Cisco IronPort AsyncOS 7.7.5 for Web ユーザ ガイド

2013 年 4 月 10 日

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

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

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

Cisco IronPort AsyncOS 7.7.5 for Web ユーザ ガイド

CONTENTS

1 セキュリティ Web アプライアンスをご使用の前に

『*Cisco AsyncOS for Web ユーザ ガイド*』では、Cisco IronPort Web セキュリティ アプライアンスのセットアップ方法、管理方法、およびモニタ方法について説明します。これらの方法は、ネットワーキングおよび Web の管理に関する知識を持つ、経験豊富なシステム管理者向けに記載されています。

今回のリリースでの変更点

ここでは、AsyncOS 7.7.5 for Web の新機能および拡張機能について説明します。このリリースの詳細については、製品リリース ノートを参照してください。リリース ノートは、次の URL の Cisco IronPort カスタマー サポート サイトから入手できます。

`http://www.cisco.com/web/ironport/index.html`

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

以前のリリースのリリース ノートで、前に追加された機能および拡張機能を参照することが役に立つ場合もあります。

表 1-1 Cisco IronPort AsyncOS 7.7.5 for Web リリースに追加された新機能および拡張機能について説明します。

表 1-1　AsyncOS for Web 7.7.5 の新機能

機能	説明
新機能	
Cisco Web セキュリティ仮想アプライアンス	シスコは、ネットワークを自らホストできる仮想マシンとして Cisco Web セキュリティ アプライアンスを提供します。 仮想アプライアンスは、VMware ESXi バージョン 4.x または 5.0 を実行する Cisco UCS サーバ（ブレードまたはラックマウント）ハードウェア プラットフォームとは別に、シスコから購入した仮想アプライアンス用のライセンスが必要です。 仮想アプライアンスの要件について詳細は、『*Cisco Security Virtual Appliance Installation Guide*』に説明されています。 新しい Web セキュリティ仮想アプライアンス モデルおよび構成は次のとおりです。 • S000V（250 GB ディスク領域、50 GB キャッシュ容量、1 コア、4 GB メモリ） • S100V（250 GB ディスク領域、50 GB キャッシュ容量、2 コア、6 GB メモリ） • S300V（1024 GB ディスク領域、200 GB キャッシュ容量、4 コア、8 GB メモリ） この機能は AsyncOs for Web で次の変更点があります。 • Web セキュリティ仮想アプライアンスは、クローン作成してネットワーク上の複数の仮想アプライアンスで実行できます。 • 仮想アプライアンスのライセンスをインストールするには `loadlicense` CLI コマンドを使用します。複数の仮想アプライアンスに同じライセンスを使用できます。 • 機能キーは仮想アプライアンスのライセンスに含まれています。機能キーはライセンスと同時に失効します。新しい機能キーの購入の際は、新しい仮想アプライアンスのライセンスをダウンロードしてインストールする必要があります。 • 仮想アプライアンスのライセンスに機能キーが含まれるため、AsyncOS 機能の 30 日間評価はありません。 • 仮想アプライアンスのライセンスをインストールする前に、テクニカル サポートのトンネルを開くことはできません。 • また、`version`、`ipcheck` および `supportrequest` CLI コマンドは、含まれる仮想アプライアンスの情報を更新します。 • 誤設定した仮想アプライアンスについて新規アラートとログがあります。

表 1-1　AsyncOS for Web 7.7.5 の新機能 （続き）

機能	説明
マルチフォレスト NTLM	複数の信頼できない NTLM レルムからのユーザを認証するように、Web セキュリティ アプライアンスを設定します。 場合によっては、各 NTLM レルム間に信頼関係を作成することは実用的ではありません。これで、同じ WSA を使用して、NTLM の信頼のイネーブル化に関連するコストと労力を費やすことなく、これらの設定をサポートできます。 複数の NTLM レルム間に信頼関係がある場合に、それらのレルムのユーザを認証します。これらの信頼できない NTLM レルムを使用して複数のアイデンティティ ポリシーを作成してから、これらのアイデンティティに関連付けられたユーザおよびグループのポリシーを設定します。詳細については、「複数の Active Directory ドメインに対するユーザ認証」（P.20-34）を参照してください。
ソフトウェア ベースの FIPS レベル 1 コンプライアンス	Federal Information Processing Standard（FIPS; 連邦情報処理標準）140-2 は、米国とカナダの連邦政府が共同で開発し、公表された標準です。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。AsyncOS 7.7 for Web では、FIPS 140-2 レベル 1 コンプライアンスを、Web セキュリティ アプライアンス GUI での簡単な手順でイネーブルにすることができます。 この機能は、以前に使用されていたハードウェア セキュリティ モジュール（HSM）の代わりに Cisco Common Crypto Module（C3M）を使用して、すべての暗号操作を行います。これは、現在サポートされているすべてのハードウェア モデルで動作する AsyncOS 7.7 for Web 経由で使用できます。詳細については、「FIPS 準拠」（P.26-28）を参照してください。
SOCKS プロキシ	ブルームバーグ端末を含む、SOCKS ベースのアプリケーションのサポート。SOCKS 固有のユーザおよびグループのポリシーの他に、特定の TCP および UDP 宛先ポートを定義します。SOCKS のログとレポートで、SOCKS プロキシの使用状況を追跡して分析することができます。詳細については、「SOCKS プロキシ サービスの概要」（P.6-1）を参照してください。
カスタマー ヘッダーの挿入	カスタム要求ヘッダーを挿入します。学校向け YouTube などの特定の Web サイトでは、そのドメインへの Web 要求に、カスタマイズされたヘッダー文字列を付加する必要があります。学校向け YouTube の場合は、アカウント固有の文字列を、YouTube のドメインへの各要求とともに送信する必要があります。これで、YouTube は Schools アカウントのユーザを認識し、それに従って機能することができます。この機能により、CLI を使用して、要求が付加されたドメインとカスタマー ヘッダー文字列を指定できます。
OCSP	Online Certificate Status Protocol（OCSP）を使用して、X.509 証明書の失効ステータスの更新を提供します。OCSP により、代わりの方法である証明書失効リスト（CRL）よりタイムリーな確認が可能になります。 現在、管理者は、ポリシーを処理する無効な証明書を [HTTPS プロキシ（HTTPS Proxy）] ページで設定できます。OCSP を有効または無効にし、Web UI を使用して、新しい OCSP ポリシーを設定します。タイムアウト値を設定し、設定されたアップストリーム プロキシ グループを選択します。WSA がアップストリーム プロキシを使用せずに直接接続する免除サーバのリストを設定します。詳細については、「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」（P.11-12）を参照してください。

