AsyncOS 8.7 for Cisco Web Security Appliances ユーザ ガイド

発行日: 2015 年 3 月 31 日

Cisco Systems, Inc.
www.cisco.com

シスコは世界各国 200 箇所にオフィスを開設しています。
所在地、電話番号、FAX 番号
は以下のシスコ Web サイトをご覧ください。
www.cisco.com/go/offices.

AsyncOS 8.7 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、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 8.7 の新機能

機能	説明
ISE の統合	AsyncOS では、同じネットワーク上に展開されている Identity Services Engine（ISE）バージョン 1.3 サーバから追加のユーザ ID 情報にアクセスできるようになりました。
SSL の設定	セキュリティを強化するために、複数のサービスに対して SSLv3 をイネーブルまたはディセーブルにできます。SSLv3 がディセーブルになっているサービスは TLSv1.0 を使用します。 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、SaaS SSO、セキュア モビリティなど）、およびアップデート サービスに対して SSLv3 をイネーブルまたはディセーブルにできます。 Web インターフェイス（[システム管理（System Administration）] > [SSL 設定（SSL configuration）]）または CLI（`sslconfig`）を使用します。

AsyncOS 8.7 の要件および制約事項

AsyncOS 8.7 には次のような要件と制限事項がありますので注意してください。

- AsyncOS 8.7 は、Identity Services Engine のバージョン1.3 のみをサポートしています。
- このリリースの AsyncOS はコネクタ モードをサポートしていません。しかし、ISE 固有のオプションはコネクタ モードで動作している場合でも表示されるので、一見すると使用できるように見えます。繰り返しますが、コネクタ モードはサポートされていません。ご使用のシステムがコネクタ モードで稼働している場合は、このリリースに**アップグレードしないでください**。

Cisco AsyncOS 8.5 の新機能

機能	説明
高可用性	このリリースには、アプライアンスが明示モードでプロキシと連動する展開に適したハイアベイラビリティ オプションが組み込まれています。 詳細については、このマニュアルの「接続、インストール、設定」の章を参照してください。
2048 ビット証明書	アプライアンスによって生成または処理される SSL 証明書のキーの長さが 2048 ビットになりました。
LDAP 認証	アプライアンスの管理ユーザの認証のために LDAP プロトコルがサポートされるようになりました。
ボリューム クォータと時間クォータ	アクセス ポリシーと復号化ポリシーに時間およびボリューム クォータを適用できます。クォータを使用すると、与えられたデータ量と時間を使い切るまで、個々のユーザはインターネット リソース（またはインターネット リソース クラス）にアクセスできます。

機能	説明
Web セキュリティ仮想アプライアンスの機能の拡張	• VMWare ESXi 5.5 のサポート • ESXi でのシン プロビジョニングのサポート • 今回、仮想アプライアンスのライセンスの失効後に 6 か月の猶予期間が設けられました。この期間中、アプライアンスは Web トランザクションの処理を続行できますが、セキュリティ サービスはありません。 ライセンスの有効期限が近づいたときにアラートを送信するように、アプライアンスを設定できます。 • 評価機能キーを仮想アプライアンスに展開できるようになりました。
マシン ID による認証	Active Directory を使用するコネクタ モードでの展開に対して、このリリースでは、デバイス ID に基づいてアクセスを許可するオプションが導入されました。
高度なマルウェア防御機能の拡張	• 高度なマルウェア防御機能によって、アーカイブ ファイルや圧縮ファイル アーカイブのマルウェアを検出できるようになりました。 • AMP サーバとの通信に使用するインターフェイスを選択できます。 • ファイル分析で追加のファイル タイプの分析がサポートされるようになりました。サポートされるファイル タイプはクラウド サービスによって決定され、いつでも変更できます。 ファイル分析機能を設定すると、分析用に送信するファイル タイプを選択したり、オプションが変更されたときにアラートを受信することを選択したりできます。 サポートされるタイプとアラートの詳細については、リリース ノートの「Which Files Can Have their Reputation Evaluated and Be Sent for Analysis?」、およびオンライン ヘルプまたは本書の「ファイル レピュテーションとファイル分析」に関する章を参照してください。
AAA 監査ロギング	AsyncOS の機能が拡張され、複数のログ間で AAA 関連のロギングを標準化して、1 つの一元的なログ サブスクリプションに集約できるようになりました。この新しいログ サブスクリプションは syslog によってエクスポートできます。
パスワード セキュリティの強化	ローカルに定義された管理ユーザ用に次のパスワードの拡張機能が導入されました。 • 新しいパスワードを入力したユーザに対してパスワード強度インジケータが表示されます。 パスワードの強度は、指定したパスワード要件によって適用されます。 • パスワードでの特定の単語の使用を禁止します。(禁止する単語のリストをアプライアンスにアップロードします)。 • ボタンをクリックしてパスワードを生成するオプション。 詳細については、本書の「管理ユーザのパスワード要件の設定」および「ローカル ユーザ アカウントの追加」を参照してください。

機能	説明
Web トラッキング機能の強化	Web トラッキングの結果をマルウェア脅威別にフィルタリングする際に、新たに [すべてのマルウェア（All Malware）] オプションを使用できます。
Cisco コンテンツ セキュリティ管理仮想アプライアンス	物理ハードウェア アプライアンスと同じ機能を持つ仮想コンテンツ セキュリティ管理アプライアンスによって、複数の Web セキュリティ アプライアンスを管理できます。
信頼できるルート証明書管理	信頼できるルート証明書管理が [セキュリティ サービス（Security Services）] > [HTTPS プロキシ（HTTPS Proxy）] から [ネットワーク（Network）] > [証明書の管理（Certificate Management）] に移動されました。
DNS サーバのフェールオーバー	プライマリ DNS サーバがユーザに指定された数だけクエリーに応答しなかった場合、そのプライマリ サーバは失敗した見なされ、クエリーはセカンダリ サーバに自動的に転送されます。

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。

アプライアンス Web インターフェイスへのアクセス

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ワードを入力します。デフォルトで、アプライアンスには次のユーザ名とパスワードが付属します。

- ユーザ名：**admin**
- パスワード：**ironport**

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、ユーザ名やパスワード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イネーブル化

（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、次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。

接続、インストール、設定

接続、インストール、設定の概要

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、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、ネットワーク タップ、およびその他のプロキシ サーバまたは Web セキュリティ アプライアンスなどがあげられます。

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（System Setup Wizard）を使用して基本的なサービスと設定項目を設定し、Web インターフェイスを介して、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。

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（2-2 ページ）
2. 設定情報を収集して記録する。	設定情報の収集（2-5 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（2-6 ページ）
4. （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（2-13 ページ）

アプライアンスの接続

はじめる前に

- 『Cisco 170 Series Hardware Installation Guide』の説明に従って、アプライアンスをマウントし、管理用にアプライアンスを配線し、アプライアンスを電源に接続します。
- トランスペアレント 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。
- 次のシスコ推奨設定に注意を払ってください。
  - 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）	• アウトバウンド管理サービスで使用可能ですが、管理には使用できません。 • [ネットワーク（Network）] > [インターフェイス（Interfaces）] ページで、[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、トランスペアレント 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	トランスペアレント リダイレクション
P1/P2	P1 のみ: • [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）	[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　(任意)レイヤ4 トラフィックをモニタするには、プロキシ ポートの後ろと、クライアント IP アドレスのネットワーク アドレス変換(NAT)を実行するデバイスの前に、タップ、スイッチ、またはハブを接続します。

イーサネット ポート	注記
T1/T2	レイヤ4 トラフィック モニタのブロッキングを許可するには、Web セキュリティ アプライアンスと同じネットワーク上にレイヤ 4 トラフィック モニタを配置します。 **推奨設定** **デバイス:ネットワーク タップ:** • **ネットワーク タップに T1 を接続し、発信クライアント トラフィックを受信します。** • **ネットワーク タップに T2 を接続し、着信インターネット トラフィックを受信します。** その他のオプション: デバイス:ネットワーク タップ: • T1 でデュプレックス ケーブルを使用し、着信および発信トラフィックを受信します。 デバイス:スイッチ上のスパン化またはミラー化されたポート • 発信クライアント トラフィックを受信するように T1 を接続し、着信インターネット トラフィックを受信するように T2 を接続します。 • (準推奨)半二重または全二重ケーブルを使用して T1 を接続し、着信と発信の両方のトラフィックを受信します。 デバイス:ハブ: • (低推奨)デュプレックス ケーブルを使用して T1 を接続し、着信と発信の両方のトラフィックを受信します。 アプライアンスは、これらのインターフェイス上のすべての TCP ポートでトラフィックをリッスンします。

ステップ 4　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。

次のステップ

- 設定情報の収集(2-5 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(2-15 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(2-19 ページ)
- WCCP サービスの追加と編集(2-23 ページ)
- トランスペアレント リダイレクションの設定(2-22 ページ)
- アップストリーム プロキシ(2-13 ページ)

設定情報の収集

次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（System Setup Wizard）の実行時に必要な設定値を記録します。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（2-8 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

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（Routes）**	
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）**	
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）	

システム セットアップ ウィザードのワークシート

インターフェイスの詳細（Interface Details）		WCCP ルータ パスワード（WCCP Router Password）	
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）		管理者パスワード（Administrator Password）	
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）	
ホスト名（Hostname）		（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）			
ホスト名（Hostname）			

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（2-2 ページ）
- 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（2-5 ページ）
- 仮想アプライアンスでシステム セットアップ ウィザードの実行を準備する場合は、`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。
- システム セットアップ ウィザード（System Setup Wizard）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 ウィザードの参照情報（2-8 ページ）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や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（System Setup Wizard）を使用してください。**

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 アドレスを入力します。初めてシステム セットアップ ウィザード（System Setup Wizard）を実行するときは、次のデフォルトの 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、アプライアンスを現在設定している場合は、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ワードを入力します。デフォルトで、アプライアンスには次のユーザ名とパスワードが付属します。

- ユーザ名：**admin**
- パスワード：**ironport**

ステップ 3　[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。

ステップ 4　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（System Setup Wizard）を続行するには、[設定情報のリセット（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 3 から再開します。

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　必要に応じて表示された参照テーブルを使用し、すべての設定項目を設定します。

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、そのセクションの [編集（Edit）] ボタンをクリックします。

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。

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。「ページを検出できない（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。

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

表 2-1

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、次のエリア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と確認応答ページ • 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 システムの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 サーバを使用する（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。
[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。
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（Time Zone）]	メッセージ ヘッダーとログファイルのタイムスタンプに影響します。

関連項目

- DNS の設定（2-33 ページ）

ネットワーク/ネットワーク コンテキスト

（注）　別のプロキシ サーバを含むネットワークでWeb セキュリティ アプライアンスを使用する場合は、プロキシ サーバのダウンストリームで、クライアントのできるだけ近くに Web セキュリティ アプライアンスを配置することを推奨します。

表 2-2

プロパティ	説明
ネットワークには他の Web プロキシがありますか?（Is there another web proxy on your network?）	ネットワークに次のような別のプロキシがあるかどうか。 a.　トラフィックが通過する必要があるプロキシ b.　Web セキュリティ アプライアンスのアップストリームになるプロキシ 両方とも該当する場合は、チェックボックスをオンにします。これにより、1 つのアップストリーム プロキシのプロキシ グループを作成できます。後で、さらにアップストリーム プロキシを追加できます。
プロキシ グループ名（Proxy group name）	アプライアンスでプロキシ グループの識別に使用される名前。
アドレス（Address）	アップストリーム プロキシ サーバのホスト名または IP アドレス。
[ポート（Port）]	アップストリーム プロキシ サーバのポート番号。

関連項目

- アップストリーム プロキシ（2-13 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

プロパティ	説明
管理（Management）	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）、管理者は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。 （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）] チェックボックスをオンにします。 （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。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ことも必要です。

データ（Data）	P1 ポートのデータ トラフィックに使用する IP アドレス、ネットワーク マスク、およびホスト名。このポートは、管理ポートで使用されるサブネットとは異なるサブネットを使用する必要があります。 クライアントはここで指定されたホスト名を（ブラウザ プロキシの設定などで）使用できますが、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。 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。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（System Setup Wizard）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（System Setup Wizard）を終了してから行う必要があります。
レイヤ4 トラフィック モニタ（Layer-4 Traffic Monitor）	「T」インターフェイスに接続されている有線接続のタイプ： • **デュプレックス タップ。** T1 ポートは、着信と発信の両方のトラフィックを受信します。 • **シンプレックス タップ。** T1 ポートは（クライアントからインターネットへの）発信トラフィックを受信し、T2 ポートは（インターネットからクライアントへの）着信トラフィックを受信します。 シスコでは、パフォーマンスおよびセキュリティを向上させることができるため、可能な限りシンプレックスを使用することを推奨します。

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。

表 2-3

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。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

表 2-4

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 アプライアンスがトランスペアレント 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、またはトランスペアレント 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。
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。 WCCP バージョン 2 ルータに接続する場合、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（System Setup Wizard）の終了後に、標準サービスをイネーブルにできます。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、パスワードを入力することもできます。ここで使用されるパスワードは、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

表 2-5

プロパティ	説明
管理者パスワード（Administrator Password）	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ワード。
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。

表 2-5

プロパティ	説明
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

表 2-6

オプション	説明
グローバル ポリシーのデフォルト アクション（Global Policy Default Action）	システム セットアップ ウィザード（System Setup Wizard）の完了後、デフォルトで、すべての Web トラフィックをブロックするか、モニタするかを選択します。グローバル アクセス ポリシーのプロトコルとユーザ エージェントの設定を編集することで、後でこの動作を変更できます。デフォルトの設定は、トラフィックのモニタです。
L4 トラフィック モニタ（L4 Traffic Monitor）	システム セットアップ ウィザード（System Setup Wizard）の完了後、デフォルトで、レイヤ4 トラフィック モニタでモニタするか、疑わしいマルウェアをブロックするかを選択します。この設定は後で変更できます。デフォルトの設定は、トラフィックのモニタです。
使用許可コントロール（Acceptable Use Controls）	[使用許可コントロール（Acceptable Use Controls）] をイネーブルにするかどうかを指定します。 イネーブルにすると、使用許可コントロールにより、URL フィルタリングに基づいてポリシーを設定できます。また、アプリケーションの可視性と制御に加えて、セーフ サーチの適用などの関連オプションを使用できるようになります。デフォルトの設定はイネーブルです。
評価フィルタリング（Reputation Filtering）	グローバル ポリシー グループに対して Web レピュテーション フィルタリングをイネーブルにするかどうかを指定します。 Web 評価フィルタは、Web サーバの動作を分析し、評価スコアを URL に割り当て、URL ベースのマルウェアを含む可能性を判定するセキュリティ機能です。デフォルトの設定はイネーブルです。
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。デフォルトの設定では、3 つのオプションがすべてイネーブルになります。 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（System Setup Wizard）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。

表 2-6

オプション	説明
Cisco データ セキュリティ フィルタリング（Cisco Data Security Filtering）	Cisco データ セキュリティ フィルタをイネーブルにするかどうかを指定します。 イネーブルにすると、Cisco データ セキュリティ フィルタはネットワークから発信されるデータを評価し、ユーザは、特定タイプのアップロード要求をブロックするシスコ データ セキュリティ ポリシーを作成できます。デフォルトの設定はイネーブルです。

アップストリーム プロキシ

Web プロキシは、宛先 Web サーバに Web トラフィックを直接転送したり、ルーティング ポリシーを使用して Web トラフィックを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ができます。

- アップストリーム プロキシのタスクの概要（2-13 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（2-13 ページ）

アップストリーム プロキシのタスクの概要

作業	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（2-2 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（2-13 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。	インターネット要求を制御するポリシーの作成

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
名前（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（Load Balancing）	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次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、グループ内のさ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類似しています。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。

次のステップ。

- ポリシーの作成（10-5 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（2-15 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（2-15 ページ）

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、次の場合における 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（2-15 ページ）
- DNS の設定（2-33 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。

表 2-7

オプション	説明
Interfaces	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（管理）（M1 (Management)）]。AsyncOS には M1 用の 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 & P2（データ）（P1 & P2 (Data)）]。IPv4 アドレス、IPv6 アドレスを使用するか、または両方のバージョンを使用します。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は、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 を管理データ専用にして、データ トラフィック用に別のポートを使用するかどうかを指定します。 **（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）	アプライアンス管理サービスがリッスンする HTTP ポートと HTTPSポート。また、HTTPS に HTTP トラフィックをリダイレクトするかどうかを指定します。
L4 トラフィック モニタ（L4 Traffic Monitor）	L4 トラフィック モニタ インターフェイスは、デュプレックスまたはシンプレックス配線タイプの設定に使用されます。 • **デュプレックス。** T1 インターフェイスは、着信および発信トラフィックを受信します。 • **シンプレックス。** T1 は発信トラフィックを受信し、T2 は着信トラフィックを受信します。

ステップ 4　変更を送信し、保存します。

次の手順

- 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（2-2 ページ）。
- IP アドレスのバージョン（2-15 ページ）
- TCP/IP トラフィック ルートの設定（2-20 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 によって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り、IP 冗長性が実現されるので、それらのホストによって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。ハイ アベイラビリティは標準モードとコネクタ モードで機能します。

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。
- 次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）
  - ホスト名（Hostname）
  - 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て、共有秘密として使用する文字列を [共有秘密（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）　共有秘密、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、優先順位の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。

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（2-15 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。

`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次の IP アドレスを指定します。

関連項目

- アプライアンスの接続（2-2 ページ）。
- TCP/IP トラフィック ルートの設定（2-20 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、次の種類のトラフィックをルーティングする必要があります。

- **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、両方のトラフィックが設定済みのすべてのネットワーク インターフェイスに定義されているルートを使用します。ただし、M1 インターフェイスを管理トラフィックでのみ使用するように、ルートの分割（「分割ルーティング」）を選択できます。分割ルーティングをイネーブルにした場合、データ トラフィックはデータ インターフェイス用に設定されたルート（P1 および P2、ただし設定されている場合）のみを使用し、管理トラフィックは設定済みのすべてのネットワーク インターフェイス用に設定されたルートを使用します。

次の表は、ルートを分割した場合に、両方のインターフェイスを通過するトラフィックのタイプを示しています。ただし、以下の情報はデフォルトの動作を示しており、分割は、ルーティング テーブルではなく、アプリケーション層に基づいています。

表 2-8　M1 および P1/P2 分割ルートを経由するトラフィックのタイプ

M1	P1（および P2、ただし設定されている場合）
• WebUI • SSH • SNMP • DC による NTML 認証 • 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よって決まります。

- **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（[ポート M1 を制限（Restrict M1 port）] 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（[ポート M1 を制限（Restrict M1 port）] 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 トラフィックのルーティングの分割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（2-15 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（2-15 ページ）。

トランスペアレント リダイレクションの設定

トランスペアレント 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、次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（2-2 ページ）。
- WCCP サービスの設定（2-23 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。

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（トランスペアレント リダイレクション デバイスの指定（2-22 ページ）を参照）。

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　[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　次の手順に従って、WCCP のオプションを設定します。

表 2-9

WCCP サービス オプション	説明
[サービスプロファイル名]	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。

表 2-9

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、次の情報を入力します。 • **サービス 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します。 • **[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）** トランスペアレント 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。**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。
Router IP Addresses	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。
Router Security	このサービスグループのパスワード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 ルータは同じパスワードを使用する必要があります。

表 2-9

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（Load-Balancing Method）]。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、ハッシュ方式によって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）]。Allow Mask Only または Allow Hash or Mask 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。

表 2-9

WCCP サービス オプション	説明
詳細設定（Advanced）（続き）	**[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 プロキシにを転送されます。 **リターン方式。**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、次のメソッド タイプのいずれかが使用されます。 • **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。

ステップ 1　T1 や T2 インターフェイス上に VLAN を作成しないでください。CLI にアクセスします。

ステップ 2　次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　次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（2-15 ページ）。
- TCP/IP トラフィック ルートの設定（2-20 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、次のエリア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

システムの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 アプライアンスが MX レコードまたは設定済み SMTP リレー ホストにリストされているメール サーバ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。

表 2-10

プロパティ	説明
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。
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 サーバを追加します。

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、当該ドメインに対する権威サーバ（最終的な DNS レコードを提供）である必要があります。

- スプリット DNS（2-33 ページ）
- DNS キャッシュのクリア（2-33 ページ）
- DNS 設定の編集（2-34 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。
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を尊重しません。
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。ドメイン名を追加し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（2-20 ページ）
- IP アドレスのバージョン（2-15 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

Cisco クラウド Web セキュリティ プロキシへのアプライアンスの接続

この章の構成は、次のとおりです。

クラウド Web セキュリティ プロキシへのアプライアンスの接続：概要

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 クラウド Web セキュリティ プロキシに接続してトラフィックをルートします。Web セキュリティ アプライアンスの標準モードには、オンサイト Web プロキシ サービスとレイヤ4 トラフィック モニタが含まれており、これらのサービスは クラウド Web セキュリティ コネクタ モードでは使用できません。

クラウド コネクタと標準モード

クラウド Web セキュリティ コネクタ モードの Web セキュリティ アプライアンスには、標準モードで使用可能な機能のサブセットが含まれています。クラウド コネクタのサブセットに含まれる機能の使用方法は、どちらのモードでも同じです。

メニュー	クラウド コネクタ モードで使用可能	標準モードで使用可能
レポート	システム ステータス（System Status）	**システム ステータス（System Status）** 概要 Users Web サイト（Web Sites） URL Categories アプリケーションの表示（Application Visibility） マルウェア対策（Anti-Malware） 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） 定期レポート（Scheduled Reports） アーカイブ レポート（Archived Reports）

メニュー	クラウド コネクタ モードで使用可能	標準モードで使用可能
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）** **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）** **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）** ポリシー 復号化ポリシー（Decryption Policies） ルーティング ポリシー（Routing Policies） アクセス ポリシー（Access Policies） 全体の帯域幅制限（Overall Bandwidth Limits） Cisco データ セキュリティ（Cisco Data Security） 発信マルウェア スキャン（Outbound Malware Scanning） 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）

メニュー	クラウド コネクタ モードで使用可能	標準モードで使用可能
セキュリティ サービス	**Web プロキシ**	**Web プロキシ** FTP プロキシ（FTP Proxy） HTTPS プロキシ（HTTPS Proxy） PAC ファイル ホスティング（PAC File Hosting） SaaS のアイデンティティ プロバイダー（Identity Provider for SaaS） 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 ユーザ通知（End-User Notification） レイヤ4 トラフィック モニタ（Layer-4 Traffic Monitor） SensorBase レポート
ネットワーク	インターフェイス トランスペアレント リダイレクション（Transparent Redirection） ルート DNS 内部 SMTP リレー（Internal SMTP Relay） 認証 外部 DLP サーバ（External DLP Servers） Cloud Connector マシン ID サービス（Machine ID Service）	インターフェイス トランスペアレント リダイレクション（Transparent Redirection） ルート DNS 内部 SMTP リレー（Internal SMTP Relay） 認証 外部 DLP サーバ（External DLP Servers） 上位プロキシ（Upstream Proxy）

メニュー	クラウド コネクタ モードで使用可能	標準モードで使用可能
システム管理	Users	Users
	アラート（Alerts）	アラート（Alerts）
	ログ サブスクリプション（Log Subscriptions）	ログ サブスクリプション（Log Subscriptions）
	Network Access	Network Access
	タイム ゾーン	タイム ゾーン
	時刻設定（Time Settings）	時刻設定（Time Settings）
	設定の概要	設定の概要
	設定ファイル（Configuration File）	設定ファイル（Configuration File）
	ライセンス キー（Feature Keys）	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）	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 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）	システム セットアップ ウィザード（System Setup Wizard）
		ポリシー トレース（Policy Trace）
		返信先アドレス（Return Addresses）
		機能キーの設定（Feature Key Settings）
		次の手順

ドキュメントのリンク

この章は本書のさまざな個所と関連しており、標準モードと クラウド Web セキュリティ コネクタ 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。クラウドへのディレクトリ グループの送信に関する情報およびクラウド コネクタの設定情報を除き、関連情報は本書の他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 クラウド Web セキュリティ コネクタの設定に関する情報が含まれています。

本書には、Cisco Cloud Web Security製品に関する情報は記載されていません。Cisco Cloud Web Securityのドキュメントは Cisco.com から入手できます。

関連項目

- http://www.cisco.com/en/US/products/ps11720/tsd_products_support_series_home.html

展開

アプライアンスの展開は標準モードとクラウド セキュリティ モードのどちらにおいても同様ですが、オンサイト Web プロキシ サービスおよびレイヤ4 トラフィック モニタ サービスは、クラウド Web セキュリティ コネクタ モードでは使用できません。

クラウド Web セキュリティ コネクタは、明示的な転送モードまたはトランスペアレント モードで展開できます。

関連項目

- 第 2 章「接続、インストール、設定」

クラウド コネクタの設定

手順 1: Web セキュリティ アプライアンスの Web インターフェイスにアクセスする

ステップ 1　インターネット ブラウザに Web セキュリティ アプライアンスの IPv4 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（System Setup Wizard）を実行するときは、次のデフォルトの IPv4 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` はデフォルトの IPv4 アドレス、`8080` は、HTTP のデフォルトの管理ポート設定、`8443` は HTTPS のデフォルトの管理ポートです。

手順 2: ライセンス契約に同意してセットアップを開始する

ステップ 1　[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）] に移動します。

ステップ 2　ライセンス契約の条項を受け入れます。

ステップ 3　[セットアップの開始（Begin Setup）] をクリックします。

手順 3: システム設定項目を設定する

設定	説明
デフォルト システム ホスト名（Default System Hostname）	Web セキュリティ アプライアンスの完全修飾ホスト名。
DNS サーバ（DNS Server(s)）	ドメイン名サービス ルックアップ用のインターネット ルート DNS サーバ。
NTP サーバ（NTP Server）	システム クロックを同期させるサーバ。デフォルトは time.ironport.com です。
[タイムゾーン（Time Zone）]	アプライアンス上にタイム ゾーンを設定して、メッセージ ヘッダーおよびログ ファイルのタイムスタンプが正確に表示されるようにします。

関連項目

- DNS の設定（2-33 ページ）

手順 4: アプライアンスのモードを設定する

ステップ 1　[クラウド Web セキュリティ コネクタ（Cloud Web Security Connector）] を選択します。

手順 5: クラウド コネクタの設定項目を設定する

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。

（注）　後で [ネットワーク（Network）] > [クラウドコネクタ（Cloud Connector）] に移動して、これらの設定に戻ることができます。

関連項目

- セキュア データの漏洩防止（3-11 ページ）
- クラウドへのディレクトリ グループの送信（3-10 ページ）

手順 6: ネットワーク インターフェイスおよび配線を設定する

設定	説明
イーサネット ポート	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。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。
IPアドレス（IP Address）	Web セキュリティ アプライアンスの管理に使用する IPv4 アドレス。
ネットワーク マスク（Network Mask）	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ネットワーク マスク。
ホスト名（Hostname）	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。

関連項目

- ネットワーク インターフェイス（2-14 ページ）

手順 7: 管理およびデータ トラフィックのルートを設定する

設定	説明
デフォルト ゲートウェイ（Default Gateway）	管理インターフェイスやデータ 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 IPv4 アドレス。
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の 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。

関連項目

- TCP/IP トラフィック ルートの設定（2-20 ページ）

手順 8: 透過的接続の設定項目を設定する

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。

設定	説明
レイヤ4 スイッチ（Layer-4 Switch） または デバイスなし（No Device）	• Web セキュリティ アプライアンスはレイヤ 4 スイッチに接続されます。 または • 明示的な転送モードでクラウド コネクタを展開します。
WCCP v2 ルータ（WCCP v2 Router）	Web セキュリティ アプライアンスは WCCP バージョン 2 対応ルータに接続されます。 注: パスワードは任意であり、7 文字以内の文字を含めることができます。

関連項目

- トランスペアレント リダイレクションの設定（2-22 ページ）

手順 9: 管理設定項目を設定する

設定	説明
管理者パスワード（Administrator Password）	Web セキュリティ アプライアンスにアクセスするためのパスワード。パスワードは 6 文字以上にする必要があります。
システム アラート メールの送信先（Email system alerts to）	アプライアンスによって送信されるアラートの宛先メール 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 がシステムによって生成された電子メール メッセージの送信に使用する SMTP リレー ホストのホスト名またはアドレス。 デフォルトの SMTP リレー ホストは、MX レコードにリストされているメール サーバです。 デフォルトのポート番号は 25 です。
オートサポート（AutoSupport）	アプライアンスは、シスコ カスタマー サポートにシステム アラートと毎週のステータス レポートを送信できます。

関連項目

- アラートの管理（22-14 ページ）
- SMTP リレー ホストの設定（2-32 ページ）

手順 10: レビューおよびインストール

ステップ 1　インストールを確認します。

ステップ 2　前に戻って変更する場合は、[前へ（Previous）] をクリックします。

ステップ 3　入力した情報を使って続行する場合は、[この設定をインストール（Install This Configuration）] をクリックします。

クラウドのディレクトリ グループ ポリシー

Cisco Cloud Web Securityを使用し、ディレクトリ グループに基づいてアクセスを制御できます。Cisco Cloud Web Securityへのトラフィックがクラウド コネクタ モードの Web セキュリティ アプライアンスを介してルーティングされている場合、Cisco Cloud Web Securityは、グループ ベースのクラウド ポリシーを適用できるように、クラウド コネクタからトランザクションと共にディレクトリ グループ情報を受け取る必要があります。これを実現するには、クラウドに特定のディレクトリ グループを送信するように、クラウド コネクタを設定します。

- クラウドへのディレクトリ グループの送信（3-10 ページ）

クラウドへのディレクトリ グループの送信

はじめる前に

- Web セキュリティ アプライアンスの設定に認証レルムを追加します。

ステップ 1　[ネットワーク（Network）] > [クラウド コネクタ（Cloud Connector）] に移動します。

ステップ 2　[クラウド ポリシー ディレクトリ グループ（Cloud Policy Directory Groups）] 領域で、[グループの編集（Edit Groups）] をクリックします。

ステップ 3　Cisco Cloud Web Security 内で作成したクラウド ポリシーの対象となる [ユーザ グループ（User Groups）] と [マシン グループ（Machine Groups）] を選択します。

ステップ 4　[追加（Add）] をクリックします。

ステップ 5　[完了（Done）] をクリックして、変更を確定します。

関連情報

- 認証レルム（5-11 ページ）

クラウド プロキシ サーバのバイパス

クラウド ルーティング ポリシーを使用すると、以下の特性に基づいて、Web トラフィックを Cisco Cloud Web Security プロキシにルーティングしたり、インターネットに直接ルーティングできます。

- **識別プロファイル（Identification Profile）**
- プロキシ ポート（Proxy Port）
- Subnet
- URL Category
- ユーザ エージェント

Cloud Connector モードでクラウド ルーティング ポリシーを作成するプロセスは、標準モードを使用してルーティング ポリシーを作成するプロセスと同じです。

関連項目

- ポリシーの作成（10-5 ページ）

FTP および HTTPS

Cloud Connector モードの Web セキュリティ アプライアンスは、FTP や HTTPS を完全にはサポートしません。

- FTP（3-11 ページ）
- HTTPS（3-11 ページ）

FTP

FTP はクラウド コネクタでサポートされません。アプライアンスがクラウド コネクタ用に設定されている場合、AsyncOS はネイティブ FTP トラフィックをドロップします。

FTP over HTTP はクラウド コネクタ モードでサポートされます。

HTTPS

クラウド コネクタは復号化をサポートしていません。復号化せずに HTTPS トラフィックを渡します。

クラウド コネクタは復号化をサポートしていないため、AsyncOS は HTTPS トラフィックのクライアント ヘッダー情報に通常はアクセスできません。したがって、AsyncOS は、暗号化されたヘッダー情報に依存するルーティング ポリシーを通常は適用できません。これは、透過 HTTPS トランザクションでよくあることです。たとえば、透過 HTTPS トランザクションの場合、AsyncOS は HTTPS クライアント ヘッダー内のポート番号にアクセスできないため、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せん。この場合、AsyncOS はデフォルトのルーティング ポリシーを使用します。

明示的な HTTPS トランザクションの場合は 2 つの例外があります。AsyncOS は、明示的 HTTPS トランザクションの次の情報にアクセスできます。

- URL
- 宛先ポート番号

明示的 HTTPS トランザクションの場合は、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。

セキュア データの漏洩防止

[ネットワーク（Network）] > [外部 DLP サーバ（External DLP Servers）] で、クラウド コネクタを外部のデータ漏洩防止サーバと統合できます。

関連項目

- 第 16 章「機密データの漏洩防止」

クラウド コネクタ ログ

クラウド コネクタ ログには、認証されたユーザやグループ、クラウド ヘッダー、認証キーなど、クラウド コネクタの問題のトラブルシューティングに役立つ情報が含まれています。

- クラウド コネクタ ログへの登録（3-12 ページ）

クラウド コネクタ ログへの登録

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 Subsctiptions）] に移動します。

ステップ 2　[ログ タイプ（Log Type）] メニューから [クラウド コネクタ ログ（Cloud Connector Logs）] を選択します

ステップ 3　[ログ名（Log Name）] フィールドに名前を入力します。

ステップ 4　ログ レベルを設定します。

ステップ 5　変更を [実行（Submit）] して [確定する（Commit）] します。

関連項目

- 第 21 章「ログによるシステム アクティビティのモニタ」

ヒント　whoami.scansafe.net にアクセスして、設定したグループ名、ユーザ名、IP アドレスを確認してください。

識別プロファイルと認証

クラウド Web セキュリティ コネクタサポートは、基本的な認証と NTLM をサポートしています。また、特定の宛先に対して認証をバイパスできます。

クラウド コネクタ モードで Active Directory レルムを使用すると、トランザクション要求を特定のマシンから発信された要求として識別できます。マシン ID サービスは標準モードでは使用できません。

2 つの例外を除き、認証は Web セキュリティ アプライアンス全体で同様に機能します。標準構成であるかクラウド コネクタ構成であるかは問いません。次に例外を示します。

- マシン ID サービスは標準モードでは使用できません。
- アプライアンスがクラウド コネクタ モードに設定されている場合、AsyncOS は Kerberos をサポートしません。

（注）　ユーザ エージェントまたは宛先 URL に基づく 識別プロファイルは、HTTPS トラフィックに対応していません。

関連項目

- ポリシーの適用に対するマシンの識別（3-13 ページ）

- 未認証ユーザのゲスト アクセス（3-13 ページ）
- 第 6 章「エンドユーザおよびクライアント ソフトウェアの分類」
- 第 5 章「エンドユーザ クレデンシャルの取得」

ポリシーの適用に対するマシンの識別

マシン ID サービスを有効にすると、AsyncOS は、認証済みユーザや IP アドレスなどの識別子ではなく、トランザクション要求を実行したマシンに基づいてポリシーを適用できるようになります。AsyncOS は NetBIOS を使用してマシン ID を取得します。

はじめる前に

- マシン ID サービスは Active Directory レルムを介してのみ使用できることに注意してください。Active Directory レルムが設定されていない場合、このサービスはディセーブルになります。

ステップ 1　[ネットワーク（Network）] > [マシン ID サービス（Machine ID Service）] を選択します。

ステップ 2　[設定の有効化と編集（Enable and Edit Settings）] をクリックします。

ステップ 3　マシン ID の設定項目を設定します。

設定	説明
マシン ID の NetBIOS の有効化（Enable NetBIOS for Machine Identification）	マシン ID サービスをイネーブルにする場合に選択します。
Realm	トランザクション要求を開始しているマシンの識別に使用する Active Directory レルム。
失敗のハンドリング（Failure Handling）	AsyncOS がマシンを識別できない場合に、トランザクションをドロップするか、ポリシーの照合を続行するかを指定します。

ステップ 4　変更を [実行（Submit）] して [確定する（Commit）] します。

未認証ユーザのゲスト アクセス

Cloud Connector モードで、未認証ユーザにゲスト アクセスを提供するように Web セキュリティ アプライアンスが設定されている場合、AsyncOS は __GUEST_GROUP__ グループにゲスト ユーザを割り当て、その情報を Cisco Cloud Web Security に送信します。未認証ユーザにゲスト アクセスを提供するには、ID を使用します。これらのゲスト ユーザを管理するには、Cisco Cloud Web Security ポリシーを使用します。

関連項目

- 認証失敗後のゲスト アクセスの許可（5-31 ページ）

設定モード

システム セットアップ ウィザードを使用して、クラウド コネクタ モードと標準モードを切り替えることができます。

- クラウド コネクタ モードへの切り替え（3-14 ページ）

クラウド コネクタ モードへの切り替え

クラウド コネクタ モードへの切り替え

ステップ 1　[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。

ステップ 2　ライセンス契約に同意します。

ステップ 3　[アプライアンス モード（Appliance Mode）] セクションで [クラウド Web セキュリティ コネクタ（Cloud Web Security Connector）] を選択します。

ステップ 4　この章の前半の説明に従って、クラウド コネクタの設定を続行します。

関連項目

- クラウド コネクタの設定（3-6 ページ）

Web 要求の代行受信

Web 要求の代行受信の概要

Web セキュリティ アプライアンスは、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、ネットワーク タップ、およびその他のプロキシ サーバまたは Web セキュリティ アプライアンス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します。	• 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）次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 プロキシの接続および設定。 • ネットワーク インターフェイス ポリシーの設定。 • トランスペアレント リダイレクション デバイスの設定。 • TCP/IP ルートの設定。 • VLAN の設定。	• アップストリーム プロキシ（2-13 ページ） • ネットワーク インターフェイス（2-14 ページ） • トランスペアレント リダイレクションの設定（2-22 ページ） • TCP/IP トラフィック ルートの設定（2-20 ページ） • VLAN の使用によるインターフェイス能力の向上（2-27 ページ）
3.	（任意）Web プロキシのフォローアップ タスクを実行します。 • 転送モードまたはトランスペアレント 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する。 • IP スプーフィングを設定する。 • Web プロキシ キャッシュを管理する。 • カスタム Web 要求ヘッダーを使用する。 • 一部の要求に対してプロキシをバイパスする。	• Web 要求を代行受信するための Web プロキシ オプション（4-3 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（4-3 ページ） • Web プロキシ キャッシュ（4-5 ページ） • Web プロキシの IP スプーフィング（4-8 ページ） • Web プロキシのバイパス（4-10 ページ）
4.	次のクライアント 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する。 • クライアントとクライアント リソースを設定する。	• 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（4-11 ページ） • クライアント アプリケーションによる PAC ファイルの使用（4-12 ページ）
5.	（任意）FTP プロキシを有効化して設定します。	• FTP プロキシ サービス（4-15 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トランスペアレント モードのままにしておきます。トランスペアレント 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。追加のプロキシ モジュールを利用してプロトコル管理を向上させることができます。

- **FTP プロキシ。** FTP プロキシを使用すると、（HTTP でエンコードされた FTP トラフィックだけでなく）ネイティブ FTP トラフィックを代行受信できます。
- **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）　トランスペアレント 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。

- **SOCKS プロキシ。** SOCKS プロキシを使用すると、SOCKS トラフィックを代行受信できます。

これらの追加プロキシが機能するためには、Web プロキシが必要です。Web プロキシをディセーブルにした場合は、これらのプロキシをイネーブルにできません。

（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。

関連項目

- FTP プロキシ サービス（4-15 ページ）。
- SOCKS プロキシ サービス（4-17 ページ）

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
HTTP Ports to Proxy	Web プロキシが HTTP 接続をリッスンするポート
Caching	Web プロキシによるキャッシュをイネーブルにするかディセーブルにするか指定します。 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。 • [トランスペアレント（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。
IP Spoofing	• [IP スプーフィングの有効化（IP Spoofing enabled）]：Web プロキシは、セキュリティを向上させるために、要求の送信元 IP アドレスを変更して Web プロキシのアドレスに一致させます。 • [IP スプーフィングの無効化（IP Spoofing disabled）]：Web プロキシは送信元アドレスを維持するので、Web セキュリティ アプライアンスではなく送信元クライアントから発信されたように見えます。

ステップ 4　必要に応じて Web プロキシの詳細設定を設定します。

プロパティ	説明
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。
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。

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。
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「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。
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）。
- トランスペアレント リダイレクションの設定（2-22 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。

```
vm10wsa0019.qa> 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　次の例のように、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、正規表現（9-21 ページ）を参照してください。

ステップ 6　値の入力を終了するには、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た場合、キャッシングが最も少なく、RFC #2616 に最も準拠しています。
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 には最小限準拠します。最適化モードと比較した場合、アグレッシブ モードでは、Web プロキシ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をキャッシュします。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 IP スプーフィング

デフォルトでは、Web プロキシは要求を転する際に、自身のアドレスに合わせて要求の送信元 IP アドレスを変更します。これによってセキュリティは向上しますが、この動作は IP スプーフィングを実装することによって変更できます。IP スプーフィングを使用すると、要求は送信元アドレスを維持するので、Web セキュリティ アプライアンスからではなく、送信元クライアントから発信されたように見えます。

IP スプーフィングは、透過的または明示的に転送されたトラフィックに対して機能します。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、IP スプーフィングを、透過的にリダイレクトされた接続に対してのみイネーブルにするか、すべての接続（透過的にリダイレクトされた接続と明示的に転送された接続）に対してイネーブルにするかを選択できます。明示的に転送された接続で IP スプーフィングを使用する場合は、リターンパケットを Web セキュリティ アプライアンスにルーティングする適切なネットワーク デバイスがあることを確認してください。

IP スプーフィングがイネーブルで、アプライアンスが WCCP ルータに接続されている場合は、2 つの WCCP サービス（送信元ポートに基づくサービスと宛先ポートに基づくサービス）を設定する必要があります。

関連項目

- Web プロキシの設定（4-3 ページ）。
- WCCP サービスの設定（2-23 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 ヘッダーを追加して、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　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 セキュリティ アプライアンス 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、次のことが可能になります。

- プロキシ サーバへの接続に HTTP ポートを使用しているが、適切に機能しない HTTP 非対応（または独自の）プロトコルが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作用します。Web プロキシは、トランスペアレント 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 セキュリティ アプライアンス 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。次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。

- **プロキシ自動設定（PAC）ファイルを使用してクライアントを設定する。**PAC ファイルは、Web 要求の送信先をクライアントに指示します。このオプションを使用すると、プロキシの詳細に対する以降の変更を一元管理できます。

PAC ファイルを使用する場合は、PAC ファイルの保存場所とクライアントがそれらを検出する方法を選択する必要があります。

関連項目

- クライアント アプリケーションによる PAC ファイルの使用（4-12 ページ）。

クライアント アプリケーションによる PAC ファイルの使用

プロキシ自動設定（PAC）ファイルのパブリッシュ オプション

クライアントがアクセスできる場所に PAC ファイルをパブリッシュする必要があります。有効な場所は次のとおりです。

- Web サーバ。
- **Web セキュリティ アプライアンス。**PAC ファイルを Web セキュリティ アプライアンスに配置できます。これはクライアントでは Web ブラウザとして表示されます。アプライアンスには、さまざまなホスト名、ポート、ファイル名を使用している要求に対応する機能など、PAC ファイルを管理するための追加オプションもあります。
- ローカル マシン。クライアントのハード ディスクに PAC ファイルをローカルに配置できます。ただし、この方法は一般的なソリューションとしてお勧めしません（自動 PAC ファイルの検出には適していませんが、テストする場合には有用です）。

関連項目

- Web セキュリティ アプライアンスでの PAC ファイルのホスティング（4-13 ページ）。
- クライアント アプリケーションでの PAC ファイルの指定（4-14 ページ）。

プロキシ自動設定（PAC）ファイルを検索するクライアント オプション

クライアントに対して PAC ファイルを使用する場合は、クライアントが PAC ファイルを検索する方法を選択する必要があります。次の 2 つの対処法があります。

- **PAC ファイルの場所をクライアントに設定する。**PAC ファイルを指し示す URL をクライアントに設定します。
- **PAC ファイルの場所を自動的に検出するようにクライアントを設定する。**DHCP または DNS とともに WPAD プロトコルを使用して PAC ファイルを自動的に検索するように、クライアントを設定します。

PAC ファイルの自動検出

WPAD は、DHCP および DNS ルックアップを使用してブラウザが PAC ファイルの場所を判別できるようにするプロトコルです。

- **DHCP と共に WPAD を使用するには**、DHCP サーバに PAC ファイルの場所の URL と共にオプション 252 を設定します。ただし、すべてのブラウザが DHCP をサポートしているわけではありません。
- **DNS と共に WPAD を使用するには**、PAC ファイルのホスト サーバを指し示すように DNS レコードを設定します。

いずれかまたは両方のオプションを設定できます。WPAD は最初に DHCP を使用して PAC ファイルの検出を試み、検出できなかった場合は DNS を使って試みます。

関連項目

- クライアントでの PAC ファイルの自動検出（4-15 ページ）

Web セキュリティ アプライアンスでの PAC ファイルのホスティング

ステップ 1　[セキュリティ サービス（Security Services）] > [PAC ファイル ホスティング（PAC File Hosting）] を選択します。

ステップ 2　[設定の有効化と編集（Enable and Edit Settings）] をクリックします。

ステップ 3　（任意）次の基本設定項目を設定します。

オプション	説明
PAC サーバ ポート（PAC Server Ports）	Web セキュリティ アプライアンスが PAC ファイル要求のリッスンに使用するポート。
PAC ファイルの有効期限（PAC File Expiration）	ブラウザ キャッシュで指定されている分数が経過した後に PAC ファイルを期限切れにできます。

ステップ 4　[PAC ファイル（PAC Files）] セクションで [参照（Browse）] をクリックし、Web セキュリティ アプライアンスにアップロードする PAC ファイルをローカル マシンから選択します。

（注）　選択したファイルの名前が `default.pac` である場合は、ブラウザで場所を設定するときにファイル名を指定する必要がありません。名前が指定されていない場合、Web セキュリティ アプライアンスは `default.pac` というファイルを検索します。

ステップ 5　[アップロード（Upload）] をクリックして、ステップ 4 で選択した PAC ファイルを Web セキュリティ アプライアンスにアップロードします。

ステップ 6　（任意）[PAC ファイルサービスを直接提供するホスト名（Hostnames for Serving PAC Files Directly）] セクションで、ポート番号を含まない PAC ファイル要求のホスト名と関連ファイル名を設定します。

オプション	説明
ホスト名（Hostname）	Web セキュリティ アプライアンスが要求を処理する場合に、PAC ファイル要求に含める必要があるホスト名。要求にはポート番号が含まれていないため、要求は Web プロキシの HTTP ポート（ポート 80）を使用して処理され、ホスト名評価から PAC ファイル要求として識別できます。
プロキシ ポートを通じた「GET」要求に対するデフォルト PAC ファイル（Default PAC File for "Get/" Request through Proxy Port）	同じ行のホスト名に関連付けられる PAC ファイル名。ホスト名に対する要求は、ここで指定した PAC ファイルを返します。 アップロード済みの PAC ファイルのみを選択できます。
行を追加（Add Row）	別の行を追加して、追加のホスト名と PAC ファイル名を指定します。

ステップ 7　変更を送信し、保存します。

クライアント アプリケーションでの PAC ファイルの指定

- クライアントでの PAC ファイルの場所の手動設定（4-14 ページ）
- クライアントでの PAC ファイルの自動検出（4-15 ページ）

クライアントでの PAC ファイルの場所の手動設定

ステップ 1　PAC ファイルを作成してパブリッシュします。

ステップ 2　ブラウザの PAC ファイル設定領域に PAC ファイルの場所を示す URL を入力します。

Web セキュリティ アプライアンスが PAC ファイルをホストしている場合、有効な URL 形式は次のようになります。

```
http://server_address[.domain][:port][/filename] | http://WSAHostname[/filename]
```

WSAHostname は、Web セキュリティ アプライアンスに PAC ファイルをホストするときに設定した [ホスト名（hostname）] の値です。ホストしていない場合、URL の形式は格納場所と（場合によっては）クライアントに応じて異なります。

関連項目

- Web セキュリティ アプライアンスでの PAC ファイルのホスティング（4-13 ページ）。

クライアントでの PAC ファイルの自動検出

ステップ 1　wpad.dat という名前の PAC ファイルを作成し、Web サーバまたは Web セキュリティ アプライアンスにパブリッシュします（DNS と共に WPAD を使用する場合は、Web サーバのルート フォルダにファイルを配置する必要があります）。

ステップ 2　次の MIME タイプで .dat ファイルを設定するように Web サーバを設定します。

