolerance for computer clock synchronization）] オプションで指定されている時間を超えていないことを確認します。
- Web セキュリティ アプライアンスがセキュリティ管理アプライアンスで管理されている場合は、異なる Web セキュリティ アプライアンス上の同名の認証レルムのプロパティが、各アプライアンスで定義されているプロパティと同一になるように設定しておきます。
- 新しいレルムを確定すると、レルムの認証プロトコルを変更できなくなるので注意してください。
- WSA は、信頼できるすべてのドメインのドメイン コントローラと、NTLM レルムに設定されたドメイン コントローラに接続する必要があります。認証が正しく機能するように、内部ドメインおよび外部ドメインのすべてのドメイン コントローラに対して次のポートを開く必要があります。

  LDAP（389 UDP および TCP）

  Microsoft SMB（445 TCP）

Kerberos（88 UDP）

エンドポイント解決：ポート マッパー（135 TCP）Net Log-on 固定ポート

- NTLMSSP の場合は、クライアント ブラウザにシングル サインオン（SSO）を設定できます。シングル サインオンの設定（5-11 ページ）を参照してください。

複数の NTLM レルムとドメインの使用について

以下のルールは、複数の NTLM レルムとドメインを使用する場合に該当します。

- 最大 10 の NTLM 認証レルムを作成できます。
- ある NTLM レルムのクライアント IP アドレスが、別の NTLM レルムのクライアント IP アドレスと重複しないようにする必要があります。
- 各 NTLM レルムは 1 つの Active Directory ドメインにのみ参加できますが、そのドメインが信頼しているあらゆるドメインのユーザを認証できます。この信頼は、同じフォレスト内の他のドメインにデフォルトで適用され、少なくとも一方向の信頼が存在しているフォレスト外部のドメインに適用されます。
- 既存の NTLM レルムが信頼していないドメインのユーザを認証するには、追加の NTLM レルムを作成します。

Active Directory 認証レルムの作成（NTLMSSP および基本）

ステップ 1　[ネットワーク（Network）] > [認証（Authentication）] を選択します。

ステップ 2　[レルムを追加（Add Realm）] をクリックします。

ステップ 3　英数字とスペース文字だけを使用して、認証レルムに一意の名前を割り当てます。

ステップ 4　[認証プロトコルと方式（Authentication Protocol and Scheme(s)）] フィールドで [Active Directory] を選択します。

ステップ 5　Active Directory サーバの完全修飾ドメイン名または IP アドレスを 3 つまで入力します。

例：`active.example.com`

IP アドレスが必要なのは、アプライアンスで設定されている DNS サーバが Active Directory サーバのホスト名を解決できない場合だけです。

レルムに複数の認証サーバを設定した場合、アプライアンスは、そのレルム内のトランザクションの認証に失敗するまでに最大 3 つの認証サーバで認証を試みます。

ステップ 6　アプライアンスをドメインに参加させます。

a.　Active Directory アカウントを設定します。

設定	説明
Active Directory ドメイン（Active Directory Domain）	Active Directory サーバのドメイン名。 DNS ドメインまたはレルムとも呼ばれます。
NetBIOS ドメイン名（NetBIOS domain name）	ネットワークで NetBIOS を使用する場合は、ドメイン名を入力します。

設定	説明
コンピュータ アカウント（Computer Account）	ドメイン上のコンピュータを一意的に識別する Active Directory コンピュータ アカウント（別名「マシン信頼アカウント」）が作成される、Active Directory ドメイン内の場所を指定します。 Active Directory 環境で、コンピュータ オブジェクトが一定の間隔で自動的に削除される場合は、自動削除から保護されているコンテナ内にコンピュータ アカウントの場所を指定します。

b. [ドメインに参加（Join Domain）] をクリックします。

（注） すでに参加しているドメインに参加しようとすると（同じクレデンシャルを使用している場合でも）、Active Directory が新しいキー セットをこの WSA を含む全てのクライアントに送信するため、既存の接続は閉じられます。影響を受けるクライアントは、ログオフしてから再度ログインする必要があります。

c. そのドメインにコンピュータ アカウントを作成する権限を持つ、既存の Active Directory ユーザの sAMAccountName ユーザ名とパスフレーズを入力します。

例：「jazzdoe」（「DOMAIN\jazzdoe」や「jazzdoe@domain」は使用しないでください）。

この情報は、コンピュータ アカウントを確立するために一度だけ使用され、保存されません。

d. [アカウントの作成（Create Account）] をクリックします。

ステップ 7　（任意）透過的認証を設定します。

設定	説明
Active Directory を使用して透過ユーザ識別を有効にする（Enable Transparent User Identification using Active Directory agent）	プライマリ Context Directory エージェントがインストールされているマシンのサーバ名と、それにアクセスするために使用する共有秘密の両方を入力します。 （任意）バックアップ Context Directory エージェントがインストールされているマシンのサーバ名とその共有秘密を入力します。

ステップ 8　ネットワーク セキュリティを設定します。

設定	説明
クライアントの署名が必須（Client Signing Required）	クライアントの署名を要求するように Active Directory サーバが設定されている場合は、このオプションを選択します。 このオプションを選択した場合、AsyncOS は、Active Directory サーバとの通信時に Transport Layer Security を使用します。

ステップ 9　（任意）[テスト開始（Start Test）] をクリックします。これにより、ユーザが実際にそれらを使用して認証を受ける前に、入力した設定をテストして正しいかどうかを確認できます。

ステップ 10　変更を送信し、保存します。

LDAP 認証レルムの作成

はじめる前に

- 組織の LDAP に関する以下の情報を取得します。
  - LDAP のバージョン
  - サーバのアドレス
  - LDAP ポート
- Web セキュリティ アプライアンスがセキュリティ管理アプライアンスで管理されている場合は、異なる Web セキュリティ アプライアンス上の同名の認証レルムのプロパティが、各アプライアンスで定義されているプロパティと同じであることを確認します。

ステップ 1　[ネットワーク（Network）] > [認証（Authentication）] を選択します。

ステップ 2　[レルムを追加（Add Realm）] をクリックします。

ステップ 3　英数字とスペース文字だけを使用して、認証レルムに一意の名前を割り当てます。

ステップ 4　[認証プロトコルと方式（Authentication Protocol and Scheme(s)）] フィールドで [LDAP] を選択します。

ステップ 5　LDAP 認証の設定を入力します。

設定	説明
LDAP のバージョン（LDAP Version）	LDAP のバージョンを選択し、セキュア LDAP を使用するかどうかを選択します。 アプライアンスは、LDAP バージョン 2 および 3 をサポートしています。セキュア LDAP には LDAP バージョン 3 が必要です。 この LDAP サーバが透過的ユーザ識別で使用する Novell eDirectory をサポートしているかどうかを選択します。
LDAP サーバ（LDAP Server）	LDAP サーバの IP アドレスまたはホスト名、およびポート番号を入力します。最大 3 つのサーバを指定できます。 ホスト名は、完全修飾ドメイン名である必要があります。例: `ldap.example.com`。IP アドレスが必要なのは、アプライアンスで設定されている DNS サーバが LDAP サーバのホスト名を解決できない場合のみです。 標準 LDAP のデフォルトのポート番号は 389 です。セキュア LDAP のデフォルトの番号は 636 です。 LDAP サーバが Active Directory サーバの場合は、ドメイン コントローラのホスト名または IP アドレス、およびポートを入力します。可能な限り、グローバル カタログ サーバの名前を入力し、ポート 3268 を使用します。ただし、グローバル カタログ サーバが物理的に離れた場所にあり、ローカル ドメイン コントローラのユーザのみを認証する必要がある場合は、ローカル ドメイン コントローラを使用することもできます。 **注:** レルムに複数の認証サーバを設定した場合、アプライアンスは、そのレルム内のトランザクションの認証に失敗するまでに最大 3 つの認証サーバで認証を試みます。

設定	説明
LDAP 持続的接続（LDAP Persistent Connections） （[詳細設定（Advanced）] セクションの下）	以下の値のいずれかを選択します。 • [永続的接続の使用（無制限）（Use persistent connections (unlimited)）]。既存の接続を使用します。使用できる接続がない場合は、新しい接続が開かれます。 • [永続的接続の使用（Use persistent connections）]。既存の接続を使用して、指定された数の要求に使用します。最大値に達すると、LDAP サーバへの新しい接続が確立されます。 • [永続的接続を使用しない（Do not use persistent connections）]。必ず、LDAP サーバへの新しい接続を作成します。
ユーザ認証（User Authentication）	以下のフィールドに値を入力します。 **[ベース識別名（ベース DN）（Base Distinguished Name (Base DN)]** LDAP データベースはツリー型のディレクトリ構造になっており、アプライアンスはベース DN を使用して、LDAP ディレクトリ ツリー内の適切な場所に移動し、検索を開始します。有効なベース DN フィルタ文字列は、`object-value` 形式の 1 つ以上のコンポーネントから構成されます。たとえば、「`dc=companyname, dc=com`」のように入力します。 **[ユーザ名属性（User Name Attribute）]** 以下の値のいずれかを選択します。 • [uid]、[cn]、[sAMAccountName]。ユーザ名を指定する、LDAP ディレクトリで一意の ID。 • [カスタム（custom）]。「`UserAccount`」などのカスタム ID。 **[ユーザフィルタクエリー（User Filter Query）]** ユーザ フィルタ クエリーは、ユーザのベース DN を見つける LDAP 検索フィルタです。これは、ユーザ ディレクトリがベース DN の下の階層にある場合、またはそのユーザのベース DN のユーザ固有コンポーネントにログイン名が含まれていない場合に必要です。 以下の値のいずれかを選択します。 • [なし（none）]。すべてのユーザを抽出します。 • [カスタム（custom）]。ユーザの特定のグループを抽出します。

設定	説明
クエリー クレデンシャル（Query Credentials）	認証サーバが匿名クエリーを受け入れるかどうかを選択します。 認証サーバが匿名クエリーを受け入れる場合は、[サーバは、匿名の質問に対応します（Server Accepts Anonymous Queries）] を選択します。 認証サーバが匿名クエリーを受け入れない場合は、[バインド DN を使用（Use Bind DN）] を選択し、以下の情報を入力します。 • [バインド DN（Bind DN）]。LDAP ディレクトリの検索を許可された外部 LDAP サーバ上のユーザ。通常、バインド DN はディレクトリ全体の検索を許可されます。 • [パスフレーズ（Passphrase）]。[バインド DN（Bind DN）] フィールドに入力するユーザに関連付けられるパスフレーズ。 以下のテキストは、[バインド DN（Bind DN）] フィールドに入力するユーザの例を示しています。 cn=administrator,cn=Users,dc=domain,dc=com sAMAccountName=jdoe,cn=Users,dc=domain,dc=com. LDAP サーバが Active Directory サーバの場合は、「DOMAIN\username」の形式でバインド DN ユーザ名を入力することもできます。

ステップ 6　（任意）グループ オブジェクトまたはユーザ オブジェクトを介して [グループ認証（Group Authorization）] をイネーブルにし、選択したオプションを設定します。

グループ オブジェクト設定	説明
グループ オブジェクト内のグループ メンバーシップ属性（Group Membership Attribute Within Group Object）	このグループに属するすべてのユーザをリストする LDAP 属性を選択します。 以下の値のいずれかを選択します。 • [member] および [uniquemember]。グループ メンバを指定する、LDAP ディレクトリで一意の ID。 • [カスタム（custom）]。「`UserInGroup`」などのカスタム ID。
グループ名を含む属性（Attribute that Contains the Group Name）	ポリシー グループの設定で使用できるグループ名を指定する LDAP 属性を選択します。 以下の値のいずれかを選択します。 • [cn]。グループ名を指定する、LDAP ディレクトリで一意の ID。 • [カスタム（custom）]。「`FinanceGroup`」などのカスタム ID。

グループ オブジェクト設定	説明
オブジェクトがグループかどうかを判別するクエリ文字列（Query string to determine if object is a group）	LDAP オブジェクトがユーザ グループを表しているかどうかを判別する LDAP 検索フィルタを選択します。 以下の値のいずれかを選択します。 • **objectclass=groupofnames** • **objectclass=groupofuniquenames** • **objectclass=group** • **[カスタム（custom）]**。「`objectclass=person`」などのカスタム フィルタ。 **注：**クエリーによって、ポリシー グループで使用できる一連の認証グループが定義されます。

ユーザ オブジェクト設定	説明
ユーザ オブジェクト内のグループ メンバーシップ属性（Group Membership Attribute Within User Object）	このユーザが属するすべてのグループをリストする属性を選択します。 以下の値のいずれかを選択します。 • [memberOf]。ユーザ メンバを指定する、LDAP ディレクトリで一意の ID。 • [カスタム（custom）]。「`UserInGroup`」などのカスタム ID。
グループ メンバーシップ属性は DN（Group Membership Attribute is a DN）	グループ メンバーシップ属性が、LDAP オブジェクトを参照する識別名（DN）であるかどうかを指定します。Active Directory サーバの場合は、このオプションをイネーブルにします。 これをイネーブルにした場合は、以下の設定を指定する必要があります。
グループ名を含む属性（Attribute that Contains the Group Name）	グループ メンバーシップ属性が DN である場合に、ポリシー グループ設定でグループ名として使用できる属性を指定します。 以下の値のいずれかを選択します。 • [cn]。グループ名を指定する、LDAP ディレクトリで一意の ID。 • [カスタム（custom）]。「`FinanceGroup`」などのカスタム ID。
オブジェクトがグループかどうかを判別するクエリ文字列（Query string to determine if object is a group）	LDAP オブジェクトがユーザ グループを表しているかどうかを判別する LDAP 検索フィルタを選択します。 以下の値のいずれかを選択します。 • **objectclass=groupofnames** • **objectclass=groupofuniquenames** • **objectclass=group** • **[カスタム（custom）]**。「`objectclass=person`」などのカスタム フィルタ。 **注：**クエリーによって、Web Security Manager ポリシーで使用できる一連の認証グループが定義されます。

ステップ 7　（任意）ユーザに対する外部 LDAP 認証を設定します。

a. [外部認証クエリ（External Authentication Queries）] を選択します。

b. ユーザ アカウントを特定します。

ベース DN（Base DN）	検索を開始する LDAP ディレクトリ ツリー内の適切な場所に移動するためのベース DN。

クエリ文字列（Query String）	一連の認証グループを返すクエリー。例:
	`(&(objectClass=posixAccount)(uid={u}))`
	または
	`(&(objectClass=user)(sAMAccountName={u}))`

ユーザのフル ネームが格納されている属性（Attribute containing the user's full name）	LDAP 属性（例：`displayName`、`gecos`）。

c. （任意）RFC 2307 アカウント有効期限 LDAP 属性に基づき、有効期限切れのアカウントはログインが拒否されます。

d. ユーザのグループ情報を取得するクエリーを入力します。

1 人のユーザが複数の LDAP グループに属しており、それぞれユーザ ロールが異なる場合は、最も限定的なロールのアクセス許可が AsyncOS によってそのユーザに付与されます。

ベース DN（Base DN）	検索を開始する LDAP ディレクトリ ツリー内の適切な場所に移動するためのベース DN。
クエリ文字列	`(&(objectClass=posixAccount)(uid={u}))`
ユーザのフル ネームが格納されている属性（Attribute containing the user's full name）	`gecos`

ステップ 8　（任意）[テスト開始（Start Test）] をクリックします。これにより、ユーザが実際にそれらを使用して認証を受ける前に、入力した設定をテストして正しいかどうかを確認できます。テストの具体的な実行方法については、「•既存の NTLM レルムが信頼していないドメインのユーザを認証するには、追加の NTLM レルムを作成します。（5-23 ページ）」を参照してください。

（注）　変更を送信して確定すると、後でレルムの認証プロトコルを変更できなくなります。

ステップ 9　変更を送信し、保存します。

次の作業

- Kerberos 認証方式を使用する識別プロファイルを作成します。ユーザおよびクライアント ソフトウェアの分類（6-3 ページ）。

関連項目

- 外部認証（5-11 ページ）

複数の NTLM レルムとドメインの使用

以下のルールは、複数の NTLM レルムとドメインを使用する場合に該当します。

- 最大 10 の NTLM 認証レルムを作成できます。
- ある NTLM レルムのクライアント IP アドレスが、別の NTLM レルムのクライアント IP アドレスと重複しないようにする必要があります。
- 各 NTLM レルムは 1 つの Active Directory ドメインにのみ参加できますが、そのドメインが信頼しているあらゆるドメインのユーザを認証できます。この信頼は、同じフォレスト内の他のドメインにデフォルトで適用され、少なくとも一方向の信頼が存在しているフォレスト外部のドメインに適用されます。
- 既存の NTLM レルムが信頼していないドメインのユーザを認証するには、追加の NTLM レルムを作成します。

認証レルムの削除について

認証レルムを削除すると関連する ID がディセーブルになり、さらに、関連するポリシーからそれらの ID が削除されます。

認証レルムを削除すると、そのレルムがシーケンスから削除されます。

グローバル認証の設定

認証レルムの認証プロトコルとは別途に、グローバル認証の設定項目を設定してすべての認証レルムに設定を適用します。

Web プロキシの展開モードは、設定できるグローバル認証の設定項目に影響します。明示的な転送モードよりも、透過モードで展開されている場合の方がより多くの設定項目を使用できます。

はじめる前に

- 以下の概念をよく理解しておいてください。
  - 認証の失敗（5-31 ページ）
  - 認証の失敗：異なるクレデンシャルによる再認証の許可（5-35 ページ）

ステップ 1　[ネットワーク（Network）] > [認証（Authentication）] を選択します。

ステップ 2　[グローバル設定を編集（Edit Global Settings）] をクリックします。

ステップ 3　[グローバル認証設定（Global Authentication Settings）] セクションで、設定を編集します。

設定	説明
認証サーバが利用できない場合のアクション（Action if Authentication Service Unavailable）	以下の値のいずれかを選択します。 • [認証なしでトラフィックの通過を許可（Permit traffic to proceed without authentication）]。処理が、ユーザが認証されたかのように続行されます。 • [認証に失敗した場合にすべてのトラフィックをブロック（Block all traffic if user authentication fails）]。処理が中止され、すべてのトラフィックがブロックされます。

設定	説明
失敗した認証手続き（Failed Authentication Handling）	識別プロファイル ポリシーでユーザにゲスト アクセスを許可する場合は、この設定項目により、Web プロキシがユーザをゲストとして識別してアクセス ログに記録する方法を指定します。 ユーザのゲスト アクセス許可の詳細については、認証失敗後のゲスト アクセスの許可（5-33 ページ）を参照してください。
再認証（Re-authentication） （URL カテゴリまたはユーザ セッションの制限によりエンドユーザがブロックされた場合に再認証プロンプトをイネーブルにする（Enable Re-Authentication Prompt If End User Blocked by URL Category or User Session Restriction））	制限が厳しい URL フィルタリング ポリシーによって、または別の IP アドレスへのログインの制限によってユーザが Web サイトからブロックされた場合に、ユーザに再認証を許可します。 新しい認証クレデンシャルを入力できるリンクが記載されたブロック ページがユーザに表示されます。より多くのアクセスを許可するクレデンシャルをユーザが入力すると、要求されたページがブラウザに表示されます。 **注：**この設定は、制限が厳しい URL フィルタリング ポリシーまたはユーザ セッションの制限によってブロックされた、認証済みユーザにのみ適用されます。認証されずに、サブネットによりブロックされたトランザクションには適用されません。 詳細については、認証の失敗：異なるクレデンシャルによる再認証の許可（5-35 ページ）を参照してください。
ベーシック認証トークン TTL（Basic Authentication Token TTL）	認証サーバによって再検証されるまで、ユーザのクレデンシャルがキャッシュ内に保管される期間を制御します。これには、ユーザ名とパスフレーズ、およびユーザに関連付けられているディレクトリ グループが含まれます。 デフォルト値は推奨されている設定です。[サロゲート タイムアウト（Surrogate Timeout）] が設定されており、その値が [ベーシック認証トークン TTL（Basic Authentication Token TTL）] よりも大きい場合は、サロゲート タイムアウトの値が優先され、Web プロキシは、サロゲート タイムアウトの期限が切れた後に認証サーバに連絡します。

その他の設定可能な認証設定項目は、Web プロキシが展開されているモード（透過モードまたは明示的な転送モード）に応じて異なります。

ステップ 4　Web プロキシが透過モードで展開されている場合は、以下の設定項目を編集します。

設定	説明
クレデンシャルの暗号化（Credential Encryption）	クライアントが暗号化 HTTPS 接続を介して Web プロキシにログイン クレデンシャルを送信するかどうかを指定します。 この設定は基本認証方式と NTLMSPP 認証方式の両方に適用されますが、特に基本認証方式の場合に役立ちます。基本認証方式では、ユーザ クレデンシャルがプレーン テキストで送信されるからです。 詳細については、認証の失敗（5-31 ページ）を参照してください。
HTTPS リダイレクト ポート（HTTPS Redirect Port）	HTTPS 接続を介してユーザ認証要求をリダイレクトする場合に使用する TCP ポートを指定します。 これによって、クライアントが HTTPS による Web プロキシへの接続を開始するポートが指定されます。これは、クレデンシャルの暗号化がイネーブルになっている場合や、アクセス コントロールの使用時にユーザに認証を求める場合に発生します。

設定	説明
リダイレクト ホスト名（Redirect Hostname）	Web プロキシが着信接続をリッスンするネットワーク インターフェイスの短いホスト名を入力します。 透過モードで展開されているアプライアンスに認証を設定した場合、Web プロキシは、ユーザの認証のためにクライアントに送信するリダイレクション URL でこのホスト名を使用します。 以下の値のいずれかを入力できます。 • [1 語のホスト名（Single word hostname）]。クライアントと Web セキュリティ アプライアンス が DNS 解決可能な 1 語のホスト名を入力できます。これにより、クライアントは、ブラウザ側を設定することなく、Internet Explorer で真のシングル サインオンを実現できます。 必ず、クライアントと Web セキュリティ アプライアンス が DNS 解決可能な 1 語のホスト名を入力してください。 たとえば、クライアントがドメイン `mycompany.com` にあり、Web プロキシがリッスンしているインターフェイスの完全なホスト名が `proxy.mycompany.com` である場合は、このフィールドに「`proxy`」と入力する必要があります。クライアントは「`proxy`」に対してルックアップを実行し、`proxy.mycompany.com` を解決できます。 • [完全修飾ドメイン名（FQDN）（Fully qualified domain name (FQDN)）]。このフィールドに、FQDN または IP アドレスを入力することもできます。ただし、その場合、Internet Explorer や Firefox ブラウザで真のシングル サインオンを実現するには、入力する FQDN または IP アドレスが、クライアント ブラウザのクライアント信頼済みサイト リストに追加されていることを確認する必要があります。 デフォルト値は、プロキシ トラフィックに使用されるインターフェイスに応じて、M1 または P1 インターフェイスの FQDN です。
クレデンシャル キャッシュ オプション:（Credential Cache Options:） サロゲート タイムアウト（Surrogate Timeout）	クライアントに認証クレデンシャルを再度要求するまでに、Web プロキシが待機する時間を指定します。クレデンシャルを再度要求するまで、Web プロキシはサロゲートに保存された値（IP アドレスまたは Cookie）を使用します。 一般的に、ブラウザなどのユーザ エージェントでは、ユーザが毎回クレデンシャルを入力する必要がないように、認証クレデンシャルがキャッシュされます。
クレデンシャル キャッシュ オプション:（Credential Cache Options:） クライアント IP アイドル タイムアウト（Client IP Idle Timeout）	IP アドレスを認証サロゲートとして使用する場合は、この設定で、クライアントがアイドル状態のときに、認証クレデンシャルをクライアントに再要求するまで Web プロキシが待機する時間を指定します。 この値がサロゲート タイムアウト値よりも大きい場合、この設定には効力がなく、サロゲート タイムアウトに達した後にクライアントへの認証要求が行われます。 この設定を使用すると、コンピュータの前にいない時間が多いユーザの脆弱性を低減できます。

設定	説明
クレデンシャル キャッシュ オプション:(Credential Cache Options:) キャッシュ サイズ(Cache Size)	認証キャッシュに格納するエントリの数を指定します。この値を設定すると、実際にこのデバイスを使用しているユーザの数に安全に対応できます。デフォルト値は推奨されている設定です。
ユーザ セッション制限(User Session Restrictions)	認証済みユーザが複数の IP アドレスから同時にインターネットにアクセスすることを許可するかどうかを指定します。 ユーザが未認証ユーザと認証クレデンシャルを共有しないように、1 つのマシンへのアクセスを制限できます。ユーザが別のマシンでログインできない場合は、エンド ユーザ通知ページが表示されます。このページの [再認証(Re-authentication)] 設定を使用し、ユーザがボタンをクリックして別のユーザ名でログインできるかどうかを指定することもできます。 この設定をイネーブルにする場合は、制限タイムアウト値を入力します。この値によって、別の IP アドレスでマシンにログインできるようになるまでのユーザの待機時間を指定します。制限タイムアウト値は、サロゲート タイムアウト値よりも大きい値でなければなりません。 `authcache` CLI コマンドを使用して、認証キャッシュから特定のユーザやすべてのユーザを削除できます。
詳細設定(Advanced)	クレデンシャルの暗号化またはアクセス コントロールを使用している場合は、アプライアンスがそれに付属しているデジタル証明書とキー(Cisco IronPort Web セキュリティ アプライアンス デモ証明書)を使用するか、ここでアップロードするデジタル証明書を使用するかを選択できます。

ステップ 5　Web プロキシが明示的な転送モードで展開されている場合は、以下の設定項目を編集します。

設定	説明
クレデンシャルの暗号化(Credential Encryption)	クライアントが暗号化 HTTPS 接続を介して Web プロキシにログイン クレデンシャルを送信するかどうかを指定します。クレデンシャルの暗号化をイネーブルにするには、[HTTPS リダイレクト(セキュアな)(HTTPS Redirect (Secure))] を選択します。クレデンシャルの暗号化をイネーブルにすると、認証のためにクライアントを Web プロキシにリダイレクトする方法を設定する追加フィールドが表示されます。 この設定は基本認証方式と NTLMSPP 認証方式の両方に適用されますが、特に基本認証方式の場合に役立ちます。基本認証方式では、ユーザ クレデンシャルがプレーン テキストで送信されるからです。 詳細については、認証の失敗(5-31 ページ)を参照してください。
HTTPS リダイレクト ポート(HTTPS Redirect Port)	HTTPS 接続を介してユーザ認証要求をリダイレクトする場合に使用する TCP ポートを指定します。 これによって、クライアントが HTTPS による Web プロキシへの接続を開始するポートが指定されます。これは、クレデンシャルの暗号化がイネーブルになっている場合や、アクセス コントロールの使用時にユーザに認証を求める場合に発生します。

設定	説明
リダイレクト ホスト名（Redirect Hostname）	Web プロキシが着信接続をリッスンするネットワーク インターフェイスの短縮形のホスト名を入力します。 上記の認証モードをイネーブルにすると、Web プロキシは、ユーザの認証のためにクライアントに送信するリダイレクション URL でこのホスト名を使用します。 以下の値のいずれかを入力できます。 • [1 語のホスト名（Single word hostname）]。クライアントと Web セキュリティ アプライアンス が DNS 解決可能な 1 語のホスト名を入力できます。これにより、クライアントは、ブラウザ側を設定することなく、Internet Explorer で真のシングル サインオンを実現できます。 必ず、クライアントと Web セキュリティ アプライアンス が DNS 解決可能な 1 語のホスト名を入力してください。 たとえば、クライアントがドメイン `mycompany.com` にあり、Web プロキシがリッスンしているインターフェイスの完全なホスト名が `proxy.mycompany.com` である場合は、このフィールドに「`proxy`」と入力する必要があります。クライアントは「`proxy`」に対してルックアップを実行し、`proxy.mycompany.com` を解決できます。 • [完全修飾ドメイン名（FQDN）（Fully qualified domain name (FQDN)）]。このフィールドに、FQDN または IP アドレスを入力することもできます。ただし、その場合、Internet Explorer や Firefox ブラウザで真のシングル サインオンを実現するには、入力する FQDN または IP アドレスが、クライアント ブラウザのクライアント信頼済みサイト リストに追加されていることを確認する必要があります。 デフォルト値は、プロキシ トラフィックに使用されるインターフェイスに応じて、M1 または P1 インターフェイスの FQDN です。
クレデンシャル キャッシュ オプション:（Credential Cache Options:） サロゲート タイムアウト（Surrogate Timeout）	クライアントに認証クレデンシャルを再度要求するまでに、Web プロキシが待機する時間を指定します。クレデンシャルを再度要求するまで、Web プロキシはサロゲートに保存された値（IP アドレスまたは Cookie）を使用します。 一般的に、ブラウザなどのユーザ エージェントでは、ユーザが毎回クレデンシャルを入力する必要がないように、認証クレデンシャルがキャッシュされます。
クレデンシャル キャッシュ オプション:（Credential Cache Options:） クライアント IP アイドル タイムアウト（Client IP Idle Timeout）	IP アドレスを認証サロゲートとして使用する場合は、この設定で、クライアントがアイドル状態のときに、認証クレデンシャルをクライアントに再要求するまで Web プロキシが待機する時間を指定します。 この値がサロゲート タイムアウト値よりも大きい場合、この設定には効力がなく、サロゲート タイムアウトに達した後にクライアントへの認証要求が行われます。 この設定を使用すると、コンピュータの前にいない時間が多いユーザの脆弱性を低減できます。

設定	説明
クレデンシャル キャッシュ オプション:(Credential Cache Options:) キャッシュ サイズ(Cache Size)	認証キャッシュに格納するエントリの数を指定します。この値を設定すると、実際にこのデバイスを使用しているユーザの数に安全に対応できます。デフォルト値は推奨されている設定です。
ユーザ セッション制限(User Session Restrictions)	認証済みユーザが複数の IP アドレスから同時にインターネットにアクセスすることを許可するかどうかを指定します。 ユーザが未認証ユーザと認証クレデンシャルを共有しないように、1 つのマシンへのアクセスを制限できます。ユーザが別のマシンでログインできない場合は、エンド ユーザ通知ページが表示されます。このページの [再認証(Re-authentication)] 設定を使用し、ユーザがボタンをクリックして別のユーザ名でログインできるかどうかを指定することもできます。 この設定をイネーブルにする場合は、制限タイムアウト値を入力します。この値によって、別の IP アドレスでマシンにログインできるようになるまでのユーザの待機時間を指定します。制限タイムアウト値は、サロゲート タイムアウト値よりも大きい値でなければなりません。 `authcache` CLI コマンドを使用して、認証キャッシュから特定のユーザやすべてのユーザを削除できます。
詳細設定(Advanced)	クレデンシャルの暗号化またはアクセス コントロールを使用している場合は、アプライアンスがそれに付属しているデジタル証明書とキー(Cisco IronPort Web セキュリティ アプライアンス デモ証明書)を使用するか、ここでアップロードするデジタル証明書を使用するかを選択できます。 デジタル証明書とキーをアップロードするには、[参照(Browse)] をクリックして、ローカル マシン上の必要なファイルに移動します。次に、目的のファイルを選択してから、[ファイルのアップロード(Upload Files)] をクリックします。

ステップ 6　変更を送信し、保存します。

認証シーケンス

認証シーケンスについて

認証シーケンスを使用すると、さまざまな認証サーバやプロトコルで 1 つ の ID によってユーザを認証できます。認証シーケンスは、プライマリ認証オプションを使用できなくなった場合にバックアップ オプションを提供する上でも役立ちます。

認証シーケンスは複数の認証レルムの集合です。使用するレルムには、さまざまな認証サーバや認証プロトコルを指定できます。認証レルムの詳細については、認証レルム（5-11 ページ）を参照してください。

2 番目の認証レルムを作成すると、[ネットワーク（Network）] > [認証（Authentication）] に、[すべてのレルム（All Realms）] というデフォルトの認証シーケンスを含む [レルム シーケンス（Realm Sequences）] セクションが自動的に表示されます。[すべてのレルム（All Realms）] シーケンスには、ユーザが定義した各レルムが自動的に含まれます。[すべてのレルム（All Realms）] シーケンス内のレルムの順序は変更できますが、[すべてのレルム（All Realms）] シーケンスを削除したり、そこからレルムを削除することはできません。

複数の NTLM 認証レルムを定義した場合、Web セキュリティ アプライアンスは、各シーケンスの 1 つの NTLM 認証レルムだけを NTLMSSP 認証方式で使用します。[すべてのレルム（All Realms）] シーケンスを含め、各シーケンス内から、NTLMSSP で使用する NTLM 認証レルムを選択できます。複数の NTLM レルムを NTLMSSP で使用するには、各レルムに対して個々に識別プロファイルを定義します。

認証で使用されるシーケンス内の認証レルムは、以下によって決まります。

- 使用される認証方式。通常これは、クライアントに入力したクレデンシャル タイプで指定されます
- シーケンス内でのレルムの順序（1 つの NTLMSSP レルムだけを使用できるので、基本レルムのみ）。

ヒント　最適なパフォーマンスを得るには、1 つのレルムを使用して同じサブネット上のクライアントを認証します。

認証シーケンスの作成

はじめる前に

- 複数の認証レルムを作成します（認証レルム（5-11 ページ）を参照）。
- Web セキュリティ アプライアンスがセキュリティ管理アプライアンスで管理されている場合は、異なる Web セキュリティ アプライアンス上の同名の認証レルムのプロパティが、各アプライアンスで定義されているプロパティと同じであることを確認します。
- AsyncOS では、レルムを使用して認証を処理する際に、リストの先頭のレルムから順番に使用されることに注意してください。

ステップ 1　[ネットワーク（Network）] > [認証（Authentication）] を選択します。

ステップ 2　[シーケンスを追加（Add Sequence）] をクリックします。

ステップ 3　英数字とスペース文字を使用して、シーケンスの一意の名前を入力します。

ステップ 4　[基本スキームのレルムシーケンス（Realm Sequence for Basic Scheme）] 領域の最初の行で、シーケンスに含める最初の認証レルムを選択します。

ステップ 5　[基本スキームのレルム シーケンス(Realm Sequence for Basic Scheme)] 領域の 2 番目の行で、シーケンスに含める以下のレルムを選択します。

ステップ 6　(任意)基本クレデンシャルを使用する他のレルムを追加するには、[行の追加(Add Row)] をクリックします。

ステップ 7　NTLM レルムを定義したら、[NTLMSSP スキームのレルム(Realm for NTLMSSP Scheme)] フィールドで NTLM レルムを選択します。

Web プロキシは、クライアントが NTLMSSP 認証クレデンシャルを送信するときに、この NTLM レルムを使用します。

ステップ 8　変更を送信し、保存します。

認証シーケンスの編集および順序変更

ステップ 1　[ネットワーク(Network)] > [認証(Authentication)] を選択します。

ステップ 2　編集または順序変更するシーケンスの名前をクリックします。

ステップ 3　レルムを配置するシーケンス内の位置番号に対応する行で、[レルム(Realms)] ドロップダウンリストからレルム名を選択します。

(注)　[すべてのレルム(All Realms)] シーケンスの場合は、レルムの順序のみを変更できます。レルム自体を変更することはできません。[すべてのレルム(All Realms)] シーケンス内のレルムの順序を変更するには、[順序(Order)] 列の矢印をクリックして、該当するレルムの位置を変更します。

ステップ 4　すべてのレルムをリストアップして順序付けするまで、必要に応じてステップ 3 を繰り返し、各レルム名が 1 つの行にのみ表示されていることを確認します。

ステップ 5　変更を送信し、保存します。

認証シーケンスの削除

はじめる前に

- 認証レルムを削除すると関連する ID がディセーブルになり、さらに、関連するポリシーからそれらの ID が削除されるので注意してください。

ステップ 1　[ネットワーク(Network)] > [認証(Authentication)] を選択します。

ステップ 2　シーケンス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 3　[削除(Delete)] をクリックして、シーケンスを削除することを確定します。

ステップ 4　変更を保存します。

認証の失敗

認証の失敗について

以下の理由により認証に失敗したため、ユーザが Web からブロックされることがあります。

- **クライアント/ユーザ エージェントの制限。**一部のクライアント アプリケーションでは、認証が適切にサポートされないことがあります。認証を必要としない識別プロファイルを設定し、識別プロファイルの基準をそのクライアント（およびアクセスする必要がある URL（任意））に基づかせることで、これらのクライアントの認証をバイパスできます。
- **認証サービスを使用できない。**ネットワークまたはサーバの問題によって、認証サービスを使用できない場合があります。このような状況が生じた場合に未認証トラフィックを許可することを選択できます。
- **クレデンシャルが無効である。**ユーザによっては、適切な認証を得るための有効なクレデンシャルを提供できないことがあります（ビジターやクレデンシャルを待っているユーザなど）。そのようなユーザに制限付きの Web アクセスを許可するかどうかを選択できます。

関連項目

- 問題のあるユーザ エージェントの認証のバイパス（5-31 ページ）
- 認証のバイパス（5-33 ページ）
- 認証サービスが使用できない場合の未認証トラフィックの許可（5-33 ページ）
- 認証失敗後のゲスト アクセスの許可（5-33 ページ）

問題のあるユーザ エージェントの認証のバイパス

一部のユーザ エージェントには、通常の動作に影響する認証問題があることが判明されています。

以下のユーザ エージェント経由で認証をバイパスする必要があります。

- Windows Update エージェント
- MICROSOFT_DEVICE_METADATA_RETRIEVAL_CLIENT
- Microsoft BITS
- SLSSoapClient
- Akamai NetSession Interface
- Microsoft CryptoAPI
- NCSI
- MSDW

- Gnotify
- msde
- Google Update

（注）　トラフィックのフィルタリング（URL カテゴリに基づく）とスキャン（McAfee、Webroot）は、引き続き、アクセス ポリシー設定に従い、アクセス ポリシーによって実行されます。

ステップ 1　指定したユーザ エージェントとの認証をバイパスするように識別プロファイルを設定します。

a. [Web セキュリティ マネージャ（Web Security Manager）] > [識別プロファイル（Identification Profile）] を選択します。

b. [識別プロファイルの追加（Add Identification Profile）] をクリックします。

c. 情報を入力します。

オプション	値
名前（Name）	ユーザ エージェントの AuthExempt 識別プロファイル。
上に挿入（Insert Above）	処理順序の最初のプロファイルに設定します。
サブネット別メンバの定義（Define Members by Subnet）	ブランクのままにします。
認証ごとにメンバを定義（Define Members by Authentication）	認証は不要です。

d. [詳細設定（Advanced）] > [ユーザ エージェント（User Agents）] をクリックします。

e. [選択なし（None Selected）] をクリックします。

f. [カスタムユーザエージェント（Custom User Agents）] で、問題のあるユーザ エージェントの文字列を指定します。

ステップ 2　アクセス ポリシーの設定

a. [Web セキュリティ マネージャ（Web Security Manager）] > [アクセス ポリシー（Access Policies）] を選択します。

b. [ポリシーを追加（Add Policy）] をクリックします。

c. 情報を入力します。

オプション	値
ポリシー名	ユーザ エージェントの認証免除
上記ポリシーを挿入（Insert Above Policy）	処理順序の最初のポリシーに設定します。
識別プロファイル ポリシー（Identification Profile Policy）	ユーザ エージェントの AuthExempt 識別プロファイル。
詳細設定（Advanced）	なし

ステップ 3　変更を送信し、保存します。

認証のバイパス

手順	詳細情報
1. [詳細設定（Advanced）] プロパティを設定して、影響を受ける Web サイトを含むカスタム URL カテゴリを作成します。	Creating and Editing Custom URL Categories（9-14 ページ）
2. 以下の特性を持つ識別プロファイルを作成します。 – 認証を必要とする ID が特に配置されている。 – カスタム URL カテゴリが含まれている。 – 影響を受けるクライアント アプリケーションが含まれている。 – 認証を必要としない。	ユーザおよびクライアント ソフトウェアの分類（6-3 ページ）
3. 識別プロファイルのポリシーを作成します。	Creating a Policy（10-7 ページ）

関連項目

- Web プロキシのバイパス

認証サービスが使用できない場合の未認証トラフィックの許可

（注） この設定は、認証サービスを使用できない場合にのみ適用されます。恒久的に認証をバイパスするわけではありません。代替の方法については、認証の失敗について（5-31 ページ）を参照してください。

ステップ 1 [ネットワーク（Network）] > [認証（Authentication）] を選択します。

ステップ 2 [グローバル設定を編集（Edit Global Settings）] をクリックします。

ステップ 3 [認証サーバが利用できない場合のアクション（Action if Authentication Service Unavailable）] フィールドで、[認証なしでトラフィックの通過を許可（Permit traffic to proceed without authentication）] をクリックします。

ステップ 4 変更を送信し、保存します。

認証失敗後のゲスト アクセスの許可

ゲスト アクセスを許可するには、以下の手順を実行する必要があります。

1. ゲスト アクセスをサポートする識別プロファイルの定義（5-34 ページ）
2. ゲスト アクセスをサポートしている識別プロファイルのポリシーでの使用（5-34 ページ）
3. （任意）ゲスト ユーザの詳細の記録方法の設定（5-35 ページ）

（注） 識別プロファイルがゲスト アクセスを許可しており、その識別プロファイルを使用しているユーザ定義のポリシーがない場合、認証に失敗したユーザは適切なポリシー タイプのグローバル ポリシーと照合されます。たとえば、MyIdentificationProfile がゲスト アクセスを許可し、MyIdentificationProfile を使用するユーザ定義のアクセス ポリシーがない場合、認証に失敗したユーザはグローバル アクセス ポリシーに一致します。ゲスト ユーザをグローバル ポリシーと照合しない場合は、ゲスト ユーザに適用してすべてのアクセスをブロックするポリシー グループを、グローバル ポリシーよりも上に作成します。

ゲスト アクセスをサポートする識別プロファイルの定義

ステップ 1 [Web セキュリティ マネージャ（Web Security Manager）] > [識別プロファイル（Identification Profiles）] を選択します。

ステップ 2 [識別プロファイルの追加（Add Identification Profile）] をクリックして新しい ID を追加するか、使用する既存の ID の名前をクリックします。

ステップ 3 [ゲスト権限をサポート（Support Guest Privileges）] 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。

ゲスト アクセスをサポートしている識別プロファイルのポリシーでの使用

ステップ 1 [Web セキュリティ マネージャ（Web Security Manager）] メニューからポリシー タイプを選択します。

ステップ 2 ポリシー テーブル内のポリシー名をクリックします。

ステップ 3 [識別プロファイルおよびユーザ（Identification Profiles And Users）] ドロップダウン リストから、[1 つ以上の識別プロファイルを選択（Select One Or More Identification Profiles）] を選択します（まだ選択していない場合）。

ステップ 4 [識別プロファイル（Identification Profile）] 列のドロップダウン リストから、ゲスト アクセスをサポートしているプロファイルを選択します。

ステップ 5 [ゲスト（認証に失敗したユーザ）（Guests (Users Failing Authentication)）] オプション ボタンをクリックします。

（注） このオプションを使用できない場合は、選択した**プロファイル**がゲスト アクセスをサポートするように設定されていないことを示しています。ステップ 4 に戻って別のものを選択するか、ゲスト アクセスをサポートする識別プロファイルの定義（5-34 ページ）を参照して、新しいポリシーを定義してください。

ステップ 6 変更を送信し、保存します。

ゲスト ユーザの詳細の記録方法の設定

ステップ 1　[ネットワーク（Network）] > [認証（Authentication）] を選択します。

ステップ 2　[グローバル設定を編集（Edit Global Settings）] をクリックします。

ステップ 3　[失敗した認証手続き（Failed Authentication Handling）] フィールドで、次に示す [ゲストユーザのログ方法（Log Guest User By）] のオプション ボタンをクリックします。

オプション ボタン	説明
[IP アドレス（IP Address）]	ゲスト ユーザのクライアント IP アドレスがアクセス ログに記録されます。
エンドユーザが入力したユーザ名（User Name As Entered By End-User）	最初に認証に失敗したユーザ名がアクセス ログに記録されます。

ステップ 4　変更を送信し、保存します。

認証の失敗：異なるクレデンシャルによる再認証の許可

異なるクレデンシャルによる再認証の許可について

前に使用したクレデンシャルが認証に失敗した場合に、ユーザが別のクレデンシャルを使用して再認証を受けることを許可するには、再認証機能を使用します。ユーザは正常に認証されますが、アクセスが許可されない限り、Web リソースにはアクセスできません。これは、認証は、検証したクレデンシャルをポリシーに渡すためにユーザを識別するだけであり、リソースへのユーザのアクセスを許可（または禁止）するのはポリシーだからです。

再認証を受けるには、ユーザは正常に認証されている必要があります。

- ユーザ定義のエンドユーザ通知ページで再認証機能を使用するには、リダイレクト URL を解析する CGI スクリプトで Reauth_URL パラメータを解析して使用する必要があります。

異なるクレデンシャルによる再認証の許可

ステップ 1　[ネットワーク（Network）] > [認証（Authentication）] を選択します。

ステップ 2　[グローバル設定を編集（Edit Global Settings）] をクリックします。

ステップ 3　[URL カテゴリまたはユーザ セッションの制限によりエンド ユーザがブロックされた場合に再認証プロンプト（Re-Authentication Prompt If End User Blocked by URL Category or User Session Restriction）] チェックボックスをオンにします。

ステップ 4　[送信（Submit）] をクリックします。

識別済みユーザの追跡

（注）　アプライアンスがクッキー ベースの認証サロゲートを使用するように設定されている場合、アプライアンスは HTTP 要求を介した HTTPS および FTP のクライアントからクッキー情報を取得しません。このため、クッキーからユーザ名を取得できません。

明示的要求でサポートされる認証サロゲート

サロゲート タイプ	クレデンシャルの暗号化がディセーブルの場合			クレデンシャルの暗号化がイネーブルの場合		
プロトコル:	HTTP	HTTPS および FTP over HTTP	ネイティブ FTP	HTTP	HTTPS および FTP over HTTP	ネイティブ FTP
サロゲートなし	○	○	○	NA	NA	NA
IP ベース	○	○	○	○	○	○
Cookie ベース	○	○***	○***	○	×/○**	○***

透過的要求でサポートされる認証サロゲート

（注）　ユーザおよびクライアント ソフトウェアの分類（6-3 ページ）の [認証サロゲート（Authentication Surrogates）] オプションの説明も参照してください。

サロゲート タイプ	クレデンシャルの暗号化がディセーブルの場合			クレデンシャルの暗号化がイネーブルの場合		
プロトコル:	HTTP	HTTPS	ネイティブ FTP	HTTP	HTTPS	ネイティブ FTP
サロゲートなし	NA	NA	NA	NA	NA	NA
IP ベース	○	×/○*	×/○*	○	×/○*	×/○*
Cookie ベース	○	×/○**	×/○**	○	×/○**	×/○**

* クライアントが HTTP サイトに要求を送信し、認証された後に機能します。その前の動作は、トランザクション タイプによって異なります。

- **ネイティブ FTP トランザクション。**トランザクションが認証をバイパスします。
- **HTTPS トランザクション。**トランザクションがドロップされます。ただし、認証を目的とする最初の HTTPS 要求を復号化するように HTTPS プロキシを設定できます。

** Cookie ベースの認証を使用している場合、Web プロキシは、HTTPS、ネイティブ FTP、および FTP over HTTP の各トランザクションに対してユーザを認証できません。この制限により、すべての HTTPS、ネイティブ FTP、FTP over HTTP の要求が認証をバイパスするため、認証は要求されません。

*** この場合は、Cookie ベースのサロゲートが設定されていても、サロゲートは使用されません。

関連項目

- 識別プロファイルと認証（6-8 ページ）

再認証ユーザの追跡

再認証の場合、より強力な権限を持つユーザが認証を求め承認されると、Web プロキシは、設定されている認証サロゲートに応じた期間だけこのユーザの ID をキャッシュします。

- [セッション Cookie（Session cookie）]。特権ユーザのアイデンティティが、ブラウザを閉じるか、セッションがタイム アウトになるまで使用されます。
- [永続的な Cookie（Persistent cookie）]。特権ユーザのアイデンティティが、サロゲートがタイムアウトするまで使用されます。
- [IP アドレス（IP Address）]。特権ユーザのアイデンティティが、サロゲートがタイムアウトするまで使用されます。
- [サロゲートなし（No surrogate）]。デフォルトでは、Web プロキシは新しい接続ごとに認証を要求しますが、再認証がイネーブルの場合は新しい要求ごとに認証を要求します。そのため、NTLMSSP を使用すると認証サーバの負荷が増大します。ただし、認証アクティビティの増加はユーザにはわからない場合があります。ほとんどのブラウザでは、ブラウザが閉じられるまで特権ユーザのクレデンシャルがキャッシュされ、再入力を求めることなく認証が行われるからです。また、Web プロキシが透過モードで展開され、[明示的転送要求に同じサロゲート設定を適用（Apply same surrogate settings to explicit forward requests）] オプションがイネーブルでない場合は、明示的な転送要求に認証サロゲートが使用されず、再認証により負荷が増加します。

（注）　Web セキュリティ アプライアンスが認証サロゲートに Cookie を使用する場合は、クレデンシャルの暗号化をイネーブルにすることを推奨します。

クレデンシャル

認証クレデンシャルは、ユーザのブラウザまたは別のクライアント アプリケーションを介してユーザに認証クレデンシャルの入力を求めることによってユーザから取得されるか、または別のソースから透過的に取得されます。

- セッション中のクレデンシャルの再利用の追跡（5-37 ページ）
- 認証および承認の失敗（5-38 ページ）
- クレデンシャルの形式（5-38 ページ）
- 基本認証のクレデンシャルの暗号化（5-39 ページ）

セッション中のクレデンシャルの再利用の追跡

セッション中に 1 回ユーザを認証した後、認証サロゲートを使用すると、新しい要求ごとにユーザを認証するのでなく、そのセッション全体におけるクレデンシャルの再利用を追跡できます。認証サロゲートは、ユーザのワークステーションの IP アドレスまたはセッションに割り当てられた Cookie に基づくことができます。

Internet Explorer の場合は、リダイレクト ホスト名として、完全修飾ドメイン名ではなく、(ドットを含まない)短縮形のホスト名または NetBIOS 名を必ず使用します。または、Internet Explorer の [ローカル イントラネット] ゾーンにアプライアンスのホスト名を追加することができます([ツール] > [インターネット オプション] > [セキュリティ] タブ)。ただし、この操作をすべてのクライアントで実行する必要があります。これに関する詳細については、『How do I properly set up NTLM with SSO (credentials sent transparently)?』を参照してください。

Firefox およびその他の Microsoft 以外のブラウザでは、パラメータ **network.negotiate-auth.delegation-uris**、**network.negotiate-auth.trusted-uris**、**network.automatic-ntlm-auth.trusted-uris** を透過モードのリダイレクト ホスト名に設定する必要があります。『Firefox is not sending authentication credentials transparently (SSO)』も参照してください。この記事には、Firefox パラメータの変更に関する一般情報が記載されています。

リダイレクト ホスト名については、グローバル認証の設定、または CLI コマンド sethostname を参照してください。

認証および承認の失敗

互換性のないクライアント アプリケーションなど、容認できる理由で認証に失敗した場合は、ゲスト アクセスを許可できます。

認証に成功したが、承認に失敗した場合は、要求したリソースへのアクセスが許可される可能性がある別のクレデンシャル セットによる再認証を許可できます。

関連項目

- 認証失敗後のゲスト アクセスの許可(5-33 ページ)
- 異なるクレデンシャルによる再認証の許可(5-35 ページ)

クレデンシャルの形式

認証方式	クレデンシャルの形式
NTLMSSP	`MyDomain\jsmith`

基本	`jsmith`
	`MyDomain\jsmith`
	(注)　ユーザが Windows ドメインを入力しなかった場合は、Web プロキシによってデフォルトの Windows ドメインが付加されます。

基本認証のクレデンシャルの暗号化

基本認証のクレデンシャルの暗号化について

暗号化した形式でクレデンシャルを HTTPS 経由で送信するには、クレデンシャルの暗号化をイネーブルにします。これによって、基本認証プロセスのセキュリティが向上します。

デフォルトでは、Web セキュリティ アプライアンスは、認証の安全を確保するために、自身の証明書と秘密キーを使用してクライアントとの HTTPS 接続を確立します。ただし、大部分のブラウザでは、この証明書が無効であることがユーザに警告されます。無効な証明書に関するメッセージをユーザに表示しないようにするには、組織で使用している有効な証明書とキーのペアをアップロードします。

クレデンシャル暗号化の設定

はじめる前に:

- IP サロゲートを使用するようにアプライアンスを設定します。
- （任意）証明書と暗号化された秘密キーを取得します。ここで設定した証明書とキーは、アクセス コントロールでも使用されます。