表 1-1　AsyncOS for Web 7.7.5 の新機能 （続き）

機能	説明
証明書信頼ストア管理	証明書と認証局の管理制御が向上します。シスコのバンドル済み証明書をすべて表示し、シスコの信頼できるルート認証局の信頼を削除して、シスコが発行したブラックリストを表示します。これで、WSA で使用される受け入れ可能および受け入れ不可能な証明書について、より柔軟に決定できるようになります。 Web UI 内で、信頼できる証明書をインポートし、信頼できるルート証明書のリストに追加します。現在のシスコの信頼できるルート証明書を表示し、WSA による個々の証明書の信頼を削除して、その証明書に優先するオプションを選択します。シスコの中間証明書ブラックリストを表示します。特定の中間 CA が侵害されている実際のインシデントにより、WSA には、ブラックリストに含まれる中間証明書のハードコード化されたリストが提供されています。このリストは、以前は管理者に対して透過的でした。これが現在、表示可能なリストになっています。詳細については、「信頼できるリストへの証明書の追加」（P.11-23）および「信頼できるリストからの証明書の削除」（P.11-23）を参照してください。
暗号化された秘密キー	暗号化され、パスワードで保護された秘密キーを使用します。暗号化された秘密キーをアップロードし、それを WSA が復号化するためのパスワードを提供します。そして、WSA は、ユーザが知らないパスワードを使用して、これらの秘密キーを暗号化/難読化して保存します。設定がファイルにエクスポートされても、秘密キーは難読化されたままであるため、ユーザは読み取ることができません。WSA は、設定が WSA にロードされると、このキーを復号化できます。詳細については、「ルート証明書およびキーのアップロード」（P.11-9）を参照してください。
拡張機能	
トランスペアレント SSL ハンドシェイクの SNI 拡張	Server Name Indication（SNI）拡張にアクセスして、宛先サーバ名を解析します。これは、youtube.com や google.com などの複数の HTTPS Web サイトをホストしている仮想サーバに要求する場合に役立ちます。 [問題番号：74969]

表 1-1　AsyncOS for Web 7.7.5 の新機能 （続き）

機能	説明
拡張対象： ネイティブ FTP プロキシ	AsyncOS for Web 7.5 には、ネイティブ FTP 機能への複数の機能強化が含まれています。 • FTP ユーザ名とパスワードには、スペースおよび @ 文字を使用できます。ただし、これらの文字の前にはバックスラッシュ（\）を指定する必要があります。[問題 ID：52183 および 55380] • FTP クライアントは、正式な形式（hostname:port）を使用する限り、コントロール接続に TCP ポートを指定できます。[問題 ID：55044] • FTP クライアントが FTP プロキシへの接続に使用するモードにかかわらず、FTP プロキシはまずパッシブ モードを使用して、FTP サーバに接続しようとします。ただし、FTP サーバがパッシブ モードを許可しない場合、FTP プロキシはアクティブ モードを使用します。[問題 ID：51308] • アプライアンスで定義されている FTP 通知メッセージは、何らかの理由により FTP プロキシが FTP サーバの接続を確立できない場合、ネイティブ FTP クライアントに表示されます。たとえば、FTP プロキシ認証でエラーや、サーバ ドメイン名のレピュテーションが悪い場合などです。これまでは、FTP プロキシ認証でエラーが発生した場合にだけ、このメッセージが表示されていました。 • 現在、アクセス ログには、ユーザが最初にネイティブ FTP セッションを開始したときのエントリが含まれます。「FTP_CONNECT」（明示的な転送接続）および「FTP_TUNNEL」（トランスペアレント接続）のアクセス ログ ファイルを検索します。 • 現在、次の FTP コマンドがサポートされています。 – XMKD、XRMD、XPWD、XCUP [問題 ID：67985] – REST、APPE [問題 ID：70135] – STOU • アクティブ モードのデータ ポート範囲に定義されたポートは、FTP over HTTP トランザクションだけでなく、ネイティブ FTP トランザクションにも適用されます。 • FTP プロキシは、Trivial Virtual File Store（TVFS）FTP 拡張をサポートします。
拡張対象： L4 トラフィック モニタのレポーティングとトラッキング	AsyncOS for Web 7.5 では、サイトやポートのブロックが特定のマルウェアの問題に対するより有効なソリューションであるかどうか、または非常にリスクの高い特定のクライアント IP アドレスに特定の対策を講じるかどうかをより適切に決定できるように、L4 トラフィック モニタ レポートが機能強化されました。 • 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 IP アドレスを上から順に表示でき、それらの結果をポートでフィルタリングできます。 • アクセス上位のマルウェア サイトをポートごとにフィルタリングできます。 • レポート内のテーブルのデータをクリックして、疑わしいサイト、ポート、またはクライアント IP アドレスの詳細を表示できます。 • マルウェアのリスク領域について多角的な検索を実行できます（ホスト名やポートなど）。 詳細については、「[L4 トラフィック モニタ（L4 Traffic Monitor）] ページ」（P.23-25）を参照してください。

表 1-1　AsyncOS for Web 7.7.5 の新機能 （続き）

機能	説明
拡張対象： 外部認証	AsyncOS for Web 7.5 では、外部認証を使用する場合に、すべての RADIUS ユーザを Administrator ユーザ ロール タイプにマップしたり、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 RADIUS ユーザをマップしたりできます。 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 RADIUS ユーザをマップするには、RADIUS CLASS 属性に、Administrator や Operator などのロール タイプを割り当てます。さまざまなロール タイプをマップすると、各 RADIUS ユーザに承認レベルを指定できます。 詳細については、「RADIUS ユーザ認証」（P.26-13）を参照してください。
拡張対象： [ユーザ確認応答（End-User Acknowledgement）] ページ	AsyncOS for Web 7.5 では、セッション cookie、またはユーザ名を使用できない場合は IP アドレスを使用して、エンド ユーザ確認応答のページを受け入れたユーザを追跡できます。これまでは、ユーザ名を使用できない場合に IP アドレスでユーザを追跡することはできませんでした。 また、AsyncOS for Web は、Web プロキシを再起動した後でも、ユーザがエンド ユーザ確認応答のページをいつ受け入れたかを記憶しています。 詳細については、「エンド ユーザ確認ページ」（P.16-12）を参照してください。
拡張対象： WCCP	AsyncOS for Web 7.5 では、WCCP の堅牢性が向上しています。たとえば、新しい設定を展開しても、Web プロキシが WCCP 通信を再ネゴシエートしません。
拡張対象： Syslog のサポート	AsyncOS for Web 7.5 は、アクセス ログの Syslog プッシュをサポートします。 [問題 ID：33010]
拡張対象： 認証	AsyncOS for Web 7.5 では、Active Directory サーバが動作中であるが、応答しなくなった場合に、このサーバと通信する内部認証プロセスを自動的に再起動するように、ネットワークのプロキシを設定できます。これを行うには、`advancedproxyconfig > authentication` CLI コマンドを使用します。 [問題 ID：35038]
拡張対象： [On-box エンド ユーザ通知（On-Box End-User Notification）] ページ	AsyncOS for Web 7.5 では、デフォルトの On-Box End-User 通知のページのルック アンド フィールが更新され、より明確に、読み取りやすくなっています。カスタマイズされた On-Box End-User 通知のページには影響はありません。
拡張対象： SNMP MIB	AsyncOS for Web 7.5 は、SNMP MIB ファイルの多くのカウンタに、32 ビット値の代わりに 64 ビット値を使用します。これは、アプライアンスに負荷がかかった場合に値がロール オーバーされる可能性を低下させます。 [問題 ID：72555]

表 1-1　AsyncOS for Web 7.7.5 の新機能 （続き）

機能	説明
拡張対象： PAC ファイルのホスティング	AsyncOS for Web 7.5 には、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機能が強化されています。 • 既存の PAC ファイルを、同じ名前のファイルの新しいバージョンに置換できます。既にアップロード済みの PAC ファイルと同じ名前の PAC ファイルをアップロードすると、GUI で、新しいファイルを現在のファイルに置き換えるかどうかが尋ねられます。 • また、[削除（Delete）] ボタン アイコンを使用して、PAC ファイルを削除できます。 • [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）] セクションに新しい行を追加した場合は、デフォルトの PAC ファイルが、アプライアンスにアップロードされる最初のファイルとなります。 [問題 ID：78598]
拡張対象： マシン クレデンシャルによる認証	AsyncOS for Web 7.5 では、NCSI を使用する Windows マシンによる認証のマシン クレデンシャルを処理する場合に使用するタイムアウト値を設定できます。 Windows 7 および Windows Vista のマシンには、ネットワーク接続状態インジケータ（NCSI）という機能があります。ネットワーク上のクライアントが NCSI を使用し、Web セキュリティ アプライアンスが NTLMSPP 認証を使用する場合は、比較的小さいタイムアウト値をマシン クレデンシャルで使用するように、アプライアンスを設定する必要があります。これを行うには、`advancedproxyconfig > authentication` CLI コマンドを使用します。 詳細については、「Windows 7 および Windows Vista の使用」（P.20-4）を参照してください。 [問題 ID：75073]