```
application/x-ns-proxy-autoconfig
```

（注）　Web セキュリティ アプライアンスはこれを自動的に実行します。

ステップ 3　DNS ルックアップをサポートするには、「wpad」から始まる、内部的に解決可能な DNS 名を作成して（例：wpad.example.com）、wpad.dat ファイルをホストしているサーバの IP アドレスに関連付けます。

ステップ 4　DHCP ルックアップをサポートするには、DHCP サーバのオプション 252 に wpad.dat ファイルの場所の URL を設定します（例：「http://wpad.example.com/wpad.dat」）。URL には、IP アドレスなど、有効な任意のホスト アドレスを使用できます。特定の DNS エントリは必要ありません。

関連項目

- クライアント アプリケーションによる PAC ファイルの使用（4-12 ページ）。
- Web セキュリティ アプライアンスでの PAC ファイルのホスティング（4-13 ページ）。

FTP プロキシ サービス

FTP プロキシ サービスの概要

Web プロキシは、次の 2 種類の FTP 要求を代行受信できます。

- **ネイティブ FTP。**ネイティブ FTP 要求は、専用 FTP クライアントによって生成されます（または、ブラウザで組み込みの FTP クライアントを使用して生成されます）。FTP プロキシが必要です。
- **FTP over HTTP。**ブラウザは、ネイティブ FTP を使用する代わりに、HTTP 要求内に FTP 要求をエンコードすることがあります。FTP プロキシは必要ありません。

関連項目

- FTP プロキシの有効化と設定（4-16 ページ）。
- FTP 通知メッセージの設定（17-14 ページ）。

FTP プロキシの有効化と設定

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

ステップ 2　[設定の有効化と編集(Enable and Edit Settings)] をクリックします(表示されるオプションが [設定の編集(Edit Settings)] だけの場合、FTP プロキシは設定済みです。)

ステップ 3　(任意)基本的な FTP プロキシ設定項目を設定します。

プロパティ	説明
Proxy Listening Port	FTP プロキシが FTP 制御接続をリッスンするポート。クライアントは、(FTP サーバに接続するためのポート(通常はポート 21 を使用)としてではなく)FTP プロキシを設定するときにこのポートを使用する必要があります。
Caching	匿名ユーザからのデータ接続をキャッシュするかどうか。 **(注)**　匿名ではないユーザからのデータはキャッシュされません。
Server Side IP Spoofing	FTP プロキシが FTP サーバの IP アドレスをシミュレートできるようにします。これによって、IP アドレスが制御接続とデータ接続で異なる場合に、トランザクションを許可しない FTP クライアントに対応できます。
Authentication Format	FTP クライアントと通信するときに FTP プロキシが使用する認証形式を選択できるようにします。
Passive Mode Data Port Range	パッシブ モード接続で FTP プロキシとのデータ接続を確立するために FTP クライアントが使用する TCP ポートの範囲。
Active Mode Data Port Range	アクティブ モード接続で FTP プロキシとのデータ接続を確立するために FTP サーバが使用する TCP ポートの範囲。この設定は、ネイティブ FTP と FTP over HTTP の両方の接続に適用されます。 ポート範囲を大きくすると、同じ FTP サーバからのさらに多くの要求に対応できます。TCP セッションの TIME-WAIT 遅延(通常数分)によって、ポートは使用された直後に、*同じ* FTP サーバで再び使用できるようになりません。その結果、所定の FTP サーバは短時間アクティブ モードで *n* 回以上 FTP プロキシに接続できません。ここでは *n* は、このフィールドに指定されたポート数です。
Welcome Banner	接続時に FTP クライアントに表示されるウェルカム バナー。次から選択します。 • **[FTP サーバメッセージを(FTP server message)]。**メッセージは宛先 FTP サーバによって表示されます。このオプションは、Web プロキシがトランスペアレント モードに設定されている場合にのみ利用でき、トランスペアレント接続にのみ適用されます。 • **[カスタム メッセージ(Custom message)]。**このオプションをオンにすると、すべてのネイティブ FTP 接続に対してこのカスタム メッセージが表示されます。オフにした場合は、明示的な転送ネイティブ FTP 接続に使用されます。

ステップ 4　(任意)FTP プロキシの詳細設定を設定します。

プロパティ	説明
Control Connection Timeouts	現在のトランザクションが完了していない場合に、アイドル状態の FTP クライアントまたは FTP サーバからの制御接続による通信を、FTP プロキシがさらに待機する最大時間(秒単位)。 • **[クライアント側(Client side)]。**アイドル状態の FTP クライアントとの制御接続のタイムアウト値。 • **[サーバ側(Server side)]。**アイドル状態の FTP サーバとの制御接続のタイムアウト値。
Data Connection Timeouts	現在のトランザクションが完了していない場合に、アイドル状態の FTP クライアントまたは FTP サーバからのデータ接続による通信を、FTP プロキシがさらに待機する時間。 • **[クライアント側(Client side)]。**アイドル状態の FTP クライアントとのデータ接続のタイムアウト値。 • **[サーバ側(Server side)]。**アイドル状態の FTP サーバとのデータ接続のタイムアウト値。

ステップ 5　変更を送信し、保存します。

関連項目

- FTP プロキシ サービスの概要(4-15 ページ)。
- FTP over HTTP 接続に適用されるプロキシ設定を設定するには、Web プロキシの設定(4-3 ページ)を参照してください。

SOCKS プロキシ サービス

SOCKS プロキシ サービスの概要

Web セキュリティ アプライアンスには、SOCKS トラフィックを処理するための SOCKS プロキシが含まれます。SOCKS ポリシーは、アクセス ポリシーと同等であり、SOCKS トラフィックを制御します。アクセス ポリシーと同様に、ID を使用して、どの SOCKS ポリシーによってどのトランザクションを管理するかを指定できます。SOCKS ポリシーをトランザクションに適用すると、ルーティング ポリシーによってトラフィックのルーティングを管理できます。

SOCKS トラフィックの処理のイネーブル化

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）] > [SOCKS プロキシ（SOCKS 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　[SOCKS プロキシを有効にする（Enable SOCKS Proxy）] 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）]）。

SOCKS プロキシの設定

ステップ 1　[セキュリティ サービス（Security Services）] > [SOCKS プロキシ（SOCKS 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　[SOCKS プロキシを有効にする（Enable SOCKS Proxy）] を選択します。

ステップ 4　基本および高度な SOCKS プロキシ設定を設定します。

プロパティ	説明
SOCKS プロキシ	イネーブル。
SOCKS Control Ports	SOCKS 要求を受け入れるポート。デフォルトは 1080 です。
UDP Request Ports	SOCKS サーバがリッスンする必要がある UDP ポート。デフォルトは 16000 ～ 16100 です。
Proxy Negotiation Timeout	ネゴシエーション段階で SOCKS クライアントからデータを送受信するのを待機する時間（秒単位）。デフォルトは 60 です。
UDP Tunnel Timeout	UDP トンネルを閉じる前に UDP クライアントまたはサーバからのデータを待機する時間（秒単位）。デフォルトは 60 です。

SOCKS ポリシーの作成

ステップ 1　[Web セキュリティ マネージャ（Web Security Manager）] > [SOCKS ポリシー（SOCKS Policies）] を選択します。

ステップ 2　[ポリシーを追加（Add Policy）] をクリックします。

ステップ 3　[ポリシー名（Policy Name）] フィールドに名前を割り当てます。

（注）　各ポリシー グループ名は、英数字またはスペース文字のみを含む、一意の名前とする必要があります。

ステップ 4　（任意）説明を追加します。

ステップ 5　[上記ポリシーを挿入（Insert Above Policy）] フィールドで、この SOCKS ポリシーに挿入する SOCKS ポリシーの場所を選択します。

（注）　複数の SOCKS ポリシーを設定する場合、各ポリシーの論理的な順序を決定します。照合が適切に行われるように、ポリシーの順序を指定してください。

ステップ 6　[アイデンティティとユーザ（Identities and Users）] セクションで、このグループ ポリシーに適用する 1 つ以上の ID を選択します。

ステップ 7　（任意）[詳細（Advanced）] セクションを拡張して、追加のメンバーシップ要件を定義します。

高度なオプション	説明
プロキシ ポート（Proxy Ports）	ブラウザに設定されたポート。 （任意）Web プロキシへのアクセスに使用するプロキシ ポートによってポリシー グループのメンバーシップを定義します。[プロキシ ポート（Proxy Ports）] フィールドに、1 つ以上のポート番号を入力します。複数のポートを指定する場合は、カンマで区切ります。 あるポート上に要求を明示的に転送するように設定されたクライアントのセットがあり、別のポート上に要求を明示的に転送するように設定された別のクライアントのセットがある場合、プロキシ ポート上でポリシー グループのメンバーシップを定義することがあります。 （注）　このポリシー グループに関連付けられている ID が この詳細設定によって ID メンバーシップを定義している場合、SOCKS ポリシー グループ レベルではこの設定項目を設定できません。
サブネット（Subnets）	（任意）サブネットまたは他のアドレスでポリシー グループのメンバーシップを定義します。 関連付けられた ID で定義できるアドレスを使用するか、または特定のアドレスをここに入力できます。 （注）　ポリシー グループに関連付けられている ID が、アドレスによってグループのメンバーシップを定義している場合は、このポリシー グループに、ID のアドレスのサブセットであるアドレスを入力する必要があります。ポリシー グループにアドレスを追加することにより、このグループ ポリシーに一致するトランザクションのリストを絞り込めます。
時間範囲（Time Range）	（任意）時間範囲別にポリシー グループのメンバーシップを定義します。 1. [時間範囲（Time Range）] から時間範囲を選択します。 2. このポリシー グループが選択した時間範囲内または範囲外の時間に適用されるかどうかを指定します。

ステップ 8　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

- （任意）SOCKS ポリシーで使用するための ID を追加します。
- SOCKS トラフィックを管理する 1 つ以上の SOCKS ポリシーを追加します。

要求の代替受信に関するトラブルシューティング

- URL カテゴリが一部の FTP サイトをブロックしない（A-5 ページ）
- 大規模 FTP 転送の切断（A-5 ページ）
- 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（A-5 ページ）
- 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（A-20 ページ）
- 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（A-14 ページ）
- 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（A-14 ページ）

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	作業	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（5-17 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（5-22 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（External Authentication）（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（5-28 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（5-36 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 ID 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.	ID 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。	• ポリシーによる Web 要求の管理：ベスト プラクティス（10-2 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。

認証の計画

- Active Directory/Kerberos（5-3 ページ）
- Active Directory/基本（5-4 ページ）
- Active Directory/NTLMSSP（5-5 ページ）
- LDAP/基本（5-5 ページ）
- ユーザの透過的識別（5-6 ページ）

Active Directory/Kerberos

明示的な転送	トランスペアレント、IP ベースのキャッシング	トランスペアレント、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 • パスワード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/基本

明示的な転送	トランスペアレント、IP ベースのキャッシング	トランスペアレント、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 • パスワード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ワードがクリア 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 • パスワードがクリア 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 • パスワードがクリア テキスト（Base64）として送信される

Active Directory/NTLMSSP

明示的な転送	トランスペアレント
利点： • パスワード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 トランスペアレント NTLMSSP 認証はトランスペアレント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ワードではなく、チャレンジ/レスポンス認証を使用します。 トランスペアレント NTLM 認証を使用する利点と欠点は、トランスペアレント基本認証を使用する場合と同様です。ただし、**トランスペアレント NTLM 認証には、パスワード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	トランスペアレント
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ワードがクリア テキスト（Base64）として送信される 回避策： • 認証の失敗（5-30 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 • パスワードがクリア 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（5-30 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ワード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。

トランスペアレント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（5-32 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次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。Identity Services Engine サービスの統合に必要なタスク（8-2 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。リモート ユーザ（10-18 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、次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、および設定の詳細については、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、ユーザのパスワード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。

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、次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。基本的な手順は次のとおりです。

- 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 は次の 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 mapping timeout for Novell eDirectory**：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、次のような 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** をトランスペアレント 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 sethostname CLI コマンド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（External Authentication）（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（5-17 ページ）
- 認証レルムの削除について（5-22 ページ）
- グローバル認証の設定（5-22 ページ）

関連項目

- RADIUS ユーザ認証（22-8 ページ）
- 認証シーケンス（5-28 ページ）

外部認証（External Authentication）

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（5-17 ページ）

手順

ステップ 1　アプライアンスで外部認証をイネーブルにします。

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. 次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対して、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（22-9 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。
  - 次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。
  - ドメイン管理者のメンバーであるユーザを Active Directory サーバ上に作成します。
  - 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。
  - トランスペアレント 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（5-22 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（5-10 ページ） を参照）。

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のみです。

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。

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。

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ワード）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。（5-22 ページ）」を参照してください。

ステップ 10　変更を送信し、保存します。

ヒント　[%m] カスタム フィールドのパラメータを使用するように、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（21-30 ページ）を参照してください。

トラブルシューティング ツール

Kerberos チケットのキャッシュを表示および消去するための KerbTray または klist（どちらも Windows Server Resource Kit に付属）。Active Directory を表示および編集するための Active Directory Explorer。Wireshark は、ネットワークのトラブルシューティングに使用できるパケット アナライザです。

次のステップ

- 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）

はじめる前に

- 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。
- 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（5-10 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

次のルールは、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 [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のみです。

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。
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。

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 ユーザ名とパスワードを入力します。

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 に関する次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。

設定	説明
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あります。 **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。
LDAP 持続的接続（LDAP Persistent Connections） （[詳細設定（Advanced）] セクションの下）	次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対応します。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）]**。常に、LDAP サーバへの新しい接続を作成します。

設定	説明
ユーザ認証	次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。例：`dc=companyname, dc=com`。 **[ユーザ名属性（User Name Attribute）]** 次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 ディレクトリにおける一意の ID。 • **[custom]。**カスタム ID（`UserAccount` など）。 **[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、またはユーザのベース DN のユーザ固有の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。 次の値のいずれかを選択します。 • **[none]。**任意のユーザを抽出します。 • **[custom]。**特定のユーザ グループを抽出します。
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、次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。 • **[パスワード（Password）]。**[バインド DN（Bind DN）] フィールドに入力したユーザに関連付けられているパスワード。 次のテキストは、[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。 次の値のいずれかを選択します。 • **[member] および [uniquemember]。**グループ メンバーを指定する、LDAP ディレクトリで一意の ID。 • **[custom]。**カスタム ID(`UserInGroup` など)。
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。 次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。 • **[custom]。**カスタム ID(`FinanceGroup` など)。
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。 次の値のいずれかを選択します。 • **objectclass=groupofnames** • **objectclass=groupofuniquenames** • **objectclass=group** • **[custom]。**カスタム フィルタ(`objectclass=person` など)。 **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。 次の値のいずれかを選択します。 • **[memberOf]。**ユーザ メンバーを指定する、LDAP ディレクトリで一意の ID。 • **[カスタム(custom)]。**カスタム ID(`UserInGroup` など)。
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。

ユーザ オブジェクト設定	説明
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。 次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。 • **[custom]。**カスタム ID（`FinanceGroup` など）。
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。 次の値のいずれかを選択します。 • **objectclass=groupofnames** • **objectclass=groupofuniquenames** • **objectclass=group** • **[custom]。**カスタム フィルタ（`objectclass=person` など）。 **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（LDAP External Authentication Query）] 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。

クエリー文字列（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。
クエリー文字列（Query String）	`(&(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。(5-22 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。

次の手順

- 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(External Authentication)(5-11 ページ)

複数の NTLM レルムとドメインの使用

次のルールは、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、トランスペアレント 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

- 次の概念をよく理解しておいてください。
  - 認証の失敗（5-30 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（5-32 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）	次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）]**。ユーザが認証されたかのように、処理が続行されます。 • **[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。
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（5-31 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（5-32 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、ユーザ名とパスワード、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（トランスペアレント 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プロキシがトランスペアレント モードで展開されている場合は、次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（5-30 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。
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。 トランスペアレント 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。 次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)）]。**このフィールドには、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。

設定	説明
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。
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、次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（5-30 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。
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。 次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)）]。**このフィールドには、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。

設定	説明
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。
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 NTLMSPP 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次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

次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 ID を設定し、ID 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

- 認証のバイパス（5-30 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（5-31 ページ）
- 認証失敗後のゲスト アクセスの許可（5-31 ページ）

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。	
2. 次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。	ポリシーの作成（10-5 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（5-30 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、次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（5-31 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（5-32 ページ）
3. （任意）ゲスト ユーザの詳細の記録方法の設定（5-32 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 アクセスを許可しており、MyIdentificationProfile を使用してい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 ポリシーと照合されます。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 **[識別プロファイルを追加（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　[識別プロファイルとユーザ（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（5-31 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 HTTPS 要求および FTP over HTTP 要求に対して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	[はい（Yes）]	[はい（Yes）]	[はい（Yes）]	NA	NA	NA
IP ベース	[はい（Yes）]	[はい（Yes）]	[はい（Yes）]	[はい（Yes）]	[はい（Yes）]	[はい（Yes）]
Cookie ベース	[はい（Yes）]	Yes***	Yes***	[はい（Yes）]	[いいえ（No）]/Yes**	Yes***

透過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	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	[はい（Yes）]	[いいえ（No）]/Yes*	No/Yes*	[はい（Yes）]	[いいえ（No）]/Yes*	No/Yes*
Cookie ベース	[はい（Yes）]	[いいえ（No）]/Yes**	No/Yes**	[はい（Yes）]	[いいえ（No）]/Yes**	No/Yes**

* 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。**トランザクションは認証をバイパスします。
- **HTTPS トランザクション。**トランザクションはドロップされます。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。

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 ID は、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 ID は、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 ID は、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 プロキシがトランスペアレント モードで展開され、[明示的フォワード要求に同じサロゲート設定を適用（Applysame 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。

資格情報

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（5-35 ページ）
- 認証および承認の失敗（5-35 ページ）
- クレデンシャルの形式（5-36 ページ）
- 基本認証のクレデンシャルの暗号化（5-36 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** をトランスペアレント 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 sethostname CLI コマンド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（5-31 ページ）
- 異なるクレデンシャルによる再認証の許可（5-33 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 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。

関連項目

- 証明書の管理（22-24 ページ）。

認証に関するトラブルシューティング

- NTLMSSP に起因する LDAP ユーザの認証の失敗（A-2 ページ）
- LDAP 紹介に起因する LDAP 認証の失敗（A-2 ページ）
- 基本認証の失敗（A-3 ページ）
- 誤ってユーザにクレデンシャルを要求する（A-3 ページ）
- 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（A-14 ページ）
- 認証をサポートしていない URL にアクセスできない（A-19 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-20 ページ）

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、次の目的のために行われます。

- ポリシーの適用(SaaS を除く)
- 識別および認証の要件の指定

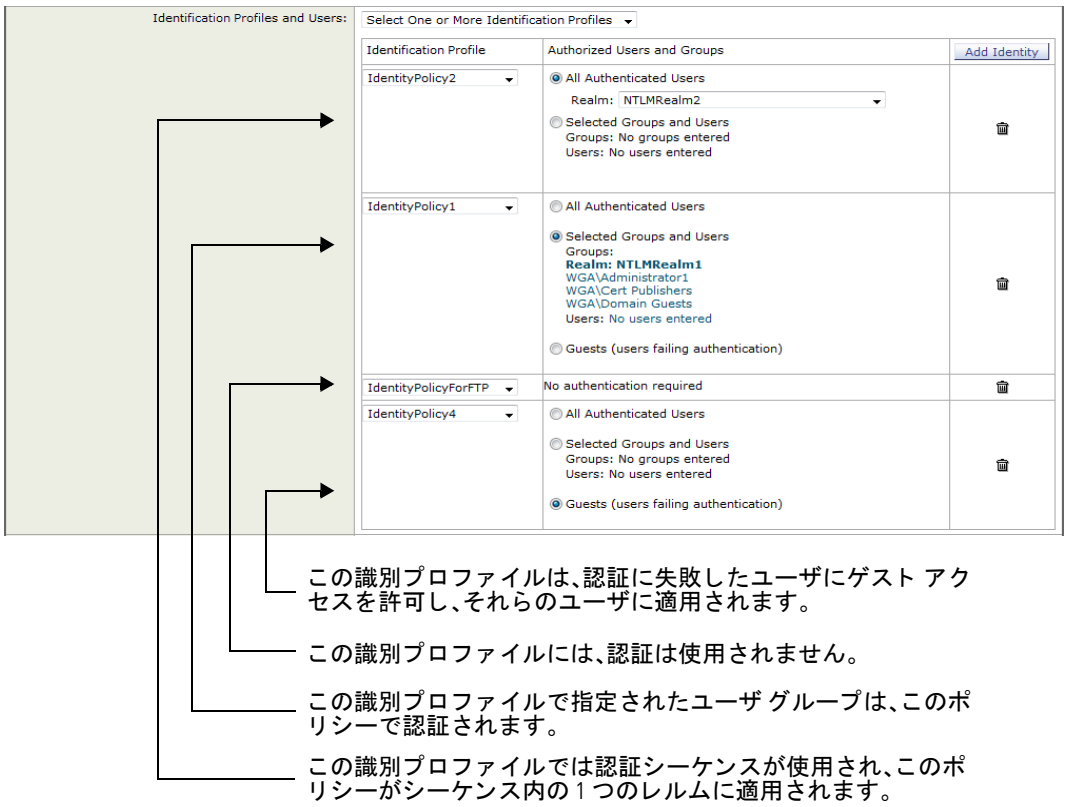
AsyncOS はすべてのトランザクションに識別プロファイルを割り当てます。

- 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 は最初の ID 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。
- トランスペアレント 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（5-30 ページ）を参照してください。

識別プロファイルの条件

オプション	説明
Subnet	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。
プロトコル	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）

オプション	説明
[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。トランスペアレント接続の場合は、宛先ポートと同じです。
ユーザ エージェント	要求を行うユーザ エージェント（クライアント ソフトウェア）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。
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（5-17 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があります。
- 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。ポリシーの適用に対するマシンの識別（3-13 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（5-28 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（5-33 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）] フィールドのドロップダウン リストで、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。

3 種類の方式（認証/識別から除外、認証済みユーザ）と、ユーザを透過的に識別する 3 種類の方法（ISE、ASA（AnyConnect セキュア モビリティ経由）、適切に設定された認証レルム）があります。後者には Active Directory レルム、または Novell eDirectory として設定された LDAP レルムのいずれかが含まれます。

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。
ISE によってユーザを透過的に識別（Transparently identify users with ISE）	ISE サービスがイネーブルの場合に使用できます（[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、ユーザ名および関連するセキュリティ グループ タグは Identity Services Engine から取得されます。詳細については、Identity Services Engine サービスの統合に必要なタスク（8-2 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、セキュア モビリティがイネーブルになっており、ASA と統合されている場合に表示されます。ユーザ名は ASA から取得され、関連ディレクトリ グループは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。
認証レルムによってユーザを透過的に識別（Transparently identify users with authentication realm）	このオプションは、1 つ以上の認証レルムが透過的識別をサポートするように定義されている場合に使用できます。

（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 タグによるポリシー メンバーシップの定義がサポートされます。

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。

認証レルムまたはゲスト特権へのフォールバック（Fallback to Authentication Realm or Guest Privileges）	ユーザ認証を ISE から取得できない場合: • [ゲスト権限をサポート（Support Guest Privileges）]：トランザクションは続行を許可され、すべての識別プロファイルのゲストユーザに対して後続のポリシーを一致させます。 • [トランザクションをブロック（Block Transactions）]：ISE で識別できないユーザにインターネット アクセスを許可しません。 • [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を保存するかどうかを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、ユーザ名やパスワード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求められません。 ただし、次の場合、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。パスワード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。
グループ認証のレルム（Realm for Group Authentication）	• [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。

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の同じドメインに対して異なるクレデンシャルを指定すると、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。 • [サロゲートなし（No Surrogate）]：Web プロキシは、サロゲートを使用してクレデンシャルをキャッシュせず、新しい TCP 接続ごとに認証済みユーザを追跡します。このオプションを選択すると、Web インターフェイスは適用されくなったその他の設定をディセーブルにします。このオプションは、明示的な転送モードに設定し、[ネットワーク（Network）] > [認証（Authentication）] ページでクレデンシャルの暗号化をディセーブルにしたときにのみ使用できます。 • [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。次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（Membership Definition）	
ユーザの場所別メンバーの定義（Define Members by User Location）	この識別プロファイルを次に対して適用するように設定します。[ローカル ユーザのみ（Local Users Only）]、[リモート ユーザのみ（Remote Users Only）]、または [両方（Both）]。ここでの選択は、この識別プロファイルで使用可能な認証設定に影響します。
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。

プロトコル別メンバの定義（Define Members by Protocol）	この識別プロファイルを適用するプロトコルを選択します。適用するすべてのプロトコルを選択してください。 • [HTTP/HTTPS]：FTP over HTTP、および 基礎のプロトコルとして HTTP または HTTPS を使用するすべての要求に適用されます。基礎のプロトコルには、FTP over HTTP、および HTTP CONNECT を使用してトンネリングされるその他のプロトコルも含まれます。 • [ネイティブ FTP（Native FTP）]：ネイティブ FTP 要求にのみ適用されます。 • [SOCKS]：SOCKS ポリシーにのみ適用されます。
マシン ID によるメンバーの定義（Define Members by Machine ID）	• [このポリシーではマシン ID を使用しないでください（Do Not Use Machine ID in This Policy）]：ユーザはマシン ID によって識別されません。 • [マシン ID をベースにしたユーザ認証ポリシーの定義（Define User Authentication Policy Based on Machine ID）]：ユーザは基本的にマシン ID によって識別されます。 [マシン グループ（Machine Groups）] 領域をクリックして、[認証済みマシン グループ（Authorized Machine Groups）] ページを表示します。 追加する各グループごとに、[ディレクトリ検索（Directory Search）] フィールドに追加するグループの名前を入力し、[追加（Add）] をクリックします。リストからグループを削除するには、グループを選択して [削除（Remove）] をクリックします。 [Done（完了）] をクリックして前のページに戻ります。 [マシン ID（Machine IDs）] 領域をクリックして、[認証済みマシン（Authorized Machines）] ページを表示します。 [認証済みマシン（Authorized Machines）] で、マシン ID を入力してポリシーに関連付け、[完了（Done）] をクリックします。 **（注）** マシン ID による認証はコネクタ モードのみでサポートされ、Active Directory を必要とします。

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。 トランスペアレント接続の場合は、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使用されるユーザ エージェント（Firefox や Chrome Web ブラウザなどのアプリケーション）別にポリシー グループのメンバーシップを定義します。一般的に定義されているブラウザを選択するか、正規表現を使用して独自のブラウザを定義できます。 このポリシー グループを、選択したエージェントにのみ適用するか、選択したエージェントのリストに含まれていない任意のユーザ エージェントに適用するかを選択します。

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）
- ポリシー タスクによる Web 要求の管理：概要（10-2 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 [アイデンティティを有効化（Enable Identity）] 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

図 6-1（ 6-9 ページ） は、識別プロファイルが以下を使用するよう設定されている場合に、Web プロキシが識別プロファイルに対してクライアント要求を評価する仕組みを示しています。

- 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　トランザクション要求のフロー：識別プロファイルと認証 - サロゲートなしおよび IP ベースのサロゲート

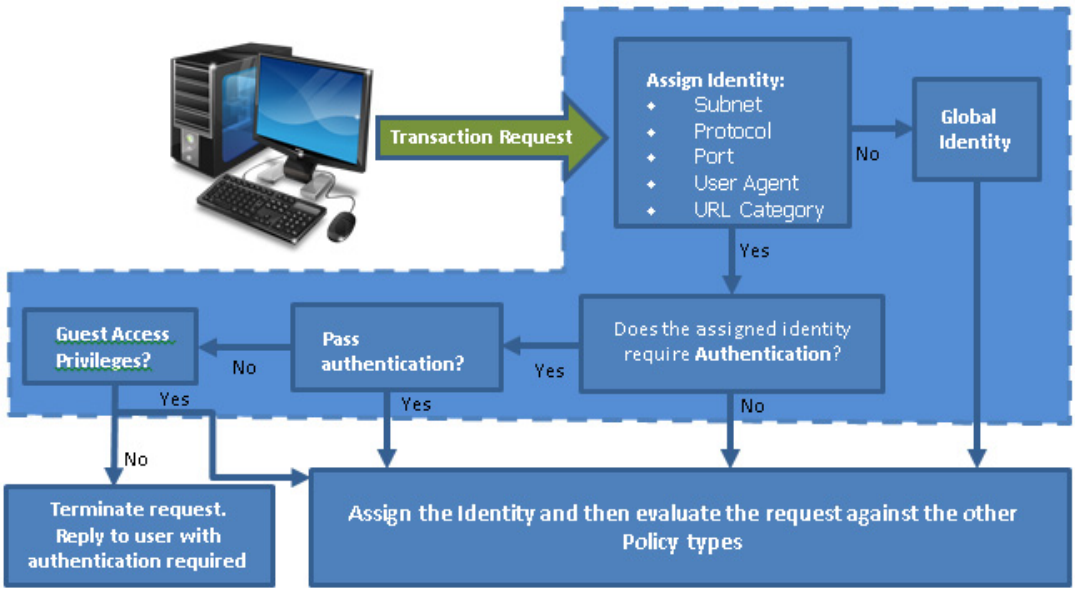
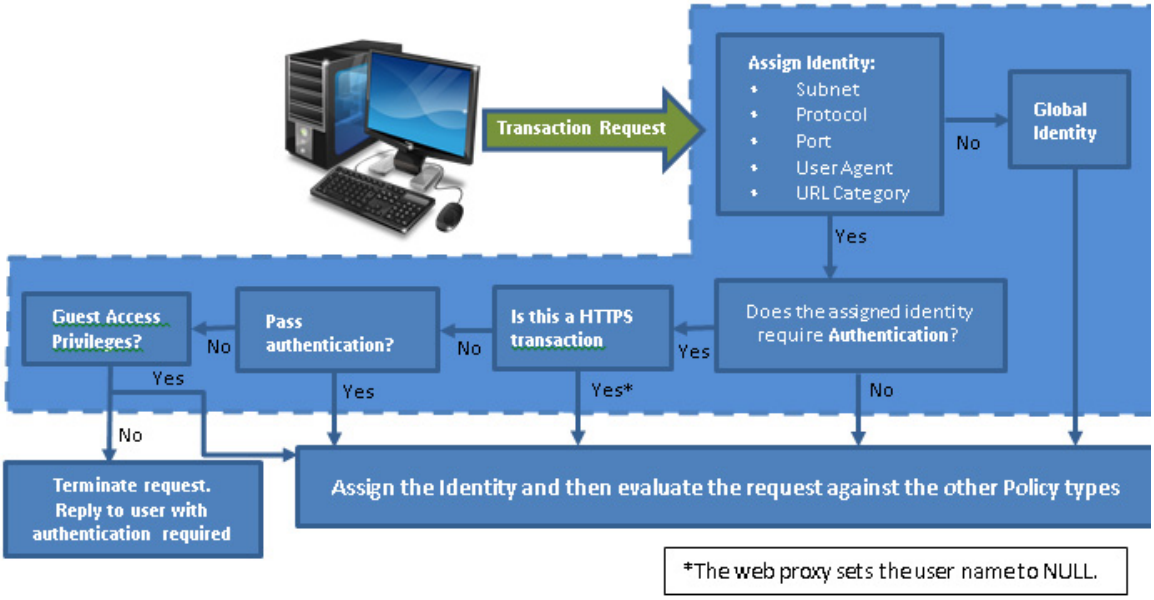


図 6-2　　トランザクション要求のフロー:識別プロファイルと認証 - TranCookie ベースのサロゲート



識別プロファイルのトラブルシューティング

SaaS アクセス コントロール

SaaS アクセス コントロールの概要

Web セキュリティ アプライアンスは、セキュリティ アサーション マークアップ言語（SAML）を使用して SaaS アプリケーション へのアクセスを承認します。SAML バージョン 2.0 に厳密に準拠している SaaS アプリケーション と連携して動作します。

Cisco SaaS アクセス コントロールによって、以下のことが可能になります。

- SaaS アプリケーション にアクセスできるユーザおよび場所を制御する。
- ユーザが組織を退職した時点で、すべての SaaS アプリケーション へのアクセスをただちに無効にする。
- ユーザに SaaS ユーザ クレデンシャルの入力を求めるフィッシング攻撃のリスクを軽減する。
- ユーザを透過的にサインインさせるか（シングル サイン オン機能）、ユーザに認証ユーザ名とパスワードの入力を求めるかを選択する。

SaaS アクセス コントロールは、Web セキュリティ アプライアンスがサポートしている認証メカニズムを必要とする SaaS アプリケーション でのみ動作します。現在、Web プロキシは「PasswordProtectedTransport」認証メカニズムを使用しています。

SaaS アクセス コントロールをイネーブルにするには、Web セキュリティ アプライアンスと SaaS アプリケーション の両方の設定を行う必要があります。

ステップ 1	Web セキュリティ アプライアンスを ID プロバイダーとして設定する。	ID プロバイダーとしてのアプライアンスの設定（7-2 ページ）
ステップ 2	SaaS アプリケーションの認証ポリシーを作成する。	SaaS アプリケーション認証ポリシーの作成（7-4 ページ）

ステップ 3	SaaS アプリケーション をシングル サイン オン用に設定する。	シングル サイン オン URL へのエンドユーザ アクセスの設定(7-7 ページ)
ステップ 4	(任意)複数の Web セキュリティ アプライアンスを設定する。	SaaS アクセス コントロールと複数のアプライアンスの使用(7-4 ページ)

ID プロバイダーとしてのアプライアンスの設定

Web セキュリティ アプライアンスを ID プロバイダーとして設定する場合、定義する設定は通信するすべての SaaS アプリケーション に適用されます。Web セキュリティ アプライアンスは、作成する各 SAML アサーションに署名するために証明書とキーを使用します。

はじめる前に

- (任意)SAML アサーションに署名するための証明書(PEM 形式)とキーを検索します。
- 各 SaaS アプリケーションに証明書をアップロードします。

ステップ 1　[ネットワーク(Network)] > [SaaS のアイデンティティ プロバイダー(Identity Provider for SaaS)] 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　[SaaS シングルサインオンサービスを有効にする(Enable SaaS Single Sign-on Service)] をオンにします。

ステップ 4　[アイデンティティ プロバイダーのドメイン名(Identity Provider Domain Name)] フィールドに仮想ドメイン名を入力します。

ステップ 5　[アイデンティティ プロバイダーのエンティティ ID(Identity Provider Entity ID)] フィールドに、一意のテキスト識別子を入力します(URI 形式の文字列を推奨)。

ステップ 6　証明書とキーをアップロードまたは生成します。

方法	この他の手順
証明書およびキーのアップロード	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。 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。 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検索します。 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。 （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。 4. [ファイルのアップロード（Upload Files）] をクリックします。 5. [証明書をダウンロード（Download Certificate）] をクリックして、Web セキュリティ アプライアンスが通信する SaaS アプリケーションに転送する証明書のコピーをダウンロードします。
証明書およびキーの生成	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。 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、署名付き証明書に表示する情報を入力します。 （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. [生成（Generate）] をクリックします。 3. [証明書をダウンロード（Download Certificate）] をクリックして、Web セキュリティ アプライアンスが通信する SaaS アプリケーション に証明書を転送します。 4. （任意）署名付き証明書を使用するには、[証明書署名要求のダウンロード（Download Certificate Signing Request）]（DCSR）リンクをクリックして、認証局（CA）に要求を送信します。CA から署名付き証明書を受信したら、[参照（Browse）] をクリックし、署名付き証明書の場所に移動します。[ファイルのアップロード（Upload File）] をクリックします。

（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、アプライアンスは、[署名証明書（Signing Certificate）] セクションで現在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 7　アプライアンスを ID プロバイダーとして設定する場合は、設定を書き留めておきます。これらの設定の一部は、SaaS アプリケーション をシングル サイン オン用に設定する際に使用する必要があります。

ステップ 8　変更を送信して確定します。

次のステップ

- SAML アサーションの署名に使用する証明書とキーを指定したら、各 SaaS アプリケーション に証明書をアップロードします。

関連項目

- シングル サイン オン URL へのエンドユーザ アクセスの設定（7-7 ページ）

SaaS アクセス コントロールと複数のアプライアンスの使用

はじめる前に

- ID プロバイダーとしてのアプライアンスの設定（15-2 ページ）

ステップ 1　各 Web セキュリティ アプライアンスに対して同じ ID プロバイダーのドメイン名を設定します。

ステップ 2　各 Web セキュリティ アプライアンスに対して同じ ID プロバイダーのエンティティ ID を設定します。

ステップ 3　[ネットワーク（Network）] > [SaaS のアイデンティティ プロバイダー（Identity Provider for SaaS）] ページで、各アプライアンスに同じ証明書と秘密キーをアップロードします。

ステップ 4　設定する各 SaaS アプリケーション にこの証明書をアップロードします。

SaaS アプリケーション認証ポリシーの作成

はじめる前に

- 関連付けられた ID を作成します。
- ID プロバイダーを設定します（ID プロバイダーとしてのアプライアンスの設定（7-2 ページ）を参照）。
- ID プロバイダーの署名証明書とキーを入力します（[ネットワーク（Network）] > [SaaS のアイデンティティ プロバイダー（Identity Provider for SaaS）] > [設定の有効化と編集（Enable and Edit Settings）]）。
- 認証レルムを作成します。認証レルム（5-11 ページ）

ステップ 1　[Web セキュリティ マネージャ（Web Security Manager）] > [SaaS ポリシー（SaaS Policies）] を選択します。

ステップ 2　[アプリケーションの追加（Add Application）] をクリックします。

ステップ 3　次の設定項目を設定します。

プロパティ	説明
アプリケーション名（Application Name）	このポリシーの SaaS アプリケーションを識別する名前を入力します。各アプリケーション名は一意である必要があります。Web セキュリティ アプライアンスは、アプリケーション名を使用してシングルサインオン URL を生成します。
説明（Description）	（任意）この SaaS ポリシーの説明を入力します。
サービス プロバイダーのメタデータ（Metadata for Service Provider）	このポリシーで参照されるサービス プロバイダーを示すメタデータを設定します。サービス プロバイダーのプロパティを手動で記述するか、または SaaS アプリケーションによって提供されるメタデータ ファイルをアップロードできます。 Web セキュリティ アプライアンスはメタデータを使用して、SAML により SaaS アプリケーション（サービス プロバイダー）と通信する方法を決定します。メタデータの適切な設定については、SaaS アプリケーションを参照してください。 **[キーの手動設定（Configure Keys Manually）]**: このオプションを選択した場合は、以下を入力します。 • **[サービス プロバイダーのエンティティ ID（Service Provider Entity ID）]**。SaaS アプリケーションが自身をサービス プロバイダーとして識別するために使用するテキスト（通常は URI 形式）を入力します。 • **[名前 ID の形式（Name ID Format）]**。サービス プロバイダーに送信する SAML アサーションでアプライアンスがユーザを識別するために使用する形式を、ドロップダウン リストから選択します。ここで入力する値は、SaaS アプリケーションの対応する設定と一致している必要があります。 • **[Assertion Consumer Service の URL（Assertion Consumer Service URL）]**。Web セキュリティアプライアンスが作成した SAML アサーションの送信先 URL を入力します。SaaS アプリケーションのマニュアルを参照して、使用する適切な URL（ログイン URL）を決定してください。 **[ハードディスクからファイルをインポート（Import File from Hard Disk）]**: このオプションを選択した場合は、[参照（Browse）] をクリックしてファイルを検索し、[インポート（Import）] をクリックします。 **（注）**　このメタデータ ファイルは、サービス プロバイダーのインスタンスを説明する SAML 標準に準拠した XML ドキュメントです。すべての SaaS アプリケーションがメタデータ ファイルを使用するわけではありませんが、使用する場合は、ファイルについて SaaS アプリケーションのプロバイダーにお問い合わせください。

プロパティ	説明
SaaS SSO のユーザ ID/認証（User Identification / Authentication for SaaS SSO）	SaaS シングル サインオンに対してユーザを識別または認証する方法を指定します。 • ユーザに対して、常にローカル認証クレデンシャルの入力を求める。 • Web プロキシが透過的にユーザ名を取得した場合に、ユーザに対してローカル認証クレデンシャルの入力を求める。 • SaaS ユーザのローカル認証クレデンシャルを使用して、ユーザを自動的にサインインさせる。 この SaaS アプリケーションにアクセスするユーザを認証するために、Web プロキシが使用する認証レルムまたはシーケンスを選択します。SaaS アプリケーションに正常にアクセスするには、ユーザは認証レルムまたは認証シーケンスのメンバーである必要があります。Identity Services Engine を認証に使用しており、LDAP を選択した場合は、SAML ユーザ名と属性のマッピングにレルムが使用されます。
SAML ユーザ名のマッピング（SAML User Name Mapping）	Web プロキシが SAML アサーションでサービス プロバイダーにユーザ名を示す方法を指定します。ネットワーク内で使用されているユーザ名を渡すか（[マッピングなし（No mapping）]）、または次のいずれかの方法で内部ユーザ名を別の形式に変更できます。 • **[LDAP クエリー（LDAP query）]。**サービス プロバイダーに送信されるユーザ名は、1 つ以上の LDAP クエリー属性に基づきます。LDAP 属性フィールドと任意のカスタム テキストを含む式を入力します。属性名は山カッコで囲む必要があります。任意の数の属性を含めることができます。たとえば、LDAP 属性が「user」と「domain」の場合は、<user>@<domain>.com と入力できます。 • **[固定ルール マッピング（Fixed Rule mapping）]。**サービス プロバイダーに送信されるユーザ名は、前または後ろに固定文字列を追加した内部ユーザ名に基づきます。[式名（Expression Name）] フィールドに固定文字列を入力し、その前または後ろに `%s` を付けて内部ユーザ名における位置を示します。
SAML 属性マッピング（SAML Attribute Mapping）	（任意）SaaS アプリケーションから要求された場合は、LDAP 認証サーバから内部ユーザに関する追加情報を SaaS アプリケーションに提供できます。各 LDAP サーバ属性を SAML 属性にマッピングします。
認証コンテキスト（Authentication Context）	Web プロキシが内部ユーザを認証するために使用する認証メカニズムを選択します。 **（注）** 認証コンテキストは、ID プロバイダーが内部ユーザの認証に使用した認証メカニズムをサービス プロバイダーに通知します。一部のサービス プロバイダーでは、ユーザに SaaS アプリケーションへのアクセスを許可するために特定の認証メカニズムが必要です。サービス プロバイダーが ID プロバイダーでサポートされていない認証コンテキストを必要とする場合、ユーザはシングル サイン オンを使用して ID プロバイダーからサービス プロバイダーにアクセスできません。

ステップ 4　変更を送信して確定します。

次の手順

- アプリケーションを設定したのと同じパラメータを使用して、SaaS アプリケーション側にシングル サインオンを設定します。

シングル サイン オン URL へのエンドユーザ アクセスの設定

Web セキュリティ アプライアンスを ID プロバイダーとして設定し、SaaS アプリケーション の SaaS アプリケーション認証ポリシーを作成すると、アプライアンスによってシングル サインオン URL（SSO URL）が作成されます。Web セキュリティ アプライアンスは SaaS アプリケーション認証ポリシーで設定されたアプリケーション名を使用して、シングル サインオン URL を生成します。SSO URL の形式は次のとおりです。

http://*IdentityProviderDomainName*/SSOURL/*ApplicationName*

ステップ 1　[Web セキュリティ マネージャ（Web Security Manager）] > [SaaS ポリシー（SaaS Policies）] ページで、シングルサインオン URL を取得します。

ステップ 2　フロー タイプに応じてエンドユーザが URL を使用できるようにします。

ステップ 3　ID プロバイダーによって開始されるフローを選択すると、アプライアンスはユーザを SaaS アプリケーション にリダイレクトします。

ステップ 4　サービス プロバイダーによって開始されるフローを選択する場合は、この URL を SaaS アプリケーション で設定する必要があります。

- 常に SaaS ユーザにプロキシ認証を要求する。ユーザは有効なクレデンシャルを入力した後、SaaS アプリケーションにログインします。
- SaaS ユーザを透過的にサインインさせる。ユーザは SaaS アプリケーションに自動的にログインします。

（注）　アプライアンスがトランスペアレント モードで展開されている場合に、明示的な転送要求を使用して、すべての認証済みユーザに対するシングル サイン オン動作を実現するには、ID グループを設定する際に、[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）] 設定を選択します。

Cisco Identity Services Engine の統合

Identity Services Engine サービスの概要

Cisco Identity Services Engine（ISE）は、ID 管理を向上させるためにネットワーク上の個々のサーバで実行されるアプリケーションです。AsyncOS は ISE バージョン 1.3 サーバからユーザ ID 情報にアクセスできます。設定されている場合は、適切に設定された識別プロファイルに対してユーザ名および関連するセキュリティ グループ タグが Identity Services Engine から取得され、それらのプロファイルを使用するように設定されたポリシーで透過的ユーザ識別が許可されます。

関連項目

- Identity Services Engine サービスの概要（8-1 ページ）
- Identity Services Engine の証明書（8-1 ページ）
- Identity Services Engine サービスの統合に必要なタスク（8-2 ページ）
- Identity Services Engine サービスへの接続（8-5 ページ）

注意 このリリースの AsyncOS はコネクタ モードをサポートしていません。しかし、ISE 固有のオプションはコネクタ モードで動作している場合でも表示されるので、一見すると使用できるように見えます。そのように見えても、ISE 機能は使用しないようにしてください。

Identity Services Engine の証明書

（注） ここでは、ISE 接続に必要な証明書について説明します。証明書の管理（22-24 ページ）には、AsyncOS の一般的な証書管理情報が記載されています。

Web セキュリティ アプライアンスと ISE サーバ間の相互認証と安全な通信のために、3 つの証明書が必要です。

- **WSA クライアント証明書**：ISE サーバで Web セキュリティ アプライアンスを認証するために使用されます。
- **ISE 管理証明書**：Web セキュリティ アプライアンスで ISE サーバの認証に使用され、ポート 443 での ISE ユーザプロファイル データの一括ダウンロードを許可します。
- **ISE pxGrid 証明書**：Web セキュリティ アプライアンス で ISE サーバの認証に使用され、ポート 5222 での WSA-ISE データ サブスクリプション（ISE サーバに対する進行中のパブリッシュ/サブスクライブ クエリー）を許可します。

この証明書は、認証局（CA）による署名でも自己署名でもかまいません。CA 署名付き証明書が必要な場合、AsyncOS には自己署名 WSA クライアント証明書、または証明書署名要求（CSR）を生成するオプションがあります。同様に ISE サーバにも、CA 署名付き証明書が必要な場合に、自己署名管理証明書や pxGrid 証明書、または CSR を生成するオプションがあります。

WSA および ISE に関連する両方の証明書について、次の点に注意してください。

- 自己署名証明書の場合、ISE pxGrid 証明書と管理証明書はどちらも ISE サーバの信頼できる証明書リストに含まれている必要があり、WSA クライアント認証も ISE の信頼できる証明書リストに含まれている必要があります。
- CA 署名付き証明書の場合：
  - 適切な CA ルート証明書が ISE サーバの信頼できる証明書リストに含まれている必要があります（[管理（Administration）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]）。
  - 適切な CA ルート証明書が WSA の信頼できる証明書リストに含まれている必要があります（[ネットワーク（Network）] > [証明書の管理（Certificate Management）] > [信頼できるルート証明書の管理（Manage Trusted Root Certificates）]）。CA ルート証明書がない場合は、プライマリの pxGrid 証明書および管理証明書用の CA ルート証明書を ISE 設定ページにアップロードします。

関連項目

- Identity Services Engine サービスの概要（8-1 ページ）
- Identity Services Engine サービスの統合に必要なタスク（8-2 ページ）
- Identity Services Engine サービスへの接続（8-5 ページ）

Identity Services Engine サービスの統合に必要なタスク

手順	タスク	関連項目および手順へのリンク
1	WSA クライアント証明書を設定する。	• CA 署名付きまたは自己署名の WSA クライアント証明書を作成するか、WSA にアップロードします。アップロードする証明書を ISE サーバにダウンロードします。Identity Services Engine サービスへの接続（8-5 ページ）および 証明書の管理（22-24 ページ）を参照してください。
2	ISE サーバに WSA クライアント証明書を追加する。	• ISE サーバで、前のステップで WSA からダウンロードした WSA クライアント証明書をインポートし、信頼できる証明書リストに追加します。（[管理（Administration）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）] > [インポート（Import）]）の順に移動）。

手順	タスク	関連項目および手順へのリンク
3	ISE サーバで ISE の管理証明書と pxGrid 証明書を設定する。	• ISE サーバで、[管理（Administration）] > [証明書（Certificates）] ページに移動します。 – CA 署名付き証明書の場合は、Admin と pxGrid 用として 2 つ証明書署名要求を作成し、証明書に署名してもらいます。CA ルート証明書が ISE サーバの信頼できる証明書リストに含まれていることを確認します。 署名付き証明書を受け取ったら、それらを ISE サーバにアップロードして、両方の証明書に対して CA 署名付き証明書のバインド操作を実行し、ISE サーバを再起動します。 – 自己署名証明書の場合は、[管理（Administration）] > [証明書（Certificates）] > [システム証明書（System Certificates）] に移動し、1 つまたは 2 つの自己署名証明書（pxGrid と管理用に 1 つずつ）を生成します。（両方に対して共通の証明書を 1 つ生成することも選択できます）。 WSA にインポートする自己署名証明書をエクスポートします。 （注）　適切な証明書が信頼できる証明書リストに追加されていることを確認します（Identity Services Engine の証明書（8-1 ページ）を参照）。
4	ISE サーバが WSA アクセス用に正しく設定されていることを確認する。	識別トピック サブスクライバ（WSA など）がリアルタイムでセッション コンテキストを取得できるように、ISE サーバを設定する必要があります。基本的な手順は次のとおりです。 • [自動登録の有効化（Enable Auto Registration）] がオンになっていることを確認します（[管理（Administration）] > [pxGrid サービス（pxGrid Services）] > [右上（Top Right）]）。 • ISE サーバから既存の WSA クライアントをすべて削除します（[管理（Administration）] > [pxGrid サービス（pxGrid Services）] > [クライアント（Clients）]）。 • ISE サーバのフッターが [pxGrid に接続（Connected to pxGrid）] に設定されていることを確認します（[管理（Administration）] > [pxGrid サービス（pxGrid Services）]）。 • ISE サーバに SGT グループを設定します（[ポリシー（Policy）] > [結果（Results）] > [TrustSec] > [セキュリティ グループ（Security Groups）]）。 • ユーザに SGT グループを関連付けるポリシーを設定します。 詳細については、『Cisco Identity Services Engine documentation』を参照してください。

手順	タスク	関連項目および手順へのリンク
5	WSA に ISE の管理証明書と pxGrid 証明書を追加する。	• CA 署名付き証明書を使用する場合は、2 つの証明書に署名した認証局が WSA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。含まれていない場合は、CA ルート証明書をインポートします。信頼できるルート証明書の管理（22-25 ページ）を参照してください。 （注）　CA 署名付き証明書を使用する場合は、WSA の Identity Services Engine ページの [ISE 管理証明書（ISE Admin Certificate）] と [ISE pxGrid 証明書（ISE pxGrid Certificate）] フィールドを、空欄のままにすることができます。 • 自己署名証明書を使用する場合は、ISE サーバからエクスポートされた証明書ファイルを WSA の Identity Services Engine ページに追加します。管理と pxGrid の両方に対して 1 つの証明書を使用する場合は、[ISE 管理証明書（ISE Admin Certificate）] と [ISE pxGrid 証明書（ISE pxGrid Certificate）] フィールドにそれぞれファイルをアップロードします（つまり、合計 2 回アップロードします）。Identity Services Engine サービスへの接続（8-5 ページ）を参照してください
6	ISE アクセスおよびロギング用に WSA を設定する。	• Identity Services Engine サービスへの接続（8-5 ページ）。 • 認証メカニズムをログ記録するために、アクセス ログにカスタム フィールド `%m` を追加します（アクセス ログのカスタマイズ（21-30 ページ））。 • ISE サービス ログが作成されていることを確認します。作成されていない場合は作成します（ログ サブスクリプションの追加と編集（21-8 ページ））。 • ISE サービス ログが作成されたことを確認します。作成されていない場合は追加します（ログ サブスクリプションの追加と編集（21-8 ページ））。 • ユーザの識別と認証のために ISE にアクセスする識別プロファイルを定義します（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））。 • ISE ID を使用してユーザ要求の条件とアクションを定義するアクセス ポリシーを設定します（ポリシーの設定（10-9 ページ））。

（注）　ISE サーバで証明書をアップロードしたり変更するたびに、ISE サービスを再起動する必要があります。また、サービスと接続が復元されるまでに数分かかることがあります。

関連項目

- Identity Services Engine サービスの概要（8-1 ページ）
- Identity Services Engine の証明書（8-1 ページ）
- Identity Services Engine に関する問題のトラブルシューティング（8-6 ページ）

Identity Services Engine サービスへの接続

注意　このリリースの AsyncOS はコネクタ モードをサポートしていません。しかし、ISE 固有のオプションはコネクタ モードで動作している場合でも表示されるので、一見すると使用できるように見えます。そのように見えても、ISE 機能は使用しないようにしてください。

はじめる前に

- ISE サーバが WSA アクセス用に正しく設定されていることを確認します（Identity Services Engine サービスの統合に必要なタスク（8-2 ページ）を参照）。
- ISE サーバの接続情報を取得します。
- 有効な ISE 関連の証明書（クライアント、ポータル、pxGrid）およびキーを取得します。また、Identity Services Engine の証明書（8-1 ページ）も参照してください。

ステップ 1　[ネットワーク（Network）] > [Identification Service Engine] 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　[ISE サービスを有効にする（Enable ISE Service）] をオンにします。

ステップ 4　ホスト名または IPv4 アドレスを使用して **ISE サーバ**を識別します。

ステップ 5　WSA と ISE サーバの相互認証用の **WSA クライアント認証**を入力します。

（注）　これは、CA の信頼できるルート証明書である必要があります。関連情報については、Identity Services Engine の証明書（8-1 ページ）を参照してください。

- [アップロードされた証明書とキーを使用（Use Uploaded Certificate and Key）]

  証明書とキーの両方に対して、[選択（Choose）] をクリックして各ファイルを参照します。

  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）] チェックボックスをオンにします。

  [ファイルのアップロード（Upload File）] をクリックします。（このオプションの詳細については、証明書およびキーのアップロード（22-26 ページ）を参照してください）。
- [生成された証明書とキーを使用（Use Generated Certificate and Key）]

  [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。（このオプションの詳細については、証明書およびキーの生成（22-27 ページ）を参照してください）。

ステップ 6　WSA クライアント証明書をダウンロードして保存し、ISE サーバ ホストにアップロードします（選択したサーバで、[管理（Administration）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）] > [インポート（Import）]）。

ステップ 7　ISE ユーザ プロファイル データを WSA に一括ダウンロードするために使用する、**ISE 管理証明書**を入力します。

証明書ファイルを参照して選択し、[ファイルのアップロード（Upload Files）] をクリックします。詳細については、証明書およびキーのアップロード（22-26 ページ）を参照してください。

ステップ 8　WSA-ISE データ サブスクリプション（ISE サーバに対して進行中のクエリー）用の **ISE pxGrid 証明書**を入力します。

証明書ファイルを参照して選択し、[ファイルのアップロード（Upload Files）] をクリックします。詳細については、証明書およびキーのアップロード（22-26 ページ）を参照してください。

ステップ 9　（任意）[テスト開始（Start Test）] をクリックして、ISE サーバの接続をテストします。

ステップ 10　[送信（Submit）] をクリックします。

次のステップ

- 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）
- インターネット要求を制御するポリシーの作成（10-1 ページ）

Identity Services Engine に関する問題のトラブルシューティング

ポリシーの適用に対する URL の分類

URL トランザクションの分類の概要

グループ ポリシーを使用して、疑わしいコンテンツを含む Web サイトへのアクセスを制御するセキュリティ ポリシーを作成できます。ブロック、許可、または復号化されるサイトは、各グループ ポリシーのカテゴリ ブロッキングを設定する際に選択するカテゴリに応じて決まります。URL カテゴリに基づいてユーザ アクセスを制御するには、Cisco Web Usage Controls をイネーブルにする必要があります。これは、ドメイン プレフィックスとキーワード分析を使用して URL を分類するマルチレイヤ URL フィルタリング エンジンです。

次のタスクを実行するときに、URL カテゴリを使用できます。

オプション	方法
ポリシー グループ メンバーシップの定義	URL と URL カテゴリの照合（9-3 ページ）
HTTP、HTTPS、および FTP 要求へのアクセスの制御	URL カテゴリによるトランザクションのフィルタリング（9-10 ページ）
特定のホスト名と IP アドレスを指定する、ユーザ定義のカスタム URL カテゴリの作成	カスタム URL カテゴリの作成および編集（9-15 ページ）

失敗した URL トランザクションの分類

動的コンテンツ分析エンジンは、アクセス ポリシーのみを使用して Web サイトへのアクセスを制御する場合に URL を分類します。ポリシー グループ メンバーシップを判別する場合や、復号化ポリシーまたはシスコ データ セキュリティ ポリシーを使用して Web サイトへのアクセスを制御する場合は、URL を分類しません。その理由は、このエンジンが宛先サーバからの応答コンテンツを分析することによって機能するからです。そのため、サーバから応答をダウンロードする前の要求時に行う必要がある決定では、このエンジンを使用できません。

未分類 URL の Web レピュテーション スコアが WBRS の許可範囲内にある場合、AsyncOS は動的コンテンツ分析を行わずに要求を許可します。

動的コンテンツ分析エンジンは URL を分類した後、カテゴリの評価と URL を一時キャッシュに格納します。これによって、以降のトランザクションで以前の応答のスキャンを利用し、応答時ではなく要求時にトランザクションを分類できます。

動的コンテンツ分析エンジンをイネーブルにすると、トランザクションのパフォーマンスに影響することがあります。ただし、ほとんどのトランザクションは Cisco Web Usage Controls URL カテゴリ データベースを使用して分類されるので、動的コンテンツ分析エンジンは通常、トランザクションのごく一部に対してのみ呼び出されます。

動的コンテンツ分析エンジンのイネーブル化

ステップ 1　[セキュリティ サービス（Security Services）] > [使用許可コントロール（Acceptable Use Controls）] を選択します。

ステップ 2　Cisco Web Usage Controls をイネーブルにします。

ステップ 3　動的コンテンツ分析エンジンを**クリック**してイネーブルにします。

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）]）。

（注）　定義済みの URL カテゴリを使用して、アクセス ポリシー（またはアクセス ポリシーで使用される ID）でポリシー メンバーシップを定義できます。また、アクセス ポリシーにより同じ URL カテゴリに対してアクションを実行できます。ID とアクセス ポリシー グループ メンバーシップを判別するときに、要求の URL を未分類にすることも可能です。ただし、サーバから応答を受信した後で動的コンテンツ分析エンジンで分類する必要があります。Cisco Web Usage Controls は動的コンテンツ分析によるカテゴリ評価を無視し、残りのトランザクションに対する URL の評価は「未分類」のままになります。ただし、それ以降のトランザクションは引き続き、新しいカテゴリ評価を利用できます。

未分類の URL

未分類の URL とは、定義済みの URL カテゴリにも *付属* のカスタム URL カテゴリにも一致しない URL です。

（注）　ポリシー グループのメンバーシップを判別するときに、カスタム URL カテゴリは、ポリシー グループのメンバーシップに対して選択されている場合にのみグループに含まれていると見なされます。

一致しないカテゴリと見なされたトランザクションはすべて、[レポート（Reporting）] > [URL カテゴリ（URL Categories）] ページで [分類されてない URL（Uncategorized URL）] として報告されます。未分類 URL の多くは、内部ネットワーク内の Web サイトへの要求から生じします。カスタム URL カテゴリを使用して内部 URL をグループ化し、内部 Web サイトに対するすべての要求を許可することを推奨します。これによって、[分類されてない URL（Uncategorized URL）] として報告される Web トランザクションの数が減少し、内部トランザクションが [バイパスされた URL フィルタリング（URL Filtering Bypassed）] 統計情報の一部として報告されるようになります。

関連項目

- フィルタリングされない未分類のデータについて（9-21 ページ）.
- カスタム URL カテゴリの作成および編集（9-15 ページ）.

URL と URL カテゴリの照合

URL フィルタリング エンジンはクライアント要求の URL と URL カテゴリを照合するときに、まず、ポリシー グループに*含まれている*カスタム URL カテゴリと照合して URL を評価します。要求の URL がグループに含まれているカスタム カテゴリと一致しない場合、URL フィルタリング エンジンはその URL を定義済みの URL カテゴリと比較します。URL がカスタム URL カテゴリにも定義済みの URL カテゴリにも一致しない場合、要求は未分類になります。

（注） ポリシー グループのメンバーシップを判別するときに、カスタム URL カテゴリは、ポリシー グループのメンバーシップに対して選択されている場合にのみグループに含まれていると見なされます。

ヒント 特定の Web サイトが割り当てられているカテゴリを確認するには、未分類の URL と誤分類された URL のレポート（9-3 ページ）の URL に移動します。

関連項目

- 未分類の URL（9-2 ページ）。

未分類の URL と誤分類された URL のレポート

未分類の URL および誤分類された URL をシスコに報告できます。シスコでは、複数の URL を同時に送信できる URL 送信ツールをシスコの Web サイトで提供しています。

`https://securityhub.cisco.com/web/submit_urls`

送信された URL のステータスを確認するには、このページの [送信した URL のステータス（Status on Submitted URLs）] タブをクリックします。また、URL 送信ツールを使用して、URL に割り当てられている URL カテゴリを検索できます。

URL カテゴリ データベース

URL が分類されるカテゴリは、フィルタリング カテゴリ データベースによって決定されます。Web セキュリティ アプライアンスは各 URL フィルタリング エンジンごとに情報を収集し、個別のデータベースに保持します。フィルタリング カテゴリ データベースは、Cisco アップデート サーバ（`https://update-manifests.ironport.com`）から定期的にアップデートを受信します。

URL カテゴリ データベースには、シスコ内部およびインターネットのさまざまなデータ要素とデータ ソースが格納されています。要素の 1 つであるオープン ディレクトリ プロジェクトからの情報は、時々検討されて当初のものから大幅に変更されます。

ヒント　特定の Web サイトが割り当てられているカテゴリを確認するには、未分類の URL と誤分類された URL のレポート（9-3 ページ）の URL に移動します。

関連項目

- セキュリティ サービスのコンポーネントの手動による更新（22-29 ページ）。

URL フィルタリング エンジンの設定

デフォルトでは、Cisco Web Usage Controls URL フィルタリング エンジンはシステム セットアップ ウィザードでイネーブルになります。

ステップ 1　[セキュリティ サービス（Security Services）] > [使用許可コントロール（Acceptable Use Controls）] 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　[使用許可コントロールを有効にする（Enable Acceptable Use Controls）] プロパティがイネーブルになっていることを確認します。

ステップ 4　動的コンテンツ分析エンジンをイネーブルにするかどうかを選択します。

ステップ 5　URL フィルタリング エンジンを利用できない場合に、Web プロキシが使用すべきデフォルトのアクション（[モニタ（Monitor）] または [ブロック（Block）]）を選択します。デフォルトは [モニタ（Monitor）] です。

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）]）。

URL カテゴリ セットの更新の管理

事前定義された URL カテゴリのセットは、新しい Web のトレンドと進化する使用パターンに合わせて時々更新されます。URL カテゴリ セットの更新は、新規 URL の追加や誤分類 URL の再マッピングによる変更とは異なります。カテゴリ セットの更新によって既存のポリシーの設定が変更されることがあるため、対処が必要になります。URL カテゴリ セットの更新は製品のリリース間で行われ、AsyncOS のアップグレードは必要ありません。

これらに関する情報は、次の URL から入手できます:
http://www.cisco.com/en/US/products/ps10164/prod_release_notes_list.html。

次の操作を実行します。

実行する時期	方法
更新が実行される前 （初期設定の一部としてこれらのタスクを実行します）	URL カテゴリ セットの更新による影響について（9-5 ページ） URL カテゴリ セットの更新の制御（9-7 ページ） 新規および変更されたカテゴリのデフォルト設定（9-8 ページ） カテゴリおよびポリシーの変更に関するアラートの受信（9-9 ページ）
更新が実行された後	URL カテゴリ セットの更新に関するアラートへの応答（9-9 ページ）

URL カテゴリ セットの更新による影響について

URL カテゴリ セットの更新は、既存のアクセス ポリシー、復号化ポリシー、シスコ データ セキュリティ ポリシー、および ID に次のような影響を与えます。

- URL カテゴリ セットの変更によるポリシー グループ メンバーシップへの影響（9-5 ページ）
- URL カテゴリ セットの更新によるポリシーのフィルタリング アクションへの影響（9-5 ページ）

URL カテゴリ セットの変更によるポリシー グループ メンバーシップへの影響

この項の内容は、URL カテゴリによって定義できるメンバーシップを含んでいるすべてのポリシー タイプ、および ID に該当します。ポリシー グループ メンバーシップが URL カテゴリによって定義されている場合、カテゴリ セットへの変更は次のような影響を及ぼす可能性があります。

- メンバーシップの唯一の条件であったカテゴリが削除された場合、ポリシーまたは ID はディセーブルになります。
- ポリシーのメンバーシップを定義していた URL カテゴリが変更され、それに伴って ACL リストも変更された場合は、Web プロキシが再起動します。

URL カテゴリ セットの更新によるポリシーのフィルタリング アクションへの影響

URL カテゴリ セットの更新により、ポリシーの動作が次のように変更される可能性があります。

変更内容	ポリシーおよび ID への影響
新しいカテゴリが追加された場合	各ポリシーにおいて、新たに追加されたカテゴリのデフォルト アクションは、そのポリシーの [分類されてない URL（Uncategorized URLs）] で指定されているアクションとなります。
カテゴリが削除された場合	削除されたカテゴリに関連付けられていたアクションは削除されます。 ポリシーが削除されたカテゴリにのみ依存していた場合、そのポリシーはディセーブルになります。 ポリシーが依存している ID が削除されたカテゴリにのみ依存していた場合、そのポリシーはディセーブルになります。
カテゴリの名前が変更された場合	既存のポリシーの動作に対する変更はありません。
カテゴリが分割された場合	1 つのカテゴリが複数の新規カテゴリとなることがあります。どちらの新規カテゴリにも、元のカテゴリに関連付けられていたアクションが含まれます。

変更内容	ポリシーおよび ID への影響
複数の既存のカテゴリがマージされた場合	ポリシーの元のカテゴリすべてに同じアクションが割り当てられていた場合、マージされたカテゴリには元のカテゴリと同じアクションが含まれます。元のカテゴリすべてが [グローバル設定を使用(Use Global Setting)] に設定されていた場合、マージされたカテゴリも [グローバル設定を使用(Use Global Setting)] に設定されます。 ポリシーの元のカテゴリにさまざまなアクションが割り当てられていた場合、マージされたカテゴリに割り当てられるアクションは、そのポリシーの [分類されてない URL(Uncategorized URLs)] の設定によって決まります。 • [分類されてない URL(Uncategorized URLs)] が [ブロック(Block)](または [グローバル設定を使用(Use Global Settings)](グローバル設定が [ブロック(Block)] の場合))に設定されている場合は、元のカテゴリにおいて最も制限が厳しいアクションがマージされたカテゴリに適用されます。 • [分類されてない URL(Uncategorized URLs)] が [ブロック(Block)] 以外(または [グローバル設定を使用(Use Global Settings)] 以外(グローバル設定が [ブロック(Block)] 以外の場合))に設定されている場合は、元のカテゴリにおいて最も制限が緩いアクションがマージされたカテゴリに適用されます。 この場合、以前ブロックされていたサイトにユーザがアクセスできるようになる可能性があります。 ポリシー メンバーシップが URL カテゴリによって定義されており、マージに関連する一部のカテゴリまたは [分類されてない URL(Uncategorized URLs)] のアクションがポリシー メンバーシップの定義に含まれていない場合は、欠落している項目に対してグローバル ポリシーの値が使用されます。 • 制限の厳しさの順位は次のとおりです(すべてのアクションをすべてのポリシー タイプで使用できるわけではありません)。ブロック • 削除 • 復号化 • 警告(Warn) • 時間ベース(Time-based) • モニタ(Monitor) • パススルー(Pass Through) **(注)** マージされたカテゴリに基づいている時間ベースのポリシーでは、元のカテゴリのいずれかに関連付けられているアクションが選択されます。(時間ベースのポリシーでは、制限が最も厳しいまたは最も緩いアクションが明確ではないことがあります)。

関連項目

- マージされたカテゴリ : 例(9-7 ページ)。

マージされたカテゴリ：例

以下の例は、ポリシーの [URL フィルタリング（URL Filtering）] ページの設定に基づいてマージされたカテゴリを示しています。

元のカテゴリ 1	元のカテゴリ 2	未分類の URL	マージされたカテゴリ
モニタ（Monitor）	モニタ（Monitor）	（該当なし）	モニタ（Monitor）
ブロック	ブロック	（該当なし）	ブロック
グローバル設定を使用（Use Global Settings）	グローバル設定を使用（Use Global Settings）	（該当なし）	グローバル設定を使用（Use Global Settings）
警告（Warn）	ブロック	モニタ（Monitor） 元のカテゴリにおいて最も制限が緩いアクションを使用。	警告（Warn）
モニタ（Monitor）	• ブロック（Block）または • グローバル設定を使用（Use Global Settings）（グローバルが [ブロック（Block）] に設定されている場合）	• ブロック（Block）または • グローバル設定を使用（Use Global Settings）（グローバルが [ブロック（Block）] に設定されている場合） 元のカテゴリにおいて最も制限が厳しいアクションを使用。	ブロック
ブロック	• モニタ（Monitor）または • グローバル設定を使用（Use Global Settings）（グローバルが [モニタ（Monitor）] に設定されている場合）	• モニタ（Monitor）または • グローバル設定を使用（Use Global Settings）（グローバルが [モニタ（Monitor）] に設定されている場合） 元のカテゴリにおいて最も制限が緩いアクションを使用。	モニタ（Monitor）
メンバーシップが URL カテゴリによって定義されているポリシーの場合： モニタ（Monitor）	カテゴリのアクションがポリシーで指定されておらず、カテゴリのグローバル ポリシーの値が [ブロック（Block）]。	未分類の URL のアクションがポリシーで指定されておらず、未分類の URL のグローバル ポリシーの値が [モニタ（Monitor）]。	モニタ（Monitor）

URL カテゴリ セットの更新の制御

デフォルトでは、URL カテゴリ セットの更新は自動的に行われます。ただし、これらの更新によって既存のポリシー設定が変更される可能性があるため、すべての自動更新をディセーブルにすることを推奨します。

オプション	方法
更新をディセーブルにした場合は、[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）] ページの [アップ デート サーバ（リスト）（Update Servers (list)）] セクションに記載されているすべてのサービスを手動で更新する必要があります。	手動による URL カテゴリ セットの更新（9-8 ページ）および セキュリティ サービスのコンポーネントの手動による更新（22-29 ページ）
すべての自動更新をディセーブルにする	アップグレードおよびサービス アップデートの設定の変更（22-33 ページ）。

（注）　CLI を使用する場合は、更新間隔をゼロ（0）に設定して更新をディセーブルにします。

手動による URL カテゴリ セットの更新

（注）　進行中の更新を中断しないでください。

自動更新をディセーブルにした場合は、必要に応じて手動で URL カテゴリ セットを更新できます。

ステップ 1　[セキュリティ サービス（Security Services）] > [使用許可コントロール（Acceptable Use Controls）] を選択します。

ステップ 2　アップデートが利用可能かどうかを確認します。

[使用許可コントロール エンジンの更新（Acceptable Use Controls Engine Updates）] テーブルの [Cisco Web利用の制御 - Web カテゴリのカテゴリ リスト（Cisco Web Usage Controls - Web Categorization Categories List）] を参照してください。

ステップ 3　更新するには、[今すぐ更新（Update Now）] をクリックします。

新規および変更されたカテゴリのデフォルト設定

URL カテゴリ セットの更新によって、既存のポリシーの動作が変更されることがあります。URL カテゴリ セットが更新されたときに対応できるように、ポリシーを設定する際は、特定の変更に対してデフォルトの設定を指定しておく必要があります。新しいカテゴリが追加された場合や既存のカテゴリが新しいカテゴリにマージされた場合、それらのカテゴリに対する各ポリシーのデフォルト アクションは、そのポリシーの [分類されてない URL（Uncategorized URLs）] 設定に左右されます。

既存の設定の確認または変更の実行

ステップ 1　[Web セキュリティ マネージャ（Web Security Manager）] を選択します。

ステップ 2　各アクセス ポリシー、復号化ポリシー、シスコ データ セキュリティ ポリシーに対して、[URL フィルタリング（URL Filtering）] リンクをクリックします。

ステップ 3　[分類されてない URL（Uncategorized URLs）] に対して選択されている設定を確認します。

関連項目

- 「URL カテゴリ セットの更新によるポリシーのフィルタリング アクションへの影響」（17-6 ページ）。

カテゴリおよびポリシーの変更に関するアラートの受信

カテゴリ セットの更新によって、次の 2 種類のアラートがトリガーされます。

- カテゴリの変更についてのアラート
- カテゴリ セットの変更によって変更またはディセーブル化されたポリシーに関するアラート

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　[受信者の追加（Add Recipient）] をクリックして電子メール アドレス（または、複数の電子メール アドレス）を追加します。

ステップ 3　受信するアラートの [アラート タイプ（Alert Types）] と [アラートの重大度（Alert Severities）] を決定します。

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）]）。

URL カテゴリ セットの更新に関するアラートへの応答

カテゴリ セットの変更に関するアラートを受信した場合は、以下を実行する必要があります。

- カテゴリがマージ、追加、削除された後でもポリシーと ID が引き続きポリシーの目標を満たしていることを確認し、
- 分割されたカテゴリに追加された事項や新規カテゴリを活用するために、ポリシーと ID を変更することを検討します。

関連項目

- URL カテゴリ セットの更新による影響について（9-5 ページ）

URL カテゴリによるトランザクションのフィルタリング

設定された URL フィルタリング エンジンを使用して、アクセス ポリシー、復号化ポリシー、データ セキュリティ ポリシーのトランザクションをフィルタリングできます。ポリシー グループの URL カテゴリを設定する際は、カスタム URL カテゴリ（定義されている場合）と定義済み URL カテゴリのアクションを設定できます。

設定できる URL フィルタリング アクションは、ポリシー グループのタイプに応じて異なります。

オプション	方法
アクセス ポリシー（Access Policies）	アクセス ポリシー グループの URL フィルタの設定（9-10 ページ）
復号化ポリシー（Decryption Policies）	復号化ポリシー グループの URL フィルタの設定（9-12 ページ）
シスコ データ セキュリティ ポリシー	データ セキュリティ ポリシー グループの URL フィルタの設定（9-13 ページ）

アクセス ポリシー グループの URL フィルタの設定

ユーザ定義のアクセス ポリシー グループおよびグローバル ポリシー グループに対して URL フィルタリングを設定できます。

ステップ 1　[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。

ステップ 2　ポリシー テーブルで、編集するポリシー グループの [URL フィルタ（URL Filtering）] 列にあるリンクをクリックします。

ステップ 3　（任意）[カスタム URL カテゴリのフィルタリング（Custom URL Category Filtering）] セクションで、アクションを実行するカスタム URL カテゴリをポリシーに追加できます。

a. [カスタム カテゴリの選択（Select Custom Categories）] をクリックします。

b. このポリシーに含めるカスタム URL カテゴリを選択して、[適用（Apply）] をクリックします。

URL フィルタリング エンジンでクライアント要求と照合するカスタム URL カテゴリを選択します。URL フィルタリング エンジンは、クライアント要求と含まれているカスタム URL カテゴリを比較します。除外されたカスタム URL カテゴリは無視されます。URL フィルタリング エンジンは、定義済みの URL カテゴリよりも前に、含まれているカスタム URL カテゴリとクライアント要求の URL を比較します。

ポリシーに含まれているカスタム URL カテゴリは、[カスタム URL カテゴリのフィルタリング（Custom URL Category Filtering）] セクションに表示されます。

ステップ 4　[カスタム URL カテゴリのフィルタリング（Custom URL Category Filtering）] セクションで、含まれている各カスタム URL カテゴリのアクションを選択します。

操作	説明
グローバル設定を使用（Use Global Setting）	グローバル ポリシー グループで設定されているこのカテゴリ用のアクションを使用します。これは、ユーザ定義のポリシー グループのデフォルト アクションです。 ユーザ定義のポリシー グループにのみ適用されます。 **（注）** カスタム URL カテゴリがグローバル アクセス ポリシーから除外されている場合、ユーザ定義のアクセス ポリシーに含まれているカスタム URL カテゴリのデフォルト アクションは、[グローバル設定を使用（Use Global Settings）] ではなく、[モニタ（Monitor）] になります。カスタム URL カテゴリがグローバル アクセス ポリシーで除外されている場合は、[グローバル設定を使用（Use Global Settings）] を選択できません。
リダイレクト	最初の宛先がこのカテゴリの URL であるトラフィックを、指定された場所にリダイレクトします。このオプションを選択すると、[リダイレクト先（Redirect To）] フィールドが表示されます。すべてのトラフィックをリダイレクトする URL を入力します。
許可（Allow）	このカテゴリの Web サイトに対してクライアント要求を常に許可します。 許可された要求は、以降のすべてのフィルタリングとマルウェア スキャンをバイパスします。 信頼できる Web サイトに対してのみこの設定を使用します。この設定は、内部サイトに対して使用することができます。
モニタ（Monitor）	Web プロキシは、要求を許可せず、ブロックもしません。代わりに、他のポリシー グループ制御設定（Web レピュテーション フィルタリングなど）と照合して、クライアント要求の評価を続行します。
警告（Warn）	当初、Web プロキシは要求をブロックして警告ページを表示しますが、ユーザは警告ページのハイパーテキスト リンクをクリックすることで続行できます。
ブロック	Web プロキシは、この設定に一致するトランザクションを拒否します。
時間ベース（Time-Based）	Web プロキシは、指定された時間範囲内で要求をブロックまたはモニタします。

ステップ 5　[事前定義された URL カテゴリのフィルタリング（Predefined URL Category Filtering）] セクションで、各カテゴリに対して次のいずれかのアクションを選択します。

- グローバル設定を使用（Use Global Settings）
- モニタ（Monitor）
- 警告（Warn）
- ブロック
- 時間ベース（Time-Based）

ステップ 6　[分類されてない URL（Uncategorized URLs）] セクションで、定義済みまたはカスタムの URL カテゴリに分類されない Web サイトへのクライアント要求に対して実行するアクションを選択します。この設定によって、URL カテゴリ セットの更新により生じた新規カテゴリとマージ カテゴリのデフォルト アクションも決まります。

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）]）。

関連項目

- アクセス ポリシーでのトラフィックのリダイレクト（9-18 ページ）。
- ユーザへの警告と続行の許可（9-19 ページ）
- カスタム URL カテゴリの作成および編集（9-15 ページ）
- URL カテゴリ セットの更新によるポリシーのフィルタリング アクションへの影響（9-5 ページ）

復号化ポリシー グループの URL フィルタの設定

ユーザ定義の復号化ポリシー グループおよびグローバル復号化ポリシー グループに対して URL フィルタリングを設定できます。

ステップ 1　[Web セキュリティ マネージャ（Web Security Manager）] > [復号化ポリシー（Decryption Policies）] を選択します。

ステップ 2　ポリシー テーブルで、編集するポリシー グループの [URL カテゴリ（URL URL Categories）] 列にあるリンクをクリックします。

ステップ 3　（任意）[カスタム URL カテゴリのフィルタリング（Custom URL Category Filtering）] セクションで、アクションを実行するカスタム URL カテゴリをポリシーに追加できます。

a. [カスタム カテゴリの選択（Select Custom Categories）] をクリックします。

b. このポリシーに含めるカスタム URL カテゴリを選択して、[適用（Apply）] をクリックします。

URL フィルタリング エンジンでクライアント要求と照合するカスタム URL カテゴリを選択します。URL フィルタリング エンジンは、クライアント要求と含まれているカスタム URL カテゴリを比較します。除外されたカスタム URL カテゴリは無視されます。URL フィルタリング エンジンは、定義済みの URL カテゴリよりも前に、含まれているカスタム URL カテゴリとクライアント要求の URL を比較します。

ポリシーに含まれているカスタム URL カテゴリは、[カスタム URL カテゴリのフィルタリング（Custom URL Category Filtering）] セクションに表示されます。

ステップ 4　カスタムまたは定義済みの各 URL カテゴリのアクションを選択します。

操作	説明
グローバル設定を使用（Use Global Setting）	グローバル復号化グループで設定されているこのカテゴリ用のアクションを使用します。これは、ユーザ定義のポリシー グループのデフォルト アクションです。 ユーザ定義のポリシー グループにのみ適用されます。 カスタム URL カテゴリがグローバル復号化ポリシーから除外されている場合、ユーザ定義の復号化ポリシーに含まれているカスタム URL カテゴリのデフォルト アクションは、[グローバル設定を使用（Use Global Settings）] でなく、[モニタ（Monitor）] になります。カスタム URL カテゴリがグローバル復号化ポリシーから除外されている場合は、[グローバル設定を使用（Use Global Settings）] を選択できません。
パススルー（Pass Through）	トラフィックコンテンツを検査せずにクライアントとサーバ間の接続をパススルーします。

操作	説明
モニタ（Monitor）	Web プロキシは、要求を許可せず、ブロックもしません。代わりに、他のポリシー グループ制御設定（Web レピュテーション フィルタリングなど）と照合して、クライアント要求の評価を続行します。
復号化	接続を許可しますが、トラフィック コンテンツを検査します。アプライアンスはトラフィックを復号化し、プレーン テキスト HTTP 接続であるかのように、復号化し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。
削除	接続をドロップし、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。

（注）　HTTPS 要求の特定の URL カテゴリを*ブロック*する場合は、復号化ポリシー グループのその URL カテゴリを復号化することを選択してから、アクセス ポリシー グループの同じ URL カテゴリをブロックすることを選択します。

ステップ 5　[分類されてない URL（Uncategorized URLs）] セクションで、定義済みまたはカスタムの URL カテゴリに分類されない Web サイトへのクライアント要求に対して実行するアクションを選択します。

この設定によって、URL カテゴリ セットの更新により生じた新規カテゴリとマージ カテゴリのデフォルト アクションも決まります。

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）]）。

データ セキュリティ ポリシー グループの URL フィルタの設定

ユーザ定義のデータ セキュリティ ポリシー グループおよびグローバル ポリシー グループに対して URL フィルタリングを設定できます。

ステップ 1　[Web セキュリティ マネージャ（Web Security Manager）] > [シスコ データ セキュリティ（Cisco Data Security）] を選択します。

ステップ 2　ポリシー テーブルで、編集するポリシー グループの [URL カテゴリ（URL URL Categories）] 列にあるリンクをクリックします。

ステップ 3　（任意）[カスタム URL カテゴリのフィルタリング（Custom URL Category Filtering）] セクションで、アクションを実行するカスタム URL カテゴリをポリシーに追加できます。

a.　[カスタム カテゴリの選択（Select Custom Categories）] をクリックします。

b.　このポリシーに含めるカスタム URL カテゴリを選択して、[適用（Apply）] をクリックします。

URL フィルタリング エンジンでクライアント要求と照合するカスタム URL カテゴリを選択します。URL フィルタリング エンジンは、クライアント要求と含まれているカスタム URL カテゴリを比較します。除外されたカスタム URL カテゴリは無視されます。URL フィルタリング エンジンは、定義済みの URL カテゴリよりも前に、含まれているカスタム URL カテゴリとクライアント要求の URL を比較します。

ポリシーに含まれているカスタム URL カテゴリは、[カスタム URL カテゴリのフィルタリング（Custom URL Category Filtering）] セクションに表示されます。

ステップ 4　[カスタム URL カテゴリのフィルタリング（Custom URL Category Filtering）] セクションで、各カスタム URL カテゴリのアクションを選択します。

操作	説明
グローバル設定を使用（Use Global Setting）	グローバル ポリシー グループで設定されているこのカテゴリ用のアクションを使用します。これは、ユーザ定義のポリシー グループのデフォルト アクションです。 ユーザ定義のポリシー グループにのみ適用されます。 カスタム URL カテゴリがグローバルなシスコ データセキュリティ ポリシーから除外されている場合、ユーザ定義のシスコ データセキュリティ ポリシーに含まれているカスタム URL カテゴリのデフォルト アクションは、[グローバル設定を使用（Use Global Settings）] でなく、[モニタ（Monitor）] になります。カスタム URL カテゴリがグローバルなシスコ データ セキュリティ ポリシーから除外されている場合は、[グローバル設定を使用（Use Global Settings）] を選択できません。
許可（Allow）	このカテゴリの Web サイトに対してアップロード要求を常に許可します。カスタム URL カテゴリにのみ適用されます 許可された要求は以降のすべてのデータ セキュリティ スキャンをバイパスし、要求はアクセス ポリシーに対して評価されます。 信頼できる Web サイトに対してのみこの設定を使用します。この設定は、内部サイトに対して使用することができます。
モニタ（Monitor）	Web プロキシは、要求を許可せず、ブロックもしません。代わりに、他のポリシー グループ制御設定（Web レピュテーション フィルタリングなど）と照合して、アップロード要求の評価を続行します。
ブロック	Web プロキシは、この設定に一致するトランザクションを拒否します。

ステップ 5　[事前定義された URL カテゴリのフィルタリング（Predefined URL Category Filtering）] セクションで、各カテゴリに対して次のいずれかのアクションを選択します。

- グローバル設定を使用（Use Global Settings）
- モニタ（Monitor）
- ブロック

ステップ 6　[分類されてない URL（Uncategorized URLs）] セクションで、定義済みまたはカスタムの URL カテゴリに分類されない Web サイトへのアップロード要求に対して実行するアクションを選択します。この設定によって、URL カテゴリ セットの更新により生じた新規カテゴリとマージ カテゴリのデフォルト アクションも決まります。

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）]）。

関連項目

- URL カテゴリ セットの更新によるポリシーのフィルタリング アクションへの影響（9-5 ページ）。

カスタム URL カテゴリの作成および編集

特定のホスト名と IP アドレスを指定する、ユーザ定義のカスタム URL カテゴリを作成することもできます。また、既存の URL カテゴリを編集したり削除することができます。これらのカスタム URL カテゴリを同じアクセス ポリシー グループ、復号化ポリシー グループ、またはシスコ データ セキュリティ ポリシー グループに含めて、各カテゴリに異なるアクションを定義すると、より上位のカスタム URL カテゴリのアクションが有効となります。

（注） Web セキュリティ アプライアンスでは、先頭に文字「c_」が付加されたカスタム URL カテゴリ名の最初の 4 文字が、アクセス ログで使用されます。Sawmill for を使用してアクセス ログを解析する場合は、カスタム URL カテゴリの名前に注意してください。カスタム URL カテゴリの最初の 4 文字にスペースが含まれていると、Sawmill for はアクセス ログ エントリを正しく解析できません。Sawmill for を使用してアクセス ログを解析する場合は、この最初の 4 文字に対してサポートされている文字のみを使用してください。カスタム URL カテゴリの完全な名前をアクセス ログに記録する場合は、%XF フォーマット指定子をアクセス ログに追加します。

ステップ 1　[Web セキュリティ マネージャ] > [カスタム URL カテゴリ] を選択します。

ステップ 2　カスタム URL カテゴリを作成または編集するには、[カスタム カテゴリを追加（Add Custom Category）] をクリックします。既存のカスタム URL カテゴリを編集するには、URL カテゴリの名前をクリックします。

ステップ 3　カスタム URL カテゴリに対して、下記の表に記載されている設定を入力します。

設定	説明
カテゴリ名（Category Name）	URL カテゴリの名前を入力します。この名前は、ポリシー グループに URL フィルタリングを設定するときに表示されます。
リスト順（List Order）	このカテゴリを配置するカスタム URL カテゴリ リスト内の順序を選択します。最上位の URL カテゴリの場合は「1」を入力します。 URL フィルタリング エンジンでは、指定した順序でカスタム URL カテゴリに対してクライアント要求が評価されます。
サイト（Sites）	カスタム カテゴリに属する 1 つまたは複数のアドレスを入力します。 複数のアドレスは、改行またはカンマで区切って入力します。
詳細設定：正規表現（Advanced: Regular Expressions）	正規表現を使用して、入力したパターンと一致する複数の Web サーバを指定できます。 **（注）** URL フィルタリング エンジンでは、まず [サイト（Sites）] フィールドに入力したアドレスと URL が比較されます。トランザクションの URL が [サイト（Sites）] フィールドの入力値と一致した場合は、ここで入力した式との比較は行われません。 正規表現の使用方法については、正規表現（9-21 ページ）を参照してください。

ステップ 4　（任意）、[URL のソート（Sort URLs）] をクリックして、[サイト（Sites）] フィールド内のすべてのアドレスをソートします。

（注）　アドレスをソートした後は、元の順序に戻すことができません。

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

- 正規表現（9-21 ページ）.
- アクセス ログのカスタマイズ（21-30 ページ）.

アダルト コンテンツのフィルタリング

一部の Web 検索や Web サイトからアダルト コンテンツをフィルタリングするように、Web セキュリティ アプライアンスを設定できます。AVC エンジンは、URL や Web クッキーを書き換えてセーフ モードを有効化することで、特定の Web サイトに実装されているセーフ モード機能を利用し、セーフ サーチやサイト コンテンツ レーティングを適用します。

次の機能によってアダルト コンテンツをフィルタリングします。

オプション	説明
セーフ サーチの適用（Enforce safe searches）	発信する検索要求がセーフ サーチ要求として検索エンジンに表示されるように、Web セキュリティ アプライアンスを設定することができます。これによって、ユーザが検索エンジンを使用して使用許可ポリシーを回避してしまうことを防止できます。
サイト コンテンツ レーティングの適用（Enforce site content ratings）	一部のコンテンツ共有サイトでは、独自のセーフ サーチ機能を適用するか、アダルト コンテンツへのアクセスをブロックするか、または両方を実行することによって、サイトのアダルト コンテンツへのユーザによるアクセスを制限しています。この分類機能は、一般的にコンテンツ レーティングと呼ばれています。

（注）　セーフ サーチ機能またはサイト コンテンツ レーティング機能を備えたアクセス ポリシーはすべて、安全なブラウジング アクセス ポリシーと見なされます。

セーフ サーチおよびサイト コンテンツ レーティングの適用

ステップ 1　[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。

ステップ 2　[URL カテゴリ（URL Categories）] 列にある、アクセス ポリシー グループまたはグローバル ポリシー グループのリンクをクリックします。

ステップ 3　ユーザ定義のアクセス ポリシーを編集する場合、[コンテンツ フィルタ（Content Filtering）] セクションの [コンテンツ フィルタ カスタム設定を定義（Define Content Filtering Custom Settings）] を選択します。

ステップ 4　[セーフ サーチを有効にする（Enable Safe Search）] チェックボックスをオンにして、セーフ サーチ機能をイネーブルにします。

ステップ 5　Web セキュリティ アプライアンスのセーフ サーチ機能で現在サポートされていない検索エンジンからユーザをブロックするかどうかを選択します。

ステップ 6　[サイト コンテンツ評価を有効にする(Enable Site Content Rating)] チェックボックスをオンにして、サイト コンテンツ レーティング機能をイネーブルにします。

ステップ 7　サポートされるコンテンツ レーティング Web サイトからのアダルト コンテンツをすべてブロックするか、エンドユーザ URL フィルタリング警告ページを表示するかを選択します。

（注）　サポートされているいずれかの検索エンジンまたはコンテンツ レーティング Web サイトの URL が、[許可(Allow)] アクションが適用されているカスタム URL カテゴリに含まれている場合、検索結果はブロックされず、すべてのコンテンツが表示されます。

ステップ 8　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

- ユーザへの警告と続行の許可(9-19 ページ)。
- 「Web アプリケーションへのアクセスの制御」(17-18 ページ)

アダルト コンテンツ アクセスのロギング

デフォルトでは、アクセス ログには安全なブラウジング スキャンの判定が含まれており、判定は各エントリの山カッコ内に記載されています。安全なブラウジング スキャンの判定は、セーフ サーチまたはサイト 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ているかどうかを示します。安全なブラウジング スキャンの判定変数をアクセス ログや W3C アクセス ログに追加することもできます。

- アクセス ログ:%XS
- W3C アクセス ログ:x-request-rewrite

値	説明
ensrch	元のクライアント要求が安全でなく、セーフ サーチ機能が適用されました。
encrt	元のクライアント要求が安全でなく、サイト コンテンツ レーティング機能が適用されました。
unsupp	元のクライアント要求がサポートされていない検索エンジン向けでした。
err	元のクライアント要求は安全ではありませんが、エラーのためにセーフ サーチ機能もサイト コンテンツ レーティング機能も適用されませんでした。
-	機能がバイパスされたため(トランザクションがカスタム URL カテゴリで許可された場合など)、またはサポートされていないアプリケーションで要求が実行されたため、セーフ サーチ機能もサイト コンテンツ レーティング機能もクライアント要求に適用されませんでした。

セーフ サーチまたはサイト コンテンツ レーティング機能によってブロックされた要求には、アクセス ログで次のいずれかの ACL デシジョン タグが使用されます。

- BLOCK_SEARCH_UNSAFE
- BLOCK_CONTENT_UNSAFE
- BLOCK_UNSUPPORTED_SEARCH_APP
- BLOCK_CONTINUE_CONTENT_UNSAFE

関連項目

- ACL デシジョン タグ（21-19 ページ）。

アクセス ポリシーでのトラフィックのリダイレクト

元の宛先がカスタム URL カテゴリの URL であるトラフィックを指定した場所にリダイレクトするように、Web セキュリティ アプライアンスを設定できます。これにより、宛先サーバではなく、アプライアンスにトラフィックをリダイレクトできます。カスタム アクセス ポリシー グループまたはグローバル ポリシー グループのトラフィックをリダイレクトできます。

はじめる前に

- トラフィックをリダイレクトするには、少なくとも 1 つのカスタム URL カテゴリを定義する必要があります。

ステップ 1　[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。

ステップ 2　[URL カテゴリ（URL Categories）] 列にある、アクセス ポリシー グループまたはグローバル ポリシー グループのリンクをクリックします。

ステップ 3　[カスタム URL カテゴリのフィルタリング（Custom URL Category Filtering）] セクションで、[カスタム カテゴリの選択（Select Custom Categories）] をクリックします。

ステップ 4　[このポリシーのカスタムカテゴリを選択（Select Custom Categories for this Policy）] ダイアログボックスで、リダイレクトするカスタム URL カテゴリに対して [ポリシーに含める（Include in policy）] を選択します。

ステップ 5　[適用（Apply）] をクリックします。

ステップ 6　リダイレクトするカスタム カテゴリの [リダイレクト（Redirect）] 列をクリックします。

ステップ 7　[リダイレクト先（Redirect to）] フィールドにトラフィックのリダイレクト先の URL を入力します。

ステップ 8　変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

（注）　トラフィックをリダイレクトするようにアプライアンスを設定する場合は、無限ループにならないように注意してください。

関連項目

- カスタム URL カテゴリの作成および編集（9-15 ページ）

ロギングとレポート

トラフィックをリダイレクトすると、最初に要求された Web サイトのアクセス ログ エントリに REDIRECT_CUSTOMCAT から始まる ACL タグが付きます。以降、アクセス ログ（通常は次の行）にリダイレクト先の Web サイトのエントリが表示されます。

[レポート（Reporting）] タブに表示されるレポートでは、リダイレクトされたトランザクションは [許可（Allowed）] と示されます。

ユーザへの警告と続行の許可

サイトが組織の利用規定を満たしていないことをユーザに警告できます。認証によってユーザ名が使用可能になっている場合、アクセス ログではユーザ名でユーザが追跡され、ユーザ名が使用できない場合は IP アドレスによって追跡されます。

次のいずれかの方法を使用して、ユーザに警告したり、続行を許可することができます。

- アクセス ポリシー グループの URL カテゴリに対して [警告（Warn）] アクションを選択します。または
- サイト コンテンツ レーティング機能をイネーブルにして、アダルト コンテンツにアクセスするユーザをブロックする代わりに、ユーザに警告します。

[エンドユーザ フィルタリング警告（End-User Filtering Warning）] ページの設定

ステップ 1　[セキュリティ サービス（Security Services）] > [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（End-User Filtering Warning）] ページで次の設定項目を設定します。

オプション	方法
警告の時間間隔（Time Between Warning）	[警告の時間間隔（Time Between Warning）] では、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 フィルタリング警告（End-User Filtering Warning）] ページを表示する頻度を指定します。 この設定は、ユーザ名によって追跡されるユーザと IP アドレスによって追跡されるユーザに適用されます。 30 ～ 2678400 秒（1 か月）の任意の値を指定します。デフォルトは 1 時間（3600 秒）です。
カスタム メッセージ（Custom Message）	カスタム メッセージは、ユーザによって入力されるテキストであり、すべての [エンドユーザ フィルタリング警告（End-User Filtering Warning）] ページに表示されます。 いくつかの単純な HTML タグを組み込み、テキストを書式設定できます。

ステップ 4　[送信（Submit）] をクリックします。

（注）「警告して継続」機能は、HTTP トランザクションと復号化された HTTPS トランザクションに対してのみ機能します。ネイティブ FTP トランザクションでは機能しません。

（注）URL フィルタリング エンジンは、特定の要求についてユーザに警告する場合に、Web プロキシがエンドユーザに送信する警告ページを提供します。（ただし、すべての Web サイトがエンドユーザに警告ページを表示するわけではありません。表示されない場合、ユーザは [警告（Warn）] オプションが割り当てられている URL からブロックされます。引き続きそのサイトにアクセスするチャンスは与えられません。

関連項目

- アダルト コンテンツのフィルタリング（9-16 ページ）
- 通知ページのカスタム テキスト（17-15 ページ）
- エンド ユーザ URL フィルタリング警告ページの設定（17-14 ページ）

時間ベースの URL フィルタの作成

Web セキュリティ アプライアンスが特定のカテゴリの URL の要求を日時別に処理する方法を設定できます。

はじめる前に

[Web セキュリティ マネージャ（Web Security Manager）] > [定義済み時間範囲（Defined Time Range）] に移動し、1 つ以上の時間範囲を定義します。

ステップ 1　[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。

ステップ 2　ポリシー テーブルで、編集するポリシー グループの [URL カテゴリ（URL URL Categories）] 列にあるリンクをクリックします。

ステップ 3　時間範囲に基づいて設定するカスタム URL カテゴリまたは定義済み URL カテゴリに対して、[時間ベース（Time-Based）] を選択します。

ステップ 4　[時間範囲内（In Time Range）] フィールドで、URL カテゴリに使用する定義済みの時間範囲を選択します。

ステップ 5　[アクション（Action）] フィールドで、定義した時間範囲内でこの URL カテゴリのトランザクションに割り当てるアクションを選択します。

ステップ 6　[それ以外の場合（Otherwise）] フィールドで、定義した時間範囲*外*でこの URL カテゴリのトランザクションに割り当てるアクションを選択します。

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）]）。

関連項目

- 時間範囲とボリューム クォータ（10-13 ページ）

URL フィルタリング アクティビティの表示

[レポート（Reporting）] > [URL カテゴリ（URL Categories）] ページには、一致した上位の URL カテゴリとブロックされた上位の URL カテゴリに関する情報を含む、総合的な URL 統計情報が表示されます。また、帯域幅の節約と Web トランザクションに関するカテゴリ固有のデータも表示されます。

関連項目

- エンドユーザのアクティビティをモニタするレポートの生成（18-1 ページ）

フィルタリングされない未分類のデータについて

[レポート（Reporting）] > [URL カテゴリ（URL Categories）] ページで URL 統計情報を検討する際は、次のデータの解釈方法を理解しておくことが大切です。

データ タイプ	説明
バイパスされた URL フィルタリング（URL Filtering Bypassed）	URL フィルタリングの前に発生する、ポリシー、ポート、admin ユーザ エージェントのブロックを表しています。
分類されてないURL（Uncategorized URL）	URL フィルタリング エンジンに照会したが、カテゴリが一致しなかったすべてのトランザクションを表しています。

アクセス ログ ファイル

アクセス ログ ファイルでは、各エントリのスキャン判定情報セクションにトランザクションの URL カテゴリが記録されます。

関連項目

- ログによるシステム アクティビティのモニタ（21-1 ページ）.
- URL カテゴリについて（9-24 ページ）.

正規表現

Web セキュリティ アプライアンスで使用される正規表現構文は、他の Velocity パターン マッチング エンジンの実装で使用される正規表現構文とはやや異なっています。また、アプライアンスは、バックスラッシュによるスラッシュのエスケープはサポートしていません。正規表現でスラッシュを使用する必要がある場合は、バックスラッシュなしでスラッシュを入力します。

（注）　技術的には、AsyncOS for Web では Flex 正規表現アナライザが使用されています。アナライザが正規表現を解読する仕組みについては、http://flex.sourceforge.net/manual/Patterns.html を参照してください。

正規表現は次の個所で使用できます。

- **アクセス ポリシーのカスタム URL カテゴリ。**アクセス ポリシー グループで使用するカスタム URL カテゴリを作成する際は、正規表現を使用して、入力したパターンと一致する複数の Web サーバを指定できます。
- **ブロックするカスタム ユーザ エージェント。**アクセス ポリシー グループをブロックするようにアプリケーションを編集する際は、正規表現を使用して、ブロックする特定のユーザ エージェントを入力できます。

（注） 広範な文字照合を実行する正規表現はリソースを消費し、システム パフォーマンスに影響を与える可能性があります。したがって、正規表現は慎重に適用する必要があります。

関連項目

- カスタム URL カテゴリの作成および編集（9-15 ページ）
- 「ポリシー：プロトコルおよびユーザ エージェント」（9-13 ページ）

正規表現の形成

正規表現は、一般的に、表現における「一致」を利用するルールです。これらを適用することで、特定の URL 宛先や Web サーバに一致させることができます。たとえば、次の正規表現は blocksite.com を含むパターンに一致します。