ステップ 1　[ネットワーク（Network）] > [認証（Authentication）] を選択します。

ステップ 2　[グローバル設定を編集（Edit Global Settings）] をクリックします。

ステップ 3　[クレデンシャルの暗号化（Credential Encryption）]フィールドで、[認証には暗号化された HTTPS 接続を使用（Use Encrypted HTTPS Connection For Authentication）] チェックボックスをオンにします。

ステップ 4　（任意）認証時のクライアントの HTTPS 接続に対して、[HTTPS リダイレクトポート（HTTPS Redirect Port）] フィールドでデフォルトのポート番号（443）を編集します。

ステップ 5　（任意）証明書とキーをアップロードします。

a. [詳細設定（Advanced）] セクションを展開します。

b. [証明書（Certificate）] フィールドで [参照（Browse）] をクリックし、アップロードする証明書ファイルを検索します。

c. [キー（Key）] フィールドで [参照（Browse）] をクリックし、アップロードする秘密キー ファイルを検索します。

d. [ファイルのアップロード（Upload File）] をクリックします。

ステップ 6　変更を送信し、保存します。

関連項目

- 証明書の管理（12-23 ページ）。

認証に関するトラブルシューティング

CHAPTER 6

エンドユーザおよびクライアント ソフトウェアの分類

ユーザおよびクライアント ソフトウェアの分類:概要

識別プロファイルによるユーザおよびユーザ エージェント(クライアント ソフトウェア)の分類は、以下の目的のために行われます。

- ポリシーの適用に対するトランザクション要求をグループ化します(SaaS を除く)。
- 識別および認証の要件の指定

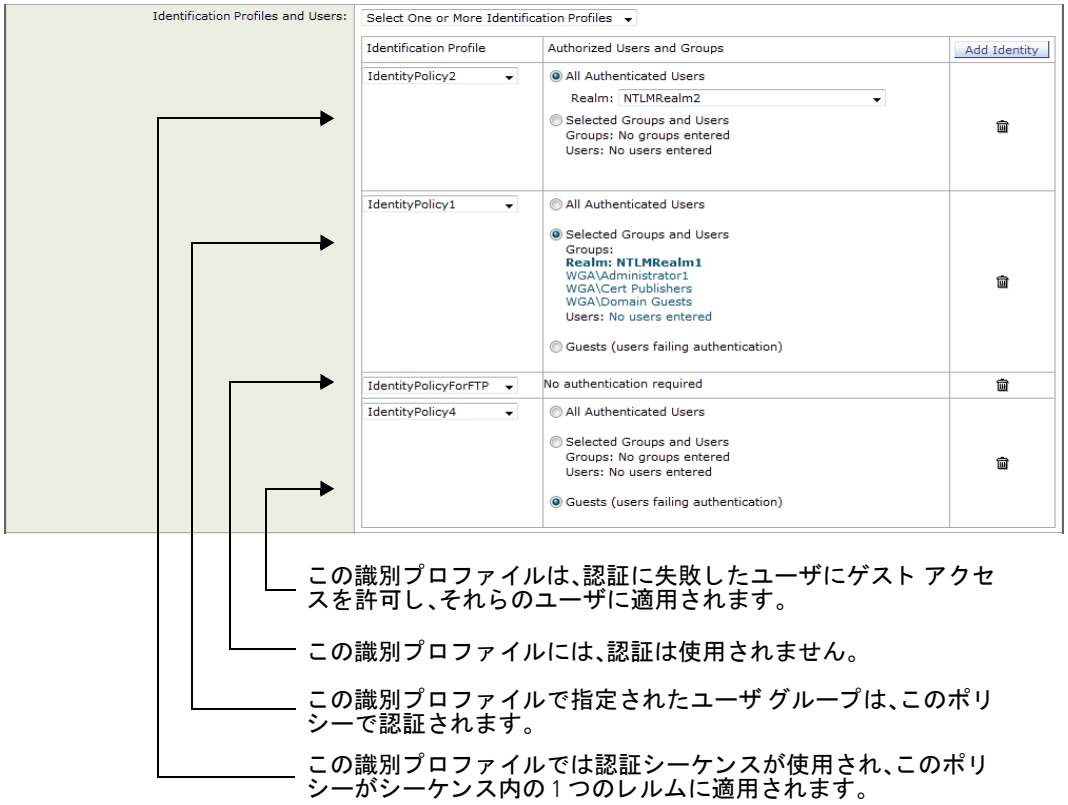
AsyncOS はすべてのトランザクションに識別プロファイルを割り当てます。

- カスタム識別プロファイル:AsyncOS は、そのアイデンティティの条件に基づいてカスタム プロファイルを割り当てます。
- グローバル識別プロファイル:AsyncOS は、カスタム プロファイルの条件を満たさないトランザクションにグローバル プロファイルを割り当てます。デフォルトでは、グローバル プロファイルには認証が必要ありません。

AsyncOS は最初から順番に識別プロファイルを処理します。グローバル プロファイルは最後のプロファイルです。

識別プロファイルには 1 つの条件だけを含めることができます。複数の条件を含む識別プロファイルはすべての条件を満たす必要があります。

1 つのポリシーによって複数の識別プロファイルを要求できます。



ユーザおよびクライアント ソフトウェアの分類:ベスト プラクティス

- 一般的な識別プロファイルを少数作成して、すべてのユーザまたは少数の大きなユーザ グループに適用します。より詳細に管理する場合は、プロファイルではなくポリシーを使用します。
- 一意の条件で識別プロファイルを作成します。
- 透過 モードで展開する場合は、認証をサポートしていないサイトの識別プロファイルを作成します。認証のバイパス (5-33 ページ) を参照してください。

識別プロファイルの条件

これらのトランザクションの特性は、以下の識別プロファイルの定義に使用できます。

オプション	説明
サブネット	クライアント サブネットは、ポリシーのサブネット リストに一致している必要があります。
[Protocol]	トランザクションで使用されるプロトコル（HTTP、HTTPS、SOCKS、またはネイティブ FTP）
[ポート（Port）]	要求のプロキシ ポートは、識別プロファイルのポート リストに記載されている必要があります（リストに記載がある場合）。明示的な転送接続のために、ブラウザに設定されたポートです。透過接続の場合は、宛先ポートと同じです。
ユーザ エージェント（User Agent）	要求を行うユーザ エージェント（クライアント アプリケーション）は、識別プロファイルのユーザ エージェント リストに記載されている必要があります（リストに記載がある場合）。一部のユーザ エージェントは認証を処理できないため、認証を必要としないプロファイルを作成する必要があります。ユーザ エージェントには、アップデータやブラウザ（Internet Explorer、Mozilla Firefox など）などのプログラムが含まれています。
URL カテゴリ（URL Category）	要求 URL の URL カテゴリは、識別プロファイルの URL カテゴリ リストに記載されている必要があります（リストに記載がある場合）。
認証要件（Authentication requirements）	識別プロファイルが認証を必要とする場合は、クライアントの認証クレデンシャルが識別プロファイルの認証要件と一致する必要があります。

ユーザおよびクライアント ソフトウェアの分類

はじめる前に

- 認証レルムを作成します。Active Directory 認証レルムの作成（NTLMSSP および基本）（5-15 ページ）または LDAP 認証レルムの作成（5-18 ページ）を参照してください。
- 識別プロファイルへの変更を確定するときに、エンド ユーザを再認証する必要あるので注意してください。
- クラウド コネクタ モードの場合は、追加の識別プロファイル オプション（マシン ID）を使用できます。Identifying Machines for Policy Application（3-7 ページ）を参照してください。
- （任意）認証シーケンスを作成します。認証シーケンスの作成（5-29 ページ）を参照してください。
- （任意）識別プロファイルにモバイル ユーザを含める場合は、セキュア モビリティをイネーブルにします。
- （任意）認証サロゲートについて理解しておきます。識別済みユーザの追跡（5-36 ページ）を参照してください。

ステップ 1　[Web セキュリティマネージャ（Web Security Manager）] > [識別プロファイル（Identification Profiles）] を選択します。

ステップ 2　[プロファイルの追加（Add Profile）] をクリックしてプロファイルを追加します。

ステップ 3　[識別プロファイルの有効化（Enable Identification Profile）] チェックボックスを使用して、このプロファイルをイネーブルにするか、プロファイルを削除せずにただちにディセーブルにします。

ステップ 4　[名前（Name）] に一意のプロファイル名を割り当てます。

ステップ 5　[説明（Description）] は任意です。

ステップ 6　[上に挿入（Insert Above）] ドロップダウン リストから、このプロファイルを配置するポリシー テーブル内の位置を選択します。

（注）　認証を必要とする最初の識別プロファイルの上に、認証を必要としない識別プロファイルを配置します。

ステップ 7　[ユーザ識別方式（User Identification Method）] セクションで、識別方式を選択して関連パラメータを指定します。表示されるオプションは、選択した方法によって異なります。

2 つのタイプの方式があります（認証/識別の除外 およびユーザの認証）。

a. [ユーザ識別方式（User Identification Method）] ドロップダウン リストから識別方式を選択します。

オプション	説明
認証/識別を免除（Exempt from authentication/ identification）	ユーザは基本的に IP アドレスによって識別されます。追加のパラメータは必要ありません。
認証済みユーザ（Authenticate users）	ユーザは入力した認証クレデンシャルによって識別されます。

（注）　少なくとも 1 つの識別プロファイルに認証または透過的識別が設定されている場合、ポリシー テーブルでは、ユーザ名、ディレクトリ グループ、セキュリティ グループ タグを使用してポリシー メンバーシップを定義できます。

b. 選択した方式に適したパラメータを指定します。この表に示したすべてのセクションが選択ごとに表示されるわけではありません。

認証レルム（Authentication Realm）	[レルムまたはシーケンスを選択（Select a Realm or Sequence）]：定義済みの認証レルムまたはシーケンスを選択します。 [スキームの選択（Select a Scheme）]：認証スキームを選択します。 • [Kerberos]：クライアントは Kerberos チケットによって透過的に認証されます。 • [基本（Basic）]：クライアントは常にユーザにクレデンシャルを要求します。ユーザがクレデンシャルを入力すると、通常は、入力したクレデンシャルの保存について指定するチェックボックスがブラウザに表示されます。ユーザがブラウザを開くたびに、クライアントはクレデンシャルの入力を要求するか、または以前に保存したクレデンシャルを再送信します。 クレデンシャルは、保護されていないクリア テキスト（Base64）として送信されます。クライアントと Web セキュリティ アプライアンス間でのパケット キャプチャにより、ユーザ名やパスフレーズが開示される可能性があります。 • [NTLMSSP]：クライアントは、Windows のログイン クレデンシャルを使用して透過的に認証します。ユーザはクレデンシャルの入力を要求されません。 ただし、以下の場合、クライアントはユーザにクレデンシャルの入力を求めます。 – Windows クレデンシャルによる認証が失敗した。 – ブラウザのセキュリティ設定が原因で、クライアントが Web セキュリティ アプライアンスを信頼しない。 クレデンシャルは、3 ウェイ ハンドシェイク（ダイジェスト形式の認証）により安全に送信されます。パスフレーズが接続を介して送信されることはありません。 • [ゲスト特権をサポート（Support Guest privileges）]：無効なクレデンシャルにより認証に失敗したユーザにゲスト アクセスを許可する場合、このチェックボックスをオンにします。

認証サロゲート（Authentication Surrogates）	認証の成功後にトランザクションをユーザに関連付ける方法を指定します（オプションは Web プロキシの展開モードにより異なります）。 • [IP アドレス（IP Address）]：Web プロキシは、特定の IP アドレスの認証済みユーザを追跡します。透過的ユーザ識別の場合は、このオプションを選択します。 • [永続的なクッキー（Persistent Cookie）]：Web プロキシは、アプリケーションごとに各ユーザ用に永続的クッキーを生成することにより、特定のアプリケーション上の認証済みユーザを追跡します。アプリケーションを終了してもクッキーは削除されません。 • [セッションクッキー（Session Cookie）]：Web プロキシは、アプリケーションごとに各ドメインの各ユーザ用に永続的クッキーを生成することにより、特定のアプリケーション上の認証済みユーザを追跡します。（ただし、ユーザが同じアプリケーションから同じドメインに対して異なるクレデンシャルを指定した場合、クッキーは上書きされます）。アプリケーションを終了するとクッキーは削除されます。 • [明示的フォワード要求に同じサロゲート設定を適用（Apply same surrogate settings to explicit forward requests）]：透過的要求に使用するサロゲートを明示的要求に適用する場合にオンにします（クレデンシャルの暗号化が自動的にイネーブルになります。）このオプションは、Web プロキシがトランスペアレント モードで展開されている場合にのみ表示されます。 **（注）** [グローバル認証設定（Global Authentication Settings）] で、すべての要求に対する認証サロゲートのタイムアウト値を定義できます。

ステップ 8　[メンバーシップの定義（Membership Definition）] セクションで、選択した識別方式に適したメンバーシップ パラメータを指定します。以下の表に示すオプションは、すべてのユーザ識別方式で使用できるわけではありません。

メンバーシップの定義	
サブネット別メンバの定義（Define Members by Subnet）	この識別プロファイルを適用するアドレスを入力します。IP アドレス、CIDR ブロック、およびサブネットを入力できます。 **（注）** 何も入力しない場合は、すべての IP アドレスにこの識別プロファイルが適用されます。

詳細設定（Advanced）	このセクションを展開して、追加のメンバーシップ要件を定義します。 • [プロキシポート（Proxy Ports）]：Web プロキシへのアクセスに使用する 1 つ以上のプロキシ ポートを指定します。ポート番号をカンマで区切って入力します。明示的な転送接続の場合、プロキシ ポートはブラウザで設定されます。 透過接続の場合は、宛先ポートと同じです。 ポート別の ID の定義は、アプライアンスが明示的な転送モードで展開されている場合、またはクライアントがアプライアンスに明示的に要求を転送する場合に最もよく機能します。クライアント要求が透過的にアプライアンスにリダイレクトされる場合は、ポート別の ID の定義によって一部の要求が拒否されることがあります。 • [URL カテゴリ（URL Categories）]：ユーザ定義または定義済みの URL カテゴリを選択します。デフォルトでは、両方のメンバーシップが除外されます。つまり、[追加（Add）] 列で選択されていない限り、Web プロキシはすべてのカテゴリを無視します。 URL カテゴリによってメンバーシップを定義する必要がある場合、そのカテゴリに対する認証要求から除外する必要のあるときは ID グループにのみ定義します。 • [ユーザ エージェント（User Agents）]：クライアント要求で見つかったユーザ エージェントごとにポリシー グループ メンバーシップを定義します。一般的に定義されているエージェントを選択するか、正規表現を使用して独自のブラウザを定義できます。 また、これらのユーザ エージェントの指定を含めるか除外するかも指定します。つまり、メンバーシップの定義に選択したユーザ エージェントのみを含めるか、選択したユーザ エージェントを明確に除外するかどうかを指定します。

ステップ 9　変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

関連項目

- エンドユーザ クレデンシャルの取得の概要（5-1 ページ）
- Managing Web Requests Through Policies Task Overview（10-3 ページ）

ID の有効化/無効化

はじめる前に

- 識別プロファイルをディセーブルにすると、関連するポリシーからその識別プロファイルが削除されるので注意してください。
- 識別プロファイルを再度イネーブルにしても、その識別プロファイルはポリシーに再び関連付けられません。

ステップ 1　[Web セキュリティマネージャ（Web Security Manager）] > [識別プロファイル（Identification Profiles）] を選択します。

ステップ 2　識別プロファイル テーブルのプロファイルをクリックして、そのプロファイルの[識別プロファイル（Identification Profile）] ページを開きます。

ステップ 3　[クライアント/ユーザ識別プロファイルの設定（Client/User Identification Profile Settings）] の真下にある [識別プロファイルの有効化（Enable dentification IProfile）] をオンまたはオフにします。

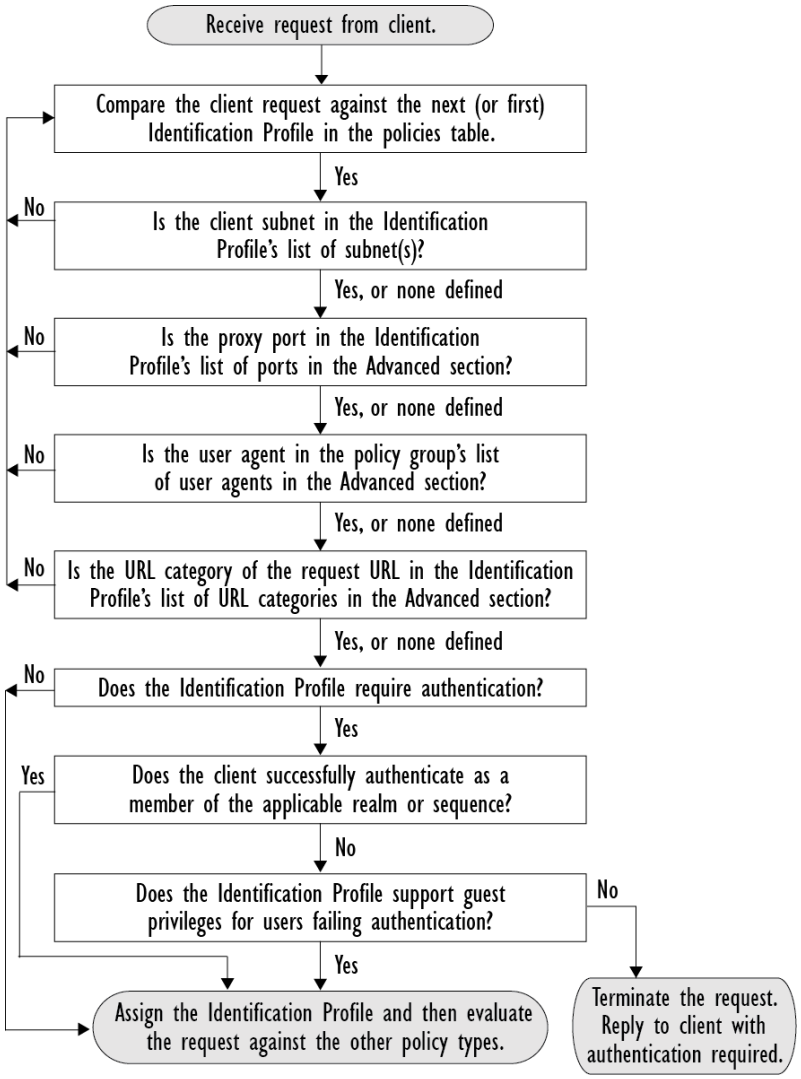
ステップ 4　変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

識別プロファイルと認証

次の図に、識別プロファイルが次を使用するように設定されているときに、Web プロキシがクライアント要求を識別プロファイルに対して評価する方法を示します。

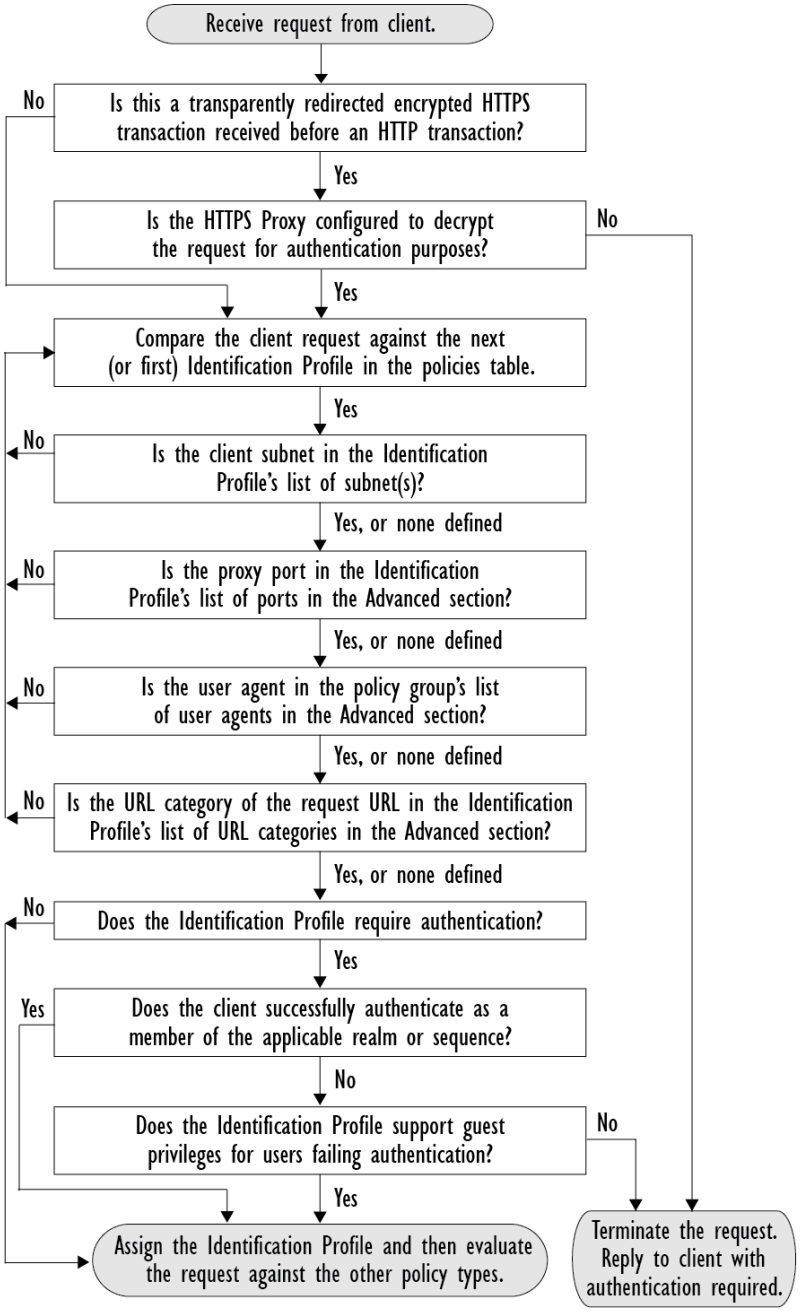
- 認証サロゲートなし
- 認証サロゲートとしての IP アドレス
- 透過的要求を使用する認証サロゲートとしてのクッキー
- 明示的要求を使用する認証サロゲートとしてのクッキー（クレデンシャルの暗号化がイネーブルになっている場合）

図 6-1　　識別プロファイルと認証プロセス：サロゲートおよび IP ベースのサロゲートなし



次の図に、識別プロファイルが認証サロゲートとして Cookie を使用し、クレデンシャルの暗号化を有効にして、要求が明示的に転送されるように設定されているときに、Web プロキシがクライアント要求を識別プロファイルに対して評価する方法を示します。

図 6-2　　識別プロファイルと認証プロセス：Cookie ベースのサロゲート



識別プロファイルのトラブルシューティング

CHAPTER 7

HTTPS トラフィックを制御する復号化ポリシーの作成

HTTPS トラフィックを制御する復号化ポリシーの作成：概要

復号化ポリシーで、Web プロキシ内の HTTPS トラフィックの処理が定義されます。

- HTTPS トラフィックを復号化するタイミング。
- 無効な、または失効したセキュリティ証明書を使用する要求の処理方法。

HTTPS トラフィックを以下のように処理する復号化ポリシーを作成できます。

- 暗号化されたトラフィックをパススルーする。
- トラフィックを復号化し、HTTP トラフィック用に定義されたコンテンツ ベースのアクセス ポリシーを適用する。これによって、マルウェア スキャンも可能になります。
- HTTPS 接続をドロップする。
- Web プロキシがポリシーに対して要求を評価しているときに、要求をモニタする（最終アクションは実行されない）。この評価によって、最終的にドロップ、パススルー、または復号化のアクションが実行されます。

注意 **個人識別情報の取り扱いに注意してください。**エンドユーザの HTTPS セッションを復号化することを選択した場合は、Web Security Appliance のアクセス ログとレポートに個人識別情報が含まれることがあります。管理者は `advancedproxyconfig` CLI コマンドと `HTTPS` サブコマンドを使用して、ログに保存する URI テキストの量を設定できます。URI 全体、またはクエリーの部分が除外された URI の部分的な形式をログに保存できます。ただし、URI からクエリーを削除することを選択した場合でも、個人を特定できる情報は残されたままになる可能性があります。

復号化ポリシー タスクによる HTTPS トラフィックの管理:概要

手順	復号化ポリシーによる HTTPS トラフィック管理のためのタスク リスト	関連項目および手順へのリンク
1	HTTPS プロキシをイネーブルにする	HTTPS プロキシのイネーブル化(7-4 ページ)
2	証明書とキーをアップロードまたは生成する	• ルート証明書およびキーのアップロード(7-10 ページ) • HTTPS プロキシ用の証明書およびキーの生成(7-10 ページ)
3	復号化オプションを設定する	復号化オプションの設定(7-7 ページ)
5	(任意)無効な証明書の処理を設定する	無効な証明書の処理の設定(7-11 ページ)
[6]	(任意)リアルタイムの失効ステータス チェックをイネーブルにする	リアルタイムの失効ステータス チェックのイネーブル化(7-12 ページ)
7	(任意)信頼された証明書とブロックされた証明書を管理する	信頼できるルート証明書(7-13 ページ)

復号化ポリシーによる HTTPS トラフィックの管理:ベスト プラクティス

- 一般的な復号化ポリシー グループを少数作成して、ネットワーク上のすべてのユーザまたは少数の大きなユーザ グループに適用します。その後、復号化された HTTPS トラフィックにきめ細かい管理を適用する必要がある場合は、より具体的なアクセス グループを使用します。

復号化ポリシー

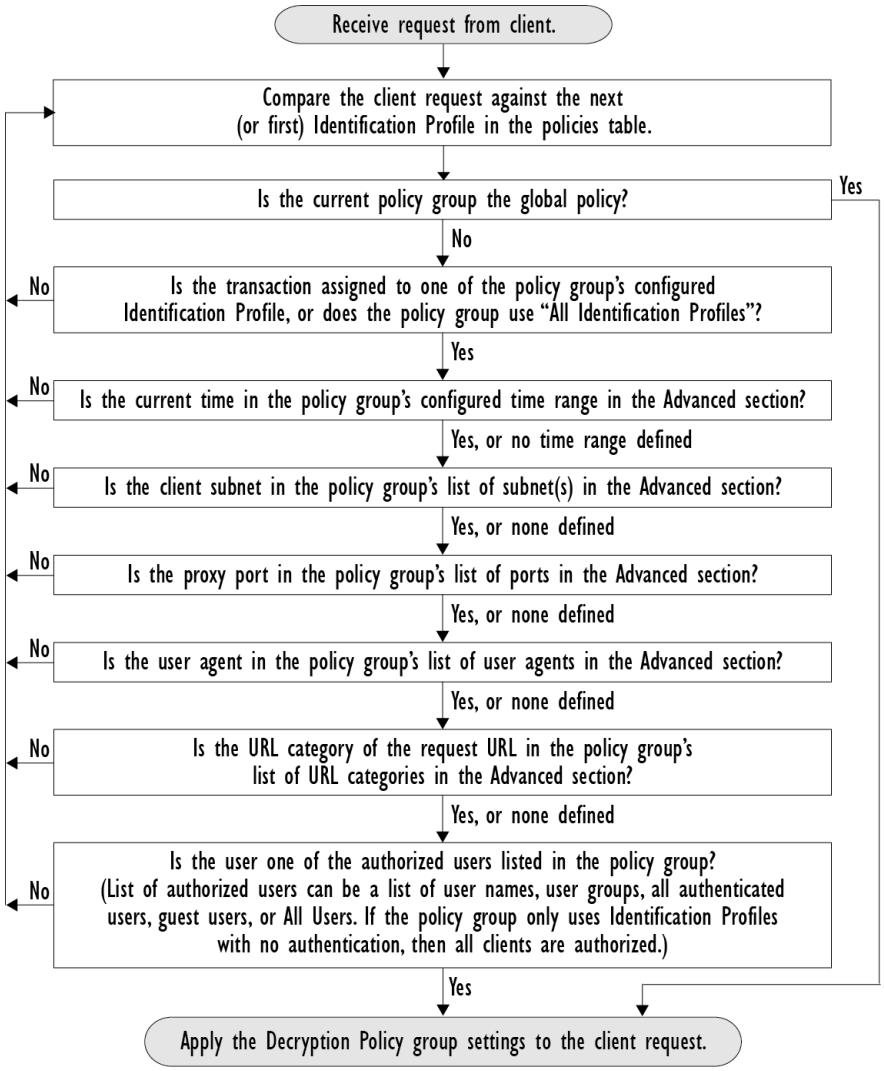
アプライアンスは、HTTPS 接続要求に対して、以下のアクションを実行できます。

オプション	説明
モニタ(Monitor)	Monitor(モニタ)は、最終的に適用される最終アクションを決定するために Web プロキシが他の管理設定に対してトランザクションを評価し続ける必要があることを示す中間のアクションです。
削除(Drop)	アプライアンスは接続をドロップします。サーバに接続要求を渡しません。アプライアンスは接続をドロップしたことをユーザに通知しません。
復号化(Decrypt)	アプライアンスは、接続を許可しますが、トラフィックの内容を検査します。トラフィックを復号化、プレーン テキスト HTTP 接続であるかのように、復号化されたトラフィックにアクセス ポリシーを適用します。接続を復号化し、アクセス ポリシーを適用することにより、トラフィックをスキャンしてマルウェアを検出できます。

Monitor 以外のすべてのアクションは、Web プロキシがトランザクションに適用する最終アクションです。最終アクションは、Web プロキシが他の管理設定に対してトランザクションを評価することを停止する操作です。たとえば、復号化ポリシーが、無効なサーバ証明書をモニタするように設定されている場合、Web プロキシは、サーバにある証明書が無効である場合の HTTPS トランザクションの処理方法についての最終決定を行いません。復号化ポリシーが、Web レピュテーション スコアが低いサーバをブロックするように設定されている場合、レピュテーション スコアが低いサーバに対するすべての要求が URL カテゴリ操作を考慮せずにドロップされます。

次の図に、Web プロキシが復号化ポリシー グループに対してクライアント要求を評価する方法を示します。図 7-2（7-6 ページ）は、復号化ポリシーの管理設定を評価するときに、Web プロキシが使用する順序を示しています。Figure 10-3（10-13 ページ）は、アクセス ポリシーの管理設定を評価するときに、Web プロキシが使用する順序を示しています。

図 7-1　　復号化ポリシーのポリシー グループ トランザクション フロー



HTTPS プロキシのイネーブル化

HTTPS トラフィックをモニタして復号化するには、HTTPS プロキシをイネーブルにする必要があります。HTTPS プロキシをイネーブルにする場合は、アプライアンスが、ネットワークのクライアント アプリケーションに自己署名済みサーバ証明書を送信するときに使用するルート証明書を設定します。組織の既存のルート証明書およびキーをアップロードするか、ユーザが入力した情報で証明書およびキーを生成するようにアプライアンスを設定することができます。

HTTPS プロキシをイネーブルした後は、すべての HTTPS ポリシー決定が復号化ポリシーによって処理されます。また、このページで、サーバ証明書が無効な場合の、アプライアンスによる HTTPS トラフィックの処理も設定できます。

はじめる前に

- HTTPS プロキシをイネーブルにすると、アクセス ポリシー内の HTTPS 専用のルールがディセーブルになり、Web プロキシは HTTP 用のルールを使用して、復号化された HTTPS トラフィックを処理します。

ステップ 1　[セキュリティサービス（Security Services）] > [HTTPS プロキシ（HTTPS Proxy）] に移動し、[設定の有効化と編集（Enable and Edit Settings）] をクリックします。

HTTPS プロキシ ライセンス契約書が表示されます。

ステップ 2　HTTPS プロキシ ライセンス契約書の条項を読み、[同意する（Accept）] をクリックします。

ステップ 3　[HTTPS プロキシを有効にする（Enable HTTPS Proxy）] フィールドがイネーブルであることを確認します。

ステップ 4　[HTTPS ポートからプロキシへ（HTTPS Ports to Proxy）] フィールドに、アプライアンスが HTTPS トラフィックをチェックするポートを入力します。ポート 443 がデフォルト ポートです。

（注）　Web Security Appliance がプロキシとして動作できるポートの最大の番号は 30 で、これには、HTTP と HTTPS の両方が含まれます。

ステップ 5　復号化に使用するルート/署名証明書をアップロード**または**生成します。

（注）　アップロードされた証明書とキーのペアと、生成された証明書とキーのペアの両方がアプライアンスにある場合は、[署名用ルート証明書（Root Certificate for Signing）] セクションで選択されている証明書とキーのペアのみを使用します。

ステップ 6　[HTTPS 透過的要求（HTTPS Transparent Request）] セクションで、以下のオプションのいずれかを選択します。

- Decrypt the HTTPS request and redirect for authentication（HTTPS 要求を復号化して、認証のためにリダイレクトする）
- Deny the HTTPS request（HTTPS 要求を拒否する）

この設定は、認証サロゲートとして IP アドレスを使用するトランザクションだけに、ユーザがまだ認証されていない場合に適用されます。

（注）　このフィールドは、アプライアンスが透過モードで展開されている場合にだけ表示されます。

ステップ 7　[HTTPS を使用するアプリケーション（Applications that Use HTTPS）] セクションで、アプリケーションの可視性とコントロールを向上させるために復号化をイネーブルにするかどうか選択します。

（注）　署名用ルート証明書がクライアントにインストールされていない場合は、復号化により、アプリケーションでエラーが発生することがあります。アプライアンス ルート証明書の詳細については、次を参照してください。

ステップ 8　変更を送信し、保存します。

関連項目

- 証明書の検証と HTTPS の復号化の管理（7-9 ページ）

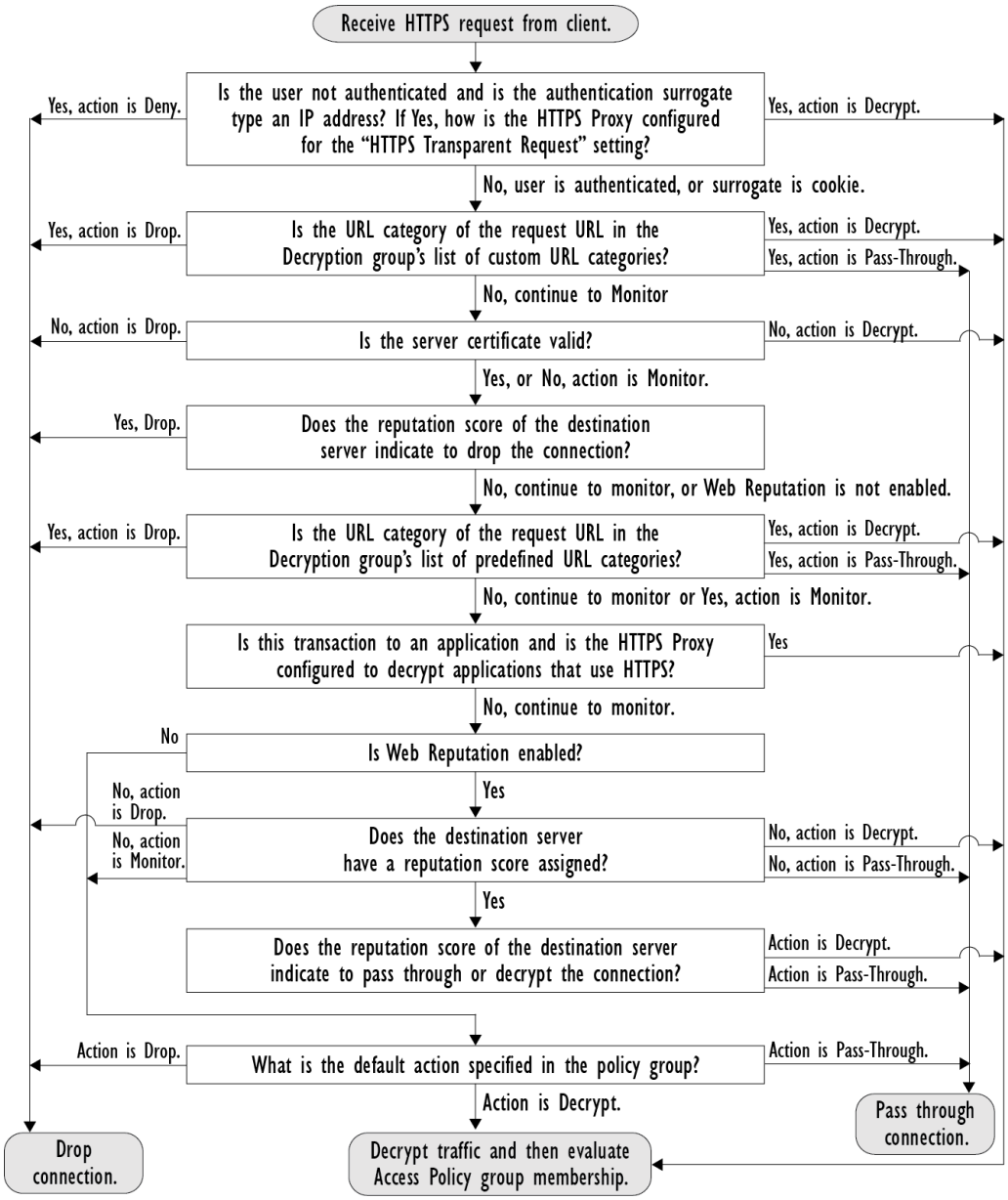
HTTPS トラフィックの制御

Web Security Appliance が復号化ポリシー グループに HTTPS 接続要求を割り当てた後、接続要求は、そのポリシー グループの管理設定を継承します。復号化ポリシー グループの管理設定で、アプライアンスが接続を復号化するか、ドロップするか、またはパススルーするかが決定されます。

オプション	説明
URL カテゴリ（URLCategories）	定義済みおよびカスタムの各 URL カテゴリについて、HTTPS 要求で実行するアクションを設定できます。[URL フィルタリング（URL Filtering）] 列にある、設定するポリシー グループのリンクをクリックします。 **（注）**　HTTPS 要求の特定の URL カテゴリをドロップ（エンドユーザ通知なし）するのではなく、*ブロック*（エンドユーザ通知あり）する場合は、復号化ポリシー グループのその URL カテゴリの復号化を選択し、その後に、アクセス ポリシー グループの同じ URL カテゴリのブロックを選択します。
Web レピュテーション（Web Reputation）	要求されたサーバの Web レピュテーション スコアに基づいて、HTTPS 要求に対して実行するアクションを設定できます。[Web レピュテーション（Web Reputation）] 列にある、設定するポリシー グループのリンクをクリックします。
デフォルト アクション（DefaultAction）	他に該当する設定がない場合にアプライアンスが実行する必要があるアクションを設定できます。[デフォルト アクション（Default Action）] 列にある、設定するポリシー グループのリンクをクリックします。 **（注）**　設定されたデフォルト アクションは、下される決定が、URL カテゴリと Web レピュテーション スコアのどちらにも基づいていない場合にのみ、トランザクションに影響します。Web レピュテーション フィルタリングがディセーブルの場合は、デフォルト アクションが、URL カテゴリの Monitor アクションに一致するすべてのトランザクションに適用されます。Web レピュテーション フィルタリングがイネーブルの場合は、スコアなしのサイトに Monitor アクションが選択されている場合にのみ、デフォルト アクションが使用されます。

次の図に、アプライアンスが特定の復号化ポリシーを HTTPS 要求に割り当てた後に、その要求で実行するアクションを決定する方法を示します。宛先サーバの Web レピュテーション スコアが評価されるのは 1 回だけですが、その結果は、決定フローの 2 つのポイントで適用されます。たとえば、Web レピュテーション スコアのドロップ アクションは、定義済みの URL カテゴリに指定されているあらゆるアクションに優先することに注意してください。

図 7-2　　復号化ポリシー アクションの適用



復号化オプションの設定

はじめる前に

- HTTPS プロキシのイネーブル化（7-4 ページ）で説明したように、HTTPS プロキシがイネーブルであることを確認します。

ステップ 1　[セキュリティサービス（Security Services）] > [HTTPS プロキシ（HTTPS Proxy）] に移動します。

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　復号化オプションをイネーブルにします。

復号化オプション	説明
認証のための復号化	この HTTPS トランザクションの前に認証されていないユーザに復号化を許可して、認証されるようにします。
エンド ユーザ通知のための復号化	AsyncOS がエンド ユーザ通知を表示できるように復号化を許可します。 **（注）**　証明書が無効であり、無効な証明書をドロップするように設定されている場合は、最初にロギングされたトランザクションのアクションがポリシー トレースの実行時に「復号化」されます。
エンド ユーザ確認応答のための復号化	この HTTPS トランザクションの前に Web のプロキシに確認応答していないユーザに復号化を許可し、AsyncOS がエンド ユーザの確認応答を表示できるようにします。
アプリケーション検出のための復号化	AsyncOS が HTTPS アプリケーションを検出する機能を強化します。

認証および HTTPS 接続

HTTPS 接続レイヤでの認証は、以下のタイプの要求で使用できます。

オプション	説明
明示的要求（Explicit requests）	• セキュア クライアント認証がディセーブルである、または • セキュア クライアント認証がイネーブルで、サロゲートが IP ベースである
透過的要求（Transparent requests）	• サロゲートが IP ベースで、認証の復号化がイネーブル、または • サロゲートが IP ベースで、クライアントが以前に HTTP 要求を使用して認証されている

ルート証明書

HTTPS プロキシは、アプライアンスにアップロードした秘密キー ファイルとルート証明書を使用して、トラフィックを復号化します。アプライアンスにアップロードするルート証明書ファイルと秘密キー ファイルは、PEM 形式である必要があります。DER 形式はサポートされていません。

ルート証明書の情報は、以下のように入力できます。

- **生成する。**基本的な設定情報を入力してから、ボタンをクリックすると、アプライアンスが、残りの証明書と秘密キーを生成します。
- **アップロードする。**アプライアンスの外部で作成された証明書ファイルとそれに一致する秘密キー ファイルをアップロードできます。

（注） また、ルート認証局によって署名された中間証明書をアップロードすることもできます。Web プロキシがサーバ証明書を模倣すると、アップロードされた証明書とともに、模倣された証明書がクライアント アプリケーションに送信されます。このように、クライアント アプリケーションが信頼するルート認証局によって中間証明書が署名されている限り、アプリケーションは模倣されたサーバ証明書も信頼します。詳細については、証明書およびキーについて（12-23 ページ）を参照してください。

Web Security Appliance が作成したルート証明書を処理する場合は、以下のいずれかを選択できます。

- **ルート証明書を受け入れるようにユーザに通知します。**組織内のユーザに、企業の新しいポリシーについて通知し、組織が提供したルート証明書を、信頼できる認証局として受け入れるように指示できます。
- クライアント マシンにルート証明書を**追加します。**ネットワーク上のすべてのクライアント マシンに、信頼できるルート認証局としてルート証明書を追加できます。そうすれば、クライアント アプリケーションは自動的にルート証明書を持つトランザクションを受け入れるようになります。

ステップ 1　[セキュリティサービス（Security Services）] > [HTTPS プロキシ（HTTPS Proxy）] に移動します。

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　生成またはアップロードされた証明書の [証明書のダウンロード（Download Certificate）] リンクをクリックします。

（注） クライアント マシンで証明書エラーが表示される可能性を減らすには、Web Security Appliance にルート証明書を生成またはアップロードした後に変更を送信してから、クライアント マシンに証明書を配布し、その後にアプライアンスへの変更をコミットします。

証明書の検証と HTTPS の復号化の管理

Web セキュリティ アプライアンスは証明書を検証してから、コンテンツを検査して復号化します。

有効な証明書

有効な証明書の条件:

- **有効期限が切れていない。**現在の日付が証明書の有効期間内です。
- **公認の認証局である。**発行認証局が、Web セキュリティ アプライアンスに保存されている、信頼できる認証局のリストに含まれています。
- **有効な署名がある。**デジタル署名が、暗号規格に基づいて適切に実装されています。
- **名前が一貫している。**通常名が、HTTP ヘッダーで指定されたホスト名に一致します。
- **失効していない。**発行認証局が証明書を無効にしていません。

関連項目

- 証明書の検証と HTTPS の復号化の管理（7-9 ページ）
- 無効な証明書の処理の設定（7-11 ページ）
- 証明書失効ステータスのチェックのオプション（7-12 ページ）
- リアルタイムの失効ステータス チェックのイネーブル化（7-12 ページ）

無効な証明書の処理

アプライアンスは、無効なサーバ証明書に対して、以下のアクションの 1 つを実行できます。

- **ドロップ。**
- **復号。**
- **モニタ。**

複数の理由で無効となる証明書

認識できないルート認証局と期限切れ証明書の両方の理由により無効なサーバ証明書に対して、HTTPS プロキシは、認識できないルート認証局に適用されるアクションを実行します。

それ以外のすべての場合は、同時に複数の理由により無効なサーバ証明書に対して HTTPS プロキシは、制限レベルが最高のアクションから最低のアクションへの順にアクションを実行します。

復号化された接続の、信頼できない証明書の警告

Web Security Appliance が無効な証明書を検出し、接続を復号化するように設定されている場合、AsyncOS は、信頼できない証明書を作成します。エンド ユーザは、これを受け入れるか、拒否する必要があります。証明書の一般名は「Untrusted Certificate Warning」です。

この信頼できない証明書を信頼できる証明書のリストに追加すると、エンド ユーザは接続を受け入れるか拒否するかを選択できなくなります。

AsyncOS は、これらの証明書のいずれかを生成するときに、「Signing untrusted key」または「Signing untrusted cert」というテキストのプロキシ ログ エントリを作成します。

ルート証明書およびキーのアップロード

はじめる前に

- HTTPS プロキシをイネーブルにします。HTTPS プロキシのイネーブル化（7-4 ページ）。

ステップ 1　[セキュリティサービス（Security Services）] > [HTTPS プロキシ（HTTPS Proxy）] に移動します。

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　[アップロードされた証明書とキーを使用（Use Uploaded Certificate and Key）] を選択します。

ステップ 4　[証明書（Certificate）] フィールドで [参照（Browse）] をクリックし、ローカル マシンに保存されている証明書ファイルに移動します。

アップロードするファイルに複数の証明書またはキーが含まれている場合、Web プロキシはファイル内の先頭の証明書またはキーを使用します。

ステップ 5　[キー（Key）] フィールドで [参照（Browse）] をクリックし、秘密キー ファイルに移動します。

（注）　キーの長さは 512、1024、または 2048 ビットである必要があります。

ステップ 6　キーが暗号化されている場合は、[キーは暗号化されています（Key is Encrypted）] を選択します。

ステップ 7　[ファイルのアップロード（Upload Files）] をクリックして、証明書およびキーのファイルを Web Security Appliance に転送します。

アップロードされた証明書の情報が [HTTPS プロキシ設定を編集（Edit HTTPS Proxy Settings）] ページに表示されます。

ステップ 8　（任意）[証明書のダウンロード（Download Certificate）] をクリックすると、ネットワーク上のクライアント アプリケーションに証明書を転送できます。

HTTPS プロキシ用の証明書およびキーの生成

はじめる前に

- HTTPS プロキシをイネーブルにします。HTTPS プロキシのイネーブル化（7-4 ページ）。

ステップ 1　[セキュリティサービス（Security Services）] > [HTTPS プロキシ（HTTPS Proxy）] に移動します。

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　[生成された証明書とキーを使用（Use Generated Certificate and Key）] を選択します。

ステップ 4　[新しい証明書とキーを生成（Generate New Certificate and Key）] をクリックします。

ステップ 5　[証明書とキーを生成（Generate Certificate and Key）] ダイアログボックスで、ルート証明書に表示する情報を入力します。

[共通名（Common Name）] フィールドには、スラッシュ（/）を除く任意の ASCII 文字を入力できます。

ステップ 6　[生成（Generate）] をクリックします。

ステップ 7　生成された証明書の情報が [HTTPS プロキシ設定を編集（Edit HTTPS Proxy Settings）] ページに表示されます。

ステップ 8　(任意)[証明書のダウンロード(Download Certificate)] をクリックすると、ネットワーク上のクライアント アプリケーションに証明書を転送できます。

ステップ 9　(任意)[証明書署名要求のダウンロード(Download Certificate Signing Request)] リンクをクリックすると、証明書署名要求(CSR)を認証局(CA)に送信できます。

ステップ 10　(任意)CA から署名付き証明書を受信した後、それを Web Security Appliance にアップロードします。この操作は、アプライアンスで証明書を生成した後はいつでも実行できます。

ステップ 11　変更を送信して確定します([送信(Submit)] と [変更を確定(Commit Changes)])。

無効な証明書の処理の設定

はじめる前に

- HTTPS プロキシのイネーブル化(7-4 ページ)で説明したように、HTTPS プロキシがイネーブルであることを確認します。

ステップ 1　[セキュリティサービス(Security Services)] > [HTTPS プロキシ(HTTPS Proxy)] に移動します。

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　証明書エラーのタイプごとに、プロキシの対応(**ドロップ**、**復号化**、**モニタ**)を定義します。

証明書エラーのタイプ	説明
期限切れ	現在の日付が、証明書の有効範囲外にあります。
ホスト名の不一致	証明書にあるホスト名が、クライアントがアクセスしようとしたホスト名に一致しません。 **(注)**　明示的な転送モードで展開されている場合にのみ、Web プロキシはホスト名の照合を実行できます。透過モードで展開されている場合は、宛先サーバのホスト名がわからない(わかっているのは IP アドレスのみです)ため、ホスト名をサーバ証明書のホスト名と比較できません。
認識できないルート認証局/発行元	ルート認証局または中間認証局が認識されません。
無効な署名証明書	署名証明書に問題があります。
無効なリーフ証明書	リーフ証明書に、拒否、でコード、または不一致などの問題が発生しました。
その他のエラー タイプ	他のほとんどのエラー タイプは、アプライアンスが HTTPS サーバとの SSL ハンドシェイクを完了できないことが原因です。サーバ証明書の詳細なエラー シナリオに関する情報については、http://www.openssl.org/docs/apps/verify.html を参照してください。

ステップ 4　変更を送信して確定します([送信(Submit)] と [変更を確定(Commit Changes)])。

証明書失効ステータスのチェックのオプション

発行認証局が証明書を失効させたかどうかを確認するために、Web Security Appliance では、以下の方法で発行認証局をチェックできます。

- **証明書失効リスト（Comodo 証明書のみ）。**Web Security Appliance は Comodo の証明書失効リストをチェックします。Comodo は、このリストを独自のポリシーに従って更新して維持します。最後に更新された日時によっては、Web Security Appliance がチェックした時点では、証明書失効リストが古くなっている可能性があります。
- **オンライン証明書ステータス プロトコル（OCSP）。**Web Security Appliance が、発行認証局で失効ステータスをリアルタイムでチェックします。発行認証局が OCSP をサポートしている場合は、リアルタイム ステータス チェック用の URL が証明書に含まれています。この機能は、新規インストールではデフォルトでイネーブルになり、更新ではデフォルトでディセーブルになります。

（注）　Web セキュリティ アプライアンスは、他のすべての点で有効であることを特定し、OCSP URL を含んでいる証明書の OCSP クエリーのみを実行します。

関連項目

- リアルタイムの失効ステータス チェックのイネーブル化（7-12 ページ）
- 無効な証明書の処理の設定（7-11 ページ）

リアルタイムの失効ステータス チェックのイネーブル化

はじめる前に

- HTTPS プロキシがイネーブルであることを確認します。HTTPS プロキシのイネーブル化（7-4 ページ）を参照してください

ステップ 1　[セキュリティサービス（Security Services）] > [HTTPS プロキシ（HTTPS Proxy）] に移動します。

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　[オンライン証明書ステータスプロトコル(OCSP)を有効にする（Enable Online Certificate Status Protocol (OCSP)）] を選択します。

ステップ 4　[OCSP結果処理（Result Handling）] の各プロパティを設定します。

シスコでは、OCSP 結果処理のオプションを、無効な証明書の処理のオプションと同じアクションに設定することを推奨します。たとえば、[モニタする期限切れ証明書（Expired Certificate to Monitor）] を設定する場合は、モニタする失効証明書を設定します。

ステップ 5　（任意）[詳細（Advanced）] 設定セクションを展開し、以下の設定項目を設定します。

フィールド名	説明
OSCP 有効応答キャッシュ タイムアウト（OCSP Valid Response Cache Timeout）	有効な OCSP 応答を再確認する前に待機する時間。単位は秒（s）、分（m）、時間（h）、または日（d）。デフォルトの単位は秒です。有効な範囲は 1 秒～ 7 日です。