このマニュアルの使い方

このマニュアルを情報源として使用し、アプライアンスの機能について学習します。項目は、論理的な順序に整理されています。必ずしもマニュアルのすべての章を通読する必要はありません。

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

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

はじめる前に

このマニュアルを読む前に、アプライアンスの『*Quick Start Guide*』と、製品の最新のリリース ノートを参照してください。このガイドでは、アプライアンスを梱包箱から取り出し、物理的にラックに取り付けて電源を投入済みであることを前提としています。

（注）　すでにアプライアンスをネットワークに配線済みの場合は、IronPort アプライアンスのデフォルト IP アドレスが、ネットワーク上の他の IP アドレスと競合していないことを確認します。管理ポートに事前に設定されている IP アドレスは、192.168.42.42 です。

詳細情報の入手先

Cisco IronPort では、セキュリティ管理アプライアンスと関連製品の詳細について学習できるよう、次の情報源を提供しています。

ドキュメント セット

Cisco IronPort アプライアンスのドキュメント セットには、次のドキュメントとマニュアルが含まれます（すべてのタイプがすべてのアプライアンスおよびリリースに使用できるとは限りません）。

- 『*Cisco AsyncOS for Web ユーザ ガイド*』（このマニュアル）
- 『*IronPort 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 IronPort 製品に関するドキュメント：	入手場所
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
電子メール セキュリティ アプライアンスおよび CLI リファレンス ガイド	http://www.cisco.com/en/US/products/ps10154/tsd_products_support_series_home.html
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
Cisco IronPort 暗号化	http://www.cisco.com/en/US/partner/products/ps10602/tsd_products_support_series_home.html

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

サード パーティ コントリビュータ

Cisco IronPort AsyncOS に含まれているソフトウェアの中には、FreeBSD, Inc.、Stichting Mathematisch Centrum、Corporation for National Research Initiatives, Inc.、およびその他のサード 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件および通知に基づいて配布されているものがあり、これらの条件はすべて Cisco IronPort ライセンス契約に組み込まれています。

サードパーティのライセンスに関する情報は、次の場所にあるライセンシング ドキュメントで利用できます。http://www.cisco.com/en/US/products/ps10155/prod_release_notes_list.html および https://support.ironport.com/3rdparty/AsyncOS_User_Guide-1-1.html

Cisco IronPort AsyncOS 内のソフトウェアの一部は、Tobi Oetiker 氏の書面による明示的な同意を得て、RRDtool をベースにしています。

本書の一部は、Dell Computer Corporation の許可を得て複製されています。本書の一部は、McAfee, Inc. の許可を得て複製されています。本書の一部は、Sophos Plc. の許可を得て複製されています。

トレーニングと認定試験

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

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

ナレッジ ベース

次の URL から Cisco IronPort カスタマー サポート サイトの Cisco IronPort ナレッジ ベースにアクセスできます。

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

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

ナレッジ ベースには、Cisco IronPort 製品に関するトピックについて豊富な情報が用意されています。

通常、記事は次のカテゴリのいずれかに分類されています。

- **手順**：手順の項目では、Cisco IronPort 製品を使用して何かを実行する方法について説明します。たとえば、How-To の記事では、アプライアンス用データベースのバックアップをとり、復元する手順について説明します。
- **問題と解決策**：問題と解決策の項目では、Cisco IronPort 製品の使用時に発生する可能性があるエラーや問題に対処します。たとえば、Problem-and-Solution の記事では、製品の新バージョンへのアップグレード時に特定のエラーメッセージが表示された場合の対応方法について説明します。
- **参考資料**：Reference の記事は、通常、特定のハードウェアに関連するエラー コードなど情報のリストを提供します。
- **トラブルシューティング**：トラブルシューティングの項目では、Cisco IronPort 製品に関連する一般的な問題を分析し、解決する方法について説明します。たとえば、Troubleshooting の記事は、DNS で問題が発生した場合に従う手順を提供します。

シスコ サポート コミュニティ

シスコ サポート コミュニティは、シスコのお客様、パートナー、および従業員のオンライン フォーラムです。電子メールおよび Web セキュリティの一般的な問題について話し合う場が用意されており、特定のシスコ製品に関する技術的な情報も提供されています。フォーラムにトピックを投稿して質問したり、他のシスコ ユーザや Cisco IronPort ユーザと情報を共有したりできます。

シスコ サポート コミュニティへのアクセス先：

- 電子メール セキュリティと関連管理：

  https://supportforums.cisco.com/community/netpro/security/email
- Web セキュリティと関連管理：

  https://supportforums.cisco.com/community/netpro/security/web

シスコのテクニカル サポート

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

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

以下を含むさまざまな作業にこの Web サイトが役立ちます。

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

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

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

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

マニュアルに関するフィードバック

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

Web セキュリティ アプライアンスの概要

Web セキュリティ アプライアンスは、企業のセキュリティを脅かし、知的財産権を侵害する Web ベースのマルウェアおよびスパイウェア プログラムから企業ネットワークを保護する、堅牢性、安全性、および効率性に優れたデバイスです。Web セキュリティ アプライアンスには、HTTP、HTTPS、FTP、および SOCKS などの標準的な通信プロトコルの保護が含まれます。

マルウェア（「悪意のあるソフトウェア」）とは、所有者の同意を得ることなく、コンピュータ システムに侵入したり、損害を与えたりするように設計されたソフトウェアです。これは、敵意のある、または侵入行為や迷惑行為を行う、あらゆるソフトウェアまたはプログラム コードです。Web ベースのマルウェアには、スパイウェア、システム モニタ、アドウェア、フィッシングとファーミングの技術、キーストローク（キー）ロガー、ブラウザ ハイジャッカー、トロイの木馬などが含まれます。

Web ベースのマルウェアは、急速に増大する脅威であり、企業の重大なダウンタイム、生産性の損失、および IT リソースへの大きな負担の原因となっています。また、企業は、ネットワークがマルウェアの被害を受けた場合、コンプライアンスおよびデータ プライバシー規制違反のリスクにさらされます。そして、高額の訴訟費用や知的財産の公開のリスクにもさらされます。

これらの脅威のネットワークへの侵入を阻止するために最適な場所はゲートウェイです。Web セキュリティ アプライアンスは、Web プロキシ サービスとレイヤ 4 トラフィック モニタリングにより、詳細なアプリケーション コンテンツを詳細にチェックします。Web プロキシおよびレイヤ 4 トラフィック モニタにより、組織では、ネットワーク内のカバレッジの範囲を保証できます。Web セキュリティ アプライアンスは、最適なパフォーマンスと有効性を備えた強力な Web セキュリティ プラットフォームを提供し、マルウェアから組織を保護します。