```
\.blocksite\.com
```

次の正規表現の例を考えてください。

```
server[0-9]\.example\.com
```

この例では、`server[0-9]` は `example.com` ドメインの `server0`、`server1`、`server2`、...`server9` と一致します。

次の例では、正規表現は `downloads` ディレクトリ内の `.exe`、`.zip`、`bin` で終わるファイルに一致します。

```
/downloads/.*\.(exe|zip|bin)
```

冗長な正規表現文字列は Web セキュリティ アプライアンスでの CPU 使用率を増加させるので、使用しないようにしてください。冗長な正規表現とは「.*」で開始または終了する表現です。

（注） 空白または英数字以外の文字を含む正規表現は、ASCII 引用符で囲む必要があります。

検証エラーを回避するための注意事項

検証エラーを最小限に抑えるため、次の注意事項に従ってください。

- 可能な限り、ワイルドカードやカッコで囲んだ式ではなく、リテラル式を使用してください。リテラル式とは、「`It's as easy as ABC123`」のような基本的に加工されていないテキストです。この式は、「`It's as easy as [A-C]{3}[1-3]{3}`」を使用するよりも失敗する可能性が低くなります。後者の式では、結果として非決定性有限オートマトン（NFA）エントリが生じるため、処理時間が大幅に長くなる可能性があります。

- エスケープしていないピリオドの使用は可能な限り避けてください。ピリオドは特別な正規表現文字であり、改行文字以外のあらゆる文字に一致します。たとえば、「url.com」などの実際のピリオドと一致させたい場合は、「url\.com」のように \ 文字を使用してピリオドをエスケープします。エスケープされたピリオドはリテラル入力と見なされるので、問題が生じません。

  可能な限り、エスケープしていないピリオドではなく、より具体的な一致パターンを使用してください。たとえば、後ろに 1 つの数字が続く URL に一致させるには、「url.」ではなく、「url[0-9]」を使用します。

- 長い正規表現でエスケープしていないピリオドを使用することは、特に問題を引き起こすので、避ける必要があります。 たとえば、「Four score and seven years ago our fathers brought forth on this continent, a new nation, conceived in Liberty, and dedicated to the proposition that all men are created .qual」はエラーを引き起こす可能性があります。ピリオドを含む「.qual」をリテラルの「equal」に置き換えると問題が解決します。

  また、パターン内のエスケープされていないピリオドは、パターン マッチング エンジンによってピリオドが無効にされた後、63 文字以上を返します。パターンを修正するか、置き換えてください。

- ワイルド カードと角カッコの組み合わせは、問題を引き起こす可能性があります。この組み合わせをできる限り使用しないようにしてください。たとえば、「id:[A-F0-9]{8}-[A-F0-9]{4}-[A-F0-9]{4}-[A-F0-9]{4}-[A-F0-9]{12}\) Gecko/20100101 Firefox/9\.0\.1\$」はエラーを引き起こしますが、「Gecko/20100101 Firefox/9\.0\.1\$」は問題ありません。後者の式にはワイルドカードやカッコで囲まれた式が含まれておらず、また、どちらの式でもエスケープされたピリオドが使用されています。

  ワイルドカードやカッコで囲まれた式を排除できない場合は、式のサイズと複雑さを減らすようにしてください。たとえば、「[0-9a-z]{64}」はエラーが引き起こす可能性があります。「[0-9]{64}」または「[0-9a-z]{40}」のように、より短いまたはより単純な表現に変更すると、問題が解決します。

エラーが発生した場合は、ワイルドカード（「*」、「+」、「.」など）やカッコで囲まれた式に上記のルールを適用して、問題を解決してください。

正規表現の文字テーブル

メタ	説明
.	改行文字（0x0A）を除く任意の文字と一致します。たとえば、正規表現「r.t」は文字列 rat、rut、r t と一致しますが、root とは一致しません。 長いパターン内、特に長いパターンの途中でエスケープしていないピリオドを使用する場合は、慎重に行ってください。詳細については、検証エラーを回避するための注意事項（9-22 ページ）を参照してください。
*	直前の正規表現の 0 回または複数回の出現と一致します。たとえば、「.*」は任意の文字列と一致し、「[0-9]*」は任意の数字と一致します。 このメタ文字を使用する場合（特にピリオドと一緒に使用する場合）は、慎重に使用してください。エスケープされていないピリオドを含むパターンは、ピリオドが無効になった後に 63 文字文字以上を返します。詳細については、検証エラーを回避するための注意事項（9-22 ページ）を参照してください。

メタ	説明
\	エスケープ文字。次のメタ文字を通常の文字として扱うための文字です。たとえば、「\^」は、行の先頭ではなく、キャレット記号(^)と一致させる場合に使用します。同様に、「\.」は、任意の 1 文字ではなく、実際のピリオドと一致させる場合に使用します。
^	行の先頭と一致します。たとえば、正規表現「^When in matches」は、「When in the course of human events」の先頭と一致しますが、「What and when in the」とは一致しません。
$	行または文字列の末尾と一致します。たとえば、「b$\.」は末尾が「b.」のあらゆる行または文字列と一致します。
+	直前の正規表現の 1 回以上の出現と一致します。たとえば、正規表現「9+」は 9、99、および 999 と一致します。
?	直前の正規表現の 0 回または 1 回の出現と一致します。たとえば、「 colou?r」は、「u」が任意であるため、「colour」と「color」のどちらとも一致します。
( )	左右のカッコの間の式を 1 つのグループとして扱い、他のメタ文字の範囲を制限します。たとえば、「(abc)+」は文字列「abc」の 1 回以上の出現と一致します。「abcabcabc」や「abc123」とは一致しますが、「abab」や「ab123」とは一致しません。
|	論理和(OR):前のパターンまたは後ろのパターンと一致します。たとえば、「(him|her)」は、行「it belongs to him」や「it belongs to her」と一致し、「it belongs to them」とは一致しません。
[ ]	カッコで囲まれた文字列の 1 文字に一致します。たとえば、正規表現「r[aou]t」は、「rat」、「rot」、「rut」と一致し、「ret」とは一致しません。 文字の範囲は先頭文字、ハイフン、および終了文字で指定します。たとえば、パターン [0-9] は任意の数字と一致します。複数の範囲も指定できます。パターン [A-Za-z] は大文字または小文字を示しています。範囲外(補集合)の文字を照合するには、左角カッコの後に先頭文字を示すキャレット記号を使用します。たとえば、式 [^269A-Z] は 2、6、9、および大文字以外の文字と一致します。
{ }	前のパターンと一致する回数を指定します。 次に例を示します。 D{1,3} は、文字 D が 1 ～ 3 回出現する場合に一致します。 前のパターンが特定の回数({*n*})または特定回数以上({*n*,})出現する場合に一致します。たとえば、式 A[0-9]{3} は後ろに 3 桁の数字が続く「A」と一致します。つまり、「A123」とは一致しますが、「A1234」とは一致しません。式 [0-9]{4,} は 4 桁以上の任意の数字と一致します。
...	引用符で囲まれた文字を文字どおり解釈します。

URL カテゴリについて

この項には、Cisco Web Usage Controls の URL カテゴリが記載されています。表には URL カテゴリ名の省略形も記載されています。これらの省略形は、アクセス ログ ファイル エントリの [Web レピュテーション フィルタリング(Web Reputation Filtering)] や [マルウェア対策スキャン(Anti-malware Scanning)] セクションに表示されることがあります。

（注）　アクセス ログでは、Cisco Web Usage Controls の URL カテゴリの各省略形の前にプレフィックス「IW_」が付いています。つまり、「art」カテゴリは「IW_art」となります。

URL カテゴリ	省略形	コード	説明	URL の例
アダルト（Adult）	adlt	1006	成人向けのコンテンツを指しますが、ポルノだけではありません。アダルト向けのナイトクラブ（ストリップ クラブ、スワッピング クラブ、同伴サービス、ストリッパーなど）、セックスに関する全般情報（ポルノとは限らない）、性器ピアス、アダルト向けの製品やグリーティング カード、健康や疾病関連以外の性行為に関する情報などもこれに含まれる場合があります。	www.adultentertainmentexpo.com www.adultnetline.com
広告（Advertisements）	adv	1027	Web ページに表示されることの多いバナー広告やポップアップ広告、その他の広告コンテンツを提供している広告関連 Web サイト。広告サービスおよび広告営業は、[ビジネスおよび産業（Business and Industry）] カテゴリに分類されます。	www.adforce.com www.doubleclick.com
アルコール（Alcohol）	alc	1077	嗜好品としての酒、ビールやワインの醸造、カクテルのレシピ、リキュール販売、ワイナリー、ブドウ園、ビール工場、アルコール類の販売元など。アルコール依存症は [健康および栄養（Health and Nutrition）] カテゴリに分類されます。バーおよびレストランは [飲食（Dining and Drinking）] カテゴリに分類されます。	www.samueladams.com www.whisky.com
芸術（Arts）	art	1002	画廊および展示会、芸術家および芸術作品、写真、文学および書籍、舞台芸術および劇場、ミュージカル、バレエ、美術館、デザイン、建築。映画およびテレビは [エンターテイメント（Entertainment）] に分類されます。	www.moma.org www.nga.gov
占星術（Astrology）	astr	1074	占星術、ホロスコープ、占い、数霊術、霊能者による助言、タロット。	www.astro.com www.astrology.com
オークション（Auctions）	auct	1088	オンラインまたはオフラインのオークション、オークション会社、オークション案内広告など。	www.craigslist.com www.ebay.com
ビジネスおよび産業（Business and Industry）	busi	1019	マーケティング、商業、企業、商慣行、労働力、人材、運輸、給与計算、セキュリティとベンチャー キャピタル、オフィス用品、工業装置（加工装置）、機械と機械システム、加熱装置、冷却装置、資材運搬機器、梱包装置、製造、固体運搬、金属製作、建造と建造物、旅客輸送、商業、工業デザイン、建築、建築資材、運送と貨物（貨物取扱業務、トラック輸送、運送会社、トラック輸送業者、貨物ブローカと輸送ブローカ、速達サービス、運送取引マッチング、追跡とトレース、鉄道輸送、海上輸送、ロード フィーダ サービス、引っ越し、保管）。	www.freightcenter.com www.staples.com

URL カテゴリ	省略形	コード	説明	URL の例
チャットおよびインスタント メッセージ（Chat and Instant Messaging）	chat	1040	Web ベースのインスタント メッセージおよびチャット ルーム。	www.icq.com www.meebo.com
不正行為および盗用（Cheating and Plagiarism）	plag	1051	不正行為を助長したり、盗用目的で学期末論文などの書物を販売するもの。	www.bestessays.com www.superiorpapers.com
児童虐待コンテンツ（Child Abuse Content）	cprn	1064	世界規模の違法な児童性的虐待コンテンツ。	—
コンピュータ セキュリティ（Computer Security）	csec	1065	企業ユーザおよび家庭ユーザ向けのセキュリティ製品およびセキュリティ サービス。	www.computersecurity.com www.symantec.com
コンピュータおよびインターネット（Computers and Internet）	comp	1003	コンピュータおよびソフトウェアに関する情報（ハードウェア、ソフトウェア、ソフトウェア サポートなど）、ソフトウェア エンジニア向けの情報、プログラミング、ネットワーク、Web サイト設計、Web およびインターネット全般、コンピュータ科学、コンピュータ グラフィック、クリップアートなど。フリーウェアとシェアウェアは、[フリーウェアおよびシェアウェア（Freeware and Shareware）] カテゴリに分類されます。	www.xml.com www.w3.org
出会い系（Dating）	date	1055	出会い系サイト、結婚紹介所など。	www.eharmony.com www.match.com
デジタル ポストカード（Digital Postcards）	card	1082	デジタル ポストカードや電子カードの送信。	www.all-yours.net www.delivr.net
飲食（Dining and Drinking）	food	1061	飲食店、レストラン、バー、居酒屋、パブ、レストラン ガイド、レストラン レビューなど。	www.hideawaybrewpub.com www.restaurantrow.com
ダイナミックおよびレジデンシャル（Dynamic and Residential）	dyn	1091	ブロードバンド リンクの IP アドレス。通常は、ホーム ネットワークへのアクセスを試みているユーザを示します。たとえば、ホーム コンピュータへのリモート セッションの場合などです。	http://109.60.192.55 http://dynalink.co.jp http://ipadsl.net
教育（Education）	edu	1001	教育関連の Web サイト。例：学校、短大、大学、教材、教師用資料、技術訓練、職業訓練、オンライン トレーニング、教育問題、教育政策、学資援助、学校助成金、規範、試験など。	www.education.com www.greatschools.org
エンターテインメント（Entertainment）	ent	1093	映画、音楽、バンド、テレビ、芸能人、ファン サイト、エンターテイメント ニュース、芸能界のゴシップ、エンターテイメント会場などに関する詳細や批評。[芸術（Arts）] カテゴリとの違いを確認してください。	www.eonline.com www.ew.com

URL カテゴリ	省略形	コード	説明	URL の例
過激（Extreme）	extr	1075	性的暴力または犯罪性のあるもの、暴力および暴力的行為、悪趣味な写真やむごたらしい写真（死体画像など）、犯罪現場写真、犯罪被害者や事故被害者の写真、過度にわいせつな文章や写真、衝撃的な内容の Web サイト。	www.car-accidents.com www.crime-scene-photos.com
ファッション（Fashion）	fash	1076	衣料、服飾、美容室、化粧品、アクセサリ、宝飾品、香水、身体改造に関連する図表や文章、タトゥー、ピアス、モデル事務所。皮膚関連製品は [健康および栄養（Health and Nutrition）] カテゴリに分類されます。	www.fashion.net www.findabeautysalon.com
ファイル転送サービス（File Transfer Services）	fts	1071	ダウンロード サービスやホスティングによるファイル共有を主目的とするファイル転送サービス	www.rapidshare.com www.yousendit.com
フィルタリング回避（Filter Avoidance）	filt	1025	検出されない匿名の Web 利用を促進および支援する Web サイト。例：cgi、php、glype を使用した匿名プロキシ サービス。	www.bypassschoolfilter.com www.filterbypass.com
財務（Finance）	fnnc	1015	金融や財務に関連するもの。例：会計実務、会計士、課税、税、銀行、保険、投資、国家経済、個人資産管理（各種保険、クレジット カード、個人退職金積立計画、遺産相続計画、ローン、住宅ローンなど）。株は [オンライン トレード（Online Trading）] に分類されます。	finance.yahoo.com www.bankofamerica.com
フリーウェアおよびシェアウェア（Freeware and Shareware）	free	1068	フリー ソフトウェアやシェアウェア ソフトウェアをダウンロードできるサイト。	www.freewarehome.com www.shareware.com
ギャンブル（Gambling）	gamb	1049	カジノ、オンライン ギャンブル、ブックメーカー、オッズ、ギャンブルに関する助言、ギャンブルの対象となっているレース、スポーツ ブッキング、スポーツ ギャンブル、株式スプレッド ベッティング サービス。ギャンブル依存を扱う Web サイトは [健康および栄養（Health and Nutrition）] に分類されます。国営宝くじは [宝くじ（Lotteries）] に分類されます。	www.888.com www.gambling.com
ゲーム（Games）	game	1007	さまざまなカード ゲーム、ボード ゲーム、ワード ゲーム、ビデオ ゲーム、戦闘ゲーム、スポーツ ゲーム、ダウンロード型ゲーム、ゲーム批評、攻略本、コンピュータ ゲーム、インターネット ゲーム（ロール プレイング ゲームなど）。	www.games.com www.shockwave.com
政府および法律（Government and Law）	gov	1011	政府 Web サイト、外交関係、政府および選挙に関するニュースや情報、法律分野に関する情報（法律家、法律事務所、法律関連の出版物、法律関連の参考資料、裁判所、訴訟事件一覧表、法律関連の協会など）、立法および判例、市民権問題、移民関連、特許、著作権、法執行制度および矯正制度に関する情報、犯罪報道、法的措置、犯罪統計、軍事（軍隊、軍事基地、軍組織など）、テロ対策。	www.usa.gov www.law.com

URL カテゴリ	省略形	コード	説明	URL の例
ハッキング（Hacking）	hack	1050	Web サイト、ソフトウェア、およびコンピュータのセキュリティを回避する方法に関する議論。	www.hackthissite.org www.gohacking.com
ヘイト スピーチ（Hate Speech）	hate	1016	社会集団、肌の色、宗教、性的指向、障がい、階級、民族、国籍、年齢、性別、性同一性に基づいて、憎悪、不寛容、差別を助長する Web サイト。人種差別、性差別、人種差別的な神学、人種差別的な音楽、ネオナチ組織、特定民族至上主義、ホロコースト否定論を助長するサイト。	www.kkk.com www.nazi.org
健康および栄養（Health and Nutrition）	hlth	1009	健康管理、疾病および障がい、医療、病院、医師、医薬品、精神衛生、精神医学、薬理学、エクササイズおよびフィットネス、身体障がい、ビタミン剤およびサプリメント、健康（疾病および健康管理）にかかわる性行為、喫煙、飲酒、薬物使用、健康（疾病および健康管理）にかかわるギャンブル、食物全般、飲食、調理およびレシピ、食物と栄養、健康維持および食事療法、レシピや料理に関する Web サイトを含む料理全般、代替医療など。	www.health.com www.webmd.com
ユーモア（Humor）	lol	1079	ジョーク、寸劇、漫画、その他のユーモラスなコンテンツ。不快感を与える可能性のあるアダルト ユーモアは [アダルト（Adult）] に分類されます。	www.humor.com www.jokes.com
違法行為（Illegal Activities）	ilac	1022	犯罪（窃盗、詐欺、電話回線への違法アクセスなど）の助長。コンピュータ ウイルス、テロ、爆弾、無政府主義。自他殺の方法の記載など殺人や自殺に関する描写を含む Web サイト。	www.ekran.no www.thedisease.net
違法ダウンロード（Illegal Downloads）	ildl	1084	著作権契約に違反して、ソフトウェアやその他の情報、シリアル番号、キー生成ツール、ソフトウェア プロテクション回避ツールなどをダウンロードできる Web サイト。Torrent は [ピア ファイル転送（Peer File Transfer）] に分類されます。	www.keygenguru.com www.zcrack.com
違法ドラッグ（Illegal Drugs）	drug	1047	娯楽用薬物、吸引道具、薬物の購入および製造に関する情報。	www.cocaine.org www.hightimes.com
インフラスおよびコンテンツ配信ネットワーク（Infrastructure and Content Delivery Networks）	infr	1018	コンテンツ配信インフラおよび動的に生成されるコンテンツ、セキュリティ保護されていたり分類が困難なために細かく分類できない Web サイト。	www.akamai.net www.webstat.net
インターネット電話（Internet Telephony）	voip	1067	インターネットを利用した電話サービス。	www.evaphone.com www.skype.com
求職（Job Search）	job	1004	職業に関する助言、履歴書の書き方、面接に関するスキル、就職斡旋サービス、求人データバンク、職業紹介所、人材派遣会社、雇用主の Web サイトなど。	www.careerbuilder.com www.monster.com

URL カテゴリ	省略形	コード	説明	URL の例
下着および水着（Lingerie and Swimsuits）	ling	1031	下着および水着。特にモデルが着用している Web サイト。	www.swimsuits.com www.victoriassecret.com
宝くじ（Lotteries）	lotr	1034	懸賞くじ、コンテスト、および公営宝くじ。	www.calottery.com www.flalottery.com
携帯電話（Mobile Phones）	cell	1070	ショート メッセージ サービス（SMS）、着信音などの携帯電話用ダウンロード サービス。携帯電話会社の Web サイトは、[ビジネスおよび産業（Business and Industry）] カテゴリに分類されます。	www.cbfsms.com www.zedge.net
自然（Nature）	natr	1013	天然資源、生態学および自然保護、森林、原生地、植物、草花、森林保護、森林、原生林および林業、森林管理（再生、保護、保全、伐採、森林状態、間伐、計画的火入れ）、農作業（農業、ガーデニング、園芸、造園、種まき、除草、灌漑、剪定、収穫）、環境汚染問題（大気質、有害廃棄物、汚染防止、リサイクル、廃棄物処理、水質、環境産業）、動物、ペット、家畜、動物学、生物学、植物学。	www.enature.com www.nature.org
ニュース（News）	news	1058	ニュース、ヘッドライン、新聞、テレビ局、雑誌、天気、スキー場情報。	www.cnn.com news.bbc.co.uk
非政府組織（Non-Governmental Organizations）	ngo	1087	クラブ、圧力団体、コミュニティ、非営利組織、労働組合など。	www.panda.org www.unions.org
性的でないヌード（Non-Sexual Nudity）	nsn	1060	ヌーディズム、ヌード、自然主義、ヌーディスト キャンプ、芸術的ヌードなど。	www.artenuda.com www.naturistsociety.com
オンライン コミュニティ（Online Communities）	comm	1024	アフィニティ グループ、同じ興味を持つ人々の集まり（SIG）、Web ニュースグループ、メッセージ ボードなど。[プロフェッショナル ネットワーキング（Professional Networking）] カテゴリまたは [ソーシャル ネットワーキング（Social Networking）] カテゴリに分類される Web サイトはここには含まれません。	www.igda.org www.ieee.org
オンライン ストレージおよびバックアップ（Online Storage and Backup）	osb	1066	バックアップ、共有、ホスティングを目的としたオフサイト ストレージおよびピアツーピア型ストレージ。	www.adrive.com www.dropbox.com
オンライン トレード（Online Trading）	trad	1028	オンライン証券会社、ユーザがオンラインで株取引できる Web サイト、株式市場。株式、債券、投資信託会社、ブローカー、株式市場の分析と解説、株式審査、株価チャート、IPO、株式分割に関する情報。株式スプレッド ベッティング サービスは [ギャンブル（Gambling）] に分類されます。その他の金融サービスは [財務（Finance）] に分類されます。	www.tdameritrade.com www.scottrade.com

URL カテゴリ	省略形	コード	説明	URL の例
業務用電子メール（Organizational Email）	pem	1085	業務上の電子メールを利用する際に使用する Web サイト（通常は Outlook Web Access によりアクセス）。	—
パーク ドメイン（Parked Domains）	park	1092	広告ネットワークの有料リスティング サービスを利用してそのドメインのトラフィックから収益を得ようとする Web サイト、またはドメイン名を販売して利益を得ようと考えている「不正占拠者」が所有する Web サイト。有料広告リンクを返す偽の検索サイトも含まれます。	www.domainzaar.com www.parked.com
ピア ファイル転送（Peer File Transfer）	p2p	1056	ピアツーピア型のファイル要求 Web サイト。ファイル転送自体のトラッキングは行いません。	www.bittorrent.com www.limewire.com
個人サイト（Personal Sites）	pers	1081	個人が運営している個人関連の Web サイト、個人用ホーム ページ サーバ、個人コンテンツが公開されている Web サイト、特定のテーマのない個人ブログなど。	www.karymullis.com www.stallman.org
写真検索および画像（Photo Searches and Images）	img	1090	画像、写真、クリップ アートの保存と検索を行うための Web サイト。	www.flickr.com www.photobucket.com
政治（Politics）	pol	1083	政治家、政党。政治、選挙、民主主義、投票などに関連するニュースや情報の Web サイト。	www.politics.com www.thisnation.com
ポルノ（Pornography）	porn	1054	性的表現が露骨な文章や画像。性的表現が露骨なアニメや漫画、性的表現が露骨な描写全般、フェチ志向の文章や画像、性的表現が露骨なチャット ルーム、セックス シミュレータ、ストリップ ポーカー、アダルト映画、わいせつな芸術、性的表現が露骨な Web メールなど。	www.redtube.com www.youporn.com
プロフェッショナル ネットワーキング（Professional Networking）	pnet	1089	キャリア開発や専門的開発を目的としたソーシャル ネットワーキング。[ソーシャル ネットワーキング（Social Networking）] も参照してください。	www.linkedin.com www.europeanpwn.net
不動産（Real Estate）	rest	1045	不動産の検索に役立つ情報、事務所および商業区画、不動産物件一覧（賃貸、アパート、戸建てなど）、住宅建築など。	www.realtor.com www.zillow.com
参考資料	ref	1017	都道府県および市区町村の案内情報、地図、時刻、参照文献、辞書、図書館など。	www.wikipedia.org www.yellowpages.com
宗教（Religion）	rel	1086	宗教に関するコンテンツ、宗教に関する情報、宗教団体。	www.religionfacts.com www.religioustolerance.org
SaaS および B2B（SaaS and B2B）	saas	1080	オンライン ビジネス サービス用 Web ポータル、オンライン会議。	www.netsuite.com www.salesforce.com
子供向け（Safe for Kids）	kids	1057	幼児や児童向けに作成されているか、明示的に幼児や児童向けと認められている Web サイト。	kids.discovery.com www.nickjr.com

URL カテゴリ	省略形	コード	説明	URL の例
科学技術（Science and Technology）	sci	1012	科学技術（航空宇宙、電子工学、工学、数学など）、宇宙探査、気象学、地理学、環境、エネルギー（化石燃料、原子力、再生可能エネルギー）、通信（電話、電気通信）など。	www.physorg.com www.science.gov
検索エンジンおよびポータル（Search Engines and Portals）	srch	1020	検索エンジンなど、インターネット上の情報にアクセスするための起点となるサイト。	www.bing.com www.google.com
性教育（Sex Education）	sxed	1052	事実に基づいて性的情報を扱う Web サイト、性的健康、避妊、妊娠など。	www.avert.org www.scarleteen.com
ショッピング（Shopping）	shop	1005	物々交換、オンライン購入、クーポン、無料提供、事務用品、オンライン カタログ、オンライン モールなど。	www.amazon.com www.shopping.com
ソーシャル ネットワーキング（Social Networking）	snet	1069	ソーシャル ネットワーキング関連。[プロフェッショナル ネットワーキング（Professional Networking）] も参照してください。	www.facebook.com www.twitter.com
社会科学（Social Science）	socs	1014	社会に関係する科学と歴史、考古学、文化人類学、文化学、歴史学、言語学、地理学、哲学、心理学、女性学。	www.archaeology.org www.anthropology.net
社会および文化（Society and Culture）	scty	1010	家族および家族関係、民族性、社会組織、家系、高齢者、保育など。	www.childcare.gov www.familysearch.org
ソフトウェア アップデート（Software Updates）	swup	1053	ソフトウェア パッケージに対する更新プログラムを提供している Web サイト。	www.softwarepatch.com www.versiontracker.com
スポーツおよび娯楽（Sports and Recreation）	sprt	1008	すべてのプロ スポーツおよびアマチュア スポーツ、レクリエーション活動、釣り、ファンタジー スポーツ（ゲーム）、公園、遊園地、レジャー プール、テーマ パーク、動物園、水族館、温泉施設など。	www.espn.com www.recreation.gov
ストリーミング オーディオ（Streaming Audio）	aud	1073	リアルタイム ストリーミング オーディオ コンテンツ（インターネット ラジオやオーディオ フィードなど）。	www.live-radio.net www.shoutcast.com
ストリーミング ビデオ（Streaming Video）	vid	1072	リアルタイム ストリーミング ビデオ（インターネット テレビ、Web キャスト、動画共有など）。	www.hulu.com www.youtube.com
タバコ（Tobacco）	tob	1078	愛煙家の Web サイト、タバコ製造会社、パイプと喫煙製品（違法薬物吸引用でないもの）など。タバコ依存症は [健康および栄養（Health and Nutrition）] カテゴリに分類されます。	www.bat.com www.tobacco.org

URL カテゴリ	省略形	コード	説明	URL の例
交通（Transportation）	trns	1044	個人用の乗り物、自動車およびバイクに関する情報、新車、中古車、オートバイの購入、自動車愛好会、小型船舶、航空機、レジャー用自動車（RV）など。自動車レースおよびバイク レースは [スポーツおよび娯楽（Sports and Recreation）] に分類されます。	www.cars.com www.motorcycles.com
旅行（Travel）	trvl	1046	出張および個人旅行、旅行情報、旅行のリソース、旅行代理店、パッケージ旅行、クルージング、宿泊、交通手段、航空便の予約、航空運賃、レンタカー、別荘など。	www.expedia.com www.lonelyplanet.com
未分類（Unclassified）	—	—	シスコのデータベースに登録されていない Web サイトは、未分類として記録され、レポートにもそのように表示されます。誤入力された URL もこれに含まれます。	—
武器（Weapons）	weap	1036	一般的な武器の購入および使用に関する情報（銃販売店、銃オークション、銃の案内広告、銃の付属品、銃の展示会、銃の訓練など）、銃に関する全般情報。その他の武器や狩猟関連画像のサイトなどが含まれる場合もあります。政府の軍に関する Web サイトは、[政府および法律（Government and Law）] カテゴリに分類されます。	www.coldsteel.com www.gunbroker.com
Web ホスティング（Web Hosting）	whst	1037	Web サイトのホスティング、帯域幅サービスなど。	www.bluehost.com www.godaddy.com
Web ページ翻訳（Web Page Translation）	tran	1063	Web ページの翻訳。	babelfish.yahoo.com translate.google.com
Web ベースの電子メール（Web-Based Email）	mail	1038	公開されている Web ベースの電子メール サービス。個人が自分の会社または組織の電子メール サービスを利用するための Web サイトは、[業務用電子メール（Organizational Email）] カテゴリに分類されます。	mail.yahoo.com www.hotmail.com

関連項目

- URL カテゴリ セットの更新の管理（9-4 ページ）
- 未分類の URL と誤分類された URL のレポート（9-3 ページ）

インターネット要求を制御するポリシーの作成

ポリシーの概要:代行受信されたインターネット要求の制御

ユーザが Web 要求を作成すると、設定されている Web セキュリティ アプライアンスが要求を代行受信し、最終結果を得るために要求が移動していくプロセスを管理します。最終結果は特定の Web サイトや電子メールにアクセスすることであったり、さらにはオンライン アプリケーションにアクセスすることであったりもします。Web セキュリティ アプライアンスを設定する際に、ユーザからの要求の基準とアクションを定義するためにポリシーが作成されます。

ポリシーは、Web セキュリティ アプライアンスが Web 要求を識別および制御する手段です。クライアントが Web 要求をサーバに送信すると、Web プロキシはその要求を受信して評価し、要求が属しているポリシー グループを判定します。その後に、ポリシーで定義されているアクションが要求に適用されます。

Web セキュリティ アプライアンスは複数のポリシー タイプを使用して、Web 要求のさまざまな側面を管理します。ポリシー タイプは独自にトランザクションを全面管理するか、追加の処理のために他のポリシー タイプにトランザクションを渡します。ポリシー タイプは、実行する機能(アクセス、ルーティング、セキュリティなど)によってグループ化できます。

AsyncOS は、アプライアンスからの不要な外部通信を避けるために、外部の依存関係を評価する前にポリシーに基づいてトランザクションを評価します。たとえば、未分類の URL をブロックするポリシーによってトランザクションがブロックされた場合、そのトランザクションが DNS エラーによって失敗することはありません。

ポリシー タスクによる Web 要求の管理：概要

手順	ポリシーによる Web 要求管理のタスク リスト	関連項目および手順へのリンク
1	認証レルムを設定して一定の順序に配置する	認証レルム（5-11 ページ）
2	（アップストリーム プロキシの場合）プロキシ グループを作成する	アップストリーム プロキシのプロキシ グループの作成（2-13 ページ）
2	（任意）カスタム クライアント アプリケーションを作成する	クライアント アプリケーション（10-11 ページ）
3	（任意）カスタム URL カテゴリを作成する	カスタム URL カテゴリ（10-16 ページ）
4	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）
5	（任意）時間範囲を作成し、時間帯によってアクセスを制限する	時間範囲とボリューム クォータ（10-13 ページ）
6	ポリシーを作成して順序付ける	• ポリシーの作成（10-5 ページ） • ポリシーの順序（10-5 ページ）

ポリシーによる Web 要求の管理：ベスト プラクティス

- Active Directory ユーザ オブジェクトを使用して Web 要求を管理する場合は、基準としてプライマリ グループを使用しないでください。Active Directory ユーザ オブジェクトにはプライマリ グループは含まれません。

ポリシー

- ポリシー タイプ（10-3 ページ）
- ポリシーの順序（10-5 ページ）
- ポリシーの作成（10-5 ページ）

ポリシー タイプ

ポリシー タイプ	要求タイプ	説明	タスクへのリンク
アクセス（Access）	• HTTP • 復号化された HTTPS • FTP	HTTP、FTP、復号化 HTTPS の着信トラフィックをブロック、許可、またはリダイレクトします。 HTTPS プロキシがディセーブルの場合、アクセス ポリシーは暗号化された着信 HTTPSトラフィックも管理します。	ポリシーの作成（10-5 ページ）
SOCKS	• SOCKS	Socks 通信要求を許可またはブロックします。	ポリシーの作成（10-5 ページ）
アプリケーション認証（Application Authentication）	• アプリケーション	Software as a Service（SaaS）アプリケーションへのアクセスを許可または拒否します。 シングル サイン オンを使用してユーザを認証し、アプリケーションへのアクセスをただちにディセーブルにすることによってセキュリティを向上させます。 ポリシーのシングル サインオン機能を使用するには、Web セキュリティ アプライアンスを ID プロバイダーとして設定し、SaaS の証明書とキーをアップロードまたは作成する必要があります。	SaaS アプリケーション認証ポリシーの作成（7-4 ページ）
暗号化 HTTPS 管理（Encrypted HTTPS Management）	• HTTPS	HTTPS 接続を復号化、パススルー、またはドロップします。 AsyncOS は、その後の処理のために、復号化したトラフィックをアクセス ポリシーに渡します。	ポリシーの作成（10-5 ページ）
データ セキュリティ	• HTTP • 復号化された HTTPS • FTP	Web へのデータのアップロードを管理します。データ セキュリティ ポリシーは発信トラフィックをスキャンし、宛先とコンテンツに基づいて、トラフィックがデータ アップロードの社内規則に準じていることを確認します。スキャンのために外部サーバに発信トラフィックをリダイレクトする外部 DLP ポリシーとは異なり、データ セキュリティ ポリシーは、Web セキュリティ アプライアンスを使用してトラフィックをスキャンし、評価します。	ポリシーの作成（10-5 ページ）

ポリシー タイプ	要求タイプ	説明	タスクへのリンク
外部 DLP（データ漏洩防止）（External DLP (Data Loss Prevention)）	• HTTP • 復号化された HTTPS • FTP	サードパーティ DLP システムを実行しているサーバに発信トラフィックを送信します。この DLP システムによってトラフィックをスキャンし、データ アップロードの社内規則に準拠していることを確認します。データのアップロードも管理するデータ セキュリティ ポリシーとは異なり、外部 DLP ポリシーは Web セキュリティ アプライアンスをスキャン作業から解放します。これによって、アプライアンスのリソースが解放され、サードパーティ製ソフトウェアによって提供されるその他の機能を活用できるようになります。	ポリシーの作成（10-5 ページ）
発信マルウェア スキャン（Outbound Malware Scanning）	• HTTP • 復号化された HTTPS • FTP	悪意のあるデータを含んでいる可能性があるデータのアップロード要求をブロック、モニタ、または許可します。 ネットワークにすでに存在しているマルウェアが外部ネットワークに送信されるのを防止します。	ポリシーの作成（10-5 ページ）
ルーティング	• HTTP • HTTPS • FTP	Web トラフィックをアップストリーム プロキシを介して送信したり、宛先サーバに送信します。既存のネットワーク設計を保護したり、Web セキュリティ アプライアンスからの処理をオフロードしたり、サードパーティのプロキシ システムによって提供される追加機能を活用するために、アップストリーム プロキシを介してトラフィックをリダイレクトできます。 複数のアップストリーム プロキシが使用可能な場合、Web セキュリティ アプライアンスはロード バランシング技術を使用して、それらのプロキシにデータを分散できます。	ポリシーの作成（10-5 ページ）

各ポリシー タイプはポリシー テーブルを使用して、ポリシーを保存および管理します。各ポリシー テーブルには、ポリシー タイプのデフォルト アクションを保守管理する、定義済みのグローバル ポリシーが用意されています。必要に応じて、追加のユーザ定義ポリシーが作成され、ポリシー テーブルに追加されます。ポリシーは、ポリシー テーブルのリストに記載されている順序で処理されます。

個々のポリシーには、ポリシーが管理するユーザ要求のタイプと要求に対して実行するアクションが定義されています。各ポリシー定義には 2 つのメイン セクションがあります。

- [識別プロファイルとユーザ（Identification Profiles and Users）]：識別プロファイルは、ポリシーのメンバーシップ基準で使用されます。Web トランザクションを識別するためのさまざまなオプションが含まれているので特に重要です。また、ポリシーと多くのプロパティを共有します。

- [詳細設定（Advanced）]：ポリシーの適用対象となるユーザの識別に使用される基準。1 つ以上の基準をポリシーで指定でき、基準を満たすにはすべてが一致する必要があります。
  - [プロトコル（Protocols）]：さまざまなネットワーク デバイス間でデータを転送できるようにします（http、https、ftp など）。
  - [プロキシ ポート（Proxy Ports）]：要求が Web プロキシにアクセスする番号付きのポート。
  - [サブネット（Subnets）]：要求が発信された、接続しているネットワーク デバイスの論理グループ（地理的な場所、ローカル エリア ネットワーク（LAN）など）。
  - [時間範囲（Time Range）]：時間範囲を作成すると、ポリシーでそれを使用して、要求が行われた時間帯に基づいて Web 要求を識別したり、Web 要求にアクションを適用できます。時間範囲は、個々のユニットとして作成されます。
  - [URL カテゴリ（URL Categories）]：URL カテゴリは Web サイトの定義済みまたはカスタムのカテゴリです（ニュース、ビジネス、ソーシャル メディアなど）。これらを使用して、Web 要求を識別したり、Web 要求にアクションを適用できます。
  - [ユーザ エージェント（User Agents）]：要求を行う際に使用されるクライアント アプリケーション（Web ブラウザの Firefox や Chromeなど）。ユーザ エージェントに基づいてポリシーの基準を定義したり、制御設定を指定できます。認証からユーザ エージェントを除外することもできます。これは、クレデンシャルの入力を求めることができないアプリケーションで役立ちます。カスタム クライアント アプリケーションを定義できますが、それらの定義を他のポリシーで再利用することはできません。

（注）　複数のメンバーシップ基準を定義した場合、クライアント要求は、ポリシーに一致するために、すべての基準を満たす必要があります。

ポリシーの順序

ポリシー テーブルにポリシーを記載する順序によって、Web 要求に適用されるポリシーの優先順位が決まります。Web 要求はテーブルの最上位のポリシーから順に照合され、要求がポリシーに一致した時点で照合は終了します。テーブルのそれ以降のポリシーは処理されません。

ユーザ定義のポリシーが Web 要求と一致しない場合は、そのポリシー タイプのグローバル ポリシーが適用されます。グローバル ポリシーは常にポリシー テーブルの最後に配置され、順序変更できません。

ポリシーの作成

はじめる前に

- 該当するプロキシをイネーブルにします。
  - Web プロキシ（HTTP、復号化されたHTTPS、および FTP 用）
  - HTTPS プロキシ
  - SOCKS プロキシ
- 関連する識別プロファイルを作成します。
- ポリシーの順序（10-5 ページ）について理解しておきます。
- （暗号化された HTTPS のみ）証明書とキーをアップロードまたは作成します。
- （データ セキュリティのみ）Cisco データ セキュリティ フィルタの設定をイネーブルにします。

- （外部 DLP のみ）外部 DLP サーバを定義します。
- （ルーティングのみ）Web セキュリティ アプライアンスに対して関連するアップストリーム プロキシを定義します。
- （任意）関連クライアント アプリケーションを作成します。
- （任意）関連する時間範囲を作成します。時間およびボリューム クォータの定義を参照してください。
- （任意）関連する URL カテゴリを作成します。カスタム URL カテゴリを参照してください。

ステップ 1　[ポリシー設定（Policy Settings）] セクションで、[アイデンティティを有効化（Enable Identity）] チェックボックスを使用して、このポリシーをイネーブルにするか、ポリシーを削除せずにただちにディセーブルにします。

ステップ 2　[名前（Name）] に一意のポリシー名を割り当てます。

ステップ 3　[説明（Description）] は任意です。

ステップ 4　[上に挿入（Insert Above）] ドロップダウン リストで、このポリシーを表示するテーブル内の位置を選択します。

（注）　ポリシーを配置します。最上位のものが最も制限が厳しく、最下位のものが最も緩くなります。詳細については、ポリシーの順序（10-5 ページ）を参照してください。

ステップ 5　[ポリシーメンバの定義（Policy Member Definition）] セクションで、ユーザおよびグループのメンバーシップの定義方法を選択します。[識別プロファイルとユーザ（Identification Profiles and Users ）] リストから、次のいずれかを選択してます。

- [すべての識別プロファイル（All Identification Profiles）] : このポリシを既存のすべてのプロファイルに適用します。少なくとも 1 つの [詳細設定（Advanced）] オプションを定義する必要があります。
- [1 つ以上の識別プロファイルを選択（Select One or More Identification Profiles）]: 個々の識別プロファイルを指定するためのテーブルが表示されます。1 行ごとに 1 つのプロファイル メンバーシップ定義が含まれています。

ステップ 6　[すべての識別プロファイル（All Identification Profile s ）] を選択した場合:

a.　次のいずれか 1 つのオプションを選択して、このポリシーを適用する承認済みユーザとグループを指定します。

- [すべての承認済みユーザ（All Authenticated Users）]: 認証または透過的 ID によって識別されたすべてのユーザ。
- [選択されたグループとユーザ（Selected Groups and Users）]: 指定したユーザとグループが使用されます。

  指定した ISE セキュリティ グループ タグ（SGT）や指定したユーザを追加または編集するには、適切なラベルのリンクをクリックします。たとえば、現在指定しているユーザのリストを編集するには、そのリストをクリックします。詳細については、ポリシーのセキュリティ グループ タグの追加と編集（10-8 ページ）を参照してください。
- [ゲスト（Guests）]: ゲストとして接続されているユーザと認証に失敗したユーザ。
- [すべてのユーザ（All Users）]: すべてのクライアント。承認済みかどうかは問いません。このオプションを選択する場合は、少なくとも 1 つの [詳細設定（Advanced）] オプションを設定する必要があります。

ステップ 7　[1 つ以上の識別プロファイルを選択（Select One or More Identification Profiles）] を選択すると、プロファイル選択テーブルが表示されます。

a. [識別プロファイル（Identity Profiles）] 列の [識別プロファイルの選択（Select Identification Profile）] ドロップダウン リストから、識別プロファイルを選択します。

b. このポリシーを適用する承認済みユーザとグループを指定します。

- [すべての承認済みユーザ（All Authenticated Users）]：認証または透過的 ID によって識別されたすべてのユーザ。
- [選択されたグループとユーザ（Selected Groups and Users）]：指定したユーザとグループが使用されます。

  指定した ISE セキュリティ グループ タグ（SGT）や指定したユーザを追加または編集するには、適切なラベルのリンクをクリックします。たとえば、現在指定しているユーザのリストを編集するには、そのリストをクリックします。詳細については、ポリシーのセキュリティ グループ タグの追加と編集（10-8 ページ）を参照してください。
- [ゲスト（Guests）]：ゲストとして接続されているユーザと認証に失敗したユーザ。

c. プロファイル選択テーブルに行を追加するには、[識別プロファイルの追加（Add Identification Profile）] をクリックします。行を削除するには、その行のゴミ箱アイコンをクリックします。

必要に応じて、ステップ (a) から (c) を繰り返して必要な識別プロファイルを追加します。

ステップ 8　[詳細設定（Advanced）] セクションを展開し、追加のグループ メンバーシップ基準を定義します。（[ポリシーメンバの定義（Policy Member Definition）] セクションで選択したオプションによっては、このステップは任意になります。また、設定するポリシーのタイプによっては、次のオプションの一部を使用できません）。

高度なオプション	説明
プロトコル（Protocols）	このポリシーを適用するプロトコルを選択します。[その他のすべて（All others）] は、選択されていないプロトコルを意味します。関連付けられている識別プロファイルを特定のプロトコルに適用すると、このポリシーもそれらのプロトコルに適用されます
プロキシ ポート（Proxy Ports）	特定のポートを使用して Web プロキシにアクセスするトラフィックにのみ、このポリシーが適用されます。1 つ以上のポート番号を入力します。複数のポートはカンマで区切ります。 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。 トランスペアレント接続の場合は、宛先ポートと同じです。 **（注）** 関連付けられている識別プロファイルを特定のプロキシ ポートにのみ適用する場合は、ここでプロキシ ポートを入力できません。
サブネット（Subnets）	特定のサブネットのトラフィックにのみこのポリシーが適用されます。[サブネット指定（Specify subnets）] を選択し、サブネットをカンマで区切って入力します。 サブネットによってさらにフィルタリングしない場合は、[選択したアイデンティティからのサブネットを使用（Use subnets from selected Identities）] はオンのままにしておきます。 **（注）** 関連付けられている ID を特定のサブネットに適用すると、このポリシーの適用を ID が適用されるアドレスのサブセットに限定できます。

高度なオプション	説明
時間範囲（Time Range）	ポリシー メンバーシップに時間範囲を適用できます。 • [時間範囲（Time Range）]：前に定義した時間範囲を選択します（時間範囲とボリューム クォータ（10-13 ページ））。 • [時間範囲の一致（Match Time Range）]：このオプションを使用して、この時間範囲を含めるか除外するかを指定します。つまり、指定した範囲内のみを照合するか、指定した範囲を除くすべての時間について照合するかを指定します。
URL Categories	特定の宛先（URL）と URL カテゴリによってポリシー メンバーシップを制限できます。すべての必要なカスタム カテゴリと定義済みカテゴリを選択します。カスタム カテゴリの詳細については、カスタム URL カテゴリ（10-16 ページ）を参照してください。
User Agents	特定のユーザ エージェントを選択し、このポリシーのユーザ定義の一部として、正規表現を使用してカスタム エージェントを定義できます。 • 共通ユーザ エージェント（Common User Agents） – [ブラウザ（Browsers）]：Internet Explorer や Firefox のバージョンを選択するには、このセクションを展開します。 – [その他（Others）]：特定のアプリケーションアップデート エージェント（Microsoft Windows、Adobe Acrobat など）を選択するには、このセクションを展開します。 • [カスタム ユーザ エージェント（Custom User Agents）]：1 つ以上の正規表現を（1 行に 1 つずつ）入力して、カスタム ユーザ エージェントを定義できます。 • [ユーザ エージェントの一致（Match User Agents）]：このオプションを使用して、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を指定します。つまり、指定した定義とのみ照合するか、ここで指定した定義以外のすべての定義と照合するかを指定します。

ポリシーのセキュリティ グループ タグの追加と編集

ポリシーの特定の識別プロファイルに割り当てられているセキュリティ グループ タグ（SGT）のリストを変更するには、[ポリシーの追加または編集（Add/Edit Policy）] ページの [選択されたグループとユーザ（Selected Groups and Users）] リストで、[ISE セキュリティ グループ タグ（ISE Secure Group Tags）] ラベルの後ろのリンクをクリックします。（ポリシーの作成（10-5 ページ） を参照）。このリンクは、[タグが未入力（No tags entered）] または現在割り当てられているタグのリストです。リンクをクリックすると [セキュア グループ タグの追加または編集（Add/Edit Group）] ページが開きます。

現在このポリシーに割り当てられている SGT が [承認済みセキュア グループ タグ（Authorized Secure Group Tags）] セクションに表示されます。接続されている ISE サーバから使用可能なすべての SGT が、[セキュリティ グループ タグの検索（Secure Group Tag Search）] セクションに表示されます。

ステップ 1　[承認済みセキュア グループ タグ（Authorized Secure Group Tags）] リストに 1 つ以上の SGT を追加するには、[セキュリティ グループ タグの検索（Secure Group Tag Search）] セクションに必要事項を入力し、[追加（Add）] をクリックします。

すでに追加されている SGT が緑色で強調表示されます。この利用可能な SGT のリストから特定の SGT を検索するには、[検索（Search）] フィールドにテキスト文字列を入力します。

ステップ 2　[承認済みセキュア グループ タグ（Authorized Secure Group Tags）] リストから 1 つ以上の SGT を削除するには、削除するエントリを選択し、[削除（Delete）] をクリックします。

ステップ 3　[Done（完了）] をクリックして、[グループの追加または編集（Add/Edit Group）] ページに戻ります。

関連項目

- 時間およびボリューム クォータの定義
- ポリシーでのクライアント アプリケーションの使用

ポリシーの設定

ポリシー テーブルの各行はポリシー定義を表し、各列には特定のリンクが含まれています。

オプション	説明
プロトコルと	プロトコルへのポリシー アクセスの制御、および特定のクライアント アプリケーション（インスタント メッセージ クライアント、Web ブラウザ、インターネット電話サービスなど）のブロック設定に使用されます。また、特定のポートの HTTP CONNECT 要求をトンネルするようにアプライアンスを設定することもできます。トンネリングがイネーブルの場合、アプライアンスは HTTP トラフィックを、評価せずに、指定されたポート経由で渡します。
URL	AsyncOS for Web では、アプライアンスが、特定の HTTP 要求または HTTPS 要求の URL カテゴリに基づいてトランザクションを処理する方法を設定できます。定義済みのカテゴリ リストを使用して、カテゴリ別に時間ベースのコンテンツをモニタ、ブロック、または設定するかを選択できます。また、カスタム URL カテゴリを作成し、カスタム カテゴリの Web サイトに対して時間ベースのトラフィックを許可、モニタ、ブロック、警告、リダイレクト、または設定することを選択できます。
アプリケーション	Application Visibility and Control（AVC）エンジンは、アクセプタブル ユース ポリシーのコンポーネントであり、Web トラフィックを検査して、アプリケーションで使用されるトラフィックをより詳しく把握し、制御します。アプライアンスでは、アプリケーション タイプごとまたは個々のアプリケーションごとにアプリケーションをブロックまたは許可するように、Web プロキシを設定できます。また、特定のアプリケーション内の特定のアプリケーション動作（ファイル転送など）に制御を適用できます。設定の詳細については、Web アプリケーションへのアクセスの管理（15-1 ページ）を参照してください。

オプション	説明
オブジェクトの	ファイル サイズやファイルなどのファイル特性に基づいてファイルのダウンロードをブロックするように、Web プロキシを設定できます。一般的に、オブジェクトとは、個々に選択、アップロード、ダウンロード、および処理できる次のような項目です。 • アプリケーション：pdf、xml、zip、exe • テキスト：cmd、csv、html、javascript • 画像：gif、jpeg、png、tiff • ビデオ：mp4、Quicktime、avi、wmv • 音声：mp4、wav、webm、mpeg • メッセージ：http、xml、rfc822、partial • x-world：wrl、wrz、xof、3dmf **（注）** オブジェクトのブロックでは、圧縮ファイルの内容は検査されません。
マルウェア対策とレピュテーション（Anti-Malware and Reputation）	Web レピュテーション フィルタを使用すると、Web ベースのレピュテーション スコアを 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定できます。マルウェア対策スキャンにより、Web ベースのマルウェアの脅威を識別して阻止します。高度なマルウェア防御機能は、ダウンロードしたファイル内のマルウェアを識別します。 マルウェア対策とレピュテーション ポリシーは、各コンポーネントごとにグローバル設定から継承されます。[セキュリティ サービス（Security Services）] > [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] では、マルウェア スキャンの判定に基づいてモニタまたはブロックするようにマルウェア カテゴリをカスタマイズしたり、Web レピュテーション スコアのしきい値をカスタマイズすることができます。マルウェア カテゴリはポリシー内でさらにカスタマイズできます。また、ファイル レピュテーション サービスと分析サービス用のグローバル設定項目もあります。 詳細については、アクセス ポリシーにおけるマルウェア対策およびレピュテーションの設定（13-10 ページ）およびファイル レピュテーション機能と分析機能の設定（14-4 ページ）を参照してください。

トランザクション要求のブロック、許可、リダイレクト

Web プロキシは、トランザクション要求のグループ用に作成されたポリシーに基づいて、Web トラフィックを制御します。

- **[許可（Allow）]**。Web プロキシは、中断のない接続を許可します。許可された接続は、DVS エンジンによってスキャンされていない可能性があります。
- **[ブロック（Block）]**。Web プロキシは、接続を許可せず、ブロックの理由を説明するエンドユーザ通知ページを表示します。
- **[リダイレクト（Redirect）]**。Web プロキシは、最初に要求された宛先サーバへの接続を許可せず、指定された別の URL に接続します（アクセス ポリシーでのトラフィックのリダイレクトを参照）。

（注）　上記のアクションは、Web プロキシがクライアント要求に対して実行する最終アクションです。アクセス ポリシーに対して設定できるモニタ アクションは最終アクションではありません。

通常、トラフィックは、トランスポート プロトコルに基づいて、さまざまなタイプのポリシーによって制御されます。

ポリシー タイプ	プロトコル				サポートされるアクション			
	HTTP	HTTPS	FTP	SOCKS	ブロック	許可（Allow）	リダイレクト	モニタ（Monitor）
アクセス（Access）	x	x	x		x	x	x	x
SOCKS				x	x	x		
SAAS	x	x						
復号化（Decryption）	x	x						x
データ セキュリティ	x	x	x		x			x
外部 DLP（External DLP）	x	x	x				x	
発信マルウェア スキャン（Outbound Malware Scanning）	x	x	x		x			x
ルーティング	x	x	x				x	

（注）　復号化ポリシーはアクセス ポリシーに優先します。

クライアント アプリケーション

クライアント アプリケーションについて

クライアント アプリケーション（Web ブラウザなど）は要求を行うために使用されます。クライアント アプリケーションに基づいてポリシー メンバーシップを定義できます。また、制御設定を指定したり、クライアント アプリケーションを認証から除外できます。これは、アプリケーションがクレデンシャルの入力を要求できない場合に役立ちます。

ポリシーでのクライアント アプリケーションの使用

クライアント アプリケーションによるポリシー メンバーシップの定義

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　[詳細設定（Advanced）] セクションを展開して、[クライアント アプリケーション（Client Applications）] フィールド内のリンクをクリックします。

ステップ 4　クライアント アプリケーションを 1 つ以上定義します。

表 10-1

オプション	方法
定義済みクライアント アプリケーションを選択する	[ブラウザ（Browser）] と [その他（Other）] セクションを展開して、必要なクライアント アプリケーションのチェックボックスをオンにします。 **ヒント**　可能な場合は [バージョン（Version）] オプションだけを選択します。これによって、複数のオプションを選択するよりもパフォーマンスが向上します。
カスタム クライアント アプリケーションを定義する	[カスタム クライアント アプリケーション（Custom Client Applications）] フィールドに適切な正規表現を入力します。必要に応じて、新規行に追加の正規表現を入力します。 **ヒント**　正規表現の例を参照するには、[クライアント アプリケーションのパターン例（Example Client Applications Patterns）] をクリックします。

ステップ 5　（任意）定義したクライアント アプリケーション**以外**のすべてのクライアント アプリケーションにポリシー メンバーシップを基づかせるには、[選択したクライアント アプリケーション以外のすべてに一致（Match All Except The Selected Client Applications Definitions）] オプション ボタンをクリックします。

ステップ 6　[完了（Done）] をクリックします。

クライアント アプリケーションによるポリシー制御設定の定義

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 テーブルで必要なポリシー名を検索します。

ステップ 3　同じ行の [プロトコルとクライアント アプリケーション（Protocols and Client Applications）] 列のセル リンクをクリックします。

ステップ 4　[プロトコルおよびクライアント アプリケーション設定の編集（Edit Protocols and Client Applications Settings）] ペインのドロップダウン リストから、[カスタム設定を定義（Define Custom Settings）] を選択します（まだ設定していない場合）。

ステップ 5　定義するクライアント アプリケーションに対応する [カスタム クライアント アプリケーション（Custom Client Applications）] フィールドに正規表現を入力します。必要に応じて、新規行に追加の正規表現を入力します。

ヒント　正規表現の例を参照するには、[クライアント アプリケーションのパターン例（Example Client Application Patterns）] をクリックします。

ステップ 6　変更を送信し、保存します。

認証からのクライアント アプリケーションの除外

手順	作業	リンク
ステップ 1	認証が不要の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
ステップ 2	除外するクライアント アプリケーションとして識別プロファイルのメンバーシップを設定する。	ポリシーでのクライアント アプリケーションの使用
ステップ 3	上記の識別プロファイル以外の他のすべての識別プロファイルを、認証が必要なポリシーのテーブルに配置する。	ポリシーの順序

時間範囲とボリューム クォータ

アクセス ポリシーと復号化ポリシーに時間およびボリューム クォータを適用して、ユーザの接続時間やデータ量（別名「帯域幅クォータ」）を制限します。クォータを使用すると、与えられたデータ量と時間を使い切るまで、個々のユーザはインターネット リソース（またはインターネット リソース クラス）にアクセスできます。AsyncOS は、HTTP、HTTPS、FTP トラフィックに定義されたクォータを適用します。

ユーザが時間またはボリューム クォータに達すると、AsyncOS は最初に警告を表示し、次にブロック ページを表示します。

時間およびボリューム クォータの使用について、以下の点に注意してください。

- AsyncOS がトランスペアレント モードで展開され、HTTPS プロキシがディセーブルの場合、ポート 443 ではリッスンされず、要求はドロップされます。これは標準の動作です。AsyncOS が明示モードで展開されている場合は、アクセス ポリシーにクォータを設定できます。

  HTTPS プロキシがイネーブルの場合、要求に対して実行可能なアクションは、パススルー、復号化、ドロップ、またはモニタとなります。全般的に、復号化ポリシーのクォータはパススルー カテゴリにのみ適用されます。

  パススルーの場合は、トンネル トラフィックのクォータを設定するオプションもあります。アクセス ポリシーで設定したクォータは復号化トラフィックに適用されるため、復号化ではこのオプションは使用できません。

- URL フィルタリングがディセーブルの場合やキーが使用できない場合、AsyncOS は URL のカテゴリを識別できず、[アクセス ポリシー（Access Policy）] -> [URL フィルタリング（URL Filtering）] ページはディセーブルになります。したがって、クォータを設定するには、機能キーが存在し、アクセプタブル ユース ポリシーがイネーブルになっている必要があります。

- Facebook や Gmail など、多くの Web サイトでは自動アップデートが頻繁に起こります。使用していないブラウザ ウィンドウやタブでこのような Web サイトを開いたままにしておくと、ユーザの時間およびボリューム クォータが消費され続けます。
- プロキシの再起動によってクォータがリセットされ、予定よりも多くのアクセスが許可される可能性があります。プロキシの再起動は、設定変更、クラッシュ、マシンのリブートなどによって発生することがあります。管理者はプロキシの再起動について明示的に通知されないため、多少の混乱が生じる可能性があります。
- decrypt-for-EUN オプションがイネーブルの場合でも、HTTPS に対して EUN ページ（警告とブロックの両方）を表示できません。

（注）　複数のクォータを特定のユーザに適用した場合は、常に最も制限が厳しいクォータが適用されます。

ボリューム クォータの計算

ボリューム クォータの計算方法は次のとおりです。

- HTTP および復号化された HTTPS トラフィック：HTTP 要求と応答の本文がクォータの上限に対してカウントされます。要求ヘッダーと応答ヘッダーは上限に対してカウントされません。
- トンネル トラフィック（トンネル化 HTTPS を含む）：AsyncOS は、トンネル化トラフィックをクライアントからサーバに（およびその逆に）移動するだけです。トンネル化トラフィックのデータ量全体が、クォータの上限に対してカウントされます。
- FTP：制御接続トラフィックはカウントされません。アップロードおよびダウンロードされたファイルのサイズは、クォータの上限に対してカウントされます。

（注）　クライアント側のトラフィックのみがクォータの上限に対してカウントされます。応答がキャッシュから送信された場合でもクライアント側のトラフィックが生成されるため、キャッシュされたコンテンツも上限に対してカウントされます。

時間クォータの計算

時間クォータの計算方法は次のとおりです。

- HTTP および復号化された HTTPS トラフィック：同じ URL カテゴリへの各接続時間（確立から切断まで）に 1 分を加えた時間が、時間クォータの上限に対してカウントされます。1 分以内に同じ URL カテゴリに対して複数の要求が行われた場合、それらは 1 つの連続セッションとしてカウントされ、セッションの最後（つまり、少なくとも 1 分の「沈黙」の後）にのみ 1 分が追加されます。
- トンネル トラフィック（トンネル化 HTTPS を含む）：トンネルの実際の期間（確立から切断まで）が、クォータの上限に対してカウントされます。複数の要求に対する上記の計算は、トンネル化トラフィックにも適用されます。
- FTP：FTP 制御セッションの実際の期間（確立から切断まで）が、クォータの上限に対してカウントされます。複数の要求に対する上記の計算は、FTP トラフィックにも適用されます。

時間およびボリューム クォータの定義

はじめる前に

- [セキュリティ サービス(Security Services)] > [使用許可コントロール(Acceptable Use Controls)] に移動し、使用許可コントロールをイネーブルにします。
- 毎日の制限としてクォータを適用しない場合は、時間範囲を定義します。時間およびボリューム クォータの定義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)] > [時間範囲およびクォータの定義(Define Time Ranges and Quotas)] に移動します。

ステップ 2　[クォータの追加(Add Quota)] をクリックします。

ステップ 3　[クォータ名(Quota Name)] に一意のクォータ名を入力します。

ステップ 4　クォータを毎日リセットするには、[毎日このクォータをリセットする時刻(Reset this quota daily at)] を選択し、フィールドに 12 時間形式で時刻を入力し、メニューから [AM] または [PM] を選択します。または、[事前定義された時間範囲プロファイルを選択します(Select a predefined time range profile)] を選択します。

ステップ 5　時間クォータを設定するには、[時間クォータTime Quota] チェックボックスをオンにして、[時間(hrs)] メニューから時間数を、[分(mins)] メニューから分数を選択し、ゼロ分(常にブロック)から 23 時間 59 分までの時間数を設定します。

ステップ 6　ボリューム クォータを設定するには、フィールドに数字を入力し、メニューから [KB](キロバイト)、[MB](メガバイト)、または [GB](ギガバイト)を選択します。

ステップ 7　[送信(Submit)] をクリックし、次に [変更を確定(Commit Changes)] をクリックして変更を適用します。または、[キャンセル(Cancel)] をクリックして変更を破棄します。

次の手順

- (任意)[セキュリティ サービス(Security Services)] > [エンドユーザ通知(End-User Notification)] に移動し、クォータ用のエンドユーザ通知を設定します。

URL カテゴリによるアクセス制御

対応する Web サイトのカテゴリに基づいて、Web 要求を識別してアクションを実行できます。Web セキュリティ アプライアンスには、多数の定義済み URL カテゴリ(Web ベースの電子メールなど)がデフォルトで用意されています。

定義済みのカテゴリおよびそれらに関連付けられている Webサイトは、Web セキュリティ アプライアンスに搭載されているフィルタリング データベースで定義されます。これらのデータベースは、Cisco によって自動的に最新の状態に維持されます。ただし、指定した IP アドレスとホスト名に対して、ユーザ定義のカスタム URL カテゴリを作成することもできます。

URL カテゴリは、要求を識別するポリシーを除くすべてのポリシーで使用できます。また、要求にアクションを適用するポリシー(アクセス、暗号化 HTTPS 管理、データ セキュリティ)でも使用できます。

カスタム URL カテゴリ

はじめる前に

- [セキュリティ サービス（Security Services）] > [使用許可コントロール（Acceptable Use Controls）] に移動し、使用許可コントロールをイネーブルにします。

ステップ 1　[Web セキュリティ マネージャ（Web Security Manager）] > [カスタム URL カテゴリ（Custom URL Categories）] を選択します。

ステップ 2　[カスタム カテゴリを追加（Add Custom Category）] をクリックします。

ステップ 3　カスタム URL カテゴリの設定を入力します。

表 10-2

設定	説明
カテゴリ名（Category Name）	URL カテゴリの名前を入力します。この名前は、ポリシーに URL フィルタリングを設定するときに表示されます。 **注：**名前の最初の 4 文字にスペースが含まれていると、Sawmill for レポーティング ツールはアクセス ログでカスタム URL カテゴリを検出できません。
リスト順（List Order）	このカテゴリを配置するカスタム URL カテゴリ リスト内の順序を選択します。最上位の URL カテゴリの場合は「1」を入力します。 URL フィルタリング エンジンでは、指定した順序でカスタム URL カテゴリに対してクライアント要求が評価されます。
サイト（Sites）	カスタム カテゴリに属する 1 つまたは複数のアドレスを入力します。 複数のアドレスは、改行またはカンマで区切って入力します。アドレスは次のいずれかの形式を使用して入力できます。 • IP アドレス。10.1.1.0 など • CIDR アドレス。10.1.1.0/24 など • ドメイン名（example.com など） • ホスト名。crm.example.com など • ホスト名の一部（.example.com など） **注：**「.example.com」など、ホスト名の一部を入力すると、www.example.com も一致するようになります。 **注**：複数のカスタム URL カテゴリで同じアドレスを使用することは可能ですが、カテゴリがリストされる順序は相互関係によります。同じポリシーにこれらのカテゴリを含め、それぞれに異なるアクションを定義した場合は、[カスタム URL カテゴリ（Custom URL Categories）] テーブルの一番上に配置されているカテゴリのアクションが効力を持ちます。
詳細設定：正規表現（Advanced: Regular Expressions）	正規表現を使用して、入力したパターンと一致する複数の Web サーバを指定できます。 **注：**URL フィルタリング エンジンでは、最初に、URL と [サイト（Sites）] フィールドに入力したアドレスが比較されます。トランザクションの URL が [サイト（Sites）] フィールドの入力値と一致した場合は、ここで入力した式との比較は行われません。

ステップ 4　(任意)[URL のソート(Sort URLs)] をクリックして、[サイト(Sites)] フィールド内のすべてのアドレスを英数字順にソートします。

(注)　アドレスをソートした後は、元の順序に戻すことができません。

ステップ 5　変更を送信し、保存します。

関連項目
- 正規表現

URL カテゴリによる Web 要求の識別

はじめる前に
- 使用許可コントロールを有効にします(URL フィルタリング エンジンの設定を参照)。
- (任意)カスタム URL カテゴリを作成します(カスタム URL カテゴリを参照)。

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(SaaS 以外)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(または新しいポリシーを追加します)。

ステップ 3　[詳細設定(Advanced)] セクションを展開して、[URL カテゴリ(URL Categories)] フィールド内のリンクをクリックします。

ステップ 4　Web 要求の識別に使用する URL カテゴリに対応する [追加(Add)] 列のセルをクリックします。この操作を、カスタム URL カテゴリと定義済み URL カテゴリのリストに対して実行します。

ステップ 5　[完了(Done)] をクリックします。

ステップ 6　変更を送信し、保存します。

URL カテゴリによる Web 要求へのアクション

はじめる前に
- 使用許可コントロールを有効にします(URL フィルタリング エンジンの設定を参照)。
- (任意)カスタム URL カテゴリを作成します(カスタム URL カテゴリを参照)。

(注)　ポリシー内で基準として URL カテゴリを使用している場合は、同じポリシー内に対してアクションを指定するときにそれらのカテゴリだけを使用できます。そのため、下記のオプションの一部が異なっていたり、使用できないことがあります。

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 [アクセス ポリシー(Access Policies)]、[Cisco データ セキュリティ ポリシー(Cisco Data Security Policies)]、または[暗号化 HTTPS 管理(Encrypted HTTPS Management)] のいずれかを選択します。

ステップ 2　ポリシー テーブルで必要なポリシー名を検索します。

ステップ 3　同じ行の [URL フィルタリング(URL Filtering)] 列のセル リンクをクリックします。

ステップ 4　（任意）カスタム URL カテゴリを追加します。

a. [カスタム カテゴリの選択（Select Custom Categories）] をクリックします。

b. このポリシーに含めるカスタム URL カテゴリを選択して、[適用（Apply）] をクリックします。

URL フィルタリング エンジンでクライアント要求と照合するカスタム URL カテゴリを選択します。URL フィルタリング エンジンは、クライアント要求と含まれているカスタム URL カテゴリを比較します。除外されたカスタム URL カテゴリは無視されます。URL フィルタリング エンジンは、定義済みの URL カテゴリよりも前に、含まれているカスタム URL カテゴリとクライアント要求の URL を比較します。

ポリシーに含まれているカスタム URL カテゴリは、[カスタム URL カテゴリのフィルタリング（Custom URL Category Filtering）] セクションに表示されます。

ステップ 5　カスタムおよび定義済みの各 URL カテゴリのアクションを選択します。

（注）　使用可能なアクションは、カスタム カテゴリと定義済みカテゴリとで異なり、ポリシー タイプによっても異なります。

ステップ 6　[分類されてない URL（Uncategorized URLs）] セクションで、定義済みまたはカスタムの URL カテゴリに分類されない Web サイトへのクライアント要求に対して実行するアクションを選択します。

ステップ 7　変更を送信し、保存します。

リモート ユーザ

リモート ユーザについて

Cisco AnyConnect Secure Mobility はネットワーク境界をリモート エンドポイントまで拡張し、Web セキュリティ アプライアンスによる Web フィルタリング サービスのシームレスな統合を実現します。

リモート ユーザおよびモバイル ユーザは Cisco AnyConnect Secure VPN（仮想プライベート ネットワーク）クライアントを使用して、適応型セキュリティ アプライアンス（ASA）との VPN セッションを確立します。ASA は、IP アドレスとユーザ名によるユーザ識別情報とともに、Web トラフィックを Web セキュリティ アプライアンスに送信します。Web セキュリティ アプライアンスは、トラフィックをスキャンしてアクセプタブル ユース ポリシーを適用し、セキュリティ上の脅威からユーザを保護します。セキュリティ アプライアンスは、安全と判断された、ユーザが受け入れ可能なすべてのトラフィックを返します。

Secure Mobility がイネーブルの場合は、ID とポリシーを設定し、ユーザの場所に応じてユーザに適用できます。

- **リモート ユーザ。**これらのユーザは、VPN を使用してリモートの場所からネットワークに接続されます。Cisco ASA と Cisco AnyConnect クライアントの両方が VPN アクセスに使用される場合、Web セキュリティ アプライアンスはリモート ユーザを自動的に識別します。それ以外の場合、Web セキュリティ アプライアンス管理者は IP アドレスの範囲を設定して、リモート ユーザを指定する必要があります。
- **ローカル ユーザ。**これらのユーザは、有線またはワイヤレスでネットワークに接続されます。

Web セキュリティ アプライアンスを Cisco ASA と統合すると、認証されたユーザ名によりユーザを透過的に識別するように設定して、リモート ユーザのシングル サインオンを実現できます。

リモート ユーザ用の ID の設定

作業	解説場所
1. リモート ユーザの ID を設定する。	リモート ユーザの ID の設定（10-19 ページ）
2. リモート ユーザの ID 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） a. [ユーザの場所別メンバーの定義（Define Members by User Location）] セクションで、[ローカル ユーザのみ（Local Users Only）] を選択します。 b. [認証ごとにメンバを定義（Define Members by Authentication）] セクションで、[Cisco ASA 統合を通じてユーザを透過的に識別する（Identify Users Transparently through Cisco ASA Integration）] を選択します。
3. リモート ユーザのポリシーを作成する。	ポリシーの作成（10-5 ページ）

リモート ユーザの ID の設定

ステップ 1　[セキュリティ サービス（Security Services）] > [AnyConnect セキュア モビリティ（AnyConnect Secure Mobility）] で、[有効（Enable）] をクリックします。

ステップ 2　AnyConnect セキュア モビリティの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　リモート ユーザの識別方法を設定します。

オプション	説明	この他の手順
[IPアドレス（IP Address）]	アプライアンスがリモート デバイスに割り当てられていると見なす IP アドレスの範囲を指定します。	1. [IP 範囲（IP Range）] フィールドに IP アドレスの範囲を入力します。 2. ステップ 4 に進みます。

オプション	説明	この他の手順
Cisco ASA 統合（Cisco ASA Integration）	Web セキュリティ アプライアンスが通信する 1 つ以上の Cisco ASA を指定します。Cisco ASAは IP アドレスとユーザのマッピングを保持し、その情報を Web セキュリティ アプライアンスに伝達します。Web プロキシはトランザクションを受信すると、IP アドレスを取得し、IP アドレスとユーザのマッピングをチェックしてユーザを特定します。Cisco ASA と統合してユーザを特定する場合は、リモート ユーザのシングル サイン オンをイネーブルにできます。	1. Cisco ASA のホスト名または IP アドレスを入力します。 2. ASA へのアクセスに使用するポート番号を入力します。Cisco ASA のデフォルト ポート番号は 11999 です。 3. クラスタ内に複数の Cisco ASA が設定されている場合は、[行の追加（Add Row）] をクリックし、クラスタ内の各 ASA を設定します。 **（注）** 2 つの Cisco ASA が高可用性に設定されている場合は、*アクティブな* Cisco ASA の 1 つのホスト名または IP アドレスのみを入力します。 4. Cisco ASA のアクセス パスワードを入力します。 **（注）** ここで入力するパスワードは、指定した Cisco ASA 用に設定されているアクセス パスワードと一致する必要があります。 5. （任意）[テスト開始（Start Test）] をクリックして、Web セキュリティ アプライアンスが設定されている Cisco ASAに接続できることを確認します。

ステップ 4　変更を送信して確定します。

ASA のリモート ユーザ ステータスと統計情報の表示

Web セキュリティ アプライアンスが ASA と統合されている場合は、次のコマンドを使用して Secure Mobility に関連する情報を表示します。

コマンド	説明
`musstatus`	このコマンドにより、次の情報が表示されます。 • Web セキュリティ アプライアンスと各 ASA との接続ステータス。 • Web セキュリティ アプライアンスと各 ASA との接続時間（分単位）。 • 各 ASA からのリモート クライアントの数。 • サービス対象のリモート クライアントの数。これは、Web セキュリティ アプライアンスを介してトラフィックの受け渡しを行ったリモート クライアントの数です。 • リモート クライアントの合計数。

ポリシーに関するトラブルシューティング

HTTPS トラフィックを制御する復号化ポリシーの作成

HTTP 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 トラフィックを次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は注意してください。**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 セキュリティ アプライアンスのアクセス 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(11-3 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(11-7 ページ) • 証明書およびキーの生成(11-8 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(11-5 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(11-9 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(11-10 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(11-11 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、次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	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。
パススルー	アプライアンスは、トラフィックの内容を検査せずに、クライアントとサーバ間の接続をパススルーします。
復号化	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。

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 セキュリティ アプライアンス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、次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、アプライアンスがトランスペアレント 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（11-6 ページ）

HTTPS トラフィックの制御

Web セキュリティ アプライアンスが復号化ポリシー 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によって、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まります。

オプション	説明
URL カテゴリ（URL Categories）	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 カテゴリ（URL Categories）] 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（Default Action）	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。

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（11-3 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、ポリシー トレースの実行時に、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「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、次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、次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（22-25 ページ）を参照してください。

Web セキュリティ アプライアンスが作成したルート証明書を処理する場合は、次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 セキュリティ アプライアンス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（11-6 ページ）
- 無効な証明書の処理の設定（11-9 ページ）
- 証明書失効ステータスのチェックのオプション（11-9 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（11-10 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、次のアクションの 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 セキュリティ アプライアンス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（11-3 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 セキュリティ アプライアンスに転送します。

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。

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（11-3 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 セキュリティ アプライアンス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（11-3 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、プロキシの応答（**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。トランスペアレント 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 セキュリティ アプライアンスでは、次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 セキュリティ アプライアンスは 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 セキュリティ アプライアンス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。
- **Online Certificate Status Protocol（OCSP）。** Web セキュリティ アプライアンスが、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（11-10 ページ）
- 無効な証明書の処理の設定（11-9 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（11-3 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
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。
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。
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。
Allowed Clock Skew	Web セキュリティ アプライアンスと 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。
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。
Use upstream proxy for OCSP checking	アップストリーム プロキシのグループ名。
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（11-3 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 ヘッダー内の次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

- 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（A-6 ページ）
- IP ベースのサロゲートと透過的要求を含む HTTPS（A-7 ページ）
- 特定 Web サイトの復号化のバイパス（A-7 ページ）
- アラート：セキュリティ証明書に関する問題（Problem with Security Certificate）（A-7 ページ）

既存の感染に対する発信トラフィックのスキャン

発信トラフィックのスキャンの概要

悪意のあるデータがネットワークから流出するのを阻止するために、Web セキュリティ アプライアンスには 発信マルウェア スキャン（Outbound Malware Scanning）機能が用意されています。ポリシー グループを使用して、マルウェアのスキャン対象となるアップロード、スキャンに使用するマルウェア対策スキャン エンジン、ブロックするマルウェアのタイプを定義できます。

Cisco IronPort Dynamic Vectoring and Streaming（DVS）エンジンは、トランザクション要求がネットワークから発信されるときにそれをスキャンします。Cisco IronPort DVS エンジンとの連携により、Web セキュリティ アプライアンスでは無意識のうちに悪意のあるデータがアップロードされるのを防止できます。

次の作業を実行できます。

タスク	タスクへのリンク
マルウェアをブロックするポリシーを作成する	発信マルウェア スキャン ポリシーの作成（12-4 ページ）
発信マルウェア ポリシー グループにアップロード要求を割り当てる	アップロード要求の制御（12-6 ページ）

要求がブロックされた場合のユーザ エクスペリエンス

Cisco IronPort DVS エンジンがアップロード要求をブロックすると、Web プロキシはエンド ユーザにブロック ページを送信します。ただし、すべての Web サイトでエンド ユーザにブロック ページが表示されるわけではありません。一部の Web 2.0 Web サイトでは、静的 Web ページの代わりに JavaScript を使用して動的コンテンツが表示され、ブロック ページが表示されることはありません。そのような場合でも、ユーザは適切にブロックされているので悪意のあるデータをダウンロードすることはありませんが、そのことが Web サイトから通知されない場合もあります。

アップロード要求について

発信マルウェア スキャン（Outbound Malware Scanning）ポリシーは、サーバにデータをアップロードするトランザクション（アップロード要求）に対して、Web プロキシが HTTP 要求と復号化 HTTPS 接続をブロックするかどうかを定義します。アップロード要求は、要求本文にコンテンツが含まれている HTTP または復号化 HTTPS 要求です。

アップロード要求を受信すると、Web プロキシは要求を発信マルウェア スキャン（Outbound Malware Scanning）ポリシー グループと比較して、適用するポリシー グループを決定します。ポリシー グループに要求を割り当てた後、ポリシー グループの設定済み制御設定と要求を比較し、要求をモニタするかブロックするかを決定します。発信マルウェア スキャン（Outbound Malware Scanning）ポリシーによる判定で要求をモニタすることが決定されると、要求はアクセス ポリシーに対して評価され、Web プロキシが実行する最終アクションが該当するアクセス ポリシーによって決定されます。

（注） サイズがゼロ（0）バイトのファイルのアップロードを試みているアップロード要求は、発信マルウェア スキャン（Outbound Malware Scanning）ポリシーに対して評価されません。

グループ メンバーシップの基準

各クライアント要求に ID が割り当てられ、次に、それらの要求が他のポリシー タイプと照合して評価され、タイプごとに要求が属するポリシー グループが判定されます。Web プロキシは、クライアント要求のポリシー グループ メンバーシップに基づいて、設定されているポリシー制御設定をクライアント要求に適用します。

Web プロキシは、特定のプロセスを実行してグループ メンバーシップの基準と照合します。グループ メンバーシップの次の要素が考慮されます。

基準	説明
ID（Identity）	各クライアント要求は、ID に一致するか、認証に失敗してゲスト アクセスが許可されるか、または認証に失敗して終了します。
権限を持つユーザ	割り当てられた ID が認証を必要とする場合は、そのユーザが発信マルウェア スキャン（Outbound Malware Scanning）ポリシー グループの承認済みユーザのリストに含まれており、ポリシー グループに一致している必要があります。承認済みユーザのリストには、任意のグループまたはユーザを指定でき、ID がゲスト アクセスを許可している場合はゲスト ユーザを指定できます。

基準	説明
詳細オプション	発信マルウェア スキャン（Outbound Malware Scanning）ポリシー グループ メンバーシップに対して複数の詳細オプションを設定できます。一部のオプション（プロキシ ポート、URL カテゴリなど）は、ID 内に定義することもできます。ID 内に詳細オプションを設定する場合、発信マルウェア スキャン（Outbound Malware Scanning）ポリシー グループ レベルでは設定できません。

クライアント要求と発信マルウェア スキャン（Outbound Malware Scanning）ポリシー グループとの照合

Web プロキシは、アップロード要求のステータスを最初のポリシー グループのメンバーシップ基準と比較します。一致した場合、Web プロキシは、そのポリシー グループのポリシー設定を適用します。

一致しない場合は、その次のポリシー グループとアップロード要求を比較します。アップロード要求をユーザ定義のポリシー グループと照合するまで、Web プロキシはこのプロセスを続行します。ユーザ定義のポリシー グループに一致しない場合は、グローバル ポリシー グループと照合します。Web プロキシは、アップロード要求をポリシー グループまたはグローバル ポリシー グループと照合するときに、そのポリシー グループのポリシー設定を適用します。

発信マルウェア スキャン（Outbound Malware Scanning）ポリシーの作成

宛先サイトの URL カテゴリや 1 つ以上の ID など、複数の条件の組み合わせに基づいて発信マルウェア スキャン（Outbound Malware Scanning）ポリシー グループを作成できます。ポリシー グループのメンバーシップには、少なくとも 1 つの条件を定義する必要があります。複数の条件が定義されている場合、アップロード要求がポリシー グループと一致するには、すべての条件を満たしていなければなりません。ただし、アップロード要求は設定された ID の 1 つとのみ一致する必要があります。

ステップ 1　[Web セキュリティ マネージャ（Web Security Manager）] > [発信マルウェア スキャン（Outbound Malware Scanning）] を選択します。

ステップ 2　[ポリシーを追加（Add Policy）] をクリックします。

ステップ 3　ポリシー グループの名前と説明（任意）を入力します。

（注）　各ポリシー グループ名は、英数字またはスペース文字のみを含む、一意の名前とする必要があります。

ステップ 4　[上記ポリシーを挿入（Insert Above Policy）] フィールドで、ポリシー テーブル内のポリシー グループを配置する場所を選択します。

複数のポリシー グループを設定する場合は、各グループに論理的な順序を指定します。

ステップ 5　[アイデンティティとユーザ（Identities and Users）] セクションで、このグループ ポリシーに適用する 1 つ以上の ID グループを選択します。

ステップ 6　（任意）[詳細（Advanced）] セクションを拡張して、追加のメンバーシップ要件を定義します。

ステップ 7　いずれかの拡張オプションを使用してポリシー グループのメンバーシップを定義するには、拡張オプションのリンクをクリックし、表示されるページでオプションを設定します。

高度なオプション	説明
プロトコル（Protocols）	クライアント要求で使用されるプロトコルによってポリシー グループのメンバーシップを定義するかどうかを選択します。含めるプロトコルを選択します。 [その他のすべて（All others）] は、このオプションの上に一覧表示されていないプロトコルを意味します。 **（注）**　HTTPS プロキシをイネーブルにすると、復号化ポリシーのみが HTTPS トランザクションに適用されます。アクセス、ルーティング、発信マルウェア スキャン（Outbound Malware Scanning）、データ セキュリティ、外部 DLP のポリシーの場合は、HTTPS プロトコルによってポリシー メンバーシップを定義できません。
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プロキシ ポートで、ポリシー グループ メンバーシップを定義するかどうかを選択します。[プロキシ ポート（Proxy Ports）] フィールドに、1 つ以上のポート番号を入力します。複数のポートを指定する場合は、カンマで区切ります。 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。トランスペアレント接続の場合は、宛先ポートと同じです。 クライアント要求がアプライアンスに透過的にリダイレクトされるときにプロキシ ポートでポリシー グループのメンバーシップを定義すると、一部の要求が拒否される場合があります。 **（注）**　このポリシー グループに関連付けられている ID が、この詳細設定によって ID メンバーシップを定義している場合、非 ID ポリシー グループ レベルではこの設定項目を設定できません。
サブネット（Subnets）	サブネットまたは他のアドレスでポリシー グループのメンバーシップを定義するかどうかを選択します。 関連 ID で定義されている可能性のあるアドレスを使用するか、またはここで特定のアドレスを入力することができます。 **（注）**　ポリシー グループに関連付けられている ID がアドレスによってグループのメンバーシップを定義している場合は、ID で定義されているアドレスのサブセットであるアドレスを、このポリシー グループに入力する必要があります。ポリシー グループにアドレスを追加することにより、このグループ ポリシーに一致するトランザクションのリストを絞り込めます。
URL カテゴリ（URL Categories）	URL カテゴリでポリシー グループのメンバーシップを定義するかどうかを選択します。ユーザ定義または定義済みの URL カテゴリを選択します。 **（注）**　このポリシー グループに関連付けられている ID が、この詳細設定によって ID メンバーシップを定義している場合、非 ID ポリシー グループ レベルではこの設定項目を設定できません。

高度なオプション	説明
ユーザ エージェント（User Agents）	クライアント要求で使用されるユーザ エージェントによってポリシー グループのメンバーシップを定義するかどうかを選択します。一般的に定義されているブラウザを選択するか、正規表現を使用して独自のブラウザを定義できます。このポリシー グループを、選択したユーザ エージェントに適用するか、または選択したユーザ エージェントのリストに含まれていないユーザ エージェントに適用するかどうかを選択します。 **（注）** このポリシー グループに関連付けられている ID が、この詳細設定によって ID メンバーシップを定義している場合、非 ID ポリシー グループ レベルではこの設定項目を設定できません。
ユーザの場所（User Location）	ユーザのリモートまたはローカルの場所でポリシー グループのメンバーシップを定義するかどうかを選択します。

ステップ 8　変更を送信します。

ステップ 9　発信マルウェア スキャン（Outbound Malware Scanning）ポリシー グループの制御設定を設定し、Web プロキシがトランザクションを処理する方法を定義します。

新しい発信マルウェア スキャン（Outbound Malware Scanning）ポリシー グループは、各制御設定のオプションが設定されるまで、グローバル ポリシー グループの設定を自動的に継承します。

ステップ 10　変更を送信して確定します。

アップロード要求の制御

各アップロード要求は、発信マルウェア スキャン（Outbound Malware Scanning）ポリシー グループに割り当てられ、そのポリシー グループの制御設定を継承します。Web プロキシがアップロード要求ヘッダーを受信すると、要求本文をスキャンする必要があるかどうかを判定するために必要な情報が提供されます。DVS エンジンは要求をスキャンし、Web プロキシに判定を返します。必要に応じて、エンド ユーザにブロック ページが表示されます。

ステップ 1　[Web セキュリティ マネージャ（Web Security Manager）] > [発信マルウェア スキャン（Outbound Malware Scanning）] を選択します。

ステップ 2　[接続先（Destinations）] 列で、設定するポリシー グループのリンクをクリックします。

ステップ 3　[接続先設定の編集（Edit Destination Settings section）] セクションで、ドロップダウン メニューから [接続先スキャンのカスタム設定の定義（Define Destinations Scanning Custom Settings）] を選択します。

ステップ 4　[スキャンする接続先（Destination to Scan）] セクションで、次のいずれかを選択します。

オプション	説明
どのアップロードもスキャンしない（Do not scan any uploads）	DVS エンジンはアップロード要求をスキャンしません。すべてのアップロード要求がアクセス ポリシーに対して評価されます。
すべてのアップロードをスキャンする（Scan all uploads）	DVS エンジンはすべてのアップロード要求をスキャンします。DVS エンジンのスキャン判定に応じて、アップロード要求はブロックされるか、またはアクセス ポリシーに対して評価されます。
指定したカスタム URL カテゴリへのアップロードをスキャン（Scan uploads to specified custom URL categories）	DVS エンジンは、特定のカスタム URL カテゴリに属するアップロード要求をスキャンします。DVS エンジンのスキャン判定に応じて、アップロード要求はブロックされるか、またはアクセス ポリシーに対して評価されます。 [カスタム カテゴリ リストを編集（Edit custom categories list）] をクリックして、スキャンする URL カテゴリを選択します。

ステップ 5　変更を送信します。

ステップ 6　[マルウェア対策フィルタリング（Anti-Malware Filtering）] 列で、ポリシー グループのリンクをクリックします。

ステップ 7　[マルウェア対策設定（Anti-Malware Settings）] セクションで、[マルウェア対策カスタム設定の定義（Define Anti-Malware Custom Settings）] を選択します。

ステップ 8　[Cisco IronPort DVS マルウェア対策設定（Cisco IronPort DVS Anti-Malware Settings）] セクションで、このポリシー グルーに対してイネーブルにするマルウェア対策スキャン エンジンを選択します。

ステップ 9　[マルウェア カテゴリ（Malware Categories）] セクションで、さまざまなマルウェア カテゴリをモニタするかブロックするかを選択します。

このセクションに表示されるカテゴリは、イネーブルにするスキャン エンジンによって異なります。

（注）　設定された最大時間に達した場合や、システムで一時的エラーが発生した場合、URL トランザクションはスキャン不可と分類されます。たとえば、スキャン エンジンのアップデート時や AsyncOS のアップグレード時に、トランザクションがスキャン不可と分類されることがあります。マルウェア スキャンの判定が SV_TIMEOUT や SV_ERROR の場合は、スキャン不可のトランザクションと見なされます。

ステップ 10　変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

ロギング

アクセス ログは、DVS エンジンがマルウェアについてアップロード要求をスキャンしたかどうかを示します。各アクセス ログ エントリのスキャン判定情報セクションには、スキャンされたアップロードに対する DVS エンジン アクティビティの値が含まれています。フィールドのいずれかを W3C またはアクセス ログに追加すると、この DVS エンジン アクティビティをより簡単に検索できます。

表 12-1　W3C ログのログ フィールドおよびアクセス ログのフォーマット指定子

W3C ログ フィールド	アクセス ログのフォーマット指定子
x-req-dvs-scanverdict	%X2
x-req-dvs-threat-name	%X4