フィールド名	説明
OSCP 無効応答キャッシュ タイムアウト（OCSP Invalid Response Cache Timeout）	無効な OCSP 応答を再確認する前に待機する時間。単位は秒（s）、分（m）、時間（h）、または日（d）。デフォルトの単位は秒です。有効な範囲は 1 秒～ 7 日です。
OSCP ネットワーク エラー キャッシュ タイムアウト（OCSP Network Error Cache Timeout）	応答がなかった後に、OCSP 応答側に連絡を再度試みる前に待機する時間。単位は秒（s）、分（m）、時間（h）、または日（d）。有効な範囲は 1 秒～ 24 時間です。
許容されるクロック スキュー（Allowed Clock Skew）	Web Security Appliance と OCSP 応答側の間で許容される設定時間の差の最大値。単位は秒（s）または分（m）。有効な範囲は 1 秒～ 60 分です。
OSCP 応答待機最大時間（Maximum Time to Wait for OCSP Response）	OCSP 応答側からの応答を待機する時間の最大値。有効な範囲は 1 秒～ 10 分です。OCSP レスポンダを使用できない場合に、HTTPS 要求へのエンド ユーザ アクセスの遅延を短縮するには、短い期間を指定します。
OSCP チェックにアップストリーム プロキシを使用（Use upstream proxy for OCSP checking）	アップストリーム プロキシのグループ名。
アップストリーム プロキシから除外するサーバ（Servers exempt from upstream proxy）	除外するサーバの IP アドレスまたはホスト名。空白のままにすることもできます。

ステップ 6　変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

信頼できるルート証明書

Web セキュリティ アプライアンスには、信頼できるルート証明書のリストが付属しており、これが維持されます。信頼できる証明書を持つ Web サイトでは、復号化は必要ありません。

信頼できる証明書のリストに証明書を追加し、機能的に証明書を削除すると、信頼できる証明書のリストを管理できます。Web セキュリティ アプライアンスは、マスター リストからは証明書を削除しませんが、証明書の信頼を無効にすることができます。これで、信頼できるリストから機能的に証明書が削除されます。

信頼できるリストへの証明書の追加

はじめる前に

- HTTPS プロキシがイネーブルであることを確認します。HTTPS プロキシのイネーブル化（7-4 ページ）を参照してください

ステップ 1　[セキュリティサービス（Security Services）] > [HTTPS プロキシ（HTTPS Proxy）] に移動します。

ステップ 2　[信頼できるルート証明書の管理（Manage Trusted Root Certificates）] をクリックします。

ステップ 3　[インポート（Import）] をクリックします。

ステップ 4　[参照（Browse）] をクリックして証明書ファイルに移動します。

ステップ 5　変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

[カスタム信頼済みルート証明書（Custom Trusted Root Certificates）] リストで、アップロードした証明書を探します。

信頼できるリストからの証明書の削除

ステップ 1　[セキュリティ サービス（Security Services）] > [HTTPS プロキシ（HTTPS Proxy）] を選択します。

ステップ 2　[信頼できるルート証明書の管理（Manage Trusted Root Certificates）] をクリックします。

ステップ 3　リストから削除する証明書に対応する [信頼をオーバーライド（Override Trust）] チェックボックスを選択します。

ステップ 4　変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

HTTPS トラフィックのルーティング

クライアントのヘッダーに保存されている情報に基づいて HTTPS トランザクションをルーティングする AsyncOS の機能は限定的であり、透過 HTTPS と明示 HTTPS で異なります。

オプション	説明
透過 HTTPS	透過 HTTPS の場合は、AsyncOS がクライアントのヘッダー情報にアクセスできません。したがって、AsyncOS は、クライアントのヘッダー情報に依存するルーティング ポリシーを適用できません。
明示 HTTPS	明示 HTTPS の場合、AsyncOS は、クライアント ヘッダー内の以下の情報にアクセスできます。 • URL • 宛先ポート番号 したがって、明示 HTTPS トランザクションでは、URL またはポート番号に基づいてルーティング ポリシーを照合できます。

暗号化/HTTPS/証明書のトラブルシューティング

CHAPTER 8

セキュリティ サービスの設定

Web レピュテーション フィルタの概要

Web レピュテーション フィルタは、Web ベースのレピュテーション スコア（WBRS）を URL に割り当て、URL ベースのマルウェアが含まれている可能性を判断します。Web Security Appliance は、Web レピュテーション スコアを使用して、未然にマルウェア攻撃を特定して防ぎます。Web レピュテーション フィルタは、アクセス ポリシー、復号化ポリシー、Cisco IronPort データ セキュリティ ポリシーで使用できます。

Web レピュテーション スコア

Web レピュテーション フィルタでは、データを使用してインターネット ドメインの信頼性が評価され、URL のレピュテーションにスコアが付けられます。Web レピュテーションの計算では、URL をネットワーク パラメータに関連付けて、マルウェアが存在する可能性が判定されます。マルウェアが存在する可能性の累計が、-10 ～ +10 の Web レピュテーション スコアにマッピングされます（+10 がマルウェアを含む可能性が最も低い）。

パラメータには、たとえば以下のものがあります。

- URL 分類データ
- ダウンロード可能なコードの存在
- 長く不明瞭なエンドユーザ ライセンス契約書（EULA）の存在
- グローバルなボリュームとボリュームの変更
- ネットワーク オーナー情報
- URL の履歴

- URL の経過時間
- ブロック リストに存在
- 許可リストに存在
- 人気のあるドメインの URL タイプミス
- ドメインのレジストラ情報
- IP アドレス情報

（注）　シスコは、ユーザ名、パスフレーズ、クライアント IP アドレスなどの識別情報を収集しません。

Web レピュテーション フィルタの動作のしくみについて

Web レピュテーション スコアは URL 要求に対して実行されるアクションに関連付けられます。各ポリシー グループを設定して、特定の Web レピュテーション スコアにアクションを関連付けることができます。使用可能なアクションは、URL 要求に割り当てられているポリシー グループのタイプによって異なります。

ポリシー タイプ	操作
アクセス ポリシー（Access Policies）	ブロック、スキャン、または許可から選択できます。
Cisco IronPort データ セキュリティ ポリシー（Cisco IronPort Data Security Policies）	ブロックまたはモニタから選択できます。

アクセス ポリシーの Web レピュテーション

アクセス ポリシーに Web レピュテーションを設定する場合は、手動で設定するか、AsyncOS for Web で適応型スキャンを使用して最適なオプションを選択することができます。適応型スキャンがイネーブルの場合は、各アクセス ポリシーで Web レピュテーション フィルタリングをイネーブルまたはディセーブルにできますが、Web レピュテーション スコアは編集できません。

スコア	アクション	説明	例
-10 ～ -6.0	ブロック（Block）	不正なサイト。要求はブロックされ、以降のマルウェア スキャンは実行されません。	• URL がユーザの許可なしに情報をダウンロード。 • URL ボリュームが急上昇。 • URL が人気のあるドメインの誤入力。
-5.9 ～ 5.9	スキャン（Scan）	判別不能なサイト。さらにマルウェア スキャンを行うために、DVS エンジンに要求が渡されます。DVS エンジンは、要求とサーバ応答のコンテンツをスキャンします。	• 動的 IP アドレスを持ち、ダウンロード可能なコンテンツを含む最近作成された URL。 • Web レピュテーション スコアがプラスのネットワーク オーナーの IP アドレス。

スコア	アクション	説明	例
6.0 ～ 10.0	許可（Allow）	正常なサイト。要求は許可されます。マルウェア スキャンは必要ありません。	• URL にダウンロード可能なコンテンツが含まれていない。 • 歴史が長く信頼できる大規模ドメイン。 • 複数の許可リストに記載されているドメイン。 • 評価が低い URL へのリンクがない。

デフォルトでは、+7 の Web レピュテーション スコアが割り当てられている HTTP 要求の URL は許可され、さらなるスキャンは必要ありません。しかし、+3 などの低いスコアの HTTP 要求は、マルウェアをスキャンする Cisco IronPort DVS エンジンに自動的に転送されます。レピュテーションが非常に低い HTTP 要求の URL はブロックされます。

関連項目

- 適応型スキャンについて（8-6 ページ）

Cisco IronPort データ セキュリティ ポリシーの Web レピュテーション

スコア	アクション	説明
-10 ～ -6.0	ブロック（Block）	不正なサイト。トランザクションはブロックされ、以降のスキャンは実行されません。
-5.9 ～ 0.0	モニタ（Monitor）	トランザクションは Web レピュテーションに基づいてブロックされず、引き続きコンテンツ（ファイル タイプとサイズ）の検査が行われます。 **（注）**　スコアがないサイトはモニタされます。

マルウェア対策 スキャンの概要

Web Security Appliance マルウェア対策機能は、Cisco IronPort DVS™ エンジンとマルウェア対策スキャン エンジンを併用して、Web ベースのマルウェアの脅威を阻止します。DVS エンジンは、Webroot™、McAfee、Sophos マルウェア対策スキャン エンジンと連携します。

スキャン エンジンはトランザクションを検査して、DVS エンジンに渡すマルウェア スキャンの判定を行います。DVS エンジンは、マルウェア スキャンの判定に基づいて、要求をモニタするかブロックするかを決定します。アプライアンスのアンチマルウェア コンポーネントを使用するには、マルウェア対策スキャンをイネーブルにして、グローバル設定値を設定してから、各種のポリシーに特定の設定を適用する必要があります。

DVS エンジンの動作のしくみについて

DVS エンジンは、Web レピュテーション フィルタから転送された URL のトランザクションに対してマルウェア対策スキャンを実行します。Web レピュテーション フィルタは、特定の URL にマルウェアが含まれている可能性を計算し、URL スコアを割り当てます。このスコアは、トランザクションをブロック、スキャンまたは許可するアクションに関連付けられています。

割り当てられた Web レピュテーション スコアがトランザクションをスキャンすることを示している場合、DVS エンジンは URL 要求とサーバ応答のコンテンツを受信します。DVS エンジンはスキャン エンジン（Webroot および（または）Sophos、または McAfee）と連携して、マルウェア スキャンの判定を返します。DVS エンジンは、マルウェア スキャンの判定およびアクセス ポリシーの設定情報を使用して、クライアントへのコンテンツをブロックするか配信するかを判定します。

複数のマルウェア判定の使用

DVS エンジンは、1 つの URL に対して複数のマルウェア判定を下すことがあります。イネーブルなスキャン エンジンの一方または両方から複数の判定が返される場合もあります。

- 異なるスキャン エンジンによるさまざまな判定。Sophos または McAfee のどちらか一方と Webroot を同時にイネーブルにすると、それぞれのスキャン エンジンが同じオブジェクトに対して異なるマルウェア判定を返すことがあります。イネーブルな両方のスキャン エンジンから 1 つの URL に対して複数の判定が返された場合、アプライアンスは最も制限が厳しいアクションを実行します。たとえば、一方のスキャン エンジンがブロックの判定を返し、他方のスキャン エンジンがモニタの判定を返した場合、DVS エンジンは常に要求をブロックします。
- **同じスキャン エンジンからの異なる判定。**オブジェクトに複数の感染が含まれている場合、1 つのスキャン エンジンが 1 つのオブジェクトに対して複数の判定を返すことがあります。同じスキャン エンジンが 1 つの URL に対して複数の判定を返した場合、アプライアンスは最も優先順位の高い判定に従ってアクションを実行します。以下のリストは、可能性があるマルウェア スキャンの判定を優先順位が高いものから順に示しています。
  - ウィルス
  - トロイのダウンローダ
  - トロイの木馬
  - トロイのフィッシャ
  - ハイジャッカー
  - システム モニタ
  - 商用システム モニタ
  - ダイヤラ
  - ワーム
  - ブラウザ ヘルパー オブジェクト
  - フィッシング URL
  - アドウェア
  - 暗号化ファイル
  - スキャン不可
  - その他のマルウェア

Webroot スキャン

Webroot スキャン エンジンはオブジェクトを検査してマルウェア スキャンの判定を行い、判定を DVS エンジンに送信します。Webroot スキャン エンジンは、以下のオブジェクトを検査します。

- **URL 要求。**Webroot は URL 要求を評価して、URL にマルウェアの疑いがあるかどうかを判別します。この URL からの応答にマルウェアが含まれている可能性があると Webroot が判断した場合、アプライアンスは、アプライアンス独自の設定に応じて、要求をモニタまたはブロックします。Webroot によって要求が正常である評価された場合、アプライアンスは URL を取得し、サーバの応答をスキャンします。
- **サーバ応答。**アプライアンスが URL を取得すると、Webroot はサーバ応答のコンテンツをスキャンし、Webroot シグニチャ データベースと照合します。

McAfee スキャン

McAfee スキャン エンジンは、HTTP 応答内の Web サーバからダウンロードされたオブジェクトを検査します。オブジェクトの検査後、マルウェア スキャンの判定を DVS エンジンに渡し、DVS エンジンが要求をモニタするかブロックするかを決定できるようにします。

McAfee スキャン エンジンは以下の方法を使用して、マルウェア スキャンの判定を行います。

- ウィルス シグニチャ パターンの照合
- ヒューリスティック分析

ウィルス シグニチャ パターンの照合

McAfee は、そのデータベース内のウィルス定義をスキャン エンジンに使用し、特定のウィルスや各種のウィルスなどの潜在的に望ましくないソフトウェアを検出します。ファイル内のウィルス シグニチャを検索します。McAfee をイネーブルにした場合、McAfee スキャン エンジンはこの方法を使用して、サーバ応答のコンテンツをスキャンします。

ヒューリスティック分析

ヒューリスティック分析は、特定のルールではなく、一般的なルールを使用して新しいウィルスとマルウェアを検出する手法です。ヒューリスティック分析を使用する場合、McAfee スキャン エンジンは、オブジェクトのコードを確認して一般的なルールを適用し、オブジェクトがどの程度ウィルスに類似しているかを判断します。

ヒューリスティック分析を使用すると、偽陽性（ウイルスと指摘された正常なコンテンツ）の報告が増加し、アプライアンスのパフォーマンスが影響を受ける可能性があります。McAfee をイネーブルにするときに、オブジェクトのスキャンでヒューリスティック分析をイネーブルにするかどうかを選択できます。

McAfee カテゴリ

McAfee の判定	マルウェア スキャン判定カテゴリ
既知のウィルス	ウィルス
トロイの木馬	トロイの木馬
ジョーク ファイル	アドウェア
テスト ファイル	ウィルス
ワナビ	ウィルス
不活化	ウィルス
商用アプリケーション	商用システム モニタ
望ましくないオブジェクト	アドウェア
望ましくないソフトウェア パッケージ	アドウェア
暗号化ファイル	暗号化ファイル

Sophos スキャン

Sophos スキャン エンジンは、HTTP 応答内の Web サーバからダウンロードされたオブジェクトを検査します。オブジェクトの検査後、マルウェア スキャンの判定を DVS エンジンに渡し、DVS エンジンが要求をモニタするかブロックするかを決定できるようにします。McAfee アンチマルウェア ソフトウェアがインストールされているときに、McAfee スキャン エンジンではなく、Sophos スキャン エンジンをイネーブルにする必要がある場合があります。

適応型スキャンについて

適応型スキャン機能は、どのマルウェア対策スキャン エンジン（ダウンロード ファイルの高度なマルウェア防御スキャンを含む）によって Web 要求を処理するかを決定します。

適応型スキャン機能は、スキャン エンジンを実行する前に、マルウェアとして特定するトランザクションに「アウトブレイク ヒューリスティック（Outbreak Heuristics）」マルウェア対策カテゴリを適用します。アプライアンスでマルウェア対策設定を行うときに、これらのトランザクションをブロックするかどうかを選択できます。

適応型スキャンとアクセス ポリシー

適応型スキャンをイネーブルにした場合は、アクセス ポリシーに設定できる Web レピュテーションとマルウェア対策の設定項目の一部がやや異なります。

- 各アクセス ポリシーでは Web レピュテーション フィルタリングをイネーブルまたはディセーブルにできますが、Web レピュテーション スコアは編集できません。
- 各アクセス ポリシーではマルウェア対策スキャンをイネーブルにできますが、どのマルウェア対策スキャン エンジンをイネーブルにするかは選択できません。適応型スキャンによって、各 Web 要求に最適なエンジンが選択されます。

（注）　適応型スキャンがイネーブルになっておらず、アクセス ポリシーに Web レピュテーションとマルウェア対策の特定の設定項目が設定されている場合に、適応型スキャンをイネーブルにすると、既存の Web レピュテーションとマルウェア対策の設定が上書きされます。

ポリシーごとの高度なマルウェア防御の設定は、適応型スキャンがイネーブルかどうかに関わらず同じです。

データベース テーブルの保持

Web レピュテーション、Webroot、Sophos、および McAfee のデータベースは、Cisco Ironport アップデート サーバから定期的にアップデートを受信します。サーバのアップデートは自動化されており、アップデート間隔はサーバによって設定されます。

Web レピュテーション データベース

Web Security Appliance が保持しているフィルタリング データベースには、統計情報およびさまざまなタイプの要求の処理方法に関する情報が含まれています。また、Cisco SensorBase ネットワーク サーバに Web レピュテーション統計情報を送信するようにアプライアンスを設定することもできます。SensorBase サーバ情報は SensorBase ネットワークからのデータ フィードに活用され、Web レピュテーション スコアの作成に使用されます。

Web レピュテーション フィルタリング アクティビティおよび DVS スキャンのロギング

アクセス ログ ファイルには、Web レピュテーション フィルタと DVS エンジンから返された各トランザクションの情報が記録されます。アクセス ログのスキャン判定情報セクションには、トランザクションに適用されたアクションの原因を把握するのに役立つ多くのフィールドがあります。たとえば、あるフィールドには、Sopho から DVS エンジンに渡された Web レピュテーション スコアやマルウェア スキャン判定が表示されます。

適応型スキャンのロギング

アクセス ログのカスタム フィールド	W3C ログのカスタム フィールド	説明
%X6	x-as-malware-threat-name	適応型スキャンから返されたマルウェア対策名。トランザクションがブロックされていない場合、このフィールドはハイフン（「-」）を返します。この変数は、スキャン判定情報（各アクセス ログ エントリの末尾の山カッコ内）に含まれています。

適応型スキャン エンジンによってブロックおよびモニタされるトランザクションは、以下の ACL デシジョン タグを使用します。

- BLOCK_AMW_RESP
- MONITOR_AMW_RESP

キャッシング

以下のガイドラインは、AsyncOS がマルウェアのスキャン中にキャッシュを使用するしくみを示しています。

- AsyncOS は、オブジェクト全体がダウンロードされたときにだけオブジェクトをキャッシュします。スキャン中にマルウェアがブロックされた場合、オブジェクト全体はダウンロードされないので、キャッシュされません。
- AsyncOS は、コンテンツの取得元がサーバであるか Web キャッシュであるかに関わらず、コンテンツをスキャンします。
- コンテンツがキャッシュされる時間はさまざまな要因によって異なります。デフォルト値はありません。
- AsyncOS は、シグニチャが更新されるとコンテンツを再スキャンします。

マルウェアのカテゴリについて

マルウェアのタイプ	説明
アドウェア	アドウェアには、販売目的でユーザを製品に誘導する、すべてのソフトウェア実行可能ファイルおよびプラグインが含まれます。また、これらのプログラムによってセキュリティ設定が変更されて、ユーザがシステム設定を変更できなくなる場合もあります。
ブラウザ ヘルパー オブジェクト	ブラウザ ヘルパー オブジェクトは、広告の表示やユーザ設定の乗っ取りに関連するさまざまな機能を実行する可能性があるブラウザ プラグインです。
商用システム モニタ	商用システム モニタは、正当な手段によって正規のライセンスで取得できる、システム モニタの特性を備えたソフトウェアです。
ダイヤラ	ダイヤラは、モデムあるいは別のタイプのインターネット アクセスを利用して、ユーザの完全な承諾なしに、長距離通話料のかかる電話回線またはサイトにユーザを接続するプログラムです。
一般的なスパイウェア	スパイウェアはコンピュータにインストールされるタイプのマルウェアで、ユーザに知られることなくその詳細情報を収集します。
ハイジャッカー	ハイジャッカーは、ユーザの承諾なしにユーザを Web サイトに誘導したりプログラムを実行したりできるように、システム設定を変更したり、ユーザのシステムに不要な変更を加えたりします。
悪意のある既知の高リスクファイル	これらは、高度なマルウェア防御ファイル レピュテーション サービスによって脅威と判定されたファイルです。
その他のマルウェア	このカテゴリは、定義済みのどのカテゴリにも当てはまらないマルウェアと疑わしい動作に使用されます。

マルウェアのタイプ	説明
フィッシング URL	フィッシング URL は、ブラウザのアドレス バーに表示されます。場合によっては、正当なドメインを模倣したドメイン名が使用されます。
PUA	望ましくないアプリケーションのこと。PUA は、悪質ではないが望ましくないと見なされるアプリケーションです。
システム モニタ	システム モニタには、以下のいずれかを実行するソフトウェアが含まれます。 • 公然と、または密かに、システム プロセスやユーザ アクションを記録する。 • これらの記録を後で取得して確認できるようにする。
トロイのダウンローダ	トロイのダウンローダは、インストール後にリモート ホスト/サイトにアクセスして、リモート ホストからパッケージやアフィリエイトをインストールするトロイの木馬です。
トロイの木馬	トロイの木馬は、安全なアプリケーションを装う有害なプログラムです。ウイルスとは異なり、トロイの木馬は自己複製しません。
トロイのフィッシャ	トロイのフィッシャは、感染したコンピュータに潜んで特定の Web ページがアクセスされるのを待ったり、感染したマシンをスキャンしてユーザ名とパスフレーズを探したりします。
ウイルス	ウイルスは、ユーザが気付かない間にコンピュータにロードされるプログラムまたはコードです。
ワーム	ワームは、コンピュータ ネットワーク上で自己を複製し、悪質なアクションを実行するプログラムまたはアルゴリズムです。

CHAPTER 9

エンドユーザへのプロキシ アクションの通知

エンドユーザ通知の概要

以下のタイプのエンドユーザへの通知を設定できます。

オプション	説明	解説場所
エンドユーザ確認ページ（End-User Acknowledgement Page）	エンドユーザに、自分の Web アクティビティがフィルタリングおよびモニタされていることを通知します。エンドユーザ確認応答ページは、ユーザが初めてブラウザにアクセスしてから一定時間経過後に表示されます。	エンドユーザ確認ページ（9-3 ページ）
エンドユーザ通知ページ	エンドユーザに、特定のブロック理由のために特定のページへのアクセスがブロックされていることを通知します。	エンドユーザ通知ページ（9-6 ページ）

オプション	説明	解説場所
エンドユーザ URL フィルタリング警告ページ	エンドユーザに、ユーザがアクセスしようとしているサイトが組織のアクセプタブル ユース ポリシーに一致しないことを警告し、ユーザが選択すればアクセスの続行を許可します。	エンド ユーザ URL フィルタリング警告ページの設定（9-10 ページ）
FTP 通知メッセージ（FTP notification messages）	エンドユーザに、ネイティブ FTP トランザクションがブロックされた理由を知らせます。	FTP 通知メッセージの設定（9-10 ページ）。
時間およびボリューム クォータの有効期限警告ページ	エンドユーザに、設定されたデータ量または時間制限に達したため、アクセスがブロックされることを通知します。	これらの設定は、[セキュリティ サービス（Security Services）] > [エンドユーザ通知（End-User Notification）] ページの [時間およびボリューム クォータの有効期限警告ページ（Time and Volume Quotas Expiry Warning Page）] セクションで行います。 Time Ranges and Quotas（10-16 ページ）も参照してください。

通知ページの一般設定項目の設定

通知ページの表示言語とロゴを指定します。制限についてはこの手順で説明します。

ステップ 1　[セキュリティ サービス（Security Services）] > [エンドユーザ通知（End-User Notification）] 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。

ステップ 3　[全般設定（General Settings）] セクションで、Web プロキシが通知ページを表示する際に使用する言語を選択します。

- HTTP の言語設定は、すべての HTTP 通知ページ（確認通知、オンボックスのエンドユーザ通知、カスタマイズしたエンドユーザ通知、エンドユーザ URL フィルタリング警告）に適用されます。
- FTP の言語は、すべての FTP 通知メッセージに適用されます。

ステップ 4　各通知ページでロゴを使用するかどうかを選択します。Cisco ロゴを指定したり、[カスタム ロゴを使用（Use Custom Logo）] フィールドに入力した URL で参照される任意のグラフィック ファイルを指定することができます。

この設定は、IPv4 を介して提供されるすべての HTTP 通知ページに適用されます。AsyncOS では IPv6 を介したイメージはサポートされません。

ステップ 5　変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

関連項目

- 通知ページの URL とロゴに関する注意事項（9-12 ページ）

エンドユーザ確認ページ

Web Security Appliance を設定して、Web アクティビティのフィルタリングとモニタリングが行われていることをユーザに通知できます。(そのように設定されている場合)アプライアンスは、HTTP または HTTPS を使用して Web にアクセスしているすべてのユーザに、エンドユーザ確認応答ページを表示します。ユーザが初めて Web サイトにアクセスを試みたとき、または設定された時間間隔の後にエンドユーザ確認応答ページが表示されます。

認証でユーザ名を使用可能な場合、Web プロキシはユーザ名によってユーザを追跡します。ユーザ名を使用できない場合は、ユーザを追跡する方法(IP アドレスまたは Web ブラウザのセッション Cookie のいずれか)を選択できます。

(注)　ネイティブ FTP トランザクションは、エンドユーザ確認ページから除外されます。

エンドユーザ確認ページによる HTTPS および FTP サイトへのアクセス

エンドユーザ確認応答ページは、アクセプタブル ユース ポリシー契約をクリックすることを求める HTML ページをエンド ユーザに表示することにより動作します。ユーザがリンクをクリックすると、Web プロキシは、最初に要求された Web サイトにクライアントをリダイレクトします。ユーザに対して使用可能なユーザ名がない場合は、ユーザがサロゲート(IP アドレスまたは Web ブラウザ セッション Cookie のいずれか)を使用してエンド ユーザ確認応答ページを受け入れた時期を記録します。

- **HTTPS。**Web プロキシは、ユーザが Cookie を使用してエンドユーザ確認応答ページを確認したかどうかを追跡しますが、トランザクションを復号化しない限り Cookie を取得できません。エンドユーザ確認応答ページがイネーブルになっており、セッション Cookie を使用してユーザを追跡する場合は、HTTPS 要求をバイパス(パススルー)するかドロップするかを選択できます。`advancedproxyconfig > EUN` CLI コマンドを使用してこの操作を実行し、「セッションベースの EUA により HTTPS 要求に対して実行されるアクション(「bypass」または「drop」)」コマンドをバイパスすることを選択します。
- **FTP over HTTP。**Web ブラウザは、FTP over HTTP トランザクションに Cookie を送信することはないので、Web プロキシは Cookie を取得できません。このような状況を回避するために、FTP over HTTP トランザクションに対してエンドユーザ確認応答ページの要求が適用されないようにできます。正規表現として「ftp://」(引用符なし)を使用してカスタム URL カテゴリを作成し、このカスタム URL カテゴリに対してユーザにエンドユーザ確認ページを表示しないようにする ID ポリシー定義します。

エンドユーザ確認応答ページについて

- ユーザが IP アドレスによって追跡される場合、アプライアンスは最大時間間隔の最短の値と IP アドレスの最長アイドル タイムアウトを使用して、エンド ユーザ確認応答ページを再表示する時点を指定します。
- ユーザがセッション Cookie を使用して追跡される場合、Web プロキシは、ユーザが Web ブラウザを閉じて再起動したときや、別の Web ブラウザ アプリケーションを開いたときに、エンドユーザ確認応答ページを再表示します。
- クライアントが FTP over HTTP を使用して HTTPS サイトまたは FTP サーバにアクセスする場合、セッション Cookie によるユーザの追跡は動作しません。

- アプライアンスが明示的転送モードで展開され、ユーザが HTTPS のサイトに移動する場合、エンドユーザ確認応答ページでは、最初に要求された URL にユーザをリダイレクトするリンクにドメイン名のみが含まれます。最初に要求された URL のドメイン名の後にテキストが含まれている場合、このテキストは切り捨てられます。
- エンド ユーザ確認ページがユーザに表示されると、そのトランザクションのアクセス ログ エントリには ACL デシジョン タグとして OTHER が表示されます。これは、最初に要求した URL がブロックされ、代わりにユーザにはエンド ユーザ確認ページが表示されたためです。

エンドユーザ確認ページの設定

Web インターフェイスまたはコマンドライン インターフェイスで、エンドユーザ確認応答ページをイネーブルにしたり、設定することができます。Web インターフェイスでエンドユーザ確認応答ページを設定する場合は、各ページに表示するカスタム メッセージを含めることができます。

CLI で、`advancedproxyconfig > eun` を使用します。

はじめる前に

- 表示言語の設定、および表示されるロゴのカスタマイズについては、通知ページの一般設定項目の設定（9-2 ページ）を参照してください。
- エンド ユーザに表示されるメッセージをカスタマイズする場合は、通知ページ上のカスタム メッセージ（9-11 ページ）を参照してください。[カスタム メッセージ（Custom Message）] ボックスでできること以上のカスタマイズが必要な場合は、通知ページ HTML ファイルの直接編集（9-13 ページ）を参照してください。

ステップ 1　[セキュリティ サービス（Security Services）] > [エンドユーザ通知（End-User Notification）] 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。

ステップ 3　[確認ページからクリックすることをエンドユーザに要求（Require end-user to click through acknowledgment page）] フィールドをイネーブルにします。

ステップ 4　オプションを入力します。

設定	説明
確認応答の時間間隔（Time Between Acknowledgements）	[確認応答の時間間隔（Time Between Acknowledgements）] では、Web プロキシがユーザごとにエンドユーザ確認ページを表示する頻度を指定します。この設定は、ユーザ名で追跡されるユーザ、および IP アドレスまたはセッション Cookie で追跡されるユーザに適用されます。30 ～ 2678400 秒（1 カ月）の任意の値を指定できます。デフォルトは 1 日（86400 秒）です。 [確認応答の時間間隔（Time Between Acknowledgements）] を変更して確定すると、Web プロキシは、Web プロキシに確認応答済みのユーザにも新しい値を使用します。
無活動タイムアウト（Inactivity Timeout）	[無活動タイムアウト（Inactivity Timeout）] では、IP アドレスまたはセッション Cookie（未認証ユーザのみ）によって追跡され確認されたユーザが、アクセプタブル ユース ポリシーに同意していないと見なされるまでに、アイドル状態を維持できる時間を指定します。30 ～ 2678400（1 か月）秒の任意の値を指定できます。デフォルトは 4 時間（14400 秒）です。

設定	説明
サロゲート タイプ（Surrogate Type）	Web プロキシがユーザの追跡に使用する方式を指定します。 • [IP アドレス（IP Address）]。Web プロキシは、その IP アドレスのユーザがエンドユーザ確認応答ページ上のリンクをクリックしたときに、任意の Web ブラウザまたはブラウザ以外の HTTP プロセスを使用して Web にアクセスできるようにします。IP アドレスによるユーザの追跡では、ユーザが非アクティブであったり設定された時間間隔が経過したために、新たな確認が必要になり、Web プロキシが新しいエンドユーザ確認応答ページを表示するまで、ユーザは Web アクセスできます。セッション Cookie による追跡とは異なり、IP アドレスによる追跡では、設定された時間間隔が経過しない限り、ユーザは複数の Web ブラウザ アプリケーションを開くことができ、エンドユーザ確認に合意する必要はありません。 （注）　IP アドレスが設定され、ユーザが認証されると、Web プロキシは、IP アドレスではなく、ユーザ名によってユーザを追跡します。 • [セッション Cookie（Session Cookie）]。ユーザがエンドユーザ確認応答ページ上のリンクをクリックすると、Web プロキシはユーザの Web ブラウザに Cookie を送信し、Cookie を使用してユーザのセッションを追跡します。[確認応答の時間間隔（Time Between Acknowledgements）] の値が失効するまで、または、ユーザが割り当てられた時間よりも長時間非アクティブであったり Web ブラウザを閉じるまで、ユーザは Web ブラウザを使用して Web にアクセスできます。 ブラウザ以外の HTTP クライアント アプリケーションを使用している場合、ユーザが Web にアクセスするには、エンドユーザ確認応答ページ上のリンクをクリックできなければなりません。別の Web ブラウザ アプリケーションを開く場合は、Web プロキシが別の Web ブラウザにセッション Cookie を送信できるように、ユーザは再度エンド ユーザ確認プロセスを実行する必要があります。 （注）　クライアントが FTP over HTTP を使用して HTTPS サイトや FTP サーバにアクセスする場合、セッション Cookie を使用したユーザの追跡はサポートされません。
カスタム メッセージ（Custom message）	各エンドユーザ確認応答ページに表示するテキストをカスタマイズします。いくつかの単純な HTML タグを組み込んでテキストを書式設定できます。 （注）　Web インターフェイスでエンドユーザ確認応答ページを設定する場合にのみカスタム メッセージを組み込むことができます。これは CLI では実行できません。 通知ページ上のカスタム メッセージ（9-11 ページ）も参照してください。

ステップ 5　(任意)[確認応答ページのカスタマイズをプレビュー(Preview Acknowledgment Page Customization)] をクリックして、別のブラウザ ウィンドウに現在のエンドユーザ確認応答ページを表示します。

(注)　HTML 通知ファイルを編集した場合、このプレビュー機能は使用できなくなります。

ステップ 6　変更を送信して確定します([送信(Submit)] と [変更を確定(Commit Changes)])。

エンドユーザ通知ページ

ポリシーが Web サイトからユーザをブロックする場合、URL 要求をブロックした理由をユーザに通知するようにアプライアンスを設定できます。これは、以下のようないくつかの方法で実行できます。

目的	参照先
Web Security Appliance でホストされている、事前定義され、カスタマイズ可能なページを表示します。	オンボックス エンドユーザ通知ページの設定 (9-6 ページ)
特定の URL にある HTTP エンドユーザ通知ページにユーザをリダイレクトします。	オフボックス エンドユーザ通知ページ (9-7 ページ)

オンボックス エンドユーザ通知ページの設定

オンボックス ページは、アプライアンス上にある、事前定義されたカスタマイズ可能な通知ページです。

はじめる前に

- 表示言語の設定、および表示されるロゴのカスタマイズについては、通知ページの一般設定項目の設定(9-2 ページ)を参照してください。
- オンボックス通知を使用して表示されるメッセージをカスタマイズする場合は、通知ページ上のカスタム メッセージ(9-11 ページ)以下のトピックを参照してください。[カスタム メッセージ(Custom Message)] ボックスでできること以上のカスタマイズが必要な場合は、通知ページ HTML ファイルの直接編集(9-13 ページ)を参照してください。

ステップ 1　[セキュリティ サービス(Security Services)] > [エンドユーザ通知(End-User Notification)] 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。

ステップ 3　[通知タイプ(Notification Type)] フィールドで、[オンボックス エンド ユーザ通知を使用(Use On Box End User Notification)] を選択します。

ステップ 4　オンボックス エンドユーザ通知ページの設定項目を設定します。

設定	説明
カスタム メッセージ（Custom Message）	各通知ページに必要なテキストを追加します。カスタム メッセージを入力すると、AsyncOS は、連絡先情報を含む通知ページの末尾の文の前にメッセージを配置します。
コンタクト情報（Contact Information）	各通知ページに表示される連絡先情報をカスタマイズします。 AsyncOS は、ユーザがネットワーク管理者に提供できる通知コードを表示する前に、連絡先情報の文をページの末尾の文として表示します。
エンドユーザ誤分類レポート（End-User Misclassification Reporting）	イネーブルにすると、ユーザは誤分類された URL をシスコに報告できます。マルウェアの疑いがあるため、または URL フィルタによってブロックされたサイトのオンボックス エンドユーザ通知ページには、追加のボタンが表示されます。このボタンを使用して、ユーザは誤分類されていると思われるページをレポートできます。その他のポリシー設定によってブロックされたページには表示されません。

ステップ 5　（任意）[通知ページのカスタマイズをプレビュー（Preview Notification Page Customization）] リンクをクリックして、別のブラウザ ウィンドウで現在のエンド ユーザ通知ページを表示します。

（注）　HTML 通知ファイルを編集した場合、このプレビュー機能は使用できなくなります。

ステップ 6　変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

オフボックス エンドユーザ通知ページ

すべての HTTP エンドユーザ通知ページを指定した特定の URL にリダイレクトするように Web プロキシを設定できます。

アクセスをブロックする理由に基づく適切なオフボックス ページの表示

デフォルトでは、AsyncOS は、元のページをブロックした理由に関係なく、ブロックしたすべての Web サイトを URL にリダイレクトします。ただし、AsyncOS はリダイレクト URL にクエリー文字列を追加し、それをパラメータとして渡すので、ブロックの理由を説明する固有のページをユーザに対して表示するように設定できます。組み込みパラメータの詳細については、オフボックス エンドユーザ通知ページのパラメータ（9-8 ページ）を参照してください。

Web サイトがブロックされた理由ごとに異なるページをユーザに表示する場合は、リダイレクト URL のクエリー文字列を解析できる CGI スクリプトを Web サーバに作成します。これによって、サーバは適切なページに別のリダイレクトを実行できます。

オフボックス通知ページの URL 基準

- 任意の HTTP または HTTPS URL を使用できます。
- URL では特定のポート番号を指定できます。
- URL では疑問符の後に引数を付けることはできません。
- URL には適切な形式のホスト名を含める必要があります。

たとえば、[カスタム URL へのリダイレクト（Redirect to Custom URL）] フィールドに以下の URL を入力したときに、

```
http://www.example.com/eun.policy.html
```

以下のアクセス ログ エントリがある場合、

```
1182468145.492 1 172.17.0.8 TCP_DENIED/403 3146 GET http://www.espn.com/index.html
HTTP/1.1 - NONE/- - BLOCK_WEBCAT-DefaultGroup-DefaultGroup-NONE-NONE-DefaultRouting
<IW_sprt,-,-,-,-,-,-,-,-,-,-,-,-,-,-,IW_sprt,-> -
```

AsyncOS は、以下のリダイレクト URL を作成します。

```
http://www.example.com/eun.policy.html?Time=21/Jun/
2007:23:22:25%20%2B0000&ID=0000000004&Client_IP=172.17.0.8&User=-
&Site=www.espn.com&URI=index.html&Status_Code=403&Decision_Tag=
BLOCK_WEBCAT-DefaultGroup-DefaultGroup-NONE-NONE-DefaultRouting
&URL_Cat=Sports%20and%20Recreation&WBRS=-&DVS_Verdict=-&
DVS_ThreatName=-&Reauth_URL=-
```

オフボックス エンドユーザ通知ページのパラメータ

AsyncOS は、HTTP GET 要求の標準 URL パラメータとして Web サーバにパラメータを渡します。以下の形式を使用します。

```
<notification_page_url>?param1=value1&param2=value2
```

以下の表は、AsyncOS がクエリー文字列に含めるパラメータを示しています。

パラメータ名	説明
Time	トランザクションの日付と時刻。
ID	トランザクション ID。
Client_IP	クライアントの IP アドレス。
User	要求を行うクライアントのユーザ名（該当する場合）。
Site	HTTP 要求の宛先ホスト名。
URI	HTTP 要求で指定された URL パス。
Status_Code	要求の HTTP ステータス コード。
Decision_Tag	DVS エンジンがトランザクションを処理した方法を示す、アクセス ログ エントリで定義されている ACL デシジョン タグ。
URL_Cat	URL フィルタリング エンジンがトランザクション要求に割り当てた URL カテゴリ。 **注：**AsyncOS for Web は、定義済みとユーザ定義の両方の URL カテゴリの URL カテゴリ名全体を送信します。カテゴリ名に対して URL エンコードが行われるため、スペースは「%20」と書き込まれます。
WBRS	Web レピュテーション フィルタが要求の URL に割り当てた WBRS スコア。
DVS_Verdict	DVS エンジンがトランザクションに割り当てるマルウェア カテゴリ。
DVS_ThreatName	DVS エンジンによって検出されたマルウェアの名前。

パラメータ名	説明
Reauth_URL	制限付き URL フィルタリング ポリシーによって Web サイトからブロックされた場合、ユーザはこの URL をクリックして再度認証を受けることができます。このパラメータは、[URL カテゴリまたはユーザ セッションの制限によりエンド ユーザがブロックされた場合に再認証プロンプトをイネーブルにする（Enable Re-Authentication Prompt If End User Blocked by URL Category or User Session Restriction）] グローバル認証設定がイネーブルになっているときに、URL カテゴリがブロックされたため、ユーザが Web サイトからブロックされた場合に使用します。 このパラメータを使用するには、CGI スクリプトで以下の手順が実行されるようにします。 1. `Reauth_Url` パラメータの値を取得する。 2. URL エンコードされた値をデコードする。 3. 値を Base64 でデコードし、実際の再認証 URL を取得する。 4. デコードした URL を何らかの方法で（リンクまたはボタンとして）エンドユーザ通知ページに組み込み、「リンクをクリックすると、より広範なアクセスが可能になる新しい認証クレデンシャルを入力できること」をユーザに示す使用説明を含める。

（注） AsyncOS は、リダイレクトされた各 URL に、常にすべてのパラメータを組み込みます。特定のパラメータの値が存在しない場合、AsyncOS はハイフン（-）を渡します。

カスタム URL へのエンドユーザ通知ページのリダイレクト（オフボックス）

ステップ 1　[セキュリティ サービス（Security Services）] > [エンドユーザ通知（End-User Notification）] 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。

ステップ 3　[エンドユーザ通知ページ（End-User Notification Pages）] セクションで、[カスタム URL へのリダイレクト（Redirect to Custom URL）] を選択します。

ステップ 4　[通知ページの URL（Notification Page URL）] フィールドに、ブロックされた Web サイトをリダイレクトする URL を入力します。

ステップ 5　（任意）[カスタム URL のプレビュー（Preview Custom URL）] をクリックします。

ステップ 6　変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

エンド ユーザ URL フィルタリング警告ページの設定

エンドユーザ URL フィルタリング警告ページは、ユーザが特定の URL カテゴリの Web サイトに初めてアクセスしてから一定時間経過後に表示されます。サイト コンテンツ レーティング機能がイネーブルのときに、ユーザがアダルト コンテンツにアクセスした場合の警告ページを設定することもできます。

はじめる前に

オンボックス通知を使用して表示されるメッセージをカスタマイズする場合は、通知ページ上のカスタム メッセージ（9-11 ページ）以下のトピックを参照してください。[カスタム メッセージ（Custom Message）] ボックスでできること以上のカスタマイズが必要な場合は、通知ページ HTML ファイルの直接編集（9-13 ページ）を参照してください。

ステップ 1　[セキュリティ サービス（Security Services）] > [エンドユーザ通知（End-User Notification）] 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。

ステップ 3　[エンドユーザフィルタリング警告ページ（End-User URL Filtering Warning Page] セクションまでスクロール ダウンします。

ステップ 4　[確認応答の時間間隔（Time Between Warning）] フィールドで、Web プロキシがユーザごとに各 URL カテゴリに対してエンドユーザ URL フィルタリング警告ページを表示する時間間隔を入力します。

30 ～ 2678400 秒（1 カ月）の任意の値を指定できます。デフォルトは 1 時間（3600 秒）です。秒、分、または日単位で値を入力できます。秒には「s」、分には「m」、日には「d」を使用します。

ステップ 5　[カスタム メッセージ（Custom Message）] フィールドで、すべてのエンドユーザ URL フィルタリング警告ページに表示するテキストを入力します。

ステップ 6　[URL カテゴリ警告ページのカスタマイズをプレビュー（Preview URL Category Warning Page Customization）] をクリックして、別のブラウザ ウィンドウでエンドユーザ URL フィルタリング警告ページを表示します。

（注）　HTML 通知ファイルを編集した場合、このプレビュー機能は使用できなくなります。

ステップ 7　変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

FTP 通知メッセージの設定

FTP サーバの認証エラーやサーバ ドメイン名に対する低いレピュテーションなど、何らかの理由により FTP プロキシが FTP サーバとの接続を確立できない場合、FTP プロキシはネイティブ FTP クライアントに定義済みのカスタマイズ可能な通知メッセージを表示します。通知は、接続がブロックされる理由によって固有なものになります。

はじめる前に

オンボックス通知を使用して表示されるメッセージをカスタマイズする場合は、通知ページ上のカスタム メッセージ（9-11 ページ）以下のトピックを参照してください。[カスタム メッセージ（Custom Message）] ボックスでできること以上のカスタマイズが必要な場合は、通知ページ HTML ファイルの直接編集（9-13 ページ）を参照してください。

ステップ 1　[セキュリティ サービス（Security Services）] > [エンドユーザ通知（End-User Notification）] 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。

ステップ 3　[ネイティブ FTP（Native FTP）] セクションまでスクロール ダウンします。

ステップ 4　[言語（Language）] フィールドで、ネイティブ FTP 通知メッセージを表示する際に使用する言語を選択します。

ステップ 5　[カスタムメッセージ（Custom Message）] フィールドで、すべてのネイティブ FTP 通知メッセージに表示するテキストを入力します。

ステップ 6　変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

通知ページ上のカスタム メッセージ

以下のセクションの説明は、[エンドユーザ通知の編集（Edit End-User Notification）] ページで設定した任意の通知タイプの [カスタム メッセージ（Custom Message）] ボックスに入力するテキストに適用されます。

- 通知ページのカスタム メッセージでサポートされる HTML タグ（9-11 ページ）
- 通知ページの URL とロゴに関する注意事項（9-12 ページ）

通知ページのカスタム メッセージでサポートされる HTML タグ

[カスタム メッセージ（Custom Message）] ボックスが用意された [エンドユーザ通知の編集（Edit End-User Notification）] ページでは、HTML タグを使用して、任意の通知のテキストを書式設定することができます。タグは小文字で入力し、標準 HTML 構文（終了タグなど）に従う必要があります。

以下の HTML タグを使用できます。

- <a>
-
-
- <big></big>
-
- <code></code>
-
-
- <small></small>
-

たとえば、一部のテキストを斜体にすることができます。

```
Please acknowledge the following statements <i>before</i> accessing the Internet.
```

 タグを使用すると、CSS スタイルでテキストを書式設定できます。たとえば、一部のテキストを赤色にすることができます。

```
<span style="color: red">Warning:</span> You must acknowledge the following statements
<i>before</i> accessing the Internet.
```

（注）　通知ページをさらに柔軟にする必要がある場合や、JavaScript を追加したい場合は、HTML 通知ファイルを直接編集します。通知の [カスタム メッセージ（Custom Message）] ボックスに入力した JavaScript は、Web ユーザのインターフェイスでは削除されます。通知ページ HTML ファイルの直接編集（9-13 ページ）を参照してください。

通知ページの URL とロゴに関する注意事項

この項は以下のいずれかのカスタマイズ行う場合に適用されます。

- [エンドユーザ通知の編集（Edit End-User Notification）] ページで、任意の通知の [カスタム メッセージ（Custom Message）] ボックスにテキストを入力する。
- オンボックス通知の HTML ファイルを直接編集する。
- カスタム ロゴを使用する。

オンボックス通知の場合、カスタム テキストにリンクが埋め込まれた URL パスとドメイン名の全組み合わせとカスタム ロゴのあらゆる組み合わせが、以下のものから免除されます。

- ユーザ認証
- エンドユーザ確認応答
- マルウェア スキャンおよび Web レピュテーション スコアなどのすべてのスキャン

たとえば、以下の URL がカスタム テキストに埋め込まれている場合、

```
http://www.example.com/index.html
```

```
http://www.mycompany.com/logo.jpg
```

以下の URL すべてがあらゆるスキャンの対象外として扱われます。

```
http://www.example.com/index.html
```

```
http://www.mycompany.com/logo.jpg
```

```
http://www.example.com/logo.jpg
```

```
 http://www.mycompany.com/index.html
```

また、埋め込まれた URL の形式が `<protocol>://<domain-name>/<directory path>/` である場合、ホスト上のそのディレクトリ パスにあるすべてのサブファイルとサブディレクトリもすべてのスキャンから除外されます。

たとえば、`http://www.example.com/gallery2/` という URL が埋め込まれている場合は、`http://www.example.com/gallery2/main.php` などの URL も対象外として扱われます。

これにより、埋め込まれたコンテンツが最初の URL に関連している限り、埋め込まれたコンテンツを使用してより高度なページを作成することができます。ただし、リンクやカスタム ロゴとして含めるパスを決定する際に注意を払う必要があります。

通知ページ HTML ファイルの直接編集

各通知ページは、Web Security Appliance に HTML ファイルとして保存されます。Web ベース インターフェイスの [カスタム メッセージ（Custom Message）] ボックスでできること以上のカスタマイズが必要な場合は、これらの HTML ファイルを直接編集できます。たとえば、標準 JavaScript を含めるか、または各ページの全体的なルック アンド フィールを編集できます。

以下の各項の情報は、エンドユーザ確認ページなど、アプライアンスの任意の種類のエンドユーザ通知 HTML ファイルに適用されます。

通知 HTML ファイルを直接編集するための要件

- 個々のカ通知ページ ファイルは、有効な HTML ファイルである必要があります。組み込むことができる HTML タグのリストについては、通知ページのカスタム メッセージでサポートされる HTML タグ（9-11 ページ）を参照してください。
- カスタマイズした通知ページ ファイルの名前は、Web Security Appliance に同梱されているファイルの名前と正確に一致する必要があります。

  `configuration\eun` ディレクトリに必要な名前を持つ特定のファイルが含まれていない場合、アプライアンスは標準のオンボックス エンドユーザ通知ページを表示します。
- HTML ファイルに URL へのリンクを含めないでください。通知ページに含まれるリンクは、アクセス ポリシーで定義されたアクセス制御ルールの対象となり、ユーザは再帰ループで終了する場合があります。
- 特に JavaScript. が含まれている場合は、期待どおりに動作することを確認するために、サポートされているクライアントのブラウザで HTML ファイルをテストします。
- カスタマイズしたページが効果を表すようにするには、`advancedproxyconfig > EUN > Refresh EUN Pages` CLI コマンドを使用して、カスタマイズしたファイルを有効化する必要があります。

通知 HTML ファイルの直接編集

はじめる前に

- 通知 HTML ファイルを直接編集するための要件（9-13 ページ）の要件を確認します。
- 通知 HTML ファイルのカスタマイズのための変数および通知 HTML ファイルでの変数の使用（9-14 ページ）を参照してください。

ステップ 1　FTP クライアントを使用して、Web Security Appliance に接続します。

ステップ 2　`configuration\eun` ディレクトリに移動します。

ステップ 3　編集する通知ページの言語ディレクトリ ファイルをダウンロードします。

ステップ 4　ローカル マシンで、テキスト エディタまたは HTML エディタを使用して HTML ファイルを編集します。

ステップ 5　FTP クライアントを使用して、ステップ 3 でこれらのファイルをダウンロードした同じディレクトリに、カスタマイズした HTML ファイルをアップロードします。

ステップ 6　SSH クライアントを開き、Web Security Appliance に接続します。

ステップ 7　`advancedproxyconfig > EUN` CLI コマンドを実行します。

ステップ 8　2 を入力して、カスタム エンド ユーザ通知ページを使用します。

ステップ 9　HTML ファイルを更新する際にカスタム エンド ユーザ通知ページ オプションがイネーブルになっている場合は、1 を入力して、カスタム エンド ユーザ通知ページを更新します。

これを実行しないと、Web プロキシを再起動するまで新しいファイルが有効になりません。

ステップ 10　変更を保存します。

ステップ 11　SSH クライアントを閉じます。

通知 HTML ファイルでの変数の使用

通知 HTML ファイルを編集する際に、条件変数を含めると、実行時点のステータスに応じて異なるアクションを実行する if-then ステートメントを作成できます。

以下の表は、さまざまな条件変数の形式を示しています。

条件変数の形式	説明
%?*V*	変数 %*V* の出力が空でない場合、この条件変数は TRUE に評価されます。
%!*V*	以下の条件を表します。 `else` これを %?*V* 条件変数とともに使用します。
%#*V*	以下の条件を表します。 `endif` これを %?*V* 条件変数とともに使用します。

たとえば、以下の HTML コードの一部であるテキストでは、再認証が提供されるかどうかをチェックする条件変数として %R が使用され、再認証 URL を提供する標準変数として %r が使用されています。

```
%?R
<div align="left">
  <form name="ReauthInput" action="%r" method="GET">
    <input name="Reauth" type="button" OnClick="document.location='%r'"
id="Reauth" value="Login as different user...">
  </form>
</div>
%#R
```

通知 HTML ファイルのカスタマイズのための変数に記載されている任意の変数を条件変数として使用できます。ただし、条件文での使用に最も適した変数は、サーバ応答ではなく、*クライアント要求*に関連する変数であり、常に TRUE に評価される変数ではなく、状況に応じて TRUE に評価される（または評価されない）変数です。

通知 HTML ファイルのカスタマイズのための変数

通知 HTML ファイルで変数を使用して、ユーザ固有の情報を表示できます。また、各変数を条件変数に変換して、if-then ステートメントを作成することもできます。詳細については、通知 HTML ファイルでの変数の使用（9-14 ページ）を参照してください。

変数	説明	条件変数として使用する場合、常に TRUE に評価
%a	FTP の認証レルム	なし
%A	ARP アドレス	あり
%b	ユーザエージェント名	なし
%B	ブロックした理由（BLOCK-SRC または BLOCK-TYPE など）	なし
%c	エラー ページの担当者	あり
%C	Set-Cookie: ヘッダー行全体、または空の文字列	なし
%d	クライアント IP アドレス	あり
%D	ユーザ名	なし
%e	エラー ページの電子メール アドレス	あり
%E	エラー ページのロゴの URL	なし
%f	ユーザ フィードバック セクション	なし
%F	ユーザ フィードバックの URL	なし
%g	Web カテゴリ名（使用可能な場合）	あり
%G	許可される最大ファイル サイズ（MB 単位）	なし
%h	プロキシのホスト名	あり
%H	URL のサーバ名	あり
%i	トランザクション ID（16 進数値）	あり
%I	管理 IP アドレス	あり
%j	URL カテゴリ警告ページのカスタム テキスト	なし
%k	エンドユーザ確認応答ページおよびエンドユーザ URL フィルタリング警告ページのリダイレクション リンク	なし
%K	レスポンス ファイル タイプ	なし
%l	WWW-Authenticate：ヘッダー行	なし
%L	Proxy-Authenticate：ヘッダー行	なし
%M	要求方式（「GET」、「POST」など）	あり
%n	マルウェア カテゴリ名（使用可能な場合）	なし
%N	マルウェア脅威名（使用可能な場合）	なし
%o	Web レピュテーションの脅威タイプ（使用可能な場合）	なし
%O	Web レピュテーションの脅威の理由（使用可能な場合）	なし
%p	Proxy-Connection HTTP ヘッダーの文字列	あり
%P	プロトコル	あり

変数	説明	条件変数として使用する場合、常に TRUE に評価
%q	ID ポリシー グループの名前	あり
%Q	非 ID ポリシーのポリシー グループ名	あり
%r	リダイレクト URL	なし
%R	再認証が提供されます。この変数は、false の場合に空の文字列を出力し、true の場合にスペースを出力するので、単独で使用しても役立ちません。代わりに、条件変数として使用します。	なし
%S	プロキシの署名	なし。常に FALSE に評価
%t	UNIX のタイムスタンプ（秒 + ミリ秒）	あり
%T	日付	あり
%u	URI の一部を構成する URL（サーバ名を除く URL）	あり
%U	要求の完全な URL	あり
%v	HTTP プロトコルのバージョン	あり
%W	管理 WebUI ポート	あり
%X	拡張ブロック コード。ACL デシジョン タグや WBRS スコアなど、アクセス ログに記録された大部分の Web レピュテーションやアンチマルウェア情報をエンコードする 16 バイトの Base64 値です。	あり
%Y	設定されている場合は、管理者のカスタム テキスト文字列。設定されていない場合は空の文字列	なし
%y	エンドユーザ確認応答ページのカスタム テキスト	あり
%z	Web レピュテーション スコア	あり
%Z	DLP メタデータ	あり
%%	通知ページにパーセント記号（%）を出力します	該当なし

通知ページのタイプ

デフォルトでは、Web プロキシは、ユーザがブロックされたことおよびその理由をユーザに知らせる通知ページを表示します。

ほとんどの通知ページは、管理者または Cisco カスタマー サポートが潜在的な問題をトラブルシューティングするのに役立つ可能性のあるさまざまなコードのセットを表示します。一部のコードはシスコ内部でのみ使用されます。通知ページに表示されるさまざまなコードは、カスタマイズした通知ページに含めることができる変数と同じです（通知 HTML ファイルのカスタマイズのための変数を参照）。

以下の表は、ユーザに表示される可能性があるさまざまな通知ページを示しています。

ファイル名および通知タイトル	通知の説明	通知テキスト
ERR_ACCEPTED フィードバックを受け取りました。(Feedback Accepted,)ありがとうございました。(Thank You)	ユーザが [誤分類をレポート(Report Misclassification)] オプションを使用した後に表示される通知ページ。	誤分類のレポートが送信されました。(The misclassification report has been sent.)フィードバックいただき、ありがとうございました。(Thank you for your feedback.)
ERR_ADAPTIVE_SECURITY ポリシー: 全般(Policy: General)	ユーザが適応型スキャン機能によってブロックされた場合に表示されるブロック ページ。	この Web サイト <URL> は、コンテンツがセキュリティ リスクであると判定されたため、組織のセキュリティ ポリシーに基づいてブロックされました。(Based on your organization's security policies, this web site *<URL>* has been blocked because its content has been determined to be a security risk.)
ERR_ADULT_CONTENT ポリシーの確認(Policy Acknowledgment)	エンドユーザがアダルト コンテンツに分類されるページにアクセスしたときに表示される警告ページ。ユーザは確認リンクをクリックして、最初に要求したサイトに進むことができます。	明示的にアダルト向けとレーティングされたコンテンツを含む Web ページにアクセスしようとしています。(You are trying to visit a web page whose content are rated as explicit or adult.)下記のリンクをクリックし、このコンテンツ タイプに対するインターネットの使用を管理している組織のポリシーを読了して同意済みであることを確認してください。(By clicking the link below, you acknowledge that you have read and agree with the organization's policies that govern the usage of the Internet for this type of content.)ブラウジング動作に関するデータがモニタされ、記録される場合があります。(Data about your browsing behavior may be monitored and recorded.)この種の Web ページに引き続きアクセスした場合は、このメッセージが定期的に提示され、確認を求められます。(You will be periodically asked to acknowledge this statement for continued access to this kind of web page.) このステートメントに同意してインターネットにアクセスするには、ここをクリックしてください。(Click here to accept this statement and access the Internet.)
ERR_AVC ポリシー: アプリケーションの制御(Policy: Application Controls)	ユーザが Application Visibility and Control エンジンによってブロックされた場合に表示されるブロック ページ。	組織のアクセス ポリシーに基づき、タイプ %2 のアプリケーション %1 へのアクセスがブロックされました。(Based on your organization's access policies, access to application %1 of type %2 has been blocked.)