2
Web セキュリティ アプライアンスの使用

Web セキュリティ アプライアンスの操作の概要

Web プロキシと L4 トラフィック モニタは独立したサービスです。Web プロキシと L4 トラフィック モニタはイネーブルにされており、別個に設定されて、多様な Web ベースのマルウェアの脅威に対する保護を最高レベルで提供します。

Web プロキシと L4 トラフィック モニタでは、フィルタリング テーブルに格納されているデータを使用して、ドメイン名および IP アドレス パス セグメントなどの URL 要求属性を評価し、ローカルで保持されているデータベース レコードと照合させます。一致が発生する場合、アクセス ポリシー設定がトラフィックをブロックまたはモニタするアクションを決定します。一致が見つからない場合は、プロセスが続行されます。

Web プロキシ

Web セキュリティ アプライアンスの Web プロキシは、次のセキュリティ機能をサポートします。

- ポリシー グループ：ポリシー グループでは、管理者がユーザのグループを作成して、各グループに異なるレベルのカテゴリベースのアクセス コントロールを適用できるようにします。
- URL フィルタリング カテゴリ：アプライアンスが特定の HTTP 要求の URL カテゴリに基づいて各 Web トランザクションを処理する方法を設定できます。
- アプリケーション：Application Visibility and Control エンジン（AVC エンジン）は、管理者が特定のアプリケーション タイプに詳細な制御を適用できるようにします。
- Web レピュテーション フィルタ：レピュテーション フィルタは、不審なアクティビティを特定して URL ベースのマルウェア脅威から保護するために Web サーバの動作と特性を分析します。
- アンチマルウェア サービス：Webroot™ および McAfee スキャン エンジンを組み合わせた Cisco IronPort DVS™ エンジンは、多様な Web ベースのマルウェア脅威を識別し、停止します。

Web プロキシ サービスに関する詳細については、「Web プロキシ サービス」（P.5-1）を参照してください。

L4 トラフィック モニタ

L4 トラフィック モニタは、不正なアクティビティのネットワーク ポートを傍受およびモニタし、企業ネットワークに害を与えるマルウェアの試行を妨げる設定可能なサービスです。さらに、L4 トラフィック モニタは感染したクライアントを検出し、企業ネットワーク外に悪意のあるアクティビティが行かないようにします。

L4 トラフィック モニタの詳細については、「L4 トラフィック モニタ」（P.21-1）を参照してください。

Web セキュリティ アプライアンスの管理

Web ベースの管理ツールを使って Web セキュリティ アプライアンスを管理できます。初めてアプライアンスにアクセスすると、初期設定を行うためのシステム セットアップ ウィザードが Web インターフェイスによってを起動されます。システム セットアップ ウィザードを実行したら、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（CLI）を使用して、設定をカスタマイズして、設定を保持できます。

CLI にアクセスして、CLI でサポートされているコマンドを一覧表示する方法については、「コマンドライン インターフェイス」（P.27-1）を参照してください。

システム セットアップ ウィザード

システム セットアップ ウィザードは、基本設定を設定して、一連のシステムのデフォルト値をイネーブルにするユーティリティです。システム セットアップ ウィザードは、[システム管理（System Administration）] タブにあります。システム セットアップ ウィザードの実行の詳細については、「システム セットアップ ウィザード」（P.4-5）を参照してください。

（注）　システムセットアップウィザードを実行すると、Web セキュリティ アプライアンスは完全に再設定され、管理者パスワードはリセットされます。初めてアプライアンスをインストールする場合、または既存の設定を完全に上書きする場合にのみ、システムセットアップウィザードを使用してください。アプライアンスの設定が完了した後にシステムセットアップウィザードを実行すると、クライアントによる Web へのアクセスが遮断される場合があります。初期設定を完了後、システムセットアップウィザードを実行するように選択する場合は、[システム管理（System Administration）] > [設定ファイル（Configuration File）] ページを使用して設定の概要を出力し、現在の設定ファイルをアーカイブします。

Web セキュリティ アプライアンスへのアクセス

アプライアンスにアクセスし、Web ベース管理ユーティリティを起動するには、Web ブラウザを開きます。サポートされている Web ブラウザの一覧については、「ブラウザ要件」（P.2-6）を参照してください。

次のいずれかの方法を使用して、管理インターフェイスに接続します。

- IP アドレスおよびポート番号

  `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。

- ホスト名およびポート番号

  https://hostname:8443

  または

  http://hostname:8080

  ここでは、hostname はアプライアンスの名前で、8080 は HTTP のデフォルトの admin ポート設定であり、8443 は HTTPS のデフォルトの admin ポートです。

（注）　システムのセットアップ時に、ホスト名パラメータが割り当てられます。ホスト名を使用して管理インターフェイスに接続するには、まず、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する必要があります。

Web インターフェイスの使用と移動の詳細については、「Web セキュリティ アプライアンスの Web インターフェイスの使用方法」（P.2-4）を参照してください。

コマンドライン インターフェイス（CLI）の使用方法

CLI を使用してアプライアンスを管理するには、次のいずれかの方法を使用します。

- **イーサネット接続。**イーサネット ケーブルで SSH セッションを確立します。詳細については、「イーサネット接続の使用」（P.2-3）を参照してください。
- **シリアル接続。**シリアル ケーブルでアプライアンスの COM ポートに接続します。詳細については、「シリアル接続の使用」（P.2-3）を参照してください。

Web セキュリティ アプライアンスの CLI はコマンドのセットのシステムへのアクセス、インストール、および管理をサポートします。アプライアンスへのアクセス、アップグレード、および管理に使用できる CLI およびサポートされているコマンドの一覧については、「コマンドライン インターフェイス」（P.27-1）を参照してください。

イーサネット接続の使用

M1 管理ポートからネットワークへのイーサネット ケーブルを使用してアプライアンスをネットワークに接続してから、SSH セッションを使用してネットワーク上のコンピュータからアプライアンスに到達させることができます。

デフォルトで、M1 管理ポートに IP アドレス 192.168.42.42 が割り当てられます。管理ポートにアクセスするには、パーソナル コンピュータに管理ポートと同じサブネット上の IP アドレス（192.168.42.43 など）を割り当てる必要があります。サブネット マスクは 255.255.255.0 です。ご使用のネットワーク コンフィギュレーションで使用可能であれば、この方法による接続が手軽です。

シリアル接続の使用

ヌル モデム ケーブル（9 ピン シリアル）を使用してアプライアンスの COM ポートに直接接続して、コマンドライン インターフェイス(CLI)セッションを確立できます。イーサネット ケーブルを使用したアプライアンスへのネットワーク接続がオプションでない場合、この設定が必要となる場合があります。

これを行うには、次の項目が必要になります。

- 9 ピンのメス/メスのシリアル ケーブル（ヌル モデム）
- シリアル コンソール クライアント（HyperTerminal や PuTTY など）

シリアル ポートの通信設定値は次のとおりです。

Bits per second：9600

データ ビット：8

パリティ：なし

ストップビット：1

フロー制御：ハードウェア

レポートとロギング

Web セキュリティ アプライアンスには、データの取得とシステム アクティビティのモニタリングに対していくつかのオプションがあります。レポートのスケジューリングの詳細については、「レポーティングの概要」（P.22-1）を参照してください。ログ ファイルの使用方法の詳細については、「ロギング」（P.24-1）を参照してください。

Web セキュリティ アプライアンスの Web インターフェイスの使用方法

Web セキュリティ アプライアンスの Web インターフェイスは、アプライアンスを設定およびモニタできる Web ベースの管理ツールです。Web インターフェイスでは、コマンドライン インターフェイス (CLI) のようにアプライアンスを設定できます。ただし Web インターフェイスで使用できる一部の機能は、CLI では使用できません。その逆の場合も同様です。CLI の詳細については、「コマンドライン インターフェイス」（P.27-1）を参照してください。