x-req-dvs-verdictname	%X3

DVS エンジンによってアップロード要求がマルウェアと判定され、DVS エンジンがマルウェアのアップロードをブロックするように設定されている場合、アクセス ログの ACL デシジョン タグは BLOCK_AMW_REQ になります。

ただし、DVS エンジンによってアップロード要求がマルウェアと判定され、DVS エンジンがマルウェアを *モニタ*するように設定されている場合、アクセス ログの ACL デシジョン タグは、実際にトランザクションに適用されるアクセス ポリシーによって決まります。

DVS エンジンがマルウェアについてアップロード要求をスキャンしたかどうかを判断するには、各アクセス ログ エントリのスキャン判定情報セクションで、DVS エンジン アクティビティの結果を確認します。

セキュリティ サービスの設定

セキュリティ サービスの設定の概要

Web セキュリティ アプライアンスは、セキュリティ コンポーネントを使用してさまざまなマルウェアの脅威からエンド ユーザを保護します。各グループ ポリシーのマルウェア対策と Web レピュテーション設定値を設定できます。アクセス ポリシーを設定すると、AsyncOS for Web はブロックするコンテンツを判定するときに、マルウェア対策スキャンと Web レピュテーション スコアの組み合わせを使用することを選択できるようになります。

マルウェアからエンド ユーザを保護するには、アプライアンスでこれらの機能をイネーブルにしてから、ポリシーごとにマルウェア対策と Web レピュテーションの設定値を設定します。

オプション	説明	リンク
マルウェア対策スキャン（Anti-malware scanning）	アプライアンスに統合された複数のマルウェア対策スキャン エンジンを使用して、マルウェアの脅威をブロックします。	マルウェア対策 スキャンの概要（13-5 ページ）

オプション	説明	リンク
Web レピュテーション フィルタ（Web Reputation Filters）	Web サーバの動作を分析し、URL に URL ベースのマルウェアが含まれているかどうか判定します。	Web レピュテーション フィルタの概要（13-2 ページ）
高度なマルウェア防御（Advanced Malware Protection）	ファイル レピュテーションを評価し、ファイルの特性を分析することによって、ダウンロード ファイルに潜む脅威から保護します。	ファイル レピュテーション フィルタリングとファイル分析の概要（14-1 ページ）

関連項目

- マルウェア対策およびレピュテーション フィルタのイネーブル化（13-8 ページ）
- 関連項目（13-10 ページ）
- 適応型スキャンについて（13-8 ページ）

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 セキュリティ アプライアンスは、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、復号化、および Cisco IronPort データ セキュリティの各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、たとえば次のものがあります。

- 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、パスワード、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。
復号化ポリシー（Decryption Policies）	ドロップ、復号化、またはパススルーから選択できます。
Cisco IronPort データ セキュリティ ポリシー	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 ポリシーで 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良の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	操作	説明	例
-10 ～ -6.0	ブロック	不正なサイト。要求はブロックされ、さらなるマルウェア 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する。 • URL ボリュームによる突然のスパイク。 • URL が人気のあるドメインの誤入力。

スコア	操作	説明	例
-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、要求および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 スコアが陽性のネットワーク オーナーの IP アドレス。
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。 • 履歴が長く信頼できるボリュームが多いドメイン。 • 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（13-8 ページ）

復号化ポリシーの Web レピュテーション

スコア	操作	説明
-10 ～ -9.0	削除	不正なサイト。要求は、エンド ユーザに通知せずにドロップされます。この設定の使用には注意が必要です。
-8.9 ～ 5.9	復号化	判別不能なサイト。要求は許可されますが、接続が復号化され、アクセス ポリシーが復号化されたトラフィックに適用されます。
6.0 ～ 10.0	パススルー	正常なサイト。要求は、検査や復号化なしで渡されます。

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	操作	説明
-10 ～ -6.0	ブロック	不正なサイト。トランザクションはブロックされ、さらなる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、コンテンツの検査（ファイル タイプとサイズ）へと進みます。 **（注）**　スコアがないサイトがモニタされます。

マルウェア対策 スキャンの概要

Web セキュリティ アプライアンス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。

関連項目

- マルウェア対策およびレピュテーション フィルタのイネーブル化（13-8 ページ）
- 関連項目（13-10 ページ）

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 つのオブジェクトに対する複数の判定が 1 つのスキャン エンジンから返されることがあります。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。次のリストは、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 エンジンに送ります。Webroot スキャン エンジンは、次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、その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。
- **サーバの応答。**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 エンジンは次の方法を使用して、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、そのデータベースにあるウィルス定義をスキャン エンジンで使用し、特定のウィルス、ウィルスのタイプ、その他の潜在的に望ましくないソフトウェアを検出します。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場合は、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（Trojan）	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場合に、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。

マルウェア対策およびレピュテーション フィルタのイネーブル化

はじめる前に

- Web レピュテーション フィルタ、DVS エンジン、およびスキャン エンジン（Webroot、McAfee、Sophos）がイネーブルになっていることを確認します。デフォルトでは、システムのセットアップ時にこれらがイネーブルになります。

ステップ 1　[セキュリティ サービス（Security Services）] > [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] 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　必要に応じて、次の項目を設定します。

設定	説明
Web レピュテーション フィルタリング（Web Reputation Filtering）	Web レピュテーション フィルタリングをイネーブルにするかどうかを選択します。
適応型スキャン（Adaptive Scanning）	適応型スキャンをイネーブルにするかどうかを選択します。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にのみ、適応型スキャンをイネーブルにできます。
ファイル レピュテーション フィルタリングとファイル分析（File Analysis）	ファイル レピュテーションおよび分析サービスの有効化と設定（14-6 ページ）を参照してください。
DVS エンジン オブジェクト スキャンの制限（DVS Engine Object Scanning Limits）	最大要求/応答サイズを指定します。 指定した [最大オブジェクト サイズ（Maximum Object Size）] の値は、すべてのマルウェア対策とウイルス対策スキャン エンジンおよび高度なマルウェア防御機能によってスキャンされる、要求と応答のサイズ全体に適用されます。アップロードまたはダウンロードのサイズがこのサイズを超えると、セキュリティ コンポーネントは、進行中のスキャンを中断し、Web プロキシにスキャンの判定を提供しない可能性があります。
Sophos	Sophos スキャン エンジンをイネーブルにするかどうかを選択します。
McAfee	McAfee スキャン エンジンをイネーブルにするかどうかを選択します。 McAfee をイネーブルにするときに、ヒューリスティック スキャンをイネーブルにするかどうかも選択できます。 **（注）** ヒューリスティック分析はセキュリティ保護を向上させますが、偽陽性が生じてパフォーマンスが低下する可能性があります。
Webroot	Webroot スキャン エンジンをイネーブルにするかどうかを選択します。 Webroot スキャン エンジンをイネーブルにするときに、脅威リスクしきい値（TRT）を設定できます。TRT はマルウェアが存在する確率に対して数値を割り当てます。 独自のアルゴリズムによって URL 照合シーケンスの結果を評価し、脅威リスク レーティング（TRR）を割り当てます。この値は、TRT 設定に関連付けられます。TRR 値が TRT 以上の場合、URL はマルウェアと見なされ、さらなる処理に渡されます。 **（注）** 脅威リスクしきい値に 90 より低い値を設定すると、URL ブロッキング レートが劇的に増加し、正当な要求が拒否されてしまいます。TRT のデフォルト値 90 を維持することを強く推奨します。TRT 設定の最小値は 51 です。

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）]）。

関連項目

- 適応型スキャンについて（13-8 ページ）
- McAfee スキャン（13-6 ページ）

ポリシーにおけるマルウェア対策およびレピュテーションの設定

[マルウェア対策およびレピュテーションフィルタ（Anti-Malware and Reputation Filters）] がアプライアンスでイネーブルの場合は、ポリシー グループでさまざまな設定値を設定できます。マルウェア スキャンの判定に基づいて、マルウェア カテゴリのモニタまたはブロックをイネーブルにできます。

次のポリシー グループにマルウェア対策を設定できます。

ポリシー タイプ	タスクへのリンク
アクセス ポリシー（Access Policies）	アクセス ポリシーにおけるマルウェア対策およびレピュテーションの設定（13-10 ページ）
Outbound Malware Scanning ポリシー	発信マルウェア スキャン ポリシーによるアップロード要求の制御

次のポリシー グループに Web レピュテーションを設定できます。

ポリシー タイプ	タスクへのリンク
アクセス ポリシー（Access Policies）	アクセス ポリシーにおけるマルウェア対策およびレピュテーションの設定（13-10 ページ）
復号化ポリシー（Decryption Policies）	復号化ポリシー グループの Web レピュテーション フィルタの設定（13-14 ページ）
シスコ データ セキュリティ ポリシー	復号化ポリシー グループの Web レピュテーション フィルタの設定（13-14 ページ）

高度なマルウェア防御機能はアクセス ポリシーにのみ設定できます。ファイル レピュテーション機能と分析機能の設定（14-4 ページ）を参照してください。

アクセス ポリシーにおけるマルウェア対策およびレピュテーションの設定

適応型スキャンがイネーブルの場合、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は、適応型スキャンがオフの場合とやや異なります。

（注）　展開にセキュリティ管理アプライアンスが含まれており、この機能を設定マスターに設定する場合、このページのオプションは、関連する設定マスターで適応型セキュリティがイネーブルになっているかどうかに応じて異なります。[Web] > [ユーティリティ（Utilities）] > [セキュリティ サービス表示（Security Services Display）] ページで、セキュリティ管理アプライアンスの設定を確認します。

関連項目

- 適応型スキャンについて（13-8 ページ）

マルウェア対策およびレピュテーションの設定（適応型スキャンがイネーブルの場合）

ステップ 1　[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。

ステップ 2　設定するアクセス ポリシーの [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] リンクをクリックします。

ステップ 3　[Web レピュテーションとマルウェア対策の設定（Web Reputation and Anti-Malware Settings）] セクションで [Web レピュテーションとマルウェア対策のカスタム設定の定義（Define Web Reputation and Anti-Malware Custom Settings）] を選択します。

これにより、このアクセス ポリシーに対して、グローバル ポリシーとは異なる Web レピュテーションとマルウェア対策の設定を指定できます。

ステップ 4　[Web レピュテーション設定（Web Reputation Settings）] セクションで、Web レピュテーション フィルタリングをイネーブルにするかどうかを選択します。適応型スキャンによって、各 Web 要求に最適な Web レピュテーション スコアのしきい値が選択されます。

ステップ 5　[高度なマルウェア防御設定（Advanced Malware Protection Settings）] セクションで設定項目を設定します。

ステップ 6　[Cisco IronPort DVS マルウェア防御設定（Cisco IronPort DVS Anti-Malware Settings）] セクションまでスクロールします。

ステップ 7　必要に応じて、ポリシーのマルウェア対策設定を指定します。

設定	説明
疑わしいユーザ エージェント スキャンを有効にする（Enable Suspect User Agent Scanning）	HTTP 要求ヘッダーで指定されているユーザ エージェント フィールドに基づいて、トラフィックをスキャンするかどうかを選択します。 このチェックボックスをオンにした場合は、ページ下部の [追加スキャン（Additional Scanning）] セクションで、疑わしいユーザ エージェントをモニタするかブロックするかを選択できます。
マルウェア対策スキャンを有効にする（Enable Anti-Malware Scanning）	マルウェアのトラフィックをスキャンするために、DVS エンジンを使用するかどうかを選択します。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。

設定	説明
マルウェア カテゴリ（Malware Categories）	マルウェア スキャンの判定に基づいて各種のマルウェア カテゴリをモニタするかブロックするかを選択します。
その他カテゴリ（Other Categories）	このセクションに表示されたオブジェクトおよび応答のタイプを、モニタするかブロックするかを選択します。 **（注）** [アウトブレイク ヒューリスティック（Outbreak Heuristics）] カテゴリは、スキャン エンジンの実行前に適応型スキャンによってマルウェアとして識別されたトランザクションに適用されます。 **（注）** 設定された最大時間に達した場合や、システムで一時的エラーが発生した場合、URL トランザクションはスキャン不可と分類されます。たとえば、スキャン エンジンのアップデート時や AsyncOS のアップグレード時に、トランザクションがスキャン不可と分類されることがあります。マルウェア スキャンの判定が SV_TIMEOUT や SV_ERROR の場合は、スキャン不可のトランザクションと見なされます。

ステップ 8　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

- マルウェアのカテゴリについて（13-17 ページ）

マルウェア対策およびレピュテーションの設定（適応型スキャンがディセーブルの場合）

ステップ 1　[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。

ステップ 2　設定するアクセス ポリシーの [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] リンクをクリックします。

ステップ 3　[Web レピュテーションとマルウェア対策の設定（Web Reputation and Anti-Malware Settings）] セクションで [Web レピュテーションとマルウェア対策のカスタム設定の定義（Define Web Reputation and Anti-Malware Custom Settings）] を選択します。

これにより、このアクセス ポリシーに対して、グローバル ポリシーとは異なる Web レピュテーションとマルウェア対策の設定を指定できます。

ステップ 4　[Web レピュテーション設定（Web Reputation Settings）] セクションで設定項目を設定します。

ステップ 5　[高度なマルウェア防御設定（Advanced Malware Protection Settings）] セクションで設定項目を設定します。

ステップ 6　[Cisco IronPort DVS マルウェア防御設定（Cisco IronPort DVS Anti-Malware Settings）] セクションまでスクロールします。

ステップ 7　必要に応じて、ポリシーのマルウェア対策設定を指定します。

（注）　Webroot、Sophos、または McAfee スキャンをイネーブルにすると、このページの [マルウェア カテゴリ（Malware Categories）] で、追加のカテゴリをモニタするかブロックするかを選択できます。

設定	説明
疑わしいユーザ エージェント スキャンを有効にする（Enable Suspect User Agent Scanning）	HTTP 要求ヘッダーで指定されているユーザ エージェント フィールドに基づいて、アプライアンスがトラフィックをスキャンできるようにするかどうかを選択します。 このチェックボックスをオンにした場合は、ページ下部の [追加スキャン（Additional Scanning）] セクションで、疑わしいユーザ エージェントをモニタするかブロックするかを選択できます。
Webroot を有効にする（Enable Webroot）	アプライアンスがトラフィックをスキャンする際に、Webroot スキャン エンジンを使用できるようにするかどうかを選択します。
Sophos または McAfee を有効にする（Enable Sophos or McAfee）	アプライアンスがトラフィックをスキャンする際に、Sophos または McAfee スキャン エンジンを使用できるようにするかどうかを選択します。
マルウェア カテゴリ（Malware Categories）	マルウェア スキャンの判定に基づいて各種のマルウェア カテゴリをモニタするかブロックするかを選択します。このセクションに表示されるカテゴリは、上記でイネーブルにするスキャン エンジンによって異なります。
その他カテゴリ（Other Categories）	このセクションに表示されたオブジェクトおよび応答のタイプを、モニタするかブロックするかを選択します。 （注）　設定された最大時間に達した場合や、システムで一時的エラーが発生した場合、URL トランザクションはスキャン不可と分類されます。たとえば、スキャン エンジンのアップデート時や AsyncOS のアップグレード時に、トランザクションがスキャン不可と分類されることがあります。マルウェア スキャンの判定が SV_TIMEOUT や SV_ERROR の場合は、スキャン不可のトランザクションと見なされます。

ステップ 8　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

- アクセス ポリシーの Web レピュテーション スコアのしきい値の設定（13-14 ページ）
- マルウェアのカテゴリについて（13-17 ページ）

Web レピュテーション スコアの設定

Web セキュリティ アプライアンスをインストールして設定すると、Web レピュテーション スコアのデフォルト設定が指定されます。ただし、Web レピュテーション スコアのしきい値の設定は組織のニーズに合わせて変更できます。各ポリシー グループに応じた Web レピュテーション フィルタを設定してください。

アクセス ポリシーの Web レピュテーション スコアのしきい値の設定

ステップ 1　[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。

ステップ 2　[マルウェア対策とレピュテーション（Anti-Malware and Reputation）] 列で、編集するアクセス ポリシー グループのリンクをクリックします。

ステップ 3　[Web レピュテーションとマルウェア対策の設定（Web Reputation and Anti-Malware Settings）] セクションで [Web レピュテーションとマルウェア対策のカスタム設定の定義（Define Web Reputation and Anti-Malware Custom Settings）] を選択します。

これにより、このアクセス ポリシーに対して、グローバル ポリシーとは異なる Web レピュテーションとマルウェア対策の設定を指定できます。

ステップ 4　[Web レピュテーション フィルタを有効にする（Enable Web Reputation Filtering）] フィールドがイネーブルになっていることを確認します。

ステップ 5　マーカーを動かして、URL のブロック、スキャン、許可の各アクションの範囲を変更します。

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）]）。

（注）　適応型スキャンがディセーブルの場合は、アクセス ポリシーの Web レピュテーション スコアのしきい値を編集できます。

復号化ポリシー グループの Web レピュテーション フィルタの設定

ステップ 1　[Web セキュリティ マネージャ（Web Security Manager）] > [復号化ポリシー（Decryption Policies）] を選択します。

ステップ 2　[Web レピュテーション（Web Reputation）] 列で、編集する復号化ポリシー グループのリンクをクリックします。

ステップ 3　[Web レピュテーション設定（Web Reputation Settings）] セクションで、[Web レピュテーションのカスタム設定の定義（Define Web Reputation Custom Settings）] を選択します。これにより、グローバル ポリシー グループによる Web レピュテーション設定を上書きすることができます。

ステップ 4　[Web レピュテーション フィルタを有効にする（Enable Web Reputation Filtering）] フィールドがオンになっていることを確認します。

ステップ 5　マーカーを動かして、URL のドロップ、復号化、およびパススルー アクションの範囲を変更します。

ステップ 6　[スコアを持たないサイト（Sites with No Score）] フィールドで、Web レピュテーション スコアが割り当てられていないサイトの要求に対して実行するアクションを選択します。

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）]）。

データ セキュリティ ポリシー グループの Web レピュテーション フィルタの設定

ステップ 1　[Web セキュリティ マネージャ（Web Security Manager）] > [Cisco IronPort データ セキュリティ（Cisco IronPort Data Security）] を選択します。

ステップ 2　[Web レピュテーション（Web Reputation）] 列で、編集するデータ セキュリティ ポリシー グループのリンクをクリックします。

ステップ 3　[Web レピュテーション設定（Web Reputation Settings）] セクションで、[Web レピュテーションのカスタム設定の定義（Define Web Reputation Custom Settings）] を選択します。

これにより、グローバル ポリシー グループによる Web レピュテーション設定を上書きすることができます。

ステップ 4　マーカーを動かして、URL のブロックおよびモニタ アクションの範囲を変更します。

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）]）。

（注）　Cisco IronPort データ セキュリティ ポリシーの Web レピュテーションのしきい値には、負またはゼロの値のみ設定できます。定義では、すべての正のスコアがモニタされます。

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（`https://update-manifests.ironport.com`）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 セキュリティ アプライアンス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。

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、次の 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

次のガイドラインは、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おそれがあるブラウザ 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。
既知の悪意のある高リスク 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。
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、次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ワードを探したりします。
ウィルス	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。

ファイル レピュテーション フィルタリングとファイル分析

ファイル レピュテーション フィルタリングとファイル分析の概要

高度なマルウェア防御機能はクラウド ベースのサービスを使用し、次の方法によってゼロデイや標的型のファイルベースの脅威から保護します。

- 各ファイルのレピュテーションを取得する。
- レピュテーションが不明なファイルの動作を分析する。
- ネットワークに侵入後に脅威であると判定されたファイルについてユーザに通知する。

これらの機能は、ファイルのダウンロードに対してのみ使用できます。アップロードされたファイルは評価されません。

ファイルの脅威判定のアップデート

脅威判定は、新たな情報に合わせて変更できます。当初ファイルが不明または正常と評価され、そのファイルへのアクセスが許可されることがあります。脅威判定が変更されると、アラートが表示され、ファイルとその新しい判定が [AMP 判定のアップデート（AMP Verdict Updates）] レポートに表示されます。脅威の影響を排除する第一歩として、ポイント オブ エントリのトランザクションを調査できます。

判定を、「悪意がある」から「正常」に変更できます。

アプライアンスが同じファイルの後続インスタンスを処理するときに、更新された結果がただちに適用されます。

関連項目

- ファイル レピュテーションおよびファイル分析のレポートとトラッキング（14-9 ページ）
- ファイルの脅威判定が変更された場合に実行する操作（14-12 ページ）

ファイル処理の概要

最初に、ファイルのダウンロード元の Web サイトが Web ベース レピュテーション サービス（WBRS）に対して評価されます。

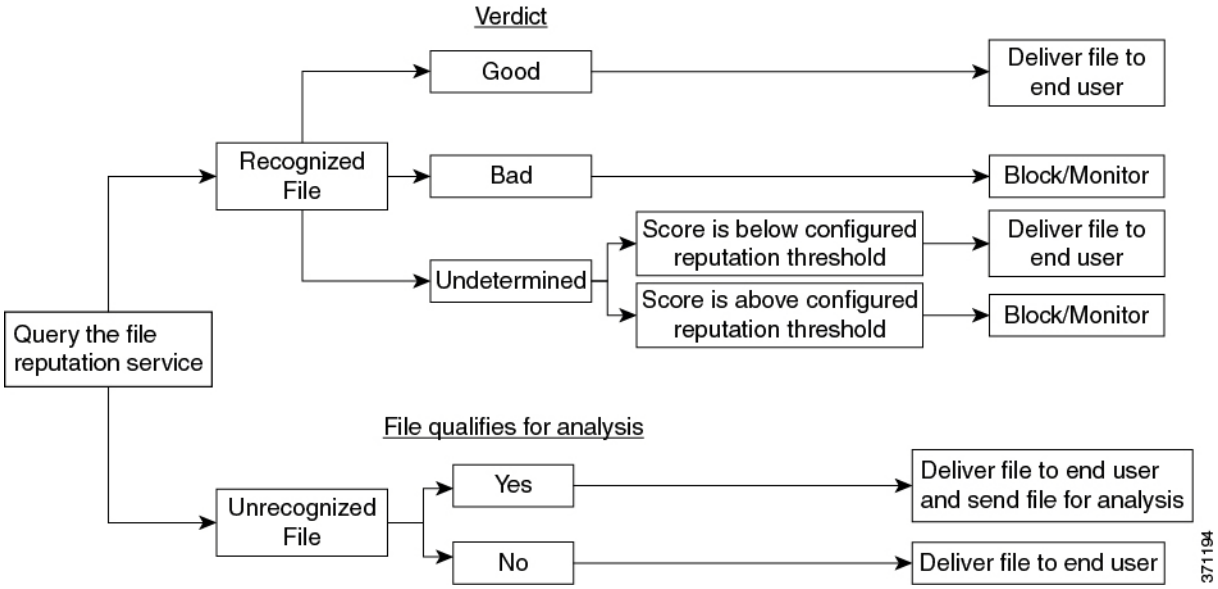
サイトの Web レピュテーション スコアが「スキャン」に設定される範囲内である場合、アプライアンスはマルウェアについてトランザクションをスキャンすると同時に、ファイルのレピュテーションについてクラウド ベース サービスに問い合わせます。（サイトのレピュテーション スコアが「ブロック」の範囲内である場合、トランザクションは適宜に処理され、ファイルをさらに処理する必要はありません）。スキャン中にマルウェアが検出された場合は、ファイル レピュテーションに関係なく、トランザクションがブロックされます。

[適応型スキャン（Adaptive Scanning）] もイネーブルになっている場合は、ファイル レピュテーションの評価とファイル分析が適応型スキャンに含まれます。

アプライアンスとファイル レピュテーション サービス間の通信は暗号化され、改ざんから保護されます。

ファイル レピュテーションの評価後：

- ファイルがファイル レピュテーション サービスにとって既知のものであり、正常と判定された場合、ファイルはエンド ユーザにリリースされます。
- ファイル レピュテーション サービスが「悪意がある」という判定を返した場合、アプライアンスは、そのようなファイルに対して指定されているアクションを適用します。
- ファイルがファイル レピュテーション サービスにとって既知のものであるが、最終判定のための情報が不足している場合、レピュテーション サービスは、脅威のフィンガープリントや動作分析など、ファイルの特性に基づいて脅威スコアを返します。このスコアが設定されているレピュテーションのしきい値（デフォルトのしきい値は変更しないでください）以上の場合、アプライアンスは、悪意のあるファイルや危険性の高いファイルに対してアクセス ポリシーで設定されているアクションを適用します。
- レピュテーション サービスにファイルに関する情報がなく、ファイルが分析の基準を満たしていない場合、ファイルは正常と見なされエンド ユーザにリリースされます。
- レピュテーション サービスにファイルに関する情報がなく、そのファイルが分析可能なファイルの基準を満たしている場合（評価および分析対象のファイル（14-3 ページ）を参照）、ファイルは正常と見なされ、状況に応じて分析用に送信されます。
- ファイル レピュテーション情報を使用できない場合（クラウド サービスとの接続がタイムアウトになった場合など）、ファイルは正常と見なされエンド ユーザにリリースされます。



ファイルが分析のために送信される場合:

- ファイルは SSL/TLSを使用して送信されます。
- 分析には通常、数分かかりますが、さらに時間がかかることもあります。
- 分析されたすべてのファイルに関する情報がレピュテーション データベースに追加されます。ファイル分析の結果はファイルのレピュテーションに影響します。

判別のアップデートの詳細については、ファイルの脅威判定のアップデート（14-1 ページ）を参照してください。

評価および分析対象のファイル

レピュテーション サービスは大部分のファイル タイプを評価します。ファイル タイプの識別はファイル コンテンツによって行われ、ファイル拡張子には依存していません。

レピュテーションが「不明」となっているファイルは脅威の特徴と対比して分析できます。ファイル分析機能を設定する際は、分析用に送信するファイル タイプを選択する必要があります。新しいタイプを動的に追加できます。アップロード可能なファイル タイプのリストが変更された場合はアラートを受け取るので、追加されたファイル タイプを選択してアップロードできます。

評価および分析対象のファイルの詳細については、使用している AsyncOS バージョンのリリース ノートを参照してください。リリース ノートは、http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-release-notes-list.html から入手できます。

関連項目

- ファイル レピュテーションおよび分析サービスの有効化と設定（14-6 ページ）
- アラートの受信の確認（14-8 ページ）
- アーカイブまたは圧縮ファイルの処理（14-4 ページ）

アーカイブまたは圧縮ファイルの処理

ファイルが圧縮またはアーカイブされている場合:

- 圧縮またはアーカイブ ファイルのレピュテーションが評価されます。
- 圧縮またはアーカイブ ファイルが圧縮解除され、すべての抽出されたファイルのレピュテーションが評価されます。

ファイル形式を含めて、検査対象となるアーカイブ ファイルや圧縮ファイルについて詳しくは、『*File Criteria for Advanced Malware Protection Services for Cisco Content Security Products*』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/email-security-appliance/products-user-guide-list.html から入手できます。

このシナリオでは、次のようになります。

- 抽出されたファイルのいずれかが悪意のあるファイルである場合、ファイル レピュテーション サービスは、その圧縮/アーカイブ ファイルに対して「悪意がある（Malicious）」という判定を返します。
- 圧縮/アーカイブ ファイルが悪意のあるファイルであり、抽出されたすべてのファイルが正常である場合、ファイル レピュテーション サービスは、圧縮/アーカイブ ファイルに対して「悪意がある（Malicious）」という判定を返します。
- 抽出されたファイルのいくつかの判定が「不明」である場合、それらの抽出ファイルは、状況に応じて、分析のために送信されます（そのように設定されており、ファイル タイプがファイル分析でサポートされている場合）。
- 圧縮/アーカイブ ファイルの圧縮解除中にファイルの抽出に失敗した場合、ファイル レピュテーション サービスは、圧縮/アーカイブ ファイルに対して「スキャン不可（Unscannable）」という判定を返します。ただし、抽出されたファイルの 1 つが悪意のあるファイルである場合、ファイル レピュテーション サービスは、圧縮/アーカイブ ファイルに対して「悪意がある（Malicious）」という判定を返します（「悪意がある（Malicious）」という判定は「スキャン不可（Unscannable）」よりも順位が高くなります）。

（注） セキュア MIME タイプの抽出ファイル（テキストやプレーン テキストなど）のレピュテーションは、評価されません。

FIPS の準拠性

ファイル レピュテーション スキャンおよびファイル分析は、FIPS に準拠しています。

ファイル レピュテーション機能と分析機能の設定

ファイル レピュテーション サービスおよび分析サービスと通信するための要件

- これらのサービスを使用するすべての Web セキュリティ アプライアンスは、インターネットに直接接続できなければなりません。
- デフォルトでは、ファイル レピュテーションおよび分析サービスとの通信は、アプライアンスの管理ポート（M1）経由でルーティングされます。アプライアンスが管理ポートを使用してデータをルーティングしていない場合は、ファイル レピュテーション サーバおよびファイル分析サーバへのデータ インターフェイスを介したトラフィックのルーティング（14-5 ページ）を参照してください。
- ファイル レピュテーションおよび分析のためのクラウド サービスとの通信は IPv4 を介して行われます。
- 次のファイアウォール ポートが開いている必要があります。

ファイアウォール ポート	説明	プロトコル	In/Out	ホスト名	アプライアンスのインターフェイス
32137（デフォルト）または 443	ファイル レピュテーションを取得するためにクラウド サービスにアクセスします。	TCP	発信（Out）	[セキュリティ サービス（Security Services）] > [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] の [詳細設定（Advanced）] セクションで、[クラウド サーバ プール（Cloud Server Pool）] パラメータに対して設定された名前。	データ ポートを介してこのトラフィックをルーティングするようにスタティック ルートが設定されていない場合は、管理インターフェイス。
443	ファイル分析のためにクラウド サービスにアクセスします。	TCP	発信（Out）	[セキュリティ サービス（Security Services）] > [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] の [詳細設定（Advanced）] セクションで設定された名前。	

- ファイル レピュテーション機能を設定する際は、ポート 443 で SSL を使用するかどうかを選択します。

関連項目

- ファイル レピュテーションおよび分析サービスの有効化と設定（14-6 ページ）

ファイル レピュテーション サーバおよびファイル分析サーバへのデータ インターフェイスを介したトラフィックのルーティング

（[ネットワーク（Network）] > [インターフェイス（Interfaces）] ページで）アプライアンスの管理ポートがアプライアンス管理サービス専用に設定されている場合は、代わりに、データ ポートを介してファイル レピュテーションおよび分析のトラフィックをルーティングするように、アプライアンスを設定します。

[ネットワーク（Network）] > [ルート（Routes）] ページでデータ トラフィックのルートを追加します。全般的な要件と手順については、TCP/IP トラフィック ルートの設定（2-20 ページ）を参照してください。

接続先	宛先ネットワーク	ゲートウェイ
ファイル レピュテーション サービス	[セキュリティ サービス（Security Services）] > [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] の [詳細設定（Advanced）] セクションで設定された、クラウド サーバ プールの IP アドレス。	データ ポートのゲートウェイの IP アドレス。
ファイル分析サービス	[セキュリティ サービス（Security Services）] > [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] の [詳細設定（Advanced）] セクションで設定された、ファイル分析サーバの IP アドレス。	データ ポートのゲートウェイの IP アドレス。

関連項目

- TCP/IP トラフィック ルートの設定（2-20 ページ）

ファイル レピュテーションおよび分析サービスの有効化と設定

はじめる前に

- ファイル レピュテーション サービスとファイル分析サービスの機能キーを取得します。
- ファイル レピュテーション サービスおよび分析サービスと通信するための要件（14-5 ページ）を満たします。
- ファイル レピュテーションおよび分析サービスにデータ ネットワーク インターフェイスを使用する場合は、アプライアンスでデータ ネットワーク インターフェイスがイネーブルになっていることを確認します。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（2-15 ページ）を参照してください。
- アップグレードおよびサービス アップデートの設定の変更（22-33 ページ）で設定したアップデート サーバへの接続を確認します。

手順

ステップ 1　[セキュリティ サービス（Security Services）] > [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] 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　[高度なマルウェア防御サービス（Advanced Malware Protection Services）] セクションで、[ファイル レピュテーション フィルタを有効にする（Enable File Reputation Filtering）] を選択します。

ステップ 4　ライセンス契約が表示された場合は、それに同意します。

ステップ 5　[高度なマルウェア防御サービス（Advanced Malware Protection Services）] セクションで、[ファイル分析を有効にする（Enable File Analysis）] を選択します。

ステップ 6　[ファイル分析（File Analysis）] セクションで、分析用にクラウドに送信するファイル タイプを選択します。

ステップ 7　[ファイル分析（File Analysis）] セクションで、分析用にクラウドに送信するファイル タイプを選択します。

ステップ 8　必要に応じて、次の詳細設定を行います。

オプション	説明
ファイル レピュテーション用の SSL 通信（SSL Communication for File Reputation）	デフォルト ポート（32137）ではなく ポート 443 で通信するには、[SSL（ポート 443）の使用（Use SSL (Port 443)）] をオンにします。 このオプションを使用すると、ファイル レピュテーション サービスとの通信用にアップストリーム プロキシを設定できます。 **（注）**　ポート 32137 で SSL 通信を行うには、ファイアウォールでこのポートを開く必要があります。
着信サービス一覧（Routing Table）	高度なマルウェア防御サービスで使用されるルーティング テーブル。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）に関連付けられています。アプライアンスで管理インターフェイスと 1 つ以上のデータ インターフェイスがイネーブルになっている場合は、[管理（Management）] または [データ（Data）] を選択できます。
レピュテーションしきい値（Reputation Threshold） • クラウド サービスの値を使用（Use value from Cloud Service） • カスタム値の入力（Enter custom value）	許容されるファイル レピュテーション スコアの上限。スコアがこのしきい値を超えた場合は、ファイルが感染していることを示しています。

（注）　シスコのサポートのガイダンスなしに、その他の詳細設定を変更しないでください。

ステップ 9　変更を送信し、保存します。

アクセス ポリシーごとのファイル レピュテーションおよび分析サービスのアクションの設定

手順

ステップ 1　[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。

ステップ 2　テーブルの [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] 列にあるポリシーのリンクをクリックします。

ステップ 3　[高度なマルウェア防御設定（Advanced Malware Protection Settings）] セクションで、[ファイル レピュテーション フィルタリングとファイル分析を有効にする（Enable File Reputation Filtering and File Analysis）] を選択します。

ファイル分析がグローバルにイネーブルになっていない場合は、ファイル レピュテーション フィルタリングだけが表示されます。

ステップ 4　[悪意のある既知の高リスク ファイル（Known Malicious and High-Risk Files）] に対してアクション（[モニタ（Monitor）] または [ブロック（Block）]）を選択します。

デフォルトは [モニタ（Monitor）] です。

ステップ 5　変更を送信し、保存します。

アラートの受信の確認

高度なマルウェア防御に関連するアラートを送信するようにアプライアンスが設定されていることを確認します。

次の場合にアラートを受信します。

アラートの説明	タイプ	重大度
機能キーが期限切れになった	（すべての機能に対する標準）	
ファイル レピュテーションまたはファイル分析サービスに到達できない	マルウェア対策（Anti-Malware）	警告
クラウド サービスとの通信が確立された	マルウェア対策（Anti-Malware）	情報（Info）
ファイル レピュテーションの判定が変更された	マルウェア対策（Anti-Malware）	情報（Info）
分析用に送信できるファイル タイプが変更された。新しいファイル タイプのアップロードをイネーブルにできる。	マルウェア対策（Anti-Malware）	情報（Info）
一部のファイル タイプの分析を一時的に利用できない	マルウェア対策（Anti-Malware）	警告
サポートされているすべてのファイル タイプの分析が一時停止後に復旧する	マルウェア対策（Anti-Malware）	情報（Info）

関連項目

- ファイル レピュテーション サーバまたは分析サーバへの接続の失敗に関するアラート（14-13 ページ）
- ファイルの脅威判定が変更された場合に実行する操作（14-12 ページ）

高度なマルウェア防御機能の集約管理レポートの設定

セキュリティ管理アプライアンスでレポートを集約管理する場合は、使用している管理アプライアンスのオンライン ヘルプまたはユーザ ガイドを参照し、Web レポーティングの章の「高度なマルウェア防御」に関する項で重要な設定要件を確認してください。

ファイル レピュテーションおよびファイル分析のレポートとトラッキング

SHA-256 ハッシュによるファイルの識別

ファイル名は簡単に変更できるため、アプライアンスはセキュア ハッシュ アルゴリズム（SHA-256）を使用して、各ファイルの ID を生成します。アプライアンスが名前の異なる同じファイルを処理する場合、すべてのインスタンスが同じ SHA-256 として認識されます。複数のアプライアンスが同じファイルを処理する場合、ファイルのすべてのインスタンスには同じ SHA-256 ID があります。

ほとんどのレポートでは、ファイルがその SHA-256 値（短縮形式）別に表示されます。組織のマルウェア インスタンスに関連付けられたファイル名を特定するには、[レポート（Reporting）] > [高度なマルウェア防御（Advanced Malware Protection）] を選択し、テーブルの SHA-256 リンクをクリックします。関連付けられたファイル名が詳細ページに表示されます。

[ファイルレピュテーション（File Reputation）] および [ファイル分析（File Analysis）] レポート ページ

レポート	説明
高度なマルウェア防御（Advanced Malware Protection）	ファイル レピュテーション サービスによって特定されたファイル ベースの脅威を示します。 各 SHA にアクセスしようとしたユーザ、およびその SHA-256 に関連付けられたファイル名を表示するには、テーブルの SHA-256 リンクをクリックします。 [マルウェア脅威ファイルの詳細（Malware Threat File Details）] レポート ページの下部にあるリンクをクリックすると、レポート用に選択された時間範囲に関係なく使用可能な最大時間範囲内に検出された、Web トラッキング内のファイルのすべてのインスタンスが表示されます。 判定が変更されたファイルについては、[AMP判定のアップデート（AMP Verdict Updates）] レポートを参照してください。これらの判定は、[高度なマルウェア防御（Advanced Malware Protection）] レポートに反映されません。 **（注）** 圧縮/アーカイブ ファイルから抽出したファイルの 1 つが悪意のあるファイルである場合は、圧縮/アーカイブ ファイルの SHA 値だけが [高度なマルウェア防御（Advanced Malware Protection）] レポートに含まれます。
ファイル分析（File Analysis）	分析用に送信された各ファイルの時間と判定（または中間判定）を表示します。 1000 を超えるファイル分析結果を表示するには、データを .csv ファイルとしてエクスポートします。 ドリル ダウンすると、各ファイルの脅威の特性およびスコアを含む詳細な分析結果が表示されます。 SHA の追加情報についてクラウド サービスを検索することもできます。リンクは結果の詳細ページにあります。 **（注）** 圧縮/アーカイブ ファイルから抽出したファイルが分析用に送信される場合は、それらの抽出ファイルの SHA 値だけが [ファイル分析（File Analysis）] レポートに含まれます。

レポート	説明
AMP判定のアップデート（AMP Verdict Updates）	このアプライアンスで処理され、トランザクションの処理後に判定が変わったファイルの一覧を示します。この状況の詳細については、ファイルの脅威判定のアップデート（14-1 ページ）を参照してください。 1000 を超える判定アップデートを表示するには、データを .csv ファイルとしてエクスポートします。 1 つの SHA-256 に対して判定が複数回変わった場合は、判定履歴ではなく最新の判定のみがこのレポートに表示されます。 SHA-256 リンクをクリックすると、レポート用に選択された時間範囲に関係なく使用可能な最大時間範囲内にこの SHA-256 が含まれた、すべてのトランザクションの Web トラッキング結果が表示されます。 特定の SHA-256 について、（レポートに対して選択した時間範囲に関係なく）使用可能な最大時間範囲内の影響を受けたすべてのトランザクションを表示するには、[マルウェアの脅威ファイル（Malware Threat Files）] ページの下部にあるリンクをクリックします。

他のレポートのファイル レピュテーション フィルタリング データの表示

該当する場合は、ファイル レピュテーションおよびファイル分析のデータを他のレポートでも使用できます。レポートによっては、[高度なマルウェア防御でブロック（Blocked by Advanced Malware Protection）] カラムがデフォルトで非表示になっている場合があります。追加カラムを表示するには、テーブルの下の [列（Columns）] リンクをクリックします。

[ユーザの場所別のレポート（Report by User Location）] に [高度なマルウェア防御（Advanced Malware Protection）] タブが含まれています。

Web トラッキング機能および高度なマルウェア防御機能について

Web トラッキングでファイルの脅威情報を検索する場合は、次の点に注意してください。

- ファイル レピュテーション サービスで検出された悪意のあるファイルを検索するには、Web トラッキングの [詳細設定（Advanced）] セクションにある [マルウェアの脅威（Malware Threat）] 領域で、[マルウェアカテゴリ別フィルタ（Filter by Malware Category）] オプションの [悪意のある既知の高リスクファイル（Known Malicious and High-Risk Files）] を選択します。
- Web トラッキングには、ファイル レピュテーション処理についての情報と、トランザクションが処理されたときに返された元のファイル レピュテーションの判定のみが含まれます。たとえば最初にファイルがクリーンであると判断され、その後、判定のアップデートでそのファイルが悪質であると判断された場合、クリーンの判定のみがトラッキング結果に表示されます。

  検索結果の [ブロック - AMP（Block - AMP）] は、ファイルのレピュテーション判定が原因でトランザクションがブロックされたことを意味します。

  トラッキングの詳細に表示される [AMP脅威スコア（AMP Threat Score）] は、ファイルを明確に判定できないときにクラウド レピュテーション サービスが提示するベスト エフォート型のスコアです。この場合のスコアは 1 ～ 100 です（AMP 判定が返された場合、またはスコアがゼロの場合は [AMP脅威スコア（AMP Threat Score）] を無視してください）。アプライアンスはこのスコアをしきい値スコア（[セキュリティサービス（Security Services）] > [マル

ウェア対策とレピュテーション（Anti-Malware and Reputation）] ページで設定）と比較して、実行するアクションを決定します。デフォルトでは、スコアが 60 ～ 100 の場合に悪意のあるファイルと見なされます。デフォルトのしきい値スコアを変更することはお勧めしません。WBRS スコアはファイルのダウンロード元となったサイトのレピュテーションです。このスコアはファイル レピュテーションとは関係ありません。

- 判定のアップデートは [AMP判定のアップデート（AMP Verdict Updates）] レポートでのみ使用できます。Web トラッキングの元のトランザクションの詳細は、判定が変更されても更新されません。特定のファイルに関連するトランザクションを表示するには、判定のアップデート レポートで SHA-256 をクリックします。
- 分析結果や分析用にファイルが送信済みかどうかといった、ファイル分析に関する情報は [ファイル分析（File Analysis）] レポートにのみ表示されます。

  分析済みファイルのその他の情報は、クラウドから入手できます。ファイルの使用可能なファイル分析情報を表示するには、[レポート（Reporting）] > [ファイル分析（File Analysis）] を選択して、ファイルを検索する SHA-256 を入力するか、Web トラッキングの詳細で SHA-256 リンクをクリックします。ファイル分析サービスによってソースのファイルが分析されると、その詳細を表示できます。分析されたファイルの結果だけが表示されます。

  分析用に送信されたファイルの後続インスタンスをアプライアンスが処理すると、そのインスタンスは Web トラッキングの検索結果に表示されるようになります。

ファイルの脅威判定が変更された場合に実行する操作

手順

ステップ 1　[AMP 判定のアップデート（AMP Verdict updates）] レポートを表示します。

ステップ 2　該当する SHA-256 リンクをクリックし、エンド ユーザがアクセスを許可されていたファイルに関連するすべてのトランザクションの Webトラッキング データを表示します。

ステップ 3　トラッキング データを使用して、侵害された可能性があるユーザ、漏えいに関連する情報（ファイル名など）、およびファイルのダウンロード元の Web サイトを特定します。

ステップ 4　ファイルの脅威の動作を詳細に把握するために、[ファイル分析（File Analysis）] レポートを検証して、この SHA-256 が分析用に送信されたかどうかを確認します。

関連項目

- ファイルの脅威判定のアップデート（14-1 ページ）

ファイル レピュテーションおよび分析のトラブルシューティング

- ログ ファイル（14-13 ページ）
- ファイル レピュテーション サーバまたは分析サーバへの接続の失敗に関するアラート（14-13 ページ）

ログ ファイル

ログの説明:

- AMP と amp は、ファイル レピュテーション サービスまたはエンジンを示しています。
- Retrospective は判定のアップデートを示しています。
- VRT と sandboxing はファイル分析サービスを示しています。

高度なマルウェア防御情報は、アクセス ログまたは AMP エンジン ログに記録されます。詳細については、ログによるシステム アクティビティのモニタリングに関する章を参照してください。

ファイル レピュテーション サーバまたは分析サーバへの接続の失敗に関するアラート

問題　ファイル レピュテーション サービスまたは分析サービスへの接続の失敗に関するアラートをいくつか受信した。(単一のアラートは一時的な問題のみを示していることがあります)。

ソリューション

- ファイル レピュテーション サービスおよび分析サービスと通信するための要件(14-5 ページ)に記載されている要件を満たしていることを確認します。
- アプライアンスとクラウド サービスとの通信を妨げている可能性があるネットワークの問題を確認します。
- [クエリー タイムアウト(Query Timeout)] の値を大きくします。

  [セキュリティ サービス(Security Services)] > [マルウェア対策とレピュテーション(Anti-Malware and Reputation)] を選択します。[クエリー タイムアウト(Query Timeout)] の値は、[高度なマルウェア防御サービス(Advanced Malware Protection Services)] セクションの [Advanced(詳細設定)] 領域にあります。

Web アプリケーションへのアクセスの管理

Web アプリケーションへのアクセスの管理：概要

Application Visibility and Control（AVC）エンジンを使用すると、各アプリケーションの基盤技術を完全に理解していなくても、ネットワーク上のアプリケーション アクティビティを制御するポリシーを作成できます。アクセス ポリシー グループのアプリケーション制御を設定できます。個々に、またはアプリケーションのタイプに応じて、アプリケーションをブロックまたは許可することができます。また、特定のアプリケーション タイプに制御を適用できます。

アクセス ポリシーを使用して、次の操作を実行できます。

- アプリケーション動作を制御する
- 特定のアプリケーション タイプで使用される帯域幅の量を制御する
- アプリケーションがブロックされたときにエンドユーザに通知する
- インスタント メッセージ、ブログ、ソーシャル メディアのアプリケーションに制御を割り当てる

AVC エンジンを使用してアプリケーションを制御するには、次のタスクを実行します。

タスク	タスクへのリンク
AVC エンジンをイネーブルにする	AVC エンジンのイネーブル化（15-2 ページ）
アクセス ポリシー グループに制御を設定する	アクセス ポリシー グループのアプリケーション制御の設定（15-4 ページ）
アプリケーション タイプが消費する帯域幅を制限して輻輳を制御する	帯域幅の制御（15-5 ページ）
インスタント メッセージ トラフィックを許可し、インスタント メッセンジャによるファイル共有を禁止する	インスタント メッセージ トラフィックの制御（15-8 ページ）

AVC エンジンのイネーブル化

をイネーブルにする場合は、AVC エンジン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）] > [使用許可コントロール（Acceptable Use Controls）] を選択します。

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

ステップ 3　がオンになっていることを確認します。

ステップ 4　[使用許可コントロール サービス（Acceptable Use Controls Service）] パネルで、**Cisco Web Usage Controls** を選択し、次に [アプリケーションの表示およびコントロールを有効にする（Enable Application Visibility and Control）] を選択します。

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）]）。

（注）　[レポート（Reporting）] > [アプリケーションの表示（Application Visibility）] ページの [アプリケーションの表示（Application Visibility）] レポートで、AVC エンジンのスキャン アクティビティを確認できます。

関連項目

- AVC エンジンのアップデーとデフォルト アクション（15-2 ページ）
- 要求がブロックされた場合のユーザ エクスペリエンス（15-3 ページ）

AVC エンジンのアップデーとデフォルト アクション

AsyncOS は定期的にアップデート サーバに問い合わせて、AVC エンジンを含めたすべてのセキュリティ サービス コンポーネントについて新しいアップデートの有無を確認します。AVC エンジンのアップデートには、新しいアプリケーション タイプやアプリケーションに対するサポートが含まれることがあります。また、アプリケーションの動作が変更された場合は、既存のアプリケーションに対するサポートも更新されます。AsyncOS バージョンの更新に合わせて AVC エンジンを更新することによって、サーバをアップグレードすることなく、Web セキュリティ アプライアンスの柔軟性が保たれます。

AsyncOS for Web は、グローバル アクセス ポリシーに次のデフォルト アクションを割り当てます。

- 新しいアプリケーション タイプのデフォルト アクションは、[モニタ（Monitor）] です。
- 特定アプリケーション内でのファイル転送のブロックなど、新しいアプリケーション動作のデフォルト アクションは、[モニタ（Monitor）] です。
- 既存のアプリケーション タイプの新しいアプリケーションのデフォルト アクションは、そのアプリケーション タイプのデフォルト アクションです。

（注）　グローバル アクセス ポリシーでは、各アプリケーション タイプのデフォルト アクションを設定できます。これによって、AVC エンジンの更新により導入された新しいアプリケーションは、指定されたデフォルト アクションを自動的に継承します。アクセス ポリシー グループのアプリケーション制御の設定（15-4 ページ）を参照してください。

要求がブロックされた場合のユーザ エクスペリエンス

AVC エンジンによってトランザクションがブロックされると、Web プロキシはエンド ユーザにブロック ページを送信します。ただし、すべての Web サイトでブロック ページが表示されるわけではありません。多くの Web サイトでは、静的 Web ページの代わりに JavaScript を使用して動的コンテンツが表示され、ブロック ページが表示されることはありません。そのような場合でも、ユーザは適切にブロックされているので悪意のあるデータをダウンロードすることはありませんが、ブロックされていることが Web サイトから通知されない場合もあります。

アプリケーション制御のポリシー設定

アプリケーションを制御するには、次の要素を設定する必要があります。

オプション	説明
アプリケーション タイプ（Application Types）	1 つまたは複数のアプリケーションを含むカテゴリ。
アプリケーション	あるアプリケーション タイプに属している特定のアプリケーション。
アプリケーション動作（Application behaviors）	管理者が制御できるアプリケーション内でユーザが実行できる特定のアクションまたは動作。すべてのアプリケーションに設定可能な動作が含まれているわけではありません。

アクセス ポリシー グループのアプリケーション制御を設定できます。[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）] ページで、設定するポリシー グループの [アプリケーション（Applications）] リンクをクリックします。アプリケーションの設定時には、次のアクションを選択できます。

オプション	説明
ブロック	このアクションは、最終アクションです。ユーザには Web ページが表示されなくなり、代わりにエンド ユーザ通知ページが表示されます。
モニタ（Monitor）	このアクションは、中間アクションです。Web プロキシは引き続きトランザクションを他の制御設定と比較して、適用する最終アクション決定します。
制限（Restrict）	このアクションは、アプリケーションの動作がブロックされることを示します。たとえば、特定のインスタント メッセージ アプリケーションのファイル転送をブロックすると、そのアプリケーションのアクションは制限されます。
帯域幅制限（Bandwidth Limit）	Media や Facebook などの特定のアプリケーションに対して、Web トラフィックで使用可能な帯域幅を制限できます。アプリケーション自体やそのアプリケーション ユーザの帯域幅を制限できます。

関連項目

- ルールとガイドライン（15-4 ページ）

ルールとガイドライン

アプリケーション制御を設定する際は、次のルールとガイドラインを考慮してください。

- サポートされるアプリケーション タイプ、アプリケーション、およびアプリケーション動作は、AsyncOS for Web のアップグレード間で、または AVC エンジンのアップデート後に変化する可能性があります。
- [アプリケーション タイプ（Application Type）] リストでは、各アプリケーション タイプの要約にアプリケーションの最終アクションが一覧表示されますが、それらのアクションがグローバル ポリシーから継承されたものか、現在のアクセス ポリシーで設定されたものかについては示されません。特定のアプリケーションのアクションについて詳細を調べるには、そのアプリケーション タイプを展開します。
- グローバル アクセス ポリシーでは、各アプリケーション タイプのデフォルト アクションを設定できます。これによって、AVC エンジンの更新により導入された新しいアプリケーションは、デフォルト アクションを自動的に継承します。
- [参照（Browse）] ビューでアプリケーション タイプの [すべてを編集（edit all）] リンクをクリックすると、そのアプリケーション タイプに属するすべてのアプリケーションに同じアクションを簡単に設定できます。ただし、設定できるのは、アプリケーション動作のアクションではなく、アプリケーションのアクションだけです。アプリケーション動作を設定するには、アプリケーションを個別に編集する必要があります。
- [検索（Search）] ビューでは、テーブルをアクション列でソートすると、テーブルが最終アクションに基づいて並べ替えられます。たとえば、[グローバル（ブロック）を使用（Use Global (Block)）] が [ブロック（Block）] の後に配置されます。
- 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。

関連項目

- アクセス ポリシー グループのアプリケーション制御の設定（15-4 ページ）
- 全体的帯域幅制限の設定（15-6 ページ）
- AVC アクティビティの表示（15-8 ページ）

アクセス ポリシー グループのアプリケーション制御の設定

ステップ 1　[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。

ステップ 2　ポリシー テーブルで、編集するポリシー グループの [アプリケーション（Applications）] 列にあるリンクをクリックします。

ステップ 3　グローバル アクセス ポリシーを設定する場合：

a.　[アプリケーション タイプのデフォルト アクション（Default Actions for Application Types）] セクションで、各アプリケーション タイプのデフォルト アクションを定義します。

b.　ページの [アプリケーション設定を編集（Edit Applications Settings）] セクションで、各アプリケーション タイプの各メンバーのデフォルト アクションを一括して、または個々に編集できます。個々のアプリケーションのデフォルト アクションを編集する手順は、以下で説明されています。

ステップ 4　ユーザ定義のアクセス ポリシーを設定する場合は、[アプリケーション設定を編集（Edit Applications Settings）] セクションで [アプリケーションのカスタム設定を定義（Define Applications Custom Settings）] を選択します。

ステップ 5　[アプリケーションの設定（Application Settings）] 領域で、ドロップダウン メニューから [参照ビュー（Browse view）] または [検索ビュー（Search view）] を選択します。

- **[参照ビュー（Browse view）]。** アプリケーション タイプを参照できます。[参照ビュー（Browse view）] を使用して、特定タイプのすべてのアプリケーションを同時に設定できます。[参照ビュー（Browse view）] でアプリケーション タイプが折りたたまれている場合は、アプリケーション タイプの要約にアプリケーションの最終アクションが一覧表示されます。ただし、それらのアクションがグローバル ポリシーから継承されたものか、現在のアクセス ポリシーで設定されたものかについては示されません。
- **[検索ビュー（Search view）]。** 名前によってアプリケーションを検索できます。すべてのアプリケーションのリストが長く、特定のアプリケーションをすばやく見つけて設定する必要がある場合は、[検索ビュー（Search view）] を使用します。

ステップ 6　各アプリケーションとアプリケーション動作のアクションを設定します。

ステップ 7　該当する各アプリケーションの帯域幅制御を設定します。

ステップ 8　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

- 帯域幅の制御（15-5 ページ）

帯域幅の制御

全体の制限とユーザの制限の両方をトランザクションに適用した場合は、最も制限の厳しいオプションが適用されます。URL カテゴリの ID グループを定義し、帯域幅を制限するアクセス ポリシーでそのグループを使用することによって、特定の URL カテゴリの帯域幅制限を定義できます。

次の帯域幅制限を定義できます。

帯域幅制限	説明	リンク先タスク
全体（Overall）	サポートされるアプリケーション タイプに対して、ネットワーク上の全ユーザ向けの全体的制限を定義します。全体的な帯域幅制限は、Web セキュリティ アプライアンスと Web サーバ間のトラフィックに影響を与えます。Web キャッシュからのトラフィックは制限されません。	全体的帯域幅制限の設定（15-6 ページ）
ユーザ（User）	アプリケーション タイプごとに、ネットワーク上の特定ユーザに対する制限を定義します。ユーザの帯域幅制限は、Web サーバからのトラフィックだけでなく、Web キャッシュからのトラフィックも制限します。	ユーザの帯域幅制限の設定（15-6 ページ）

（注）　帯域幅制限を定義しても、ユーザへのデータ転送が遅れるだけです。クォータに達したかどうかに基づいてデータがブロックされるわけではありません。Web プロキシによって各アプリケーションのトランザクションに遅延が生じ、サーバへのリンクが減速したように見えます。

全体的帯域幅制限の設定

ステップ 1　[Web セキュリティ マネージャ（Web Security Manager）] > [全体の帯域幅制限（Overall Bandwidth Limits）] を選択します。

ステップ 2　[設定を編集（Edit Settings）] をクリックします。

ステップ 3　[制限値（Limit to）] オプションを選択します。

ステップ 4　メガビット/秒（Mbps）またはキロビット/秒（kbps）単位で、制限するトラフィック量を入力します。

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）]）。

ユーザの帯域幅制限の設定

ユーザの帯域幅制限を定義するには、アクセス ポリシーの Applications Visibility and Control ページで帯域幅制御を設定します。アクセス ポリシーで、ユーザに対して次のタイプの帯域幅制御を定義できます。

オプション	説明	タスクへのリンク
アプリケーション タイプのデフォルトの帯域幅制限（Default bandwidth limit for an application type）	グローバル アクセス ポリシーでは、あるアプリケーション タイプに属するすべてのアプリケーションに対してデフォルトの帯域幅制限を定義できます。	アプリケーション タイプのデフォルトの帯域幅制限の設定（15-7 ページ）
アプリケーション タイプの帯域幅制限（Bandwidth limit for an application type）	ユーザ定義のアクセス ポリシーでは、グローバル アクセス ポリシーで定義されたアプリケーション タイプのデフォルトの帯域幅制限を無効にすることができます。	アプリケーション タイプのデフォルトの帯域幅制限の無効化（15-7 ページ）
アプリケーションの帯域幅制限（Bandwidth limit for an application）	ユーザ定義のアクセス ポリシーまたはグローバル アクセス ポリシーで、アプリケーション タイプの帯域幅制限を適用するか、制限しないか（アプリケーション タイプの制限を免除）を選択できます。	アプリケーションの帯域幅制御の設定（15-7 ページ）

アプリケーション タイプのデフォルトの帯域幅制限の設定

ステップ 1　[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。

ステップ 2　ポリシー テーブルで、グローバル アクセス ポリシーの [アプリケーション（Applications）] 列にあるリンクをクリックします。

ステップ 3　[アプリケーション タイプのデフォルト アクション（Default Actions for Application Types）] セクションで、編集するアプリケーション タイプの [帯域幅制限（Bandwidth Limit）] の横にあるリンクをクリックします。

ステップ 4　[帯域幅制限を設定（Set Bandwidth Limit）] を選択し、制限するトラフィック量を、メガビット/秒（Mbps）またはキロビット/秒（kbps）単位で入力します。

ステップ 5　[適用（Apply）] 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）]）。

アプリケーション タイプのデフォルトの帯域幅制限の無効化

ユーザ定義のアクセス ポリシーでは、グローバル アクセス ポリシー グループで定義されたデフォルトの帯域幅制限を無効にすることができます。これは [参照ビュー（Browse view）] でのみ実行できます。

ステップ 1　[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。

ステップ 2　ポリシー テーブルで、編集するユーザ定義ポリシー グループの [アプリケーション（Applications）] 列にあるリンクをクリックします。

ステップ 3　[アプリケーション設定を編集（Edit Applications Settings）] セクションで [アプリケーションのカスタム設定を定義（Define Applications Custom Settings）] を選択します。

ステップ 4　編集するアプリケーション タイプの [帯域幅制限（Bandwidth Limit）] の横にあるリンクをクリックします。

ステップ 5　別の帯域幅制限値を選択するには、[帯域幅制限を設定（Set Bandwidth Limit）] を選択し、制限するトラフィック量を、メガビット/秒（Mbps）またはキロビット/秒（kbps）単位で入力します。帯域幅制限を指定しない場合は、[アプリケーション タイプに対する帯域幅制限なし（No Bandwidth Limit for Application Type）] を選択します。

ステップ 6　[適用（Apply）] をクリックします。

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）]）。

アプリケーションの帯域幅制御の設定

ステップ 1　[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。

ステップ 2　ポリシー テーブルで、編集するポリシー グループの [アプリケーション（Applications）] 列にあるリンクをクリックします。

ステップ 3　定義するアプリケーションが含まれているアプリケーション タイプを展開します。

ステップ 4　設定するアプリケーションのリンクをクリックします。

ステップ 5　[モニタ（Monitor）] を選択し、次に、アプリケーション タイプに対して定義されている帯域幅制限を使用するか、制限しないかを選択します。

（注）　帯域幅制限の設定は、アプリケーションがブロックされている場合や、アプリケーション タイプに対して帯域幅制限が定義されていない場合は適用できません。

ステップ 6　[完了（Done）] をクリックします。

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）]）。

インスタント メッセージ トラフィックの制御

IM トラフィックのブロックやモニタを実行したり、IM サービスによっては、IM セッションの特定のアクティビティ（アプリケーション動作）をブロックすることもできます。

ステップ 1　[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。

ステップ 2　ポリシー テーブルで、編集するポリシー グループの [アプリケーション（Applications）] 列にあるリンクをクリックします。

ステップ 3　[アプリケーションのカスタム設定を定義（Define Applications Custom Settings）] を選択します。

ステップ 4　[インスタント メッセージ（Instant Messaging）] アプリケーション タイプを展開します。

ステップ 5　設定する IM アプリケーションの横にあるリンクをクリックします。

ステップ 6　この IM アプリケーションのすべてのトラフィックをブロックするには、[ブロック（Block）] を選択します。

ステップ 7　IM アプリケーションをモニタしながら、アプリケーション内の特定のアクティビティをブロックするには、[モニタ（Monitor）] を選択してから、アプリケーション動作として [ブロック（Block）] を選択します。

ステップ 8　[完了（Done）] をクリックします。

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）]）。

AVC アクティビティの表示

[レポート（Reporting）] > [アプリケーションの表示（Application Visibility）] ページには、使用される上位のアプリケーションとアプリケーション タイプに関する情報が表示されます。また、ブロックされている上位のアプリケーションとアプリケーション タイプも表示されます。

アクセス ログ ファイル

アクセス ログ ファイルには、トランザクションごとに Application Visibility and Control エンジンから返された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、次のようなフィールドがあります。

説明	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
アプリケーション名	%XO	x-avc-app
アプリケーション タイプ（Application Type）	%Xu	x-avc-type
アプリケーション動作	%Xb	x-avc-behavior

機密データの漏洩防止

機密データの漏洩防止の概要

Web セキュリティ アプライアンスは次の機能によってデータの安全を確保します。

オプション	説明
Cisco IronPort データ セキュリティ フィルタ	Web セキュリティ アプライアンスの Cisco IronPort データ セキュリティ フィルタは、HTTP、HTTPS、FTP を介してネットワークから発信されるデータを評価します。
サードパーティ製データ漏洩防止（DLP）の統合。	Web セキュリティ アプライアンスは、機密データを識別して保護する代表的なサードパーティ製コンテンツ対応 DLP システムを統合します。Web プロキシは Internet Content Adaptation Protocol（ICAP）を使用して、プロキシ サーバが外部システムにコンテンツ スキャンをオフロードできるようにします。

アップロード要求を受信すると、Web プロキシは要求をデータ セキュリティ ポリシー グループや外部 DLP ポリシー グループと比較して、適用するポリシー グループを決定します。両方のタイプのポリシーが設定されている場合は、外部 DLP ポリシーと比較する前に、Cisco IronPort データ セキュリティ ポリシーと要求を比較します。ポリシー グループに要求を割り当てた後、ポリシー グループの設定済み制御設定と要求を比較し、要求に対して実行するアクションを決定します。アップロード要求を処理するためのアプライアンスの設定方法は、ポリシー グループのタイプによって異なります。

（注）　サイズがゼロ（0）バイトのファイルのアップロードを試みているアップロード要求は、Cisco IronPort データ セキュリティ ポリシーまたは外部 DLP ポリシーに対して評価されません。

ネットワークから発信されるデータを制限したり制御するには、次のタスクを実行します。

タスク	タスクへのリンク
Cisco IronPort データ セキュリティ ポリシーを作成する	アップロード要求の管理（13-2 ページ）
外部 DLP ポリシーを作成する	外部 DLP システムにおけるアップロード要求の管理（13-3 ページ）
データ セキュリティ ポリシーおよび外部 DLP ポリシーを作成する	データ セキュリティ ポリシーおよび外部 DLP ポリシーの作成（16-5 ページ）
Cisco IronPort データ セキュリティ ポリシーを使用してアップロード要求を制御する	アップロード要求の設定の管理（13-7 ページ）
外部 DLP ポリシーを使用してアップロード要求を制御する	外部 DLP ポリシーによるアップロード要求の制御（13-11 ページ）

最小サイズ以下のアップロード要求のバイパス

ログ ファイルに記録されるアップロード要求の数を減らすために、最小要求サイズを定義できます。このサイズを下回る場合、アップロード要求は Cisco IronPort データセキュリティ フィルタや外部 DLP サーバによってスキャンされません。

これを実行するには、次の CLI コマンドを使用します。

- **datasecurityconfig**。Cisco IronPort データ セキュリティ フィルタに適用します。
- **externaldlpconfig**。設定済みの外部 DLP サーバに適用します。

デフォルトでは、どちらの CLI コマンドでも要求本文の最小サイズは 4 KB（4096 バイト）です。有効な値は 1 ～ 64 KB です。指定したサイズは、アップロード要求の本文全体のサイズに適用されます。

（注）　すべてのチャンク エンコードされたアップロードとすべてのネイティブ FTP トランザクションは、Cisco IronPort データ セキュリティ フィルタまたは外部 DLP サーバによってスキャンされます（イネーブルの場合）。ただし、カスタム URL カテゴリに基づいてこれらをバイパスできます。

要求がブロックされた場合のユーザ エクスペリエンス

Cisco IronPort データセキュリティ フィルタや外部 DLP サーバは、アップロード要求をブロックするときに、Web プロキシがエンド ユーザに送信するブロック ページを提供します。すべての Web サイトでエンド ユーザにブロック ページが表示されるわけではありません。たとえば、Web 2.0 Web サイトでは、静的 Web ページの代わりに JavaScript を使用して動的コンテンツが表示され、ブロック ページが表示されることはありません。そのような場合でも、データ セキュリティ違反が発生しないようにユーザは適切にブロックされていますが、そのことが Web サイトから通知されない場合もあります。

アップロード要求の管理

はじめる前に

- [セキュリティ サービス（Security Services）] > [データ セキュリティ フィルタ（Data Security Filters）] に移動し、Cisco IronPort データ セキュリティ フィルタをイネーブルにします。

ステップ 1　**データ セキュリティ ポリシー グループを作成して設定します。**Cisco IronPort データセキュリティ ポリシーは、アップロード要求を評価する際に、URL フィルタリング、Web レピュテーション、およびアップロード コンテンツ情報を使用します。これらのセキュリティ コンポーネントを個々に設定し、アップロード要求をブロックするかどうかを決定します。

Web プロキシはアップロード要求を制御設定と比較する際に、順番に設定を評価します。各制御設定は、Cisco IronPort データ セキュリティ ポリシーの次のアクションのいずれかを実行するように設定できます。

操作	説明
ブロック	Web プロキシは、接続を許可せず、ブロックの理由を説明するエンド ユーザ通知ページを表示します。
許可（Allow）	Web プロキシは、データ セキュリティ ポリシーの残りのセキュリティ サービス スキャンをバイパスし、最終アクションを実行する前にアクセス ポリシーに対して要求を評価します。 Cisco IronPort データ セキュリティ ポリシーでは、残りのデータ セキュリティ スキャンをバイパスできますが、外部 DLP やアクセス ポリシーのスキャンはバイパスしません。Web プロキシが要求に対して実行する最終アクションは、該当するアクセス ポリシー（または要求をブロック可能性のある、該当する外部 DLP ポリシー）によって決まります。
モニタ（Monitor）	Web プロキシは、トランザクションと他のデータ セキュリティ ポリシー グループの制御設定との比較を続行し、トランザクションをブロックするか、またはアクセス ポリシーに対して評価するかを決定します。

Cisco IronPort データ セキュリティ ポリシーの場合、Web プロキシがクライアント要求に対して実行する最終アクションは「ブロック」アクションだけです。「モニタ」および「許可」アクションは中間アクションです。いずれの場合も、Web プロキシは、トランザクションを外部 DLP ポリシー（設定されている場合）およびアクセス ポリシーに対して評価します。Web プロキシは、アクセス ポリシー グループの制御設定（または、要求をブロックする可能性のある該当する外部 DLP ポリシー）に基づいて適用する最終アクションを決定します。

関連項目

- 外部 DLP システムにおけるアップロード要求の管理（13-3 ページ）
- アップロード要求の設定の管理（16-8 ページ）

外部 DLP システムにおけるアップロード要求の管理

外部 DLP システムでアップロード要求を処理するように Web セキュリティ アプライアンスを設定するには、次のタスクを実行します。

ステップ 1　[ネットワーク（Network）] > [外部 DLP サーバ（External DLP Servers）] を選択します。外部 DLP システムを定義します。スキャンのためにアップロード要求を外部 DLP システムに渡すには、少なくとも 1 つの ICAP 準拠 DLP システムを Web セキュリティ アプライアンスで定義する必要があります。

ステップ 2　**外部 DLP ポリシー グループを作成して設定します。**外部 DLP システムを定義したら、外部 DLP ポリシー グループを作成して設定し、スキャンのために DLP システムに送信するアップロード要求を決定します。

ステップ 3　アップロード要求が外部 DLP ポリシーに一致した場合、Web プロキシは、Internet Content Adaptation Protocol（ICAP）を使用して、スキャンのためにアップロード要求を DLP システムに送信します。DLP システムは、要求本文のコンテンツをスキャンし、Web プロキシにブロックまたは許可の判定を返します。許可の判定は、アップロード要求がアクセス ポリシーと比較される Cisco IronPort データ セキュリティ ポリシーの許可アクションに似ています。Web プロキシが要求に対して実行する最終アクションは、適用されるアクセス ポリシーによって決まります。

関連項目

- 外部 DLP ポリシーによるアップロード要求の制御（16-11 ページ）
- 外部 DLP システムの定義（16-9 ページ）

データ セキュリティおよび外部 DLP ポリシー グループのメンバーシップの評価

各クライアント要求に ID が割り当てられ、次に、それらの要求が他のポリシー タイプと照合して評価され、タイプごとに要求が属するポリシー グループが判定されます。Web プロキシは、データ セキュリティおよび外部 DLP ポリシーに対して*アップロード要求*を評価します。Web プロキシは、クライアント要求のポリシー グループ メンバーシップに基づいて、設定されているポリシー制御設定をクライアント要求に適用します。

クライアント要求とデータ セキュリティおよび外部 DLP ポリシー グループとの照合

クライアント要求と一致するポリシー グループを判定するために、Web プロキシは、特定のプロセスを実行してグループ メンバーシップの基準と照合します。グループ メンバーシップの次の要素が考慮されます。

- **ID。**各クライアント要求は、ID に一致するか、認証に失敗するか、ゲスト アクセスが許可されるか、または認証に失敗して終了します。

- **権限を持つユーザ。**割り当てられた ID が認証を必要とする場合は、そのユーザがデータ セキュリティまたは外部 DLP ポリシー グループの承認済みユーザのリストに含まれており、ポリシー グループに一致している必要があります。承認済みユーザのリストには、任意のグループまたはユーザを指定でき、ID がゲスト アクセスを許可している場合はゲスト ユーザを指定できます。
- **高度なオプション。**データ セキュリティおよび外部 DLP ポリシー グループのメンバーシップに対して複数の詳細オプションを設定できます。一部のオプション（プロキシ ポート、URL カテゴリなど）は、ID 内に定義することもできます。ID 内に詳細オプションを設定する場合、データ セキュリティまたは外部 DLP ポリシー グループ レベルでは設定できません。

この項では、Web プロキシがアップロード要求をデータ セキュリティおよび外部 DLP の両方のポリシー グループと照合する方法について概要を説明します。

Web プロキシは、ポリシー テーブルの各ポリシー グループを順番に読み取ります。次に、アップロード要求のステータスを最初のポリシー グループのメンバーシップ基準と比較します。一致した場合、Web プロキシは、そのポリシー グループのポリシー設定を適用します。

一致しない場合は、その次のポリシー グループとアップロード要求を比較します。アップロード要求をユーザ定義のポリシー グループと照合するまで、Web プロキシはこのプロセスを続行します。ユーザ定義のポリシー グループに一致しない場合は、グローバル ポリシー グループと照合します。Web プロキシは、アップロード要求をポリシー グループまたはグローバル ポリシー グループと照合するときに、そのポリシー グループのポリシー設定を適用します。

データ セキュリティ ポリシーおよび外部 DLP ポリシーの作成

宛先サイトの URL カテゴリや 1 つ以上の ID など、複数の条件の組み合わせに基づいてデータ セキュリティおよび外部 DLP ポリシー グループを作成できます。ポリシー グループのメンバーシップには、少なくとも 1 つの条件を定義する必要があります。複数の条件が定義されている場合、アップロード要求がポリシー グループと一致するには、すべての条件を満たしていなければなりません。ただし、アップロード要求は設定された ID の 1 つとのみ一致する必要があります。

ステップ 1　[Web セキュリティ マネージャ（Web Security Manager）] > [Cisco IronPort データ セキュリティ（Cisco IronPort Data Security）]（データ セキュリティ ポリシーのグループ メンバーシップを定義する場合）、または [Web セキュリティ マネージャ（Web Security Manager）] > [外部データ漏洩防止（External Data Loss Prevention）]（外部 DLP ポリシーのグループ メンバーシップを定義する場合）を選択します。

ステップ 2　[ポリシーを追加（Add Policy）] をクリックします。

ステップ 3　[ポリシー名（Policy Name）] フィールドにポリシー グループの名前を入力し、[説明（Description）] フィールドに説明を追加します。

（注）　各ポリシー グループ名は、英数字またはスペース文字のみを含む、一意の名前とする必要があります。

ステップ 4　[上記ポリシーを挿入（Insert Above Policy）] フィールドで、ポリシー テーブル内でポリシー グループを配置する場所を選択します。

複数のポリシー グループを設定する場合は、各グループに論理的な順序を指定します。ポリシー グループが正しく照合されるように順序を指定してください。

ステップ 5　[アイデンティティとユーザ（Identities and Users）] セクションで、このグループ ポリシーに適用する 1 つ以上の ID グループを選択します。

ステップ 6　（任意）[詳細（Advanced）] セクションを拡張して、追加のメンバーシップ要件を定義します。

ステップ 7　いずれかの拡張オプションを使用してポリシー グループのメンバーシップを定義するには、拡張オプションのリンクをクリックし、表示されるページでオプションを設定します。

高度なオプション	説明
プロトコル（Protocols）	クライアント要求で使用されるプロトコルによってポリシー グループのメンバーシップを定義するかどうかを選択します。含めるプロトコルを選択します。 [その他のすべて（All others）] は、このオプションの上に一覧表示されていないプロトコルを意味します。 **（注）** HTTPS プロキシをイネーブルにすると、復号化ポリシーのみが HTTPS トランザクションに適用されます。アクセス、ルーティング、発信マルウェア スキャン（Outbound Malware Scanning）、データ セキュリティ、外部 DLP のポリシーの場合は、HTTPS プロトコルによってポリシー メンバーシップを定義できません。
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プロキシ ポートで、ポリシー グループ メンバーシップを定義するかどうかを選択します。[プロキシ ポート（Proxy Ports）] フィールドに、1 つ以上のポート番号を入力します。複数のポートを指定する場合は、カンマで区切ります。 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。トランスペアレント接続の場合は、宛先ポートと同じです。あるポート上に要求を明示的に転送するように設定されたクライアントのセットがあり、別のポート上に要求を明示的に転送するように設定された別のクライアントのセットがある場合、プロキシ ポート上でポリシー グループのメンバーシップを定義することがあります。 シスコでは、アプライアンスが明示的な転送モードで配置されている場合、またはクライアントがアプライアンスに要求を明示的に転送する場合にだけ、プロキシ ポートでポリシー グループのメンバーシップを定義することを推奨します。クライアント要求がアプライアンスに透過的にリダイレクトされるときにプロキシ ポートでポリシー グループのメンバーシップを定義すると、一部の要求が拒否される場合があります。 **（注）** このポリシー グループに関連付けられている ID が、この詳細設定によって ID メンバーシップを定義している場合、非 ID ポリシー グループ レベルではこの設定項目を設定できません。
サブネット（Subnets）	サブネットまたは他のアドレスでポリシー グループのメンバーシップを定義するかどうかを選択します。 関連付けられた ID で定義できるアドレスを使用するか、または特定のアドレスをここに入力できます。 **（注）** ポリシー グループに関連付けられている ID がアドレスによってグループのメンバーシップを定義している場合は、ID で定義されているアドレスのサブセットであるアドレスを、このポリシー グループに入力する必要があります。ポリシー グループにアドレスを追加することにより、このグループ ポリシーに一致するトランザクションのリストを絞り込めます。

高度なオプション	説明
URL カテゴリ（URL Categories）	URL カテゴリでポリシー グループのメンバーシップを定義するかどうかを選択します。ユーザ定義または定義済みの URL カテゴリを選択します。 **（注）** このポリシー グループに関連付けられている ID が、この詳細設定によって ID メンバーシップを定義している場合、非 ID ポリシー グループ レベルではこの設定項目を設定できません。
ユーザ エージェント（User Agents）	クライアント要求で使用されるユーザ エージェントによってポリシー グループのメンバーシップを定義するかどうかを選択します。一般的に定義されているブラウザを選択するか、正規表現を使用して独自のブラウザを定義できます。このポリシー グループを、選択したユーザ エージェントに適用するか、または選択したユーザ エージェントのリストに含まれていないユーザ エージェントに適用するかどうかを選択します。 **（注）** このポリシー グループに関連付けられている ID が、この詳細設定によって ID メンバーシップを定義している場合、非 ID ポリシー グループ レベルではこの設定項目を設定できません。
ユーザの場所（User Location）	ユーザのリモートまたはローカルの場所でポリシー グループのメンバーシップを定義するかどうかを選択します。 このオプションは、Secure Mobility がイネーブルの場合にのみ表示されます。

ステップ 8　変更を送信します。

ステップ 9　データ セキュリティ ポリシー グループを作成する場合は、その制御設定を設定して、Web プロキシがアップロード要求を処理する方法を定義します。

新しいデータ セキュリティ ポリシー グループは、各制御設定のオプションが設定されるまで、グローバル ポリシー グループの設定を自動的に継承します。

外部 DLP ポリシー グループを作成する場合は、その制御設定を設定して、Web プロキシがアップロード要求を処理する方法を定義します。

新しい外部 DLP ポリシー グループは、カスタム設定が設定されるまで、グローバル ポリシー グループの設定を自動的に継承します。

ステップ 10　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

- データ セキュリティおよび外部 DLP ポリシー グループのメンバーシップの評価（16-4 ページ）
- クライアント要求とデータ セキュリティおよび外部 DLP ポリシー グループとの照合（16-4 ページ）
- アップロード要求の設定の管理（16-8 ページ）
- 外部 DLP ポリシーによるアップロード要求の制御（16-11 ページ）

アップロード要求の設定の管理

各アップロード要求は、データ セキュリティ ポリシー グループに割り当てられ、そのポリシー グループの制御設定を継承します。データ セキュリティ ポリシー グループの制御設定によって、アプライアンスが接続をブロックするか、またはアクセス ポリシーに対して接続を評価するかが決まります。

[Web セキュリティ マネージャ（Web Security Manager）] > [Cisco IronPort Data Security] ページで、データ セキュリティ ポリシー グループの制御設定を設定します。

次の設定項目を設定して、アップロード要求で実行するアクションを決定できます。

オプション	リンク
URL Categories	URL カテゴリ（13-8 ページ）
Web レピュテーション	Web レピュテーション（13-8 ページ）
目次	コンテンツ ブロッキング（13-8 ページ）

データ セキュリティ ポリシー グループがアップロード要求に割り当てられた後、ポリシー グループの制御設定が評価され、要求をブロックするかアクセス ポリシーに対して評価するかが決定されます。

URL カテゴリ

AsyncOS for Web では、アプライアンスが特定の要求の URL カテゴリに基づいてトランザクションを処理する方法を設定できます。定義済みのカテゴリ リストを使用して、カテゴリ別にコンテンツをモニタするかブロックするかを選択できます。カスタム URL カテゴリを作成し、カスタム カテゴリの Web サイトに対してトラフィックを許可、モニタ、またはブロックするかを選択することもできます。

Web レピュテーション

Web レピュテーションの設定はグローバル設定を継承します。特定のポリシー グループ用に Web レピュテーション フィルタリングをカスタマイズするには、[Web レピュテーション設定（Web Reputation Settings）] プルダウン メニューを使用して Web レピュテーション スコアのしきい値をカスタマイズします。

Cisco IronPort データ セキュリティ ポリシーの Web レピュテーションのしきい値には、負またはゼロの値のみ設定できます。定義では、すべての正のスコアがモニタされます。

コンテンツのブロック

[Cisco IronPort データ セキュリティ ポリシー（Cisco IronPort Data Security Policies）] > [コンテンツ（Content）] ページの設定項目を使用し、Web プロキシが次のファイル特性に基づいてデータのアップロードをブロックするように設定できます。

- **[ファイルサイズ（File size）]。** 許容される最大アップロード サイズを指定できます。指定した最大値以上のサイズのアップロードはすべてブロックされます。HTTP/HTTPS およびネイティブ FTP 要求に対して異なる最大ファイル サイズを指定できます。

アップロード要求サイズが最大アップロード サイズと最大スキャン サイズ（[セキュリティ サービス（Security Services）] > [マルウェア対策（Anti-Malware）] ページの [DVS エンジン オブジェクト スキャンの制限（DVS Engine Object Scanning Limits）] フィールドで設定）のどちらよりも大きい場合、アップロード要求はブロックされますが、ファイル名とコンテンツ タイプはデータ セキュリティ ログに記録されません。アクセス ログのエントリは変更されません。

- **[ファイル タイプ（File type）]。** 定義済みのファイル タイプまたは入力したカスタム MIME タイプをブロックできます。定義済みファイル タイプをブロックする場合は、そのタイプのすべてのファイルまたは指定したサイズよりも大きいファイルをブロックできます。ファイル タイプをサイズによってブロックする場合は、最大ファイル サイズとして、[セキュリティ サービス（Security Services）] > [マルウェア対策（Anti-Malware）] ページの [DVS エンジン オブジェクト スキャンの制限（DVS Engine Object Scanning Limits）] フィールドの値と同じ値を指定できます。デフォルトでは、この値は 32 MB です。

  Cisco IronPort データ セキュリティ フィルタは、ファイル タイプによってブロックする場合にアーカイブ ファイルのコンテンツを検査しません。アーカイブ ファイルは、ファイル タイプまたはファイル名によってブロックできます。コンテンツによってブロックすることはできません。

（注）　一部の MIME タイプのグループでは、1 つのタイプをブロックすると、グループ内のすべての MIME タイプがブロックされます。たとえば、application/x-java-applet をブロックすると、application/java や application/javascript など、すべての MIME タイプがブロックされます。

- **[ファイル名（File name）]。** 指定した名前のファイルをブロックできます。ブロックするファイル名を指定する場合、リテラル文字列または正規表現をテキストとして使用できます。

（注）　8 ビット ASCII 文字のファイル名のみを入力してください。Web プロキシは、8 ビット ASCII 文字のファイル名のみを照合します。

外部 DLP システムの定義

Web セキュリティ アプライアンスでは、アプライアンスに複数の DLP サーバを定義することにより、同じベンダーの複数の外部 DLP サーバを統合できます。Web プロキシが DLP システムを接続する際に使用するロード バランシング技術を定義できます。これは、複数の DLP システムを定義する場合に役立ちます。

（注）　外部 DLP サーバが Web プロキシによって変更されたコンテンツを送信しないことを確認します。AsyncOS for Web は、アップロード要求をブロックまたは許可する機能のみをサポートします。外部 DLP サーバによって変更されたコンテンツのアップロードはサポートしません。

外部 DLP サーバの設定

ステップ 1　[ネットワーク（Network）] > [外部 DLP サーバ（External DLP Servers）] 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。

設定	説明
外部 DLP サーバ（External DLP Servers）	次の情報を入力して、ICAP 準拠 DLP システムにアクセスします。 • [サーバ アドレス（Server address）] と [ポート（Port）]：DLP システムにアクセスするホスト名/IP アドレスと TCP ポート。 • [再接続の試行（Reconnection attempts）]：失敗するまでに Web プロキシが DLP システムへの接続を試行する回数。 • [DLP サービスの URL（DLP Service URL）]：特定の DLP サーバに固有の ICAP クエリー URL。Web プロキシは、ここに入力された情報を外部 DLP サーバに送信する ICAP 要求に含めます。URL は、ICAP プロトコル「icap://」から始める必要があります。
ロード バランシング（Load Balancing）	複数の DLP サーバを定義する場合は、Web プロキシがさまざまな DLP サーバにアップロード要求を分散する際に使用するロード バランシング技術を選択します。次のロード バランシング技術を選択できます。 • **[なし（フェールオーバー）（None(failover）]。** Web プロキシは、1 つの DLP サーバにアップロード要求を送信します。一覧表示されている順序で DLP サーバへの接続を試みます。ある DLP サーバに到達できない場合、Web プロキシはリストの次のサーバへの接続を試みます。 • **[最少接続（Fewest connections）]。** Web プロキシは、各 DLP サーバが扱ってい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 DLP サーバにアップロード要求を送信します。 • **[ハッシュ ベース（Hash based）]。** Web プロキシは、ハッシュ関数を使用して、DLP サーバに要求を分散します。ハッシュ関数はプロキシ ID と URL を入力として使用し、同じ URL の要求が常に同じ DLP サーバに送信されるようにします。 • **[ラウンド ロビン（Round robin）]。** Web プロキシは、リストされた順序ですべての DLP サーバ間にアップロード要求を均等に分散します。
サービス要求タイムアウト（Service Request Timeout）	Web プロキシが DLP サーバからの応答を待機する時間を入力します。この時間が経過すると、ICAP 要求は失敗し、[失敗のハンドリング（Failure Handling）] の設定に応じて、アップロード要求はブロックまたは許可されます。 デフォルトは 60 秒です。
最大同時接続数（Maximum Simultaneous Connections）	Web セキュリティ アプライアンスから設定されている各外部 DLP サーバへの同時 ICAP 要求接続の最大数を指定します。このページの [失敗のハンドリング（Failure Handling）] 設定は、この制限を超えるすべての要求に適用されます。 デフォルトは 25 です。

設定	説明
失敗のハンドリング（Failure Handling）	DLP サーバがタイムリーに応答できなかった場合に、アップロード要求をブロックするか許可するか（評価のためにアクセス ポリシーに渡されるか）を選択します。 デフォルトは、許可（[すべてのデータ転送をスキャンなしで許可する（Permit all data transfers to proceed without scanning）]）です。

ステップ 3　（任意）[行を追加（Add Row）] をクリックし、表示される新しいフィールドに DLP サーバ情報を入力することによって、別の DLP サーバを追加できます。

ステップ 4　[テスト開始（Start Test）] をクリックして、Web セキュリティ アプライアンスと定義済み外部 DLP サーバ間の接続をテストできます。

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）]）。

外部 DLP ポリシーによるアップロード要求の制御

Web プロキシがアップロード要求ヘッダーを受信すると、スキャンのために要求を外部 DLP システムに送信する必要があるかどうかを決定するために必要な情報が提供されます。DLP システムは要求をスキャンし、Web プロキシに判定（ブロックまたはモニタ）を返します（要求はアクセス ポリシーに対して評価されます）。

ステップ 1　[Web セキュリティ マネージャ（Web Security Manager）] > [外部データ漏洩防止（External Data Loss Prevention）] を選択します。

ステップ 2　[接続先（Destinations）] 列で、設定するポリシー グループのリンクをクリックします。

ステップ 3　[接続先設定の編集（Edit Destination Settings section）] セクションで、[接続先スキャンのカスタム設定の定義（Define Destinations Scanning Custom Settings）] を選択します。

ステップ 4　[スキャンする接続先（Destination to Scan）] セクションで、次のオプションのいずれかを選択します。

- **[どのアップロードもスキャンしない（Do not scan any uploads）]。**アップロード要求は、スキャンのために設定済み DLP システムに送信されません。すべてのアップロード要求がアクセス ポリシーに対して評価されます。
- **[すべてのアップロードをスキャンする（Scan all uploads）]** すべてのアップロード要求は、スキャンのために設定済み DLP システムに送信されます。アップロード要求は、DLP システムのスキャン判定に応じて、ブロックされるか、アクセス ポリシーに対して評価されます。
- **[指定したカスタム URL カテゴリへのアップロードのみをスキャン（Scan uploads to specified custom URL categories only）]。**特定のカスタム URL カテゴリに分類されるアップロードが、スキャンのために設定済み DLP システムに送信されます。アップロード要求は、DLP システムのスキャン判定に応じて、ブロックされるか、アクセス ポリシーに対して評価されます。[カスタム カテゴリ リストを編集（Edit custom categories list）] をクリックして、スキャンする URL カテゴリを選択します。

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）]）。

ロギング

アクセス ログは、アップロード要求が Cisco IronPort データ セキュリティ フィルタまたは外部 DLP サーバのいずれかによってスキャン済みかどうかを示します。アクセス ログ エントリには、Cisco IronPort データ セキュリティ ポリシーのスキャン判定用のフィールド、および外部 DLP スキャン判定に基づく別のフィールドが含まれています。

アクセス ログに加えて、Web セキュリティ アプライアンスには、Cisco IronPort データ セキュリティ ポリシーや外部 DLP ポリシーをトラブルシューティングするための次のようなログ ファイルが用意されています。

- **データ セキュリティ ログ。**Cisco IronPort データ セキュリティ フィルタによって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。
- **データ セキュリティ モジュール ログ。**Cisco IronPort データ セキュリティ フィルタに関連するメッセージを記録します。
- **デフォルト プロキシ ログ。**Web プロキシに関連するエラーの記録に加えて、デフォルト プロキシ ログには外部 DLP サーバへの接続に関連するメッセージが含まれています。これにより、外部 DLP サーバとの接続や統合に関する問題をトラブルシューティングできます。

次のテキストは、データ セキュリティ ログのエントリのサンプルを示しています。