ファイル名および 通知タイトル	通知の説明	通知テキスト
ERR_BAD_REQUEST 不正な要求（Bad Request）	無効なトランザクション要求によって生じるエラー ページ。	システムはこの要求を処理できません。（The system cannot process this request.）非標準のブラウザによって無効な HTTP 要求が生成された可能性があります。（A non-standard browser may have generated an invalid HTTP request.） 標準ブラウザを使用している場合は、要求を再試行してください。（If you are using a standard browser, please retry the request.）
ERR_BLOCK_DEST ポリシー：宛先（Policy: Destination）	ブロックされている Web サイトのアドレスにユーザがアクセスを試みた場合に表示されるブロック ページ。	組織のアクセス ポリシーに基づき、この Web サイト <URL> へのアクセスがブロックされました。（Based on your organization's Access Policies, access to this web site <*URL*> has been blocked.）
ERR_BROWSER セキュリティ：ブラウザ（Security: Browser）	マルウェアまたはスパイウェアによって侵害されていると識別されたアプリケーションからトランザクション要求が発信された場合に表示されるブロック ページ。	組織のネットワークに対するセキュリティ上の脅威であると判定されたため、組織のアクセス ポリシーに基づき、コンピュータからの要求がブロックされました。（Based on your organization's Access Policies, requests from your computer have been blocked because it has been determined to be a security threat to the organization's network.）「<マルウェア名>」として識別されたマルウェア/スパイウェア エージェントによってブラウザが侵害されている可能性があります。（Your browser may have been compromised by a malware/spyware agent identified as “<*malware name*>”.） <担当者名> <電子メール アドレス> に連絡し、以下に示すコードを提出してください。（Please contact <*contact name*> <*email address*> and provide the codes shown below.） 非標準のブラウザを使用しており、誤って分類されたと思われる場合は、以下のボタンを使用してこの誤分類をレポートしてください。（If you are using a non-standard browser and believe it has been misclassified, use the button below to report this misclassification.）
ERR_BROWSER_ CUSTOM ポリシー：ブラウザ（Policy: Browser）	ブロックされたユーザ エージェントからトランザクション要求が発信されたときに表示されるブロック ページ。	組織のアクセス ポリシーに基づき、ブラウザからの要求がブロックされました。（Based on your organization's Access Policies, requests from your browser have been blocked.）このブラウザ「<ブラウザ タイプ>」は、潜在的なセキュリティ リスクのため許可されません。（This browser “<*browser type*>” is not permitted due to potential security risks.）

ファイル名および通知タイトル	通知の説明	通知テキスト
ERR_CERT_INVALID 無効な証明書（Invalid Certificate）	要求された HTTPS サイトが無効な証明書を使用している場合に表示されるブロック ページ。	サイト <ホスト名> が無効な証明書を提示したため、セキュア セッションを確立できません。（A secure session cannot be established because the site <*hostname*> provided an invalid certificate.）
ERR_CONTINUE_UNACKNOWLEDGED ポリシーの確認（Policy Acknowledgment）	警告アクションが割り当てられているカスタム URL カテゴリのサイトをユーザが要求した場合に表示される警告ページ。ユーザは確認リンクをクリックして、最初に要求したサイトに進むことができます。	URL カテゴリ <URL カテゴリ> に分類される Web ページにアクセスしようとしています。（You are trying to visit a web page that falls under the URL Category <*URL category*>.）下記のリンクをクリックし、このコンテンツ タイプに対するインターネットの使用を管理している組織のポリシーを読了して同意済みであることを確認してください。（By clicking the link below, you acknowledge that you have read and agree with the organization's policies that govern the usage of the Internet for this type of content.）ブラウジング動作に関するデータがモニタされ、記録される場合があります。（Data about your browsing behavior may be monitored and recorded.）この種の Web ページに引き続きアクセスした場合は、このメッセージが定期的に提示され、確認を求められます。（You will be periodically asked to acknowledge this statement for continued access to this kind of web page.） このステートメントに同意してインターネットにアクセスするには、ここをクリックしてください。（Click here to accept this statement and access the Internet.）

ファイル名および通知タイトル	通知の説明	通知テキスト
ERR_DNS_FAIL DNS の障害（DNS Failure）	要求された URL に無効なドメイン名が含まれている場合に表示されるエラー ページ。	このホスト名 <ホスト名> のホスト名解決（DNS ルックアップ）に失敗しました。（The hostname resolution (DNS lookup) for this hostname <*hostname*> has failed.）インターネット アドレスのスペルが誤っているか、インターネット アドレスが廃止されているか、ホスト <ホスト名> が一時的に利用できないか、または DNS サーバが無応答状態になっている可能性があります。（The Internet address may be misspelled or obsolete, the host <*hostname*> may be temporarily unavailable, or the DNS server may be unresponsive.） 入力したインターネット アドレスのスペルを確認してください。（Please check the spelling of the Internet address entered.）スペルが正しい場合は、後でこの要求を試行してください。（If it is correct, try this request later.）
ERR_EXPECTATION_FAILED 予測の失敗（Expectation Failed）	トランザクション要求が HTTP 417「Expectation Failed」応答をトリガーしたときに表示されるエラー ページ。	システムはこのサイト <URL> に対する要求を処理できません。（The system cannot process the request for this site <*URL*>.）非標準のブラウザによって無効な HTTP 要求が生成された可能性があります。（A non-standard browser may have generated an invalid HTTP request.） 標準ブラウザを使用している場合は、要求を再試行してください。（If using a standard browser, please retry the request.）
ERR_FILE_SIZE ポリシー:ファイル サイズ（Policy: File Size）	要求されたファイルが許容される最大ファイル サイズよりも大きい場合に表示されるブロック ページ。	ダウンロード サイズが許容限度を超えているため、組織のアクセス ポリシーに基づき、この Web サイトまたはダウンロード <URL> へのアクセスがブロックされました。（Based on your organization's Access Policies, access to this web site or download <*URL*> has been blocked because the download size exceeds the allowed limit.）
ERR_FILE_TYPE ポリシー:ファイル タイプ（Policy: File Type）	要求したファイルがブロックされているファイル タイプである場合に表示されるブロック ページ。	ファイル タイプ「<ファイル タイプ>」は許可されていないため、組織のアクセス ポリシーに基づき、この Web サイトまたは ダウンロード <URL> へのアクセスがブロックされました。（Based on your organization's Access Policies, access to this web site or download <*URL*> has been blocked because the file type “<*file type*>” is not allowed.）

ファイル名および通知タイトル	通知の説明	通知テキスト
ERR_FILTER_FAILURE フィルタの障害（Filter Failure）	URL フィルタリング エンジンが一時的に URL フィルタリング応答を配信できず、[到達不能サービスに対するデフォルトアクション（Default Action for Unreachable Service）] オプションが [ブロック（Block）] に設定されている場合に表示されるエラー ページ。	内部サーバが到達不能または過負荷になっているため、ページ <URL> の要求が拒否されました。（The request for page <*URL*> has been denied because an internal server is currently unreachable or overloaded.） 後で要求を再試行してください。（Please retry the request later.）
ERR_FOUND 検出（Found）	一部のエラー用の内部リダイレクション ページ。	ページ <URL> は <リダイレクト先 URL> にリダイレクトされます。（The page <*URL*> is being redirected to <*redirected URL*>.）
ERR_FTP_ABORTED FTP 中断（FTP Aborted）	FTP over HTTP トランザクション要求が HTTP 416「Requested Range Not Satisfiable」応答をトリガーしたときに表示されるエラー ページ。	ファイル <URL> に対する要求が成功しませんでした。（The request for the file <*URL*> did not succeed.）FTP サーバ <ホスト名> が突然接続を終了しました。（The FTP server <*hostname*> unexpectedly terminated the connection.） 後で要求を再試行してください。（Please retry the request later.）
ERR_FTP_AUTH_REQUIRED FTP 認可が必要（FTP Authorization Required）	FTP over HTTP トランザクション要求が FTP 530「Not Logged In」応答をトリガーしたときに表示されるエラー ページ。	FTP サーバ <ホスト名> には認証が必要です。（Authentication is required by the FTP server <*hostname*>.）プロンプトに従って有効なユーザ ID とパスフレーズを入力してください。（A valid user ID and passphrase must be entered when prompted.） 場合により、FTP サーバが匿名接続の数を制限する可能性があります。（In some cases, the FTP server may limit the number of anonymous connections.）通常、匿名ユーザとしてこのサーバに接続している場合は、後で再試行してください。（If you usually connect to this server as an anonymous user, please try again later.）
ERR_FTP_CONNECTION_FAILED FTP 接続の失敗（FTP Connection Failed）	FTP over HTTP トランザクション要求が FTP 425「Can't open data connection」応答をトリガーしたときに表示されるエラー ページ。	システムが FTP サーバ <ホスト名> と通信できません。（The system cannot communicate with the FTP server <*hostname*>.）FTP サーバが一時的または恒久的にダウンしているか、ネットワークの問題により到達不能になっている可能性があります。（The FTP server may be temporarily or permanently down, or may be unreachable because of network problems.） 入力したアドレスのスペルを確認してください。（Please check the spelling of the address entered.）スペルが正しい場合は、後でこの要求を試行してください。（If it is correct, try this request later.）

ファイル名および通知タイトル	通知の説明	通知テキスト
ERR_FTP_FORBIDDEN FTP の禁止（FTP Forbidden）	FTP over HTTP トランザクション要求が、ユーザ アクセスが許可されないオブジェクトに対して行われた場合に表示されるエラー ページ。	FTP サーバ <ホスト名> によってアクセスが拒否されました。（Access was denied by the FTP server <*hostname*>.）ご使用の ID にはこのドキュメントへのアクセス権がありません。（Your user ID does not have permission to access this document.）
ERR_FTP_NOT_FOUND FTP が検出されない（FTP Not Found）	FTP over HTTP トランザクション要求が、サーバ上に存在しないオブジェクトに対して行われた場合に表示されるエラー ページ。	ファイル <URL> が見つかりませんでした。（The file <*URL*> could not be found.）アドレスが間違っているか、または廃止されています。（The address is either incorrect or obsolete.）
ERR_FTP_SERVER_ERR FTP サーバ エラー（FTP Server Error）	FTP をサポートしていないサーバにアクセスを試みている FTP over HTTP トランザクションに対して表示されるエラー ページ。通常、サーバは HTTP 501「Not Implemented」応答を返します。	システムが FTP サーバ <ホスト名> と通信できません。（The system cannot communicate with the FTP server <*hostname*>.）FTP サーバが一時的または恒久的にダウンしているか、このサービスを提供していない可能性があります。（The FTP server may be temporarily or permanently down, or may not provide this service.） 有効なアドレスであることを確認してください。（Please confirm that this is a valid address.）スペルが正しい場合は、後でこの要求を試行してください。（If it is correct, try this request later.）
ERR_FTP_SERVICE_UNAVAIL FTP サービス使用不可（FTP Service Unavailable）	使用できない FTP サーバにアクセスを試みている FTP over HTTP トランザクションに対して表示されるエラー ページ。	システムが FTP サーバ <ホスト名> と通信できません。（The system cannot communicate with the FTP server <*hostname*>.）FTP サーバがビジー状態であるか、恒久的にダウンしているか、またはこのサービスを提供していない可能性があります。（The FTP server may be busy, may be permanently down, or may not provide this service.） 有効なアドレスであることを確認してください。（Please confirm that this is a valid address.）スペルが正しい場合は、後でこの要求を試行してください。（If it is correct, try this request later.）

ファイル名および 通知タイトル	通知の説明	通知テキスト
ERR_GATEWAY_TIMEOUT ゲートウェイのタイムアウト（Gateway Timeout）	要求されたサーバがタイムリーに応答しなかったときに表示されるエラー ページ。	システムが外部サーバ <ホスト名> と通信できません。（The system cannot communicate with the external server <*hostname*>.）インターネット サーバがビジー状態か、恒久的にダウンしているか、またはネットワークの問題により到達不能になっている可能性があります。（The Internet server may be busy, may be permanently down, or may be unreachable because of network problems.） 入力したインターネット アドレスのスペルを確認してください。（Please check the spelling of the Internet address entered.）スペルが正しい場合は、後でこの要求を試行してください。（If it is correct, try this request later.）
ERR_IDS_ACCESS_FORBIDDEN IDS アクセスの禁止（IDS Access Forbidden）	設定済みの Cisco データ セキュリティ ポリシーによってブロックされているファイルを、ユーザがアップロードしようとした場合に表示されるエラー ページ。	組織のデータ転送ポリシーに基づき、アップロード要求がブロックされました。（Based on your organization's data transfer policies, your upload request has been blocked.）ファイルの詳細（File details）: <*ファイルの詳細*>
ERR_INTERNAL_ERROR 内部エラー（Internal Error）	内部エラーが発生した場合に表示されるエラー ページ。	ページ <URL> に対する要求を処理中に内部システム エラーが発生しました。（Internal system error when processing the request for the page <*URL*>.） この要求を再試行してください。（Please retry this request.） この状態が続く場合は、<担当者名> <電子メール アドレス> に連絡し、以下に示すコードを提出してください。（If this condition persists, please contact <*contact name*> <*email address*> and provide the code shown below.）

ファイル名および 通知タイトル	通知の説明	通知テキスト
ERR_MALWARE_SPECIFIC セキュリティ：マルウェアの検出（Security: Malware Detected）	ファイルのダウンロード時にマルウェアが検出された場合に表示されるブロック ページ。	この Web サイト <URL> は、コンピュータまたは組織のネットワークに対するセキュリティ上の脅威と判定されたため、組織のアクセス ポリシーに基づいてブロックされました。（Based on your organization's Access Policies, this web site <*URL*> has been blocked because it has been determined to be a security threat to your computer or the organization's network.） カテゴリ <マルウェア カテゴリ> のマルウェア <マルウェア名> がこのサイトで検出されました。（Malware <*malware name*> in the category <*malware category*> has been found on this site.）
ERR_MALWARE_SPECIFIC_OUTGOING セキュリティ：マルウェアの検出（Security: Malware Detected）	ファイルのアップロード時にマルウェアが検出された場合に表示されるブロック ページ。	受信側端末のネットワーク セキュリティにとって有害なマルウェアがこのファイルから検出されたため、組織のポリシーに基づいて URL（<URL>）へのこのファイルのアップロードがブロックされました。（Based on your organization's policy, the upload of the file to URL (<*URL*>) has been blocked because the file was detected to contain malware that will be harmful to the receiving end's network security.） マルウェア名（Malware Name）：<*マルウェアの名前*> マルウェア カテゴリ（Malware Category）：<*マルウェアのカテゴリ*>
ERR_NATIVE_FTP_DENIED	ネイティブ FTP トランザクションがブロックされたときに、ネイティブ FTP クライアントで表示されるブロック メッセージ。	530 ログインが拒否されました（530 Login denied）
ERR_NO_MORE_FORWARDS これ以上転送なし（No More Forwards）	Web プロキシとネットワーク上の他のプロキシ サーバ間に転送ループがあることをアプライアンスが検出した場合に表示されるエラー ページ。Web プロキシはループを切断し、クライアントにこのメッセージを表示します。	ページ <URL> に対する要求が失敗しました。（The request for the page <*URL*> failed.） サーバ アドレス <ホスト名> が無効であるか、またはこのサーバにアクセスするにはポート番号を指定する必要があります。（The server address <*hostname*> may be invalid, or you may need to specify a port number to access this server.）
ERR_POLICY ポリシー：全般（Policy: General）	要求が何らかのポリシー設定によってブロックされた場合に表示されるブロック ページ。	組織のアクセス ポリシーに基づき、この Web サイト <URL> へのアクセスがブロックされました。（Based on your organization's Access Policies, access to this web site <*URL*> has been blocked.）

ファイル名および通知タイトル	通知の説明	通知テキスト
ERR_PROTOCOL ポリシー:プロトコル（Policy: Protocol）	使用しているプロトコルに基づいて要求がブロックされた場合に表示されるブロック ページ。	データ転送プロトコル「<プロトコル タイプ>」が許可されていないため、組織のアクセス ポリシーに基づき、この要求はブロックされました。（Based on your organization's Access Policies, this request has been blocked because the data transfer protocol "*<protocol type>*" is not allowed.）
ERR_PROXY_AUTH_REQUIRED プロキシ認可が必要（Proxy Authorization Required）	続行するために認証クレデンシャルを入力する必要がある場合に表示される通知ページ。これは明示的なトランザクション要求に使用されます。	このシステムを使用してインターネットにアクセスするには、認証が必要です。（Authentication is required to access the Internet using this system.）プロンプトに従って有効なユーザ ID とパスフレーズを入力してください。（A valid user ID and passphrase must be entered when prompted.）
ERR_PROXY_PREVENT_MULTIPLE_LOGIN 別のマシンからログイン済み（Already Logged In From Another Machine）	別のマシンの Web プロキシですでに認証されているユーザ名と同じユーザ名を使用して Web へのアクセスが試みられた場合に表示されるブロック ページ。これは、[ユーザ セッション制限（User Session Restrictions）] グローバル認証オプションがイネーブルの場合に使用されます。	このユーザ ID には別の IP アドレスからのアクティブ セッションが存在するため、組織のポリシーに基づき、インターネットへのアクセス要求が拒否されました。（Based on your organization's policies, the request to access the Internet was denied because this user ID has an active session from another IP address.） 別のユーザとしてログインする場合は、下のボタンをクリックして、別のユーザ名とパスフレーズを入力してください。（If you want to login as a different user, click on the button below and enter a different a user name and passphrase.）
ERR_PROXY_REDIRECT リダイレクト（Redirect）	リダイレクション ページ。	この要求は、リダイレクトされます。（This request is being redirected.）このページが自動的にリダイレクトされない場合は、ここをクリックして続行してください。（If this page does not automatically redirect, click here to proceed.）

ファイル名および通知タイトル	通知の説明	通知テキスト
ERR_PROXY_UNACKNOWLEDGED ポリシーの確認（Policy Acknowledgment）	エンドユーザ確認ページ 詳細については、エンドユーザ通知ページ (9-6 ページ) を参照してください。	インターネットにアクセスする前に、以下のステートメントを確認してください。（Please acknowledge the following statements before accessing the Internet.） 危険なコンテンツを検出して組織のポリシーを適用するために、Web トランザクションは自動的にモニタされ処理されます。（Your web transactions will be automatically monitored and processed to detect dangerous content and to enforce organization's policies.）下記のリンクをクリックすると、モニタリングに同意し、訪問したサイトに関するデータが記録される可能性について承認したものと見なされます。（By clicking the link below, you acknowledge this monitoring and accept that data about the sites you visit may be recorded.）モニタリング システムの存在について、定期的に承認を求められます。（You will be periodically asked to acknowledge the presence of the monitoring system.）ユーザには、インターネット アクセスに関する組織のポリシーに従う責任があります。（You are responsible for following organization's polices on Internet access.） このステートメントに同意してインターネットにアクセスするには、ここをクリックしてください。（Click here to accept this statement and access the Internet.）
ERR_PROXY_UNLICENSED プロキシのライセンスなし（Proxy Not Licensed）	Web Security Appliance Web プロキシの有効なライセンス キーがない場合に表示されるブロック ページ。	セキュリティ デバイスの適切なライセンスがないため、インターネットにアクセスできません。（Internet access is not available without proper licensing of the security device.） <担当者名> <電子メール アドレス> に連絡し、以下に示すコードを提出してください。（Please contact <*contact name*> <*email address*> and provide the code shown below.） **（注）** セキュリティ デバイスの管理インターフェイスにアクセスするには、ポートに設定されている IP アドレスを入力します。

ファイル名および通知タイトル	通知の説明	通知テキスト
ERR_RANGE_NOT_SATISFIABLE 範囲が不適切（Range Not Satisfiable）	Web サーバが要求されたバイト範囲に対応できない場合に表示されるエラー ページ。	システムはこの要求を処理できません。（The system cannot process this request.）非標準のブラウザによって無効な HTTP 要求が生成された可能性があります。（A non-standard browser may have generated an invalid HTTP request.） 標準ブラウザを使用している場合は、要求を再試行してください。（If you are using a standard browser, please retry the request.）
ERR_REDIRECT_PERMANENT 永続的リダイレクト（Redirect Permanent）	内部リダイレクション ページ。	ページ <URL> は <リダイレクト先 URL> にリダイレクトされます。（The page <*URL*> is being redirected to <*redirected URL*>.）
ERR_REDIRECT_REPEAT_REQUEST リダイレクト	内部リダイレクション ページ。	要求を繰り返してください。（Please repeat your request.）
ERR_SAAS_AUTHENTICATION ポリシー:アクセス拒否（Policy: Access Denied）	続行するために認証クレデンシャルを入力する必要がある場合に表示される通知ページ。これはアプリケーションへのアクセスに使用されます。	組織のポリシーに基づき、<URL> へのアクセス要求は、ログイン クレデンシャルの入力が必要なページにリダイレクトされました。（Based on your organization's policy, the request to access <*URL*> was redirected to a page where you must enter the login credentials.）認証に成功し、適切な権限が付与されている場合は、アプリケーションへのアクセスが許可されます。（You will be allowed to access the application if authentication succeeds and you have the proper privileges.）
ERR_SAAS_AUTHORIZATION ポリシー:アクセス拒否（Policy: Access Denied）	ユーザがアクセス権限のないアプリケーションにアクセスを試みた場合に表示されるブロック ページ。	承認されたユーザではないため、組織のポリシーに基づき、アプリケーション <URL> へのアクセスがブロックされました。（Based on your organization's policy, the access to the application <*URL*> is blocked because you are not an authorized user.）別のユーザとしてログインする場合は、このアプリケーションへのアクセスを認可されているユーザのユーザ名とパスフレーズを入力してください。（If you want to login as a different user, enter a different username and passphrase for a user that is authorized to access this application.）
ERR_SAML_PROCESSING ポリシー:アクセス拒否（Policy: Access Denied）	アプリケーションにアクセスするためのシングル サインオン URL の処理に内部プロセスが失敗した場合に表示されるエラー ページ。	シングル サインオン要求の処理中にエラーが検出されたため、<ユーザ名> へのアクセス要求が完了しませんでした。（The request to access <*user name*> did not go through because errors were found during the process of the single sign on request.）

ファイル名および通知タイトル	通知の説明	通知テキスト
ERR_SERVER_NAME_EXPANSION サーバ名の拡張（Server Name Expansion）	自動的に URL を展開し、その更新した URL にユーザをリダイレクトする内部リダイレクション ページ。	サーバ名 <ホスト名> は省略形と見なされ、<リダイレクト先 URL> にリダイレクトされます。（The server name <*hostname*> appears to be an abbreviation, and is being redirected to <*redirected URL*>.）
ERR_URI_TOO_LONG URI が長すぎる（URI Too Long）	URL が長すぎる場合に表示されるブロック ページ。	要求された URL が長すぎるため、処理できませんでした。（The requested URL was too long and could not be processed.）これはネットワークへの攻撃を示している可能性があります。（This may represent an attack on your network.） <担当者名> <電子メール アドレス> に連絡し、以下に示すコードを提出してください。（Please contact <*contact name*> <*email address*> and provide the code shown below.）
ERR_WBRS セキュリティ：マルウェアのリスク（Security: Malware Risk）	Web レピュテーション スコアが低いため、Web レピュテーション フィルタによってサイトがブロックされた場合に表示されるブロック ページ。	この Web サイト <URL> は、Web レピュテーション フィルタによって、コンピュータまたは組織のネットワークに対するセキュリティ上の脅威であると判定されたため、組織のアクセス ポリシーに基づいてブロックされました。（Based on your organization's access policies, this web site <*URL*> has been blocked because it has been determined by Web Reputation Filters to be a security threat to your computer or the organization's network.）この Web サイトは、マルウェア/スパイウェアと関連付けられています。（This web site has been associated with malware/spyware.） 脅威のタイプ（Threat Type）：%o 脅威の理由（Threat Reason）：%O
ERR_WEBCAT ポリシー：URL フィルタリング（Policy: URL Filtering）	ブロックされた URL カテゴリの Web サイトにユーザがアクセスを試みた場合に表示されるブロック ページ。	Web カテゴリ「<カテゴリ タイプ>」は許可されていないため、組織のアクセス ポリシーに基づき、この Web サイト <URL> へのアクセスはブロックされました。（Based on your organization's Access Policies, access to this web site <*URL*> has been blocked because the web category “<*category type*>” is not allowed.）
ERR_WWW_AUTH_REQUIRED WWW 認可が必要（WWW Authorization Required）	要求されたサーバが続行するために認証クレデンシャルの入力を必要とする場合に表示される通知ページ。	要求した Web サイト <ホスト名> にアクセスするには認証が必要です。（Authentication is required to access the requested web site <*hostname*>.）プロンプトに従って有効なユーザ ID とパスフレーズを入力してください。（A valid user ID and passphrase must be entered when prompted.）

CHAPTER 10

Web セキュリティ アプライアンスのレポート

[概要（Overview）] ページ

ログインまたは [ホーム（Home）] ボタンのクリックで表示される [システム ステータス（System Status）] ページには、アプライアンス ステータス、クラウド コミュニケーション ステータス、および設定情報の「スナップショット」が表示されます。

[システム容量（System Capacity）] ページ

[レポート（Reporting）] > [システム容量（System Capacity）] ページには、Web セキュリティ アプライアンスのリソース使用率に関する現在および履歴情報が表示されます。

[システム容量（System Capacity）] ページにデータを表示する時間範囲を選択する場合、以下のことに留意することが重要です。

- **Hour レポート。**Hour レポートは、分テーブルに照会して、60 分間を超える分単位で、1 分間にアプライアンスに記録されたアイテム（バイトや接続など）の正確な数を表示します。
- **Day レポート。**Day レポートは、時間テーブルに照会して、24 分間を超える時間単位で、1 時間にアプライアンスに記録されたアイテム（バイトや接続など）の正確な数を表示します。この情報は時間テーブルから収集されます。

Week レポートおよび 30 Days レポートは、Hour レポートおよび Day レポートと同じように動作します。

[システム ステータス（System Status）] ページ

システム ステータスをモニタするには、[レポート（Reporting）] > [システム ステータス（System Status）] ページを使用します。このページは、Web セキュリティ アプライアンスの現在のステータスと設定を表示します。

セクション	表示内容
Web セキュリティ アプライアンスのステータス（Web Security Appliance Status）	• システムの動作期間 • システム リソースの使用率：レポーティングおよびロギングに使用される CPU 使用率、RAM 使用率、およびディスク領域の使用率。 このページに表示される CPU 使用率値はさまざまな瞬間に個別に読み取られるため、システムの [概要（Overview）] ページ（[概要（Overview）] ページ（10-1 ページ））に表示される CPU 値と若干異なる場合があります。 システムによって使用されない RAM は Web オブジェクト キャッシュによって使用されるので、効率的に動作する RAM 使用率は 90 % を超える場合があります。システムで重大なパフォーマンス問題が発生していない場合で、この値が 100 % に固定されない場合、システムは正常に動作しています。 （注）　プロキシバッファ メモリは、この RAM を使用する 1 つのコンポーネントです。
プロキシ トラフィックの特性（Proxy Traffic Characteristics）	• 1 秒あたりのトランザクション • 帯域幅 • 応答時間 • キャッシュ ヒット率 • 接続
高可用性	
外部サービス（External Services）	• Identity Services Engine
現在の設定（Current Configuration）	Web プロキシ設定： • Web プロキシのステータス：イネーブルまたはディセーブル。 • 展開トポロジ • Web プロキシ モード：フォワードまたは透過。 L4 トラフィック モニタ設定： • L4 トラフィック モニタのステータス：イネーブルまたはディセーブル。 • L4 トラフィック モニタの配線。 • L4 トラフィック モニタのアクション：モニタまたはブロック。 Web セキュリティ アプライアンスのバージョン情報 ハードウェア情報

関連項目

- [システム容量（System Capacity）] ページ（10-1 ページ）

ログによるシステム アクティビティのモニタ

ログ の概要

Web Security Appliance では、システムとトラフィックの管理アクティビティの記録がログファイル上に書き込まれます。管理者はこれらのログ ファイルを参照して、アプライアンスをモニタし、トラブルシューティングできます。

各種アクティビティはいくつかのロギング タイプごとに記録されるため、特定のアクティビティに関する情報の検索が容易です。多くのロギング タイプはデフォルトでイネーブルなりますが、いくつかは、必要に応じて手動でイネーブルにする必要があります。

ログ ファイルをイネーブルにして管理するには、ログ ファイル サブスクリプションを設定します。サブスクリプションにより、ログ ファイルの作成、カスタマイズ、および管理に関する設定を定義できます。

通常、管理者が主に使用するログ ファイルは、以下の 2 種類です。

- **アクセス ログ。**すべての Web プロキシ フィルタリングとスキャン アクティビティが記録されます。
- **トラフィック モニタ ログ。**すべての L4 トラフィック モニタ アクティビティが記録されます。

これらのログ タイプおよびその他のログ タイプを使用して、アプライアンスの現在と過去のアクティビティを確認できます。ログ ファイル エントリの内容を理解できるように、リファレンス テーブルが用意されています。

関連項目

- ログの共通タスク（11-2 ページ）
- ログ ファイルのタイプ（11-3 ページ）

ログの共通タスク

タスク	関連項目および手順へのリンク
ログを使用して Web プロキシの問題をトラブルシューティングする	ログによる Web プロキシのトラブルシューティング（11-2 ページ）
ログ サブスクリプションを追加および編集する	ログ サブスクリプションの追加と編集（11-8 ページ）
ログ ファイルを表示する	ログ ファイルの表示（11-15 ページ）
ログ ファイルを解釈する	アクセス ログのスキャン判定エントリの解釈（11-23 ページ）
ログ ファイルをカスタマイズする	アクセス ログのカスタマイズ（11-30 ページ）
別のサーバにログ ファイルをプッシュする	別のサーバへのログ ファイルのプッシュ（11-13 ページ）
ログ ファイルをアーカイブする	ログ ファイルのアーカイブ（11-13 ページ）

ログのベスト プラクティス

- ログ サブスクリプションの数を最小限にすると、システム パフォーマンスが向上します。
- 記録する詳細を少なくすると、システム パフォーマンスが向上します。

ログによる Web プロキシのトラブルシューティング

Web Security Appliance では、デフォルトで、Web プロキシ ロギング メッセージ用の 1 つのログ サブスクリプションが作成されます（「デフォルト プロキシ ログ」と呼ばれます）このログには、すべての Web プロキシ モジュールに関する基本的な情報が記録されます。アプライアンスには、各 Web プロキシ モジュールのログ ファイル タイプも含まれているので、デフォルト プロキシ ログを画面いっぱいに散乱させることなく、各モジュールのより詳細なデバッグ情報を読み取ることができます。

使用可能な各種のログを使用して Web プロキシの問題をトラブルシューティングするには、以下の手順に従います。

ステップ 1　デフォルト プロキシ ログを読みます。

ステップ 2　問題を解決するためにより詳細な情報が必要な場合は、その問題に関連する特定の Web プロキシ モジュールのログ サブスクリプションを作成します。以下の Web プロキシ モジュール ログ タイプのサブスクリプションを作成できます。

アクセス コントロール エンジン ログ
AVC エンジン フレームワーク ログ
設定ログ
接続管理ログ
データ セキュリティ モジュール ログ
DCA エンジン フレームワーク ログ
ディスク マネージャ ログ
FireAMP
FTP プロキシ ログ
HTTPS ログ
ハイブリッド サービス ログ
ライセンス モジュール ログ
ロギング フレームワーク ログ
McAfee 統合フレームワーク ログ
メモリ マネージャ ログ
その他のプロキシ モジュール ログ
リクエスト デバッグ ログ
SNMP モジュール ログ
Sophos 統合フレームワーク ログ
WBRS フレームワーク ログ
WCCP モジュール ログ
Webcat 統合フレームワーク ログ
Webroot 統合フレームワーク ログ

ステップ 3　問題を再現して、その問題に関する新しい Web プロキシ モジュール ログを確認します。

ステップ 4　必要に応じて、他の Web プロキシ モジュール ログを使用して繰り返します。

ステップ 5　不要になったサブスクリプションを削除します。

関連項目

- ログ ファイルのタイプ（11-3 ページ）
- ログ サブスクリプションの追加と編集（11-8 ページ）

ログ ファイルのタイプ

Web プロキシ コンポーネントに関するいくつかのログ タイプはイネーブルになっていません。「デフォルト プロキシ ログ」と呼ばれるメインの Web プロキシ ログ タイプはデフォルトでイネーブルになっており、すべての Web プロキシ モジュールの基本的な情報が記録されます。各 Web プロキシ モジュールには、必要に応じてイネーブルにできる独自のログ タイプがあります。

以下の表は、Web Security Appliance のログ ファイル タイプを示しています。

ログ ファイル タイプ	説明	syslog プッシュのサポート	デフォルトのイネーブル設定
アクセス コントロール エンジン ログ	Web プロキシ ACL（アクセス コントロール リスト）の評価エンジンに関連するメッセージを記録します。	なし	なし

ログ ファイル タイプ	説明	syslog プッシュのサポート	デフォルトのイネーブル設定
AMP エンジン ログ	ファイル レピュテーション スキャンとファイル分析に関する情報（高度なマルウェア防御）を記録します。 Log Files, page 14-17 も参照してください。	あり	あり
監査ログ	認証、許可、アカウンティングのイベント（AAA: Authentication、Authorization、および Accounting）を記録します。アプリケーションおよびコマンドライン インターフェイスにおけるすべてのユーザ操作を記録し、変更内容を保存します。	あり	あり
アクセス ログ	Web プロキシのクライアント履歴を記録します。	あり	あり
認証フレームワーク ログ	認証履歴とメッセージを記録します。	なし	あり
AVC エンジン フレームワーク ログ	Web プロキシと AVC エンジン間の通信に関連するメッセージを記録します。	なし	なし
AVC エンジン ログ	AVC エンジンからのデバッグ メッセージを記録します。	あり	あり
CLI 監査ログ	コマンドライン インターフェイス アクティビティの監査履歴を記録します。	あり	あり
設定ログ	Web プロキシ コンフィギュレーション管理システムに関連するメッセージを記録します。	なし	なし
接続管理ログ	Web プロキシ接続管理システムに関連するメッセージを記録します。	なし	なし
データ セキュリティ ログ	Cisco データ セキュリティ フィルタで評価されたアップロード要求のクライアント履歴を記録します。	あり	あり
データ セキュリティ モジュール ログ	Cisco データ セキュリティ フィルタに関するメッセージを記録します。	なし	なし
DCA エンジン フレームワーク ログ（動的コンテンツ分析）	Web プロキシと Cisco Web Usage Controls 動的コンテンツ分析エンジン間の通信に関連するメッセージを記録します。	なし	なし
DCA エンジン ログ（動的コンテンツ分析）	Cisco Web Usage Controls 動的コンテンツ分析エンジンに関連するメッセージを記録します。	あり	あり

ログ ファイル タイプ	説明	syslog プッシュのサポート	デフォルトのイネーブル設定
デフォルト プロキシ ログ	Web プロキシに関連するエラーを記録します。 これは、Web プロキシに関連するすべてのログの最も基本的なものです。Web プロキシに関連するより具体的な分野のトラブルシューティングを行うには、該当する Web プロキシ モジュールのログ サブスクリプションを作成します。	あり	あり
ディスク マネージャ ログ	ディスク上のキャッシュの書き込みに関連する Web プロキシ メッセージを記録します。	なし	なし
外部認証ログ	外部認証サーバによる通信の成功または失敗など、外部認証機能の使用に関連するメッセージを記録します。 外部認証がディセーブルされている場合でも、このログにはローカル ユーザのログインの成功または失敗に関するメッセージが記録されています。	なし	あり
フィードバック ログ	誤って分類されたページをレポートする Web ユーザを記録します。	あり	あり
FTP プロキシ ログ	FTP プロキシに関連するエラーおよび警告メッセージを記録します。	なし	なし
FTP サーバ ログ	FTP を使用して、Web Security Appliance にアップロードされ、ダウンロードされるすべてのファイルを記録します。	あり	あり
GUI ログ (グラフィカル ユーザ インターフェイス)	Web インターフェイスのページ更新履歴を記録します。GUI ログには、SMTP トランザクションに関する情報も記録されます。たとえば、アプライアンスから電子メールで送信されるスケジュール済みレポートに関する情報などが記録されます。	あり	あり
Haystack ログ	Haystack ログには、データ処理をトラッキングする Web トランザクションが記録されます。	あり	あり
ハイブリッド サービス ログ	アプライアンスと ScanCenter ポータル間の通信と、ハイブリッド登録、アップデート、およびアップデート サーバに関するすべての通信を記録します。	なし	あり
HTTPS ログ	HTTPS プロキシ固有の Web プロキシ メッセージを記録します(HTTPS プロキシがイネーブルの場合)。	なし	なし
ISE サーバ ログ	ISE サーバの接続および動作情報を記録します。	あり	あり
ライセンス モジュール ログ	Web プロキシのライセンスおよび機能キー処理システムに関するメッセージを記録します。	なし	なし
ロギング フレームワーク ログ	Web プロキシのロギング システムに関するメッセージを記録します。	なし	なし

ログ ファイル タイプ	説明	syslog プッシュのサポート	デフォルトのイネーブル設定
ロギング ログ	ログ管理に関連するエラーを記録します。	あり	あり
McAfee 統合フレームワーク ログ	Web プロキシと McAfee スキャン エンジン間の通信に関連するメッセージを記録します。	なし	なし
McAfee ログ	McAfee スキャン エンジンからアンチマルウェア スキャン アクティビティのステータスを記録します。	あり	あり
メモリ マネージャ ログ	Web プロキシ プロセスのメモリ内キャッシュを含むすべてのメモリの管理に関連する Web プロキシ メッセージを記録します。	なし	なし
その他のプロキシ モジュール ログ	主に開発者やカスタマー サポートによって使用される Web プロキシ メッセージを記録します。	なし	なし
AnyConnect セキュア モビリティ デーモン ログ	ステータス チェックなど、Web セキュリティ アプライアンスと AnyConnect クライアント間の相互作用を記録します。	あり	あり
NTP ログ (ネットワーク タイム プロトコル)	ネットワーク タイム プロトコルによって作成されたシステム時刻に変更します。	あり	あり
PAC ファイル ホスティング デーモン ログ	クライアントによるプロキシ自動設定(PAC)ファイルの使用状況を記録します。	あり	あり
プロキシ バイパス ログ	Web プロキシをバイパスするトランザクションを記録します。	なし	あり
レポーティング ログ	レポート生成履歴を記録します。	あり	あり
レポーティング クエリー ログ	レポート生成に関連するエラーを記録します。	あり	あり
リクエスト デバッグ ログ	すべての Web プロキシ モジュール ログ タイプから、特定の HTTP トランザクションに関する非常に詳細なデバッグ情報を記録します。他のすべてのプロキシ ログ サブスクリプションを作成することなく、特定のトランザクションによるプロキシ問題のトラブルシューティングを行うために、このログ サブスクリプションを作成する場合があります。 **注:** CLI でのみ、このログ サブスクリプションを作成できます。	なし	なし
認証ログ	アクセス コントロール機能に関するメッセージを記録します。	あり	あり
SHD ログ (システム ヘルス デーモン)	システム サービスの動作状態の履歴および予期しないデーモンの再起動の履歴を記録します。	あり	あり

ログ ファイル タイプ	説明	syslog プッシュのサポート	デフォルトのイネーブル設定
SNMP ログ	SNMP 管理エンジンに関連するデバッグ メッセージを記録します。	あり	あり
SNMP モジュール ログ	SNMP モニタリング システムとの対話に関連する Web プロキシ メッセージを記録します。	なし	なし
Sophos 統合フレームワーク ログ	Web プロキシと Sophos スキャン エンジン間の通信に関連するメッセージを記録します。	なし	なし
Sophos ログ	Sophos スキャン エンジンからアンチマルウェア スキャン アクティビティのステータスを記録します。	あり	あり
ステータス ログ	機能キーのダウンロードなど、システムに関連する情報を記録します。	あり	あり
システム ログ	DNS、エラー、およびコミット アクティビティを記録します。	あり	あり
トラフィック モニタリング エラー ログ	L4TM インターフェイスおよびキャプチャ エラーを記録します。	あり	あり
トラフィック モニタ ログ	L4TM ブロックおよび許可リストに追加されたサイトを記録します。	なし	あり
UDS ログ (ユーザ検出サービス)	Web プロキシが実際の認証を行わずにユーザ名を検出する方法に関するデータを記録します。Secure Mobility 用の Cisco 適応型セキュリティ アプライアンスとの対話、および透過的ユーザ ID 用の Novell eDirectory サーバとの統合に関する情報が含まれます。	あり	あり
アップデータ ログ	WBRS およびその他の更新の履歴を記録します。	あり	あり
W3C ログ	W3C 準拠の形式で Web プロキシ クライアント履歴を記録します。 詳細については、W3C 準拠のアクセス ログ ファイル(11-28 ページ)を参照してください。	あり	なし
WBNP ログ (SensorBase ネットワーク参加)	SensorBase ネットワークへの Cisco SensorBase ネットワーク参加のアップロード履歴を記録します。	なし	あり
WBRS フレームワーク ログ (Web レピュテーション スコア)	Web プロキシと Web レピュテーション フィルタ間の通信に関連するメッセージを記録します。	なし	なし
WCCP モジュール ログ	WCCP の実装に関連する Web プロキシ メッセージを記録します。	なし	なし
Webcat 統合フレームワーク ログ	Web プロキシと Cisco Web Usage Controls に関連付けられた URL フィルタリング エンジン間の通信に関連するメッセージを記録します。	なし	なし

ログ ファイル タイプ	説明	syslog プッシュのサポート	デフォルトのイネーブル設定
Webroot 統合フレームワーク ログ	Web プロキシと Webroot スキャン エンジン間の通信に関連するメッセージを記録します。	なし	なし
Webroot ログ	Webroot スキャン エンジンからアンチマルウェア スキャン アクティビティのステータスを記録します。	あり	あり
ウェルカム ページ確認ログ	エンド ユーザの確認ページで [同意する（Accept）] ボタンをクリックする Web クライアントの履歴を記録します。	あり	あり

ログ サブスクリプションの追加と編集

ログ ファイルのタイプごとに複数のログ サブスクリプションを作成できます。サブスクリプションには、以下のようなアーカイブおよびストレージに関する設定の詳細が含まれています。

- ロールオーバー設定。ログ ファイルをアーカイブするタイミングを決定します。
- アーカイブ ログの圧縮設定。
- アーカイブ ログの取得の設定。ログをリモート サーバに保存するか、アプライアンスに保存するかを指定します。

ステップ 1　[システム管理（System Administration）] > [ログ サブスクリプション（Log Subscriptions）] を選択します。

ステップ 2　ログ サブスクリプションを追加するには、[ログ設定を追加（Add Log Subscription）] をクリックします。あるいは、ログ サブスクリプションを編集するには、[ログ名（Log Name）] フィールドのログ ファイルの名前をクリックします。

ステップ 3　サブスクリプションを設定します。

オプション	説明
ログ タイプ（Log Type）	ユーザが登録できる使用可能なログ ファイル タイプのリスト。このページの他のオプションは、選択したログ ファイル タイプによって異なります。 **（注）**　[リクエスト デバッグ ログ（Request Debug Logs）] タイプは CLI を使用してのみ登録でき、このリストには表示されません。
ログ名（Log Name）	Web Security Appliance でサブスクリプションの参照に使用される名前。この名前は、サブスクリプションのログ ファイルを保存するログ ディレクトリにも使用されます。
ファイルサイズ別ロールオーバー（Rollover by File Size）	ログ ファイルの最大ファイル サイズ。このサイズを超えるとそのファイルがアーカイブされ、新しいログ ファイルが作成されます。100 キロバイトから 10 ギガバイトまでの数値を入力してください。

オプション	説明
時刻によりロールオーバー（Rollover by Time）	ログ ファイルの最大記録時間。この時間を超えるとそのファイルがアーカイブされ、新しいファイルが作成されます。設定可能なオプションは、以下のとおりです。 • [なし（None）]。AsyncOS は、ログ ファイルが最大ファイル サイズに達した場合にのみロールオーバーを実行します。 • [カスタム時間間隔（Custom Time Interval）]。AsyncOS は、以前のロールオーバーから指定された時間が経過した後にロールオーバーを実行します。末尾に d、h、m、s を追加して、ロールオーバー間の日数、時間、分、秒を指定します。 • [日次ロールオーバー（Daily Rollover）]。AsyncOS は、毎日指定された時刻にロールオーバーを実行します。1 日に複数の時刻を設定するには、カンマを使用して区切ります。1 時間ごとにロールオーバーを実行するように指定するには、時間にアスタリスク（*）を使用します。また、1 分ごとにロールオーバーするためにアスタリスクを使用することもできます。 • [週次ロールオーバー（Weekly Rollover）]。AsyncOS は、1 つ以上の曜日の指定された時刻にロールオーバーを実行します。
ログ スタイル（Log Style） （アクセス ログ）	使用するログ形式（[Squid]、[Apache]、または [Squid の詳細（Squid Details）] のいずれか）を選択します。

カスタム フィールド（Custom Fields）
（アクセス ログ）
	各アクセス ログ エントリにカスタム情報を含めることができます。
	[カスタム フィールド（Custom Fields）] にフォーマット指定子を入力する構文は以下のとおりです。
	`<format_specifier_1> <format_specifier_2> ...`
	例：`%a %b %E`
	フォーマット指定子の前にトークンを追加して、アクセス ログ ファイルの説明テキストを表示できます。次に例を示します。
	`client_IP %a body_bytes %b error_type %E`
	この場合、`client_IP` はログ フォーマット指定子 `%a` の説明トークンです（以下同様）。

ファイル名（File Name）	ログ ファイルの名前。最新のログ ファイルには拡張子 .c が付き、ロール オーバー済みのログには、ファイル作成時のタイムスタンプと拡張子 .s が付きます。

オプション	説明
ログ フィールド（Log Fields） （W3C アクセス ログ）	W3C アクセス ログに含めるフィールドを選択できます。 [使用可能フィールド（Available Fields）] リストでフィールドを選択するか、[カスタム フィールド（Custom Field）] ボックスにフィールドを入力し、[追加（Add）] をクリックします。 [選択されたログ フィールド（Selected Log Fields）] リストに表示されるフィールドの順序によって、W3C アクセス ログ ファイルのフィールドの順序が決まります。[上へ移動（Move Up）] または [下へ移動（Move Down）] ボタンを使用してフィールドの順序を変更できます。[選択されたログ フィールド（Selected Log Fields）] リストでフィールドを選択し、[削除（Remove）] をクリックして、それを削除できます [カスタム フィールド（Custom Field）] ボックスに複数のユーザ定義フィールドを入力し、それらを同時に入力できます。ただし、[追加（Add）] をクリックする前に、各エントリが改行（Enter キーを押します）で区切られている必要があります。 W3C ログ サブスクリプションに含まれるログ フィールドを変更すると、ログ サブスクリプションは自動的にロール オーバーします。これにより、ログ ファイルの最新バージョンに適切な新しいフィールド ヘッダーを含めることができます。
ログ圧縮（Log Compression）	ロール オーバー ファイルを圧縮するかどうかを指定します。AsyncOS は gzip 圧縮形式を使用してログ ファイルを圧縮します。
ログ除外（Log Exclusions）（任意） （アクセス ログ）	HTTP ステータス コード（4xx または 5xx のみ）を指定して、関連するトランザクションをアクセス ログまたは W3C アクセス ログから除外します。 たとえば、401 を入力すると、そのトランザクション番号を持つ、認証に失敗した要求が除外されます。