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は、アプライアンスを設定またはモニタできる複数のタブがあります。必要に応じてアクセス ポリシーの設定、レポートのスケジューリング、機能のイネーブル化、設定の変更ができます。また、Web インターフェイスには、基本的な管理タスクを実行できる 2 つのメニューがあります。

Web インターフェイスを使用するには、Web ブラウザを開き、ログインします。詳細については、「Web セキュリティ アプライアンスへのアクセス」（P.2-2）を参照してください。サポートされている Web ブラウザの一覧については、「ブラウザ要件」（P.2-6）を参照してください。

サポートされる言語の一覧については、「サポートされる言語」（P.2-6）を参照してください。

Web インターフェイスには、次のメニューが含まれます。

- **オプション（Options）**：このメニューでユーザ アカウントを管理できます。ログアウトするか Web インターフェイスにログインするときに使用するパスワードを変更できます。
- **ヘルプ（Help）**：このメニューから、マニュアルまたは Cisco IronPort カスタマー サポートのヘルプにアクセスできます。[ヘルプ（Help）] タスクについては、オンライン ヘルプまたは IronPort カスタマー サポート サイトにアクセスできます。[テクニカル サポート（Technical Support）] タスクでは、Cisco IronPort カスタマー サポートにサポート要求電子メールを送信したり、Cisco IronPort カスタマーが Web セキュリティ アプライアンスにリモート アクセスできるようにします。[テクニカル サポート（Technical Support）] タスクの詳細については、「サポート コマンド」（P.26-2）を参照してください。

Web インターフェイスには次のタブがあります。

- **レポート（Reporting）：**このタブのページを使用して、Web サイトのアクティビティ、アプライアンス アクティビティ、およびアクションの表示ダイナミック データでアプライアンスのレポートを表示します。詳細については、「[レポート（Reporting）] タブ」（P.2-7）を参照してください。
- **Web セキュリティ マネージャ（Web Security Manager）：**このタブのページを使用して、どのグループがどの Web サイトのタイプにアクセスできるかを定義するアクセス ポリシーを作成および設定します。詳細については、「[Web セキュリティ マネージャ（Web Security Manager）] タブ」（P.2-7）を参照してください。
- **セキュリティ サービス（Security Services）：**このタブのページを使用して、アプライアンスがどのようにネットワークをモニタし、保護するかを設定します。詳細については、「「[セキュリティ サービス（Security Services）] タブ」（P.2-8）」を参照してください。
- **ネットワーク（Network）：**このタブのページを使用して、アプライアンスが配置されるネットワークを定義します。詳細については、「[ネットワーク（Network）] タブ」（P.2-8）を参照してください。
- **システム管理（System Administration）：**このタブのページを使用して、ユーザ、アラート、システム時刻などの管理オプションを設定します。初期設定中にイネーブルにした機能のキーを入力することもできます。詳細については、「[システム管理（System Administration）] タブ」（P.2-9）を参照してください。

各タブには、選択可能なメニュー選択のリストがあります。各メニュー選択は、さらに情報やアクティビティをグループ化する Web インターフェイスのさまざまなページを表します。一部のページは、カテゴリにグループ化されます。各タブの見出しの上にカーソルを合わせ、表示されるメニューのメニュー オプションをクリックすることで、Web インターフェイスのセクション間を移動します。

ハイパーテキスト リンクとボタンをクリックすることで、Web インターフェイスの他のページを開きます。さまざまなリンクを検索するには、Web インターフェイスのテキスト上にカーソルを合わせます。カーソルが上にある場合に、テキストの下に下線と共にリンクが表示されます。

Web インターフェイスの特定のページを参照する場合は、マニュアルではそれに沿ってタブ名に続けて矢印とページ名を表記して使用します。たとえば、[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）] になります。

ログイン

Web インターフェイスにアクセスするすべてのユーザは、ログインする必要があります。ユーザ名とパスワードを入力してから [ログイン（Login）] をクリックして Web インターフェイスにアクセスします。サポートされる Web ブラウザを使用する必要があります（「ブラウザ要件」（P.2-6）を参照）。アプライアンスで作成された admin アカウントまたは任意のユーザ アカウントを使用してログインできます。アプライアンス ユーザの作成の詳細については、「ユーザ アカウントの管理」（P.26-9）を参照してください。

ログインしたら、[レポート（Reporting）] > [概要（Overview）] ページが表示されます。

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。たとえば、次のブラウザを使用できます。

ブラウザ	OS	公式にサポートされますか？
Internet Explorer 9.0	Win 7	Yes
Internet Explorer 8.0	Win XP、Win 7	Yes
Internet Explorer 7.0	Win XP	Yes
Safari 4.0 以降	OS X	Yes
Firefox 10x およびそれ以降	すべて	Yes
Firefox 4x-9x	すべて	条件付き **
Firefox 3.6x	すべて	段階的に廃止 *
Google Chrome	すべて	Yes
Internet Explorer 6.0	Win XP	段階的に廃止 *
Opera 10.0.x	Win XP	条件付き **
Safari 3.1	OS X	段階的に廃止 *

* 段階的に廃止：シスコは不具合に対処しません。

** 条件付き：シスコは、主要な機能の不具合にのみ対処します。

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 ブロックの設定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。

サポートされる言語

該当するライセンス キーを使用すると、AsyncOS では、次の言語で GUI および CLI を表示できます。

- 英語
- フランス語
- スペイン語
- ドイツ語
- イタリア語
- 韓国語
- 日本語

- ポルトガル語（ブラジル）
- 中国語（中国と台湾）
- ロシア語

[レポート（Reporting）] タブ

[レポート（Reporting）] タブを使用して、Web サイトのアクティビティ、アプライアンス アクティビティ、およびアクションのダイナミック データを表示することで、アプライアンスをモニタします。

[レポート（Reporting）] タブには、次のページが含まれています。

- 概要（Overview）
- ユーザ（Users）
- Web サイト（Web Sites）
- URL カテゴリ（URL Categories）
- アプリケーションの表示（Application Visibility）
- マルウェア対策（Anti-Malware）
- 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）
- L4 トラフィック モニタ（L4 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）
- 定期レポート（Scheduled Reports）
- アーカイブ レポート（Archived Reports）

[Web セキュリティ マネージャ（Web Security Manager）] タブ

[Web セキュリティ マネージャ（Web Security Manager）] タブを使用して、どのグループがどの Web サイトのタイプにアクセスできるかを定義するアクセス ポリシーを作成および設定します。

[Web セキュリティ マネージャ（Web Security Manager）] タブには、次のページが含まれています。

- アイデンティティ（Identities）
- SaaS ポリシー（SaaS Policies）
- 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 IronPort データ セキュリティ ポリシー（Cisco IronPort Data Security）
- 発信マルウェア スキャン（Outbound Malware Scanning）
- 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）
- 定義済み時間範囲（Defined Time Ranges）
- バイパス設定（Bypass Settings）
- L4 トラフィック モニタ（L4 Traffic Monitor）

[セキュリティ サービス（Security Services）] タブ

このタブを使用して、アプライアンスがどのようにネットワークをモニタし、保護するかを設定します。

[セキュリティ サービス（Security Services）] タブには、次のページが含まれています。

- Web プロキシ（Web Proxy）
- 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（Anti-Malware）
- データ転送フィルタ（Data Transfer Filters）
- AnyConnect セキュア モビリティ（AnyConnect Secure Mobility）
- Web レピュテーション フィルタ（Web Reputation Filters）
- ユーザ通知（End-User Notification）
- L4 トラフィック モニタ（L4 Traffic Monitor）
- SensorBase