```
Mon Mar 30 03:02:13 2009 Info: 303 10.1.1.1 - -
<<bar,text/plain,5120><foo,text/plain,5120>>
BLOCK_WEBCAT_IDS-allowall-DefaultGroup-DefaultGroup-NONE-DefaultRouting ns server.com nc
```

フィールド値	説明
`Mon Mar 30 03:02:13 2009 Info:`	タイムスタンプおよびトレース レベル
`303`	トランザクション ID
`10.1.1.1`	ソース IP アドレス
`-`	ユーザ名（User name）
`-`	承認されたグループ名。
`<<bar,text/plain,5120><foo,text/plain,5120>>`	一度にアップロードされる各ファイルのファイル名、ファイル タイプ、ファイル サイズ **（注）** このフィールドには、設定されている最小の要求本文サイズ（デフォルトは 4096 バイト）よりも小さいテキスト/プレーン ファイルは含まれません。
`BLOCK_WEBCAT_IDS-allowall-DefaultGroup-DefaultGroup-NONE-DefaultRouting`	Cisco IronPort データ セキュリティ ポリシーおよびアクション
`ns`	Web レピュテーション スコア
`server.com`	発信 URL
`nc`	URL カテゴリ

（注） サイトへのデータ転送（POST 要求など）がいつ外部 DLP サーバによってブロックされたかを確認するには、アクセス ログの DLP サーバの IP アドレスまたはホスト名を検索します。

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

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。これらのページは、エンド ユーザ通知ページと呼ばれます。

次のタイプの通知ページおよび設定を設定できます。

オプション	説明	解説場所
一般通知設定。	HTTP および FTP の両方のオンボックス エンドユーザ通知ページで使用する言語を設定できます。HTTP 要求のオンボックス エンドユーザ通知ページに使用するロゴを設定することもできます。	通知ページの一般設定項目の設定（17-4 ページ）。
オンボックス エンドユーザ通知ページ。	URL 要求をブロックした理由に応じて、カスタマイズ可能な定義済み通知ページが表示されます。	オンボックス エンドユーザ通知ページの設定（17-5 ページ）。 オンボックス エンドユーザ通知ページの編集（17-5 ページ）

オプション	説明	解説場所
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。Web プロキシには、リダイレクトされた URL にブロックの理由を示すパラメータが含まれています。これにより、リダイレクトされた URL のサーバは表示するページをカスタマイズできます。	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（17-10 ページ）。
エンドユーザ確認ページ。	Web アクティビティのフィルタリングやモニタリングが行われていることをユーザに通知するように、Web プロキシを設定できます。エンド ユーザ確認ページは、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の設定（17-13 ページ）
エンドユーザ URL フィルタリング警告ページ。	組織が許可する利用規定をサイトが満たしていないことをユーザに警告し、ユーザが選択した場合は続行を許可するように、Web プロキシを設定できます。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。	エンド ユーザ URL フィルタリング警告ページの設定（17-14 ページ）
FTP 通知メッセージ。	FTP プロキシは、ネイティブ FTP トランザクションをブロックする理由に応じて、さまざまな定義済みの通知メッセージを表示します。カスタム メッセージを使用して、これらのページをカスタマイズできます。	FTP 通知メッセージの設定（17-14 ページ）。

通知のベスト プラクティス

オンボックス エンドユーザ通知ページの編集

- 個々のカスタマイズしたオンボックス エンドユーザ通知ページ 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、通知ページでサポートされる HTML タグ（17-15 ページ）を参照してください。
- カスタマイズしたオンボックス エンドユーザ通知ページ ファイルの名前は、Web セキュリティ アプライアンス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。
- 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。

- 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。
- カスタマイズした新しいオンボックス エンドユーザ通知ページを有効にするには、まずカスタマイズしたファイルをアプライアンスにアップロードし、`advancedproxyconfig > EUN` CLI コマンドを使用して、カスタマイズしたファイルをイネーブルにします。

通知ページのカスタム URL の入力:

- 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）] フィールドに次の URL を入力したときに、

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

次のアクセス 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、次のリダイレクト 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=-
```