オプション	説明
ログ レベル（Log Level）	ログ エントリの詳細のレベルを設定します。次から選択します。 • [クリティカル（Critical）]。エラーだけが記録されます。これは、最小限の設定であり、syslog レベルの [アラート（Alert）] と同等です。 • [警告（Warning）]。エラーと警告が記録されます。このログ レベルは、syslog レベルの [警告（Warning）] と同等です。 • [情報（Information）]。エラー、警告、および他のシステム操作が記録されます。これはデフォルトの詳細レベルであり、syslog レベルの [情報（Information）] と同等です。 • [デバッグ（Debug）]。システム問題のデバッグに役立つデータが記録されます。エラーの原因を調べるときは、Debug ログ レベルを使用します。この設定は一時的に使用し、後でデフォルト レベルに戻します。このログ レベルは、syslog レベルの [デバッグ（Debug）] と同等です。 • [トレース（Trace）]。これは、詳細レベルの最も高い設定です。このレベルには、システム操作とアクティビティの完全な記録が含まれます。Trace ログ レベルは、開発者にのみ推奨されます。このレベルを使用すると、システムのパフォーマンスが大きく低下するので、推奨されません。このログ レベルは、syslog レベルの [デバッグ（Debug）] と同等です。 **（注）** 詳細レベルの設定を高くするほど、作成されるログ ファイルが大きくなり、システム パフォーマンスに大きな影響を及ぼします。
取得方法（Retrieval Method）	ロール オーバー ログ ファイルを保存する場所と、閲覧用に取得する方法を指定します。利用可能な方法の説明については、下記を参照してください。
取得方法: アプライアンス上の FTP（FTP on Appliance）	[アプライアンス上の FTP（FTP on Appliance）] 方式（FTP ポーリングと同等）では、ログ ファイルを取得するために、管理者ユーザまたはオペレータ ユーザのユーザ名とパスフレーズを使用して、リモート FTP クライアントからアプライアンスにアクセスする必要があります。 この方法を選択した場合、アプライアンスに保存するログ ファイルの最大数を入力する必要があります。最大数に達すると、最も古いファイルが削除されます。 これは、デフォルトの取得方法です。
取得方法: リモート サーバでの FTP（FTP on Remote Server）	[リモート サーバでの FTP（FTP on Remote Server）] 方式（FTP プッシュと同等）では、リモート コンピュータ上の FTP サーバに定期的にログ ファイルをプッシュします。 この方法を選択した場合、以下の情報を入力する必要があります。 • FTP サーバのホスト名 • ログ ファイルを保存する FTP サーバのディレクトリ • FTP サーバに接続する権限を持つユーザのユーザ名とパスフレーズ **（注）** AsyncOS for Web は、リモート FTP サーバのパッシブ モードのみをサポートします。アクティブ モードの FTP サーバにログ ファイルをプッシュできません。

オプション	説明
取得方法: リモート サーバでの SCP（SCP on Remote Server）	[リモート サーバでの SCP（SCP on Remote Server）] 方式（SCP プッシュと同等）では、セキュア コピー プロトコルを使用して、リモート SCP サーバに定期的にログ ファイルをプッシュします。この方法には、SSH2 プロトコルを使用するリモート コンピュータ上の SSH SCP サーバが必要です。サブスクリプションには、ユーザ名、SSH キー、およびリモート コンピュータ上の宛先ディレクトリが必要です。ログ ファイルは、ユーザが設定したロールオーバー スケジュールに基づいて転送されます。 この方法を選択した場合、以下の情報を入力する必要があります。 • SCP サーバのホスト名 • ログ ファイルを保存する SCP サーバのディレクトリ • SCP サーバに接続する権限を持つユーザのユーザ名
取得方法: Syslog 送信（Syslog Push）	テキスト ベースのログの syslog のみを選択できます。 [Syslog 送信（Syslog Push）] 方式では、ポート 514 でリモート Syslog サーバにログ メッセージを送信します。この方法は、RFC 3164 に準拠しています。 この方法を選択した場合、以下の情報を入力する必要があります。 • Syslog サーバのホスト名 • 転送に使用するプロトコル（UDP または TCP） • 最大メッセージ サイズ（Maximum message size） UDP で有効な値は 1024 ～ 9216 です。 TCP で有効な値は 1024 ～ 65535 です。 最大メッセージ サイズは syslog サーバの設定に応じて異なります。 • ログで使用するファシリティ

ステップ 4　変更を送信し、保存します。

次の作業

- 取得方法として SCP を選択した場合は、アプライアンスによって SSH キーが表示されます。このキーを SCP サーバ ホストに追加します。別のサーバへのログ ファイルのプッシュ（11-13 ページ）を参照してください。

関連項目

- ログ ファイルのタイプ（11-3 ページ）
- ログのファイル名とアプライアンスのディレクトリ構造（11-14 ページ）

別のサーバへのログ ファイルのプッシュ

はじめる前に

- 必要なログ サブスクリプションを作成または編集し、取得方法として SCP を選択します。ログ サブスクリプションの追加と編集（11-8 ページ）

ステップ 1　リモート システムにキーを追加します。

a. CLI にアクセスします。

b. `logconfig -> hostkeyconfig` コマンドを入力します。

c. 以下のコマンドを使用してキーを表示します。

コマンド（Command）	説明
ホスト	システム ホスト キーを表示します。これは、リモート システムの「known_hosts」ファイルに記入される値です。
ユーザ（User）	リモート マシンにログをプッシュするシステム アカウントの公開キーを表示します。これは、SCP プッシュ サブスクリプションを設定するときに表示されるキーと同じです。これは、リモート システムの「authorized_keys」ファイルに記入される値です。

d. これらのキーをリモート システムに追加します。

ステップ 2　CLI で、リモート サーバの SSH 公開ホスト キーをアプライアンスに追加します。

コマンド（Command）	説明
新規作成（New）	新しいキーを追加します。
フィンガープリント（Fingerprint）	システム ホスト キーのフィンガープリントを表示します。

e. 変更を保存します。

ログ ファイルのアーカイブ

AsyncOS は、最新のログ ファイルがユーザ指定の上限（最大ファイル サイズまたは最大時間）に達すると、ログ サブスクリプションをアーカイブ（ロール オーバー）します。

ログ サブスクリプションには以下のアーカイブ設定が含まれます。

- ファイルサイズ別ロールオーバー（Rollover by File Size）
- 時刻によりロールオーバー
- ログ圧縮（Log Compression）
- 取得方法

また、ログ ファイルを手動でアーカイブ（ロールオーバー）することもできます。

ステップ 1　[システム管理（System Administration）] > [ログ サブスクリプション（Log Subscriptions）] を選択します。

ステップ 2　アーカイブするログ サブスクリプションの [ロールオーバー（Rollover）] 列のチェックボックスをオンにするか、[すべて（All）] をオンにしてすべてのサブスクリプションを選択します。

ステップ 3　[今すぐロールオーバー（Rollover Now）] をクリックして、選択したログをアーカイブします。

関連項目

- ログ サブスクリプションの追加と編集（11-8 ページ）
- ログのファイル名とアプライアンスのディレクトリ構造（11-14 ページ）

ログのファイル名とアプライアンスのディレクトリ構造

アプライアンスは、ログ サブスクリプション名に基づいてログ サブスクリプションごとにディレクトリを作成します。ディレクトリ内のログ ファイル名は、以下の情報で構成されます。

- ログ サブスクリプションで指定されたログ ファイル名
- ログ ファイルが開始された時点のタイムスタンプ
- `.c`（「current（現在）」を表す）、または `.s`（「saved（保存済み）」を表す）のいずれかを示す単一文字ステータス コード

ログのファイル名は、以下の形式で作成されます。

```
/LogSubscriptionName/LogFilename.@timestamp.statuscode
```

（注）　保存済みのステータスのログ ファイルのみを転送する必要があります。

ログ ファイルの閲覧と解釈

Web Security Appliance をモニタしてトラブルシューティングする手段として、現在のログ ファイルのアクティビティを確認できます。これを行うには、アプライアンスのインターフェイスを使用します。

また、過去のアクティビティの記録についてアーカイブ ファイルを閲覧することもできます。アーカイブ ファイルがアプライアンスに保存されている場合は、アプライアンスのインターフェイスから閲覧できます。それ以外の場合は、適切な方法で外部ストレージの場所から読み取る必要があります。

ログ ファイルの各情報項目は、フィールド変数によって示されます。どのフィールドがどの情報項目を表しているのかを判別することにより、フィールドの機能を調べて、ログ ファイルの内容を解釈できます。W3C 準拠のアクセス ログの場合は、ファイル ヘッダーに、ログに表示される順でフィールド名がリストされます。しかし、標準のアクセス ログの場合は、このログ タイプに関するドキュメントを参照して、フィールドの順序について調べる必要があります。

関連項目

- ログ ファイルの表示（11-15 ページ）。
- アクセス ログ ファイル内の Web プロキシ情報（11-15 ページ）。
- W3C アクセス ログの解釈（11-28 ページ）。
- トラフィック モニタ ログの解釈（11-34 ページ）。
- ログ ファイルのフィールドとタグ（11-34 ページ）。

ログ ファイルの表示

はじめる前に

- ここでは、アプライアンス上に保存されているログ ファイルの表示方法について説明します。外部に格納されているファイルの表示方法については、このマニュアルでは説明しません。

ステップ 1　[システム管理（System Administration）] > [ログ サブスクリプション（Log Subscriptions）] を選択します。

ステップ 2　ログ サブスクリプション リストの [ログ ファイル（Log Files）] 列にあるログ サブスクリプション名をクリックします。

ステップ 3　プロンプトが表示されたら、アプライアンスにアクセスするための管理者のユーザ名とパスフレーズを入力します。

ステップ 4　ログ インしたら、ログ ファイルのいずれかをクリックして、ブラウザで表示するか、またはディスクに保存します。

ステップ 5　最新の結果を表示するには、ブラウザの表示を更新します。

（注）　ログ サブスクリプションが圧縮されている場合は、ダウンロードし、復元してから開きます。

関連項目

- アクセス ログ ファイル内の Web プロキシ情報（11-15 ページ）。
- W3C アクセス ログの解釈（11-28 ページ）。
- トラフィック モニタ ログの解釈（11-34 ページ）。

アクセス ログ ファイル内の Web プロキシ情報

アクセス ログ ファイルには、すべての Web プロキシ フィルタリングとスキャン アクティビティに関する記述が含まれています。アクセス ログ ファイル エントリは、アプライアンスが各トランザクションを処理した方法を表示します。

アクセス ログには 2 つの形式（標準および W3C 準拠）があります。W3C 準拠のログ ファイルは、標準のアクセス ログよりも記録内容とレイアウトをさらにカスタマイズできます。

以下のテキストは、1 つのトランザクションに対するアクセス ログ ファイル エントリの例を示します。

```
1278096903.150 97 172.xx.xx.xx TCP_MISS/200 8187 GET http://my.site.com/ -
DIRECT/my.site.com text/plain
DEFAULT_CASE_11-PolicyGroupName-Identity-OutboundMalwareScanningPolicy-DataSecurityPolic
y-ExternalDLPPolicy-RoutingPolicy
<IW_comp,6.9,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-","-",-,-,IW_comp,-,"-","-","Unknown","Un
known","-","-",198.34,0,-,[Local],"-",37,"W32.CiscoTestVector",33,0,"WSA-INFECTED-FILE.p
df","fd5ef49d4213e05f448f11ed9c98253d85829614fba368a421d14e64c426da5e"> -
```

フォーマット指定子	フィールド値	フィールドの説明
%t	1278096903.150	UNIX エポック以降のタイムスタンプ。
%e	97	経過時間（遅延）（ミリ秒単位）。
%a	172.xx.xx.xx	クライアント IP アドレス。 **注：**advancedproxyconfig > authentication CLI コマンドを使用して、アクセス ログの IP アドレスをマスクするように選択できます。
%w	TCP_MISS	トランザクション結果コード。 詳細については、W3C 準拠のアクセス ログ ファイル（11-28 ページ）を参照してください。
%h	200	HTTP 応答コード。
%s	8187	応答サイズ（ヘッダー + 本文）。
%2r	GET http://my.site.com/	要求の先頭行。 **注：**要求の先頭行がネイティブ FTP トランザクション用の場合、ファイル名の一部の特殊文字はアクセス ログでは符号化された URL を表します。たとえば、「@」記号は、アクセス ログに「%40」として書き込まれます。 以下の文字が符号化された URL に使用されます。 & # % + , : ; = @ ^ { } [ ]
%A	-	認証されたユーザ名。 **注：**advancedproxyconfig > authentication CLI コマンドを使用して、アクセス ログのユーザ名をマスクするように選択できます。
%H	DIRECT	要求コンテンツを取得するために接続されたサーバを説明するコード。 最も一般的な値は以下のとおりです。 • **NONE。**Web プロキシにコンテンツが含まれていたので、コンテンツを取得するために他のサーバに接続されませんでした。 • **DIRECT。**Web プロキシは、コンテンツを取得するための要求で指定されたサーバに移行しました。 • **DEFAULT_PARENT。**Web プロキシは、コンテンツを取得するためにプライマリ ペアレント プロキシまたは外部 DLP サーバに移行しました。

フォーマット指定子	フィールド値	フィールドの説明
%d	`my.site.com`	データ ソースまたはサーバの IP アドレス。
%c	`text/plain`	応答本文の MIME タイプ。
%D	`DEFAULT_CASE_11`	ACL デシジョン タグ。 **注:** ACL デシジョン タグの末尾に、Web プロキシが内部的に使用する動的に生成された数値が含まれます。この数値は無視できます。 詳細については、ACL デシジョン タグ（11-19 ページ）を参照してください。
N/A（ACL デシジョン タグの一部）	`PolicyGroupName`	このトランザクションについて最終決定を行うポリシー グループの名前（アクセス ポリシー、復号化ポリシー、またはデータ セキュリティ ポリシー）。トランザクションがグローバル ポリシーに一致する場合、この値は「DefaultGroup」になります。 ポリシー グループ名のスペースは、アンダースコア（_）に置き換えられます。
N/A（ACL デシジョン タグの一部）	`ID(Identity)`	ID ポリシー グループの名前。 ポリシー グループ名のスペースは、アンダースコア（_）に置き換えられます。
N/A（ACL デシジョン タグの一部）	`OutboundMalwareScanning` ポリシー	発信マルウェア スキャン ポリシー グループの名前。 ポリシー グループ名のスペースは、アンダースコア（_）に置き換えられます。
N/A（ACL デシジョン タグの一部）	`DataSecurityPolicy`	Cisco IronPort データ セキュリティ ポリシー グループの名前。トランザクションがグローバルな Cisco IronPort データ セキュリティ ポリシーに一致する場合、この値は「DefaultGroup」になります。このポリシー グループ名は、Cisco IronPort データ セキュリティ フィルタがイネーブルの場合にのみ表示されます。データ セキュリティ ポリシーに一致しなかった場合は、「NONE」と表示されます。 ポリシー グループ名のスペースは、アンダースコア（_）に置き換えられます。
N/A（ACL デシジョン タグの一部）	`ExternalDLPPolicy`	外部 DLP ポリシー グループの名前。トランザクションがグローバル外部 DLP ポリシーに一致する場合、この値は「DefaultGroup」になります。外部 DLP ポリシーに一致しなかった場合は、「NONE」と表示されます。 ポリシー グループ名のスペースは、アンダースコア（_）に置き換えられます。
N/A（ACL デシジョン タグの一部）	`RoutingPolicy`	ルーティング ポリシー グループ名は *ProxyGroupName/ProxyServerName*。 トランザクションがグローバル ルーティング ポリシーに一致する場合、この値は「DefaultRouting」になります。アップストリーム プロキシ サーバを使用しない場合、この値は「DIRECT」になります。 ポリシー グループ名のスペースは、アンダースコア（_）に置き換えられます。

フォーマット指定子	フィールド値	フィールドの説明
%Xr	<IW_comp,6.9,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-","-",-,-,IW_comp,-,"-","-","Unknown","Unknown","-","-",198.34,0,-,[Local],"-",37,"W32.CiscoTestVector",33,0,"WSA-INFECTED-FILE.pdf","fd5ef49d4213e05f448f11ed9c98253d85829614fba368a421d14e64c426da5e">	スキャン判定情報。アクセス ログでは、山カッコ内にさまざまなスキャン エンジンの判定情報が含まれています。 山カッコ内の値の詳細については、アクセス ログのスキャン判定エントリの解釈（11-23 ページ）およびマルウェア スキャンの判定値（11-45 ページ）を参照してください。
%?BLOCK_SUSPECT_USER_AGENT, MONITOR_SUSPECT_USER_AGENT?% <User-Agent:%!%-%.	-	不審なユーザ エージェント。

トランザクション結果コード

アクセス ログ ファイルのトランザクション結果コードは、アプライアンスがクライアント要求を解決する方法を示します。たとえば、オブジェクトの要求がキャッシュから解決可能な場合、結果コードは TCP_HIT です。ただし、オブジェクトがキャッシュに存在せず、アプライアンスが元のサーバからオブジェクトをプルする場合、結果コードは TCP_MISS です。以下の表に、トランザクション結果コードを示します。

結果コード	説明
TCP_HIT	要求されたオブジェクトがディスク キャッシュから取得されました。
TCP_IMS_HIT	クライアントがオブジェクトの IMS（If-Modified-Since）要求を送信し、オブジェクトがキャッシュ内で見つかりました。プロキシは 304 応答を返します。
TCP_MEM_HIT	要求されたオブジェクトがメモリ キャッシュから取得されました。
TCP_MISS	オブジェクトがキャッシュ内で見つからなかったため、元のサーバから取得されました。
TCP_REFRESH_HIT	オブジェクトはキャッシュ内にありましたが、期限切れでした。プロキシが元のサーバに IMS（If-Modified-Since）要求を送信し、サーバはオブジェクトが変更されていないことを確認しました。そのため、アプライアンスはディスクまたはメモリ キャッシュのいずれかからオブジェクトを取得しました。
TCP_CLIENT_REFRESH_MISS	クライアントが「Pragma: no-cache」ヘッダーを発行して、「don't fetch response from cache」要求を送信しました。クライアントから送信されたこのヘッダーにより、アプライアンスは元のサーバからオブジェクトを取得しました。
TCP_DENIED	クライアント要求がアクセス ポリシーによって拒否されました。
UDP_MISS	オブジェクトは発信サーバから取得されました。
NONE	トランザクションでエラーが発生しました。DNS 障害やゲートウェイのタイムアウトなど。

ACL デシジョン タグ

ACL デシジョン タグは、Web プロキシがトランザクションを処理した方法を示すアクセス ログ エントリのフィールドです。Web レピュテーション フィルタ、URL カテゴリ、およびスキャン エンジンの情報が含まれます。

（注） ACL デシジョン タグの末尾に、Web プロキシがパフォーマンスを高めるために内部的に使用する動的に生成された数値が含まれます。この数値は無視できます。

以下の表は、ACL デシジョン タグの値を示しています。

ACL デシジョン タグ	説明
ALLOW_ADMIN_ERROR_PAGE	Web プロキシが、通知ページとそのページで使用される任意のロゴへのトランザクションを許可しました。
ALLOW_CUSTOMCAT	Web プロキシが、アクセス ポリシー グループのカスタム URL カテゴリ フィルタリング設定に基づいてトランザクションを許可しました。
ALLOW_REFERER	Web プロキシが、埋め込み/参照コンテンツの免除に基づいてトランザクションを許可しました。
ALLOW_WBRS	Web プロキシが、アクセス ポリシー グループの Web レピュテーション フィルタ設定に基づいてトランザクションを許可しました。
BLOCK_ADMIN	アクセス ポリシー グループのデフォルト設定に基づいてトランザクションがブロックされました。
BLOCK_ADMIN_CONNECT	アクセス ポリシー グループの HTTP CONNECT ポート設定で定義された宛先の TCP ポートに基づいてトランザクションがブロックされました。
BLOCK_ADMIN_CUSTOM_USER_AGENT	アクセス ポリシー グループの [ブロックするユーザエージェント（Block Custom User Agents）] 設定で定義されたユーザ エージェントに基づいてトランザクションがブロックされました。
BLOCK_ADMIN_HTTPS_NonLocalDestination	トランザクションがブロックされました。クライアントは、SSL ポートを明示的なプロキシとして使用して認証をバイパスしようとしました。これを防ぐために、SSL 接続が WSA 自体に向けられている場合、実際の WSA リダイレクトホスト名への要求だけが許可されます。
BLOCK_ADMIN_IDS	データ セキュリティ ポリシー グループで定義された要求本文のコンテンツの MIME タイプに基づいてトランザクションがブロックされました。
BLOCK_ADMIN_FILE_TYPE	アクセス ポリシー グループで定義されたファイル タイプに基づいてトランザクションがブロックされました。
BLOCK_ADMIN_PROTOCOL	アクセス ポリシー グループの [ブロックするプロトコル（Block Protocols）] 設定で定義されたプロトコルに基づいてトランザクションがブロックされました。
BLOCK_ADMIN_SIZE	アクセス ポリシー グループの [オブジェクト サイズ（Object Size）] 設定で定義された応答のサイズに基づいてトランザクションがブロックされました。

ACL デシジョン タグ	説明
BLOCK_ADMIN_SIZE_IDS	データ セキュリティ ポリシー グループで定義された要求本文のコンテンツのサイズに基づいてトランザクションがブロックされました。
BLOCK_AMP_RESP	Web プロキシが、アクセス ポリシー グループの高度なマルウェア防御設定に基づいて応答をブロックしました。
BLOCK_AMW_REQ	Web プロキシが、発信マルウェア スキャン ポリシー グループの Anti-Malware 設定に基づいて要求をブロックしました。要求の本文はポジティブなマルウェアの判定を生成しました。
BLOCK_AMW_RESP	Web プロキシが、アクセス ポリシー グループの Anti-Malware 設定に基づいて応答をブロックしました。
BLOCK_AMW_REQ_URL	Web プロキシが HTTP 要求の URL が安全ではないと疑い、アクセス ポリシー グループの Anti-Malware 設定に基づいて要求時にトランザクションをブロックしました。
BLOCK_AVC	アクセス ポリシー グループの設定されたアプリケーション設定に基づいてトランザクションがブロックされました。
BLOCK_CONTENT_UNSAFE	アクセス ポリシー グループのサイト コンテンツ レーティング設定に基づいてトランザクションがブロックされました。クライアント要求はアダルト コンテンツに対するものであり、ポリシーはアダルト コンテンツをブロックするように設定されています。
BLOCK_CONTINUE_CONTENT_UNSAFE	アクセス ポリシー グループのサイト コンテンツ レーティング設定に基づいてトランザクションがブロックされ、[警告して継続（Warn and Continue）] ページが表示されました。クライアント要求はアダルト コンテンツに対するものであり、ポリシーはアダルト コンテンツにアクセスするユーザに警告を表示するように設定されています。
BLOCK_CONTINUE_CUSTOMCAT	[警告（Warn）] に設定されているアクセス ポリシー グループのカスタム URL カテゴリに基づいてトランザクションがブロックされ、[警告して継続（Warn and Continue）] ページが表示されました。
BLOCK_CONTINUE_WEBCAT	[警告（Warn）] に設定されているアクセス ポリシー グループの定義済み URL カテゴリに基づいてトランザクションがブロックされ、[警告して継続（Warn and Continue）] ページが表示されました。
BLOCK_CUSTOMCAT	アクセス ポリシー グループのカスタム URL カテゴリ フィルタリング設定に基づいてトランザクションがブロックされました。
BLOCK_ICAP	Web プロキシが、外部 DLP ポリシー グループで定義された外部 DLP システムの判定に基づいて要求をブロックしました。
BLOCK_SEARCH_UNSAFE	クライアント要求には危険な検索クエリーが含まれており、アクセス ポリシーは安全検索を実行するように設定されているので、元のクライアント要求がブロックされました。

ACL デシジョン タグ	説明
BLOCK_SUSPECT_USER_AGENT	アクセス ポリシー グループの [疑わしいユーザエージェント（Suspect User Agent）] 設定に基づいてトランザクションがブロックされました。
BLOCK_UNSUPPORTED_SEARCH_APP	アクセス ポリシー グループの安全検索設定に基づいてトランザクションがブロックされました。トランザクションはサポートされない検索エンジンに対するものであり、ポリシーはサポートされない検索エンジンをブロックするように設定されています。
BLOCK_WBRS	アクセス ポリシー グループの Web レピュテーション フィルタ設定に基づいてトランザクションがブロックされました。
BLOCK_WBRS_IDS	Web プロキシが、Data Security ポリシー グループの Web レピュテーション フィルタ設定に基づいてアップロード要求をブロックしました。
BLOCK_WEBCAT	アクセス ポリシー グループの URL カテゴリ フィルタリング設定に基づいてトランザクションがブロックされました。
BLOCK_WEBCAT_IDS	Web プロキシが、Data Security ポリシー グループの URL カテゴリ フィルタリング設定に基づいてアップロード要求をブロックしました。
DECRYPT_ADMIN	Web プロキシが、復号化ポリシー グループのデフォルト設定に基づいてトランザクションを復号化しました。
DECRYPT_ADMIN_EXPIRED_CERT	サーバ証明書が失効していますが、Web プロキシががトランザクションを復号化しました。
DECRYPT_WEBCAT	Web プロキシが、復号化ポリシー グループの URL カテゴリ フィルタリング設定に基づいてトランザクションを復号化しました。
DECRYPT_WBRS	Web プロキシが、復号化ポリシー グループの Web レピュテーション フィルタ設定に基づいてトランザクションを復号化しました。
DEFAULT_CASE	AsyncOS サービスが Web レピュテーションやアンチマルウェア スキャンなど、トランザクションで処理を行わなかったため、Web プロキシがクライアントにサーバへのアクセスを許可しました。
DROP_ADMIN	Web プロキシが、復号化ポリシー グループのデフォルト設定に基づいてトランザクションをドロップました。
DROP_ADMIN_EXPIRED_CERT	サーバ証明書が失効しているため、Web プロキシがトランザクションをドロップしました。
DROP_WEBCAT	Web プロキシが、復号化ポリシー グループの URL カテゴリ フィルタリング設定に基づいてトランザクションをドロップしました。
DROP_WBRS	Web プロキシが、復号化ポリシー グループの Web レピュテーション フィルタ設定に基づいてトランザクションをドロップしました。

ACL デシジョン タグ	説明
MONITOR_ADMIN_EXPIRED_CERT	サーバ証明書が失効しているため、Web プロキシがサーバ応答をモニタしました。
MONITOR_AMP_RESP	Web プロキシが、アクセス ポリシー グループの高度なマルウェア防御設定に基づいてサーバの応答をモニタしました。
MONITOR_AMW_RESP	Web プロキシが、アクセス ポリシー グループの Anti-Malware 設定に基づいてサーバ応答をモニタしました。
MONITOR_AMW_RESP_URL	Web プロキシが HTTP 要求の URL が安全ではないと疑っていますが、アクセス ポリシー グループの Anti-Malware 設定に基づいてトランザクションをモニタしました。
MONITOR_AVC	Web プロキシが、アクセス ポリシー グループのアプリケーション設定に基づいてトランザクションをモニタしました。
MONITOR_CONTINUE_CONTENT_UNSAFE	任意で、Web プロキシが、アクセス ポリシー グループのサイト コンテンツ レーティング設定に基づいてトランザクションをブロックし、[警告して継続（Warn and Continue）] ページを表示しました。クライアント要求はアダルト コンテンツに対するものであり、ポリシーはアダルト コンテンツにアクセスするユーザに警告を表示するように設定されています。ユーザが警告を受け入れ、続けて最初に要求したサイトにアクセスし、その後他のスキャン エンジンは要求をブロックしませんでした。
MONITOR_CONTINUE_CUSTOMCAT	当初、Web プロキシは、[警告（Warn）] に設定されているアクセス ポリシー グループのカスタム URL カテゴリに基づいて、トランザクションをブロックし、[警告して継続（Warn and Continue）] ページを表示しました。ユーザが警告を受け入れ、続けて最初に要求したサイトにアクセスし、その後他のスキャン エンジンは要求をブロックしませんでした。
MONITOR_CONTINUE_WEBCAT	当初、Web プロキシは、[警告（Warn）] に設定されているアクセス ポリシー グループの定義済み URL カテゴリに基づいて、トランザクションをブロックし、[警告して継続（Warn and Continue）] ページを表示しました。ユーザが警告を受け入れ、続けて最初に要求したサイトにアクセスし、その後他のスキャン エンジンは要求をブロックしませんでした。
MONITOR_IDS	Web プロキシが、データ セキュリティ ポリシーまたは外部 DLP ポリシーのいずれかを使用してアップロード要求をスキャンしましたが、要求をブロックしませんでした。Web プロキシは、アクセス ポリシーに対して要求を評価しました。
MONITOR_SUSPECT_USER_AGENT	Web プロキシが、アクセス ポリシー グループの Suspect User Agent 設定に基づいてトランザクションをモニタしました。
MONITOR_WBRS	Web プロキシが、アクセス ポリシー グループの Web レピュテーション フィルタ設定に基づいてトランザクションをモニタしました。

ACL デシジョン タグ	説明
NO_AUTHORIZATION	ユーザが、ある認証レルムに対して認証済みであったが、アプリケーション認証ポリシーに設定されている認証レルムに対して未認証であったため、Web プロキシはアプリケーションへのユーザ アクセスを許可しませんでした。
NO_PASSWORD	ユーザが認証に失敗しました。
PASSTHRU_ADMIN	Web プロキシが、復号化ポリシー グループのデフォルト設定に基づいてトランザクションをパススルーました。
PASSTHRU_ADMIN_EXPIRED_CERT	サーバ証明書が失効していますが、Web プロキシがトランザクションをパススルーしました。
PASSTHRU_WEBCAT	Web プロキシが、復号化ポリシー グループの URL カテゴリ フィルタリング設定に基づいてトランザクションをパススルーしました。
PASSTHRU_WBRS	Web プロキシが、復号化ポリシー グループの Web レピュテーション フィルタ設定に基づいてトランザクションをパススルーしました。
REDIRECT_CUSTOMCAT	Web プロキシが、[リダイレクト（Redirect）] に設定されているアクセス ポリシー グループのカスタム URL カテゴリに基づいて、トランザクションを別の URL にリダイレクトしました。
SAAS_AUTH	ユーザが、アプリケーション認証ポリシーに設定されている認証レルムに対して透過的に認証されていたため、Web プロキシはそのユーザがアプリケーションにアクセスすることを許可しました。
OTHER	認可の失敗、サーバの切断、クライアントによる中止などのエラーにより、Web プロキシが要求を完了できませんでした。

アクセス ログのスキャン判定エントリの解釈

アクセス ログ ファイル エントリは、URL フィルタリング、Web レピュテーション フィルタリング、アンチマルウェア スキャンなど、さまざまなスキャン エンジンの結果を集約して表示します。アプライアンスは、各アクセス ログ エントリの末尾の山カッコ内にこの情報を表示します。

以下のテキストは、アクセス ログ ファイル エントリからのスキャン判定情報です。この例では、Webroot スキャン エンジンがマルウェアを検出しました。

```
<IW_infr,ns,24,"Trojan-Phisher-Gamec",0,354385,12559,-,"-",-,-,-,"-",-,-,"-","-",-,-,
IW_infr,-,"Trojan Phisher","-","Unknown","Unknown","-","-",489.73,0,-,[Local],"-"
,37,"W32.CiscoTestVector",33,0,"WSA-INFECTED-FILE.pdf","fd5ef49d4213e05f448f11ed9c98253d
85829614fba368a421d14e64c426da5e">
```

（注）　すべてのアクセス ログ ファイル エントリの例については、アクセス ログ ファイル内の Web プロキシ情報（11-15 ページ）を参照してください。

この例の各要素は、以下の表に示すログ ファイル フォーマット指定子に対応しています。

位置	フィールド値	フォーマット指定子	説明
1	IW_infr	%XC	トランザクションに割り当てられたカスタム URL カテゴリ（省略形）。カテゴリが割り当てられない場合、このフィールドには「nc」が表示されます。
2	ns	%XW	Web レピュテーション フィルタリング スコア。このフィールドには、スコアの数値、「ns」（スコアがない場合）、または「dns」（DNS ルックアップ エラーがある場合）が表示されます。
3	24	%Xv	Webroot が DVS エンジンに渡したマルウェア スキャンの判定。Webroot でのみ検出された応答に適用します。 詳細については、マルウェア スキャンの判定値（11-45 ページ）を参照してください。
4	"Trojan-Phisher-Gamec"	"%Xn"	オブジェクトに関連付けられているスパイウェアの名前。Webroot でのみ検出された応答に適用します。
5	[0]	%Xt	マルウェアが存在する可能性を判断する脅威リスク比（TRR）に関連付けられた Webroot 固有の値。Webroot でのみ検出された応答に適用します。
[6]	354385	%Xs	Webroot が脅威識別子として使用する値。シスコ カスタマー サポートでは、問題のトラブルシューティングを行うときにこの値を使用することがあります。Webroot でのみ検出された応答に適用します。
7	12559	%Xi	Webroot がトレース識別子として使用する値。シスコ カスタマー サポートでは、問題のトラブルシューティングを行うときにこの値を使用することがあります。Webroot でのみ検出された応答に適用します。
8	-	%Xd	McAfee が DVS エンジンに渡したマルウェア スキャンの判定。McAfee でのみ検出された応答に適用します。 詳細については、マルウェア スキャンの判定値（11-45 ページ）を参照してください。
9	"-"	"%Xe"	McAfee がスキャンしたファイルの名前。McAfee でのみ検出された応答に適用します。
10	-	%Xf	McAfee がスキャン エラーとして使用する値。シスコ カスタマー サポートでは、問題のトラブルシューティングを行うときにこの値を使用することがあります。McAfee でのみ検出された応答に適用します。
11	-	%Xg	McAfee が検出タイプとして使用する値。シスコ カスタマー サポートでは、問題のトラブルシューティングを行うときにこの値を使用することがあります。McAfee でのみ検出された応答に適用します。
12	-	%Xh	McAfee がウイルス タイプとして使用する値。シスコ カスタマー サポートでは、問題のトラブルシューティングを行うときにこの値を使用することがあります。McAfee でのみ検出された応答に適用します。
13	"-"	"%Xj"	McAfee がスキャンしたウイルスの名前。McAfee でのみ検出された応答に適用します。

位置	フィールド値	フォーマット指定子	説明
14	-	%XY	Sophos が DVS エンジンに渡したマルウェア スキャンの判定。Sophos でのみ検出された応答に適用します。 詳細については、マルウェア スキャンの判定値（11-45 ページ）を参照してください。
15	-	%Xx	Sophos がスキャン戻りコードとして使用する値。シスコ カスタマー サポートでは、問題のトラブルシューティングを行うときにこの値を使用することがあります。Sophos でのみ検出された応答に適用します。
16	"-"	"%Xy"	Sophos が好ましくないコンテンツを検出したファイルの名前。Sophos でのみ検出された応答に適用します。
17	"-"	"%Xz"	Sophos が脅威名として使用する値。シスコ カスタマー サポートでは、問題のトラブルシューティングを行うときにこの値を使用することがあります。Sophos でのみ検出された応答に適用します。
18	-	%Xl	Cisco データ セキュリティ ポリシーの [コンテンツ（Content）] 列のアクションに基づく、Cisco データ セキュリティのスキャン判定。以下のリストは、このフィールドで使用できる値を示します。 • **0.** 許可（Allow） • **1.** ブロック（Block） • **-（ハイフン）**Cisco データ セキュリティ フィルタによるスキャンが開始されませんでした。この値は、Cisco データ セキュリティ フィルタがディセーブルの場合、または URL カテゴリ アクションが [許可（Allow）] に設定されている場合に表示されます。
19	-	%Xp	ICAP 応答で指定された結果に基づく外部 DLP スキャンの評価。以下のリストは、このフィールドで使用できる値を示します。 • **0.** 許可（Allow） • **1.** ブロック（Block） • **-（ハイフン）**外部 DLP サーバによるスキャンが開始されませんでした。この値は、外部 DLP スキャンがディセーブルの場合、または [外部 DLP ポリシー（External DLP Policies）] > [接続先（Destinations）] ページに除外 URL カテゴリがあるため、コンテンツがスキャンされなかった場合に表示されます。
20	IW_infr	%XQ	要求側のスキャン時に決定された定義済み URL カテゴリの判定（省略形）。URL フィルタリングがディセーブルの場合、このフィールドにはハイフン（-）が表示されます。 URL カテゴリの省略形の一覧については、URL Category Descriptions（9-25 ページ）を参照してください。

位置	フィールド値	フォーマット指定子	説明
21	-	%XA	応答側のスキャン中に動的コンテンツ分析エンジンによって判定された URL カテゴリの評価（省略形）。Cisco Web Usage Controls URL フィルタリング エンジンにのみ適用されます。動的コンテンツ分析エンジンがイネーブルになっており、要求時にカテゴリが割り当てられなかった場合にのみ適用されます（値「nc」が要求側のスキャン判定に表示されます）。 URL カテゴリの省略形の一覧については、URL Category Descriptions（9-25 ページ）を参照してください。
22	"Trojan Phisher"	"%XZ"	どのスキャン エンジンがイネーブルになっているかに関係なく、マルウェア カテゴリを提供する統合された応答側アンチマルウェア スキャンの判定。サーバ応答のスキャンによってブロックまたはモニタされるトランザクションに適用されます。
23	"-"	"%Xk"	Web レピュテーション フィルタによって返された脅威タイプ。これは、ターゲット Web サイトのレピュテーションを低下させます。通常、このフィールドにはレピュテーションが -4 以下のサイトが入力されます。
24	"Unknown"	"%XO"	AVC エンジンによって返されたアプリケーションの名前（該当する場合）。AVC エンジンがイネーブルの場合にのみ適用されます。
25	"Unknown"	"%Xu"	AVC エンジンによって返されたアプリケーションのタイプ（該当する場合）。AVC エンジンがイネーブルの場合にのみ適用されます。
26	"-"	"%Xb"	AVC エンジンによって返されたアプリケーションの動作（該当する場合）。AVC エンジンがイネーブルの場合にのみ適用されます。
27	"-"	"%XS"	安全なブラウジング スキャンの判定。この値は、セーフ サーチ機能またはサイト コンテンツ レーティング機能がトランザクションに適用されたかどうかを示します。 可能な値のリストについては、Logging Adult Content Access（9-18 ページ）を参照してください。
28	489.73	%XB	要求に対応するために使用された平均帯域幅（KB/秒）。
29	[0]	%XT	帯域幅制限の制御設定によって要求が絞り込まれたかどうかを示す値。「1」は要求が絞り込まれたことを示し、「0」は絞り込まれなかったことを示します。
30	[Local]	%l	要求を行なっているユーザのタイプ（[ローカル（Local）] または [リモート（Remote）]）。AnyConnect Secure Mobility がイネーブルの場合にのみ適用されます。イネーブルでない場合、値はハイフン（-）です。
31	"-"	"%X3"	どのスキャン エンジンがイネーブルになっているかに依存しない、統合された要求側アンチマルウェア スキャンの判定。発信マルウェア スキャン ポリシーが適用されるときに、クライアント要求のスキャンによってブロックまたはモニタされるトランザクションに適用されます。

位置	フィールド値	フォーマット指定子	説明
32	"-"	“%X4”	該当する発信マルウェア スキャン ポリシーによってブロックまたはモニタされるクライアント要求に割り当てられた脅威の名前。 この脅威の名前は、どのアンチマルウェア スキャン エンジンがイネーブルになっているかには依存しません。
33	37	%X#1#	高度なマルウェア防御ファイル スキャンの判定: • 0:悪意のないファイル • 1:ファイル タイプが原因で、ファイルがスキャンされなかった • 2:ファイル スキャンがタイムアウト • 3:スキャン エラー • 3 よりも大きい値:悪意のあるファイル
34	"W32.CiscoTestVector"	%X#2#	高度なマルウェア防御ファイル スキャンで判定された脅威の名前。「-」は脅威がないことを示します。
35	33	%X#3#	高度なマルウェア防御ファイル スキャンのレピュテーション スコア。このスコアは、クラウド レピュテーション サービスがファイルを正常と判定できない場合にのみ使用されます。 詳細については、第 14 章「Overview of File Reputation Filtering and File Analysis」の「脅威スコアとレピュテーションしきい値」に関する情報を参照してください。
36	[0]	%X#4#	アップロードおよび分析要求のインジケータ: 「0」は、高度なマルウェア防御で分析用にファイルのアップロードが要求されなかったことを示します。 「1」は、高度なマルウェア防御で分析用にファイルのアップロードが要求されたことを示します。
37	"WSA-INFECTED-FILE.pdf"	%X#5#	ダウンロードして分析するファイルの名前。
38	"fd5ef49d4213e05f448f11ed9c98253d85829614fba368a421d14e64c426da5e	%X#6#	このファイルの SHA-256 ID。

各フォーマット指定子の機能については、ログ ファイルのフィールドとタグ（11-34 ページ）を参照してください。

関連項目

- アクセス ログ ファイル内の Web プロキシ情報（11-15 ページ）
- アクセス ログのカスタマイズ（11-30 ページ）。
- W3C 準拠のアクセス ログ ファイル（11-28 ページ）
- ログ ファイルの表示（11-15 ページ）
- ログ ファイルのフィールドとタグ（11-34 ページ）

W3C 準拠のアクセス ログ ファイル

Web Security Appliance には、Web プロキシ トランザクション情報を記録する 2 つの異なるログ タイプ（アクセス ログと W3C 形式のアクセス ログ）が用意されています。W3C アクセス ログは World Wide Web コンソーシアム（W3C）準拠であり、W3C 拡張ログ ファイル（ELF）形式でトランザクション履歴を記録します。

W3C フィールド タイプ

W3C アクセス ログ サブスクリプションを定義する場合は、ACL デシジョン タグまたはクライアント IP アドレスなど、含めるログ フィールドを選択します。以下のいずれかのログ フィールドのタイプを含めることができます。

- **定義済み。**Web インターフェイスには、選択できるフィールドのリストが含まれています。
- **ユーザ定義。**定義済みリストに含まれていないログ フィールドを入力できます。

W3C アクセス ログの解釈

W3C アクセス ログを解釈するときは、以下のルールとガイドラインを考慮してください。

- 各 W3C アクセス ログ サブスクリプションに記録されるデータは、管理者が指定します。したがって、W3C アクセス ログには設定済みのフィールド形式がありません。
- W3C ログは自己記述型です。ファイル形式（フィールドのリスト）は、各ログ ファイルの先頭のヘッダーで定義されます。
- W3C アクセス ログのフィールドは空白で区切ります。
- フィールドに特定のエントリのデータが含まれていない場合、ログ ファイルには代わりにハイフン（-）が表示されます。
- W3C アクセス ログ ファイルの各行は、1 つのトランザクションに対応し、各行は改行シーケンスで終了します。

W3C ログ ファイルのヘッダー

各 W3C ログ ファイルには、ファイルの先頭にヘッダー テキストが含まれています。各行は、# 文字で始まり、ログ ファイルを作成した Web Security Appliance に関する情報を提供します。W3C ログ ファイルのヘッダーには、ログ ファイルを自己記述型にするファイル形式（フィールドのリスト）が含まれています。

以下の表は、各 W3C ログ ファイルの先頭に配置されているヘッダー フィールドの説明です。

ヘッダー フィールド	説明
バージョン（Version）	使用される W3C の ELF 形式バージョン
日付（Date）	ヘッダー（およびログ ファイル）が作成された日時。
システム（System）	ログ ファイルを生成した Web Security Appliance（「Management_IP - Management_hostname」形式）。
ソフトウェア（Software）	これらのログを生成したソフトウェア
フィールド（Fields）	ログに記録されたフィールド

W3C ログ ファイルの例:

```
#Version: 1.0

#Date: 2009-06-15 13:55:20

#System: 10.1.1.1 - wsa.qa

#Software: AsyncOS for Web 6.3.0

#Fields: timestamp x-elapsed-time c-ip x-resultcode-httpstatus sc-bytes cs-method
cs-url cs-username x-hierarchy-origin cs-mime-type x-acltag x-result-code
x-suspect-user-agent
```

W3C フィールドのプレフィックス

ほとんどの W3C ログ フィールドの名前には、クライアントやサーバなど、値を取得したヘッダーを識別するプレフィックスが含まれています。プレフィックスのないログ フィールドは、トランザクションに関与するコンピュータに関係ない値を参照します。以下の表は、W3C ログ フィールドのプレフィックスの説明です。

プレフィックスのヘッダー	説明
c	クライアント
s	サーバ
cs	クライアントからサーバへ
sc	サーバからクライアントへ
x	アプリケーション固有の識別子。

たとえば、W3C ログ フィールド「cs-method」は、クライアントからサーバに送信された要求のメソッドを示し、「c-ip」はクライアントの IP アドレスを示しています。

関連項目

- アクセス ログ ファイル内の Web プロキシ情報（11-15 ページ）。
- アクセス ログのカスタマイズ（11-30 ページ）。

- トラフィック モニタのログ ファイル（11-34 ページ）。
- ログ ファイルのフィールドとタグ（11-34 ページ）。
- ログ ファイルの表示（11-15 ページ）。

アクセス ログのカスタマイズ

標準アクセス ログや W3C アクセス ログをカスタマイズしてさまざまな定義済みフィールドやユーザ定義フィールドを追加して、ネットワーク内の Web トラフィックに関する包括的な情報を取得できます。

関連項目

- 定義済みフィールドの一覧については、ログ ファイルのフィールドとタグ（11-34 ページ）を参照してください。
- ユーザ定義フィールドの詳細については、アクセス ログのユーザ定義フィールド（11-30 ページ）を参照してください。

アクセス ログのユーザ定義フィールド

定義済みのフィールドだけではアクセス ログや W3C ログに記録できない HTTP/HTTPS トランザクションのヘッダー情報がある場合は、カスタム ログ フィールドを追加できます。これを行うには、アクセス ログや W3C ログのサブスクリプションを設定するときに、[カスタム フィールド（Custom Fields）] テキスト ボックスにユーザ定義のログ フィールドを入力します。

カスタム ログ フィールドは、クライアントまたはサーバから送信される任意のヘッダーから任意のデータをとることができます。ログ サブスクリプションに追加されるヘッダーが要求または応答に含まれていない場合、ログ ファイルはログ フィールド値としてハイフンを使用します。

以下の表は、アクセス ログおよび W3C ログにカスタム フィールドを追加するときの構文を示しています。

ヘッダー タイプ	アクセス ログ フォーマット指定子の構文	W3C ログ カスタム フィールドの構文
クライアント アプリケーションからヘッダー	%<*ClientHeaderName*:	cs(*ClientHeaderName*)
サーバからヘッダー	%<*ServerHeaderName*:	sc(*ServerHeaderName*)

たとえば、クライアント要求の If-Modified-Since ヘッダー値のログを記録する場合、W3C ログ サブスクリプションの [カスタム フィールド（Custom Field）] ボックスに以下のテキストを入力します。

```
cs(If-Modified-Since)
```

関連項目

- 標準アクセス ログのカスタマイズ（11-31 ページ）。
- W3C アクセス ログのカスタマイズ（11-31 ページ）。

標準アクセス ログのカスタマイズ

ステップ 1　[システム管理（System Administration）] > [ログ サブスクリプション（Log Subscriptions）] を選択します。

ステップ 2　アクセス ログ サブスクリプションを編集するには、アクセス ログ ファイル名をクリックします。

ステップ 3　[カスタム フィールド（Custom Fields）] に、必要なフォーマット指定子を入力します。

[カスタム フィールド（Custom Fields）] にフォーマット指定子を入力する構文は以下のとおりです。

```
<format_specifier_1> <format_specifier_2> ...
```

例：`%a %b %E`

フォーマット指定子の前にトークンを追加して、アクセス ログ ファイルの説明テキストを表示できます。例：

```
client_IP %a body_bytes %b error_type %E
```

この場合、`client_IP` はログ フォーマット指定子 `%a`の説明トークンです（以下同様）。

（注）　クライアント要求またはサーバ応答の任意のヘッダーにカスタム フィールドを作成できます。

ステップ 4　変更を送信し、保存します。

関連項目

- アクセス ログ ファイル内の Web プロキシ情報（11-15 ページ）。
- ログ ファイルのフィールドとタグ（11-34 ページ）。
- アクセス ログのユーザ定義フィールド（11-30 ページ）。

W3C アクセス ログのカスタマイズ

ステップ 1　[システム管理（System Administration）] > [ログ サブスクリプション（Log Subscriptions）] を選択します。

ステップ 2　W3C ログ サブスクリプションを編集するには、W3C ログ ファイル名をクリックします。

ステップ 3　[カスタム フィールド（Custom Fields）] ボックスにフィールドを入力し、[追加（Add）] をクリックします。

[選択されたログ フィールド（Selected Log Fields）] リストに表示されるフィールドの順序によって、W3C アクセス ログ ファイルのフィールドの順序が決まります。[上へ移動（Move Up）] または [下へ移動（Move Down）] ボタンを使用してフィールドの順序を変更できます。[選択されたログ フィールド（Selected Log Fields）] リストでフィールドを選択し、[削除（Remove）] をクリックして、それを削除できます

[カスタム フィールド（Custom Field）] ボックスに複数のユーザ定義フィールドを入力し、それらを同時に入力できます。ただし、[追加（Add）] をクリックする前に、各エントリが改行（Enter キーを押します）で区切られている必要があります。

W3C ログ サブスクリプションに含まれるログ フィールドを変更すると、ログ サブスクリプションは自動的にロール オーバーします。これにより、ログ ファイルの最新バージョンに適切な新しいフィールド ヘッダーを含めることができます。

（注）　クライアント要求またはサーバ応答の任意のヘッダーにカスタム フィールドを作成できます。

ステップ 4　変更を送信し、保存します。

関連項目

- W3C 準拠のアクセス ログ ファイル（11-28 ページ）。
- ログ ファイルのフィールドとタグ（11-34 ページ）。
- アクセス ログのユーザ定義フィールド（11-30 ページ）。
- CTA 固有のカスタム W3C ログの設定（11-32 ページ）。

CTA 固有のカスタム W3C ログの設定

WSA を、Cognitive Threat Analytics（CTA）（分析とレポートのための Cisco Cloud Web Security サービス固有のカスタム W3C アクセス ログ）を「プッシュ」するよう設定することができます。Cisco ScanCenter は Cloud Web Security（CWS）の管理ポータルです。

はじめる前に

- **SCP** を自動アップロード プロトコルとして選択して WSA の Cisco ScanCenter にデバイスのアカウントを作成します（詳細については、『*Cisco ScanCenter Administrator Guide*』の「プロキシ デバイスのアップロード」のセクションを参照してください）。SCP（セキュア コピー プロトコル）のホスト名と生成された WSA のユーザ名（大文字小文字を区別、デバイスごと異なる）をメモします。

ステップ 1　W3C アクセス ログのカスタマイズ（11-31 ページ）の手順に従って新しい W3C アクセス ログ サブスクリプションを追加し、[ログタイプ（Log Type）] として [W3Cログ（W3C Logs）] を選択します。

ステップ 2　[ログ名（Log Name）] は説明的な名前にします。

ステップ 3　[選択されたログフィールド（Selected Log Fields）] リストのエントリをすべて削除します（[すべて（All）] を選択し、[削除（Remove）] をクリックします）。

ステップ 4　[選択されたログフィールド（Selected Log Fields）] リストに以下のフィールドを追加します。

a. 以下をコピーして [カスタム フィールド（Custom Field）] ボックス内に貼り付け、[追加（Add）] をクリックします。

```
timestamp
x-elapsed-time
c-ip
cs-username
c-port
s-ip
s-port
cs-url
cs-bytes
sc-bytes
```

```
cs(User-Agent)
cs-mime-type
cs-method
sc-http-status
cs(Referer)
sc(Location)
x-amp-sha
x-amp-verdict
x-amp-malware-name
x-amp-score
```

ステップ 5　[ファイルサイズによりロールオーバー(Rollover by File Size)] を指定します。この場合、500M が推奨されます。

ステップ 6　[時刻によりロールオーバー(Rollover by Time)] オプションを選択します。

[以下の間隔でロールオーバー:(Rollover every)] を以下のガイドラインに基づく間隔に指定した、[カスタム時間間隔(Custom Time Interval)] を推奨します。