[ネットワーク（Network）] タブ

[ネットワーク（Network）] タブを使用して、アプライアンスが配置されているネットワークについて説明し、アプライアンスのネットワーク設定を定義します。

[ネットワーク（Network）] タブには、次のページが含まれています。

- インターフェイス（Interfaces）
- トランスペアレント リダイレクション（Transparent Redirection）
- ルート（Routes）
- 内部 SMTP リレー（Internal SMTP Relay）
- 認証（Authentication）
- 上位プロキシ（Upstream Proxy）
- 外部 DLP サーバ（External DLP Servers）
- DNS

[システム管理（System Administration）] タブ

[システム管理（System Administration）] タブを使用して、ユーザ、アラート、システム時刻などの管理オプションを設定します。初期設定中にイネーブルにした機能のキーを入力することもできます。

[システム管理（System Administration）] タブには、次のページが含まれています。

- ポリシー トレース（Policy Trace）
- ユーザ（Users）
- アラート（Alerts）
- ログ サブスクリプション（Log Subscriptions）
- 返信先アドレス（Return Addresses）
- タイム ゾーン（Time Zone）
- 時刻設定（Time Settings）
- 設定のサマリー（Configuration Summary）
- 設定ファイル（Configuration File）
- ライセンス キーの設定（Feature Key Settings）
- ライセンス キー（Feature Keys）
- アップグレードとアップデートの設定（Upgrade and Update Settings）
- システム 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）
- 次のステップ（Next Steps）

変更内容のコミットおよびクリア

一部の Web セキュリティ アプライアンスの設定を変更する場合、実施される前に変更内容をコミットする必要があります。または、コミットしない場合、実施した変更内容をクリアすることもできます。変更内容をコミットおよびクリアする方法は、使用するインターフェイスに左右されます。

- Web インターフェイス
- コマンドライン インターフェイス

一部の Web セキュリティ アプライアンスの設定をコミットする場合、変更内容をイネーブルにするために Web プロキシを再起動する必要があります。詳細については、「コミット時の Web プロキシ再起動のチェック」（P.2-10）を参照してください。

Web インターフェイスの変更内容のコミットおよびクリア

Web インターフェイスの右上隅の [変更を確定（Commit Changes）] ボタンを使用して変更内容をコミットします。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。変更を行うと、[変更を確定（Commit Changes）] ボタンの色は黄色になり、ボタン テキストが図 2-1 に示すように「Commit Changes」に変わります。

図 2-1　[確定する（Commit）] ボタン : [保留中の変更あり（Changes Pending）]

コミットに変更がない場合、ボタンの色はグレーになり、ボタン テキストは「No Changes Pending」になります。図 2-2 は、コミットする変更内容がない場合の Web インターフェイスを示します。

図 2-2　[確定する（Commit）] ボタン : [保留中の変更なし（No Changes Pending）]

また、[変更を確定（Commit Changes）] ボタンを使用して、最後にコミットまたはクリアしてから行われた変更内容をクリアします。

Web インターフェイスでの変更内容のコミット

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。

CLI での変更内容のコミットおよびクリア

`commit` コマンドを使用して、変更内容をコミットします。`commit` コマンドを発行するまで、コマンドライン インターフェイス（CLI）で実施する設定変更のほとんどはイネーブルになりません。コメントとして最大 255 文字を使用できます。変更内容は、タイムスタンプとともに確認を受け取るまでは、確定されたものとして認められません。`commit` または `clear` コマンドが最後に発行されてから、`commit` コマンドは行われた設定変更をアプライアンスに適用します。

`commit` コマンドの使用の詳細については、「設定変更の確定」（P.27-5）を参照してください。

`clear` コマンドを使用して変更内容をクリアします。`clear` コマンドの使用の詳細については、「設定変更のクリア」（P.27-5）を参照してください。

コミット時の Web プロキシ再起動のチェック

Web プロキシに加えた一部の設定変更は、変更内容をコミットするときに、Web プロキシの再起動をトリガーします。Web プロキシが再起動すると、Web アプライアンスは Web トラフィックを継続させますが、アンチマルウェア スキャンなどの Web プロキシが短時間中断されます。通常、設定変更により Web プロキシは 30 秒未満で再起動します。（内部エラーにより Web プロキシが再起動する場合は、アプライアンス上のすべてのサービスを開始するのに全再起動プロセスに数分かかる場合があります）。

スキャンされない Web トラフィックからのセキュリティ リスクを最小限にするには、コミットする前に、設定変更が Web プロキシの再起動をトリガーするかどうかを指定できます。次に、夜間など Web プロキシがより少ないユーザ トランザクションを処理するときに、時間に対する設定変更をコミットするようにスケジューリングできます。チェック方法は、インターフェイスに応じて異なります。

- **Web インターフェイス。**[変更を確定（Commit Changes）] ボタンをクリックすると、Web インターフェイスは Web プロキシがコミットの結果として再起動する [未確定の変更（Uncommitted Changes）] ページの警告を表示します。
- **CLI。**`commit` コマンドの前に `checkproxyrestart` コマンドを使用します。設定変更で Web プロキシの再起動が必要な場合、CLI は「The changes will trigger a proxy restart」を表示します。

Web プロキシ サービスが一時的に中断するだけでなく、Web プロキシが再起動するときに次の影響を認識できます。

- 認証キャッシュはクリアされ、ユーザは再認証される必要があります。
- 統計情報の追跡がリセットされます。値が統計情報に左右されるため、これは SNMP にも影響します。
- Web プロキシの DNS キャッシュがクリアされます。
- HTTPS 証明書のキャッシュがクリアされます。
- 認証サーバへの接続が再ネゴシエートされます。
- ディスクに書き込まれていない Web プロキシ キャッシュのデータが失われます。
- ログ ファイルに書き込まれていないロギング データは失われます。

Cisco SensorBase ネットワークへの参加

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。

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。システムの設定後、[セキュリティ サービス（Security Services）] > [SensorBase] ページで参加レベルおよびその他の設定を編集できます。

ステップ 1　[セキュリティ サービス（Security Services）] > [SensorBase] ページの順に移動します。

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。詳細については、「セキュア モビリティの実現」（P.14-1）を参照してください。

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。

データの共有

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、悪質に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。

3
導入

導入の概要

Web セキュリティ アプライアンス は、クライアントとインターネット間のネットワークに追加のレイヤとして設置するのが通常です。クライアント トラフィックをアプライアンスに送信するためのレイヤ 4（L4）スイッチまたは WCCP ルータが必要かどうかは、アプライアンスをどのように展開するかによります。

Web セキュリティ アプライアンスを導入する場合、次の機能の 1 つまたは両方をイネーブルにできます。

- **セキュアな Web プロキシ。**アプライアンスの Web プロキシ サービスは、Web トラフィックで、悪意のあるコンテンツをモニタし、スキャンします。Web プロキシをイネーブルにすると、透過的または明示的な転送モード設定できます。
- **L4 トラフィック モニタ。**L4 トラフィック モニタは、すべてのポートおよび IP アドレスの不正なトラフィックを検出し、ブロックします。L4 トラフィック モニタは、アプライアンス上のすべてのポートと IP アドレスを介して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、発信トラフィックを許可するかどうかを決定します。