エンドユーザの確認ページのイネーブル化

- 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 を使用したユーザの追跡は動作しません。
- アプライアンスが明示的な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。

一般通知設定

通知ページの一般設定について

次の一般的な設定を設定できます。

- **言語。**HTTP および FTP エンド ユーザ通知ページの言語を設定できます。HTTP の言語設定は、すべての HTTP 通知ページ（確認、オンボックス エンド ユーザ、カスタマイズしたエンド ユーザ、およびエンド ユーザ URL フィルタリング警告）に適用され、FTP の言語はすべての FTP 通知メッセージに適用されます。
- **ロゴ。**HTTP エンド ユーザ通知ページ専用のロゴを設定できます。ロゴの設定は、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。

通知ページの一般設定項目の設定

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 HTTP 通知ペ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 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。

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

- カスタム テキストおよびロゴ：認証、およびエンド ユーザ確認ページ（17-16 ページ）

オンボックス エンドユーザ通知ページ

イネーブルの場合、Web プロキシは、元のページをブロックした理由に応じて異なるページを表示します。各ページは組織に固有なものにカスタマイズできます。

オンボックス エンドユーザ通知ページの設定

はじめる前に

- 通知ページでサポートされる HTML タグ（17-15 ページ）を確認してください。

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 をシスコにレポートできます。不審なマルウェアや 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、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）　エンドユーザ通知ページを編集した場合、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）]）。

オンボックス エンドユーザ通知ページの編集

各オンボックス エンドユーザ通知ページは、Web セキュリティ アプライアンスに HTML ファイルとして保存されます。これらの HTML ページのコンテンツを編集して、追加のテキストを組み込んだり、各ページの全体的なルック アンド フィールを編集したりできます。

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。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、カスタマイズしたオンボックス エンドユーザ通知ページでの変数の使用（17-8 ページ）を参照してください。

次の表は、カスタマイズしたエンド ユーザ通知ページに組み込むことができる変数を示しています。

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	[いいえ(No)]
%A	ARP アドレス	[はい(Yes)]
%b	ユーザエージェント名	[いいえ(No)]
%B	ブロックした理由(BLOCK-SRC または BLOCK-TYPE など)	[いいえ(No)]
%c	エラー ページの担当者	[はい(Yes)]
%C	Set-Cookie: ヘッダー行全体、または空の文字列	[いいえ(No)]
%d	クライアント IP アドレス	[はい(Yes)]
%D	ユーザ名(User name)	[いいえ(No)]
%e	エラー ページの電子メール アドレス	[はい(Yes)]
%E	エラー ページのロゴの URL	[いいえ(No)]
%f	ユーザ フィードバック セクション	[いいえ(No)]
%F	ユーザ フィードバックの URL	[いいえ(No)]
%g	Web カテゴリ名(使用可能な場合)	[はい(Yes)]
%G	許可された最大ファイル サイズ(MB 単位)	[いいえ(No)]
%h	プロキシのホスト名	[はい(Yes)]
%H	URL のサーバ名	[はい(Yes)]
%i	トランザクション ID(16 進数値)	[はい(Yes)]
%I	管理 IP アドレス(Management IP Address)	[はい(Yes)]
%j	URL カテゴリ警告ページのカスタム テキスト	[いいえ(No)]
%k	エンドユーザ確認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	[いいえ(No)]
%K	レスポンス ファイル タイプ	[いいえ(No)]
%l	WWW-Authenticate: ヘッダー行	[いいえ(No)]
%L	Proxy-Authenticate: ヘッダー行	[いいえ(No)]
%M	要求方式(「GET」、「POST」など)	[はい(Yes)]
%n	マルウェア カテゴリ名(使用可能な場合)	[いいえ(No)]
%N	マルウェア脅威名(使用可能な場合)	[いいえ(No)]
%o	Web レピュテーションの脅威タイプ(使用可能な場合)	[いいえ(No)]
%O	Web レピュテーションの脅威の理由(使用可能な場合)	[いいえ(No)]
%p	Proxy-Connection HTTP ヘッダーの文字列	[はい(Yes)]
%P	プロトコル	[はい(Yes)]
%q	ID ポリシー グループの名前。	[はい(Yes)]
%Q	非 ID ポリシーのポリシー グループ名	[はい(Yes)]
%r	リダイレクト URL	[いいえ(No)]

変数	説明	条件変数として使用する場合、常に TRUE に評価
%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。	[いいえ（No）]
%S	プロキシの署名	No。常に FALSE に評価
%t	UNIX のタイムスタンプ（秒 + ミリ秒）	[はい（Yes）]
%T	日付	[はい（Yes）]
%u	URI の一部を構成する URL（サーバ名を除く URL）	[はい（Yes）]
%U	要求の完全な URL	[はい（Yes）]
%v	HTTP プロトコルのバージョン	[はい（Yes）]
%W	管理 WebUI ポート	[はい（Yes）]
%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。	[はい（Yes）]
%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	[いいえ（No）]
%y	エンド ユーザ確認ページのカスタム テキスト	[はい（Yes）]
%z	Web レピュテーション スコア	[はい（Yes）]
%Z	DLP メタデータ	[はい（Yes）]
%%	通知ページにパーセント記号（%）を出力します	該当なし

オンボックス エンドユーザ通知ページを編集するには、次の手順を実行します。

ステップ 1　FTP クライアントを使用して、Web セキュリティ アプライアンスに接続します。

ステップ 2　`configuration\eun` ディレクトリに移動します。

ステップ 3　編集するオンボックス エンドユーザ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、オンボックス エンドユーザ通知ページの各 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 セキュリティ アプライアンスに接続します。

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。

（注）　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する必要があります。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 9　変更を保存し、SSH クライアントを閉じます。

カスタマイズしたオンボックス エンドユーザ通知ページでの変数の使用

オンボックス エンドユーザ通知ページを編集する際に、条件変数を含めて、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。

次の表は、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	次の条件を表します。 `else` これを *%?V* 条件変数とともに使用します。
%#V	次の条件を表します。 `endif` これを *%?V* 条件変数とともに使用します。

たとえば、次の 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
```

オンボックス エンドユーザ通知ページの編集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。

オフボックス エンドユーザ通知ページ

指定したカスタム URL にすべての通知ページをリダイレクトすることで、Web セキュリティ アプライアンスの外部に通知ページを定義できます。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 Web サイトをすべて 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、エンド ユーザ通知ページのパラメータ（17-9 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。

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。次の形式を使用します。

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

次の表は、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
時刻（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。
ユーザ（User）	要求を行うクライアントのユーザ名（該当する場合）。
サイト	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 URL カテゴリとユーザ定義 URL カテゴリの両方の 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。

パラメータ名	説明
DVS_ThreatName	DVS エンジンによって検出されたマルウェアの名前。
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、ブロックされている URL カテゴリによってユーザが 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 スクリプトで次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（リンクまたはボタンなど）でエンドユーザ通知ページに組み込む。同時に、「リンクをクリックすると、より広範囲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」をユーザに通知する手順を組み込む。

（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

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　[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）]）。

エンドユーザ確認ページ

Web セキュリティ アプライアンス 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。

次の表は、エンドユーザ確認ページをイネーブルにした場合に設定できる項目を示しています。

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(1 か月)秒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、確認応答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	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。**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ことによって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）] の値の期限が切れるまで、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るか、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、エンドユーザ確認ページ上のリンクをクリックできる必要があります。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。

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。

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　[確認応答の時間間隔（Time Between Acknowledgements）] フィールドで、アプライアンスがエンドユーザ確認ページの表示間隔として使用する時間間隔を入力します。

30 ～ 2678400（1 か月）秒の任意の値を指定できます。デフォルトは 1 日（86400 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　[無活動タイムアウト（Inactivity Timeout）] フィールドで、IP アドレスの最長アイドル タイムアウトを入力します。

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。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 6　[サロゲート タイプ（Surrogate Type）] を選択します。

ステップ 7　[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確認ページに表示するテキストを入力します。

ステップ 8　（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ページを表示します。

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

- カスタム テキストおよびロゴ：認証、およびエンド ユーザ確認ページ（17-16 ページ）
- 通知ページでサポートされる HTML タグ（17-15 ページ）

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ように強制する 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）を使用していつエンド ユーザ確認ページを受け入れたかを記録します。

- **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。エンドユーザの確認ページがイネーブルになっていて、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、「EUA に基づくセッションを使用して HTTPS 要求にアクションを実行する（「bypass」または「drop」）」コマンドをバイパスするように選択します。

- **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 URL フィルタリング警告ページの設定

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（1 か月）秒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。

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）]）。

関連項目

- 通知ページでサポートされる HTML タグ（17-15 ページ）

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 ドメイン名の悪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通知メッセージを表示します。

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　[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）]）。

通知ページのカスタム テキスト

次の各項は、オンボックス エンドユーザ通知およびエンドユーザ確認ページに入力するカスタム テキストに適用されます。

通知ページでサポートされる HTML タグ

いくつかの HTML タグを使用して、オンボックス エンドユーザ通知ページやエンドユーザ確認ページのテキストを書式設定できます。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。

次の 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.
```

 タグにより、CSS スタイルを使用して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.
```

カスタム テキストおよびロゴ：認証、およびエンド ユーザ確認ページ

カスタム テキスト内に埋め込まれたリンクの URL パスとドメイン名のすべての組み合わせ、およびオンボックス エンドユーザ通知ページ、エンドユーザ確認ページ、エンドユーザ URL フィルタリング警告ページのカスタム ロゴは、以下の対象外となります。

- ユーザ認証
- エンドユーザ確認
- 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、次の 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
```

次の 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、管理者は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、管理者はリンクやカスタム 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には、管理者またはシスコ 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上で役立つさまざまなコード セットが表示されます。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（オンボックス エンドユーザ通知ページの編集 を参照）。

次の表は、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たエラー 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、次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）	要求され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 とパスワードを入力してください。（A valid user ID and password 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、ユーザの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このファイルの URL（<URL>）へ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 とパスワードを入力してください。（A valid user ID and password 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ワード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 password.）
ERR_PROXY_REDIRECT リダイレクト	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 Acknowledgement）	エンドユーザ確認ページ 詳細については、オンボックス エンドユーザ通知ページ（17-4 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、次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 セキュリティ アプライアンス 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（Redirect）	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ワードを入力してください。（If you want to login as a different user, enter a different username and password 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 を拡張し、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 とパスワードを入力してください。（A valid user ID and password must be entered when prompted.）

エンドユーザのアクティビティをモニタするレポートの生成

レポートの概要

Web セキュリティ アプライアンスでは概要レポートが生成されるので、ネットワークで起きていることを把握したり、特定のドメイン、ユーザ、カテゴリのトラフィックの詳細を表示することができます。レポートを実行して特定の期間内のシステム アクティビティをインタラクティブに表示したり、レポートをスケジュールして定期的に実行することができます。

関連項目

- レポート ページからのレポートの印刷とエクスポート（18-6 ページ）

レポートでのユーザ名の使用

認証をイネーブルにすると、ユーザは Web プロキシで認証される際にユーザ名でレポートに一覧表示されます。デフォルトでは、ユーザ名は認証サーバに表示されたとおりに書き込まれます。ただし、すべてのレポートでユーザ名を識別できないようにすることができます。

（注） 管理者は、レポートでユーザ名を常に確認します。

ステップ 1 [セキュリティ サービス（Security Services）] > [レポート（Reporting）] を選択し、[設定を編集（Edit Settings）] をクリックします。

ステップ 2　[ローカル レポート（Local Reporting）] で、[レポートでユーザ名を匿名にする（Anonymize usernames in reports）] を選択します。

ステップ 3　**変更を送信して確定します（[送信（Submit）]** と [変更を確定（Commit Changes）]）。

レポート ページ

Web セキュリティ アプライアンスには次のレポートがあります。

- 概要
- Users
- Web サイト（Web Sites）
- URL Categories
- アプリケーションの表示（Application Visibility）
- マルウェア対策（Anti-Malware）
- 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（System Status）

[レポート（Reporting）] タブの使用

[レポート（Reporting）] タブには、システム データを表示するためのオプションがいくつかあります。レポート ページには、システム アクティビティの概要が表示され、システム データを表示するための複数のオプションがあります。Web サイトおよびクライアント固有のデータをページごとに検索することもできます。

[レポート（Reporting）] タブでは、ほとんどのレポートで次のタスクを実行できます。

オプション	タスクへのリンク
レポートで表示する時間範囲を変更する	時間範囲の変更（18-3 ページ）
特定のクライアントとドメインを検索する	データの検索（18-3 ページ）
チャートに表示するデータを選択する	チャート化するデータの選択（18-4 ページ）
列を選択してソートする	関連項目（18-4 ページ）
レポートを外部ファイルにエクスポートする	レポート ページからのレポートの印刷とエクスポート（18-6 ページ）

時間範囲の変更

[時間範囲（Time Range）] フィールドを使用して、各セキュリティ コンポーネントの表示データを更新できます。このオプションを使用して、定義済みの時間範囲のアップデートを生成できます。また、開始から終了までの時刻を指定してカスタム時間範囲を定義することもできます。

（注）　選択した時間範囲は、[時間範囲（Time Range）] メニューで異なる値を選択するまで、すべてのレポート ページ全体で使用されます。

時間範囲	返されるデータ
時間（Hour）	60 分間に、最大 5 分間が追加されます。
日（Day）	直近の 24 時間とその時点の 1 時間未満の時間を含めた時間に対して 1 時間間隔
Week	直近の 7 日間にその時点の日にちを足した日数に対して 1 日間隔
月（30 日）（Month (30 days)）	直近の 30 日間にその時点の日にちを足した日数に対して 1 日間隔
昨日（Yesterday）	直近の 24 時間（00:00～23:59）（Web セキュリティ アプライアンスで定義されたタイムゾーンを使用）
カスタム範囲（Custom Range）	ユーザ定義のカスタム時間範囲。 [カスタム範囲（Custom Range）] を選択すると、開始時刻と終了時刻を入力できるダイアログボックスが表示されます。

（注）　すべてのレポートで、システム設定の時間帯に基づき、グリニッジ標準時（GMT）オフセットで日付および時刻情報が表示されます。ただし、データ エクスポートでは、世界の複数のタイム ゾーンの複数のシステムに対応するために、GMT で時刻が表示されます。

データの検索

一部のレポートには、特定のデータ ポイントを検索できるフィールドがあります。データを検索するときに、レポートでは、検索対象の特定のデータ セットに合わせてレポート データが調整されます。入力した文字列に完全に一致する値や入力文字列から始まる値を検索できます。次のレポート ページには検索フィールドがあります。

検索フィールド	説明
Users	ユーザ名またはクライアント IP アドレスでユーザを検索します。
Web サイト（Web Sites）	ドメインまたはサーバの IP アドレスでサーバを検索します。
URL Categories	URL カテゴリを検索します。

検索フィールド	説明
Users	ユーザ名またはクライアント IP アドレスでユーザを検索します。
アプリケーションの表示（Application Visibility）	AVC エンジンがモニタしてブロックするアプリケーション名を検索します。
クライアント マルウェア リスク（Client Malware Risk）	ユーザ名またはクライアント IP アドレスでユーザを検索します。

（注）　クライアント IP アドレスおよびクライアント ユーザ ID を表示するには、認証を設定する必要があります。

チャート化するデータの選択

各 Web レポーティング ページのデフォルト チャートには、一般に参照されるデータが表示されますが、代わりに異なるデータをチャート化するように選択できます。ページに複数のチャートがある場合は、チャートごとに変更できます。チャートのオプションは、レポートのテーブルの列見出しと同じです。

ステップ 1　チャートの下の [グラフ オプション（Chart Options）] をクリックします。

ステップ 2　表示するデータを選択します。

ステップ 3　[完了（Done）] をクリックします。

関連項目

- 関連項目（18-4 ページ）

カスタム レポート

既存のレポート ページのチャート（グラフ）とテーブルを組み合わせて、カスタム レポート ページを作成できます。

目的	操作内容
カスタム レポート ページへのモジュールの追加	参照先: • カスタム レポートに追加できないモジュール（18-5 ページ）。 • カスタム レポート ページの作成（18-5 ページ）
カスタム レポート ページの表示	1. **[レポート（Reporting）] > [マイレポート（My Reports）] を選択します。** 2. 表示する時間範囲を選択します。選択した時間範囲は、[マイレポート（My Reports）] ページのすべてのモジュールを含め、すべてのレポートに適用されます。 新たに追加されたモジュールは関連するセクションの上部に表示されます。

目的	操作内容
カスタム レポート ページでのモジュールの再配置	目的の場所にモジュールをドラッグ アンド ドロップします。
カスタム レポート ページからのモジュールの削除	モジュールの右上にある [X] をクリックします。
カスタム レポートの PDF または CSV バージョンの生成	[レポート（Reporting）] > [アーカイブ レポート（Archived Reports）] を選択し、[今すぐレポートを生成（Generate Report Now）] をクリックします。
カスタム レポートの PDF または CSV バージョンの定期的な生成	[レポート（Reporting）] > [スケジュールされたレポート（Scheduled Reports）] を選択します。

カスタム レポートに追加できないモジュール

- 検索結果、Web トラッキングの検索結果を含む

カスタム レポート ページの作成

はじめる前に

- 追加対象のモジュールが追加可能であることを確認します。カスタム レポートに追加できないモジュール（18-5 ページ）を参照してください。
- モジュールの右上の [X] をクリックして、不要なデフォルト モジュールを削除します。

ステップ 1　次のいずれかの方法でカスタム レポート ページにモジュールを追加します。

（注） 一部のモジュールは、次のいずれかの方法を使用した場合のみ利用できます。ある方式を使用してモジュールを追加できない場合は、別の方法を試してください。

- 追加するモジュールがあるレポート ページに移動し、モジュールの上部にある [+] ボタンをクリックしてレポート ページに移動します。
- **[レポート（Reporting）] > [マイレポート（My Reports）]** に移動し、いずれかのセクションの上部にある **[+]** ボタンをクリックして、追加するレポート モジュールを選択します。検索しているモジュールを表示するには、[マイレポート（My Reports）] ページの各セクションの **[+]** ボタンをクリックする必要があります。

各モジュールは一度だけ追加できます。すでに特定のモジュールをレポートに追加している場合は、追加オプションが利用できなくなっています。

ステップ 2　（たとえば、列の追加、削除、並べ替えなどを行って、あるいはチャートにデフォルト以外のデータを表示して）カスタマイズしたモジュールを追加する場合は、[マイレポート（My Reports）] ページでそのモジュールをカスタマイズします。

モジュールがデフォルト設定に追加されます。元のモジュールの時間範囲は保持されません。

ステップ 3　別に凡例を持つチャート（たとえば、[概要（Overview）] ページからのグラフ）を追加する場合は、別途凡例を追加します。必要に応じて、説明するデータの隣にドラッグ アンド ドロップします。

レポートおよびトラッキングにおけるサブ ドメインとセカンド レベル ドメインの比較

レポートおよびトラッキングの検索では、セカンドレベルのドメイン（http://george.surbl.org/two-level-tlds に一覧表示されている地域ドメイン）は、ドメイン タイプがサブドメインと同じように見えますが、サブドメインとは別の方法で処理されます。次に例を示します。

- レポートには、co.uk などの 2 レベルのドメインの結果は含まれませんが、foo.co.uk の結果は含まれます。レポートには、cisco.com などの主要な企業ドメインの下にサブドメインが含まれます。
- 地域ドメイン co.uk に対するトラッキング検索結果には、foo.co.uk などのドメインは含まれませんが、cisco.com に対する検索結果には subdomain.cisco.com などのサブドメインが含まれます。

レポート ページからのレポートの印刷とエクスポート

ページ右上隅の [印刷可能（PDF）（Printable (PDF)）] リンクをクリックすると、すべてのレポート ページを読みやすい印刷形式の PDF 版で生成できます。また、[エクスポート（Export）] リンクをクリックして、未処理データをカンマ区切り形式（CSV）ファイルとしてエクスポートすることもできます。

CSV エクスポートには未処理データのみが含まれるため、Web ベースのレポート ページからエクスポートされたデータには、パーセンテージなどの計算データが含まれていない場合があります（そのデータが Web ベースのレポートで表示される場合でも、含まれていない場合があります）。

レポート データのエクスポート

ほとんどのレポートには、未処理データをカンマ区切り形式（CSV）のファイルにエクスポートできる [エクスポート（Export）] リンクが用意されています。CSV ファイルにデータをエクスポートすると、Microsoft Excel などのアプリケーションを使用し、データにアクセスして処理することができます。

エクスポートされた CSV データは、Web セキュリティ アプライアンスでの設定にかかわらず、すべてのメッセージ トラッキングおよびレポーティング データをグリニッジ標準時（GMT）で示します。GMT 時間への変換の目的は、アプライアンスに依存せずにデータを使用したり、複数の時間帯にあるアプライアンスからのデータを参照する際にデータを使用したりできるようにするためです。

次の例は、Anti-Malware カテゴリ レポートの raw データ エクスポートのエントリであり、太平洋夏時間（PDT）が GMT - 7 時間で表示されています。

```
Begin Timestamp, End Timestamp, Begin Date, End Date, Name, Transactions Monitored,
Transactions Blocked, Transactions Detected

1159772400.0, 1159858799.0, 2006-10-02 07:00 GMT, 2006-10-03 06:59 GMT, Adware, 525,
2100, 2625
```

カテゴリ ヘッダー	値	説明
Begin Timestamp	1159772400.0	エポックからの秒数で表されたクエリー開始時刻。
End Timestamp	1159858799.0	エポックからの秒数で表されたクエリー終了時刻。

（続き）

カテゴリ ヘッダー	値	説明
Begin Date	2006-10-02 07:00 GMT	クエリーの開始日。
End Date	2006-10-03 06:59 GMT	クエリーの終了日。
Name	Adware	マルウェア カテゴリの名前。
Transactions Monitored	525	モニタリングされたトランザクション数。
Transactions Blocked	2100	ブロックされたトランザクション数。
Transactions Detected	2625	トランザクションの合計数: 検出されたトランザクション数 + ブロックされたトランザクション数。

（注） カテゴリ ヘッダーは、レポートのタイプごとに異なります。

（注） ローカライズされた CSV データをエクスポートすると、ブラウザによっては見出しが正しく表示されない場合があります。これは、ブラウザによっては、ローカライズされたテキストに対して適切な文字セットが使用されない場合があることから発生します。この問題の回避策として、ローカル マシンにファイルを保存し、[ファイル（File）] > [開く（Open）] を使用して任意の Web ブラウザでファイルを開きます。ファイルを開いたら、ローカライズされたテキストを表示するための文字セットを選択します。

集約管理レポートのイネーブル化

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によって管理されている場合、Web セキュリティ アプライアンスによって処理される Web トラフィックのレポートを表示するアプライアンスを選択できます。セキュリティ管理アプライアンスによって複数の Web セキュリティ アプライアンスを管理している場合は、[集約管理レポート（Centralized Reporting）] をイネーブルにする必要があるかもしれません。

（注） [集約管理レポート（Centralized Reporting）] をイネーブルにした場合は、[システム容量（System Capacity）] レポートと [システム ステータス（System Status）] レポートのみを Web セキュリティ アプライアンスで利用できます。他のレポートを表示するには、セキュリティ管理アプライアンスに接続します。

ステップ 1　[セキュリティ サービス（Security Services）] > [レポート（Reporting）] を選択し、[設定を編集（Edit Settings）] をクリックします。

ステップ 2　[集約管理レポート（Centralized Reporting）] を選択します。

ステップ 3　**変更を送信して確定します（[送信（Submit）]** と [変更を確定（Commit Changes）]）。

レポートのスケジュール設定

日単位、週単位、または月単位で実行されるようにレポートをスケジュール設定することができます。スケジュール化したレポートは、前日、過去 7 日間、前月のデータを含めるように設定できます。

レポートをスケジュール設定できるレポート タイプは次のとおりです。

- 概要
- Users
- Web サイト（Web Sites）
- URL Categories
- アプリケーションの表示（Application Visibility）
- マルウェア対策（Anti-Malware）
- 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）
- SOCKS プロキシ
- ユーザの場所別レポート（Reports by User Location）
- システム容量（System Capacity）
- マイレポート（My Reports）

スケジュール設定されたレポートの追加

ステップ 1　[レポート（Reporting）] > [スケジュールされたレポート（Scheduled Reports）] を選択し、[定期レポートの追加（Add Scheduled Report）] をクリックします。

ステップ 2　レポートの種類を選択します。

ステップ 3　レポートのタイトルを入力します。同じ名前のレポートを複数作成しないために、わかりやすいタイトルを使用するようにしてください。

ステップ 4　レポートに含めるデータの時間範囲を選択します。

ステップ 5　生成されるレポートの形式を選択します。

デフォルト形式は PDF です。ほとんどのレポートでは、raw データを CSV ファイルとして保存することも可能です。

ステップ 6　設定するレポートのタイプに応じて、含める行数やデータをソートする列など、さまざまなレポート オプションを指定できます。必要に応じて、これらのオプションを設定します。

ステップ 7　[スケジュール（Schedule）] セクションで、レポートを実行する周期（毎日、毎週、または毎月）と時間を選択します。

ステップ 8　[メール（Email）] フィールドに、生成されたレポートを送信する電子メール アドレスを入力します。

電子メール アドレスを指定しなかった場合は、レポートのアーカイブのみが行われます。

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）]）。

スケジュール設定されたレポートの編集

ステップ 1　**[レポート（Reporting）] > [スケジュールされたレポート（Scheduled Reports）] を選択します。**

ステップ 2　リストからレポートのタイトルを選択します。

ステップ 3　設定を変更します。

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）]）。

スケジュール設定されたレポートの削除

ステップ 1　[レポート（Reporting）] > [スケジュールされたレポート（Scheduled Reports）] を選択します。

ステップ 2　削除するレポートに対応するチェックボックスをオンにします。

ステップ 3　スケジュール設定されたレポートをすべて削除するには、[すべて（All）] チェックボックスをオンにします。

ステップ 4　**削除して変更を確定します（[削除（Delete）]** と [変更を確定（Commit Changes）]）。

（注）　削除されたレポートのアーカイブ版は削除されません。

オンデマンドでのレポートの生成

ステップ 1　[レポート（Reporting）] > [アーカイブレポート（Archived Reportss）] を選択します。

ステップ 2　**[今すぐレポートを生成（Generate Report Now）] をクリックします。**

ステップ 3　レポートの種類を選択し、タイトルを編集します。

ステップ 4　レポートに含めるデータの時間範囲を選択します。

ステップ 5　生成されるレポートの形式を選択します。

デフォルト形式は PDF です。ほとんどのレポートでは、raw データを CSV ファイルとして保存することも可能です。

ステップ 6　設定するレポートのタイプに応じて、含める行数やデータをソートする列など、さまざまなレポート オプションを指定できます。必要に応じて、これらのオプションを設定します。

ステップ 7　レポートをアーカイブするかどうかを選択します（アーカイブする場合には、レポートが [アーカイブレポート（Archived Reportss）] ページに表示されます）。

ステップ 8　レポートを電子メールで送信し、受信者の電子メール アドレスをリストするかどうかを指定します。

ステップ 9　[このレポートを配信（Deliver This Report）] をクリックして、レポートを生成します。

ステップ 10　**変更を確定します。**

アーカイブ レポート

[レポート（Reporting）] > [アーカイブレポート（Archived Reportss）] ページには、使用可能なレポートが一覧表示されます。[レポートのタイトル（Report Title）] 列のレポート名はインタラクティブになっており、各レポートのビューにリンクしています。[表示（Show）] メニューは、一覧表示されたレポートのタイプをフィルタリングします。インタラクティブな列見出しを使用して、各列のデータをソートすることができます。

アプライアンスでは、スケジュール設定されたレポートごとに最大 12 のインスタンスが保存されます（最大 1000 レポート）。アーカイブ済みのレポートは、アプライアンスの `/periodic_reports` ディレクトリに保管されます。アーカイブ済みのレポートは自動的に削除されます。新しいレポートが追加されると、古いレポートが削除され、常に 1000 という数が維持されます。12 インスタンスという制限は、同じ名前と時間範囲のスケジュール設定された各レポートに適用されます。

SNMP モニタリング

AsyncOS オペレーティング システムは、SNMP（簡易ネットワーク管理プロトコル）を使用したシステム ステータスのモニタリングをサポートしています。これには、シスコのエンタープライズ MIB、asyncoswebsecurityappliance-mib.txt が含まれます。asyncoswebsecurityappliance-mib を使用することで、管理者はシステムの状態をモニタしやすくなります。また、このリリースには、RFC 1213 および 1907 に規定されている MIB-II の読み取り専用のサブセットが実装されています（SNMP の詳細については、RFC 1065、1066、および 1067 を参照してください）。次の点に注意してください。

- SNMP は、デフォルトで**オフ**になります。
- SNMP SET 動作（コンフィギュレーション）は実装されません。
- AsyncOS は SNMPv1、v2、および v3 をサポートしています。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は、メッセージ認証と暗号化が必須です。認証のパスワードと暗号は異なっている必要があります。暗号化アルゴリズムは AES（推奨）または DES を指定できます。認証アルゴリズムは SHA-1（推奨）または MD5 を指定できます。次回 `snmpconfig` コマンドを実行するときには、コマンドにこのパスワードが「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限り機能します）。

snmpconfig コマンドを使用して、アプライアンスの SNMP システム ステータスを設定します。インターフェイスの値を選択し、設定し終えると、アプライアンスは SNMPv3 GET 要求に応答します。これらのバージョン 3 要求には、一致するパスワードが含まれている必要があります。デフォルトでは、バージョン 1 および 2 要求は拒否されます。イネーブルにする場合は、バージョン 1 および 2 要求に一致するコミュニティ ストリングが含まれている必要があります。

MIB ファイル

シスコでは、電子メールと 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 に加えて、「Structure of Management Information」（SMI）ファイルを用意しています。

- 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：asyncoswebsecurityappliance-mib の役割を定義します。

これらのファイルは、Cisco Web セキュリティ アプライアンス アプライアンスに付属のドキュメンテーション CD に収録されています。これらのファイルは、次の URL から入手できます。

http://www.cisco.com/en/US/customer/products/ps10164/tsd_products_support_series_home.html

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、および電源モジュール ステータスが報告されます。

表示されている数字は、モニタできるオブジェクトのインスタンスの数です。たとえば、S350 アプライアンスの 4 つのファンの RPM について照会できます。

モデル	周囲温度	ファン	電源モジュール	ディスク ステータス	NIC リンク
S160	1	2	1	2	6
S350	1	4	2	6	6
S360	[1]	4	2	4	6
S650	[1]	4	2	6	6
S660	[1]	4	2	6	6

ハードウェア トラップ

モデル	高温（周囲）	ファン障害	電源モジュール	RAID	リンク
S160/S350/S360/ S650/S660	47C	0 RPM	ステータスの変化	ステータスの変化	ステータスの変化

ステータス変更トラップは、ステータスが変更されると送信されます。ファン障害および高温トラップは、5 秒ごとに送信されます。その他のトラップは障害条件アラーム トラップです。これらのトラップは、ステータスが（良好から障害へ）変更されたときに一度だけ送信されます。重大値の 10 % 以内の温度を不安原因と考えることができます。

（注）　障害状態アラーム トラップは個々のコンポーネントの重大な障害を示しますが、システム全体にわたる障害を引き起こすとは限りません。

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、標準の SNMP トラップ ポートであるポート 162 経由で送信します。次の例では、トラップ ターゲット `10.1.1.29` およびトラップ コミュニティ ストリングが入力されています。これは、アプライアンスから SNMP トラップを受信する SNMP 管理コンソール ソフトウェアを実行しているホストです。

インターフェイスに対して SNMP をイネーブルにするときに、SNMP トラップを設定（特定のトラップをイネーブルまたはディセーブルに）できます。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。

CLI の例

次の例では、`snmpconfig` コマンドを使用して、ポート 161 の「PublicNet」インターフェイスで SNMP をイネーブルにしています。バージョン 3 のパスフレーズが入力され、確認のために再入力されています。- システムは、バージョン 1 および 2 要求を処理するように設定されており、これらのバージョン 1 および 2 からの GET 要求に対してコミュニティ ストリング `public` が入力されています。`10.1.1.29` のトラップ ターゲットが入力されます。最後に、システムの場所と連絡先情報が入力されています。

```
example.com > snmpconfig
Current SNMP settings:
SNMP Disabled.

Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]> setup

Do you want to enable SNMP? [N]> y

Please choose an IP interface for SNMP requests.
1. Management (192.168.1.1/24: wsa01-vmw1-tpub.qa)
2. P1 (192.168.20.40/24: wsa01-vmw1-tpub.qa
[1]>

Enter the SNMPv3 passphrase.
>
Please enter the SNMPv3 passphrase again to confirm.
>
Which port shall the SNMP daemon listen on?
[161]>
```

```
Service SNMP V1/V2c requests? [N]\> y

Enter the SNMP V1/V2c community string.
[]> public

From which network shall SNMP V1/V2c requests be allowed?
[192.168.1.1]>

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.
[None]> 10.1.1.29

Enter the Trap Community string.
[]> tcomm

Enterprise Trap Status
1. CPUUtilizationExceeded       Disabled
2. RAIDStatusChange             Enabled
3. connectivityFailure          Disabled
4. fanFailure                   Enabled
5. highTemperature              Enabled
6. keyExpiration                Enabled
7. linkDown                     Enabled
8. linkUp                       Enabled
9. memoryUtilizationExceeded    Disabled
10. powerSupplyStatusChange     Enabled
11. resourceConservationMode    Enabled
12. updateFailure               Enabled
13. upstream_proxy_failure      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.
[]> 1,3

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]>

Enterprise Trap Status
1. CPUUtilizationExceeded       Enabled
2. RAIDStatusChange             Enabled
3. connectivityFailure          Enabled
4. fanFailure                   Enabled
5. highTemperature              Enabled
6. keyExpiration                Enabled
7. linkDown                     Enabled
8. linkUp                       Enabled
9. memoryUtilizationExceeded    Disabled
10. powerSupplyStatusChange     Enabled
11. resourceConservationMode    Enabled
12. updateFailure               Enabled
13. upstream_proxy_failure      Enabled
Do you want to change any of these settings?[N]>

Enter the System Location string.
[Unknown: Not Yet Configured]> Network Operations Center - west; rack #30, position 3
```

```
Enter the System Contact string.
[snmp@localhost]> Joe Administrator, x8888

Current SNMP settings:
Listening on interface "Management" 192.168.1.1 port 161.
SNMP v3: Enabled.
SNMP v1/v2: Enabled, accepting requests from subnet 192.168.1.1.
SNMP v1/v2 Community String: public
Trap target: 10.1.1.29
Location: Network Operations Center - west; rack #30, position 3
System Contact: Joe Administrator, x8888

Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]>

example.com>
```

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

[レポート（Reporting）] > [概要（Overview）] ページには、Web セキュリティ アプライアンスでのアクティビティの概要が表示されます。このページには、Web セキュリティ アプライアンスで処理される Web トラフィックに関するグラフおよびサマリー テーブルが含まれています。

セクション	説明
時間範囲（Time Range）（ドロップダウン リスト）	レポートに含めるデータの時間範囲を選択できるメニュー。

（続き）

セクション	説明
Web プロキシ アクティビティ総数（Total Web Proxy Activity）	トランザクションの実際の数（縦の目盛り）、および（Web プロキシ）アクティビティが発生したおよその日付（横の時間軸）が表示されます。
Web プロキシの概要（Web Proxy Summary）	疑わしいまたは正常な Web プロキシ アクティビティの比率を表示できます。
L4 トラフィック モニタの概要（L4 Traffic Monitor Summary）	L4 トラフィック モニタによってモニタされ、ブロックされたトラフィックをレポートします。
疑わしいトランザクション（Suspect Transactions）	さまざまなセキュリティ コンポーネントによって疑わしいトランザクションと分類された Web トランザクションを表示できます。 トランザクションの実際の数、およびアクティビティが発生したおよその日付が表示されます。
Suspect Transactions Summary	ブロックまたは警告された疑わしいトランザクションの比率を表示できます。
総トランザクション数別上位 URL カテゴリ（Top URL Categories by Total Transactions）	ブロックされた上位 10 の URL カテゴリが表示されます。
総トランザクション数別上位アプリケーション タイプ（Top Application Types by Total Transactions）	AVC エンジンによってブロックされた上位アプリケーション タイプが表示されます。
検出された上位マルウェア カテゴリ（Top Malware Categories Detected）	検出されたすべてのマルウェア カテゴリが表示されます。
ブロックまたは警告されたトランザクション上位ユーザ（Top Users Blocked or Warned Transactions）	ブロックされたトランザクションまたは警告されたトランザクションを生成しているユーザが表示されます。認証されたユーザはユーザ名で表示され、認証されていないユーザは IP アドレスで表示されます。

[ユーザ（Users）] ページ

[Web] > [レポート（Reporting）] > [ユーザ（Users）] ページには、個々のユーザの Web トラフィック情報を表示するためのリンクが提供されています。ネットワーク上のユーザがインターネット、特定の Web サイト、または特定の URL で費やした時間と、ユーザが使用した帯域幅の量を表示できます。

セクション	説明
時間範囲（Time Range）（ドロップダウン リスト）	レポートに含めるデータの時間範囲を選択できるメニュー。
ブロックされたトランザクション数別上位ユーザ（Top Users by Transactions Blocked）	ブロックされたトランザクションの数（横の目盛り）が最大のユーザ（縦の目盛り）が表示されます。

セクション	説明
使用した帯域幅別上位ユーザ(Top Users by Bandwidth Used)	システム上で最も帯域幅(ギガバイト単位の使用量を示す横の目盛り)を使用しているユーザ(縦の目盛り)が表示されます。
ユーザ テーブル(Users Table)	個々のユーザを一覧表示し、ユーザごとに複数の統計情報を表示します。

[ユーザの詳細(User Details)] ページ

[ユーザの詳細(User Details)] ページには、[レポート(Reporting)] > [ユーザ(Users)] ページの [ユーザ テーブル(Users Table)] で選択した特定のユーザに関する情報が表示されます。

セクション	説明
時間範囲(Time Range)(ドロップダウン リスト)	レポートに含めるデータの時間範囲を選択できるメニュー。
総トランザクション数別 URL カテゴリ(URL Categories by Total Transactions)	特定のユーザが使用している特定の URL カテゴリのリストが表示されます。
総トランザクション数別トレンド(Trend by Total Transaction)	ユーザが Web にいつアクセスしたかが表示されます。
一致した URL カテゴリ(URL Categories Matched)	完了したトランザクションとブロックされたトランザクションの両方について、指定した時間範囲内で一致したすべての URL カテゴリが表示されます。
一致したドメイン(Domains Matched)	このユーザがアクセスした特定のドメインまたは IP アドレスに関する情報が表示されます。 **(注)** このドメインのデータを csv ファイルにエクスポートする場合は、先頭から 300,000 件のエントリのみがファイルにエクスポートされるので注意してください。
一致したアプリケーション(Applications Matched)	AVC エンジンによって検出された、特定のユーザが使用している特定のアプリケーションが表示されます。
検出されたマルウェア脅威(Malware Threats Detected)	特定のユーザによって引き起こされているマルウェアの脅威の内、上位のものが表示されます。
一致したポリシー(Policies Matched)	この特定のユーザに適用されている特定のポリシーが表示されます。

[Web サイト（Web Sites）] ページ

[レポート（Reporting）] > [Web サイト（Web Sites）] ページは、Web セキュリティ アプライアンスで発生しているアクティビティ全体を集約したものです。

セクション	説明
時間範囲（Time Range）（ドロップダウン リスト）	このメニューからレポートに含めるデータの時間範囲を選択できます。
総トランザクション数別上位ドメイン（Top Domains by Total Transactions）	サイト上のアクセス上位ドメインがグラフ形式で表示されます。
ブロックされたトランザクション数別上位ドメイン（Top Domains by Transactions Blocked）	トランザクションごとに発生するブロック アクションをトリガーした上位ドメインが、グラフ形式で表示されます。
一致したドメイン（Domains Matched）	サイト上のアクセスされたドメインがインタラクティブなテーブルに表示されます。 **（注）** このドメインのデータを csv ファイルにエクスポートする場合は、先頭から 300,000 件のエントリのみがファイルにエクスポートされるので注意してください。

[URL カテゴリ（URL Categories）] ページ

[レポート（Reporting）] > [URL カテゴリ（URL Categories）] ページでは、ネットワーク上のユーザがアクセスしている URL カテゴリを表示できます。[URL カテゴリ（URL Categories）] ページを [アプリケーションの表示（Application Visibility）] ページおよび [ユーザ（Users）] ページと併用すると、特定のユーザとそのユーザがアクセスを試みているアプリケーションや Web サイトのタイプを調べることができます。

（注） すでに定義されている一連の URL カテゴリは更新されることがあります。

セクション	説明
時間範囲（Time Range）（ドロップダウン リスト）	レポートの時間範囲を選択します。
総トランザクション数別上位 URL カテゴリ（Top URL Categories by Total Transactions）	このセクションには、サイト上でアクセスされた上位 URL カテゴリがグラフ形式で表示されます。

セクション	説明
ブロックまたは警告を受けたトランザクション数別上位 URL カテゴリ（Top URL Categories by Blocked and Warned Transactions）	トランザクションごとに発生するブロックまたは警告アクションをトリガーした上位 URL がグラフ形式で表示されます。
一致した URL カテゴリ（URL Categories Matched）	指定した時間範囲における URL カテゴリ別のトランザクションの傾向、および各カテゴリで使用された帯域幅と費やされた時間が表示されます。 未分類の URL の比率が 15 ～ 20 % を上回る場合は、次のオプションを検討してください。 • 特定のローカライズされた URL の場合は、カスタム URL カテゴリを作成し、特定のユーザまたはグループ ポリシーに適用できます。 • 評価およびデータベース更新用に、未分類の URL と誤って分類された URL をシスコにレポートできます。 • Web レピュテーション フィルタリングと、アンチマルウェア フィルタリングがイネーブルになっていることを確認してください。

URL カテゴリ セットの更新とレポート

Web セキュリティ アプライアンスでは、一連の定義済み URL カテゴリが定期的に自動更新される場合があります。

これらの更新が行われると、古いカテゴリに関連づけられたデータが古すぎてレポートに含まれなくなるまで、古いカテゴリ名は引き続きレポートに表示されます。URL カテゴリ セットの更新後に生成されたレポート データには新しいカテゴリが使用されるので、同じレポートに新旧両方のカテゴリが表示される場合があります。

[アプリケーションの表示（Application Visibility）] ページ

[レポート（Reporting）] > [アプリケーションの表示（Application Visibility）] ページには、Application Visibility and Control エンジンによって検出されたとおり、使用され、ブロックされるアプリケーションおよびアプリケーション タイプが表示されます。

セクション	説明
時間範囲（Time Range）（ドロップダウン リスト）	レポートに含めるデータの時間範囲を選択できるメニュー。
総トランザクション数別上位アプリケーション タイプ（Top Application Types by Total Transactions）	このセクションには、サイト上でアクセスされた上位アプリケーション タイプがグラフ形式で表示されます。

（続き）

セクション	説明
ブロックされたトランザクション数別上位アプリケーション（Top Applications by Blocked Transactions）	トランザクションごとに発生するブロック アクションをトリガーした上位アプリケーション タイプが、グラフ形式で表示されます。
一致したアプリケーション タイプ（Application Types Matched）	[総トランザクション数別上位アプリケーション タイプ（Top Applications Type by Total Transactions）] グラフに表示されているアプリケーション タイプについて、さらに詳しい情報を表示できます。
一致したアプリケーション（Applications Matched）	指定した時間範囲内のすべてのアプリケーションが表示されます。

[マルウェア対策(Anti-Malware)] ページ

[レポート(Reporting)] > [マルウェア対策(Anti-Malware)] ページでは、Cisco IronPort DVS エンジンによって検出されたマルウェアをモニタおよび識別することができます。

セクション	説明
時間範囲(Time Range)（ドロップダウン リスト）	レポートに含めるデータの時間範囲を選択できるメニュー。
検出された上位マルウェア カテゴリ(Top Malware Categories Detected)	DVS エンジンによって検出された上位のマルウェア カテゴリが表示されます。
検出された上位マルウェア脅威（Top Malware Threats Detected）	DVS エンジンによって検出された上位のマルウェア脅威が表示されます。
マルウェア カテゴリ(Malware Categories)	[検出された上位マルウェア カテゴリ(Top Malware Categories Detected)] セクションに表示されている特定のマルウェア カテゴリに関する情報が表示されます。
マルウェア脅威(Malware Threats)	[上位マルウェア脅威(Top Malware Threats)] セクションに表示されている特定のマルウェアの脅威に関する情報が表示されます。

[マルウェア カテゴリ(Malware Category)] レポート ページ

ステップ 1　[レポート(Reports)] > [マルウェア対策(Anti-Malware)] を選択します。

ステップ 2　[マルウェア カテゴリ(Malware Categories)] インタラクティブ テーブルで、[マルウェア カテゴリ(Malware Category)] カラム内のカテゴリをクリックします。

[マルウェア脅威（Malware Threats）] レポート ページ

ステップ 1　[レポート（Reports）] > [マルウェア対策（Anti-Malware）] を選択します。

ステップ 2　[マルウェア脅威（Malware Threats）] テーブルで、[マルウェア カテゴリ（Malware Category）] カラム内のカテゴリをクリックします。