プロキシの背後のユーザ数	推奨ロールオーバー期間
不明または 2000 未満	55 分
2000 ～ 4000	30 分
4000 ～ 6000	20 分
6000 超	10 分

ステップ 7　[検索方法(Retrieval Method)] には、[リモート SCP サーバ(SCP on Remote Server)] を選択して CWS のアカウントからの CTA サーバ情報を入力します。

a. [SCP ホスト(SCP Host)] フィールドに、Cisco ScanCenter で指定した SCP ホスト(たとえば etr.cloudsec.sco.cisco.com)を入力します。

b. [SCP ポート(SCP Port)] フィールドに 22 と入力します。

c. [ディレクトリ(Directory)] フィールドに /upload と入力します。

d. [ユーザ名(Username)] フィールドに、Cisco ScanCenter のデバイス用に生成されたユーザ名を入力します。デバイス ユーザ名は大文字と小文字が区別され、プロキシ デバイスごとに異なります。

e. [ホストキーチェックを有効化(Enable Host Key Checking)] をオンにし、[自動スキャン(Automatically Scan)] を選択します。

ステップ 8　WSA で、[送信(Submit)] をクリックします。

公開 SSH キーが WSA によって生成され、管理コンソールに表示されます。

ステップ 9　WSA によって生成された公開 SSH キーをクリップボードにコピーします。

ステップ 10　Cisco ScanCenter ポータルに切り替え、適切なデバイス アカウントを選択し、公開 SSH キーを [CTA デバイス プロビジョニング(CTA Device Provisioning)] ページに貼り付けます。(詳細については、『*Cisco ScanCenter Administrator Guide*』の「プロキシ デバイスの アップロード」のセクションを参照してください。

プロキシ デバイスと CTA システム間の認証が成功すると、ログ ファイルをプロキシ デバイスから CTA システムにアップロードし、分析できるようになります。

Cisco ScanCenter は、Cisco Cloud Web Security の管理ポータルです。
http://www.cisco.com/c/en/us/support/security/cloud-web-security/products-installation-and-configuration-guides-list.html を参照してください。

ステップ 11　WSA に戻り、[変更を確定(Commit Changes)] をクリックします。

（注）　設定の変更を確定すると WSA は再起動します。したがって、接続されたユーザは一時的に切断される場合があります。

トラフィック モニタのログ ファイル

レイヤ 4 トラフィック モニタ ログ ファイルには、レイヤ 4 モニタリング アクティビティの詳細が記録されます。レイヤ 4 トラフィック モニタ ログ ファイルのエントリを表示して、ファイアウォール ブロック リストやファイアウォール許可リストのアップデートを追跡できます。

トラフィック モニタ ログの解釈

下記の例では、トラフィック モニタ ログに記録されるさまざまなタイプのエントリの意味について説明します。

例 1

```
172.xx.xx.xx discovered for blocksite.net (blocksite.net) added to firewall block list.
```

この例では、一致する場所がブロック リストのファイアウォール エントリとなります。レイヤ 4 トラフィック モニタにより、アプライアンスを通過した DNS 要求に基づいて、ブロック リストのドメイン名への IP アドレスが検出されました。その後で、その IP アドレスがファイアウォールのブロック リストに追加されました。

例 2

```
172.xx.xx.xx discovered for www.allowsite.com (www.allowsite.com) added to firewall allow list.
```

この例では、一致が許可リストのファイアウォール エントリとなります。レイヤ 4 トラフィック モニタによりドメイン名エントリが照合され、一致がアプライアンスの許可リストに追加されました。その後で、その IP アドレスがファイアウォールの許可リストに追加されました。

例 3

```
Firewall noted data from 172.xx.xx.xx to 209.xx.xx.xx (allowsite.net):80.
```

この例では、レイヤ 4 トラフィック モニタにより内部 IP アドレスとブロック リストに記載されている外部 IP アドレス間で渡されたデータ レコードが記録されています。この場合、レイヤ 4 トラフィック モニタは、「ブロック」ではなく「モニタ」に設定されています。

関連項目

- ログ ファイルの表示(11-15 ページ)

ログ ファイルのフィールドとタグ

- アクセス ログのフォーマット指定子と W3C ログ ファイルのフィールド(11-35 ページ)
- トランザクション結果コード(11-18 ページ)
- ACL デシジョン タグ(11-19 ページ)
- マルウェア スキャンの判定値(11-45 ページ)

アクセス ログのフォーマット指定子と W3C ログ ファイルのフィールド

ログ ファイルでは、各ログ ファイル エントリを構成している情報項目を表すために変数が使用されます。これらの変数は、アクセス ログではフォーマット指定子、W3C ログではログ フィールドと呼ばれ、各フォーマット指定子には対応するログ フィールドがあります。

アクセス ログにこれらの値を表示するよう設定する方法については、アクセス ログのカスタマイズ（11-30 ページ）、およびログ サブスクリプションの追加と編集（11-8 ページ）のカスタム フィールドに関する情報を参照してください。

以下の表は、これらの変数に関する説明です。

アクセス ログのフォーマット指定子	W3C ログのログ フィールド	説明
%:<1	x-p2s-first-byte-time	Web プロキシがサーバへの接続を開始した時点から最初にサーバに書き込みが行えるようになるまでの時間。Web プロキシが複数のサーバに接続してトランザクションを完了する必要がある場合、これらの時間の合計になります。
%:<a	x-p2p-auth-wait-time	Web プロキシが要求を送信後、Web プロキシの認証プロセスからの応答を受信する待機時間。
%:<b	x-p2s-body-time	ヘッダーの後、要求本文をサーバに書き込むまでの待機時間。
%:<d	x-p2p-dns-wait-time	Web プロキシが Web プロキシ DNS プロセスに DNS 要求を送信するのにかかった時間。
%:<h	x-p2s-header-time	最初のバイトの後、要求ヘッダーをサーバに書き込むまでの待機時間。
%:<r	x-p2p-reputation-wait-time	Web プロキシが要求を送信した後、Web レピュテーション フィルタから応答を受信するまでの待機時間。
%:<s	x-p2p-asw-req-wait-time	Web プロキシが要求を送信した後、Web プロキシのアンチスパイウェア プロセスからの判定を受信するまでの待機時間。
%:>1	x-s2p-first-byte-time	サーバからの最初の応答バイトの待機時間
%:>a	x-p2p-auth-svc-time	Web プロキシの認証プロセスからの応答を受信する待機時間（Web プロキシが要求を送信するのに必要な時間を含む）。
%:>b	x-s2p-body-time	ヘッダーの受信後、応答本文全体を待機する時間
%:>c	x-p2p-fetch-time	Web プロキシがディスク キャッシュからの応答を読み取るのに必要な時間。
%:>d	x-p2p-dns-svc-time	Web プロキシ DNS プロセスが Web プロキシに DNS 結果を返送するのにかかった時間。
%:>h	x-s2p-header-time	最初の応答バイト後のサーバ ヘッダーの待機時間
%:>r	x-p2p-reputation-svc-time	Web レピュテーション フィルタからの判定を受信する待機時間（Web プロキシが要求を送信するのに必要な時間を含む）。

アクセス ログのフォーマット指定子	W3C ログのログ フィールド	説明
%:>s	x-p2p-asw-req-svc-time	Web プロキシのアンチス パイウェア プロセスからの判定を受信する待機時間（Web プロキシが要求を送信するのに必要な時間を含む）。
%:1<	x-c2p-first-byte-time	新しいクライアント接続からの最初の要求バイトを待機する時間。
%:1>	x-p2c-first-byte-time	最初のバイトがクライアントに書き込まれるまでの待機時間。
%:A<	x-p2p-avc-svc-time	AVC プロセスからの応答を受信する待機時間（Web プロキシが要求を送信するのに必要な時間を含む）。
%:A>	x-p2p-avc-wait-time	Web プロキシが要求を送信後、AVC プロセスからの応答を受信する待機時間。
%:b<	x-c2p-body-time	クライアント本文全体を待機する時間。
%:b>	x-p2c-body-time	本文全体がクライアントに書き込まれるまでの待機時間。
%:C<	x-p2p-dca-resp-svc-time	動的コンテンツ分析からの判定を受信する待機時間（Web プロキシが要求を送信するのに必要な時間を含む）。
%:C>	x-p2p-dca-resp-wait-time	Web プロキシが要求を送信後、動的コンテンツ分析からの応答を受信する待機時間。
%:h<	x-c2p-header-time	最初のバイトの後の完全なクライアント ヘッダーの待機時間
%:h>	x-s2p-header-time	クライアントに書き込まれる完全なヘッダーの待機時間
%:m<	x-p2p-mcafee-resp-svc-時刻	McAfee スキャン エンジンからの判定を受信する待機時間（Web プロキシが要求を送信するのに必要な時間を含む）。
%:m>	x-p2p-mcafee-resp-wait-時刻	Web プロキシが要求を送信後、McAfee スキャン エンジンからの応答を受信する待機時間。
%:p<	x-p2p-sophos-resp-svc-時刻	Sophos スキャン エンジンからの判定を受信する待機時間（Web プロキシが要求を送信するのに必要な時間を含む）。
%:p>	x-p2p-sophos-resp-wait-時刻	Web プロキシが要求を送信後、Sophos スキャン エンジンからの応答を受信する待機時間。
%:w<	x-p2p-webroot-resp-svc-時刻	Webroot スキャン エンジンからの判定を受信する待機時間（Web プロキシが要求を送信するのに必要な時間を含む）。
%:w>	x-p2p-webroot-resp-wait-time	Web プロキシが要求を送信後、Webroot スキャン エンジンからの応答を受信する待機時間。

アクセス ログのフォーマット指定子	W3C ログのログ フィールド	説明
%?BLOCK_SUSPECT_USER_AGENT,MONITOR_SUSPECT_USER_AGENT?%<User-Agent:%!%-%.	x-suspect-user-agent	不審なユーザ エージェント（該当する場合）。ユーザ エージェントが疑わしいと Web プロキシが判定した場合、そのユーザ エージェントがこのフィールドに記録されます。それ以外の場合、ハイフンが表示されます。このフィールドは、二重引用符付きでアクセス ログに書き込まれます。
%<Referer:	cs(Referer)	Referer ヘッダー
%>Server:	sc(Server)	応答の Server ヘッダー
%a	c-ip	クライアント IP アドレス。
%A	cs-username	認証されたユーザ名。このフィールドは、二重引用符付きでアクセス ログに書き込まれます。
%b	sc-body-size	本文のコンテンツ用に Web プロキシからクライアントに送信されたバイト数。
%B	bytes	使用された合計バイト数（要求サイズ + 応答サイズ、つまり %q + %s）。
%c	cs-mime-type	応答本文の MIME タイプ。このフィールドは、二重引用符付きでアクセス ログに書き込まれます。
%C	cs(Cookie)	Cookie ヘッダー。このフィールドは、二重引用符付きでアクセス ログに書き込まれます。
%d	s-hostname	データ ソースまたはサーバの IP アドレス。
%D	x-acltag	ACL デシジョン タグ。
%e	x-elapsed-time	ミリ秒単位の経過時間。 TCP トラフィックの場合、HTTP 接続の開始から完了までの経過時間です。 UDP トラフィックの場合、最初のデータグラムを送信してから、最後のデータグラムが許可される時間までの経過時間です。UDP トラフィックの経過時間が大きいと、タイムアウト値が大きくなる可能性があり、存続時間の長い UDP アソシエーションの許容データグラムが必要以上に長く許可される可能性があります。
%E	x-error-code	カスタマー サポートが失敗したトランザクションの原因をトラブルシューティングするのに役立つエラー コード番号。
%f	cs(X-Forwarded-For)	X-Forwarded-For ヘッダー
%F	c-port	クライアントの送信元ポート

アクセス ログのフォーマット指定子	W3C ログのログ フィールド	説明
%g	cs-auth-group	承認されたグループ名。このフィールドは、二重引用符付きでアクセス ログに書き込まれます。 このフィールドは、ユーザが適切なグループまたはポリシーに一致しているかどうかを判断する、認証問題のトラブルシューティングに使用されます。
%h	sc-http-status	HTTP 応答コード。
%H	s-hierarchy	階層の取得。
%i	x-icap-server	要求の処理中に接続した最後の ICAP サーバの IP アドレス。
%I	x-transaction-id	トランザクション ID。

アクセス ログのフォーマット指定子	W3C ログのログ フィールド	説明
%j	DCF	応答コードをキャッシュしません（DCF フラグ）。 応答コードの説明: • クライアント要求に基づく応答コード: – 1 = 要求に「no-cache」ヘッダーがあった。 – 2 = 要求に対してキャッシングが許可されていない。 – 4 = 要求に「Variant」ヘッダーがない。 – 8 = ユーザ要求にユーザ名またはパスフレーズが必要。 – 20 = 指定された HTTP メソッドへの応答。 • アプライアンスで受信された応答に基づく応答コード: – 40 = 応答に「Cache-Control: private」ヘッダーが含まれている。 – 80 = 応答に「Cache-Control: no-store」ヘッダーが含まれている。 – 100 = 応答は、要求がクエリーだったことを示している。 – 200 = 応答に含まれている「有効期限」の値が小さい（期限切れ間近）。 – 400 = 応答に「Last Modified」ヘッダーがない。 – 1000 = 応答がただちに期限切れになる。 – 2000 = 応答ファイルが大きすぎてキャッシュできない。 – 20000 = ファイルの新しいコピーがある。 – 40000 = 応答の「Vary」ヘッダーに不正/無効な値がある。 – 80000 = 応答には Cookie の設定が必要。 – 100000 = キャッシュ不可の HTTP ステータス コード。 – 200000 = アプライアンスが受信したオブジェクトが不完全（サイズに基づく）。 – 800000 = 応答トレーラがキャッシュなしを示している。 – 1000000 = 応答のリライトが必要。

アクセス ログのフォーマット指定子	W3C ログのログ フィールド	説明
%k	s-ip	データ ソースの IP アドレス(サーバの IP アドレス) この値は、ネットワーク上の侵入検知デバイスによって IP アドレスがフラグ付けされたときに、要求元を決定するのに使用されます。これにより、フラグ付けされた IP アドレスを参照したクライアントの検索が可能になります。
%l	user-type	ユーザのタイプ(ローカルまたはリモート)。
%L	x-local_time	人間が読み取れる形式の要求のローカル時刻: DD/MMM/YYYY : hh:mm:ss +nnnn。このフィールドは、二重引用符付きでアクセス ログに書き込まれます。 このフィールドを有効にすると、各ログ エントリのエポック タイムからローカルタイムを計算せずにログを問題に関連付けることができます。
%m	cs-auth-mechanism	認証問題をトラブルシューティングするのに使用されます。 トランザクションで使用する認証メカニズム。値は以下のとおりです。 • **BASIC。**ユーザ名が基本認証方式を使用して認証されました。 • **NTLMSSP。**ユーザ名が NTLMSSP 認証方式を使用して認証されました。 • **Kerberos。**ユーザ名は Kerberos 認証方式を使用して認証されました。 • **SSO_TUI。**クライアント IP アドレスと透過的ユーザ ID を使用して認証されたユーザ名を照合することによって、ユーザ名が取得されました。 • **SSO_ISE。**ユーザは ISE サーバによって認証されました(ISE 認証のフォールバック メカニズムとして選択されている場合、ログには GUEST と表示されます)。 • **SSO_ASA。**ユーザがリモート ユーザで、ユーザ名は Secure Mobility を使用して Cisco ASA から取得されました。 • **FORM_AUTH。**アプリケーションへのアクセス時に、ユーザが Web ブラウザのフォームに認証クレデンシャルを入力しました。 • **GUEST。**ユーザが認証に失敗し、代わりにゲスト アクセスが許可されました。
%M	CMF	キャッシュ ミス フラグ(CMF フラグ)。

アクセス ログのフォーマット指定子	W3C ログのログ フィールド	説明
%N	s-computerName	サーバ名または宛先ホスト名。このフィールドは、二重引用符付きでアクセス ログに書き込まれます。
%p	s-port	宛先ポート番号。
%P	cs-version	プロトコル。
%q	cs-bytes	要求サイズ(ヘッダー + 本文)。
%r	x-req-first-line	要求の先頭行:要求方法(URI)。
%s	sc-bytes	応答サイズ(ヘッダー + 本文)。
%t	timestamp	UNIX エポックのタイムスタンプ **注:** サードパーティ製のログ アナライザ ツールを使用して W3C アクセス ログを解析する場合は、timestamp フィールドを含める必要があります。ほとんどのログ アナライザは、このフィールドで提供される形式の時間のみ認識します。
%u	cs(User-Agent)	ユーザ エージェント。このフィールドは、二重引用符付きでアクセス ログに書き込まれます。 このフィールドは、アプリケーションが認証に失敗しているかどうか、および/または別のアクセス権限が必要かどうかを判断するのに役立ちます。
%U	cs-uri	要求 URI。
%v	date	YYYY-MM-DD 形式の日付。
%V	時刻	HH:MM:SS 形式の時刻。
%w	sc-result-code	結果コード。例:TCP_MISS、TCP_HIT。
%W	sc-result-code-denial	結果コードの拒否。
%x	x-latency	待ち時間。
%X0	x-resp-dvs-scanverdict	どのスキャン エンジンがイネーブルになっているかに関係なく、*マルウェア カテゴリ番号*を提供する統合された応答側アンチマルウェア スキャンの判定。サーバ応答のスキャンによってブロックまたはモニタされるトランザクションに適用されます。 このフィールドは、二重引用符付きでアクセス ログに書き込まれます。
%X1	x-resp-dvs-threat-name	どのスキャン エンジンがイネーブルになっているかに関係なく、*マルウェア脅威の名前*を提供する統合された応答側アンチマルウェア スキャンの判定。サーバ応答のスキャンによってブロックまたはモニタされるトランザクションに適用されます。 このフィールドは、二重引用符付きでアクセス ログに書き込まれます。

アクセス ログのフォーマット指定子	W3C ログのログ フィールド	説明
%X2	x-req-dvs-scanverdict	要求側 DVS スキャンの判定
%X3	x-req-dvs-verdictname	要求側 DVS 判定の名前
%X4	x-req-dvs-threat-name	要求側 DVS 脅威の名前
%X6	x-as-malware-threat-name	マルウェア対策スキャン エンジンを起動することなく、適応型スキャンによってトランザクションがブロックされたかどうかを示します。設定可能な値は次のとおりです。 • **1.** トランザクションがブロックされました。 • **0.** トランザクションはブロックされませんでした。 この変数は、スキャン判定情報（各アクセス ログ エントリの末尾の山カッコ内）に含まれています。
%XA	x-webcat-resp-code-abbr	応答側のスキャン中に判定された URL カテゴリの評価（省略形）。Cisco Web Usage Controls URL フィルタリング エンジンにのみ適用されます。
%Xb	x-avc-behavior	AVC エンジンによって識別される Web アプリケーションの動作。
%XB	x-avg-bw	帯域幅制限が AVC エンジンで定義されている場合、ユーザの平均帯域幅。
%XC	x-webcat-code-abbr	トランザクションに割り当てられたカスタム URL カテゴリの URL カテゴリの省略形。
%Xd	x-mcafee-scanverdict	McAfee 固有の ID:（スキャン判定）。
%Xe	x-mcafee-filename	McAfee 固有の ID:（判定を生成するファイル名）このフィールドは二重引用符付きでアクセス ログに書き込まれます。
%Xf	x-mcafee-av-scanerror	McAfee 固有の ID:（スキャン エラー）。
%XF	x-webcat-code-full	トランザクションに割り当てられた URL カテゴリの完全名。このフィールドは、二重引用符付きでアクセス ログに書き込まれます。
%Xg	x-mcafee-av-detecttype	McAfee 固有の ID:（検出タイプ）。
%XG	x-avc-reqhead-scanverdict	AVC 要求ヘッダーの判定。
%Xh	x-mcafee-av-virustype	McAfee 固有の ID:（ウイルス タイプ）。
%XH	x-avc-reqbody-scanverdict	AVC 要求本文の判定。
%Xi	x-webroot-trace-id	Webroot 固有のスキャン識別子:（トレース ID）
%Xj	x-mcafee-virus-name	McAfee 固有の ID:（ウイルス名）このフィールドは、二重引用符付きでアクセス ログに書き込まれます。
%Xk	x-wbrs-threat-type	Web レピュテーションの脅威タイプ。
%XK	x-wbrs-threat-reason	Web レピュテーションの脅威の理由。

アクセス ログのフォーマット指定子	W3C ログのログ フィールド	説明
%Xl	x-ids-verdict	Cisco データ セキュリティ ポリシーのスキャン判定。このフィールドが含まれている場合は IDS 判定が表示されます。IDS がアクティブでドキュメントが「正常」とスキャン判定された場合は「0」、要求に対する IDS ポリシーがアクティブでない場合は「-」が表示されます。
%XL	x-webcat-resp-code-full	応答側のスキャン時に決定された URL カテゴリの判定（完全名）。Cisco Web Usage Controls URL フィルタリング エンジンにのみ適用されます。
%XM	x-avc-resphead-scanverdict	AVC 応答ヘッダーの判定。
%Xn	x-webroot-threat-name	Webroot 固有の ID:（脅威の名前）このフィールドは二重引用符付きでアクセス ログに書き込まれます。
%XN	x-avc-reqbody-scanverdict	AVC 応答本文の判定。
%XO	x-avc-app	AVC エンジンによって識別される Web アプリケーション。
%Xp	x-icap-verdict	外部 DLP サーバのスキャン判定。
%XP	x-acl-added-headers	認識されないヘッダー。クライアント要求の追加ヘッダーのログを記録するには、このフィールドを使用します。クライアント要求を認証してリダイレクトする方法として要求にヘッダーを追加する、特殊なシステム（YouTube for Schools など）のトラブルシューティングをサポートします。
%XQ	x-webcat-req-code-abbr	要求側のスキャン時に決定された定義済み URL カテゴリの判定（省略形）。
%Xr	x-result-code	スキャン判定情報。
%XR	x-webcat-req-code-full	要求側のスキャン中に判定された URL カテゴリの評価（完全名）。
%Xs	x-webroot-spyid	Webroot 固有の ID:（スパイ ID）。
%XS	x-request-rewrite	安全なブラウジング スキャンの判定。 セーフ サーチ機能またはサイト コンテンツ レーティング機能がトランザクションに適用されたかどうかを示します。
%Xt	x-webroot-trr	Webroot 固有の ID:（脅威リスク比率（TRR））。
%XT	x-bw-throttled	帯域幅制限がトランザクションに適用されたかどうかを示すフラグ。
%Xu	x-avc-type	AVC エンジンによって識別される Web アプリケーションのタイプ。
%Xv	x-webroot-scanverdict	Webroot からのマルウェア スキャンの判定。

アクセス ログのフォーマット指定子	W3C ログのログ フィールド	説明
%XV	x-request-source-ip	Web プロキシ設定で、[X-Forwarded-For を使用したクライアント IP アドレスの識別を有効にする（Enable Identification of Client IP Addresses using X-Forwarded-For）] チェックボックスをオンにした場合のダウンストリーム IP アドレス。
%XW	x-wbrs-score	復号化された WBRS スコア <-10.0-10.0>。
%Xx	x-sophos-scanerror	Sophos 固有の ID:（スキャンの戻りコード）。
%Xy	x-sophos-file-name	Sophos が好ましくないコンテンツを検出したファイルの名前。Sophos でのみ検出された応答に適用します。
%XY	x-sophos-scanverdict	Sophos 固有の ID:（スキャン判定）。
%Xz	x-sophos-virus-name	Sophos 固有の ID:（脅威の名前）。
%XZ	x-resp-dvs-verdictname	どのスキャン エンジンがイネーブルになっているかに関係なく、*マルウェア カテゴリ*を提供する統合された応答側アンチマルウェア スキャンの判定。サーバ応答のスキャンによってブロックまたはモニタされるトランザクションに適用されます。 このフィールドは、二重引用符付きでアクセス ログに書き込まれます。
%X#1#	x-amp-verdict	高度なマルウェア防御ファイル スキャンの判定: • 0:悪意のないファイル。 • 1:ファイル タイプが原因で、ファイルがスキャンされなかった。 • 2:ファイル スキャンがタイムアウト。 • 3:スキャン エラー。 • 3 よりも大きい値:悪意のあるファイル。
%X#2#	x-amp-malware-name	高度なマルウェア防御ファイル スキャンで判定された脅威の名前。「-」は脅威がないことを示します。
%X#3#	x-amp-score	高度なマルウェア防御ファイル スキャンのレピュテーション スコア。 このスコアは、クラウド レピュテーション サービスがファイルを正常と判定できない場合にのみ使用されます。 詳細については、第 14 章「Overview of File Reputation Filtering and File Analysis」の「脅威スコアとレピュテーションしきい値」に関する情報を参照してください。

アクセス ログのフォーマット指定子	W3C ログのログ フィールド	説明
%X#4#	x-amp-upload	アップロードおよび分析要求のインジケータ： 「0」は、高度なマルウェア防御で分析用にファイルのアップロードが要求されなかったことを示します。 「1」は、高度なマルウェア防御で分析用にファイルのアップロードが要求されたことを示します。
%X#5#	x-amp-filename	ダウンロードして分析するファイルの名前。
%X#6#	x-amp-sha	このファイルの SHA-256 ID。
%y	cs-method	方式。
%Y	cs-url	URL 全体。
該当なし	x-hierarchy-origin	要求コンテンツを取得するために接続したサーバを示すコード（DIRECT/www.example.com など）。
該当なし	x-resultcode-httpstatus	結果コードおよび HTTP 応答コード（間をスラッシュ（/）で区切ります）。

関連項目

- アクセス ログ ファイル内の Web プロキシ情報（11-15 ページ）。
- W3C アクセス ログの解釈（11-28 ページ）。

マルウェア スキャンの判定値

マルウェア スキャンの判定は、マルウェアを含む可能性を判別する、URL 要求またはサーバ応答に割り当てられた値です。Webroot、McAfee、および Sophos のスキャン エンジンは、マルウェア スキャンの判定を DVS エンジンに返し、DVS エンジンが要求をモニタするかブロックするかを決定できるようにします。特定のアクセス ポリシーに対するアンチマルウェア設定を編集した場合、各マルウェア スキャンの判定は、[アクセス ポリシー（Access Policies）] > [レピュテーションおよびマルウェア対策設定（Reputation and Anti-Malware Settings）] ページにリストされているマルウェア カテゴリに対応します。

以下のリストは、さまざまなマルウェア スキャンの判定値および対応するマルウェア カテゴリを示しています。

マルウェア スキャンの判定値	マルウェア カテゴリ
-	設定しない
[0]	不明
1	スキャンしない
2	Timeout
3	エラー（Error）
4	スキャン不可
10	一般的なスパイウェア
12	ブラウザ ヘルパー オブジェクト

マルウェア スキャンの判定値	マルウェア カテゴリ
13	アドウェア
14	システム モニタ
18	商用システム モニタ
19	ダイヤラ
20	ハイジャッカー
21	フィッシング URL
22	トロイのダウンローダ
23	トロイの木馬
24	トロイのフィッシャ
25	ワーム
26	暗号化ファイル
27	ウィルス
33	その他のマルウェア
34	PUA
35	中断
36	アウトブレイク ヒューリスティック
37	既知の悪意のある高リスク ファイル

関連項目

- アクセス ログ ファイル内の Web プロキシ情報（11-15 ページ）。
- W3C アクセス ログの解釈（11-28 ページ）。

ロギングのトラブルシューティング

- アクセス ログ エントリにカスタム URL カテゴリが表示されない（A-9 ページ）
- HTTPS トランザクションのロギング（A-9 ページ）
- アラート：生成データのレートを維持できない（A-9 ページ）
- W3C アクセス ログでサードパーティ製ログ アナライザ ツールを使用する場合の問題（A-10 ページ）

CHAPTER 12

システム管理タスクの実行

システム管理の概要

S シリーズ アプライアンスは、システム管理用の各種のツールを提供します。[システム管理（System Administration）] タブの機能は、以下のタスクの管理を支援します。

- アプライアンスの設定
- 機能キー
- ユーザ アカウントの追加、編集、および削除
- AsyncOS ソフトウェアのアップグレードとアップデート
- システム時刻

アプライアンス設定の保存、ロード、およびリセット

Web セキュリティ アプライアンス のすべての設定は、1 つの XML コンフィギュレーション ファイルで管理できます。

アプライアンス設定の表示と印刷

ステップ 1　[システム管理（System Administration）] > [設定のサマリー（Configuration Summary）] を選択します。

ステップ 2　必要に応じて、[設定のサマリー（Configuration Summary）] ページを表示または印刷します。

アプライアンス設定ファイルの保存

ステップ 1　[システム管理（System Administration）] > [設定ファイル（Configuration File）] を選択します。

ステップ 2　[設定ファイル（Configuration File）] のオプションを設定します。

オプション	説明
以下のオプションから選択します。 • [表示または保存するローカルコンピュータにファイルをダウンロード（Download file to local computer to view or save）] • [ファイルをこのアプライアンス（example.com）に保存（Save file to this appliance (example.com)）] • [ファイルをメールで送信（Email file to）]	ファイルを保存する場所を選択できます。
[設定ファイルでパスフレーズをマスクする（Mask passphrases in the Configuration Files）]	イネーブルにすると、エクスポートまたは保存したファイルで、元の暗号化されたパスフレーズが「*****」に置き換えられます。ただし、パスフレーズがマスクされた設定ファイルを直接 AsyncOS for Web に再ロードすることはできません。
以下のファイル名オプションから選択します。 • [システムにより生成されたファイル名を使用（Use system-generated file name）] • [ユーザ定義ファイル名を使用：（Use user-defined file name:）]	コンフィギュレーション ファイルの命名方法を選択できます。

ステップ 3　[送信（Submit）] をクリックします。

アプライアンス設定ファイルのロード

注意　設定をロードすると、現在の設定がすべて完全に削除されます。以下の操作を実行する前に設定を保存することを強く推奨します。

（注）　互換性のあるコンフィギュレーション ファイルが、アプライアンスの現在インストールされているバージョンより URL カテゴリのセットの古いバージョンに基づいている場合、コンフィギュレーション ファイルのポリシーと ID が自動的に変更される場合があります。

ステップ 1　[システム管理（System Administration）] > [設定ファイル（Configuration File）] を選択します。

ステップ 2　[設定をロード（Load Configuration）] オプションとロードするファイルを選択します。（注）

パスフレーズがマスクされているファイルはロードできません。

ファイルには以下のヘッダーが必要です。

```
<?xml version="1.0" encoding="ISO-8859-1"?> <!DOCTYPE config SYSTEM "config.dtd">
```

また、正しくフォーマットされた config セクションも必要です。

```
<config> ... your configuration information in valid XML </config>
```

ステップ 3　[ロード（Load）] をクリックします。

ステップ 4　表示される警告を確認します。処理の結果を確認したら、[続行（Continue）] をクリックします。

アプライアンス設定の出荷時デフォルトへのリセット

アプライアンス設定をリセットするときに、既存のネットワーク設定を保持するかどうかを選択できます。

このアクションでは、コミットする必要はありません。

はじめる前に

アプライアンスから任意の場所に設定を保存します。

ステップ 1　[システム管理（System Administration）] > [設定ファイル（Configuration File）] を選択します。

ステップ 2　下方向にスクロールして、[構成のリセット（Reset Configuration）] セクションを表示します。

ステップ 3　ページに表示された情報を読み、オプションを選択します。

ステップ 4　[リセット（Reset）] をクリックします。

機能キーの使用

機能キーはシステム上で固有の機能をイネーブル化します。キーはアプライアンスのシリアル番号に固有のものです（機能キーを別のアプライアンスで再使用することはできません）。

機能キーの表示と更新

ステップ 1　[システム管理（System Administration）] > [機能キー（Feature Keys）] を選択します。

ステップ 2　保留中のキーのリストを更新するには、[新しいキーをチェック（Check for New Keys）] をクリックします。

ステップ 3　新しい機能キーを手動で追加するには、[ライセンス キー（Feature Keys）] フィールドにキーを貼り付けるか、入力し、[キーを送信（Submit Key）] をクリックします。機能キーが有効な場合は、そのキーが画面に追加されます。

ステップ 4　[保留中のライセンス（Pending Activation）] リストの新しい機能キーをアクティブ化するには、そのキーの [選択（Select）] チェックボックスをオンにして、[選択したキーを有効化（Activate Selected Keys）] をクリックします。

新しいキーが発行されたときに、キーを自動的にダウンロードおよびインストールするように、アプライアンスを設定できます。この場合、[保留中のライセンス（Pending Activation）]一覧は常に空白になります。[ライセンス キーの設定（Feature Key Settings）] ページで自動確認をディセーブルにした場合であっても、[新しいキーをチェック（Check for New Keys）] ボタンをクリックすることにより、新しいキーを検索するよう AsyncOS にいつでも指示できます。

機能キーの更新設定の変更

[ライセンス キーの設定（Feature Key Settings）] ページは、新しい機能キーを確認およびダウンロードするかどうかや、これらのキーを自動的にアクティベートするかどうかを制御するために使用します。

ステップ 1　[システム管理（System Administration）] > [ライセンス キーの設定（Feature Key Settings）] を選択します。

ステップ 2　[設定の編集（Edit Settings）] をクリックします。

ステップ 3　必要に応じて [ライセンス キーの設定（Feature Key Settings）] を変更します。

オプション	説明
[ライセンス キーの自動適用（Automatic Serving of Feature Keys）]	機能キーを自動的にチェックしてダウンロードし、ダウンロードした機能キーを自動的にアクティブ化します。 自動チェックは通常、月に 1 回実行されますが、機能キーが 10 日未満で期限切れになる場合は 1 日に 1 回実行されます。キーの失効後の 1 か月間は、1 日に 1 回実行されます。1 か月が経過すると、期限が切れたキーは期限切れ間近/期限切れのキーのリストに示されなくなります。

ステップ 4　変更を送信し、保存します。

仮想アプライアンスのライセンス

Cisco Web Security 仮想アプライアンスでは、ホスト上で仮想アプライアンスを実行する追加ライセンスが必要です。

仮想アプライアンスのライセンスの詳細については、『*Cisco Content Security Virtual Appliance Installation Guide*』を参照してください。このドキュメントは、http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html から入手できます。

（注）　仮想アプライアンスのライセンスをインストールする前に、テクニカル サポートのトンネルを開くことはできません。

ライセンスの期限が切れた後、アプライアンスは、180 日間セキュリティ サービスなしで、Web プロキシとして動作を継続します。この期間中、セキュリティ サービスは更新されません。

ライセンスの期限切れに関する警告を受信するように、アプライアンスを設定できます。

関連項目

- アラートの管理（12-13 ページ）

仮想アプライアンスのライセンスのインストール

『*Cisco Content Security Virtual Appliance Installation Guide*』を参照してください。このドキュメントは、http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html から入手できます。

リモート電源再投入の有効化

アプライアンス シャーシの電源をリモートでリセットする機能は、80-シリーズ ハードウェアでのみ使用できます。

アプライアンスの電源をリモートでリセットする場合は、このセクションで説明されている手順を使用して、この機能を事前に有効にし、設定しておく必要があります。

はじめる前に

- 専用のリモート電源再投入（RPC）ポートをセキュア ネットワークに直接、ケーブル接続します。詳細については、お使いのアプライアンス モデルのハードウェア ガイドを参照してください。このドキュメントの場所については、ドキュメント セット（C-2 ページ）を参照してください。
- ファイアウォールを通過するために必要なポートを開くなど、アプライアンスがリモート アクセス可能であることを確認します。

- この機能を使用するには、専用のリモート電源再投入インターフェイスの一意の IPv4 アドレスが必要です。このインターフェイスは、このセクションで説明されている手順でのみ設定可能です。`ipconfig` コマンドを使用して設定することはできません。
- アプライアンスの電源を再投入するには、Intelligent Platform Management Interface（IPMI）バージョン 2.0 をサポートするデバイスを管理できるサードパーティ製ツールが必要です。このようなツールを使用できるように準備されていることを確認します。
- コマンドライン インターフェイスの詳細については、次を参照してください。付録 B「コマンドライン インターフェイス」

ステップ 1　SSH またはシリアル コンソール ポートを使用して、コマンドライン インターフェイスにアクセスします。

ステップ 2　管理者権限を持つアカウントを使用してログインします。

ステップ 3　以下のコマンドを入力します。

```
remotepower
setup
```

ステップ 4　プロンプトに従って、以下の情報を指定します。

- この機能専用の IP アドレスと、ネットマスクおよびゲートウェイ。
- 電源の再投入コマンドを実行するために必要なユーザ名とパスフレーズ。

  これらのクレデンシャルは、アプライアンスへのアクセスに使用する他のクレデンシャルに依存しません。

ステップ 5　`commit` を入力して変更を保存します。

ステップ 6　設定をテストして、アプライアンスの電源をリモートで管理できることを確認します。

ステップ 7　入力したクレデンシャルが、将来、いつでも使用できることを確認します。たとえば、この情報を安全な場所に保管し、このタスクを実行する必要がある管理者が、必要なクレデンシャルにアクセスできるようにします。

関連項目

- ハードウェア アプライアンス：アプライアンスの電源のリモート リセット（A-13 ページ）

ユーザ アカウントの管理

以下のタイプのユーザは、Web セキュリティ アプライアンスにログインして、アプライアンスを管理できます。

- **ローカル ユーザ。**アプライアンス自体にローカルにユーザを定義できます。
- **外部システムに定義されたユーザ。**アプライアンスにログインするユーザを認証するために、外部 RADIUS サーバに接続するようにアプライアンスを設定できます。

（注）　Web インターフェイスにログインするか、SSH を使用するなどの任意の方法を使用して、アプライアンスにログインできます。

関連項目

- ローカル ユーザ アカウントの管理（12-7 ページ）。
- RADIUS ユーザ認証（12-9 ページ）。

ローカル ユーザ アカウントの管理

Web セキュリティ アプライアンスに任意の数のユーザをローカルに定義できます。

デフォルトのシステム admin アカウントは、すべての管理者権限を持っています。admin アカウントのパスフレーズは変更できますが、このアカウントを編集したり削除することはできません。

（注） admin ユーザのパスフレーズを紛失した場合は、シスコ サポート プロバイダーに問い合わせしてください。

ローカル ユーザ アカウントの追加

はじめる前に

すべてのユーザ アカウントが従うべきパスフレーズ要件を定義します。管理ユーザのパスフレーズ要件の設定（12-11 ページ）を参照してください。

ステップ 1　[システム管理（System Administration）] > [ユーザ（Users）] を選択します。

ステップ 2　[ユーザの追加（Add User）] をクリックします。

ステップ 3　以下のルールに注意して、ユーザ名を入力します。

- ユーザ名に小文字、数字、およびダッシュ（-）記号を使用することはできますが、最初の文字をダッシュにすることはできません。
- ユーザ名は 16 文字以下です。
- ユーザ名としてシステムで予約されている特殊名（「operator」や「root」など）を指定することはできません。
- 外部認証も使用する場合は、ユーザ名が外部認証されたユーザ名と重複しないようにしてください。

ステップ 4　ユーザの氏名を入力します。

ステップ 5　ユーザ タイプを選択します。

ユーザ タイプ	説明
管理者（Administrator）	すべてのシステム設定に対する完全なアクセス権を許可します。ただし、`upgradecheck` および `upgradeinstall` CLI コマンドは、システム定義の「admin」アカウントからのみ発行できます。
演算子	ユーザ アカウントを作成、編集、および削除できません。オペレータ グループでは、以下の CLI コマンドの使用も制限されます。 • `resetconfig` • `upgradecheck` • `upgradeinstall` • `systemsetup` またはシステム セットアップ ウィザードの実行

ユーザ タイプ	説明
オペレータ（読み取り専用）（Read-Only Operator）	このロールのユーザ アカウントは、 • 設定情報を表示できます。 • 機能の設定方法を確認するために変更を行って送信はできますが、コミットはできません。 • キャッシュをクリアしたり、ファイルを保存するなどのアプライアンスへの他の変更を加えることはできません。 • ファイル システム、FTP、または SCP にアクセスできません。
ゲスト	ゲスト グループのユーザは、レポートやトラッキングなど、システムのステータス情報の参照のみを実行できます。

ステップ 6　パスフレーズを入力するか、または作成します。

ステップ 7　変更を送信し、保存します。

ユーザ アカウントの削除

ステップ 1　[システム管理（System Administration）] > [ユーザ（Users）] を選択します。

ステップ 2　プロンプトが表示されたら、一覧表示されているユーザ名に対応するゴミ箱アイコンをクリックして確認します。

ステップ 3　変更を送信し、保存します。

ユーザ アカウントの編集

ステップ 1　[システム管理（System Administration）] > [ユーザ（Users）] を選択します。

ステップ 2　ユーザ名をクリックします。

ステップ 3　必要に応じて、[ユーザの編集（Edit User）] ページでユーザに変更を加えます。

ステップ 4　変更を送信し、保存します。

パスフレーズの変更

現在ログインしているアカウントのパスフレーズを変更するには、ウィンドウの右上で、[オプション（Options）] > [パスフレーズの変更（Change Passphrase）] を選択します。

他のアカウントの場合は、[ローカルユーザ設定（Local User Settings）] ページで、アカウントを編集してパスフレーズを変更します。

関連項目

- ユーザ アカウントの編集（12-8 ページ）
- 管理ユーザのパスフレーズ要件の設定（12-11 ページ）

RADIUS ユーザ認証

Web セキュリティ アプライアンスは RADIUS ディレクトリ サービスを使用して、HTTP、HTTPS、SSH、および FTP によりアプライアンスにログインするユーザを認証します。PAP または CHAP 認証を使用して、認証のために複数の外部サーバと連携するように、アプライアンスを設定できます。外部ユーザのグループを Web セキュリティ アプライアンスのさまざまなユーザ ロール タイプにマッピングできます。

RADIUS 認証のイベントのシーケンス

外部認証がイネーブルになっている場合にユーザが Web セキュリティ アプライアンスにログインすると、アプライアンスは以下を実行します。

1. ユーザがシステム定義の「admin」アカウントであるかどうかを確認します。
2. 「admin」アカウントでない場合は、まず、設定されている外部サーバをチェックし、ユーザがそのサーバで定義されているかどうかを確認します。
3. 最初の外部サーバに接続できない場合、アプライアンスはリスト内の以下の外部サーバをチェックします。
4. アプライアンスが外部サーバに接続できない場合、アプライアンスは Web セキュリティ アプライアンスで定義されたローカル ユーザとしてユーザを認証しようとします。
5. そのユーザが外部サーバまたはアプライアンスに存在しない場合、またはユーザが間違ったパスフレーズを入力した場合は、アプライアンスへのアクセスが拒否されます。

RADIUS を使用した外部認証のイネーブル化

ステップ 1　[システム管理（System Administration）] > [ユーザ（Users）] ページで、[外部認証を有効にする（Enable External Authentication）] をクリックします。

ステップ 2　認証タイプとして [RADIUS] を選択します。

ステップ 3　RADIUS サーバのホスト名、ポート番号、共有シークレット パスフレーズを入力します。デフォルトのポートは 1812 です。

ステップ 4　タイムアウトまでにアプライアンスがサーバからの応答を待つ時間を秒単位で入力します。

ステップ 5　RADIUS サーバが使用する認証プロトコルを選択します。

ステップ 6　（任意）[行を追加（Add Row）] をクリックして別の RADIUS サーバを追加します。各 RADIUS ログについて、3 ～ 5 のステップを繰り返します。

（注）　最大 10 個の RADIUS サーバを追加できます。

ステップ 7　再認証のために再び RADIUS サーバに接続するまでに、AsyncOS が外部認証クレデンシャルを保存する秒数を [外部認証キャッシュ タイムアウト（External Authentication Cache Timeout）] フィールドに入力します。デフォルトは 0 です。

（注）　RADIUS サーバがワンタイム パスフレーズ（トークンから作成されたパスフレーズなど）を使用している場合は、ゼロ（0）を入力します。値をゼロに設定すると、AsyncOS は、現在のセッション中に認証のために RADIUS サーバに再アクセスしません。

ステップ 8　グループ マッピングを設定します。すべての外部認証されたユーザ全員を管理者ロールにマッピングするか、異なるアプライアンス ユーザ ロール タイプにマッピングするかを選択します。

設定	説明
外部認証されたユーザを複数のローカル ロールにマッピング。	RADIUS CLASS 属性で定義されたグループ名を入力し、アプライアンス ロール タイプを選択します。[行の追加（Add Row）] をクリックして、さらにロール マッピングを追加できます。 AsyncOS は、RADIUS CLASS 属性に基づいて、RADIUS ユーザをアプライアンス ロールに割り当てます。CLASS 属性の要件: • 最小 3文字 • 最大 253 文字 • コロン、カンマ、または改行文字なし • 各 RADIUS ユーザに対し 1 つ以上のマップ済み CLASS 属性（この設定を使用する場合、AsyncOS は、マップ済み CLASS 属性のない RADIUS ユーザへのアクセスを拒否します）。 複数の CLASS 属性のある RADIUS ユーザの場合、AsyncOS は最も制限されたロールを割り当てます。たとえば、Operator ロールにマッピングされている CLASS 属性と、Read-Only Operator ロールにマッピングされている CLASS 属性の 2 つが RADIUS ユーザにある場合、AsyncOS は、Operator ロールよりも制限された Read-Only Operator ロールに RADIUS ユーザを割り当てます。 以下のアプライアンス ロールは、最も制限が厳しいものから順番に並んでいます。 • 管理者（Administrator） • 演算子 • Read-Only Operator • ゲスト
外部認証されたすべてのユーザを管理ロールにマップします。	AsyncOS は すべての RADIUS ユーザを Administrator ロールに割り当てます。

ステップ 9　変更を送信し、保存します。

関連項目

- 外部認証（5-11 ページ）
- ローカル ユーザ アカウントの追加（12-7 ページ）。

ユーザ プリファレンスの定義

レポートの表示形式などのプリファレンス設定は、各ユーザごとに保存され、ユーザがどのクライアント マシンからアプライアンスにログインするかに関係なく同じ設定が適用されます。

ステップ 1　[オプション（Options）] > [環境設定（Preferences）] を選択します。

ステップ 2　[ユーザ設定（User Preferences）] ページで、[設定を編集（Edit Preferences）] をクリックします。

ステップ 3　必要に応じて、プリファレンスを設定します。

プリファレンス設定	説明
言語の表示（Language Display）	Web インターフェイスおよび CLI で使用する言語の Web 用 AsyncOS。
ランディング ページ（Landing Page）	ユーザがアプライアンスにログインするときに表示されるページ。
表示されるレポート時間範囲（Reporting Time Range Displayed）（デフォルト）	[レポート（Reporting）] タブでレポートに対して表示するデフォルトの時間範囲。
表示するレポート行の数（Number of Reporting Rows Displayed）	デフォルトで各レポートに表示されるデータの行数。

ステップ 4　変更を送信し、保存します。

管理者の設定

管理ユーザのパスフレーズ要件の設定

アプライアンスでローカル定義された管理ユーザのパスフレーズ要件を設定するには、以下の手順を実行します。

ステップ 1　[システム管理（System Administration）] > [ユーザ（Users）] を選択します。

ステップ 2　[パスフレーズの設定（Passphrase Settings）] セクションで、[設定を編集（Edit Settings）] をクリックします。

ステップ 3　以下のオプションから選択します。

オプション	説明
パスフレーズで許可しない単語の一覧（List of words to disallow in passphrases）	1 行ごとに各禁止単語を記入した .txt ファイルを作成し、そのファイルを選択してアップロードします。後続のアップロードによって以前のアップロードが上書きされます。

オプション	説明
パスフレーズの強度（Passphrase Strength）	管理ユーザが新しいパスフレーズを入力するときに、パスフレーズ強度インジケータを表示できます。 この設定によって強固なパスフレーズが作成されるわけではありません。この設定は、入力したパスフレーズの推測されやすさを示すだけです。 インジケータを表示する対象ロールを選択します。次に、選択したロールごとにゼロより大きい数字を入力します。数値が大きいほど、強固なパスフレーズとして登録されるパスフレーズの実現が困難になります。この設定には最大値がありませんが、非常に大きな数値を指定すると、「適切」として評価されるパスフレーズの作成が事実上不可能になります。 さまざまな値を試すことで、最も要件を満たす数値を確認してください。 パスフレーズの強度は対数目盛で測定されます。評価は、NIST SP 800-63 付則 A の定義に準拠する、米国国立標準技術研究所のエントロピー ルールに基づいています。 一般的に、強固なパスフレーズは以下のような特徴を備えています。 • 長い。 • 大文字、小文字、数字、および特殊文字を含む。 • あらゆる言語の辞書にある語を含まない。 これらの特徴を備えたパスフレーズを適用するには、このページの他の設定を使用します。

ステップ 4　変更を送信し、保存します。

アプライアンスの割り当てに対するセキュリティ設定の追加

アプライアンスにログインする管理者の認証により厳しいアクセス要件を設けるように、Web セキュリティ アプライアンスを設定できます。

コマンド（Command）	説明
adminaccessconfig > banner	管理者がログインを試みるときに指定のテキストを表示するように、アプライアンスを設定します。Web インターフェイスや FTP 経由など、どのようなインターフェイスからでも、管理者がアプライアンスにアクセスすると、カスタム バナー テキストが表示されます。 CLI プロンプトに貼り付けるか、Web セキュリティ アプライアンスにあるファイルからコピーすることで、カスタム テキストをロードできます。ファイルからテキストをアップロードするには、まず、FTP を使用してアプライアンスの configuration ディレクトリにファイルを転送します。

コマンド（Command）	説明
adminaccessconfig > ipaccess	管理者が Web セキュリティ アプライアンスにアクセスするときの接続元の IP アドレスを制御します。管理者は、任意のマシンまたは指定する一覧の IP アドレスを持つマシンからアプライアンスにアクセスできます。 一覧を許可するためにアクセスを制限するには、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。 デフォルトでは、アプライアンスにアクセスできるアドレスを一覧表示すると、現在のマシンの IP アドレスが許可リストの最初のアドレスとして一覧表示されます。許可リストから現在のマシンの IP アドレスは削除できません。
adminaccessconfig > strictssl	管理者がより強力な SSL 暗号（56 ビット暗号化以上）を使用してポート 8443 の Web インターフェイスにログインできるように、アプライアンスを設定します。 より強力な SSL 暗号を必要とするようにアプライアンスを設定すると、その変更は HTTPS を使用して管理の目的でアプライアンスにアクセスする管理者にのみ適用されます。HTTPS を使用して Web プロキシに接続されている他のネットワーク トラフィックには適用されません。

管理者パスフレーズのリセット

すべての管理者レベルのユーザは、「admin」ユーザのパスフレーズを変更できます。

はじめる前に

- admin アカウントのパスフレーズが不明な場合は、カスタマー サポート プロバイダーに連絡してパスフレーズをリセットしてください。
- パスフレーズの変更は即座に有効になり、変更を送信する必要はありません。

ステップ 1　[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザ（Users）] を選択します。

ステップ 2　[User（ユーザ）] リストで [admin] リンクをクリックします。

ステップ 3　[パスフレーズの変更（Change Passphrase）] を選択します。

ステップ 4　新しいパスフレーズを作成するか、または入力します。

アラートの管理

アラートとは、Cisco Web セキュリティ アプライアンス 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（情報）からメジャー（クリティカル）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。

（注）　アラートと通知メール通知を受信するには、アプライアンスが電子メール メッセージへの送信に使用する SMTP リレー ホストを設定する必要があります。

アラートの分類とコンポーネント

アラートに含まれる情報は、アラートの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。

アラートの分類

AsyncOS は以下のタイプのアラートを送信します。

- システム（System）
- ハードウェア（Hardware）
- アップデータ（Updater）
- Web プロキシ（Web Proxy）
- マルウェア対策（Anti-Malware）
- L4 トラフィック モニタ（L4 Traffic Monitor）

アラートの重大度

アラートは、次の重大度に従って送信されます。

- **クリティカル**：ただちに対処する必要があります。
- **警告**：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場合もあります。
- **情報**：デバイスのルーティン機能で生成される情報。

アラート受信者の管理

（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。

アラート受信者の追加および編集

ステップ 1　[システム管理（System Administration）] > [アラート（Alerts）] を選択します。

ステップ 2　[アラート受信者（Alert Recipients）] リストで受信者をクリックして編集するか、[受信者の追加（Add Recipient）] をクリックして新しい受信者を追加します。

ステップ 3　受信者の電子メール アドレスを追加または編集します。複数のアドレスをカンマで区切って入力することもできます。

ステップ 4　各アラート タイプごとに、受信するアラートの重大度を選択します。

ステップ 5　変更を送信し、保存します。

アラート受信者の削除

ステップ 1　[システム管理（System Administration）] > [アラート（Alerts）] を選択します。

ステップ 2　[アラート受信者（Alert Recipient）] のリストで、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て確定します。

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。

ステップ 1　[システム管理（System Administration）] > [アラート（Alerts）] 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。