デフォルトでは、L4 トラフィック モニタと Web プロキシの両方がシステムセットアップウィザードでイネーブルになっています。これらの機能の両方または 1 つをディセーブルにする必要がある場合、初期設定後に Web インターフェイスから実行できます。

イネーブルにする機能によって、ネットワークにアプライアンスを導入し、物理的に接続する方法が決まります。イネーブルにする機能がアプライアンスの導入に与える影響の詳細については、「導入の準備」（P.3-2）を参照してください。ネットワークへのアプライアンスの物理的接続に使用されるイーサネット ポートの詳細については、「アプライアンスのインターフェイス」（P.3-2）を参照してください。

導入の準備

Web セキュリティ アプライアンスをインストールする前に、次の質問を読み、各質問に対する回答を使用して、アプライアンスを導入する方法とネットワークに配置する場所を決定できます。それぞれの回答には、回答をより詳しく説明する別のセクションへの参照が含まれています。

1. Web セキュリティ アプライアンスをトランスペアレント プロキシまたは明示的な転送プロキシとして導入しますか。
   - **明示的な転送プロキシ。**Web ブラウザなどのクライアント アプリケーションは、Web プロキシを認識するため、単一の Web セキュリティ アプライアンスを指すように設定する必要があります。この導入では、標準ネットワーク スイッチに接続する必要があります。Web プロキシを明示的な転送モードで導入する場合、ネットワークの任意の場所に配置できます。詳細については、「明示的な転送モードでの Web プロキシの導入」（P.3-4）を参照してください。
   - **トランスペアレント プロキシ。**クライアント アプリケーションは Web プロキシを認識しないため、プロキシに接続するように設定する必要はありません。この導入では、レイヤ 4 スイッチまたは WCCP v2 ルータが必要です。詳細については、「トランスペアレント モードでの Web プロキシの導入」（P.3-5）を参照してください。

（注）　レイヤ 4 スイッチは、ポリシー ベース ルーティングを実行できるスイッチです。

2. ネットワークに既存のプロキシが存在しますか。

   存在する場合は、Web セキュリティ アプライアンスを既存のプロキシ サーバからダウンストリームに（つまり、クライアントの近くに）導入することを推奨します。システムセットアップウィザードは、これをアップストリーム プロキシ コンフィギュレーションとして参照します。

   詳細については、「既存のプロキシ環境での Web セキュリティ アプライアンスの使用」（P.3-11）を参照してください。

3. L4 トラフィック モニタをイネーブルにしますか。

   L4 トラフィック モニタの導入は、Web プロキシの導入とは独立して行われます。L4 トラフィック モニタをネットワーク タップまたはスイッチのミラー /SPAN ポートに接続できます。

   詳細については、「L4 トラフィック モニタの導入」（P.3-12）を参照してください。

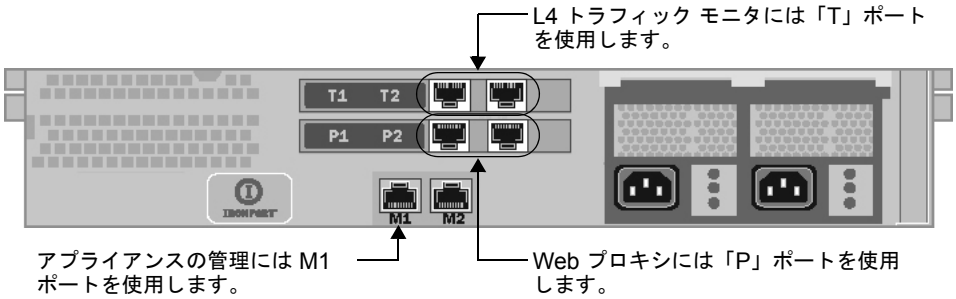
アプライアンスのインターフェイス

Web セキュリティ アプライアンスには、システム背面に 6 個の物理イーサネット ポートが装備されています。各イーサネット ポートは、異なるネットワーク インターフェイスに対応します。イーサネット ポートは、次のネットワーク インターフェイスのタイプにグループ化されます。

- **管理** 管理インターフェイスには M1 と M2 があります。ただし、アプライアンスでは M1 インターフェイスのみイネーブルになります。詳細については、「管理インターフェイス」（P.3-3）を参照してください。
- **データ。**データ インターフェイスには P1 と P2 があります。Web プロキシ データ トラフィックには、データ インターフェイスを使用します。詳細については、「データ インターフェイス」（P.3-3）を参照してください。
- **L4 トラフィック モニタ。**L4 トラフィック モニタのインターフェイスには T1 と T2 があります。L4 トラフィック モニタのトラフィックのモニタおよびブロックには、これらのインターフェイスを使用します。詳細については、「L4 トラフィック モニタ インターフェイス」（P.3-4）を参照してください。

図 3-1 は、Web セキュリティ アプライアンス ブレードの背面のイーサネット ポートを示します。

図 3-1　Web セキュリティ アプライアンスのイーサネット ポート



管理インターフェイス

アプライアンスの管理には M1 を使用します。任意で、Web プロキシのデータ トラフィックを処理するように M1 インターフェイスを設定することもできます。組織が別個の管理ネットワークを使用しない場合、M1 インターフェイスをデータ トラフィックに使用する場合があります。

M1 ポートを使用してアプライアンスを設定および管理する方法の詳細については、「アプライアンスへのラップトップの接続」（P.4-2）を参照してください。

ネットワーク インターフェイスの設定に関する詳細については、「ネットワーク インターフェイスの設定」（P.25-2）を参照してください。

データ インターフェイス

アプライアンスは、Web プロキシ トラフィックにデータ インターフェイスを使用します。データ トラフィックにポート P1 のみをイネーブルにして使用するか、または P1 および P2 ポートの両方をイネーブルにして使用することができます。

- **P1 のみイネーブル化。**P1 のみをイネーブルにする場合、着信および発信トラフィックの両方のネットワークに P1 を接続します。
- **P1 および P2 のイネーブル化。**P1 および P2 の両方をイネーブルにする場合、各インターフェイスを別のサブネットに接続する必要があります。通常、P1 は内部ネットワークに接続され、P2 はインターネットに接続されます。ただし、アプライアンスはインライン モードではサポートできないことに注意してください。

（注） システムセットアップウィザードでは、データ トラフィックにのみ P1 インターフェイスをイネーブルにし、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 セットアップを行った後に、Web インターフェイスまたは `ifconfig` コマンドを使用して実行する必要があります。P2 インターフェイスの設定の詳細については、「ネットワーク インターフェイスの設定」（P.25-2）を参照してください。

データ インターフェイスをネットワークに物理的に接続する方法は、アプライアンスを導入する方法によって異なります。詳細については、「明示的な転送モードでの Web プロキシの導入」（P.3-4）および「トランスペアレント モードでの Web プロキシの導入」（P.3-5）を参照してください。

L4 トラフィック モニタ インターフェイス

アプライアンスは、すべての TCP ポート上のトラフィックをリスニングするために、T1 および T2 インターフェイスを使用します。シンプレックスまたはデュプレックス通信を使用するかどうかに応じて、イーサネット ケーブルを使用して T1 のみ、または T1 および T2 の両方を接続できます。