[高度なマルウェア防御（Advanced Malware Protection）] ページ

ファイル レピュテーションおよびファイル分析のレポートとトラッキング（14-9 ページ）を参照してください。

[ファイル分析（File Analysis）] ページ

ファイル レピュテーションおよびファイル分析のレポートとトラッキング（14-9 ページ）を参照してください。

[AMP 判定のアップデート（AMP Verdict Updates）] ページ

ファイル レピュテーションおよびファイル分析のレポートとトラッキング（14-9 ページ）を参照してください。

[クライアント マルウェア リスク（Client Malware Risk）] ページ

[レポート（Reporting）] > [クライアント マルウェア リスク（Client Malware Risk）] ページは、クライアント マルウェア リスク アクティビティをモニタするために使用できるセキュリティ関連のレポーティング ページです。[クライアント マルウェア リスク（Client Malware Risk）] ページには、L4 トラフィック モニタ（L4TM）によって特定された、頻度の高いマルウェア接続に関与しているクライアント IP アドレスが表示されます。

セクション	説明
時間範囲（Time Range）（ドロップダウン リスト）	レポートに含めるデータの時間範囲を選択できるメニュー。
Web プロキシ：マルウェア リスク別上位クライアント（Web Proxy: Top Clients by Malware Risk）	このチャートには、マルウェアのリスクが発生した上位 10 人のユーザが表示されます。

（続き）

セクション	説明
L4 トラフィック モニタ:検出されたマルウェア接続数(L4 Traffic Monitor: Malware Connections Detected)	このチャートには、組織内で最も頻繁にマルウェア サイトに接続しているコンピュータの IP アドレスが表示されます。
Web プロキシ:マルウェア リスク別クライアント(Web Proxy: Clients by Malware Risk)	[Web プロキシ:マルウェア リスク別クライアント(Web Proxy: Clients by Malware Risk)] テーブルには、[Web プロキシ:マルウェア リスク別上位クライアント(Web Proxy: Top Clients by Malware Risk)] セクションに表示されている個々のクライアントに関する詳細情報が表示されます。
L4 Traffic Monitor: Clients by Malware Risk	このテーブルには、マルウェア サイトに頻繁にアクセスしている組織内のコンピュータの IP アドレスが表示されます。

[Web プロキシ:マルウェア リスク別クライアント(Web Proxy: Clients by Malware Risk)] の [クライアントの詳細(Client Detail)] ページ

[クライアントの詳細(Client Detail)] ページには、指定した時間範囲における特定クライアントの Web アクティビティとマルウェア リスクの全データが表示されます。

ステップ 1　[レポート(Reporting)] > [クライアント マルウェア リスク(Client Malware Risk)] を選択します。

ステップ 2　[Web プロキシ:マルウェア リスク別クライアント(Web Proxy: Clients by Malware Risk)] セクションで、[ユーザ ID/クライアント IP アドレス(User ID / Client IP Address)] 列のユーザをクリックします。

関連項目

- [ユーザの詳細(User Details)] ページ(23-3 ページ)

[Web レピュテーション フィルタ(Web Reputation Filters)] ページ

[レポート(Reporting)] > [Web レピュテーション フィルタ(Web Reputation Filters)] ページは、指定した時間範囲内のトランザクションに対する Web レピュテーション フィルタ(ユーザが設定)の結果を表示する、セキュリティ関連のレポーティング ページです。

セクション	説明
時間範囲(Time Range)(ドロップダウン リスト)	レポートに含めるデータの時間範囲を選択できるメニュー。
Web レピュテーション アクション(トレンド)(Web Reputation Actions (Trend))	指定した時間(横方向の時間軸)に対する Web レピュテーション アクションの総数(縦方向の目盛り)が、グラフ形式で表示されます。

セクション	説明
Web レピュテーション アクション（ボリューム）（Web Reputation Actions (Volume)）	Web レピュテーション アクションのボリュームがトランザクション数との対比で表示されます。
ブロックされたトランザクション別 Web レピュテーション脅威タイプ（Web Reputation Threat Types by Blocked Transactions）	レピュテーション スコアが低いためブロックされた脅威タイプが表示されます。
詳細にスキャンされたトランザクション別 Web レピュテーション脅威タイプ（Web Reputation Threat Types by Scanned Further Transactions）	トランザクションのスキャンを指示するレピュテーション スコアが生じた、脅威タイプが表示されます。
Web レピュテーション アクション（スコア別明細）（Web Reputation Actions (Breakdown by Score)）	各アクションの Web レピュテーション スコアの内訳が表示されます。

[L4 トラフィック モニタ（L4 Traffic Monitor）] ページ

[レポート（Reporting）] > [L4 トラフィック モニタ（L4 Traffic Monitor）] ページはセキュリティ関連のレポーティング ページであり、指定した時間範囲内で L4 トラフィック モニタによって検出されたマルウェア ポートとマルウェア サイトに関する情報が表示されます。マルウェア サイトに頻繁にアクセスしているクライアントの IP アドレスも表示されます。

L4 トラフィック モニタは、アプライアンスのすべてのポートに着信するネットワーク トラフィックをリッスンし、ドメイン名と IP アドレスを独自のデータベース テーブルのエントリと照合して、発着信トラフィックを許可するかどうかを決定します。

セクション	説明
時間範囲（Time Range）（ドロップダウン リスト）	レポート対象の時間範囲を選択できるメニュー。
上位クライアント IP（Top Client IPs）	組織内で最も頻繁にマルウェア サイトに接続しているコンピュータの IP アドレスがグラフ形式で表示されます。
上位マルウェア サイト（Top Malware Sites）	L4 トラフィック モニタによって検出された上位のマルウェア ドメインがグラフ形式で表示されます。
クライアント ソース IP（Client Source IPs）	頻繁にマルウェア サイトに接続している組織内のコンピュータの IP アドレスが表示されます。
マルウェア ポート（Malware Ports）	L4 トラフィック モニタによって最も頻繁にマルウェアが検出されたポートが表示されます。
検出されたマルウェア サイト（Malware Sites Detected）	L4 トラフィック モニタによって最も頻繁にマルウェアが検出されたドメインが表示されます。

[SOCKS プロキシ(SOCKS Proxy)] ページ

[レポート(Reporting)] > [SOCKS プロキシ(SOCKS Proxy)] ページでは、上位宛先およびユーザに関する情報を含む、SOCKS プロキシを介して処理されたトランザクションのデータとトレンドを表示できます。

[ユーザの場所別レポート(Reports by User Location)] ページ

[レポート(Reporting)] > [ユーザの場所別レポート(Reports by User Location)] ページで、ローカルおよびリモート ユーザが実行しているアクティビティを確認できます。

対象となるアクティビティは次のとおりです。

- ローカル ユーザおよびリモート ユーザがアクセスしている URL カテゴリ。
- ローカル ユーザおよびリモート ユーザがアクセスしているサイトによってトリガーされているアンチマルウェア アクティビティ。
- ローカル ユーザおよびリモート ユーザがアクセスしているサイトの Web レピュテーション。
- ローカル ユーザおよびリモート ユーザがアクセスしているアプリケーション。
- ユーザ(ローカルおよびリモート)。
- ローカル ユーザおよびリモート ユーザがアクセスしているドメイン。

セクション	説明
時間範囲(Time Range)(ドロップダウン リスト)	レポートに含めるデータの時間範囲を選択できるメニュー。
Web プロキシ アクティビティ総数:リモート ユーザ(Total Web Proxy Activity: Remote Users)	指定した時間(横方向)におけるリモート ユーザのアクティビティ(縦方向)が表示されます。
Web プロキシの概要(Web Proxy Summary)	ネットワーク上のローカル ユーザとリモート ユーザのアクティビティの要約が表示されます。
Total Web Proxy Activity: Local Users	指定した時間(横方向)におけるリモート ユーザのアクティビティ(縦方向)が表示されます。
Suspect Transactions Detected: Remote Users	指定した時間内(横方向)に、リモート ユーザ向けに定義されたアクセス ポリシーによって検出された、疑わしいトランザクション(縦方向)が表示されます。
Suspect Transactions Summary	ネットワーク上のリモート ユーザの疑わしいトランザクションの要約が表示されます。
Suspect Transactions Detected: Local Users	指定した時間内(横方向)に、リモート ユーザ向けに定義されたアクセス ポリシーによって検出された、疑わしいトランザクション(縦方向)が表示されます。
Suspect Transactions Summary	ネットワーク上のローカル ユーザの疑わしいトランザクションの要約が表示されます。

[Web トラッキング（Web Tracking）] ページ

[Web トラッキング（Web Tracking）] ページを使用して、個々のトランザクションまたは疑わしいトランザクションのパターンを検索し、その詳細を取得します。必要に応じて、次のタブのいずれかで検索を行います。

[Web トラッキング（Web Tracking）] ページ	タスクへのリンク
Web プロキシによって処理されたトランザクション（Transactions processed by the Web Proxy）	Web プロキシによって処理されるトランザクションの検索（19-11 ページ）
L4 トラフィック モニタによって処理されたトランザクション（Transactions processed by the L4 Traffic Monitor）	L4 トラフィック モニタによって処理されるトランザクションの検索（19-14 ページ）
SOCKS プロキシによって処理されたトランザクション（Transactions processed by the SOCKS Proxy）	SOCKS プロキシによって処理されるトランザクションの検索（19-14 ページ）

Web プロキシによって処理されるトランザクションの検索

[レポート（Reporting）] > [Web トラッキング（Web Tracking）] ページの [プロキシ サービス（Proxy Services）] タブを使用し、特定のユーザまたはすべてのユーザの Web の使用状況を追跡してレポートできます。

所定の期間内に記録されたトランザクションのタイプ（ブロック、モニタリング、および警告されたトランザクション、完了したトランザクションなど）の検索結果を表示できます。URL カテゴリ、マルウェアの脅威、アプリケーションなど、複数の条件を使用してデータ結果をフィルタリングすることもできます。

（注）　Web プロキシは、「OTHER-NONE」以外の ACL デシジョン タグを含むトランザクションのみレポートします。

ステップ 1　[レポート（Reporting）] > [Web トラッキング（Web Tracking）] を選択します。

ステップ 2　[プロキシ サービス（Proxy Services）] タブをクリックします。

ステップ 3　設定項目を設定します。

設定	説明
時間範囲（Time Range）	レポート対象の時間範囲を選択します。
ユーザ/クライアント IP	（任意）レポートに表示される認証ユーザ名、または追跡対象のクライアント IP アドレスを入力します。IP 範囲を CIDR 形式で入力することもできます。 このフィールドを空にしておくと、すべてのユーザに関する検索結果が返されます。

設定	説明
Web サイト	（任意）追跡対象の Web サイトを入力します。このフィールドを空にしておくと、すべての Web サイトに関する検索結果が返されます。
トランザクション タイプ（Transaction Type）	追跡対象のトランザクションのタイプを [すべてのトランザクション（All Transactions）]、[完了したもの（Completed）]、[ブロック対象（Blocked）]、[モニタ対象（Monitored）]、または [警告対象（Warned）] から選択します。

ステップ 4　（任意）[詳細設定（Advanced）] セクションを展開してフィールドを設定し、より詳細な条件で Web トラッキングの結果をフィルタリングします。

設定	説明
URL Category	URL カテゴリでフィルタリングするには、[URL カテゴリ別フィルタ（Filter by URL Category）] を選択し、フィルタリング対象とする URL カテゴリの先頭文字を入力します。表示されたリストからカテゴリを選択します。
Application	アプリケーションでフィルタリングするには、[アプリケーション別フィルタ（Filter by Application）] を選択し、フィルタリングに使用するアプリケーションを選択します。 アプリケーション タイプでフィルタリングするには、[アプリケーション タイプ別フィルタ（Filter by Application Type）] を選択し、フィルタリングに使用するアプリケーション タイプを選択します。
ポリシー	このトランザクションに対して最終決定を行うポリシーの名前でフィルタするには、[アクション ポリシーによってフィルタ（Filter by Action Policy）] を選択し、フィルタリングに使用するポリシー グループ名（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）を入力します。詳細については、アクセス ログ ファイル（21-15 ページ）の `PolicyGroupName` に関する説明を参照してください。
高度なマルウェア防御（Advanced Malware Protection）	Web トラッキング機能および高度なマルウェア防御機能について（14-11 ページ）を参照してください。
Malware Threat	特定のマルウェアの脅威でフィルタリングするには、[マルウェア脅威でフィルタ（Filter by Malware Threat）] を選択し、フィルタリングに使用するマルウェアの脅威名を入力します。 マルウェア カテゴリでフィルタリングするには、[マルウェア カテゴリ別フィルタ（Filter by Malware Category）] を選択し、フィルタリングに使用するマルウェア カテゴリを選択します。

（続き）

設定	説明
WBRS	[WBRS] セクションでは、Web レピュテーション スコアによるフィルタリングと、特定の Web レピュテーションの脅威によるフィルタリングが可能です。 • Web レピュテーション スコアでフィルタリングするには、[スコア範囲（Score Range）] を選択し、フィルタリングに使用する上限値と下限値を選択します。あるいは、[スコアなし（No Score）] を選択すると、スコアがない Web サイトをフィルタリングできます。 • Web レピュテーションの脅威でフィルタリングするには、[レピュテーション脅威別フィルタ（Filter by Reputation Threat）] を選択し、フィルタリングに使用する Web レピュテーションの脅威を入力します。
AnyConnect セキュア モビリティ	ユーザの場所（リモートまたはローカル）によってフィルタリングするには、[ユーザの場所でフィルタ（Filter by User Location）] を選択し、フィルタリングするユーザ タイプを選択します。
User Request	クライアントによって開始されたトランザクションでフィルタリングするには、[ユーザが要求したトランザクションによるフィルタ（Filter by User-Requested Transactions）] を選択します。 **（注）** このフィルタをイネーブルにすると、検索結果に「最も想定される」トランザクションが含まれることがあります。

ステップ 5　[検索（Search）] をクリックします。

結果はタイム スタンプでソートされ、最新の結果が最上部に表示されます。

[詳細の表示（Display Details）] リンクの下のカッコ内の数値は、ロードされたイメージ、実行された JavaScript、アクセスされたセカンダリ サイトなど、ユーザが開始したトランザクションによって発生した関連トランザクションの数を示しています。

ステップ 6　（任意）[トランザクション（Transactions）] 列の [詳細の表示（Display Details）] をクリックし、各トランザクションに関する詳細情報を表示します。

（注） 1000 件を超える結果を表示する場合は、[印刷可能なダウンロード（Printable Download）] リンクをクリックすると、関連トランザクションの詳細以外の raw データ一式が含まれた CSV ファイルを取得できます。

ヒント　URL が短縮されている場合は、アクセス ログで完全な URL を確認できます）。

500 件までの関連トランザクションの詳細を表示するには、[関連トランザクション（Related Transactions）] リンクをクリックします。

関連項目

- URL カテゴリ セットの更新とレポート（19-5 ページ）
- マルウェアのカテゴリについて（13-17 ページ）
- Web トラッキング機能および高度なマルウェア防御機能について（14-11 ページ）

L4 トラフィック モニタによって処理されるトランザクションの検索

[レポート(Reporting)] > [Web トラッキング(Web Tracking)] ページの [L4 トラフィック モニタ(L4 Traffic Monitor)] タブには、マルウェア サイトおよびポートへの接続に関する詳細情報が表示されます。マルウェア サイトへの接続は、次のタイプの情報によって検索できます。

- 時間範囲
- サイト、使用された IP アドレスまたはドメイン
- [ポート(Port)]
- 組織内のコンピュータに関連付けられた IP アドレス
- 接続タイプ

一致した検索結果のうち最初の 1000 件が表示されます。

SOCKS プロキシによって処理されるトランザクションの検索

ブロックまたは完了したトランザクション、ユーザ、および宛先ドメイン、IP アドレス、またはポートなど含む、さまざまな基準を満たすトランザクションを検索できます。

ステップ 1　[Web] > [レポート(Reporting)] > [Web トラッキング(Web Tracking)] を選択します。

ステップ 2　[SOCKS プロキシ(SOCKS Proxy)] タブをクリックします。

ステップ 3　結果をフィルタリングするには、[詳細(Advanced)] をクリックします。

ステップ 4　検索条件を入力します。

ステップ 5　[検索(Search)] をクリックします。

関連項目

- [SOCKS プロキシ(SOCKS Proxy)] ページ(19-10 ページ)

[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、次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	• 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。 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、効率的に稼動しているシステムの 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	• 1 秒あたりのトランザクション • Bandwidth • 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：フォワードまたはトランスペアレント。 • IP スプーフィング：イネーブルまたはディセーブル。 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（19-14 ページ）

非標準ポートでの不正トラフィックの検出

不正トラフィックの検出の概要

Web セキュリティ アプライアンスは、すべてのネットワーク ポート全体にわたって不正なトラフィックを検出し、マルウェアがポート 80 をバイパスしようとするのを阻止する統合レイヤ 4 トラフィック モニタを備えています。内部クライアントがマルウェアに感染し、標準以外のポートとプロトコルを介して Phone Home を試みた場合、L4 トラフィック モニタは Phone Home アクティビティが企業ネットワークから外部に発信されるのを阻止します。デフォルトでは、L4 トラフィック モニタがイネーブルになり、すべてのポートでトラフィックをモニタするように設定されます。これには、DNS やその他のサービスが含まれます。

L4 トラフィック モニタは、独自の内部データベースを使用し、保持します。このデータベースは、IP アドレスとドメイン名の一致した結果によって継続的に更新されます。

L4 トラフィック モニタの設定

はじめる前に

- ファイアウォールの内側に L4 トラフィック モニタを設定します。
- L4 トラフィック モニタが、プロキシ ポートの後ろ、かつクライアント IP アドレスのネットワーク アドレス変換（NAT）を実行する任意のデバイスの前に、「論理的に」接続されていることを確認します。

ステップ 1	グローバル設定項目を設定する	L4 トラフィック モニタのグローバル設定 (20-2 ページ) を参照してください。
ステップ 2	L4 トラフィック モニタのポリシーを作成する	不正トラフィック検出ポリシーの作成 (20-3 ページ) を参照してください。

既知のサイトのリスト

アドレス	説明
既知の許可アドレス（Known allowed）	[許可リスト（Allow List）] プロパティに記載されている IP アドレスまたはホスト名。これらのアドレスは、「ホワイトリスト」アドレスとしてログ ファイルに表示されます。
未記載（Unlisted）	マルウェア サイトであるか既知の許可アドレスであるかが不明な IP アドレス。これらは、[許可リスト（Allow List）] や [追加するサスペクト マルウェア アドレス（Additional Suspected Malware Addresses）] プロパティに記載されておらず、L4 トラフィック モニタ データベースにも含まれていません。これらのアドレスはログ ファイルに表示されません。
不明瞭なアドレス（Ambiguous）	これらは「グレーリスト」アドレスとしてログ ファイルに表示され、次のアドレスが該当します。 – リストに記載されていない*ホスト名*と既知のマルウェアの*ホスト名*の両方に関連付けられている *IP アドレス*。 – リストに記載されていない*ホスト名*と [追加するサスペクト マルウェア アドレス（Additional Suspected Malware Addresses）] プロパティに含まれる*ホスト名*の両方に関連付けられている *IP アドレス*。
既知のマルウェア（Known malware）	これらは「ブラックリスト」アドレスとしてログ ファイルに表示され、次のアドレスが該当します。 – L4 トラフィック モニタ データベースで既知のマルウェア サイトと判定され、[許可リスト（Allow List）] に*記載されていない* IP アドレスまたはホスト名。 – [追加するサスペクト マルウェア アドレス（Additional Suspected Malware Addresses）] プロパティに記載され、[許可リスト（Allow List）] リストに*記載されていない*、*不明瞭ではない IP アドレス*。

L4 トラフィック モニタのグローバル設定

ステップ 1　[セキュリティ サービス（Security Services）] > [L4 トラフィック モニタ（L4 Traffic Monitor）] 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　L4 トラフィック モニタをイネーブルにするかどうかを選択します。

ステップ 4　L4 トラフィック モニタをイネーブルにする場合は、モニタ対象のポートを選択します。

- **[すべてのポート（All ports）]。**不正なアクティビティに対して TCP ポート 65535 をすべてモニタします。
- [プロキシ ポートを除くすべてのポート（All ports except proxy ports）]。不正なアクティビティに対して、次のポートを除くすべての TCP ポートをモニタします。
  - [セキュリティ サービス（Security Services）] > [Web プロキシ（Web Proxy）] ページの [プロキシを設定する HTTP ポート（HTTP Ports to Proxy）] プロパティで設定したポート（通常はポート 80）。
  - [セキュリティ サービス（Security Services）] > [HTTPS プロキシ（HTTPS Proxy）] ページの [プロキシを設定する透過 HTTPS ポート（Transparent HTTPS Ports to Proxy）] プロパティで設定したポート（通常はポート 443）。

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）]）。

L4 トラフィック モニタのマルウェア対策ルールのアップデート

ステップ 1　[セキュリティ サービス（Security Services）] > [L4 トラフィック モニタ（L4 Traffic Monitor）] を選択します。

ステップ 2　[今すぐ更新（Update Now）] をクリックします。

不正トラフィック検出ポリシーの作成

L4 トラフィック モニタが実行するアクションは、設定する L4 トラフィック モニタのポリシーに応じて異なります。

ステップ 1　[Web セキュリティ マネージャ（Web Security Manager）] > [L4 トラフィック モニタ（L4 Traffic Monitor）] 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　[L4 トラフィック モニタのポリシーの編集（Edit L4 Traffic Monitor Policies）] ページで、L4 トラフィック モニタのポリシーを設定します。

a. [許可リスト（Allow List）] を**定義します**。

b. [許可リスト（Allow List）] に既知の安全なサイトを追加します。

（注）　[許可リスト（Allow List）] には Web セキュリティ アプライアンスの IP アドレスやホスト名を含めないでください。それらを含めると、L4 トラフィック モニタがトラフィックを一切ブロックしなくなります。

c. **不審なマルウェア アドレス**に対して実行するアクションを決定します。

操作	説明
許可（Allow）	既知の許可されたアドレスおよびリストに未記載のアドレスの発着信トラフィックを常に許可します。
モニタ（Monitor）	次のような状況の下で、トラフィックをモニタします。 – [サスペクト マルウェア アドレスに対するアクション（Action for Suspected Malware Addresses）] オプションが [モニタ（Monitor）] に設定されている場合、既知の許可されたアドレスのすべての着発信トラフィックを常にモニタします。 – [サスペクト マルウェア アドレスに対するアクション（Action for Suspected Malware Addresses] オプションが [ブロック（Block）] に設定されている場合、不明瞭なアドレスのすべての着発信トラフィックをモニタします。
ブロック	[サスペクト マルウェア アドレスに対するアクション（Action for Suspected Malware Addresses] オプションが [ブロック（Block）] に設定されている場合、既知のマルウェア アドレスのすべての着発信トラフィックをブロックします。

（注）　不審なマルウェア トラフィックをブロックすることを選択した場合は、不明瞭なアドレスを常にブロックするかどうかも選択できます。デフォルトでは、不明瞭なアドレスはモニタされます。

（注）　ブロックを実行するように L4 トラフィック モニタを設定する場合は、L4 トラフィック モニタと Web プロキシを同じネットワーク上に設定する必要があります。すべてのクライアントがデータ トラフィック用に設定されたルートにアクセスできることを確認するには、[ネットワーク（Network）] > [ルート（Routes）] ページを使用します。

d. [追加するサスペクト マルウェア アドレス（Additional Suspected Malware Addresses）] プロパティを定義します。

（注）　[追加するサスペクト マルウェア アドレス（Additional Suspected Malware Addresses）] のリストに内部 IP アドレスを追加すると、正当な宛先 URL が L4 トラフィック モニタのレポートにマルウェアとして表示されます。このような誤りを回避するために、[Web セキュリティ マネージャ（Web Security Manager）] > [L4 トラフィック モニタ ポリシー（L4 Traffic Monitor Policies）] ページの [追加するサスペクト マルウェア アドレス（Additional Suspected Malware Addresses）] フィールドに内部 IP アドレスを入力しないでください。

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）]）。

関連項目

- 不正トラフィックの検出の概要（20-1 ページ）
- 有効な形式（20-5 ページ）。

有効な形式

[許可リスト（Allow List）] または [追加するサスペクト マルウェア アドレス（Additional Suspected Malware Addresses）] プロパティにアドレスを追加する場合は、空白カンマを使用して複数のエントリを区切ります。次のいずれかの形式でアドレスを入力できます。

- **IPv4 IP アドレス。**例：IPv4 形式：10.1.1.0。IPv6 形式：2002:4559:1FE2::4559:1FE2
- **CIDR アドレス。**例：10.1.1.0/24。
- **ドメイン名。**例：example.com
- **ホスト名。**例：crm.example.com

L4 トラフィック モニタのアクティビティの表示

S シリーズ アプライアンスは、サマリー統計情報の機能固有のレポートおよびインタラクティブな表示を生成するために、複数のオプションをサポートしています。

モニタリング アクティビティとサマリー統計情報の表示

[レポート（Reporting）] > [L4 トラフィック モニタ（L4 Traffic Monitor）] ページには、モニタリング アクティビティの統計的なサマリーが表示されます。次の表示とレポート ツールを使用して、L4 トラフィック モニタのアクティビティの結果を表示できます。

表示対象	参照先
クライアントの統計	[レポート（Reporting）] > [クライアント アクティビティ（Client Activity）]
マルウェアの統計情報 ポートの統計情報	[レポート（Reporting）] > [L4 トラフィック モニタ（L4 Traffic Monitor）]
L4 トラフィック モニタのログ ファイル	[システム管理（System Administration）] > [ログサブスクリプション（Log Subscriptions）] • trafmon_errlogs • trafmonlogs

（注） Web プロキシが転送プロキシとして設定され、L4 トラフィック モニタがすべてのポートをモニタするように設定されている場合は、プロキシのデータ ポートの IP アドレスが記録され、[レポート（Reporting）] > [クライアント アクティビティ（Client Activity）] ページのクライアント アクティビティ レポートにクライアント IP アドレスとして表示されます。Web プロキシがトランスペアレント プロキシとして設定されている場合は、クライアント IP アドレスが正しく記録され、表示されるように IP スプーフィングを有効にします。

L4 トラフィック モニタのログ ファイルのエントリ

L4 トラフィック モニタ ログ ファイルはモニタリング アクティビティの詳細を記録します。

CHAPTER 21

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 セキュリティ アプライアンスでは、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、次の 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（21-2 ページ）
- ログ ファイルのタイプ（21-3 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（21-2 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（21-8 ページ）
ログ ファイルを表示する	ログ ファイルの表示（21-15 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（21-23 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（21-30 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（21-13 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（21-13 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 セキュリティ アプライアンスでは、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、次の手順に従います。

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
- 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（21-3 ページ）
- ログ サブスクリプションの追加と編集（21-8 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。

次の表は、Web セキュリティ アプライアンスのログ 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。	[いいえ（No）]	[いいえ（No）]
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。 ログ ファイル（14-13 ページ）も参照してください。	[はい（Yes）]	[はい（Yes）]
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。	[はい（Yes）]	[はい（Yes）]
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。	[はい（Yes）]	[はい（Yes）]
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	[はい（Yes）]
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。	[いいえ（No）]	[いいえ（No）]
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。	[はい（Yes）]	[はい（Yes）]
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。	[はい（Yes）]	[はい（Yes）]
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。	[いいえ（No）]	[いいえ（No）]
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。	[いいえ（No）]	[いいえ（No）]
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。	[はい（Yes）]	[はい（Yes）]
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。	[いいえ（No）]	[いいえ（No）]
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。	[いいえ（No）]	[いいえ（No）]
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。	[はい（Yes）]	[はい（Yes）]

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。	[はい（Yes）]	[はい（Yes）]
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。	[いいえ（No）]	[いいえ（No）]
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。	[いいえ（No）]	[はい（Yes）]
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。	[はい（Yes）]	[はい（Yes）]
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。	[いいえ（No）]	[いいえ（No）]
FTP サーバ ログ	FTP を使用して、Web セキュリティ アプライアンス 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。	[はい（Yes）]	[はい（Yes）]
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。	[はい（Yes）]	[はい（Yes）]
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。	[はい（Yes）]	[はい（Yes）]
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）。	[いいえ（No）]	[いいえ（No）]
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。	[はい（Yes）]	[はい（Yes）]
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。	[いいえ（No）]	[いいえ（No）]

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 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。	[いいえ（No）]	[いいえ（No）]
ロギング ログ	ログ管理に関連するエラーを記録します。	[はい（Yes）]	[はい（Yes）]
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。	[いいえ（No）]	[いいえ（No）]
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。	[はい（Yes）]	[はい（Yes）]
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。	[いいえ（No）]	[いいえ（No）]
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。	[いいえ（No）]	[いいえ（No）]
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。	[はい（Yes）]	[はい（Yes）]
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。	[はい（Yes）]	[はい（Yes）]
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。	[はい（Yes）]	[はい（Yes）]
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。	[いいえ（No）]	[はい（Yes）]
レポーティング ログ	レポート生成履歴を記録します。	[はい（Yes）]	[はい（Yes）]
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。	[はい（Yes）]	[はい（Yes）]
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。	[いいえ（No）]	[いいえ（No）]
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。	[はい（Yes）]	[はい（Yes）]

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
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。	[はい(Yes)]	[はい(Yes)]
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。	[はい(Yes)]	[はい(Yes)]
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。	[いいえ(No)]	[いいえ(No)]
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。	[いいえ(No)]	[いいえ(No)]
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。	[はい(Yes)]	[はい(Yes)]
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。	[はい(Yes)]	[はい(Yes)]
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。	[はい(Yes)]	[はい(Yes)]
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。	[はい(Yes)]	[はい(Yes)]
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。	[いいえ(No)]	[はい(Yes)]
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。	[はい(Yes)]	[はい(Yes)]
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。	[はい(Yes)]	[はい(Yes)]
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(21-28 ページ)を参照してください。	[はい(Yes)]	[いいえ(No)]
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。	[いいえ(No)]	[はい(Yes)]

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
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。	[いいえ(No)]	[いいえ(No)]
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。	[いいえ(No)]	[いいえ(No)]
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。	[いいえ(No)]	[いいえ(No)]
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。	[いいえ(No)]	[いいえ(No)]
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。	[はい(Yes)]	[はい(Yes)]
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。	[はい(Yes)]	[はい(Yes)]

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、次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 セキュリティ アプライアンス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。
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、次のとおりです。 • **なし。** 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次のとおりです。
	`<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）。

オプション	説明
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。
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、最新のログ ファイル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: （Retrieval Method:） アプライアンス上の FTP	[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ワードを使用して、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: （Retrieval Method:） リモート サーバ上の FTP	[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、次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ワード **（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: (Retrieval Method:) リモート サーバ上の SCP	[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、次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: (Retrieval Method:) 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、次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 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。

次の手順

- 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(21-13 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(21-3 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(21-14 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（21-8 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. 次のコマンドを使用してキーを表示します。

コマンド	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	説明
新規作成（New）	新しいキーを追加します。
Fingerprint	システム ホスト キーのフィンガープリントを表示します。

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次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（Rollover by Time）
- ログ圧縮（Log Compression）
- 取得方法（Retrieval Method）

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(21-8 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(21-14 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、次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、次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 セキュリティ アプライアンス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(21-15 ページ)。
- アクセス ログ ファイル(21-15 ページ)。
- W3C アクセス ログの解釈(21-28 ページ)。
- トラフィック モニタ ログの解釈(21-32 ページ)。
- ログ ファイルのフィールドとタグ(21-32 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　[管理（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ワードを入力します。

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（21-15 ページ）。
- W3C アクセス ログの解釈（21-28 ページ）。
- トラフィック モニタ ログの解釈（21-32 ページ）。

アクセス ログ ファイル

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。

次のテキストは、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（21-28 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。 次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。 最も一般的な値は次のとおりです。 • **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。
%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（21-19 ページ）を参照してください。

フォーマット指定子	フィールド値	フィールドの説明
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	Outbound Malware Scanning 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（21-23 ページ）およびマルウェア スキャンの判定値（21-43 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。次の表に、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。

次の表は、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_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	Web プロキシが、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をブロックしました。
BLOCK_ADMIN_CONNECT	Web プロキシが、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をブロックしました。
BLOCK_ADMIN_CUSTOM_USER_AGENT	Web プロキシが、アクセス ポリシー グループの 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をブロックしました。
BLOCK_ADMIN_IDS	Web プロキシは、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をブロックしました。
BLOCK_ADMIN_FILE_TYPE	Web プロキシが、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をブロックしました。
BLOCK_ADMIN_PROTOCOL	Web プロキシが、アクセス ポリシー グループの 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をブロックしました。
BLOCK_ADMIN_SIZE	Web プロキシが、アクセス ポリシー グループの 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をブロックしました。
BLOCK_ADMIN_SIZE_IDS	Web プロキシが、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をブロックしました。
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。

ACL デシジョン タグ	説明
BLOCK_AMW_REQ	Web プロキシが、Outbound Malware Scanning 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	Web プロキシが、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をブロックしました。
BLOCK_CONTENT_UNSAFE	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	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。
BLOCK_CONTINUE_CUSTOMCAT	Web プロキシが、[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。
BLOCK_CONTINUE_WEBCAT	Web プロキシが、[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。
BLOCK_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ブロックしました。
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。
BLOCK_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ブロックしました。

ACL デシジョン タグ	説明
BLOCK_UNSUPPORTED_SEARCH_APP	Web プロキシが、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をブロックしました。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	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ブロックしました。
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	Web プロキシが、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をブロックしました。
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_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_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。
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。

ACL デシジョン タグ	説明
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。
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_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。

ACL デシジョン タグ	説明
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。

次のテキストは、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（21-15 ページ）を参照してください。

この例の各要素は、次の表に示すログ 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 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。 URL カテゴリの省略形の一覧については、URL カテゴリについて（9-24 ページ）を参照してください。
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。

位置	フィールド値	フォーマット指定子	説明
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（21-43 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（21-43 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。
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（21-43 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
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見つけたファイルの場所。非アーカイブ ファイルの場合、この値はファイル名だけです。アーカイブ ファイルの場合は、アーカイブ内のオブジェクト（`archive.zip/virus.exe` など）です。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。次のリストは、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 • **-（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。次のリストは、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 • **-（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 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 カテゴリについて（9-24 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	応答側のスキャン時に動的コンテンツ分析エンジンによって決定された URL カテゴリの判定（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 カテゴリについて（9-24 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、アダルト コンテンツ アクセスのロギング（9-17 ページ）を参照してください。
36	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。Outbound Malware Scanning 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 Outbound Malware Scanning 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「ファイル レピュテーション フィルタリングとファイル分析」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 (21-32 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 (21-15 ページ)
- アクセス ログのカスタマイズ (21-30 ページ)。
- W3C 準拠のアクセス ログ ファイル (21-28 ページ)
- ログ ファイルの表示 (21-15 ページ)
- ログ ファイルのフィールドとタグ (21-32 ページ)

W3C 準拠のアクセス ログ ファイル

Web セキュリティ アプライアンスには、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 アクセス ログ）が用意されています。W3C アクセス ログは W3C に準拠しており、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（21-28 ページ）
- W3C アクセス ログの解釈（21-28 ページ）

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。次のいずれかのログ 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（21-28 ページ）
- W3C フィールドのプレフィックス（21-29 ページ）

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 セキュリティ アプライアンス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。

次の表は、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
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。

ヘッダー フィールド	説明
System	ログ ファイルを生成した Web セキュリティ アプライアンス（「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	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。次の表は、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（21-15 ページ）。
- アクセス ログのカスタマイズ（21-30 ページ）。
- トラフィック モニタのログ ファイル（21-32 ページ）。
- ログ ファイルのフィールドとタグ（21-32 ページ）。
- ログ ファイルの表示（21-15 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（21-32 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（21-30 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。

次の表は、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）] ボックスに次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（21-30 ページ）。
- W3C アクセス ログのカスタマイズ（21-31 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次のとおりです。

```
<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（21-15 ページ）。
- ログ ファイルのフィールドとタグ（21-32 ページ）。
- アクセス ログのユーザ定義フィールド（21-30 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、最新のログ ファイル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（21-28 ページ）。
- ログ ファイルのフィールドとタグ（21-32 ページ）。
- アクセス ログのユーザ定義フィールド（21-30 ページ）。

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（21-15 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（21-33 ページ）
- トランザクション結果コード（21-18 ページ）

- ACL デシジョン タグ（21-19 ページ）
- マルウェア スキャンの判定値（21-43 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。

次の表は、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
%:<l	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、これはそ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。
%:>l	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

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
%:>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）。
%:>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）。

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
%: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。
%?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	エラー コード番号。カスタマー サポートでトランザクションの問題をトラブルシューティングするときに参照します。
%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。
%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ワードが必要。 – 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)
%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。
%m	cs-auth-mechanism	トランザクションで使用する認証メカニズム。値は次のとおりです。 • **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)。
%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	Protocol.
%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)。

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
%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。
%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。
%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

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
%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 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 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	要求側のスキャン時に決定された URL カテゴリの判定（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見つけたファイルの場所。非アーカイブ ファイルの場合、この値はファイル名だけです。アーカイブ ファイルの場合、`archive.zip/virus.exe` などのアーカイブ内のオブジェクトです。
%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。

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#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「ファイル レピュテーション フィルタリングとファイル分析」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。
%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（21-15 ページ）。
- W3C アクセス ログの解釈（21-28 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。

次のリストは、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
13	アドウェア
18	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（21-15 ページ）。
- W3C アクセス ログの解釈（21-28 ページ）。

ロギングのトラブルシューティング

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、次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とロード

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ワードをマスクする（Mask passwords 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ワードが「*****」に置き換えられます。ただし、パスワードがマスクされたコンフィギュレーション 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

警告　**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。**

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）

- パスワードがマスクされているファイルはロードできません。
- ファイルには次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。

（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。

機能キーの使用

機能キーによってシステムの特定の機能がイネーブルになります。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（22-14 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。

リモート電源管理のイネーブル化

アプライアンス シャーシの電源をリモートからリセットする機能は、S380 および S680でのみ使用できます。

アプライアンスの電源をリモートでリセットする場合は、このセクションで説明されている手順を使用して、この機能を事前にイネーブルにし、設定しておく必要があります。

はじめる前に

- 専用リモート電源管理ポートをセキュア ネットワークに直接、ケーブル接続します。詳細については、ハードウェア インストレーション ガイドを参照してください。
- ファイアウォールを通過するために必要なポートを開くなど、アプライアンスがリモートアクセス可能であることを確認します。
- この機能では、専用のリモート電源管理インターフェイス用に一意の IPv4 アドレスが必要です。このインターフェイスは、このセクションで説明されている手順でのみ設定可能です。`ipconfig` コマンドを使用して設定することはできません。
- アプライアンスの電源を再投入するには、Intelligent Platform Management Interface（IPMI）バージョン 2.0 をサポートするデバイスを管理できるサードパーティ製ツールが必要です。このようなツールを使用できるように準備されていることを確認します。
- コマンドライン インターフェイスへのアクセスに関する詳細については、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」

手順

ステップ 1　SSH、Telnet、またはシリアル コンソール ポートを使用して、コマンドライン インターフェイスにアクセスします。

ステップ 2　管理者権限を持つアカウントを使用してログインします。

ステップ 3　次のコマンドを入力します。

`remotepower`

セットアップ

ステップ 4　プロンプトに従って、次の情報を指定します。

- この機能専用の IP アドレスと、ネットマスクおよびゲートウェイ。
- 電源の再投入コマンドを実行するために必要なユーザ名とパスワード。

  これらのクレデンシャルは、アプライアンスへのアクセスに使用する他のクレデンシャルに依存しません。

ステップ 5　`commit` を入力して変更を保存します。

ステップ 6　設定をテストして、アプライアンスの電源をリモートで管理できることを確認します。

ステップ 7　入力したクレデンシャルが、将来、いつでも使用できることを確認します。たとえば、この情報を安全な場所に保管し、このタスクを実行する必要がある管理者が、必要なクレデンシャルにアクセスできるようにします。

関連項目

- 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-18 ページ）

ユーザ アカウントの管理

次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（22-6 ページ）。
- RADIUS ユーザ認証（22-8 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 パスワードを変更できますが、このアカウントを編集または削除できません。

（注）　admin ユーザ パスワードを紛失した場合は、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ワード要件を定義します。管理ユーザのパスワード要件の設定（22-11 ページ）を参照してください。

手順

ステップ 1　[システム管理（System Administration）] > [ユーザ（Users）] を選択します。

ステップ 2　[ユーザの追加（Add User）] をクリックします。

ステップ 3　次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。
オペレータ（Operator）	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、次の 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
読み取り専用オペレータ（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（Guest）	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　パスワードを入力するか、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。

パスワードの変更

現在ログインしているアカウントのパスワードを変更するには、ウィンドウの右上で、[オプション（Options）] > [パスワードの変更（Change Password）] 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ワードを変更します。

関連項目

- ユーザ アカウントの編集（22-8 ページ）
- 管理ユーザのパスワード要件の設定（22-11 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次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ワードを入力した場合は、アプライアンスへのアクセスが拒否されます。

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 パスワードを入力します。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 パスワード（たとえば、トークンから作成されるパスワード）を使用する場合、ゼロ（0）を入力します。値をゼロに設定すると、AsyncOS は、現在のセッション中に認証のために RADIUS サーバに再アクセスしません。

ステップ 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
Map externally authenticated users to multiple local roles.	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） • オペレータ（Operator） • 読み取り専用オペレータ（Read-Only Operator） • ゲスト（Guest）
Map all externally authenticated users to the Administrator role.	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（External Authentication）（5-11 ページ）
- ローカル ユーザ アカウントの追加（22-6 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
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。
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。
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。
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

管理ユーザのパスワード要件の設定

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ワード要件を設定するには、次の手順を実行します。

手順

ステップ 1　[システム管理（System Administration）] > [ユーザ（Users）] を選択します。

ステップ 2　[パスワードの設定（Password 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　次のオプションから選択します。

オプション	説明
パスワードで許可しない単語の一覧（List of words to disallow in passwords）	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
パスワードの強度（Password Strength）	管理ユーザが新しいパスワードを入力するときに、パスワード強度インジケータを表示できます。 この設定は強固なパスワードの作成を強制するものではありません。入力されたパスワードがどの程度簡単に推測されるかを示すだけです。 インジケータを表示するロールを選択します。次に、選択した各ロールに対して、0 よりも大きい数値を入力します。数値が大きいほど、強力なパスワードとして登録されたパスワードが推測困難であることを意味します。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パスワードの作成が非常に困難になります。 いくつかの数値を試して最適な値を見つけてください。 パスワード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、強固なパスワードは次のような特徴を備えています。 • 長い • 大文字、小文字、数字、特殊文字が含まれている • どのような言語であれ辞書にある単語が含まれていない このような特徴を持つパスワードを強制するには、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	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	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。

管理者パスワードのリセット

すべての管理者レベルのユーザは、「admin」ユーザのパスワードを変更できます。

はじめる前に

- admin アカウントのパスワードが不明な場合は、カスタマー サポート プロバイダーに連絡してパスワードをリセットしてください。
- パスワード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　[admin] リンクを選択します。

ステップ 3　[パスワード（Password）] フィールドと [パスワード再入力（Retype Password）] フィールドに新しいパスワードを入力します。

生成されたメッセージの返信アドレスの設定

レポート用に AsyncOS によって生成されたメールの返信アドレスを設定できます。

ステップ 1　[システム管理（System Administration）] > [返信先アドレス（Return Addresses）] 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　表示名、ユーザ名、およびドメイン名を入力します。

ステップ 4　変更を送信し、保存します。

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 は次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。

- Critical：ただちに対処する必要があります。
- Warning：今後モニタリングが必要な問題またはエラー。すぐに対処が必要な場合もあります。
- Information：デバイスのルーティン機能で生成される情報。

アラート受信者の管理

（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。

オプション	説明
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。この増加は、待機する秒数に、直前の間隔の 2 倍を加えたものになります。つまり、この値を 5 秒に設定すると、アラートは 5 秒後、15 秒後、35 秒後、75 秒後、155 秒後、315 秒後といった間隔で送信されます。 [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。
Cisco AutoSupport	シスコに次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

次の項では、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（critical、information、または warning）およびメッセージのテキストに含まれるパラメータ（存在する場合）が含まれています。

機能キー アラート

次の表は、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 “$feature” key was downloaded from the key server and placed into the pending area. EULA acceptance required.	Information。	**$feature**：機能の名前。
Your “$feature” evaluation key has expired. Please contact your authorized sales representative.	Warning。	**$feature**：機能の名前。
Your “$feature” evaluation key will expire in under $days day(s). Please contact your authorized sales representative.	Warning。	**$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

次の表は、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: $error	警告	**$error**：RAID エラーのテキスト。

ロギング アラート

次の表は、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
$error.	Information。	**$error**：エラーのトレースバック文字列。
Log Error: Subscription $name: Log partition is full.	Critical。	**$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: $reason.	Critical。	**$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: $reason.	Critical。	**$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: $reason',	Critical。	**$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。

メッセージ	アラートの重大度	パラメータ
Log Error: 'Subscription $name: Failed to connect to $hostname ($ip): $error.	Critical。	**$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): $error	Critical。	**$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).	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.	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: $files_removed.	Information。	**$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

次の表は、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.	Critical。	適用なし
The reporting system is now able to handle new data.	Information。	適用なし
A failure occurred while building periodic report ‘$report_title’. This subscription should be examined and deleted if its configuration details are no longer valid.	Critical。	**$report_title**：レポートのタイトル。
A failure occurred while emailing periodic report ‘$report_title’. This subscription has been removed from the scheduler.	Critical。	**$report_title**：レポートのタイトル。

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 $threshold percent, full processing of reporting data will be restarted automatically.	Warning。	**$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.	Critical。	**$report_title**：レポートのタイトル。 **$file_name**：ファイルの名前。
Counter group "$counter_group" does not exist.	Critical。	**$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.	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. $error_text	Critical。	**$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。
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 $threshold percent, full processing of reporting data will be restarted automatically.	Warning。	**$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: $err_msg	Critical。	**$err_msg**：エラー メッセージ テキスト。

システム アラート

次の表は、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: $message	Critical。	**$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: $output',	Critical。	**$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: $output	Critical。	**$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 $dependency as a dependency, but it does not exist.	Critical。	**$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 $dependency is not a wait_init process.	Critical。	**$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 $name listed itself as a dependency.	Critical。	**$name**：プロセスの名前。
Process $name listed $dependency as a dependency multiple times.	Critical。	**$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: $cycle.	Critical。	**$cycle**：サイクルに関係するプロセス名のリスト。
An error occurred while attempting to share statistical data through the Network Participation feature. Please forward this tracking information to your support provider: Error: $error.	Warning。	**$error**：例外に関連付けられたエラー メッセージ。
There is an error with “$name”.	Critical。	**$name**：コア ファイルを生成したプロセスの名前。
An application fault occurred: “$error”	Critical。	**$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 $port	Information。	**$port**：サービス トンネルに使用されるポート番号。

メッセージ	アラートの重大度	パラメータ
Tech support: Service tunnel has been disabled.	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 $ip has been removed from the blacklist	Warning。	**$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 10 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 アドレスからのユーザ ログインが成功した場合、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。 1 日が経過すると、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

次の表は、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 $attempts times to successfully complete an update. This may be due to a network configuration issue or temporary outage.	Warning。	**$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 $threshold.	Warning。	**$threshold:**：しきい値の時間。
Unknown error occurred: $traceback.	Critical。	**$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、アラートの受信の確認（14-8 ページ）を参照してください。

FIPS の準拠性

Federal Information Processing Standard（FIPS）は、機密情報であるが機密扱いされていない情報を保護するために、すべての政府機関で使用される暗号化モジュールの要件を規定しています。FIPS は、連邦政府のセキュリティとデータ プライバシー要件の遵守を確実にするために役立ちます。国立標準技術研究所（NIST）によって開発された FIPS は、連邦政府の要件を満たす任意の規格がない場合に使用されます。

WSA は Cisco Common Cryptographic Module(C3M)を使用して FIPS モードの FIPS 140-2 レベル 1 準拠を実現します。デフォルトでは、FIPS モードはディセーブルです。

FIPS 証明書の要件

FIPS モードでは、Web セキュリティ アプライアンスでイネーブルになっているすべての暗号化サービスについて FIPS 準拠の証明書を使用する必要があります。これは、次の暗号化サービスに適用されます。

- HTTPS プロキシ（HTTPS Proxy）
- 認証
- SaaS のアイデンティティ プロバイダー（Identity Provider for SaaS）
- アプライアンス管理 HTTPS サービス

（注） アプライアンス管理 HTTPS サービスは、FIPS モードを有効にする前にイネーブルにする必要があります。他の暗号化サービスはイネーブルにする必要はありません。

FIPS 準拠の証明書は次の要件を満たす必要があります。

証明書	アルゴリズム（SNMP (v3) Auth. Alrorithm）	ビット キー サイズ	署名アルゴリズム	注記
X509	RSA	1024、2048、3072、または 4096	sha1WithRSAEncryption	最適な復号化パフォーマンスと十分なセキュリティを実現するために、1024 ビットのキーサイズを推奨します。ビットサイズをさらに大きくすると、セキュリティは向上しますが、復号化のパフォーマンスに影響します。
	DSA	1024	dsaWithSHA1	

FIPS モードのイネーブル化/ディセーブル化

はじめる前に

- FIPS モードで使用される証明書で、FIPS 140-2 認定の公開キー アルゴリズムが使用されていることを確認します（FIPS 証明書の要件（22-22 ページ）を参照）。

（注） FIPS モードを変更すると、アプライアンスが再起動されます。

ステップ 1　[システム管理（System Administration）] > [FIPS モード（FIPS Mode）] 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　[FIPS レベル 1 準拠を有効にする（Enable FIPS Level 1 Compliance）] チェックボックスをオンまたはオフにします。

ステップ 4　[送信（Submit）] をクリックします。

ステップ 5　[続行（Continue）] をクリックして、アプライアンスの再起動を許可します。

システムの日時の管理

Web セキュリティ アプライアンスは、ネットワーク タイム プロトコル（NTP）サーバを照会することで現在の日時を追跡できます。または、手動でシステムの日時を設定できます。システムの日時は、GMT オフセットまたはグローバル地域、国、およびローカル タイム ゾーンで設定できるタイム ゾーンを反映しています。

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

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。

設定から NTP サーバを削除します。

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　サーバ名の右側にあるゴミ箱アイコンをクリックして、削除します。

ステップ 4　変更を送信し、保存します。

手動による GUI でのシステムの日時の設定

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　[時刻を手動で設定（Set Time Manually）] オプション ボタンをクリックします。

ステップ 3　日時を設定します。

ステップ 4　[実行（Submit）] をクリックします。

SSL の設定

セキュリティを強化するために、複数のサービスに対して SSLv3 をイネーブルまたはディセーブルにできます。SSLv3 がディセーブルになっているサービスは TLSv1.0 を使用します。

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　対応するチェックボックスをオンにして、次のサービスに対して SSLv3 をイネーブルにします。

- [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。
- [セキュア LDAP サービス（Secure LDAP Services）]：認証、外部認証、SaaS SSO、およびセキュア モビリティが含まれます。
- **[アップデート サービス（Update Service）]**

ステップ 4　[送信（Submit）] をクリックします。

（注）　これらの機能は、`sslv3config` 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。

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（22-25 ページ）
- 証明書の更新（22-25 ページ）
- 信頼できるルート証明書の管理（22-25 ページ）
- ブロックされた証明書の表示（22-26 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（22-26 ページ）
- 証明書署名要求（22-27 ページ）
- 中間証明書（22-28 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、次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、次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、次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、次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、次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

一部の AsyncOS 機能では、接続の確立、確認、または保護のために証明書とキーが必要です。たとえば、Identity Services Engine（ISE）や Identity Provider for SaaS などの機能がこれに該当します。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、次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（22-27 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（22-25 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、次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。

AsyncOS for Web をアップグレードするためのベスト プラクティス

- アップグレードを開始する前に、[システム管理（System Administration）] >; [設定ファイル（Configuration File）] ページまたは saveconfig コマンドを使用して、Web セキュリティ アプライアンスから XML コンフィギュレーション ファイルを保存します。
- PAC ファイルやカスタマイズしたエンドユーザ通知ページなど、アプライアンスに格納されている他のファイルを保存します。
- アップグレード時には、さまざまなプロンプトで長い時間作業を中断しないでください。TCP セッションがダウンロード中にタイムアウトしてしまった場合、アップグレードが失敗する可能性があります。
- アップグレードが完了したら、XML ファイルに設定情報を保存します。

関連項目

- アプライアンス設定の保存とロード（22-2 ページ）。

AsyncOS およびセキュリティ サービス コンポーネントのアップグレードとアップデート

AsyncOS for Web のアップグレード

はじめる前に

- アプライアンスのコンフィギュレーション ファイルを保存します（アプライアンス設定の保存とロード（22-2 ページ）を参照）。

ステップ 1　[システム管理（System Administration）] > [システム アップグレード（System Upgrade）] を選択します。

ステップ 2　[使用可能なアップグレード（Available Upgrades）] をクリックします。

ステップ 3　入手可能なアップグレードのリストからアップグレードを選択して、[アップグレード開始（Begin Upgrade）] をクリックし、アップグレード プロセスを開始します。表示される質問に答えます。

ステップ 4　アップグレードが完了したら、Web セキュリティ アプライアンスを再起動するには、[今すぐ再起動（Reboot Now）] をクリックします。

関連項目

- ローカルおよびリモート アップデート サーバ（22-30 ページ）。

自動および手動によるアップデート/アップグレードのクエリー

AsyncOS は、新しい AsyncOS アップグレードを除く、すべてのセキュリティ サービス コンポーネントへの新しいアップデートがないか、定期的にアップデート サーバに問い合わせます。AsyncOS をアップグレードするには、AsyncOS が使用可能なアップグレードを問い合わせるよう、手動で要求する必要があります。AsyncOS が使用可能なセキュリティ サービス アップデートを問い合わせるよう、手動で要求することもできます。詳細については、以前のバージョンの AsyncOS for Web への復元（22-34 ページ）を参照してください。

AsyncOS がアップデートまたはアップグレードのアップデート サーバを照会する場合は、次の手順を実行します。

1. アップデート サーバに問い合わせます。

   シスコでは、アップデート サーバに次のソースを使用できます。

   - **Cisco アップデート サーバ。**詳細については、Cisco アップデート サーバからのアップデートとアップグレード（22-31 ページ）を参照してください。
   - **ローカル サーバ。**詳細については、ローカル サーバからのアップグレード（22-31 ページ）を参照してください。
2. 入手可能なアップデートまたは AsyncOS のアップグレード バージョンを一覧表示する XML ファイルを受信します。この XML ファイルは「マニフェスト」と呼ばれます。
3. アップデートまたはアップグレード イメージ ファイルをダウンロードします。

セキュリティ サービスのコンポーネントの手動による更新

デフォルトでは、各セキュリティ サービス コンポーネントは、Cisco アップデート サーバからデータベース テーブルに定期的にアップデートを受信します。ただし、手動でデータベース テーブルを更新できます。

（注）　一部のアップデートは、機能に関連した GUI ページからオンデマンド単位で利用できます。

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　[更新設定を編集（Edit Update Settings）] をクリックします。

ステップ 3　アップデート ファイルの場所を指定します。

ステップ 4　[セキュリティ サービス（Security Services）] タブにあるコンポーネント ページの [今すぐ更新（Update Now）] 機能キーを使用してアップデートを開始します。たとえば、[セキュリティ サービス（Security Services）] > [Web レピュテーション フィルタ（Web Reputation Filters）] ページです。

（注）　処理中のアップデートは中断できません。すべての処理中のアップデートは、新しい変更が適用される前に完了する必要があります。

ヒント　アップデータ ログ ファイルのアップデート アクティビティの記録を表示してください。[システム管理（System Administration）] > [ログ サブスクリプション（Log Subscriptions）] ページのアップデータ ログ ファイルに登録します。

ローカルおよびリモート アップデート サーバ

デフォルトでは、AsyncOS は、アップデート イメージとアップグレード イメージおよびマニフェスト XML ファイルについて、Cisco アップデート サーバに問い合わせます。ただし、ユーザは、アップグレード イメージやアップデート イメージおよびマニフェスト ファイルのダウンロード元を選択できます。次の理由から、イメージ ファイルまたはマニフェスト ファイルにローカル アップデート サーバを使用します。

- **同時にアップグレードするアプライアンスが複数あります。**ネットワーク内の Web サーバにアップグレード イメージをダウンロードして、ネットワーク内のすべてのアプライアンスに使用できます。
- **ファイアウォールの設定には、Cisco アップデート サーバのスタティック IP アドレスが必要です。**Cisco アップデート サーバは、ダイナミック IP アドレスを使用します。ファイアウォール ポリシーを厳しく設定している場合、アップデートおよび AsyncOS アップグレードに対して静的な参照先を設定する必要がある場合があります。詳細については、Cisco アップデート サーバのスタティック アドレスの設定（22-31 ページ）を参照してください。

（注）　ローカル アップデート サーバはセキュリティ サービスのアップデートを自動的に受信しません。AsyncOS のアップグレードのみを受信します。AsyncOS のアップグレードにローカル アップデート サーバを使用した後は、アップデートとアップグレードの設定を変更して、再び Cisco アップデート サーバを使用するようにします。これにより、セキュリティ サービスが再び自動的にアップデートされるようになります。

Cisco アップデート サーバからのアップデートとアップグレード

Web セキュリティ アプライアンスは、Cisco アップデート サーバに直接接続して、アップグレード イメージとセキュリティ サービス アップデートをダウンロードできます。各アプライアンスは、個別にアップデートとアップグレードをダウンロードします。

Cisco アップデート サーバのスタティック アドレスの設定

Cisco アップデート サーバは、ダイナミック IP アドレスを使用します。ファイアウォール ポリシーを厳しく設定している場合、アップデートおよび AsyncOS アップグレードに対して静的な参照先を設定する必要がある場合があります。

ステップ 1　シスコ カスタマー サポートに問い合わせて、スタティック URL アドレスを取得します。

ステップ 2　[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）] ページの順に進み、[更新設定を編集（Edit Update Settings）] をクリックします。

ステップ 3　[アップデート設定を編集（Edit Update Settings）] ページの [アップデート サーバ（イメージ）（Update Servers (images)）] セクションで、[ローカル アップデート サーバ（Local Update Servers）] を選択し、ステップ 1 で取得したスタティック URL アドレスを入力します。

ステップ 4　[アップデート サーバ（リスト）（Update Servers (list)）] セクションで Cisco アップデート サーバが選択されていることを確認します。

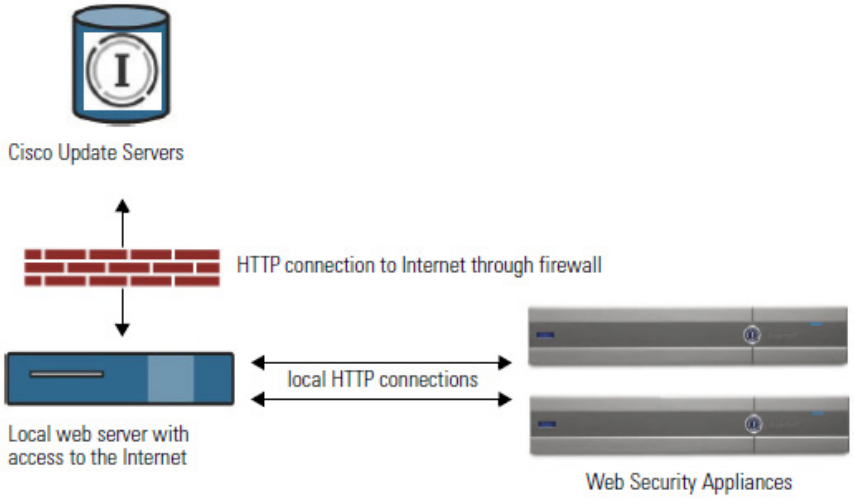
ステップ 5　変更を送信し、保存します。

ローカル サーバからのアップグレード

Web セキュリティ アプライアンスは、Cisco アップデート サーバからアップグレードを直接取得する代わりに、ネットワーク内のサーバから AsyncOS のアップグレードをダウンロードできます。この機能を使用すると、シスコから 1 回だけアップグレード イメージをダウンロードして、ネットワーク内のすべての Web セキュリティ アプライアンスでそれを使用することができます。

図 22-1 は、Web セキュリティ アプライアンスがローカル サーバからアップグレード イメージをダウンロードする方法を示します。

図 22-1　　ローカル サーバからのアップグレード



ローカル アップグレード サーバのハードウェアおよびソフトウェア要件

AsyncOS アップグレード ファイルをダウンロードする場合は、Web ブラウザと Cisco アップデート サーバへのインターネット アクセス機能を備えたシステムを、内部ネットワーク内に用意する必要があります。

（注）　このアドレスへの HTTP アクセスを許可するファイアウォール設定値を設定する必要がある場合、特定の IP アドレスではなく DNS 名を使用して設定する必要があります。

AsyncOS アップグレード ファイルのホスティングでは、内部ネットワーク上のサーバは、次の機能を持つ Microsoft IIS（Internet Information Services）などの Web サーバまたは Apache のオープン ソース サーバを持つ必要があります。

- 24 文字を超えるディレクトリまたはファイル名の表示をサポートしていること
- ディレクトリの参照ができること
- 匿名（認証なし）または基本（「簡易」）認証用に設定されている
- 各 AsyncOS アップデート イメージ用に最低 350 MB 以上の空きディスク領域が存在すること

ローカル サーバからのアップグレードの設定

ステップ 1　アップグレード ファイルを取得および供給するようにローカル サーバを設定します。

ステップ 2　アップグレード zip ファイルをダウンロードします。

ローカル サーバのブラウザを使用して、`http://updates.ironport.com/fetch_manifest.html` に進み、アップグレード イメージの zip ファイルをダウンロードします。イメージをダウンロードするには、シリアル番号（物理アプライアンス用）または VLN（仮想アプライアンス用）およびアプライアンスのバージョン番号を入力します。利用可能なアップグレードのリストが表示されます。ダウンロードするアップグレード バージョンをクリックします。

ステップ 3　ディレクトリ構造を変更せずにローカル サーバのルート ディレクトリにある ZIP ファイルを解凍します。

ステップ 4　[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）] ページまたは `updateconfig` コマンドを使用して、ローカル サーバを使用するようにアプライアンスを設定します。

ステップ 5　[システム管理（System Administration）] > [システム アップグレード（System Upgrade）] ページで、[使用可能なアップグレード（Available Upgrades）] をクリックするか、`upgrade` コマンドを実行します。

（注）　アップグレードの完了後にセキュリティ サービス コンポーネントが引き続き自動更新されるように、アップデートとアップグレードの設定を変更して、Cisco アップデート サーバ（ダイナミックまたはスタティック アドレスを使用）を使用することを推奨します。

ローカルとリモートにおけるアップグレード方法の相違

次の相違点は、Cisco アップデート サーバからではなく、ローカル サーバから AsyncOS をアップグレードする場合に該当します。

1. *ダウンロード中に*、アップグレードによるインストールがすぐに実行されます。
2. アップグレード プロセスの開始時に、バナーが 10 秒間表示されます。このバナーが表示されている間は、Control を押した状態で C を押すと、ダウンロードの開始前にアップグレード プロセスを終了できます。

アップグレードおよびサービス アップデートの設定の変更

Web セキュリティ アプライアンスがセキュリティ サービス アップデートや AsyncOS for Web のアップグレードをダウンロードする方法を設定できます。たとえば、ファイルをダウンロードするときに使用するネットワーク インターフェイスを選択したり、アップデート間隔を設定したり、自動アップデートをディセーブルにしたりできます。

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　[更新設定を編集（Edit Update Settings）] をクリックします。

ステップ 3　次の情報を参考にして、設定値を設定します。

設定	説明
Automatic Updates	セキュリティ コンポーネントの自動アップデートをイネーブルにするかどうかを選択します。自動更新を選択する場合、時間間隔を入力します。デフォルトはイネーブルで、更新間隔は 5 分です。
Upgrade Notifications	AsyncOS への新規のアップグレードが入手可能である場合に、Web インターフェイスの上部に通知を表示するかどうかを選択します。アプライアンスは、管理者に対してのみこの通知を表示します。 詳細については、AsyncOS for Web のアップグレード（22-28 ページ）を参照してください。

設定	説明
Update Servers (list)	利用可能なアップグレードとアップデートのリスト（マニフェスト XML ファイル）を、Cisco アップデート サーバまたはローカル Web サーバのどちらからダウンロードするかを選択します。 ローカル アップデート サーバを選択した場合、サーバのファイル名およびポート番号を含む、リストのマニフェスト XML ファイルの完全なパスを入力します。ポートのフィールドを空のままにした場合、AsyncOS はポート 80 を使用します。サーバが認証を必要とする場合、有効なユーザ名とパスワードも入力します。
Update Servers (images)	アップグレード イメージやアップデート イメージを、Cisco アップデート サーバまたはローカル Web サーバのどちらからダウンロードするかを選択します。 ローカル アップデート サーバを選択した場合は、サーバのベース URL とポート番号を入力します。ポートのフィールドを空のままにした場合、AsyncOS はポート 80 を使用します。サーバが認証を必要とする場合、有効なユーザ名とパスワードも入力します。
着信サービス一覧（Routing Table）	アップデート サーバに接続するときに、どのネットワーク インターフェイスのルーティング テーブルを使用するかを選択します。
Proxy Server（オプション）	アップストリームのプロキシ サーバが存在し、認証が必要な場合は、サーバ情報、ユーザ名、およびパスワードをここに入力します。

ステップ 4　変更を送信し、保存します。

関連項目

- ローカルおよびリモート アップデート サーバ（22-30 ページ）。
- 自動および手動によるアップデート/アップグレードのクエリー（22-29 ページ）。
- AsyncOS およびセキュリティ サービス コンポーネントのアップグレードとアップデート（22-28 ページ）。

以前のバージョンの AsyncOS for Web への復元

Web 用 AsyncOS には、緊急時に Web 用オペレーティング システム AsyncOS を以前の認定済みのビルドに戻す機能があります。

（注）　バージョン 7.5 よりも前の Web 用 AsyncOS のバージョンには戻せません。

仮想アプライアンスの AsyncOS を復元した場合のライセンスへの影響

AsyncOS 8.5 から AsyncOS 8.0 に復元した場合、アプライアンスがセキュリティ機能なしで Web トランザクションを処理する 180 日の猶予期間はありません。ライセンスの有効期限は影響を受けません。

復元プロセスでのコンフィギュレーション ファイルの使用

バージョン 7.5 で有効であり、それ以降のバージョンにアップグレードする場合、アップグレード プロセスは Web セキュリティ アプライアンスのファイルに現在のシステム設定を自動的に保存します（ただし、バックアップとして、コンフィギュレーション ファイルをローカル マシンに手動で保存することを推奨します）。これによって、以前のバージョンに復元した後、AsyncOS for Web が以前のリリースに関連するコンフィギュレーション ファイルをロードできます。ただし、復元を実行すると、管理インターフェイスに現在のネットワーク設定を使用します。

SMA によって管理されるアプライアンスの AsyncOS の復元

Web セキュリティ アプライアンスから Web 用 AsyncOS に復元することができます。ただし 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、次のルールとガイドラインを考慮してください。

- 中央集中型レポーティングをWeb セキュリティ アプライアンスでイネーブルにすると、Web 用 AsyncOS は復帰を開始する前にセキュリティ管理アプライアンスへのレポート データの転送を終了します。セキュリティ管理アプライアンスへのファイルの転送に 40 秒以上かかる場合は、Web 用 AsyncOS がファイルの転送をこのまま待機するように促すか、すべてのファイルを転送せずに復帰を続けます。
- 復元後、適切な設定マスターに Web セキュリティ アプライアンスを関連付ける必要があります。それ以外の場合、セキュリティ管理アプライアンスから Web セキュリティ アプライアンスに設定をプッシュすると失敗する可能性があります。

以前のバージョンへの Web 用の AsyncOS の復元

警告　Web セキュリティ アプライアンスのオペレーティング システムの復元は非常に破壊的な操作であり、すべての設定ログとデータベースが削除されます。さらに、アプライアンスが再設定されるまで、復元によって Web トラフィック処理が中断されます。初期の Web セキュリティ アプライアンス設定に応じて、この操作がネットワークの設定を破壊する場合があります。このような場合、復元の実行後にアプライアンスへの物理的なローカル アクセスが必要になります。

はじめる前に

- Cisco Quality Assurance に問い合わせて、目的とする復元が実行可能かどうかを確認してください。
- Web セキュリティ アプライアンスから別のマシンに次の情報をバックアップします。
  - システム コンフィギュレーション ファイル（パスワードをマスクしない状態）。
  - 保持するログ ファイル。
  - 保持するレポート。
  - アプライアンスに保存されるカスタマイズされたエンド ユーザ通知ページ。
  - アプライアンス上に格納されている PAC ファイル。

ステップ 1　バージョンを戻すアプライアンスの CLI にログインします。

（注）　次のステップで revert コマンドの実行するときに、いくつかの警告プロンプトが発行されます。これらの警告プロンプトに同意すると、すぐにバージョンを戻す動作が開始します。このため、復元に向けた準備手順が完了するまで、復元プロセスを開始しないてください。

ステップ 2　revert コマンドを入力します。

ステップ 3　復元で続行するアプライアンスを 2 回確認します。

ステップ 4　戻る利用可能なバージョンの 1 つを選択します。

アプライアンスが 2 回リブートします。

（注）　復元プロセスは時間のかかる処理です。復元が完了して、アプライアンスへのコンソール アクセスが再び利用可能になるまでには、15 ～ 20 分かかります。

アプライアンスは、選択された Web バージョンの AsyncOS を使用して稼働します。Web ブラウザから Web インターフェイスにアクセスできます。

（注）　URL カテゴリ セットのアップデートが利用可能な場合は、AsyncOS の復元後に適用されます。

トラブルシューティング

認証に関する問題

LDAP に関する問題

NTLMSSP に起因する LDAP ユーザの認証の失敗

LDAP サーバは NTLMSSP をサポートしていません。一部のクライアント アプリケーション（Internet Explorer など）は、NTLMSSP と Basic の選択肢が与えられたときに、常に NTLMSSP を選択します。次の条件がすべて該当する場合は、ユーザの認証に失敗します。

- ユーザが LDAP レルムにのみ存在する。
- 識別プロファイルで LDAP レルムと NTLM レルムの両方を含むシーケンスを使用している。
- 識別プロファイルで「基本または NTLMSSP」認証方式を使用している。
- ユーザが Basic を介して NTLMSSP を選択するアプリケーションから要求を送信する。

上記の条件の少なくとも 1 つが該当する場合は、認証プロファイル、認証レルム、またはアプリケーションを再設定してください。

LDAP 紹介に起因する LDAP 認証の失敗

次の条件がすべて該当する場合は、LDAP 認証に失敗します。

- LDAP 認証レルムで Active Directory サーバを使用している。
- Active Directory サーバが別の認証サーバへの LDAP 紹介を使用している。
- 紹介された認証サーバが Web セキュリティ アプライアンスで使用できない。

回避策：

- アプライアンスで LDAP認証レルムを設定するときに、Active Directory フォレストにグローバル カタログ サーバ（デフォルト ポートは 3268）を指定します。
- `advancedproxyconfig > authentication` CLI コマンドを使用して、LDAP 紹介をディセーブルにします。デフォルトでは、LDAP 紹介はディセーブルになります。

基本認証に関する問題

関連する問題

基本認証の失敗

基本認証方式を使用する場合、AsyncOS for Web では 7 ビット ASCII 文字のパスワードのみがサポートされます。パスワードに 7 ビット ASCII 以外の文字が含まれていると、基本認証は失敗します。

シングル サインオンに関する問題

誤ってユーザにクレデンシャルを要求する

Web セキュリティ アプライアンスが WCCP v2 対応デバイスに接続されている場合、NTLM 認証が機能しないことがあります。トランスペアレント NTLM 認証を適切に実行しない、非常にロックダウンされた Internet Explorer バージョンを使ってユーザが要求を行っており、アプライアンスが WCCP v2対応デバイスに接続されている場合、ブラウザはデフォルトで基本認証を使用します。その結果、認証クレデンシャルが不要な場合でも、ユーザはクレデンシャルの入力を要求されます。

回避策

Internet Explorer で、[ローカル イントラネット] ゾーンの [信頼済みサイト] リストに Web セキュリティ アプライアンスのリダイレクト ホスト名を追加します([ツール] > [インターネット オプション] > [セキュリティ] タブ)。

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 セキュリティ アプライアンスにホストされている場合に、WPAD と共に Firefox(または、DHCP をサポートしていないの他のブラウザ)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 プロキシを指すようにブラウザが手動で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 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 要求と一致しません。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、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。

ハードウェアに関する問題

アラート：380 または 680 ハードウェアでバッテリ再学習タイムアウト（RAID イベント）（Battery Relearn Timed Out (RAID Event) on 380 or 680 Hardware）

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表示されない場合は、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
- アラート：セキュリティ証明書に関する問題（Problem with Security Certificate）
- 次のセクションも参照してください。
  - HTTPS トランザクションのロギング
  - HTTPS に対してアクセス ポリシーを設定できない
  - 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、サーバ名およびそれが属する 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。

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。

アラート：セキュリティ証明書に関する問題（Problem with Security Certificate）

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 要求を送信した場合、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。

Identity Services Engine に関する問題

ISE 問題のトラブルシューティング ツール

次のツールは、ISE 関連の問題をトラブルシューティングする際に役立ちます。

- ISE テスト ユーティリティ。ISE サーバへの接続のテストに使用され、貴重な接続関連情報を提供します。これは、[Identity Services Engine] ページの [テスト開始(Start Test)] オプションです(Identity Services Engine サービスへの接続を参照)。
- ISE およびプロキシ ログ。ログによるシステム アクティビティのモニタを参照してください。
- ISE 関連の CLI コマンド `iseconfig`および`isedata`。特に `isedata`は、セキュリティ グループ タグ(SGT)のダウンロードを確認するために使用します。詳細については、Web セキュリティ アプライアンスの CLI コマンドを参照してください。
- Web トラッキング機能およびポリシー トレース機能。これらを使用してポリシーの一致に関する問題をデバッグできます。たとえば、許可されるべきユーザがブロックされた場合(または、その逆の場合)などに使用できます。詳細については、[Web トラッキング(Web Tracking)] ページおよびポリシーのトラブルシューティング ツール:ポリシー トレースを参照してください。
- パケット キャプチャ(サポートの使用 する場合)
- 認証ステータスを確認する場合は、`openssl` Online Certificate Status Protocol(`ocsp`)ユーティリティを使用できます。これは www.openssl.org から入手できます。

ISE サーバの接続に関する問題

証明書の問題

WSA と ISE サーバは 証明書を使用して正常な接続を相互認証します。したがって、一方のエンティティによって指定された各証明書を、もう一方が認識できなければなりません。たとえば、WSA のクライアント証明書が自己署名の場合、該当する ISE サーバの信頼できる証明書リストに同じ証明書が含まれている必要があります。同様に、WSA クライアント証明書が CA 署名付きの場合も、該当する ISE サーバにその CA ルート証明書が存在している必要があります。同様の要件は、ISE サーバ関連の管理証明書および pxGrid 証明書にも該当します。

証明書の要件およびインストールについては、Cisco Identity Services Engine の統合 で説明されています。証明書関連の問題が発生した場合は、以下を確認してください。

- CA 署名付き証明書を使用する場合:
  - 管理証明書および pxGrid 証明書のルート CA 署名証明書が WSA に存在していることを確認します。
  - WSA クライアント証明書のルート CA 署名証明書が ISE サーバの信頼できる証明書リストに含まれていることを確認します。

- 自己署名証明書を使用する場合:
  - (WSAで生成され、ダウンロードされた)WSA クライアント証明書が、ISE サーバにアップロードされており、ISE サーバの信頼できる証明書リストに含まれていることを確認します。
  - (ISE サーバで生成され、ダウンロードされた)ISE 管理者証明書および pxGrid 証明書が、WSA にアップロードされており、WSA の証明書リストに含まれていることを確認します。
- 期限切れの証明書:
  - アップロード時に有効だった証明書が、期限切れでないことを確認します。

証明書の問題を示すログ出力

次の ISE サービス ログの抜粋は、証明書の欠落または無効な証明書による接続タイムアウトを示しています。