ステップ 3　必要に応じて、アラートの設定値を設定します。

オプション	説明
アラートの送信元アドレス（From Address to Use When Sending Alerts）	アラートを送信するときに使用する RFC 2822 準拠の「Header From:」アドレス。システムのホスト名（「alert@<hostname>」）に基づいてアドレスを自動生成するオプションが用意されています。
重複アラート送信時の待ち時間（Wait Before Sending a Duplicate Alert）	重複アラートの時間間隔を指定します。2 つの設定があります。 [重複アラート初回送信時の待ち時間（秒）（Initial Number of Seconds to Wait Before Sending a Duplicate Alert）]。この値を 0 に設定した場合、重複したアラートのサマリーは送信されず、代わりにすべての重複したアラートがリアルタイムに送信されます（短時間に大量の電子メールを受信する可能性があります）。重複したアラートを送信するまでに待機する秒数は、アラートを送信するたびに増加します。増加する秒数は、前回の待機間隔の 2 倍の値を足した秒数です。つまり、この値を 5 秒に設定すると、アラートは 5 秒後、15 秒後、35 秒後、75 秒後、155 秒後、315 秒後といった間隔で送信されます。 [重複アラート送信時の最大待ち時間（秒）（Maximum Number of Seconds to Wait Before Sending a Duplicate Alert）]。[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、15 秒、35 秒、60 秒、120 秒などの間隔で送信されます。

オプション	説明
Cisco AutoSupport	シスコに以下の情報を送信するかどうかを指定します。 • システムで生成されたすべてのアラート メッセージのコピー • 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週報 また、シスコに送信したあらゆるメッセージのコピーを内部のアラート受信者に送信するかどうかを指定します。これは、重大度が「情報（Information）」のシステム アラートを受信するよう設定されている受信者にのみ適用されます。

ステップ 4　変更を送信し、保存します。

アラート リスト

以下の項では、分類別にアラートを一覧表示します。各項の表には、アラート名（内部で使用される descriptor）、アラートの実際のテキスト、説明、重大度（クリティカル、情報、または警告）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。

機能キー アラート

以下の表は、AsyncOS で生成されるさまざまな機能キー アラートのリストです。アラートの説明と重大度が記載されています。

メッセージ	アラートの重大度	パラメータ
A “$feature” key was downloaded from the key server and placed into the pending area. EULA acceptance required.	情報（Information）。	**$feature**：機能の名前。
Your “$feature” evaluation key has expired. Please contact your authorized sales representative.	警告（Warning）。	**$feature**：機能の名前。
Your “$feature” evaluation key will expire in under $days day(s). Please contact your authorized sales representative.	警告（Warning）。	**$feature**：機能の名前。 **$days**：機能キーの期限が切れるまでの日数。

ハードウェア アラート

以下の表は、AsyncOS で生成されるさまざまなハードウェア アラートのリストです。アラートの説明と重大度が記載されています。

メッセージ	アラートの重大度	パラメータ
A RAID-event has occurred: $error	警告（Warning）	**$error**：RAID エラーのテキスト。

ロギング アラート

以下の表は、AsyncOS で生成されるさまざまなロギング アラートのリストです。アラートの説明と重大度が記載されています。

メッセージ	アラートの重大度	パラメータ
$error.	情報（Information）。	**$error**：エラーのトレースバック文字列。
Log Error: Subscription $name: Log partition is full.	クリティカル（Critical）。	**$name**：ログ サブスクリプション名。
Log Error: Push error for subscription $name: Failed to connect to $ip: $reason.	クリティカル（Critical）。	**$name**：ログ サブスクリプション名。 **$ip**：リモート ホストの IP アドレス。 **$reason**：接続エラーについて説明するテキスト。
Log Error: Push error for subscription $name: An FTP command failed to $ip: $reason.	クリティカル（Critical）。	**$name**：ログ サブスクリプション名。 **$ip**：リモート ホストの IP アドレス。 **$reason**：問題点について説明するテキスト。
Log Error: Push error for subscription $name: SCP failed to transfer to $ip:$port: $reason',	クリティカル（Critical）。	**$name**：ログ サブスクリプション名。 **$ip**：リモート ホストの IP アドレス。 **$port**：リモート ホストのポート番号。 **$reason**：問題点について説明するテキスト。
Log Error: 'Subscription $name: Failed to connect to $hostname ($ip): $error.	クリティカル（Critical）。	**$name**：ログ サブスクリプション名。 **$hostname**：Syslog サーバのホスト名。 **$ip**：Syslog サーバの IP アドレス。 **$error**：エラー メッセージのテキスト。
Log Error: Subscription $name: Network error while sending log data to syslog server $hostname ($ip): $error	クリティカル（Critical）。	**$name**：ログ サブスクリプション名。 **$hostname**：Syslog サーバのホスト名。 **$ip**：Syslog サーバの IP アドレス。 **$error**：エラー メッセージのテキスト。
Subscription $name: Timed out after $timeout seconds sending data to syslog server $hostname ($ip).	クリティカル（Critical）。	**$name**：ログ サブスクリプション名。 **$timeout**：秒単位のタイムアウト。 **$hostname**：Syslog サーバのホスト名。 **$ip**：Syslog サーバの IP アドレス。
Subscription $name: Syslog server $hostname ($ip) is not accepting data fast enough.	クリティカル（Critical）。	**$name**：ログ サブスクリプション名。 **$hostname**：Syslog サーバのホスト名。 **$ip**：Syslog サーバの IP アドレス。
Subscription $name: Oldest log file(s) were removed because log files reached the maximum number of $max_num_files. Files removed include: $files_removed.	情報（Information）。	**$name**：ログ サブスクリプション名。 **$max_num_files**：ログ サブスクリプションごとに許可されるファイルの最大数。 **$files_removed**：削除されたファイルのリスト。

レポート アラート

以下の表は、AsyncOS で生成されるさまざまなレポート アラートのリストです。アラートの説明と重大度が記載されています。

メッセージ	アラートの重大度	パラメータ
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。	適用なし
The reporting system is now able to handle new data.	情報（Information）。	適用なし
A failure occurred while building periodic report ‘$report_title’. This subscription should be examined and deleted if its configuration details are no longer valid.	クリティカル（Critical）。	**$report_title**：レポートのタイトル。
A failure occurred while emailing periodic report ‘$report_title’. This subscription has been removed from the scheduler.	クリティカル（Critical）。	**$report_title**：レポートのタイトル。
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 $threshold percent, full processing of reporting data will be restarted automatically.	警告（Warning）。	**$threshold:**：しきい値。
PERIODIC REPORTS: While building periodic report $report_title' the expected domain specification file could not be found at ‘$file_name’. No reports were sent.	クリティカル（Critical）。	**$report_title**：レポートのタイトル。 **$file_name**：ファイルの名前。
Counter group “$counter_group” does not exist.	クリティカル（Critical）。	**$counter_group**：counter_group の名前。
PERIODIC REPORTS: While building periodic report $report_title’ the domain specification file ‘$file_name’ was empty. No reports were sent.	クリティカル（Critical）。	**$report_title**：レポートのタイトル。 **$file_name**：ファイルの名前。
PERIODIC REPORTS: Errors were encountered while processing the domain specification file ‘$file_name’ for the periodic report ‘$report_title’. Any line which has any reported problem had no report sent. $error_text	クリティカル（Critical）。	**$report_title**：レポートのタイトル。 **$file_name**：ファイルの名前。 **$error_text**：発生したエラーのリスト。

メッセージ	アラートの重大度	パラメータ
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 $threshold percent, full processing of reporting data will be restarted automatically.	警告（Warning）。	**$threshold**：しきい値。
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: $err_msg	クリティカル（Critical）。	**$err_msg**：エラー メッセージ テキスト。

システム アラート

以下の表は、AsyncOS で生成されるさまざまなシステム アラートのリストです。アラートの説明と重大度が記載されています。

メッセージ	アラートの重大度	パラメータ
Startup script $name exited with error: $message	クリティカル（Critical）。	**$name**：スクリプトの名前。 **$message**：エラー メッセージ テキスト。
System halt failed: $exit_status: $output',	クリティカル（Critical）。	**$exit_status**：コマンドの終了コード。 **$output**：コマンドからの出力。
System reboot failed: $exit_status: $output	クリティカル（Critical）。	**$exit_status**：コマンドの終了コード。 **$output**：コマンドからの出力。
Process $name listed $dependency as a dependency, but it does not exist.	クリティカル（Critical）。	**$name**：プロセスの名前。 **$dependency**：一覧表示されている依存性の名前。
Process $name listed $dependency as a dependency, but $dependency is not a wait_init process.	クリティカル（Critical）。	**$name**：プロセスの名前。 **$dependency**：一覧表示されている依存性の名前。
Process $name listed itself as a dependency.	クリティカル（Critical）。	**$name**：プロセスの名前。
Process $name listed $dependency as a dependency multiple times.	クリティカル（Critical）。	**$name**：プロセスの名前。 **$dependency**：一覧表示されている依存性の名前。
Dependency cycle detected: $cycle.	クリティカル（Critical）。	**$cycle**：サイクルに関係するプロセス名のリスト。

メッセージ	アラートの重大度	パラメータ
An error occurred while attempting to share statistical data through the Network Participation feature. Please forward this tracking information to your support provider: Error: $error.	警告（Warning）。	**$error**：例外に関連付けられたエラー メッセージ。
There is an error with “$name”.	クリティカル（Critical）。	**$name**：コア ファイルを生成したプロセスの名前。
An application fault occurred: “$error”	クリティカル（Critical）。	**$error**：エラーのテキスト（通常はトレースバック）。
Tech support: Service tunnel has been enabled, port $port	情報（Information）。	**$port**：サービス トンネルに使用されるポート番号。
Tech support: Service tunnel has been disabled.	情報（Information）。	適用なし
• The host at $ip has been added to the blacklist because of an SSH DOS attack. • The host at $ip has been permanently added to the ssh whitelist. • The host at $ip has been removed from the blacklist	警告（Warning）。	**$ip**：ログインが試行された IP アドレス。 **説明：** SSH を介してアプライアンスへの接続を試みているが、有効なクレデンシャルを提示しない IP アドレスは、2 分以内に 11 回以上試行に失敗した場合、SSH のブラックリストに追加されます。 同じ IP アドレスからユーザが正常にログインすると、その IP アドレスはホワイトリストに追加されます。 ホワイトリストのアドレスは、ブラックリストにも登録されていてもアクセスが許可されます。 約 1 日経過後にそのエントリはブラックリストから自動的に削除されます。

アップデータ アラート

以下の表は、AsyncOS で生成されるさまざまなアップデータ アラートのリストです。アラートの説明と重大度が記載されています。

メッセージ	アラートの重大度	パラメータ
The $app application tried and failed $attempts times to successfully complete an update. This may be due to a network configuration issue or temporary outage.	警告（Warning）。	**$app** Web セキュリティ アプライアンス：セキュリティ サービス名。 **$attempts**：試行回数。
The updater has been unable to communicate with the update server for at least $threshold.	警告（Warning）。	**$threshold:**：しきい値の時間。
Unknown error occurred: $traceback.	クリティカル（Critical）。	**$traceback**：トレースバック情報。

マルウェア対策アラート

高度なマルウェア対策に関連するアラートについては、Ensuring That You Receive Alerts About Advanced Malware Protection Issues（14-10 ページ）を参照してください。

システムの日時の管理

時間帯の設定

ステップ 1　[システム管理（System Administration）] > [タイム ゾーン（Time Zone）] 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。

ステップ 3　地域、国、およびタイム ゾーンを選択するか、GMT オフセットを選択します。

ステップ 4　変更を送信し、保存します。

NTP サーバによるシステム クロックの同期

アプライアンスで手動で時間を設定するのではなく、ネットワーク タイム プロトコル（NTP）サーバに照会して現在の日時を追跡できるように、Web セキュリティ アプライアンスを設定することをお勧めします。これは、特にアプライアンスが他のデバイスと統合されている場合に該当します。統合されたすべてのデバイスが同じ NTP サーバを使用する必要があります。

ステップ 1　[システム管理（System Administration）] > [時間の設定（Time Settings）] 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。

ステップ 3　[時刻の設定方法（Time Keeping Method）] として [NTP（Network Time Protocol）を使用（Use Network Time Protocol）] を選択します。

ステップ 4　サーバの追加が必要な場合は、[行の追加（Add Row）] をクリックして、NTP サーバの完全修飾ホスト名または IP アドレスを入力します。

ステップ 5　（任意）NTP クエリーに使用するアプライアンスのネットワーク インターフェイス タイプ（管理またはデータのいずれか）に関連付けられている、ルーティング テーブルを選択します。これは、NTP クエリーが発信される IP アドレスになります。

（注）　このオプションは、アプライアンスがデータ トラフィック用と管理トラフィック用に分割ルーティングを使用している場合にのみ変更できます。

ステップ 6　変更を送信し、保存します。

SSL の設定

セキュリティを向上させるために、いくつかのサービスで SSL v3 とさまざまなバージョンの TLS をイネーブルまたはディセーブルにできます。最善のセキュリティを実現するために、すべてのサービスで SSL v3 をディセーブルにすることをお勧めします。デフォルトでは、すべてのバージョンの TLS がイネーブルに設定され、SSL がディセーブルに設定されます。

（注） これらの機能は、`sslconfig` CLI コマンドを使用してイネーブルまたはディセーブルにすることもできます。Web セキュリティ アプライアンスの CLI コマンド（B-6 ページ）を参照してください。

ステップ 1　[システム管理（System Administration）] > [SSL 設定（SSL Configuration）] 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。

ステップ 3　これらのサービスで SSL v3 と TLS v1.x をイネーブルにするには、対応するチェックボックスをオンにします。

- [アプライアンス管理 Web ユーザインターフェイス（Appliance Management Web User Interface）]：この設定を変更すると、すべてのアクティブ ユーザの接続が切断されます。
- [プロキシ サービス（Proxy Services）]：セキュア クライアント用の HTTPS プロキシとクレデンシャル暗号化が含まれます。このセクションには以下も含まれています。
  - [使用する暗号（Cipher(s) to Use）]：プロキシ サービスとの通信に使用する追加の暗号スイートを入力できます。スイートの区切りにはコロン（:）を使用します。特定の暗号の使用を防止するには、その文字列の先頭に感嘆符（!）を追加します。たとえば `!EXP-DHE-RSA-DES-CBC-SHA` と入力します。

    確認済みの TLS/SSL バージョンに適切なスイートのみを入力するようにしてください。詳細および暗号リストについては、https://www.openssl.org/docs/manmaster/apps/ciphers.html を参照してください。

    AsyncOS バージョン 9.0 以前のデフォルトの暗号は、`DEFAULT:+kEDH` です。AsyncOS バージョン 9.1 以降では、デフォルトの暗号は `EECDH:DSS:RSA:!NULL:!eNULL:!EXPORT:!3DES:!RC4:!RC2:!DES:!SEED:!CAMELLIA:!SRP:!IDEA:!ECDHE-ECDSA-AES256-SHA:!ECDHE-RSA-AES256-SHA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA` になります。いずれの場合も、ECDHE 暗号の選択によって変わる可能性があります。

    （注） ただし、バージョンに関係なく、新しい AsyncOS バージョンにアップグレードする際にデフォルトの暗号は変わりません。たとえば、以前のバージョンから AsyncOS 9.1 にアップグレードする場合、デフォルトの暗号は `DEFAULT:+kEDH` です。つまり、アップグレード後に、現在の暗号スイートを自分で更新する必要があります。シスコでは、`EECDH:DSS:RSA:!NULL:!eNULL:!EXPORT:!3DES:!RC4:!RC2:!DES:!SEED:!CAMELLIA:!SRP:!IDEA:!ECDHE-ECDSA-AES256-SHA:!ECDHE-RSA-AES256-SHA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA` への更新を推奨します。
  - [TLS 圧縮の無効化（推奨）（Disable TLS Compression (Recommended)）]：TLS 圧縮を無効にするには、このチェックボックスをオンにします。最善のセキュリティを実現するには、この設定が推奨されます。
- [セキュア LDAP サービス（Secure LDAP Services）]：認証、外部認証、セキュア モビリティが含まれます。

- [セキュア ICAP サービス（外部DLP）（Secure ICAP Services (External DLP)）]：アプライアンスと外部 DLP（データ漏洩防止）サーバ間の ICAP 通信の保護に使用するプロトコルを選択します。詳細については、Configuring External DLP Servers（16-9 ページ）を参照してください。
- [サービスの更新（Update Service）]：アプライアンスと利用可能なアップデート サーバ間の通信に使用するプロトコルを選択します。サービスの更新の詳細については、AsyncOS for Web のアップグレードとアップデート（12-27 ページ）を参照してください。

（注）　シスコのアップデート サーバは SSL v3 をサポートしていません。したがって、TLS 1.0 以上を Cisco アップデート サービスでイネーブルにしておく必要があります。ただし、ローカル アップデート サーバでは現在も SSL v3 を使用することができます（そのように設定されている場合）。それらのサーバでサポートされている SSL/TLS のバージョンを確認してください。

ステップ 4　[送信（Submit）] をクリックします。

証明書の管理

アプライアンスでは、デジタル証明書を使用してさまざまな接続を確立、確認、保護します。[証明書の管理（Certificate Management）] ページでは、現在の証明書リストの表示や更新、信頼できるルート証明書の管理、およびブロックされた証明書の表示を行うことができます。

関連項目

- 証明書およびキーについて（12-23 ページ）
- 証明書の更新（12-24 ページ）
- 信頼できるルート証明書の管理（12-24 ページ）
- ブロックされた証明書の表示（12-24 ページ）

証明書およびキーについて

ユーザに認証を要求するときに、ブラウザはセキュア HTTPS 接続を使用して Web プロキシに認証クレデンシャルを送信します。Web セキュリティ アプライアンスは、デフォルトで付属の「Cisco Web セキュリティ アプライアンス デモ証明書（Cisco Web Security Appliance Demo Certificate）」を使用して、クライアントとの HTTPS 接続を確立します。多くのブラウザでは、証明書が無効であるという内容の警告が表示されます。無効な証明書に関するメッセージをユーザに表示しないようにするには、アプリケーションで自動的に認識される証明書とキーのペアをアップロードします。

関連項目

- 証明書とキーのアップロードまたは生成（12-25 ページ）
- 証明書署名要求（12-26 ページ）
- 中間証明書（12-27 ページ）

信頼できるルート証明書の管理

Web セキュリティ アプライアンスには、信頼できるルート証明書のリストが付属しており、これが維持されます。信頼できる証明書を持つ Web サイトでは、復号化は必要ありません。

信頼できる証明書のリストに証明書を追加し、機能的に証明書を削除すると、信頼できる証明書のリストを管理できます。Web セキュリティ アプライアンスは、マスター リストからは証明書を削除しませんが、証明書の信頼を無効にすることができます。これで、信頼できるリストから機能的に証明書が削除されます。

信頼できるルート証明書を追加、上書き、ダウンロードするには、以下の手順を実行します。

ステップ 1　[ネットワーク（Network）] > [証明書の管理（Certificate Management）] の順に選択します。

ステップ 2　[証明書の管理（Certificate Management）] ページの [信頼できるルート証明書の管理（Manage Trusted Root Certificates）] をクリックします。

ステップ 3　シスコ認識済みリストに記載されていない認証局の署名が付いたカスタムの信頼できるルート証明書を追加するには、以下の手順を実行します。

[インポート（Import）] をクリックし、証明書ファイルを参照して選択し、[送信（Submit）] します。

ステップ 4　1 つ以上のシスコ認識済み証明書の信頼を上書きするには、以下の手順を実行します。

a.　上書きする各エントリの [信頼を上書き（Override Trust）] チェックボックスをオンにします。

b.　[送信（Submit）] をクリックします。

ステップ 5　特定の証明書のコピーをダウンロードするには、以下の手順を実行します。

a.　シスコの信頼できるルート証明書リストで証明書の名前をクリックし、エントリを展開します。

b.　[証明書をダウンロード（Download Certificate）] をクリックします。

証明書の更新

[更新（Updates）] セクションには、アプライアンス上のシスコの信頼できるルート証明書とブラックリストのバンドルについて、バージョン情報と最終更新情報が一覧表示されます。これらのバンドルは定期的に更新されます。

ステップ 1　[証明書の管理（Certificate Management）] ページで [今すぐ更新（Update Now）] をクリックし、アップデート可能なすべてのバンドルを更新します。

ブロックされた証明書の表示

シスコにより無効であると判定されてブロックされた証明書のリストを表示するには、以下の手順を実行します。

ステップ 1　[ブロック済み証明書を表示（View Blocked Certificates）] をクリックします。

証明書とキーのアップロードまたは生成

AsyncOS 機能によっては、接続を確立、確認、保護するために証明書とキーが必要です。既存の証明書とキーをアップロードしたり、機能を設定するときに新しい証明書とキーを生成したりできます。

証明書およびキーのアップロード

アプライアンスにアップロードする証明書は、以下の要件を満たしている必要があります。

- X.509 標準を使用していること。
- 一致する秘密キーが PEM 形式で含まれていること。DER 形式はサポートされていません。

ステップ 1　[アップロードされた証明書とキーを使用（Use Uploaded Certificate and Key）] を選択します。

ステップ 2　[証明書（Certificate] フィールドで [参照（Browse）] をクリックし、アップロードするファイルを検索します。

（注）　Web プロキシは、ファイル内の最初の証明書またはキーを使用します。証明書ファイルは PEM 形式にする必要があります。DER 形式はサポートされていません。

ステップ 3　[キー（Key）] フィールドで [参照（Browse）] をクリックし、アップロードするファイルを指定します。

（注）　キーの長さは 512、1024、または 2048 ビットである必要があります。秘密キー ファイルは PEM 形式でなければなりません。DER 形式はサポートされていません。

ステップ 4　キーが暗号化されている場合は、[キーは暗号化されています（Key is Encrypted）] を選択します。

ステップ 5　[ファイルのアップロード（Upload File）] をクリックします。

証明書およびキーの生成

ステップ 1　[生成された証明書とキーを使用（Use Generated Certificate and Key）] を選択します。

ステップ 2　[新しい証明書とキーを生成（Generate New Certificate and Key）] をクリックします。

a.　[証明書とキーを生成（Generate Certificate and Key）] ダイアログボックスで、必要な生成情報を入力します。

（注）　[共通名（Common Name）] フィールドには、スラッシュ（/）を除く任意の ASCII 文字を入力できます。

b. [証明書とキーを生成（Generate Certificate and Key）] ダイアログボックスで、[生成（Generate）] をクリックします。

生成が完了すると、[証明書（Certificate）] セクションに、証明書の情報と 2 つのリンク（[証明書をダウンロードDownload Certificate] と [証明書署名要求のダウンロード（Download Certificate Signing Request）]）が表示されます。また、認証局（CA）から署名付き証明書を受信したときに、それをアップロードするために使用する [署名付き証明書（Signed Certificate）] オプションも表示されます。

ステップ 3　[証明書をダウンロードDownload Certificate] をクリックして、アプライアンスにアップロードする新しい証明書をダウンロードします。

ステップ 4　[証明書署名要求のダウンロード（Download Certificate Signing Request）] をクリックして、署名のために認証局（CA）に送信する新しい証明書ファイルをダウンロードします。この処理の詳細については、証明書署名要求（12-26 ページ）を参照してください。

a. CA から署名付き証明書が返送されたら、[証明書（Certificate）] フィールドの [署名付き証明書（Signed Certificate）] で [参照（Browse）] をクリックして、署名付き証明書ファイルを指定し、[ファイルのアップロード（Upload File）] をクリックしてアプライアンスにアップロードします。

b. CA のルート証明書がアプライアンスの信頼できるルート証明書リストに含まれていることを確認します。リストにない場合は追加します。詳細については、信頼できるルート証明書の管理（12-24 ページ）を参照してください。

証明書署名要求

Web セキュリティ アプライアンスは、アプライアンスにアップロードされた証明書の証明書署名要求（CSR）を生成することはできません。そのため、アプライアンス用に作成された証明書を使用するには、別のシステムから署名要求を発行する必要があります。後でアプライアンスにインストールする必要があるため、このシステムから PEM 形式のキーを保存します。

最新バージョンの OpenSSL がインストールされた、任意の UNIX マシンを使用できます。CSR にアプライアンスのホスト名があることを確認してください。OpenSSL を使用した CSR の生成の詳細については、以下の場所にあるガイドラインを参照してください。

`http://www.modssl.org/docs/2.8/ssl_faq.html#ToC28`

CSR が生成されたら、認証局（CA）に送信します。CA は、証明書を PEM 形式で返します。

初めて証明書を取得する場合は、インターネットで「certificate authority services SSL server certificates（SSL サーバ証明書を提供している認証局）」を検索して、環境のニーズに最も適したサービスを選択します。サービスの手順に従って、SSL 証明書を取得します。

（注）　独自の証明書を生成して署名することもできます。そのためのツールは `http://www.openssl.org` の無料のソフトウェア OpenSSL に含まれています。

中間証明書

ルート認証局（CA）の証明書検証に加えて、AsyncOS では、中間証明書の検証の使用もサポートされます。中間証明書とは信頼できるルート認証局によって発行された証明書であり、追加の証明書を作成するために使用されます。これは、信頼の連鎖を作成します。たとえば、信頼できるルート認証局によって証明書を発行する権利が与えられた example.com によって証明書が発行されたとします。example.com によって発行された証明書は、example.com の秘密キーおよび信頼できるルート認証局の秘密キーと照合して検証する必要があります。

AsyncOS for Web のアップグレードとアップデート

シスコでは、AsyncOS for Web とそのコンポーネント向けに、アップグレード（新しいソフトウェア バージョン）とアップデート（現在のソフトウェア バージョンの変更）を定期的にリリースしています。

ハイブリッド モードでは、アップグレードは、使用可能な場合は自動的にダウンロードされ、指定された時間帯でインストールされます。現在の時間帯を変更するには、次の手順を実行します。

ステップ 1　[システム管理（System Administration）] > [アップグレードとアップデートの設定（Upgrade and Update Settings）] を選択します。

ステップ 2　[アップグレードのタイミングの編集（Edit Upgrade Timing）] をクリックします。

ステップ 3　アップグレードのインストールを開始する [曜日（Day of Week）] と [時間（Time）] の時間および分を選択して、アップグレードの時間帯を定義します。

アップグレード/更新プログラムのインストールを開始する 2 時間の枠の始まりを定義します。インストールが完了するとアプライアンスが再起動するため、できるだけ影響の少ない時間を指定します。

ステップ 4　次回のアップグレードのインストール予定を変更するには、[次のターゲット アップグレードの例外を設定（Set Exception for Next Target Upgrade）] をオンにしてから [例外の日付（Exception Date）] を選択し、例外開始 [時間（Time）] の時間および分を選択します。

これは、デフォルトの日時に優先する一度限りの例外です。つまり、デフォルトの日時よりも前に保留中のアップグレードをインストールしたり、デフォルトの日時を無視して以降の日時でアップグレードをインストールする「ブラックアウトの時間帯」を設定したりすることができます。

ステップ 5　[送信（Submit）] をクリックします。

SNMP を使用したシステムの状態のモニタリング

AsyncOS オペレーティング システムは、SNMP（シンプル ネットワーク管理プロトコル）を使用したシステム ステータスのモニタリングをサポートしています。（SNMP の詳細については、RFC 1065、1066、および 1067 を参照してください）。

以下の点に注意してください。

- SNMP は、デフォルトで**オフ**になります。
- SNMP SET 動作（コンフィギュレーション）は実装されません。
- AsyncOS は SNMPv1、v2、および v3 をサポートしています。SNMPv3 の詳細については、RFC 2571-2575 を参照してください。

- SNMPv3 をイネーブルにする場合、メッセージ認証と暗号化は必須です。認証のパスフレーズと暗号は異なっていなければなりません。暗号化アルゴリズムには AES（推奨）または DES を指定できます。認証アルゴリズムには SHA-1（推奨）または MD5 を指定できます。次に `snmpconfig` コマンドを実行する際には、コマンドにこのパスフレーズが「記憶」されています。
- SNMPv3 ユーザ名は v3get です。

```
> snmpwalk -v 3 -l AuthNoPriv -u v3get -a MD5 serv.example.com
```

- SNMPv1 または SNMPv2 のみを使用する場合は、コミュニティ ストリングを設定する必要があります。コミュニティ ストリングは、`public` にデフォルト設定されません。
- SNMPv1 および SNMPv2 の場合、どのネットワークからの SNMP GET 要求を受け入れるかを指定する必要があります。
- トラップを使用するには、SNMP マネージャ（AsyncOS には含まれていません）が実行中であり、その IP アドレスがトラップ ターゲットとして入力されている必要があります（ホスト名を使用できますが、その場合、トラップは DNS が動作しているときにのみ機能します）。

MIB ファイル

MIBファイルは http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html から入手できます。各 MIB ファイルの最新バージョンを使用します。

以下の複数の MIB ファイルがあります。

- syncoswebsecurityappliance-mib.txt：Web セキュリティ アプライアンス用のエンタープライズ MIB の SNMPv2 互換の説明。
- ASYNCOS-MAIL-MIB.txt：電子メール セキュリティ アプライアンス用のエンタープライズ MIB の SNMPv2 互換の説明。
- IRONPORT-SMI.txt：この「管理情報構造」ファイルは、asyncoswebsecurityappliance-mib の役割を定義します。

このリリースには、RFC 1213 および 1907 に規定されている MIB-II の読み取り専用のサブセットが実装されています。

SNMP モニタリングのイネーブル化と設定

アプライアンスのシステム ステータス情報を収集するように SNMP を設定するには、コマンドライン インターフェイス（CLI）で `snmpconfig` コマンドを使用します。インターフェイスの値を選択し、設定し終えると、アプライアンスは SNMPv3 GET 要求に応答します。

SNMP モニタリングを使用する場合、以下の点に注意してください。

- これらのバージョン 3 要求には、一致するパスフレーズが含まれている必要があります。
- デフォルトでは、バージョン 1 および 2 要求は拒否されます。
- イネーブルにする場合は、バージョン 1 および 2 要求に一致するコミュニティ ストリングが含まれている必要があります。

ハードウェア オブジェクト

Intelligent Platform Management Interface Specification（IPMI）準拠のハードウェア センサーによって、温度、ファン スピード、電源モジュール ステータスなどの情報が報告されます。

モニタリング可能なハードウェア関連のオブジェクト（ファンの数や動作温度範囲など）を決定するには、アプライアンス モデルのハードウェア ガイドを参照してください。

関連項目

- ドキュメント セット（C-2 ページ）

SNMP トラップ

SNMP には、1 つまたは複数の条件が合致したときにトラップ（または通知）を送信して管理アプリケーションに知らせる機能が備わっています。トラップとは、トラップを送信するシステムのコンポーネントに関するデータを含むネットワーク パケットです。トラップは、SNMP エージェント（この場合は Cisco Web セキュリティ アプライアンス アプライアンス）で、ある条件が満たされた場合に生成されます。条件が満たされると、SNMP エージェントは SNMP パケットを形成し、SNMP 管理コンソール ソフトウェアが稼働するホストに送信します。

インターフェイスに対して SNMP をイネーブルにするときに、SNMP トラップを設定（特定のトラップをイネーブル化またはディセーブル化）できます。

複数のトラップ ターゲットの指定方法: トラップ ターゲットの入力を求められたときに、カンマで区切った IP アドレスを 10 個まで入力できます。

関連項目

- SNMP の connectivityFailure トラップについて（12-29 ページ）

SNMP の connectivityFailure トラップについて

connectivityFailure トラップは、インターネットへのアプライアンスの接続をモニタするために使用されます。これは、5～7 秒ごとに 1 つの外部サーバに接続して HTTP GET 要求を送信する試みにより実行されます。デフォルトでは、モニタされる URL はポート 80 上の `downloads.ironport.com` です。

モニタする URL またはポートを変更するには、`snmpconfig` コマンドを実行し、connecivityFailure トラップをイネーブルにします（すでにイネーブルになっている場合も実行します）。URL を変更するプロンプトが表示されます。

ヒント　connectivityFailure トラップをシミュレートするために、`dnsconfig` CLI コマンドを使用して、未使用の DNS サーバを入力することができます。downloads.ironport.com の検索は失敗し、5～7 秒ごとにトラップが送信されます。テストが完了したら、DNS サーバを使用中のサーバーに戻してください。

CLI の例 : snmpconfig

```
wsa.example.com> snmpconfig

Current SNMP settings:
SNMP Disabled.

Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]> SETUP

Do you want to enable SNMP?
[Y]>

Please choose an IP interface for SNMP requests.
1. Management (198.51.100.1: wsa.example.com)
[1]>

Which port shall the SNMP daemon listen on interface "Management"?
[161]>

Please select SNMPv3 authentication type:
1. MD5
2. SHA
[1]> 2

Please select SNMPv3 privacy protocol:
1. DES
2. AES
[1]> 2

Enter the SNMPv3 authentication passphrase.
[]>
Please enter the SNMPv3 authentication passphrase again to confirm.
[]>
Enter the SNMPv3 privacy passphrase.
[]>
Please enter the SNMPv3 privacy passphrase again to confirm.
[]>

Service SNMP V1/V2c requests?
[N]> Y

Enter the SNMP V1/V2c community string.
[ironport]> public

Shall SNMP V2c requests be serviced from IPv4 addresses?
[Y]>

From which IPv4 networks shall SNMP V1/V2c requests be allowed? Separate
multiple networks with commas.
[127.0.0.1/32]>

Enter the Trap target as a host name, IP address or list of IP
addresses separated by commas (IP address preferred). Enter "None" to disable traps.
[127.0.0.1]> 203.0.113.1

Enter the Trap Community string.
[ironport]> tcomm

Enterprise Trap Status
1. CPUUtilizationExceeded       Disabled
2. FIPSModeDisableFailure       Enabled
```

```
3. FIPSModeEnableFailure        Enabled
4. FailoverHealthy              Enabled
5. FailoverUnhealthy            Enabled
6. RAIDStatusChange             Enabled
7. connectivityFailure          Disabled
8. fanFailure                   Enabled
9. highTemperature              Enabled
10. keyExpiration               Enabled
11. linkUpDown                  Enabled
12. memoryUtilizationExceeded   Disabled
13. powerSupplyStatusChange     Enabled
14. resourceConservationMode    Enabled
15. updateFailure               Enabled
Do you want to change any of these settings?
[N]> Y

Do you want to disable any of these traps?
[Y]> n

Do you want to enable any of these traps?
[Y]> y

Enter number or numbers of traps to enable. Separate multiple numbers with
commas.
[]> 1,7,12

What threshold would you like to set for CPU utilization?
[95]>

What URL would you like to check for connectivity failure?
[http://downloads.ironport.com]>

What threshold would you like to set for memory utilization?
[95]>

Enter the System Location string.
[Unknown: Not Yet Configured]> Network Operations Center - west; rack #30, position 3

Enter the System Contact string.
[snmp@localhost]> wsa-admin@example.com

Current SNMP settings:
Listening on interface "Management" 198.51.100.1 port 161.
SNMP v3: Enabled.
SNMP v1/v2: Enabled, accepting requests from subnet 127.0.0.1/32 .
SNMP v1/v2 Community String: public
Trap target: 203.0.113.1
Location: Network Operations Center - west; rack #30, position 3
System Contact: wsa-admin@example.com

Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]>

wsa.example.com> commit

Please enter some comments describing your changes:
[]> Enable and configure SNMP

Changes committed: Fri Nov 06 18:13:16 2015 GMT
wsa.example.com>
```

トラブルシューティング

一般的なトラブルシューティングとベスト プラクティス

以下のカスタム フィールドを含むようにアクセス ログを設定します。

%u、%g、%m、%k、%L（これらの値は大文字と小文字が区別されます）。

これらのフィールドの説明については、アクセス ログのフォーマット指定子と W3C ログ ファイルのフィールド（11-35 ページ）を参照してください。

設定の手順については、アクセス ログのカスタマイズ（11-30 ページ）およびログ サブスクリプションの追加と編集（11-8 ページ）を参照してください。

ハイブリッド Web セキュリティ の問題

登録(エンロールメントを含む)

- API ゲートウェイと Enrollment over Secure Transport(EST)サーバ間の接続エラー:ログをトレース レベルに設定してログをキャプチャし、サポートに問い合わせます。
- API ゲートウェイと EST サーバのルート証明書が WSA に存在しないことによる接続の失敗:ログをトレース レベルに設定してログをキャプチャし、サポートに問い合わせます。
- 無効な認証キー:新しいキーを試します。失敗する場合は、サポートに問い合わせます。

ポリシーのダウンロード

- API ゲートウェイとの接続エラー:サポートに問い合わせます。

ポリシーの変換

- AVC の不一致:CLI `updatenow` コマンドを使用して WSA で強制的に更新を実行します。失敗する場合は、サポートに問い合わせます。
- AVC、Sophos などのさまざまなモジュールの動的更新が受信されない:CLI `updatenow` コマンドを使用して WSA で強制的に更新を実行します。失敗する場合は、サポートに問い合わせます。
- 変換に時間がかかり(20 分以上)、タイムアウトする:サポートに問い合わせます。

ハイブリッド アップグレード

- 接続エラー:サポートに問い合わせます。
- アップグレード サーバ証明書の検証の失敗:アップグレード サーバとの接続を確認します。失敗する場合は、サポートに問い合わせます。
- アップグレード イメージのダウンロードの失敗:アップグレード サーバとの接続を確認します。失敗する場合は、サポートに問い合わせます。
- アップグレード自体の失敗:サポートに問い合わせます。
- アップグレードの時間帯の設定エラー:ソフトウェア セットアップ ウィザードを使用して WSA で設定したタイムゾーンを確認します。

ブラウザに関する問題

Firefox で WPAD を使用できない

Firefox ブラウザが WPAD による DHCP ルックアップをサポートしていない可能性があります。最新の情報については、`https://bugzilla.mozilla.org/show_bug.cgi?id=356831` を参照してください。

PAC ファイルが Web Security Appliance にホストされている場合に、Firefox（または、DHCP をサポートしていない他のブラウザ）で WPAD を使用するには、ポート 80 を介して PAC ファイルを使用するようにアプライアンスを設定します。

ステップ 1　[セキュリティサービス（Security Services）] > [Web プロキシ（Web Proxy）] を選択し、[プロキシを設定する HTTP ポート（HTTP Ports to Proxy）] フィールドからポート 80 を削除します。

ステップ 2　アプライアンスにファイルをアップロードする場合、PAC サーバ ポートとしてポート 80 を使用します。

ステップ 3　ポート 80 の Web プロキシを指し示すようにブラウザが手動設定されている場合は、[プロキシを設定するHTTP ポート（HTTP Ports to Proxy）] フィールドで、別のポートを指し示すようにブラウザを再設定します。

ステップ 4　PAC ファイルのポート 80 への参照を変更します。

DNS に関する問題

アラート：DNS キャッシュのブートに失敗（Failed to bootstrap the DNS cache）

アプライアンスのリブート時に、「DNS キャッシュのブートに失敗（Failed to bootstrap the DNS cache）」というメッセージを含むアラートが生成された場合は、システムがプライマリ DNS サーバに接続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。

機能 キーの期限切れ

（Web インターフェイスから）アクセスしようとしている機能の機能キーの有効期限が切れている場合は、シスコの担当者またはサポート組織までご連絡ください。

フェールオーバーに関する問題

フェールオーバーの誤った設定

フェールオーバー グループを誤って設定すると、複数のマスター アプライアンスが生じたり、その他のフェールオーバー問題が引き起こされる可能性があります。`failoverconfig` CLI コマンドの `testfailovergroup` サブコマンドを使用して、フェールオーバーの問題を診断します。

次に例を示します。

```
wsa.wga> failoverconfig
Currently configured failover profiles:
1.      Failover Group ID: 61
        Hostname: failoverV4P1.wga, Virtual IP: 10.4.28.93/28
        Priority: 100, Interval: 3 seconds
        Status: MASTER
Choose the operation you want to perform:
- NEW - Create new failover group.
- EDIT - Modify a failover group.
- DELETE - Remove a failover group.
- PREEMPTIVE - Configure whether failover is preemptive.
- TESTFAILOVERGROUP - Test configured failover profile(s)
[]> testfailovergroup
Failover group ID to test (-1 for all groups):
[]> 61
```

仮想アプライアンスでのフェールオーバーに関する問題

仮想アプライアンス上に展開している場合は、ハイパーバイザのインターフェイス/仮想スイッチが無差別モードを使用するように設定されていることを確認してください。

FTP に関する問題

URL カテゴリが一部の FTP サイトをブロックしない

ネイティブ FTP 要求が FTP プロキシに透過的にリダイレクトされる場合、FTP サーバに対するホスト名情報は含まれず、IP アドレス情報だけが含まれます。そのため、要求の宛先がそれらのサーバである場合でも、ホスト名情報しか持っていない一部の定義済み URL カテゴリと Web レピュテーション フィルタが、ネイティブ FTP 要求と一致しなくなります。それらのサイトへのアクセスをブロックする場合は、サイトの IP アドレスを使用してサイト用のカスタム URL カテゴリを作成する必要があります。

大規模 FTP 転送の切断

FTP プロキシと FTP サーバとの接続が遅い場合、特に、Cisco データ セキュリティ フィルタがイネーブルのときに、大きなファイルのアップロードに時間がかかることがあります。そのため、FTP プロキシがファイル全体をアップロードする前に FTP クライアントがタイムアウトしてしまい、トランザクション失敗の通知を受け取る場合があります。しかし、トランザクションは失敗しておらず、バックグラウンドで続行され、FTP プロキシによって完了されます。

FTP クライアントのアイドル タイムアウト値を適切に増加することにより、この問題を回避できます。

ファイルのアップロード後に FTP サーバにゼロ バイト ファイルが表示される

発信マルウェア対策スキャンによって FTP プロキシがアップロードをブロックすると、FTP クライアントは FTP サーバ上にゼロ バイト ファイルを作成します。

Chrome ブラウザが FTP-over-HTTP 要求でユーザ エージェントとして検出されない

FTP-over-HTTP 要求では、Chrome ブラウザはユーザ エージェント文字列を含まないためユーザ エージェントとして検出されません。

ハードウェアに関する問題

アプライアンスの電源の再投入

重要 x80 アプライアンスの電源を再投入する場合は、電源ボタンを押す前に、アプライアンスが回復する（すべての LED がグリーンになる）まで、少なくとも 20 分間お待ちください。

アプライアンスの状態およびステータス インジケータ

ハードウェア アプライアンスの前面パネルおよび/または後面パネルのライトは、アプライアンスの状態およびステータスを示します。これらのインジケータについては、http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html から使用できるハードウェア ガイドを参照してください。

温度範囲など、アプライアンスの仕様についてもこれらのマニュアルで確認できます。

アラート：380 または 680 ハードウェアでの [バッテリ再学習タイムアウト（Battery Relearn Timed Out）]（RAID イベント）

このアラートは、問題を示している場合と示していない場合があります。バッテリ再学習タイムアウト自体は、RAID コントローラに問題があることを示すものではありません。コントローラは、後続の再学習で回復します。以降 48 時間他の RAID アラートに関する電子メールを監視して、この問題が他の問題の副作用ではないことを確認してください。システムから他の RAID タイプのアラートが示されない場合は、この警告を無視してかまいません。

HTTPS/復号化/証明書に関する問題

- URL カテゴリ基準を使用しているルーティング ポリシーによる HTTPS サイトへのアクセス
- HTTPS 要求の失敗
- 特定 Web サイトの復号化のバイパス
- 埋め込み/参照コンテンツのブロックの例外に対する条件および制約事項
- アラート：セキュリティ証明書に関する問題
- 以下の項も参照してください。
  - HTTPS トランザクションのロギング
  - HTTP および FTP over HTTP 要求が、認証を必要としないアクセス ポリシーにのみ一致する

URL カテゴリ基準を使用しているルーティング ポリシーによる HTTPS サイトへのアクセス

透過的にリダイレクトされた HTTPS 要求の場合、Web プロキシは宛先サーバとやり取りして、サーバ名とサーバが属する URL カテゴリを判別する必要があります。したがって、Web プロキシがルーティング ポリシー グループのメンバーシップを評価する時点では、まだ宛先サーバとやり取りしていないので、HTTPS 要求の URL カテゴリが不明です。URL カテゴリが不明だと、Web プロキシは透過的 HTTPS 要求を、メンバーシップ基準として URL カテゴリを使用しているルーティング ポリシーと照合できません。

その結果、透過的にリダイレクトされた HTTPS トランザクションは、ルーティング ポリシー グループのメンバーシップ基準を URL カテゴリによって定義していないルーティング ポリシーとのみ照合されます。すべてのユーザ定義のルーティング ポリシーがメンバーシップを URL カテゴリによって定義している場合、透過的 HTTPS トランザクションはデフォルトのルーティング ポリシー グループと照合されます。

HTTPS 要求の失敗

IP ベースのサロゲートと透過的要求を含む HTTPS

HTTPS 要求が、以前の HTTP 要求の認証情報を利用できないクライアントから発信された場合、AsyncOS は、HTTPS プロキシの設定に応じて、HTTPS 要求に失敗するか、またはユーザを認証するために HTTPS 要求を復号化します。この動作を定義するには、[セキュリティサービス（Security Services）] > [HTTPS プロキシ（HTTPS Proxy）] ページで [HTTPS 透過的要求（HTTPS Transparent Request）] 設定を使用します。「復号化ポリシー」の章の「HTTPS プロキシの有効化」に関する項を参照してください。

カスタムおよびデフォルト カテゴリの異なるクライアントの「Hello」動作

パケット キャプチャをスキャンすると、カスタム カテゴリおよびデフォルト（Web）カテゴリの HTTPS 復号化パススルー ポリシーに対して別々の時間で「Client Hello」ハンドシェイクが送信されます。

デフォルト カテゴリを介した HTTPS ページのパススルーでは、要求元から Client Hello を受信する前に Client Hello が送信され、接続が失敗します。カスタム URL カテゴリを介した HTTPS ページのパススルーでは、要求元から Client Hello を受信した後に Client Hello が送信され、接続が成功します。

対応策として、SSL 3.0 のみと互換性がある Web ページのパススルー アクションを使用して、カスタム URL カテゴリを作成することができます。

特定 Web サイトの復号化のバイパス

HTTPS サーバへのトラフィックが、Web プロキシなどのプロキシ サーバによって復号化されると、一部の HTTPS サーバは期待どおりに機能しなくなります。たとえば、セキュリティの高い銀行のサイトなど、一部の Web サイトとそれらに関連する Web アプリケーションおよびアプレットは、オペレーティング システムの証明書ストアを使用するのではなく、信頼できる証明書のハードコードされたリストを維持します。

すべてのユーザがこれらのタイプのサイトにアクセスできるようにするには、これらのサーバへの HTTPS トラフィックの復号化をバイパスします。

ステップ 1　拡張プロパティを設定して、影響を受ける HTTPS サーバを含むカスタム URL カテゴリを作成します。

ステップ 2　メンバーシップの一環としてステップ 1 で作成されたカスタム URL カテゴリを使用する復号化ポリシーを作成し、カスタム URL カテゴリに対するアクションを [通過（Pass Through）] に設定します。

埋め込み/参照コンテンツのブロックの例外に対する条件および制約事項

Referer ベースの例外は、アクセス ポリシーでのみサポートされます。HTTPS トラフィックでこの機能を使用するには、アクセス ポリシーで例外を定義する前に、例外用に選択する URL カテゴリの HTTPS 復号化を設定する必要があります。ただし、この機能は特定の条件下では機能しません。

- 接続がトンネル化されていて HTTPS 復号化が有効になっていない場合、この機能は HTTPS サイトに発行される要求に対して機能しません。
- RFC 2616 に従って、ブラウザ クライアントにはオープンに/匿名で参照するためのトグル スイッチが用意されている場合があります。これによって、Referer および参照元情報の送信をそれぞれ有効/無効にすることができます。この機能は Referer ヘッダーのみに依存しており、それらの送信をオフにするとこの機能は使用できなくなります。
- RFC 2616 に従って、参照元ページがセキュアなプロトコルで転送された場合、クライアントには（セキュアでない）HTTP 要求の Referer ヘッダー フィールドは含まれません。そのため、HTTPS ベースのサイトから HTTP ベースのサイトに対するすべての要求には Referer ヘッダーが含まれず、この機能は期待どおりに動作しません。
- 復号ポリシーが設定されている場合（カスタム カテゴリが復号ポリシーと一致する場合やアクションがドロップに設定されている場合など）、そのカテゴリのすべての着信要求はドロップされ、バイパスは実行されません。

アラート：セキュリティ証明書に関する問題

通常、アプライアンスで生成またはアップロードされるルート証明書情報は、信頼できるルート認証局としてクライアント アプリケーションで認識されません。ユーザが HTTPS 要求を送信すると、大部分の Web ブラウザでは、デフォルトで、Web サイトのセキュリティ証明書に問題があることを知らせる警告メッセージがクライアント アプリケーションによって表示されます。通常、エラー メッセージには、Web サイトのセキュリティ証明書が信頼できる認証局によって発行されていないこと、または Web サイトが未知の認証局によって認証されていることが表示されます。クライアント アプリケーションによっては、この警告メッセージがユーザに示されず、ユーザは承認されない証明書を受け入れることができません。

（注）　**Mozilla Firefox ブラウザ：**Mozilla Firefox ブラウザで使用するには、アップロードする証明書に「basicConstraints=CA:True」を含める必要があります。この制約により、Firefox は、信頼されたルート認証局としてルート証明書を認識できるようになります。

ロギングに関する問題

アクセス ログ エントリにカスタム URL カテゴリが表示されない

Web アクセス ポリシー グループに、[モニタ（Monito）] に設定されたカスタム URL カテゴリ セットとその他のコンポーネント（Web レピュテーション フィルタ、DVS エンジンなど）がある場合に、カスタム URL カテゴリ内の URL に対する要求を許可するかブロックするかについて最終決定が行われると、要求のアクセス ログ エントリには、カスタム URL カテゴリの代わりに、定義済みの URL カテゴリが表示されます。

HTTPS トランザクションのロギング

アクセス ログでの HTTPS トランザクションの表示は、HTTP トランザクションと似ていますが、特性は少し異なります。記録される内容は、トランザクションが HTTPS プロキシに明示的に送信されるか、または透過的にリダイレクトされるかどうかによって異なります。

- **TUNNEL。**これは、HTTPS 要求が HTTPS プロキシに透過的にリダイレクトされたときにアクセス ログに記録されます。
- **CONNECT。**これは、HTTPS 要求が HTTPS プロキシに明示的に送信されたときにアクセス ログに記録されます。

HTTPS トラフィックが復号化されたときは、アクセス ログにトランザクションに対して、以下の 2 つのエントリが含まれます。

- TUNNEL または CONNECT が、処理された要求のタイプに応じて記録されます。
- HTTP 方式および復号化された URL。例：「GET https://ftp.example.com」。

完全な URL は、HTTPS プロキシがトラフィックを復号化するときだけ表示されます。

アラート：生成データのレートを維持できない

内部ロギング プロセスがフル バッファにより Web トランザクション イベントをドロップする場合、AsyncOS for Web が設定されたアラート受信者にクリティカルな電子メール メッセージを送信します。

デフォルトでは、Web プロキシが非常に高い負荷を受けたときに、内部ロギング プロセスは Web プロキシの負荷を減らす際にそれらを記録するイベントをバッファします。ロギング バッファ ファイルが完全に満杯になったときに、Web プロキシはトラフィックの処理を続行しますが、ロギング プロセスはイベントの一部をアクセス ログまたは Web トラッキング レポートに記録しません。これは、Web トラフィックのスパイク時に発生する可能性があります。

ただし、アプライアンスが持続的に過剰容量になっている場合にも、ロギング バッファが満杯になることがあります。AsyncOS for Web は、ロギング プロセスがデータをドロップしなくなるまで、数分ごとにクリティカルな電子メール メッセージを送信し続けます。

クリティカルなメッセージは以下のようなテキストが含まれます。

```
Reporting Client: The reporting system is unable to maintain the rate of data being
generated. Any new data generated will be lost.
```

AsyncOS for Web が、このクリティカルなメッセージを継続的または頻繁に送信する場合、アプライアンスは過剰容量になっている可能性があります。Web Security Appliance の容量を追加する必要があるかどうかを確認するには、シスコ カスタマー サポートにお問い合わせください。

W3C アクセス ログでサードパーティ製ログ アナライザ ツールを使用する場合の問題

サードパーティ製のログ アナライザ ツールを使用して、W3C アクセス ログを閲覧したり解析する場合は、状況に応じて [タイムスタンプ（timestamp）] フィールドを含める必要があります。W3C の [タイムスタンプ（timestamp）] フィールドには、UNIX エポック以降の時間が表示され、ほとんどのログ アナライザはこの形式の時間のみ認識します。