```
Tue Mar 24 03:56:14 2015 Debug: ISELoggerThread: Logging queue starting
Tue Mar 24 03:56:14 2015 Info: ISEService: Successfully loaded configuration from: /data/ise/ise_service.ini
Tue Mar 24 03:56:14 2015 Debug: Statistics loaded from file
Tue Mar 24 03:56:14 2015 Info: ISEService: RPC Server Socket :/tmp/ise_fastrpc.sock
Tue Mar 24 03:56:14 2015 Info: RPCServer: Starting at: /tmp/ise_fastrpc.sock
Tue Mar 24 03:56:14 2015 Info: ISEService: Running
Tue Mar 24 03:56:14 2015 Debug: ISEEngineManager: Creating ISE client attempt 0
Tue Mar 24 03:56:14 2015 Debug: ISEEngineManager: Creating ISE connection with reconnection True
Tue Mar 24 03:56:14 2015 Info: ISEService: Sending ready signal...
Tue Mar 24 03:56:14 2015 Info: ISEDynamicConfigThread: Started Server..
Tue Mar 24 03:56:14 2015 Debug: ISEEngineManager: Successfully created ISE client
Tue Mar 24 03:56:14 2015 Trace: ISEEngineManager: Waiting for client connection, 0 seconds of 30
Tue Mar 24 03:56:17 2015 Trace: ISEEngineManager: Waiting for client connection, 3 seconds of 30
Tue Mar 24 03:56:20 2015 Trace: ISEEngineManager: Waiting for client connection, 6 seconds of 30
Tue Mar 24 03:56:23 2015 Trace: ISEEngineManager: Waiting for client connection, 9 seconds of 30
Tue Mar 24 03:56:26 2015 Trace: ISEEngineManager: Waiting for client connection, 12 seconds of 30
Tue Mar 24 03:56:29 2015 Trace: ISEEngineManager: Waiting for client connection, 15 seconds of 30
Tue Mar 24 03:56:32 2015 Trace: ISEEngineManager: Waiting for client connection, 18 seconds of 30
Tue Mar 24 03:56:35 2015 Trace: ISEEngineManager: Waiting for client connection, 21 seconds of 30
Tue Mar 24 03:56:38 2015 Trace: ISEEngineManager: Waiting for client connection, 24 seconds of 30
Tue Mar 24 03:56:41 2015 Trace: ISEEngineManager: Waiting for client connection, 27 seconds of 30
Tue Mar 24 03:56:44 2015 Trace: ISEEngineManager: Waiting for client connection, 30 seconds of 30
Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Waiting for client connection timed out
Tue Mar 24 03:56:47 2015 Debug: ISEEngineManager: Stopping client...
```

WSA のこれらのトレース レベル ログ エントリは、30 秒後に ISE サーバへの接続の試行が終了されることを示しています。

ネットワークの問題

- Identity Services Engine で [テスト開始(Start Test)] を実行中に ISE サーバへの接続が失敗した場合、Identity Services Engine サービスへの接続は、ポート 443 と 5222 に設定されている ISE サーバへの接続を確認します。

  ポート 5222 は公式のクライアント/サーバ Extensible Messaging and Presence Protocol (XMPP)ポートであり、ISE サーバへの接続に使用されます。また、Jabber や Google Talk などのアプリケーションでも使用されます。ただし、一部のファイアウォールはポート 5222 をブロックするように設定されています。

  接続の確認に使用できるツールには、`telnet` や `tcpdump`.などがあります。

ISE サーバの接続に関する問題

WSA が ISE サーバへの接続を試みたときに、次の問題によって失敗することがあります。

- ISE サーバのライセンスの期限が切れている。
- ISE サーバの [管理(Administration)] > [pxGrid サービス(pxGrid Services)] ページで、pxGrid ノードのステータスが [未接続(not connected)] になっている。このページで [自動登録の有効化(Enable Auto-Registration)] がオンになっていることを確認してください。

- 失効した WSA クライアント（特に「test_client」または「pxgrid_client」）が、ISE サーバ上に存在する。これらは削除する必要があります。ISE サーバの [管理（Administration）] > [pxGrid サービス（pxGrid Services）] > [クライアント（Clients）] を参照してください。
- すべてのサービスが起動して実行される前に、WSA が ISE サーバへの接続を試みている。

  ISE サーバに対する一部の変更（証明書のアップデートなど）では、ISE サーバまたはそこで実行されているサービスの再起動が必要です。この間に ISE サーバへの接続を試みると失敗しますが、最終的に接続に成功します。

ISE 関連の重要なログ メッセージ

ここでは、WSA における ISE 関連の重要なログ メッセージについて説明します。

- `Tue Mar 24 03:56:47 2015 Critical: ISEService: Unable to load configuration!! Config file /data/ise/ise_service.ini not found`

  「thirdparty」プロセスがコンフィギュレーション ファイル `/data/ise/ise_service.ini`.の生成に失敗しました。「thirdparty」ログを確認します。
- `Tue Mar 24 03:56:47 2015 Critical: ISEService: Unable to load configuration from: /data/ise/ise_service.ini!! エラー…`

  `/data/ise/ise_service.ini` または `ise_service.ini.factory` ファイルの内容を確認します。
- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Waiting for client connection timed out`

  WSA の ISE プロセスが 30 秒以内に ISE サーバに接続できませんでした。
- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: WSA Client cert/key missing. Please check ISE config`

  WSA クライアント証明書とキーが WSA の [Identity Service Engine] 設定ページでアップロードされなかったか、生成されませんでした。
- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: ISE service exceeded maximum allowable disconnect duration with ISE server`

  WSA の ISE プロセスが 120 秒以内に ISE サーバに接続できず、終了しました。
- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Subscription to updates failed …`

  WSA の ISE プロセスが、アップデートのために ISE サーバに登録できませんでした。
- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Could not create ISE client: …`

  ISE サーバ接続用の WSA の ISE クライアントを作成するときに、内部エラーが発生しました。
- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Bulk Download thread failed: …`

  この内部エラーは、接続または再接続時に SGT の一括ダウンロードに失敗したことを示しています。
- `Tue Mar 24 03:56:47 2015 Critical: ISEService: Unable to start service. エラー:…`

  WSA の ISE サービスの起動に失敗しました。
- `Tue Mar 24 03:56:47 2015 Critical: ISEService: Unable to send ready signal …`

  WSA の ISE サービスが `heimdall` に Ready 信号を送信できませんでした。
- `Tue Mar 24 03:56:47 2015 Critical: ISEService: Unable to send restart signal …`

  WSA の ISE サービスが `heimdall` に再起動信号を送信できませんでした。

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、次の 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（Unable to Maintain the Rate of Data Being Generated）

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次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。シスコ カスタマー サポートに連絡して、Web セキュリティ アプライアンスの容量を追加する必要があるかどうかを確認してください。

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、[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

- HTTPS に対してアクセス ポリシーを設定できない
- 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消えた
- ポリシーの照合に失敗
- ポリシーのトラブルシューティング ツール：ポリシー トレース
- 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

HTTPS に対してアクセス ポリシーを設定できない

HTTPS プロキシをイネーブルにすると、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、アクセスおよびルーティング ポリシー グループ メンバーシップを HTTPS で定義することも、HTTPS トランザクションをブロックするようにアクセス ポリシーを設定することもできなくなります。

一部のアクセスおよびルーティング ポリシー グループのメンバーシップが HTTPS によって定義されており、一部のアクセス ポリシーが HTTPS をブロックする場合は、HTTPS プロキシをイネーブルにすると、それらのアクセスおよびルーティング ポリシー グループがディセーブルになります。ポリシーは、いつでもイネーブルにすることができますが、そうすると、HTTPS 関連の設定がすべて削除されます。

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

[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 セキュリティ アプライアンスを設定すると、Windows OneCare の更新がブロックされます。

識別プロファイルがポリシーから消えた

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れが削除されます。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が同じ基準である場合、AsyncOS は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、認証のためにクライアントを Web プロキシj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ことは、次の動作を引き起こします。

- **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ときに、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では、ネットワーク接続状態インジケータ（NCSI）が使用されます。
- Web セキュリティ アプライアンスでは NTLMSSP 認証が使用されます。
- 識別 プロファイルでは、IP ベースのサロゲートが使用されます。

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。

ポリシーのトラブルシューティング ツール:ポリシー トレース

ポリシー トレース ツールについて

ポリシー トレース ツールはクライアント要求をエミュレートし、Web プロキシによる要求の処理方法を詳しく示します。Web プロキシの問題をトラブルシューティングするときに、このツールを使用し、クライアント要求を追跡してポリシー処理をデバッグできます。基本トレースを実行したり、詳細なトレース設定を行ってオプションをオーバーライドしたりできます。

ポリシー トレース ツールは、要求を Web プロキシだけで使用されるポリシーと照合して評価します。これらのポリシーには、アクセス、暗号化 HTTPS 管理、ルーティング、セキュリティ、発信マルウェア スキャンがあげられます。

（注）　SOCKS および外部 DLP ポリシーは、ポリシー トレース ツールによって評価されません。

（注）　ポリシー トレース ツールを使用する場合、Web プロキシはアクセス ログまたはレポート データベース内の要求を記録しません。

クライアント要求のトレース

ステップ 1　[システム管理（System Administration）] > [ポリシー トレース（Policy Trace）] を選択します。

ステップ 2　[送信先 URL（Destination URL）] フィールドに、トレースする URL を入力します。

ステップ 3　（任意）追加のエミュレーション パラメータを入力します。

エミュレート対象	入力
要求を行う際に使用されるクライアントの送信元 IP アドレス。	[クライアント IP アドレス（Client IP Address）] フィールドに IP アドレス。 **（注）** IP アドレスを指定しない場合、AsyncOS は localhost を使用します。また、SGT（セキュリティ グループ タグ）は取得できず、SGT に基づくポリシーは照合されません。
要求を行う際に使用される認証/識別クレデンシャル。	[ユーザ名（User Name）] フィールドにユーザ名を入力し、[認証/識別（Authentication/Identification）] ドロップダウン リストから [Identity Services Engine] または認証レルムを選択します。 **（注）** イネーブルになっているオプションのみを使用できます。つまり、認証オプションと ISE オプションは、両方がイネーブルになっている場合にのみを使用できます。 ここで入力するユーザの認証については、そのユーザが Web セキュリティ アプライアンスを介して認証済みである必要があります。

ステップ 4　[一致するポリシーの検索（Find Policy Match）] をクリックします。

ポリシー トレースの出力が [結果（Find Policy Match）] ペインに表示されます。

関連項目

- 詳細設定：要求の詳細（A-16 ページ）
- 詳細設定：レスポンスの詳細の上書き（A-17 ページ）

詳細設定：要求の詳細

[ポリシー トレース（Policy Trace）] ページの [詳細設定（Advanced）] セクションで、[要求の詳細（Request Details）] ペインの設定項目を使用し、このポリシー トレース用に発信マルウェア スキャン要求を調整できます。

ステップ 1　[ポリシー トレース（Policy Trace）] ページの [詳細設定（Advanced）] セクションを展開します。

ステップ 2　[要求の詳細（Request Details）] ペインのフィールドを必要に応じて設定します。

設定	説明
プロキシ ポート（Proxy Port）	プロキシ ポートに基づいてポリシー グループ メンバーシップをテストするトレース要求に対して、使用する特定のプロキシ ポートを選択します。
ユーザ エージェント（User Agent）	要求でシミュレートするユーザ エージェントを指定します。
要求の時間帯	要求でシミュレートする日付と時間帯を指定します。

設定	説明
ファイルのアップロード（Upload File）	要求でアップロードをシミュレートするローカル ファイルを選択します。 ここでアップロードするファイルを指定する場合、Web プロキシは、GET 要求ではなく HTTP POST 要求をシミュレートします。
オブジェクトのサイズ	要求オブジェクトのサイズ（バイト単位）を入力します。キロバイト、メガバイト、またはギガバイトを表す、K、M、または G を入力できます。
MIME タイプ	MIME タイプを入力します。
マルウェア対策スキャンの判定（Anti-malware Scanning Verdicts）	Webroot、McAfee、Sophos スキャンの判定をオーバーライドするには、オーバーライドする特定タイプの判定を選択します。

ステップ 3　[一致するポリシーの検索（Find Policy Match）] をクリックします。

ポリシー トレースの出力が [結果（Find Policy Match）] ペインに表示されます。

詳細設定：レスポンスの詳細の上書き

[ポリシー トレース（Policy Trace）] ページの [詳細設定（Advanced）] セクションで、[レスポンスの詳細の上書き（Response Detail Overrides）] ペインの設定項目を使用し、このポリシー トレース用に Web アクセス ポリシー レスポンスのアスペクトを「調整」できます。

ステップ 1　[ポリシー トレース（Policy Trace）] ページ内の [詳細設定（Advanced）] セクションを展開します。

ステップ 2　[レスポンスの詳細の上書き（Response Detail Overrides）] ペインのフィールドを必要に応じて設定します。

設定	説明
URL Category	トレース応答の URL トランザクション カテゴリをオーバーライドするには、この設定を使用します。応答結果の URL カテゴリと置き換えるカテゴリを選択します。
Application	同様に、トレース応答のアプリケーション カテゴリをオーバーライドするには、この設定を使用します。応答結果のアプリケーション カテゴリと置き換えるカテゴリを選択します。
オブジェクトのサイズ	応答オブジェクトのサイズ（バイト単位）を入力します。キロバイト、メガバイト、またはギガバイトを表す、K、M、または G を入力できます。
MIME タイプ	MIME タイプを入力します。
Web レピュテーション スコア	Web レピュテーション スコア（-10.0 ～ 10.0）を入力します。
マルウェア対策スキャンの判定（Anti-malware Scanning Verdicts）	これらのオプションを使用して、トレース応答で提供される特定のマルウェア対策スキャンの判定をオーバーライドします。応答結果の Webroot、McAfee、または Sophos のスキャン判定と置き換える判定を選択します。

ステップ 3　[一致するポリシーの検索(Find Policy Match)] をクリックします。

ポリシー トレースの出力が [結果(Find Policy Match)] ペインに表示されます。

ファイル レピュテーションとファイル分析に関する問題

ファイル レピュテーションおよび分析のトラブルシューティング(14-12 ページ)を参照してください。

リブートの問題

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。仕様については、「リモート電源管理のイネーブル化」(21-4 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。詳細については、「リモート電源管理のリモート電源管理のイネーブル化」(21-4 ページ)を参照してください。
- 次の 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。

手順

ステップ 1　IPMI を使用して、必要なクレデンシャルとともに、先に設定したリモート電源管理ポートに割り当てられた IP アドレスに、サポートされている電源の再投入コマンドを発行します。

たとえば、IPMI をサポートする UNIX タイプのマシンからは、次のようなコマンドを発行します。

```
ipmitool -I lan -H 192.0.2.1 -U remoteresetuser -P password chassis power reset
```

192.0.2.1 は、リモート電源管理ポートに割り当てられている IP アドレス、remoteresetuser と password はこの機能を有効にするときに入力したクレデンシャルです。

ステップ 2　アプライアンスが再起動されるまで、少なくとも 5 分間待ちます。

サイトへのアクセスに関する問題

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に、Web セキュリティ アプライアンスがトランスペアレント 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（5-30 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、アクセス制御シングル 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） アクセス制御を使用すると、アプリケーション認証ポリシーで設定された Assertion Consumer Service（ACS）の認証をバイパスできます。

関連項目

- 認証のバイパス（5-30 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

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 セキュリティ アプライアンスとアップストリーム プロキシ サーバで基本認証を使用します。
- ダウンストリームの Web セキュリティ アプライアンスでクレデンシャルの暗号化をイネーブルにします。

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、および FTP 要求にのみに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 [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次の操作は、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。

- VMware の [電源オフ（Power Off）] と [リセット（Reset）] 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）。

WCCP に関する問題

最大ポート エントリ数

WCCP を使用している展開では、HTTP、HTTPS、および FTP の各ポートの合計 30 が最大ポート エントリ数です。

サポートの使用

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、契約番号と製品 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次の表を使用すると、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 マルウェア対策シグネチャ
Web セキュリティ マルウェア対策（Web Security Anti-Malware）	WSA-WSM-LIC=	Sophos および Webroot マルウェア対策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（Advanced Malware Protection）	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ワード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。

オプション	説明
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。 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ませんが、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て書き留めます。

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。

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、新しいファイルが開始されます。

オプション	説明
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	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すると、ポートや IP アドレスによって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

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。

（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。

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 セキュリティ アプライアンス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

管理者アカウントを使用して CLI に初回アクセスした後、さまざまな許可レベルの他のユーザを追加できます システム セットアップ ウィザードでは、管理者アカウントのパスワードの変更を要求されます。

管理者アカウントのパスワードは、`passwd` コマンドを使用していつでもリセットできます。

次のいずれかの方法で接続できます。

- **イーサネット。** Web セキュリティ アプライアンスの 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。

下記のユーザ名およびパスワードを入力してアプライアンスにログインします。

- ユーザ名：**admin**
- パスワード：**ironport**

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 モードで動作している場合、CLI コマンド構文は単一のコマンドから構成されます。空白スペースを含まず、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。大文字と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 機能では、設定済みの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 (press the Tab key)
setgateway, setgoodtable, sethostname, settime, settz
example.com> seth (pressing the Tab again completes the entry with sethostname)
```

設定変更の確定

設定の変更は、確定するまで有効になりません。Web の通常の動作を妨げることなく、設定を変更できます。

ステップ 1　コマンド プロンプトで `commit` コマンドを発行します。

ステップ 2　`commit` コマンドに必要な入力値を指定します。

ステップ 3　CLI で `commit` 処理の確認を受け取ります。

（注）　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。

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。

設定変更の確定

`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。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。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。

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
```

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

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>
```

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
```

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
```

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。

コマンド	説明
advancedproxyconfig	認証や DNS パラメータなどの高度な Web プロキシ設定を行います。
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 セキュリティ アプライアンスを設定できます。
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。
bwcontrol	デフォルトのプロキシ ログ ファイルの帯域幅制御デバッグ メッセージを有効にします。
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。
datasecurityconfig	要求の最小本文サイズを定義します。これよりも本文サイズが小さい場合、アップロード要求は Cisco IronPort データ セキュリティ フィルタによってスキャンされません。
date	現在の日付を表示します。例: `Thu Jan 10 23:13:40 2013 GMT`
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。
externaldlpconfig	要求の最小本文サイズを定義します。これよりも本文サイズが小さい場合、アップロード要求は外部 DLP サーバでスキャンされません。
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	名前付き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。
iccm_message	この 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（M-Series）によって管理される時期を示すメッセージを、Web インターフェイスと CLI からクリアします。
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、インターフェイスを作成、編集、削除する操作メニューを提供します。
iseconfig	現在の ISE 設定パラメータを表示します。実行する ISE 設定操作を指定できます。 • setup：ISE の設定項目を設定します（有効化/無効化、ISE サーバ名または IPv4 アドレス、プロキシ キャッシュのタイムアウト、統計情報のバックアップ間隔）。
isedata	ISE データ関連の操作を指定します。 statistics：ISE サーバのステータスと ISE 統計情報を表示します。 statistics：ISE キャッシュを表示するか、IP アドレスを確認します。 show：ISE ID キャッシュを表示します。 checkip：IP アドレスのローカル ISE キャッシュを照会します。 sgts：ISE セキュア グループ タグ（SGT）テーブルを表示します。
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。
musconfig	このコマンドを使用して Secure Mobility を有効化し、リモート ユーザの識別方法を設定します（IP アドレスによって識別するか、1 つ以上の Cisco 適応型セキュリティ アプライアンスと統合することで識別）。 **（注）** このコマンドを使って変更すると、Web プロキシが再起動されます。

musstatus	Web セキュリティ アプライアンスを適応型セキュリティ アプライアンスと統合したときに、このコマンドを使用して Secure Mobility に関連する情報を表示します。 このコマンドにより、次の情報が表示されます。 • Web セキュリティ アプライアンスと個々の適応型セキュリティ アプライアンスとの接続の状態。 • Web セキュリティ アプライアンスと個々の適応型セキュリティ アプライアンスとの接続時間（分単位）。 • 個々の適応型セキュリティ アプライアンスからのリモート クライアントの数。 • サービス対象のリモート クライアントの数。これは、Web セキュリティ アプライアンスを介してトラフィックの受け渡しを行ったリモート クライアントの数です。 • リモート クライアントの合計数。
nslookup	指定されたホストとドメインの情報を得るために、または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	パスワードを設定します。
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。
reportingconfig	レポーティング システムを設定します。
resetconfig	出荷時の初期状態に設定を復元します。
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）**　注：ユーザのパスワードは暗号化されます。
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、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、セキュア LDAP サービス、セキュア モビリティ、アップデート サービスに対して、および HTTPS プロキシ サービスと LDAP サービス向けの ECDHE 暗号に対して SSLv3 をイネーブルまたはディセーブルにします。
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。これには、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。
telnet	Telnet プロトコルを使用して、他のホストと通信します。

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。
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。
upgrade	AsyncOS ソフトウェアのアップグレードをインストールします。
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	システムにログインしているユーザを表示します。
whoami	ユーザ情報を表示します。

関連リソース

ドキュメント セット

Cisco コンテンツ セキュリティ アプライアンスのマニュアル セットには次のマニュアルが含まれています。

- *Cisco AsyncOS for Web User Guide*（このマニュアル）
- *『Cisco AsyncOS CLI Reference Guide』*

このドキュメントおよびその他のドキュメントは、次の場所にあります。

Cisco コンテンツ セキュリティ製品のマニュアル:	URL
Web セキュリティ アプライアンス	http://www.cisco.com/en/US/products/ps10164/tsd_products_support_series_home.html
セキュリティ管理アプライアンス	http://www.cisco.com/en/US/products/ps10155/tsd_products_support_series_home.html
Cisco Cloud Web Security	http://www.cisco.com/c/en/us/support/security/cloud-web-security/tsd-products-support-series-home.html

トレーニング

セキュリティ テクノロジー トレーニングに関する情報:

- シスコの電子メールと Web コンテンツ セキュリティ トレーニングの Web サイト
  http://www.cisco.com/web/learning/le31/email_sec/index.html
- シスコ セキュリティ テクノロジーのトレーニングに関するメールお問い合わせ先
  stbu-trg@cisco.com
- シスコ製品に関するシスコ トレーニングの Web サイト
  http://www.cisco.com/web/learning/training-index.html

ナレッジ ベース

次の URL からシスコ カスタマー サポート サイトのシスコ ナレッジ ベースにアクセスできます。

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

ナレッジ ベースには、シスコ製品に関するハウツー、トラブルシューティング、参考資料が用意されています。

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、次の 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/netpro/security/web

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

サポートを受けるには、次の方法を使用してください。

米国外: http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

サポート サイト: http://www.cisco.com/web/services/acquisitions/ironport.html

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

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-21 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。コメントや提案がございましたら、次のメール 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。

End User License Agreement

Cisco Systems End User License Agreement

IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. IT IS VERY IMPORTANT THAT YOU CHECK THAT YOU ARE PURCHASING CISCO SOFTWARE OR EQUIPMENT FROM AN APPROVED SOURCE AND THAT YOU, OR THE ENTITY YOU REPRESENT (COLLECTIVELY, THE "CUSTOMER") HAVE BEEN REGISTERED AS THE END USER FOR THE PURPOSES OF THIS CISCO END USER LICENSE AGREEMENT. IF YOU ARE NOT REGISTERED AS THE END USER YOU HAVE NO LICENSE TO USE THE SOFTWARE AND THE LIMITED WARRANTY IN THIS END USER LICENSE AGREEMENT DOES NOT APPLY. ASSUMING YOU HAVE PURCHASED FROM AN APPROVED SOURCE, DOWNLOADING, INSTALLING OR USING CISCO OR CISCO-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.

CISCO SYSTEMS, INC. OR ITS SUBSIDIARY LICENSING THE SOFTWARE INSTEAD OF CISCO SYSTEMS, INC. ("CISCO") IS WILLING TO LICENSE THIS SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU PURCHASED THE SOFTWARE FROM AN APPROVED SOURCE AND THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS END USER LICENSE AGREEMENT PLUS ANY ADDITIONAL LIMITATIONS ON THE LICENSE SET FORTH IN A SUPPLEMENTAL LICENSE AGREEMENT ACCOMPANYING THE PRODUCT OR AVAILABLE AT THE TIME OF YOUR ORDER (COLLECTIVELY THE "AGREEMENT"). TO THE EXTENT OF ANY CONFLICT BETWEEN THE TERMS OF THIS END USER LICENSE AGREEMENT AND ANY SUPPLEMENTAL LICENSE AGREEMENT, THE SUPPLEMENTAL LICENSE AGREEMENT SHALL APPLY. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU ARE REPRESENTING THAT YOU PURCHASED THE SOFTWARE FROM AN APPROVED SOURCE AND BINDING YOURSELF TO THE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED CD PACKAGE AND ANY WRITTEN MATERIALS) FOR A FULL REFUND, OR, IF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM AN APPROVED SOURCE, AND APPLIES ONLY IF YOU ARE THE ORIGINAL AND REGISTERED END USER PURCHASER. FOR THE PURPOSES OF THIS END USER LICENSE AGREEMENT, AN "APPROVED SOURCE" MEANS (A) CISCO; OR (B) A DISTRIBUTOR OR SYSTEMS INTEGRATOR AUTHORIZED BY CISCO TO DISTRIBUTE /

SELL CISCO EQUIPMENT, SOFTWARE AND SERVICES WITHIN YOUR TERRITORY TO END USERS; OR (C) A RESELLER AUTHORIZED BY ANY SUCH DISTRIBUTOR OR SYSTEMS INTEGRATOR IN ACCORDANCE WITH THE TERMS OF THE DISTRIBUTOR'S AGREEMENT WITH CISCO TO DISTRIBUTE / SELL THE CISCO EQUIPMENT, SOFTWARE AND SERVICES WITHIN YOUR TERRITORY TO END USERS.

THE FOLLOWING TERMS OF THE AGREEMENT GOVERN CUSTOMER'S USE OF THE SOFTWARE (DEFINED BELOW), EXCEPT TO THE EXTENT: (A) THERE IS A SEPARATE SIGNED CONTRACT BETWEEN CUSTOMER AND CISCO GOVERNING CUSTOMER'S USE OF THE SOFTWARE, OR (B) THE SOFTWARE INCLUDES A SEPARATE "CLICK-ACCEPT" LICENSE AGREEMENT OR THIRD PARTY LICENSE AGREEMENT AS PART OF THE INSTALLATION OR DOWNLOAD PROCESS GOVERNING CUSTOMER'S USE OF THE SOFTWARE. TO THE EXTENT OF A CONFLICT BETWEEN THE PROVISIONS OF THE FOREGOING DOCUMENTS, THE ORDER OF PRECEDENCE SHALL BE (1)THE SIGNED CONTRACT, (2) THE CLICK-ACCEPT AGREEMENT OR THIRD PARTY LICENSE AGREEMENT, AND (3) THE AGREEMENT. FOR PURPOSES OF THE AGREEMENT, "SOFTWARE" SHALL MEAN COMPUTER PROGRAMS, INCLUDING FIRMWARE AND COMPUTER PROGRAMS EMBEDDED IN CISCO EQUIPMENT, AS PROVIDED TO CUSTOMER BY AN APPROVED SOURCE, AND ANY UPGRADES, UPDATES, BUG FIXES OR MODIFIED VERSIONS THERETO (COLLECTIVELY, "UPGRADES"), ANY OF THE SAME WHICH HAS BEEN RELICENSED UNDER THE CISCO SOFTWARE TRANSFER AND RE-LICENSING POLICY (AS MAY BE AMENDED BY CISCO FROM TIME TO TIME) OR BACKUP COPIES OF ANY OF THE FOREGOING.

License. Conditioned upon compliance with the terms and conditions of the Agreement, Cisco grants to Customer a nonexclusive and nontransferable license to use for Customer's internal business purposes the Software and the Documentation for which Customer has paid the required license fees to an Approved Source. "Documentation" means written information (whether contained in user or technical manuals, training materials, specifications or otherwise) pertaining to the Software and made available by an Approved Source with the Software in any manner (including on CD-Rom, or on-line). In order to use the Software, Customer may be required to input a registration number or product authorization key and register Customer's copy of the Software online at Cisco's website to obtain the necessary license key or license file.

Customer's license to use the Software shall be limited to, and Customer shall not use the Software in excess of, a single hardware chassis or card or such other limitations as are set forth in the applicable Supplemental License Agreement or in the applicable purchase order which has been accepted by an Approved Source and for which Customer has paid to an Approved Source the required license fee (the "Purchase Order").

Unless otherwise expressly provided in the Documentation or any applicable Supplemental License Agreement, Customer shall use the Software solely as embedded in, for execution on, or (where the applicable Documentation permits installation on non-Cisco equipment) for communication with Cisco equipment owned or leased by Customer and used for Customer's internal business purposes. No other licenses are granted by implication, estoppel or otherwise.

For evaluation or beta copies for which Cisco does not charge a license fee, the above requirement to pay license fees does not apply.

General Limitations. This is a license, not a transfer of title, to the Software and Documentation, and Cisco retains ownership of all copies of the Software and Documentation. Customer acknowledges that the Software and Documentation contain trade secrets of Cisco or its suppliers or licensors, including but not limited to the specific internal design and structure of individual programs and associated interface information. Except as otherwise expressly provided under the Agreement, Customer shall only use the Software in connection with the use of Cisco equipment purchased by the Customer from an Approved Source and Customer shall have no right, and Customer specifically agrees not to:

(i) transfer, assign or sublicense its license rights to any other person or entity (other than in compliance with any Cisco relicensing/transfer policy then in force), or use the Software on Cisco equipment not purchased by the Customer from an Approved Source or on secondhand Cisco equipment, and Customer acknowledges that any attempted transfer, assignment, sublicense or use shall be void;

(ii) make error corrections to or otherwise modify or adapt the Software or create derivative works based upon the Software, or permit third parties to do the same;

(iii) reverse engineer or decompile, decrypt, disassemble or otherwise reduce the Software to human-readable form, except to the extent otherwise expressly permitted under applicable law notwithstanding this restriction or except to the extent that Cisco is legally required to permit such specific activity pursuant to any applicable open source license;

(iv) publish any results of benchmark tests run on the Software;

(v) use or permit the Software to be used to perform services for third parties, whether on a service bureau or time sharing basis or otherwise, without the express written authorization of Cisco; or

(vi) disclose, provide, or otherwise make available trade secrets contained within the Software and Documentation in any form to any third party without the prior written consent of Cisco. Customer shall implement reasonable security measures to protect such trade secrets.

To the extent required by applicable law, and at Customer's written request, Cisco shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of Cisco's applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Cisco makes such information available.

Software, Upgrades and Additional Copies. NOTWITHSTANDING ANY OTHER PROVISION OF THE AGREEMENT: (1) CUSTOMER HAS NO LICENSE OR RIGHT TO MAKE OR USE ANY ADDITIONAL COPIES OR UPGRADES UNLESS CUSTOMER, AT THE TIME OF MAKING OR ACQUIRING SUCH COPY OR UPGRADE, ALREADY HOLDS A VALID LICENSE TO THE ORIGINAL SOFTWARE AND HAS PAID THE APPLICABLE FEE TO AN APPROVED SOURCE FOR THE UPGRADE OR ADDITIONAL COPIES; (2) USE OF UPGRADES IS LIMITED TO CISCO EQUIPMENT SUPPLIED BY AN APPROVED SOURCE FOR WHICH CUSTOMER IS THE ORIGINAL END USER PURCHASER OR LESSEE OR OTHERWISE HOLDS A VALID LICENSE TO USE THE SOFTWARE WHICH IS BEING UPGRADED; AND (3) THE MAKING AND USE OF ADDITIONAL COPIES IS LIMITED TO NECESSARY BACKUP PURPOSES ONLY.

Proprietary Notices. Customer agrees to maintain and reproduce all copyright, proprietary, and other notices on all copies, in any form, of the Software in the same form and manner that such copyright and other proprietary notices are included on the Software. Except as expressly authorized in the Agreement, Customer shall not make any copies or duplicates of any Software without the prior written permission of Cisco.

Term and Termination. The Agreement and the license granted herein shall remain effective until terminated. Customer may terminate the Agreement and the license at any time by destroying all copies of Software and any Documentation. Customer's rights under the Agreement will terminate immediately without notice from Cisco if Customer fails to comply with any provision of the Agreement. Upon termination, Customer shall destroy all copies of Software and Documentation in its possession or control. All confidentiality obligations of Customer, all restrictions and limitations imposed on the Customer under the section titled "General Limitations" and all limitations of liability and disclaimers and restrictions of warranty shall survive termination of this Agreement. In addition, the provisions of the sections titled "U.S. Government End User Purchasers" and "General Terms Applicable to the Limited Warranty Statement and End User License Agreement" shall survive termination of the Agreement.

Customer Records. Customer grants to Cisco and its independent accountants the right to examine Customer's books, records and accounts during Customer's normal business hours to verify compliance with this Agreement. In the event such audit discloses non-compliance with this Agreement, Customer shall promptly pay to Cisco the appropriate license fees, plus the reasonable cost of conducting the audit.

Export, Re-Export, Transfer and Use Controls. The Software, Documentation and technology or direct products thereof (hereafter referred to as Software and Technology), supplied by Cisco under the Agreement are subject to export controls under the laws and regulations of the United States (U.S.) and any other applicable countries' laws and regulations. Customer shall comply with such laws and regulations governing export, re-export, transfer and use of Cisco Software and Technology and will obtain all required U.S. and local authorizations, permits, or licenses. Cisco and Customer each agree to provide the other information, support documents, and assistance as may reasonably be required by the other in connection with securing authorizations or licenses. Information regarding compliance with export, re-export, transfer and use may be located at the following URL:

http://www.cisco.com/web/about/doing_business/legal/global_export_trade/general_export/contract_compliance.html.

U.S. Government End User Purchasers. The Software and Documentation qualify as "commercial items," as that term is defined at Federal Acquisition Regulation ("FAR") (48 C.F.R.) 2.101, consisting of "commercial computer software" and "commercial computer software documentation" as such terms are used in FAR 12.212. Consistent with FAR 12.212 and DoD FAR Supp. 227.7202-1 through 227.7202-4, and notwithstanding any other FAR or other contractual clause to the contrary in any agreement into which the Agreement may be incorporated, Customer may provide to Government end user or, if the Agreement is direct, Government end user will acquire, the Software and Documentation with only those rights set forth in the Agreement. Use of either the Software or Documentation or both constitutes agreement by the Government that the Software and Documentation are "commercial computer software" and "commercial computer software documentation," and constitutes acceptance of the rights and restrictions herein.

Identified Components; Additional Terms. The Software may contain or be delivered with one or more components, which may include third-party components, identified by Cisco in the Documentation, readme.txt file, third-party click-accept or elsewhere (e.g. on www.cisco.com) (the "Identified Component(s)") as being subject to different license agreement terms, disclaimers of warranties, limited warranties or other terms and conditions (collectively, "Additional Terms") than those set forth herein. You agree to the applicable Additional Terms for any such Identified Component(s)."

Limited Warranty

Subject to the limitations and conditions set forth herein, Cisco warrants that commencing from the date of shipment to Customer (but in case of resale by an Approved Source other than Cisco, commencing not more than ninety (90) days after original shipment by Cisco), and continuing for a period of the longer of (a) ninety (90) days or (b) the warranty period (if any) expressly set forth as applicable specifically to software in the warranty card accompanying the product of which the Software is a part (the "Product") (if any): (a) the media on which the Software is furnished will be free of defects in materials and workmanship under normal use; and (b) the Software substantially conforms to the Documentation. The date of shipment of a Product by Cisco is set forth on the packaging material in which the Product is shipped. Except for the foregoing, the Software is provided "AS IS". This limited warranty extends only to the Software purchased from an Approved Source by a Customer who is the first registered end user. Customer's sole and exclusive remedy and the entire liability of Cisco and its suppliers under this limited warranty will be (i) replacement of defective media and/or (ii) at Cisco's option, repair, replacement, or refund of the purchase price of the Software, in both cases subject to the condition that any error or defect constituting a breach of this limited warranty is reported to the Approved Source supplying the Software to Customer, within the warranty period. Cisco or the Approved Source supplying the Software to Customer may, at its option, require return of the Software and/or Documentation as a condition to the remedy. In no event does Cisco warrant that the Software is

error free or that Customer will be able to operate the Software without problems or interruptions. In addition, due to the continual development of new techniques for intruding upon and attacking networks, Cisco does not warrant that the Software or any equipment, system or network on which the Software is used will be free of vulnerability to intrusion or attack.

Restrictions. This warranty does not apply if the Software, Product or any other equipment upon which the Software is authorized to be used (a) has been altered, except by Cisco or its authorized representative, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Cisco, (c) has been subjected to abnormal physical or electrical stress, abnormal environmental conditions, misuse, negligence, or accident; or (d) is licensed for beta, evaluation, testing or demonstration purposes. The Software warranty also does not apply to (e) any temporary Software modules; (f) any Software not posted on Cisco's Software Center; (g) any Software that Cisco expressly provides on an "AS IS" basis on Cisco's Software Center; (h) any Software for which an Approved Source does not receive a license fee; and (i) Software supplied by any third party which is not an Approved Source.

DISCLAIMER OF WARRANTY

EXCEPT AS SPECIFIED IN THIS WARRANTY SECTION, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, SATISFACTORY QUALITY, NON-INTERFERENCE, ACCURACY OF INFORMATIONAL CONTENT, OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW AND ARE EXPRESSLY DISCLAIMED BY CISCO, ITS SUPPLIERS AND LICENSORS. TO THE EXTENT THAT ANY OF THE SAME CANNOT BE EXCLUDED, SUCH IMPLIED CONDITION, REPRESENTATION AND/OR WARRANTY IS LIMITED IN DURATION TO THE EXPRESS WARRANTY PERIOD REFERRED TO IN THE "LIMITED WARRANTY" SECTION ABOVE. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY IN SUCH STATES. THIS WARRANTY GIVES CUSTOMER SPECIFIC LEGAL RIGHTS, AND CUSTOMER MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. This disclaimer and exclusion shall apply even if the express warranty set forth above fails of its essential purpose.

Disclaimer of Liabilities - Limitation of Liability. IF YOU ACQUIRED THE SOFTWARE IN THE UNITED STATES, LATIN AMERICA, CANADA, JAPAN OR THE CARIBBEAN, NOTWITHSTANDING ANYTHING ELSE IN THE AGREEMENT TO THE CONTRARY, ALL LIABILITY OF CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS COLLECTIVELY, TO CUSTOMER, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), BREACH OF WARRANTY OR OTHERWISE, SHALL NOT EXCEED THE PRICE PAID BY CUSTOMER TO ANY APPROVED SOURCE FOR THE SOFTWARE THAT GAVE RISE TO THE CLAIM OR IF THE SOFTWARE IS PART OF ANOTHER PRODUCT, THE PRICE PAID FOR SUCH OTHER PRODUCT. THIS LIMITATION OF LIABILITY FOR SOFTWARE IS CUMULATIVE AND NOT PER INCIDENT (I.E. THE EXISTENCE OF TWO OR MORE CLAIMS WILL NOT ENLARGE THIS LIMIT).

IF YOU ACQUIRED THE SOFTWARE IN EUROPE, THE MIDDLE EAST, AFRICA, ASIA OR OCEANIA, NOTWITHSTANDING ANYTHING ELSE IN THE AGREEMENT TO THE CONTRARY, ALL LIABILITY OF CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS COLLECTIVELY, TO CUSTOMER, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), BREACH OF WARRANTY OR OTHERWISE, SHALL NOT EXCEED THE PRICE PAID BY CUSTOMER TO CISCO FOR THE SOFTWARE THAT GAVE RISE TO THE CLAIM OR IF THE SOFTWARE IS PART OF ANOTHER PRODUCT, THE PRICE PAID

FOR SUCH OTHER PRODUCT. THIS LIMITATION OF LIABILITY FOR SOFTWARE IS CUMULATIVE AND NOT PER INCIDENT (I.E. THE EXISTENCE OF TWO OR MORE CLAIMS WILL NOT ENLARGE THIS LIMIT). NOTHING IN THE AGREEMENT SHALL LIMIT (I) THE LIABILITY OF CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS TO CUSTOMER FOR PERSONAL INJURY OR DEATH CAUSED BY THEIR NEGLIGENCE, (II) CISCO'S LIABILITY FOR FRAUDULENT MISREPRESENTATION, OR (III) ANY LIABILITY OF CISCO WHICH CANNOT BE EXCLUDED UNDER APPLICABLE LAW.

Disclaimer of Liabilities - Waiver of Consequential Damages and Other Losses. IF YOU ACQUIRED THE SOFTWARE IN THE UNITED STATES, LATIN AMERICA, THE CARIBBEAN OR CANADA, REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE OR OTHERWISE, IN NO EVENT WILL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR LOST OR DAMAGED DATA, BUSINESS INTERRUPTION, LOSS OF CAPITAL, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY OR WHETHER ARISING OUT OF THE USE OF OR INABILITY TO USE SOFTWARE OR OTHERWISE AND EVEN IF CISCO OR ITS SUPPLIERS OR LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

IF YOU ACQUIRED THE SOFTWARE IN JAPAN, EXCEPT FOR LIABILITY ARISING OUT OF OR IN CONNECTION WITH DEATH OR PERSONAL INJURY, FRAUDULENT MISREPRESENTATION, AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE OR OTHERWISE, IN NO EVENT WILL CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR LOST OR DAMAGED DATA, BUSINESS INTERRUPTION, LOSS OF CAPITAL, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY OR WHETHER ARISING OUT OF THE USE OF OR INABILITY TO USE SOFTWARE OR OTHERWISE AND EVEN IF CISCO OR ANY APPROVED SOURCE OR THEIR SUPPLIERS OR LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IF YOU ACQUIRED THE SOFTWARE IN EUROPE, THE MIDDLE EAST, AFRICA, ASIA OR OCEANIA, IN NO EVENT WILL CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS, BE LIABLE FOR ANY LOST REVENUE, LOST PROFIT, OR LOST OR DAMAGED DATA, BUSINESS INTERRUPTION, LOSS OF CAPITAL, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES, HOWSOEVER ARISING, INCLUDING, WITHOUT LIMITATION, IN CONTRACT, TORT (INCLUDING NEGLIGENCE) OR WHETHER ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF, IN EACH CASE, CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS, HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT FULLY APPLY TO YOU. THE FOREGOING EXCLUSION SHALL NOT APPLY TO ANY LIABILITY ARISING OUT OF OR IN CONNECTION WITH: (I) DEATH OR PERSONAL INJURY, (II) FRAUDULENT MISREPRESENTATION, OR (III) CISCO'S LIABILITY IN CONNECTION WITH ANY TERMS THAT CANNOT BE EXCLUDED UNDER APPLICABLE LAW.

Customer acknowledges and agrees that Cisco has set its prices and entered into the Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the parties.

Controlling Law, Jurisdiction. If you acquired, by reference to the address on the purchase order accepted by the Approved Source, the Software in the United States, Latin America, or the Caribbean, the Agreement and warranties ("Warranties") are controlled by and construed under the laws of the State of California, United States of America, notwithstanding any conflicts of law provisions; and the state and federal courts of California shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties. If you acquired the Software in Canada, unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of the Province of Ontario, Canada, notwithstanding any conflicts of law provisions; and the courts of the Province of Ontario shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties. If you acquired the Software in Europe, the Middle East, Africa, Asia or Oceania (excluding Australia), unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of England, notwithstanding any conflicts of law provisions; and the English courts shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties. In addition, if the Agreement is controlled by the laws of England, no person who is not a party to the Agreement shall be entitled to enforce or take the benefit of any of its terms under the Contracts (Rights of Third Parties) Act 1999. If you acquired the Software in Japan, unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of Japan, notwithstanding any conflicts of law provisions; and the Tokyo District Court of Japan shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties. If you acquired the Software in Australia, unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of the State of New South Wales, Australia, notwithstanding any conflicts of law provisions; and the State and federal courts of New South Wales shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties. If you acquired the Software in any other country, unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of the State of California, United States of America, notwithstanding any conflicts of law provisions; and the state and federal courts of California shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties.

For all countries referred to above, the parties specifically disclaim the application of the UN Convention on Contracts for the International Sale of Goods. Notwithstanding the foregoing, either party may seek interim injunctive relief in any court of appropriate jurisdiction with respect to any alleged breach of such party's intellectual property or proprietary rights. If any portion hereof is found to be void or unenforceable, the remaining provisions of the Agreement and Warranties shall remain in full force and effect. Except as expressly provided herein, the Agreement constitutes the entire agreement between the parties with respect to the license of the Software and Documentation and supersedes any conflicting or additional terms contained in any Purchase Order or elsewhere, all of which terms are excluded. The Agreement has been written in the English language, and the parties agree that the English version will govern.

Product warranty terms and other information applicable to Cisco products are available at the following URL:

http://www.cisco.com/go/warranty

Supplemental End User License Agreement for Cisco Systems Content Security Software

IMPORTANT: READ CAREFULLY

This Supplemental End User License Agreement ("SEULA") contains additional terms and conditions for the Software product licensed under the End User License Agreement ("EULA") between You ("You" as used herein means You and the business entity you represent or "Company") and Cisco (collectively, the "Agreement"). Capitalized terms used in this SEULA but not defined will have the meanings assigned to them in the EULA. To the extent that there is a conflict between the terms and conditions of the EULA and this SEULA, the terms and conditions of this SEULA will take precedence.

In addition to the limitations set forth in the EULA on your access and use of the Software, you agree to comply at all times with the terms and conditions provided in this SEULA.

DOWNLOADING, INSTALLING, OR USING THE SOFTWARE CONSTITUTES ACCEPTANCE OF THE AGREEMENT, AND YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT TO THE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED CD PACKAGE AND ANY WRITTEN MATERIALS) FOR A FULL REFUND, OR, IF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM CISCO OR AN AUTHORIZED CISCO RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL END USER PURCHASER.

For purposes of this SEULA, the Product name and the Product description You have ordered is any of the following Cisco Systems Email Security Appliance ("ESA"), Cisco Systems Web Security Appliance ("WSA") and Cisco Systems Security Management Application ("SMA") (collectively, "Content Security") and their Virtual Appliance equivalent ("Software"):

Cisco AsyncOS for Email

Cisco AsyncOS for Web

Cisco AsyncOS for Management

Cisco Email Anti-Spam, Sophos Anti-Virus

Cisco Email Outbreak Filters

Cloudmark Anti-Spam

Cisco Image Analyzer

McAfee Anti-Virus

Cisco Intelligent Multi-Scan

Cisco RSA Data Loss Prevention

Cisco Email Encryption

Cisco Email Delivery Mode

Cisco Web Usage Controls

Cisco Web Reputation

Sophos Anti-Malware

Webroot Anti-Malware

McAfee Anti-Malware

Cisco Email Reporting

Cisco Email Message Tracking

Cisco Email Centralized Quarantine

Cisco Web Reporting

Cisco Web Policy and Configuration Management

Cisco Advanced Web Security Management with Splunk

Email Encryption for Encryption Appliances

Email Encryption for System Generated Bulk Email

Email Encryption and Public Key Encryption for Encryption Appliances

Large Attachment Handling for Encryption Appliances

Secure Mailbox License for Encryption Appliances

Definitions

For purposes of this SEULA, the following definitions apply:

"Company Service" means the Company's email, Internet, security management services provided to End Users for the purposes of conducting Company's internal business.

"End User" means: (1) for the WSA and SMA, the employee, contractor or other agent authorized by Company to access the Internet and the SMA via the Company Service; and (2) for the ESA, the email boxes of the employees, contractors, or other agent authorized by Company to access or use the email services via the Company Service.

"Ordering Document" means the purchase agreement, evaluation agreement, beta, pre-release agreement or similar agreement between the Company and Cisco or the Company and a Cisco reseller, or the valid terms of any purchase order accepted by Cisco in connection therewith, containing the purchase terms for the Software license granted by this Agreement.

"Personally Identifiable Information" means any information that can be used to identify an individual, including, but not limited to, an individual's name, user name, email address and any other personally identifiable information.

"Server" means a single physical computer or devices on a network that manages or provides network resources for multiple users.

"Services" means Cisco Software Subscription Services.

"Service Description" means the description of the Software Subscription Support Services at http://www.cisco.com/web/about/doing_business/legal/service_descriptions/index.html

"Telemetry Data" means samples of Company's email and web traffic, including data on email message and web request attributes and information on how different types of email messages and web requests were handled by Company's Cisco hardware products. Email message metadata and web requests included in Telemetry Data are anonymized and obfuscated to remove any Personally Identifiable Information.

"Term" means the length of the Software subscription You purchased, as indicated in your Ordering Document.

"Virtual Appliance" means the virtual version of Cisco's email security appliances, web security appliances, and security management appliances.

"Virtual Machine" means a software container that can run its own operating system and execute applications like a Server.

Additional License Terms and Conditions

LICENSE GRANTS AND CONSENT TO TERMS OF DATA COLLECTION

License of Software.

By using the Software and the Documentation, Company agrees to be bound by the terms of this Agreement, and so long as Company is in compliance with this Agreement, Cisco hereby grants to Company a nonexclusive, non-sublicensable, non-transferable, worldwide license during the Term to use the Software only on Cisco's hardware products, or in the case of the Virtual Appliances, on a Virtual Machine, solely in connection with the provision of the Company Service to End Users. The number of End Users licensed for the use of the Software is limited to the number of End Users specified in the Ordering Documents. In the event that the number of End Users in connection with the provision of the Company Service exceeds the number of End Users specified in the Ordering Documents, Company shall contact an Approved Source to purchase additional licenses for the Software. The duration and scope of this license(s) is further defined in the Ordering Document. The Ordering Document supersedes the EULA with respect to the term of the Software license. Except for the license rights granted herein, no right, title or interest in any Software is granted to the Company by Cisco, Cisco's resellers or their respective licensors. Your entitlement to Upgrades to the Software is subject to the Service Description. This Agreement and the Services are co-terminus.

Consent and License to Use Data.

Subject to the Cisco Privacy Statement at http://www.cisco.com/web/siteassets/legal/privacy.html, Company hereby consents and grants to Cisco a license to collect and use Telemetry Data from the Company. Cisco does not collect or use Personally Identifiable Information in the Telemetry Data. Cisco may share aggregated and anonymous Telemetry Data with third parties to assist us in improving your user experience and the Software and other Cisco security products and services. Company may terminate Cisco's right to collect Telemetry Data at any time by disabling SenderBase Network Participation in the Software. Instructions to enable or disable SenderBase Network Participation are available in the Software configuration guide.

Description of Other Rights and Obligations

Please refer to the Cisco Systems, Inc. End User License Agreement, Privacy Statement and Service Description of Software Subscription Support Services.

A

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

Y

あ

い

え

お

か

き

く

け

こ

さ

し

す

せ

た

つ

て

と

に

ね

は

ひ

ふ

へ

ほ

ま

み

む

め

も

ゆ

り

る

れ

ろ