ポリシーに関する問題

- オブジェクトのブロックに関する問題
- 識別プロファイルがポリシーから削除される
- ポリシーの照合に失敗
- 次のセクションも参照してください。URL カテゴリ基準を使用しているルーティング ポリシーによる HTTPS サイトへのアクセス

オブジェクトのブロックに関する問題

- 一部の Microsoft Office ファイルがブロックされない
- DOS の実行可能オブジェクト タイプをブロックすると、Windows OneCare の更新がブロックされる

一部の Microsoft Office ファイルがブロックされない

[ブロックするオブジェクト タイプ（Block Object Type）] セクションで Microsoft Office ファイルをブロックすると、一部の Microsoft Office ファイルがブロックされない可能性があります。

すべての Microsoft Office ファイルをブロックする必要がある場合は、[ブロックする MIME タイプ（Block Custom MIME Types）] フィールドに **`application/x-ole`** を追加します。ただし、このカスタム MIME タイプをブロックすると、Visio ファイルや一部のサード パーティ アプリケーションなど、すべての Microsoft 複合オブジェクト フォーマット タイプがブロックされます。

DOS の実行可能オブジェクト タイプをブロックすると、Windows OneCare の更新がブロックされる

DOS の実行可能オブジェクト タイプをブロックするように Web Security Applianceを設定すると、Windows OneCare のアップデートがブロックされます。

識別プロファイルがポリシーから削除される

識別プロファイルをディセーブルにすると、その識別プロファイルは関連するポリシーから削除されます。識別プロファイルがイネーブルになっていることを確認し、再びポリシーに追加します。

ポリシーの照合に失敗

ポリシーが適用されない

複数の識別プロファイルの基準が同じである場合、AsyncOS は一致する最初の識別プロファイルにトランザクションを割り当てます。したがって、トランザクションはその他の同じ基準の識別プロファイルとは照合されず、以降の同じ基準の識別プロファイルに適用されるポリシーは照合も適用もされません。

HTTP および FTP over HTTP 要求が、認証を必要としないアクセス ポリシーにのみ一致する

クレデンシャルの暗号化がイネーブルの場合は、サロゲートとして IP アドレスを使用するようにアプライアンスを設定する必要があります。

クレデンシャルの暗号化がイネーブルになっており、サロゲート タイプとして Cookie を使用するように設定されている場合、認証は HTTPS 要求や FTP over HTTP 要求で機能しません。クレデンシャルの暗号化がイネーブルの場合、Web プロキシは HTTPS 接続を使用して、クライアントを認証のために Web プロキシ自体にリダイレクトするからです。認証が成功した後、Web プロキシは元の Web サイトにクライアントをリダイレクトします。ユーザの識別を続行するために、Web プロキシはサロゲート（IP またはクッキー）を使用する必要があります。ただし、要求が HTTP または FTP over HTTP を使用している場合、Cookie を使用してユーザを追跡すると、以下の動作が引き起こされます。

- **HTTPS。**Web プロキシは、復号化ポリシーを割り当てる前にユーザのアイデンティティを解決（したがって、トランザクションを復号化）する必要がありますが、トランザクションを復号化しない限り、Cookie を取得してユーザを識別することはできません。
- **FTP over HTTP。**FTP over HTTP を使用して FTP サーバにアクセスする場合のジレンマは、HTTPS サイトにアクセスする場合と同様です。Web プロキシは、アクセス ポリシーを割り当てる前にユーザのアイデンティティを解決する必要がありますが、FTP トランザクションから Cookie を設定できません。

したがって、HTTP 要求と FTP over HTTP 要求は、認証を必要としないアクセス ポリシーとのみ一致します。通常、これらの要求は、認証を必要としないグローバル アクセス ポリシーに一致します。

HTTPS 要求および FTP over HTTP 要求の場合にユーザがグローバル ポリシーに一致

アプライアンスがクッキー ベースの認証を使用する場合、Web プロキシは、HTTP 要求を介した HTTPS および FTP のクライアントからクッキー情報を取得しません。このため、クッキーからユーザ名を取得できません。

HTTPS 要求や FTP over HTTP 要求は、他のメンバーシップ基準に従って識別プロファイルと照合されますが、識別プロファイルで認証が必要な場合でも、Web プロキシはクライアントに認証を要求しません。代わりに、Web プロキシはユーザ名を NULL に設定し、ユーザを未認証と見なします。

その後、ポリシーと照合して評価される際に、未認証の要求は [すべての ID（All Identities）] を指定しているポリシーとのみ一致し、[すべてのユーザ（All Users）] が適用されます。通常、これはグローバル アクセス ポリシーなどのグローバル ポリシーです。

ユーザに誤ったアクセス ポリシーが割り当てられる

- ネットワーク上のクライアントが、ネットワーク接続状態インジケータ（NCSI）を使用している。
- Web Security Appliance が NTLMSSP 認証を使用している。
- 識別プロファイルが IP ベースのサロゲートを使用している。

ユーザは自分のクレデンシャルではなく、マシン クレデンシャルを使用して識別され、その結果、誤ったアクセス ポリシーが割り当てられる場合があります。

回避策：

- マシン クレデンシャルのサロゲート タイムアウト値を小さくします。

ステップ 1　advancedproxyconfig > authentication CLI コマンドを使用します。

ステップ 2　マシン クレデンシャルのサロゲート タイムアウトを入力します。

リブートの問題

KVM で動作する仮想アプライアンスがリブート時にハングアップ

（注）　これは KVM の問題であり、状況によって異なる場合があります。

詳細については、https://www.mail-archive.com/kvm@vger.kernel.org/msg103854.html および https://bugs.launchpad.net/qemu/+bug/1329956 を参照してください。

ステップ 1　次の点をチェックします。

```
cat /sys/module/kvm_intel/parameters/enable_apicv
```

ステップ 2　上記の値が Y に設定されている場合：

a.　仮想アプライアンスを停止し、KVM カーネル モジュールを再インストールします。

```
rmmod kvm_intel
modprobe kvm_intel enable_apicv=N
```

b.　仮想アプライアンスを再起動します。

ハードウェア アプライアンス：アプライアンスの電源のリモート リセット

アプライアンスのハード リセットが必要な場合は、サードパーティの Platform Management（IPMI）ツールを使用してアプライアンス シャーシをリモートからリブートできます。

制約事項

- リモート電源管理は、特定のハードウェアでのみ使用できます。詳細については、リモート電源再投入の有効化（12-5 ページ）を参照してください。
- この機能を使用する場合は、使用が必要になる前に、あらかじめ有効にしておく必要があります。詳細は、リモート電源再投入の有効化（12-5 ページ）を参照してください。
- 以下の IPMI コマンドだけがサポートされます：status、on、off、cycle、reset、diag、soft。サポートされていないコマンドを発行すると、「権限不足」エラーが発生します。

はじめる前に

- IPMI バージョン 2.0 を使用してデバイスを管理できるユーティリティを取得し、設定します。
- サポートされている IPMI コマンドの使用方法を理解します。IPMI ツールのマニュアルを参照してください。

ステップ 1　IPMI を使用して、必要なクレデンシャルと共に、先に設定したリモート電源管理ポートに割り当てられた IP アドレスに、サポートされている電源の再投入コマンドを発行します。

たとえば、IPMI をサポートする UNIX タイプのマシンからは、次のようなコマンドを発行します。

```
ipmitool -I lan -H 192.0.2.1 -U remoteresetuser -P passphrase chassis power reset
```

ここで 192.0.2.1 は、リモート電源管理ポートに割り当てられた IP アドレスであり、remoteresetuser および passphrase は、この機能を有効にしたときに入力したクレデンシャルです。

ステップ 2　アプライアンスが再起動されるまで、少なくとも 11 分間待ちます。

サイトへのアクセスに関する問題

- 次のセクションも参照してください。特定 Web サイトの復号化のバイパス

認証をサポートしていない URL にアクセスできない

以下は、認証をサポートしていないため、Web Security Appliance が透過モードで展開されている場合に使用できないアプリケーションのリストの一部です。

- Mozilla Thunderbird
- Adobe Acrobat アップデート
- HttpBridge
- CollabNet の Subversion

- Microsoft Windows アップデート
- Microsoft Visual Studio

回避策：認証を必要としない URL のユーザ クラスを作成します。

関連項目

- 認証のバイパス（5-33 ページ）

POST 要求を使用してサイトにアクセスできない

ユーザの最初のクライアント要求が POST 要求で、ユーザの認証が必要な場合、POST 本文のコンテンツは失われます。この問題は、アクセス コントロールのシングル サインオン機能を使用しているアプリケーションに対して POST 要求を行った場合に発生することがあります。

回避策：

- 最初の要求として POST を使用する URL に接続する前に、ブラウザから別の URL を要求して、最初に Web プロキシでユーザを認証させます。
- 最初の要求として POST を使用する URL の認証をバイパスします。

（注） アクセス コントロールを使用すると、アプリケーション認証ポリシーで設定された Assertion Consumer Service（ACS）URL の認証をバイパスできます。

関連項目

- 認証のバイパス（5-33 ページ）。

アップストリーム プロキシに関する問題

- アップストリーム プロキシが基本クレデンシャルを受け取らない
- クライアント要求がアップストリーム プロキシで失敗する

アップストリーム プロキシが基本クレデンシャルを受け取らない

アプライアンスとアップストリーム プロキシの両方が NTLMSPP による認証を使用している場合、設定によっては、アプライアンスとアップストリーム プロキシで、認証クレデンシャルを要求する無限ループが発生する可能性があります。たとえば、アップストリーム プロキシでは基本認証が必要だが、アプライアンスでは NTLMSPP 認証が必要な場合、アプライアンスはアップストリーム プロキシに正常に基本認証クレデンシャルを渡すことができません。これは、認証プロトコルの制限によるものです。

クライアント要求がアップストリーム プロキシで失敗する

設定:

- Web Security Appliance とアップストリーム プロキシ サーバが基本認証を使用している。
- ダウンストリームの Web Security Appliance でクレデンシャルの暗号化がイネーブルになっている。

Web プロキシはクライアントから「Authorization」HTTP ヘッダーを受信しますが、アップストリーム プロキシ サーバは「Proxy-Authorization」HTTP ヘッダーを要求するため、クライアント要求はアップストリーム プロキシで失敗します。

アップストリーム プロキシ経由で FTP 要求をルーティングできない

ネットワークに FTP 接続をサポートしていないアップストリーム プロキシが含まれる場合は、すべての ID に適用され、かつ FTP 要求にのみ適用されるルーティング ポリシーを作成する必要があります。ルーティング ポリシーを設定して、FTP サーバに直接接続するか、プロキシのすべてが FTP 接続をサポートしているプロキシ グループに接続します。

仮想アプライアンス

AsyncOS の起動中に [強制リセット（Reset）]、[電源オフ（Power Off）]、または [リセット（Reset）] オプションを使用しないでください

仮想ホストにおける以下の操作は、ハードウェア アプライアンスのプラグを抜くことと同等であり、特に AsyncOS の起動中ではサポートされていません。

- KVM の強制リセットオプション。
- VMware の電源オフとリセット オプション。（これらのオプションは、アプライアンスが完全に起動してから安全に使用できます）。

KVM 展開でネットワーク接続が最初は機能するが、その後失敗する

問題　前回の作業後にネットワーク接続が失われる。

ソリューション　これは KVM の問題です。OpenStack ドキュメントの「KVM: Network connectivity works initially, then fails」の項を参照してください。このドキュメントは、http://docs.openstack.org/admin-guide-cloud/content/section_network-troubleshoot.html にあります。

KVM 展開におけるパフォーマンスの低下、ウォッチドッグの問題、および CPU の使用率が高い

問題　Ubuntu 仮想マシン上で実行しているときに、アプライアンスのパフォーマンスが低下して、ウォッチドッグの問題が発生し、アプライアンスが異常に高い CPU　使用率を示す。

ソリューション　Ubuntu から最新の Host OS アップデートをインストールしてください。

Linux ホストで実行している仮想アプライアンスの一般的なトラブルシューティング

問題　KVM 展開で実行されている仮想アプライアンスに関する問題は、ホスト OS の設定の問題と関連している可能性があります。

ソリューション　『*Virtualization Deployment and Administration Guide*』のトラブルシューティンに関する項およびその他の情報を参照してください。このドキュメントは、https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/pdf/Virtualization_Deployment_and_Administration_Guide/Red_Hat_Enterprise_Linux-7-Virtualization_Deployment_and_Administration_Guide-en-US.pdf から入手できます。

WCCP に関する問題

最大ポート エントリ数

WCCP を使用した展開では、HTTP、HTTPS、および FTP ポートを合わせたポート エントリの最大数は 30 です。

パケット キャプチャ

アプライアンスでは、アプライアンスが接続されているネットワークで送受信される TCP/IP と他のパケットをキャプチャして表示できます。

（注）　パケット キャプチャ機能は UNIX の tcpdump コマンドに似ています。

パケット キャプチャの開始

ステップ 1　[ヘルプとサポート（Help and Support）] > [パケットキャプチャ（Packet Capture）] を選択します。

ステップ 2　（任意）[設定の編集（Edit Settings）] をクリックし、パケット キャプチャの設定を変更します。

オプション	説明
キャプチャ ファイル サイズ制限（Capture File Size Limit）	キャプチャ ファイルを拡大できる最大サイズを指定します。[キャプチャ期間（Capture Duration）] が [ファイルサイズの上限に達するまでキャプチャを実行（Run Capture Until File Size Limit Reached）] に設定されていない場合は、上限に達すると、データが破棄されて新しいファイルが開始されます。
キャプチャ期間（Capture Duration）	キャプチャを自動的に停止するとき（および場合）のオプション。次から選択します。 • [ファイルサイズの上限に達するまでキャプチャを実行（Run Capture Until File Size Limit Reached）]。キャプチャはファイル サイズの上限に達するまで実行されます。 • [制限時間に達するまでキャプチャを実行（Run Capture Until Time Elapsed Reaches）]。キャプチャは指定された期間だけ実行されます。単位を指定せずに時間の長さを入力すると、AsyncOS は、デフォルトで秒を使用します。 • [制限なしでキャプチャを実行（Run Capture Indefinitely）]。パケット キャプチャは、手動で停止するまで実行されます。 **（注）**　キャプチャは手動でいつでも終了できます。
インターフェイス	トラフィックがキャプチャされるインターフェイス。
フィルタ（Filters）	パケットをキャプチャするときに適用するフィルタリング オプション。フィルタリングを使用すると、必要なパケットだけをキャプチャできます。次から選択します。 • [フィルタなし（No Filters）]。すべてのパケットがキャプチャされます。 • [事前定義されたフィルタ（Predefined Filters）]。定義済みのフィルタを使用して、ポートや IP アドレスによりフィルタリングできます。何も指定しなかった場合は、すべてのトラフィックがキャプチャされます。 • [カスタムフィルタ（Custom Filter）]。必要なパケット キャプチャ オプションの正確な構文がわかっている場合は、このオプションを使用します。標準の tcpdump 構文を使用します。

（任意）パケット キャプチャの変更を送信して確定します。

（注）　変更内容をコミットせずにパケット キャプチャ設定を変更し、パケット キャプチャを開始する場合、AsyncOS は新しい設定を使用します。これにより、今後のパケット キャプチャの実行に対する設定を適用せずに現在のセッションで新しい設定を使用することができます。この設定は、クリアするまで有効なままになります。

ステップ 3　[キャプチャを開始（Start Capture）] をクリックします。実行中のキャプチャを手動で停止するには、[キャプチャを停止（Stop Capture）] をクリックします。

パケット キャプチャ ファイルの管理

アプライアンスは、取り込んだパケット アクティビティをファイルに保存し、そのファイルをローカルに格納します。デバッグやトラブルシューティングのために、FTP を使用してパケット キャプチャ ファイルをシスコ カスタマー サポートに送信できます。

- パケット キャプチャ ファイルのダウンロードまたは削除

パケット キャプチャ ファイルのダウンロードまたは削除

（注）　また、FTP を使用してアプライアンスに接続し、captures ディレクトリからパケット キャプチャ ファイルを取り出すこともできます。

ステップ 1　[ヘルプとサポート（Help and Support）] > [パケットキャプチャ（Packet Capture）] を選択します。

ステップ 2　[パケットキャプチャファイルの管理（Manage Packet Capture Files）] ペインから、使用するパケット キャプチャ ファイルを選択します。このペインが表示されない場合は、アプライアンスにパケット キャプチャ ファイルが保存されていません。

ステップ 3　必要に応じて、[ファイルのダウンロード（Download File）] または [選択ファイルの削除（Delete Selected File）] をクリックします。

サポートの使用

- 効率的なサービス提供のため情報収集（A-18 ページ）
- テクニカル サポート要請の開始（A-18 ページ）
- 仮想アプライアンスのサポートの取得（A-19 ページ）
- アプライアンスへのリモート アクセスのイネーブル化（A-20 ページ）

効率的なサービス提供のため情報収集

サポートに問い合わせる前に以下の手順を実行してください。

- 一般的なトラブルシューティングとベスト プラクティス（A-1 ページ）の説明に従い、カスタム ログのフィールドを有効にします。
- パケット キャプチャを実行することを検討してください。パケット キャプチャ（A-16 ページ）を参照してください。

テクニカル サポート要請の開始

緊急ではない場合は、アプライアンスを使用してサポート要請をシスコ カスタマー サポートに送信できます。アプライアンスは要請を送信する際に、アプライアンスの設定も送信します。サポート要求を送信するには、アプライアンスがインターネットに電子メールを送信できる必要があります。

（注）　緊急の問題がある場合は、Cisco Worldwide Support Center に連絡してください。

はじめる前に

- 自身の Cisco.com ユーザ ID がこのアプライアンスのサービス契約に関連付けられていることを確認します。Cisco.com プロファイルに現在関連付けられているサービス契約のリストを閲覧するには、Cisco.com Profile Manager（https://sso.cisco.com/autho/forms/CDClogin.html）にアクセスしてください。Cisco.com のユーザ ID がない場合は、登録して ID を取得してください。

ステップ 1　[ヘルプとサポート（Help and Support）] > [テクニカルサポートに問い合わせる（Contact Technical Support）] を選択します。

ステップ 2　（任意）要請のその他の受信者を選択します。デフォルトでは、サポート要請とコンフィギュレーション ファイルがシスコ カスタマー サポートに送信されます。

ステップ 3　自身の連絡先情報を入力します。

ステップ 4　問題の詳細を入力します。

- この問題に関するカスタマー サポート チケットをすでに持っている場合は、それを入力してください。

ステップ 5　[送信（Send）] をクリックします。トラブル チケットがシスコで作成されます。

仮想アプライアンスのサポートの取得

Cisco Content Security 仮想アプライアンスのサポート ケースを報告する場合は、仮想ライセンス番号（VLN）、契約番号、および製品 ID コード（PID）を提供する必要があります。

発注書を参照するか以下の表を使用すると、仮想アプライアンスで動作中のソフトウェア ライセンスに基づく PID を特定できます。

機能	PID	説明
Web Security Essentials	WSA-WSE-LIC=	内容: • Web Usage Controls • Web レピュテーション
Web Security Premium	WSA-WSP-LIC=	内容: • Web Usage Controls • Web レピュテーション • Sophos および Webroot Anti-Malware シグネチャ
Web Security Anti-Malware	WSA-WSM-LIC=	Sophos および Webroot Anti-Malware シグネチャが含まれます。
McAfee Anti-Malware	WSA-AMM-LIC=	—
高度なマルウェア防御	WSA-AMP-LIC=	—

アプライアンスへのリモート アクセスのイネーブル化

[リモートアクセス(Remote Access)] オプションを使用すると、シスコ カスタマー サポートがサポートのためにリモート アプライアンスにアクセスできるようになります。

ステップ 1　[ヘルプとサポート(Help and Support)] > [リモートアクセス(Remote Access)] を選択します。

ステップ 2　[有効(Enable)] をクリックします。

ステップ 3　[カスタマーサポートのリモートアクセス(Customer Support Remote Access)] オプションを設定します。

オプション	説明
シード文字列(Seed String)	文字列を入力する場合は、その文字列が既存または将来のパスフレーズと一致しないようにしてください。 [送信(Submit)] をクリックすると、文字列がページの上部に表示されます。 この文字列をサポート担当者に提出します。
セキュア トンネル(Secure Tunnel)(推奨)	リモート アクセス接続にセキュア トンネルを使用するかどうかを指定します。 このオプションがイネーブルの場合、アプライアンスは、指定されたポートからサーバ upgrades.ironport.com への SSH トンネルを作成します(デフォルトでは、ポート 443)。接続が確立されると、シスコ カスタマー サポートは SSH トンネルを使用してアプライアンスにアクセスできるようになります。 techsupport トンネルがイネーブルになると、`upgrades.ironport.com` に 7 日間接続されたままになります。7 日が経過すると、techsupport トンネルを使用して新しい接続を作成できなくなりますが、既存の接続は存続し、機能します。 リモート アクセス アカウントは、明確に非アクティブ化されるまでアクティブな状態を維持します。

ステップ 4　変更を送信し、保存します。

ステップ 5　ページ上部近くに表示される成功メッセージでシード文字列を検索し、書き留めます。

セキュリティ上の理由から、この文字列はアプライアンスに保存されず、後から文字列を確認する方法はありません。

安全な場所にこのシード文字列を保存します。

ステップ 6　シード文字列をサポート担当者に提出します。

コマンドライン インターフェイス

コマンド ライン インターフェイスの概要

AsyncOS コマンドライン インターフェイス（CLI）を使用して、Web Security Appliance を設定したりモニタすることができます。コマンドライン インターフェイスには、それら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 を使用してアクセスするか、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。デフォルトでは、SSH は管理ポートに設定されます。

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、必要な情報の入力を求めるプロンプトが表示されます。

コマンドライン インターフェイスへのアクセス

以下のいずれかの方法で接続できます。

- **イーサネット。**Web Security Appliance の IP アドレスを使用して SSH セッションを開始します。工場出荷時のデフォルト IP アドレスは 192.168.42.42 です。SSH は、ポート 22 を使用するように設定されています。
- **シリアル接続**シリアル ケーブルが接続されているパーソナル コンピュータの通信ポートを使用して、ターミナル セッションを開始します。

初回アクセス

admin アカウントを使用して初めて CLI にアクセスした後は、さまざまな許可レベルにより他のユーザを追加できます。以下のデフォルトの **admin** ユーザ名とパスフレーズを入力してアプライアンスにログインします。

- ユーザ名：**admin**
- パスフレーズ：**ironport**

デフォルトのパスフレーズで初めてログインすると、システム セットアップ ウィザードのプロンプトにより **admin** アカウントのパスフレーズを変更するよう求められます。

admin アカウントのパスフレーズは、passwd コマンドを使用していつでもリセットできます。

以降のアクセス

有効なユーザ名とパスフレーズを使用して、いつでもアプライアンス接続してログインできます。現在のユーザ名での最近のアプライアンスへのアクセス試行（成功、失敗を含む）の一覧が、ログイン時に自動的に表示されることに注意してください。

追加のユーザの設定については、userconfig コマンド、または ユーザ アカウントの管理（12-6 ページ）を参照してください。

コマンド プロンプトの使用

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。

```
example.com>
```

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 が入力を待機しているときは、プロンプトとして、角カッコ（[]）で囲まれたデフォルト値の後ろに大なり記号（>）が表示されます。デフォル値がない場合、カッコ内は空です。

次に例を示します。

```
example.com> routeconfig

Choose a routing table:
- MANAGEMENT - Routes for Management Traffic
- DATA - Routes for Data Traffic
[]>
```

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。

```
example.com> setgateway

Warning: setting an incorrect default gateway may cause the current connection
to be interrupted when the changes are committed.
Enter new default gateway:
[172.xx.xx.xx]>
```

デフォルト設定が表示されたときに Return キーを押すと、デフォルト値を受け入れたことになります。

コマンドの構文

インタラクティブ モードで操作している場合、CLI コマンド構文は単一のコマンドから構成されます。スペースは含まれず、引数やパラメータもありません。次に例を示します。

```
example.com> logconfig
```

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. Critical
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 the proxy? [Y]> Y
```

サブコマンド

一部のコマンドでは、NEW、EDIT、DELETE などのサブコマンド命令を使用できます。EDIT および DELETE 関数では、設定されている値のリストが表示されます。

次に例を示します。

```
example.com> interfaceconfig

Currently configured interfaces:

1. Management (172.xxx.xx.xx/xx: example.com)

Choose the operation you want to perform:

- NEW - Create a new interface.

- EDIT - Modify an interface.
```

```
- 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。

サブコマンドのエスケープ

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

コマンド履歴

CLI は、セッション中に入力された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、キーボードの上下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。

コマンドのオートコンプリート

AsyncOS CLI は、コマンド補完機能をサポートしています。コマンドの先頭の数文字を入力して Tab キーを押すと、CLI によって残りの文字列が補完されます。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。

```
example.com> set (Tab キーを押す)
setgateway, setgoodtable, sethostname, settime, settz
example.com> seth(もう一度 Tab キーを押すと sethostname での入力が完了)
```

CLI を使用した設定変更の確定

- 設定の変更の多くは、確定するまで有効になりません。
- commit コマンドを使用すると、他の操作を通常どおりに実行しながら設定を変更できます。
- 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** キーを押します。
- 確定されていない設定の変更は記録されますが、commit コマンドを実行するまで有効になりません。ただし、一部のコマンドは commit コマンドを実行しなくても有効になります。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。
- ユーザが確認とタイムスタンプを受け取るまで、変更は実際に確定されません。

汎用 CLI コマンド

ここでは、変更の確定やクリアなど、一般的な CLI セッションで使用される基本的なコマンドについて説明します。

CLI の例：設定変更の確定

commit コマンドの後のコメントの入力は任意です。

```
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 2007
```

CLI の例：設定変更のクリア

clear コマンドは、commit または clear コマンドが最後に実行された以降にアプライアンスの設定に対して行われた変更をすべてクリアします。

```
example.com> clear

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

Changes cleared: Wed Jan 01 12:00:01 2007

example.com>
```

CLI の例：コマンドライン インターフェイス セッションの終了

exit 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されます。確定されていない設定変更はクリアされます。

```
example.com> exit

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
```

CLI の例：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。

```
example.com> help
```

さらに、**help** *commandname* を入力して、特定のコマンドのヘルプにアクセスできます。

関連項目

- Web セキュリティ アプライアンスの CLI コマンド（27-6 ページ）。

Web セキュリティ アプライアンスの CLI コマンド

Web セキュリティ アプライアンスの CLI は、システムへのアクセスおよびシステムのアップグレードと管理を実行する、一連のプロキシ コマンドと UNIX コマンドをサポートしています。

（注） すべての CLI コマンドをすべての動作モード（標準 クラウド Web セキュリティ コネクタおよびハイブリッド Web セキュリティ）で適用/使用できるわけではありません。

コマンド（Command）	説明
advancedproxyconfig	Web プロキシの詳細設定を設定します。サブコマンドは以下のとおりです。 **Authentication**：認証設定オプション。 • When would you like to forward authorization request headers to a parent proxy • Enter the Proxy Authorization Realm to be displayed in the end user authentication dialog • Would you like to log the username that appears in the request URI • Should the Group Membership attribute be used for directory lookups in the Web UI (when it is not used, empty groups and groups with different membership attributes will be displayed) • Would you like to use advanced Active Directory connectivity checks • Would you like to allow case insensitive username matching in policies • Would you like to allow wild card matching with the character * for LDAP group names • Enter the charset used by the clients for basic authentication [ISO-8859-1/UTF-8] • Would you like to enable referrals for LDAP • Would you like to enable secure authentication • Enter the hostname to redirect clients for authentication • Enter the surrogate timeout for user credentials • Enter the surrogate timeout for machine credentials • Enter the surrogate timeout in the case traffic permitted due to authentication service unavailability • Enter re-auth on request denied option [disabled / embedlinkinblockpage] • Would you like to send Negotiate header along with NTLM header for NTLMSSP authentication • Configure username and IP address masking in logs and reports

advancedproxyconfig（続き）	**CACHING**：プロキシ キャッシュ モード。以下のうち 1 つを選択します。 • Safe Mode • Optimized Mode • Aggressive Mode • Customized Mode Web プロキシのキャッシュ モードの選択（4-7 ページ）も参照してください。 **DNS**：DNS 設定オプション。 • Enter the URL format for the HTTP 307 redirection on DNS lookup failure • Would you like the proxy to issue a HTTP 307 redirection on DNS lookup failure • Would you like proxy not to automatically failover to DNS results when upstream proxy (peer) is unresponsive • Find web server by: 0 = Always use DNS answers in order 1 = Use client-supplied address then DNS 2 = Limited DNS usage 3 = Very limited DNS usage オプション 1 および 2 では、[Web レピュテーション（Web Reputation）] がイネーブルに設定されている場合、DNS が使用されます。オプション 2 および 3 では、DNS は、アップストリーム プロキシがない場合、または設定されたアップストリーム プロキシが失敗するイベントで、明示的なプロキシ要求に使用されます。すべてのオプションで、[宛先 IP アドレス（Destination IP Addresses）] がポリシー メンバーシップで使用されている場合、DNS が使用されます。 **EUN**：エンドユーザ通知パラメータ。 • Choose: 1. Refresh EUN pages 2. Use Custom EUN pages 3. Use Standard EUN pages • Would you like to turn on presentation of the User Acknowledgement page? Web プロキシ使用規約（4-10 ページ）とエンドユーザ通知の概要（9-1 ページ）も参照してください。 **NATIVEFTP**：ネイティブ FTP の設定。 • Would you like to enable FTP proxy • Enter the ports that FTP proxy listens on • Enter the range of port numbers for the proxy to listen on for passive FTP connections • Enter the range of port numbers for the proxy to listen on for active FTP connections • Enter the authentication format: 1. Check Point 2. No Proxy Authentication 3. Raptor

advancedproxyconfig（続き）	• Would you like to enable caching • Would you like to enable server IP spoofing • Would you like to pass FTP server welcome message to the clients • Enter the max path size for the ftp server directory **FTPOVERHTTP**：FTP Over HTTP オプション。 • Enter the login name to be used for anonymous FTP access • Enter the password to be used for anonymous FTP access **HTTPS**：HTTPS 関連のオプション。 • HTTPS URI Logging Style - fulluri or stripquery • Would you like to decrypt unauthenticated transparent HTTPS requests for authentication purpose • Would you like to decrypt HTTPS requests for End User Notification purpose • Action to be taken when HTTPS servers ask for client certificate during handshake: 1. Pass through the transaction 2. Reply with certificate unavailable • Do you want to enable server name indication (SNI) extension? • Do you want to enable automatic discovery and download of missing Intermediate Certificates? • Do you want to enable session resumption? HTTPS トラフィックを制御する復号化ポリシーの作成：概要（7-1 ページ）も参照してください。 **SCANNING**：スキャン オプション。 • Would you like the proxy to do malware scanning all content regardless of content type • Enter the time to wait for a response from an anti-malware scanning engine (Sophos, McAfee, or Webroot), in seconds • Do you want to disable Webroot body scanning マルウェア対策 スキャンの概要（8-3 ページ）と Overview of Scanning Outbound Traffic（12-1 ページ）も参照してください。 **PROXYCONN**：プロキシ接続ヘッダーを含むことができないユーザ エージェントのリストを管理します。リストのエントリは、Flex（Fast Lexical Analyzer）の正規表現として解釈されます。その文字列の一部がリスト内の正規表現のいずれかに一致するユーザ エージェントは、一致とされます。 • 実行する操作を選択します。 NEW - Add an entry to the list of user agents DELETE - Remove an entry from the list **CUSTOMHEADERS**：特定のドメインのカスタム要求ヘッダーを管理します。 • 実行する操作を選択します。 DELETE - Delete entries NEW - Add new entries EDIT - Edit entries Web 要求へのカスタム ヘッダーの追加（4-8 ページ）も参照してください。

advancedproxyconfig（続き）	**MISCELLANEOUS**：その他のプロキシ関連パラメータ。 • Would you like proxy to respond to health checks from L4 switches (always enabled if WSA is in L4 transparent mode) • Would you like proxy to perform dynamic adjustment of TCP receive window size • Would you like proxy to perform dynamic adjustment of TCP send window size • Enable caching of HTTPS responses • Enter minimum idle timeout for checking unresponsive upstream proxy (in seconds) • Enter maximum idle timeout for checking unresponsive upstream proxy (in seconds) • Mode of the proxy: 1. Explicit forward mode only 2. Transparent mode with L4 Switch or no device for redirection 3. Transparent mode with WCCP v2 Router for redirection • Spoofing of the client IP by the proxy: 1. Disable 2. Enable for all requests 3. Enable for transparent requests only **（注）** スプーフィングは、Web ハイブリッド モードではサポートされていません。これらのデフォルト値を変更しないでください。 • Do you want to pass HTTP X-Forwarded-For headers? • Would you like to permit tunneling of non-HTTP requests on HTTP ports? • Would you like to block tunneling of non-SSL transactions on SSL Ports? • Would you like proxy to log values from X-Forwarded-For headers in place of incoming connection IP addresses? • Do you want proxy to throttle content served from cache? • Would you like the proxy to use client IP addresses from X-Forwarded-For headers • Do you want to forward TCP RST sent by server to client? • Do you want to enable URL lower case conversion for velocity regex? Web プロキシ データに対する P2 データ インターフェイスの使用（3-27 ページ）と Web プロキシの設定（4-3 ページ）も参照してください。 **SOCKS**：SOCKS プロキシのオプション。 • Would you like to enable SOCKS proxy • Proxy Negotiation Timeout • UDP Tunnel Timeout • SOCKS Control Ports • UDP Request Ports Web プロキシ データに対する P2 データ インターフェイスの使用（3-27 ページ）も参照してください。

advancedproxyconfig（続き）	**CONTENT-ENCODING**：コンテンツエンコーディング タイプを許可およびブロックします。 現在許可されているコンテンツエンコーディング タイプ：compress、deflate、gzip 現在ブロックされているコンテンツエンコーディング タイプ：該当なし 特定のコンテンツエンコーディング タイプの設定を変更するには、次のオプションを選択します。 1. compress 2. deflate 3. gzip [1]> The encoding type "compress" is currently allowed Do you want to block it? [N]>
adminaccessconfig	アプライアンスにログインする管理者の認証により厳しいアクセス要件を設けるように、Web Security Appliance を設定できます。
alertconfig	アラートの受信者を指定し、システム アラートを送信するためのパラメータを設定します。
authcache	認証キャッシュから 1 つまたはすべてのエントリ（ユーザ）を削除できるようにします。また、その時点で認証キャッシュに含まれているすべてのユーザのリストを表示できます。
certconfig	セキュリティの証明書とキーを設定します。
clear	前回の確定以降の保留されている設定変更をクリアします。
commit	システム設定に対する保留中の変更を確定します。
createcomputerobject	指定された場所にコンピュータ オブジェクトを作成します。
date	現在の日付を表示します。例： `Thu Jan 10 23:13:40 2013 GMT`

diagnostic	プロキシおよびレポート関連のサブコマンド: **NET**:ネットワーク診断ユーティリティ このコマンドは廃止されました。アプライアンスでネットワーク トラフィックをキャプチャするには、packetcapture を使用します。 **PROXY**:プロキシ デバッグ ユーティリティ 実行する操作を選択します。 – SNAP:プロキシのスナップショットを取得します。 – OFFLINE:プロキシをオフラインにします(WCCP 経由)。 – RESUME:プロキシのトラフィックを再開します(WCCP 経由)。 – CACHE:プロキシのキャッシュをクリアします。 **REPORTING**:レポート ユーティリティ レポート システムは現在有効になっています。 実行する操作を選択します。 – DELETEDB:レポート データベースを再度初期化します。 – DISABLE:レポート システムを無効にします。 – DBSTATS:データベースおよびエクスポート ファイルをリストします (export_files および always_onbox フォルダの下の未処理のファイルおよびフォルダのリストを表示します)。 – DELETEEXPORTDB:エクスポート ファイルを削除します (export_files および always_onbox フォルダの下の未処理のファイルおよびフォルダをすべて削除します)。 – DELETEJOURNAL:ジャーナル ファイルを削除します (すべての aclog_journal_files を削除します)。
dnsconfig	DNS サーバのパラメータを設定します。
dnsflush	アプライアンスの DNS エントリをフラッシュします。
etherconfig	イーサネット ポート接続を設定します。
featurekey	有効なキーを送信して、ライセンスされた機能をアクティブ化します。
featurekeyconfig	自動的に機能キーをチェックして更新します。
grep	指定された入力ファイルを検索して、特定のパターンに一致するものを含む行を見つけます。
help	コマンドのリストを返します。
ifconfig または interfaceconfig	M1、P1、P2 などのネットワーク インターフェイスを設定して管理します。現在設定されているインターフェイスを表示し、インターフェイスの作成、編集、削除のための操作メニューを提供します。
last	tty やホストなどのユーザ固有のユーザ情報を新しい順に並べて一覧表示したり、指定した日時にログインしたユーザのリストを表示します。
loadconfig	システム コンフィギュレーション ファイルをロードします。
logconfig	ログ ファイルへのアクセスを設定します。
mailconfig	指定されたアドレスに現在のコンフィギュレーション ファイルをメールで送信します。

maxhttpheadersize	プロキシ要求の最大 HTTP ヘッダー サイズを設定します。値をバイト単位で入力するか、キロバイトを表す場合は数値に K を付記します。 多数の認証グループに属するユーザの場合はポリシー トレースが失敗する可能性があります。また、HTTP 応答ヘッダーのサイズが現在の「最大ヘッダー サイズ」よりも大きい場合、失敗することがあります。この値を大きくすると、このような障害を軽減できます。最小値は 32 KB、デフォルト値は 32 KB、最大値は 1024 KB です。
networktuning	WSA は、複数のバッファおよび最適化アルゴリズムを使用して数百もの TCP 接続を同時に処理し、一般的な Web トラフィック（つまり、一時的な HTTP 接続）に対して高いパフォーマンスを実現します。 大容量ファイル（100 MB 以上）が頻繁にダウンロードされるような特定の状況では、バッファが大きいほど接続ごとのパフォーマンスが向上する可能性があります。ただし、全体的なメモリ使用量が増加するため、システムで使用可能なメモリに応じてバッファを増やす必要があります。 送信および受信スペース変数は、指定の TCP ソケットを介した通信用にデータを保存するために使用されるバッファを表します。自動送信および受信変数は、ウィンドウ サイズを動的に制御するための FreeBSD 自動調整アルゴリズムを有効または無効にするために使用されます。これら 2 つのパラメータは、FreeBSD カーネルに直接適用されます。 networktuning サブコマンドは、次のとおりです。 **SENDSPACE**：TCP 送信スペースのバッファ サイズ。8192 ～ 131072 バイトの範囲で、デフォルトは 16000 バイトです。 **RECVSPACE**：TCP 受信スペースのバッファ サイズ。8192 ～ 131072 バイトの範囲で、デフォルトは 32768 バイトです。 **SEND-AUTO**：TCP 送信の自動調整を有効または無効にします。1 はオン、0 はオフで、デフォルトはオフです。TCP 送信の自動調整を有効にする場合、必ず advancedproxyconfig > miscellaneous > Would you like proxy to perform dynamic adjustment of TCP send window size? の順に使用して、送信バッファの自動調整を無効にしてください。 **RECV-AUTO**：TCP 受信の自動調整を有効または無効にします。1 はオン、0 はオフで、デフォルトはオフです。TCP 受信の自動調整を有効にする場合、必ず advancedproxyconfig > miscellaneous > Would you like proxy to perform dynamic adjustment of TCP receive window size? の順に使用して、受信バッファの自動調整を無効にしてください。 **MBUF CLUSTER COUNT**：使用可能な mbuf クラスタの数を変更します。許容範囲は 98304 ～ 1572864 です。この値は、インストールされたシステム メモリによって変わります。98304 * (X/Y) の計算を使用し、X はシステム上の RAM のギガバイトで、Y は 4 GB です。たとえば 4 GB RAM の場合、推奨値は 98304 * (4/4) = 98304 になります。RAM が増加する場合は、線形スケーリングが推奨されます。 **SENDBUF-MAX**：最大送信バッファ サイズを指定します。範囲は 131072 ～ 2097152 バイトで、デフォルトは 1 MB（1048576 バイト）です。 **RECVBUF-MAX**：最大受信バッファ サイズを指定します。範囲は 131072 ～ 2097152 バイトで、デフォルトは 1 MB（1048576 バイト）です。

networktuning（続き）	**CLEAN-FIB-1**：データルーティング テーブルからすべての M1/M2 エントリを削除します。基本的には、コントロールプレーン/データプレーンの分離を有効にします。つまり、「分離ルーティング」が有効になっている場合に M1 インターフェイス経由のデータ送信からデータプレーン プロセスを無効にします。データプレーン プロセスは、「データ ルーティング テーブルの使用」が有効になっているプロセス、または非管理トラフィックを厳密に伝達するプロセスです。コントロールプレーン プロセスでは、依然として M1 または P1 インターフェイスのいずれかを介してデータを送信できます。 これらのパラメータに何らかの変更を行った後は、必ず変更を確定してアプライアンスを再起動してください。 ⚠ **注意**　副次的な影響を理解している場合にのみ、このコマンドを使用してください。TAC ガイダンスを受けている場合にのみ使用することを推奨します。
nslookup	指定されたホストとドメインの情報を取得したり、ドメイン内のホストのリストを印刷するために、インターネット ドメイン ネーム サーバに照会します。
ntpconfig	NTP サーバの設定現在設定されているインターフェイスを表示し、インターフェイスを追加、削除、または設定する操作メニューを提供します。このインターフェイスの IP アドレスから NTP クエリーが発信されます。
packetcapture	アプライアンスが接続されているネットワーク上で送受信されている TCP/IP などのパケットを代行受信して表示します。
passwd	パスフレーズを設定します。
pathmtudiscovery	パス MTU ディスカバリをイネーブルまたはディセーブルにします。 パケット フラグメンテーションが必要な場合は、パス MTU ディスカバリをディセーブルにすることができます。
ping	指定されたホストまたはゲートウェイに ICMP エコー要求を送信します。
proxyconfig <enable | disable>	Web プロキシをイネーブルまたはディセーブルにします。
proxystat	Web プロキシの統計情報を表示します。
quit、q、exit	アクティブなプロセスまたはセッションを終了します。
reboot	ファイル システム キャッシュをディスクにフラッシュし、実行中のすべてのプロセスを停止して、システムを再起動します。
resetconfig	出荷時の初期状態に設定を復元します。
revert	Web オペレーティング システム用の AsyncOS を以前の認定済みビルドに復元します。これは非常に危険な操作で、すべての設定ログおよびデータベースを破棄します。
rollovernow	ログ ファイルをロール オーバーします。
routeconfig	トラフィックの宛先 IP アドレスとゲートウェイを設定します。現在設定されているルートを表示し、エントリを作成、編集、削除、クリアするための操作メニューを提供します。
saveconfig	現在の設定のコピーをファイルに保存します。必要に応じて、このファイルを使用してデフォルトを復元できます。

setgateway	マシンのデフォルト ゲートウェイを設定します。
sethostname	hostname パラメータを設定します。
setntlmsecuritymode	NTLM 認証レルムのセキュリティ設定を、「ads」または「domain」に変更します。 • domain：AsyncOS は Active Directory ドメインにドメイン セキュリティ信頼アカウントを結合します。AsyncOS では、Active Directory はこのモードでネストされた Active Directory グループだけを使用する必要があります。 • ads：AsyncOS は、Active Directory のネイティブ メンバーとしてドメインを結合します。 デフォルト設定は ads です。
settime	システム時刻を設定します。
settz	現在のタイム ゾーンとタイム ゾーンのバージョンを表示します。ローカル タイム ゾーンを設定する操作メニューを提供します。
showconfig	すべての設定値を表示します。 **（注）**　ユーザのパスフレーズは暗号化されます。
shutdown	接続を終了してシステムをシャット ダウンします。
smtprelay	内部的に生成された電子メールの SMTP リレー ホストを設定します。SMTP リレー ホストは、システムで生成された電子メールやアラートを受け取るために必要です。
snmpconfig	SNMP クエリーをリッスンして SNMP 要求を受け入れるように、ローカル ホストを設定します。
sshconfig	信頼できるサーバのホスト名とホスト キー オプションを設定します。

sslconfig	アプライアンス管理 Web ユーザ インターフェイス、プロキシ サービス（HTTPS プロキシ、セキュア クライアントのクレデンシャル暗号化など）、セキュア LDAP サービス（認証、外部認証、セキュア モビリティなど）、アップデート サービスにおける、通信プロトコル TLS v1.x および SSL v3 の使用に関するコマンド。 VERSIONS：特定のサービスでイネーブルであるプロトコルを表示および変更します。 COMPRESS：TLS 圧縮をイネーブルまたはディセーブルにします。最高のセキュリティのためにディセーブルに設定することが推奨されます。 CIPHERS：選択したプロトコルで使用可能な追加/アップデート暗号スイートを追加します。 AsyncOS バージョン 9.0 以前のデフォルトの暗号は、DEFAULT:+kEDH です。AsyncOS バージョン 9.1 以降では、デフォルトの暗号は EECDH:DSS:RSA:!NULL:!eNULL:!EXPORT:!3DES:!RC4:!RC2:!DES:!SEED:!CAMELLIA:!SRP:!IDEA:!ECDHE-ECDSA-AES256-SHA:!ECDHE-RSA-AES256-SHA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA になります。いずれの場合も、ECDHE 暗号の選択によって変わる可能性があります。 **（注）** ただし、バージョンに関係なく、新しい AsyncOS バージョンにアップグレードする際にデフォルトの暗号は変わりません。たとえば、以前のバージョンから AsyncOS 9.1 にアップグレードする場合、デフォルトの暗号は DEFAULT:+kEDH です。つまり、アップグレード後に、現在の暗号スイートを自分で更新する必要があります。シスコでは、EECDH:DSS:RSA:!NULL:!eNULL:!EXPORT:!3DES:!RC4:!RC2:!DES:!SEED:!CAMELLIA:!SRP:!IDEA:!ECDHE-ECDSA-AES256-SHA:!ECDHE-RSA-AES256-SHA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA への更新を推奨します。 FALLBACK：SSL/TLS のフォールバック オプションをイネーブルまたはディセーブルにします。イネーブルの場合、リモート サーバとの通信は、ハンドシェイクの失敗後、最も低く設定されているプロトコルにフォールバックします。 プロトコル バージョンがクライアントとサーバの間でネゴシエートされると、実装の問題が原因でハンドシェイクが失敗する可能性があります。このオプションがイネーブルの場合、プロキシは現在設定されている TLS/SSL プロトコルの最も低いバージョンを使用して接続を試みます。 **（注）** AsyncOS 9.x の新規インストール時、フォールバックはデフォルトでディセーブルに設定されています。フォールバック オプションがある以前のバージョンからアップグレードする場合、現在の設定が保持されます。そうでない場合、つまりこのオプションがないバージョンからアップグレードする場合、フォールバックはデフォルトでイネーブルに設定されています。

sslconfig（続き）	ECDHE：LDAP での ECDHE 暗号の使用をイネーブルまたはディセーブルにします。 その後のリリースで追加の ECDH 暗号がサポートされていますが、追加の暗号とともに提供された特定の名前付き曲線が原因で、セキュア LDAP 認証と HTTPS トラフィック復号化の際中に、アプライアンスが接続をクローズする場合があります。追加の暗号の指定については、SSL の設定（12-22 ページ）を参照してください。 これらの問題がある場合は、このオプションを使用して、一方または両方の機能で ECDHE 暗号の使用をディセーブルにするか、またはイネーブルにします。
status	システム ステータスを表示します。
supportrequest	サポート要求の電子メールを Cisco IronPort カスタマー サポートに送信します。このメールには、マスター設定のコピーおよびシステム情報が含まれています。

tail	ログ ファイルの末尾を表示します。コマンドには、ログ ファイル名または番号をパラメータとして指定できます。
	
	`example.com> tail system_logs`
	
	`example.com> tail 9`

tcpservices	開かれている TCP/IP サービスに関する情報を表示します。
techsupport	Cisco IronPort カスタマー サポートがシステムにアクセスしてトラブルシューティングを支援できるように、一時的な接続を提供します。
testauthconfig	特定の認証レルムで定義された認証サーバに対して、そのレルムの認証設定をテストします。 `testauthconfig [-d level] [realm name]` オプションを指定せずにコマンドを実行すると、設定されている認証レルムのリストが表示されるので、そのリストから選択できます。 デバッグ フラグ（- d）によってデバッグ情報のレベルが制御されます。指定できるレベルの範囲は 0～10 です。指定しない場合は、レベル 0 が使用されます。レベル 0 の場合は、コマンドによって成功または失敗が返されます。テスト設定が失敗すると、失敗の原因が一覧表示されます。 **（注）** レベル 0 を使用することを推奨します。トラブルシューティングのためにさらに詳細な情報が必要な場合にのみ、別のデバッグ レベルを使用してください。
traceroute	ゲートウェイを通過し、宛先ホストまでのパスをたどって、IP パケットをトレースします。
tuiconfig tuistatus	これらの 2 つのコマンドについては、CLI を使用した透過的ユーザ識別の詳細設定（5-10 ページ）で説明しています。
updateconfig	アップデートおよびアップグレードを設定します。
updatenow	すべてのコンポーネントを更新します。
userconfig	システム管理者を設定します。
version	一般的なシステム情報、インストールされているシステム ソフトウェアのバージョン、およびルールの定義を表示します。

webcache	プロキシ キャッシュの内容を確認または変更したり、アプライアンスにキャッシュされないドメインと URL を設定します。管理者は特定の URL をプロキシ キャッシュから削除したり、プロキシ キャッシュに保存しないドメインや URL を指定できます。
who	CLI および Web インターフェイス セッションの両方について、システムにログインしているユーザを表示します。 **（注）**　各ユーザは、最大 10 の同時セッションを持つことができます。
whoami	ユーザ情報を表示します。

関連リソース

Cisco 通知サービス

セキュリティ アドバイザリ、フィールド ノーティス、販売終了とサポート終了の通知、およびソフトウェア アップデートと既知の問題に関する情報などの Cisco コンテンツ セキュリティ アプライアンスに関連する通知が配信されるように署名して参加します。

受信する情報通知の頻度やタイプなどのオプションを指定できます。使用する製品ごとの通知に個別に参加する必要があります。

参加するには、次に移動します。http://www.cisco.com/cisco/support/notifications.html

Cisco.com アカウントが必要です。ない場合は、リソースにアクセスするためのシスコ アカウントの登録（C-3 ページ）を参照してください。

ドキュメント セット

Cisco Web セキュリティ アプライアンスの関連資料は、以下の場所から入手できます。

製品	リンク
Web セキュリティ アプライアンスs （ハードウェア マニュアルを含む）。	http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html
Content セキュリティ管理アプライアンスs （ハードウェア マニュアルを含む）。	http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html
Cisco Cloud Web Security （ハードウェア マニュアルを含む）。	http://www.cisco.com/c/en/us/support/security/cloud-web-security/tsd-products-support-series-home.html

トレーニング

Cisco 電子メールおよび Web セキュリティ製品のトレーニングは以下で提供しています。

http://www.cisco.com/c/en/us/training-events/training-certifications/supplemental-training/email-and-web-security.html

ナレッジ ベースの記事（TechNotes）

ステップ 1　メイン製品ページにアクセスします（http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html）

ステップ 2　名前に **TechNotes** が付くリンクを探します。

シスコ サポート コミュニティ

Web セキュリティと関連管理については、以下の URL からシスコ サポート コミュニティにアクセスしてください。

https://supportforums.cisco.com/community/5786/web-security

シスコ サポート コミュニティは、Web セキュリティに関する一般的な問題や、特定のシスコ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。たとえば、投稿にトラブルシューティングのビデオが添えられていることもあります。

カスタマー サポート

Cisco TAC：http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

従来の IronPort のサポート サイト：http://www.cisco.com/web/services/acquisitions/ironport.html

仮想アプライアンスについては、『*Cisco Content Security Virtual Appliance Installation Guide*』を参照してください。

重大ではない問題の場合は、アプライアンスからサポート事例を開くこともできます。

関連項目

- サポートの使用（A-18 ページ）。

リソースにアクセスするためのシスコ アカウントの登録

Cisco.com の多数のリソースへアクセスするには、シスコのアカウントが必要です。

Cisco.com のユーザ ID をお持ちでない場合は、https://tools.cisco.com/RPF/register/register.do で登録できます。

サード パーティ コントリビュータ

AsyncOS に含まれてい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.

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

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

マニュアルに関するフィードバック

シスコのテクニカル マニュアル チームは、製品ドキュメントの向上に努めています。コメントおよびご提案をお待ちしています。以下のメール アドレスまでご意見をお寄せください：
contentsecuritydocs@cisco.com

このマニュアルの表紙に記載されているタイトルと発行日をメールの件名欄に記入してください。

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、以下の 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。

各種製品保証規定やシスコ製品に関するその他の情報は、以下の URL でご確認ください。

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.