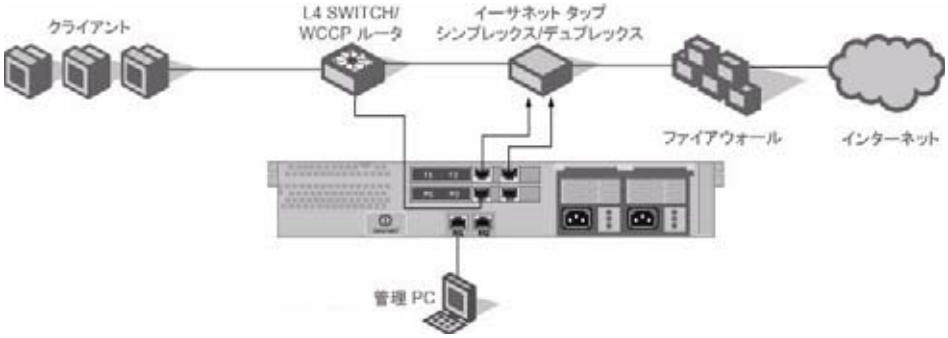
- **T1 のみ接続（デュプレックス）。**デュプレックス通信を使用するようにアプライアンスを設定する場合は、T1 をネットワークに接続して、すべての着信および発信トラフィックを受信します。
- **T1 および T2 を接続（シンプレックス）。**シンプレックス通信を使用するようにアプライアンスを設定する場合は、T1 をネットワークに接続して、すべての発信トラフィック（クライアントからインターネットへ）を受信し、T2 をネットワークに接続して、すべての着信トラフィック（インターネットからクライアントへ）を受信します。

L4 トラフィック モニタ ポートをネットワークに接続する方法の詳細については、「L4 トラフィック モニタの導入」（P.3-12）を参照してください。

導入例

図 3-2（P.3-4）は、イネーブル化した Web プロキシおよび L4 トラフィック モニタの両方の導入シナリオの例を示します。この例では、Web プロキシはトランスペアレント モードで導入され、P1 ポートだけがレイヤ 4 スイッチまたは WCCP ルータのいずれかに接続されます。

図 3-2　Web セキュリティ アプライアンスの導入シナリオ



明示的な転送モードでの Web プロキシの導入

アプライアンスが明示的な転送プロキシとして設定されている場合、クライアント アプリケーションは、そのトラフィックをアプライアンスに転送するように設定する必要があります。Web プロキシを明示的な転送モードで設定する場合は、次のコンポーネントを設定する必要があります。

- クライアント アプリケーション
- アプライアンス ポート

ヒント　組織では、現在明示的な転送モードを使用する必要があるが、将来トランスペアレント モードが必要になる可能性がある場合、Web プロキシをトランスペアレント モードで導入し、接続タイプとしてレイヤ 4 スイッチを選択することを検討します。レイヤ 4 スイッチがない場合、アプライアンスを正常にネットワークに接続でき、アプライアンスは明示的な転送モードで動作します。Web プロキシがトランスペアレント モードで導入されている場合、透過的にリダイレクトされたトランザクションと明示

的に転送されたトランザクションの両方を受け入れることができます。将来トランスペアレント モードを使用するために、アプライアンスをレイヤ 4 スイッチに接続でき、後で Web プロキシ モードを変更することなくトランスペアレント モードで動作します。ただし、[セキュリティサービス（Security Services）] > [Web プロキシ（Web Proxy）] ページで、導入モードをいつでも簡単に変更できます。

クライアント アプリケーションの設定

Web プロキシをポイントするためにネットワーク上で使用されるすべてのクライアント アプリケーション（Web ブラウザや FTP クライアントなど）を設定する必要があります。次の方法で、各クライアントを設定できます。

- **手動。**アプライアンスのホスト名または IP アドレス、およびデータ トラフィックのリスニングに使用するポート番号（3128 など）を指定して、アプライアンスの Web プロキシをポイントするように、各クライアント アプリケーションを設定します。
- **自動。**PAC ファイルを使用して、アプライアンスの Web プロキシを自動的に検出するように、各クライアント アプリケーションを設定します。その後、PAC ファイルを編集して、アプライアンスの Web プロキシ情報を指定できます。PAC ファイルは Web ブラウザでのみ動作します。詳細については、「PAC ファイルでの操作」（P.5-14）を参照してください。

アプライアンス インターフェイスの接続

イーサネット ケーブルを使用して、P1 インターフェイスまたは P1 および P2 インターフェイスの両方をネットワーク スイッチに接続できます。特定のスイッチやルータなどの特別なハードウェアを必要ありません。データ インターフェイス（P1 および P2）の接続方法の詳細については、「データ インターフェイス」（P.3-3）を参照してください。

明示的な転送設定のテスト

明示的な転送プロキシ設定をテストする場合、ネットワーク インフラストラクチャのサブセットから転送トラフィックを分離できます。この設定を個別にテストするために、クライアントは 1 つの Web ブラウザからアプライアンスにトラフィックを転送し、別の Web ブラウザを使用してインターネットに接続できます。また、この方法により、テスト中にインターネットへの代替パスが確保されます。

トランスペアレント モードでの Web プロキシの導入

アプライアンス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、クライアント アプリケーションは、トラフィックがアプライアンスにリダイレクトされたことを認識せず、アプライアンスをポイントするように設定する必要はありません。このモードでアプライアンスを導入するには、アプライアンスを Web トラフィックに透過的にリダイレクトするために、次のタイプのハードウェアのいずれかが必要になります。

- **WCCP v2 ルータ。**WCCP ルータを指定する場合、アプライアンスで追加設定を設定する必要があります。WCCP ルータによるアプライアンスの使用方法の詳細については、「アプライアンスの WCCP ルータへの接続」（P.3-6）を参照してください。
- **レイヤ 4 スイッチ。**レイヤ 4 スイッチを指定する場合、アプライアンスを設定するときに、アプライアンスがレイヤ 4 スイッチに接続されるように指定する必要があります。アプライアンスでその他の設定を行う必要はありません。

通常、初期システム セットアップ時に、レイヤ 4 スイッチまたは 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。ただし、[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）] ページで、初期設定後にレイヤ 4 スイッチまたは WCCP v2 ルータのいずれかを使用するように設定できます。[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）] ページの詳細については、「透過的リダイレクションの設定」（P.25-11）を参照してください。

（注）　Web プロキシがトランスペアレント モードで設定されている場合、アプライアンスが HTTPS トラフィックを受信するには、HTTPS プロキシをイネーブルにする必要があります。HTTPS プロキシをディセーブルにする場合、Web プロキシは明示的な HTTPS 接続をパススルーし、リダイレクトされた HTTPS 要求を透過的にドロップします。アクセス ログには、明示的な HTTPS 接続に対する CONNECT 要求が含まれますが、透過的にリダイレクトされた HTTPS 要求のドロップに関するエントリは存在しません。

アプライアンス インターフェイスの接続

Web プロキシをトランスペアレント モードに設定する場合、P1 ポートまたは P1 および P2 ポートの両方を、イーサネット ケーブルを使用してレイヤ 4 スイッチまたは WCCP ルータに接続できます。データ インターフェイス（P1 および P2）の接続方法の詳細については、「データ インターフェイス」（P.3-3）を参照してください。

アプライアンスの WCCP ルータへの接続

アプライアンスを WCCP ルータに接続する場合は、次のタスクの実行する必要があります。

1. アプライアンス上に少なくとも 1 つの WCCP サービスを作成する必要があります。詳細については、「「Web セキュリティ アプライアンスの設定」（P.3-6）」を参照してください。
2. WCCP サービスを作成した後に、ルータが Web セキュリティ アプライアンスと連携するように設定する必要があります。詳細については、「「WCCP ルータの設定」（P.3-7）」を参照してください。

アプライアンスを複数の WCCP ルータに接続することもできます。詳細については、「「複数のアプライアンスおよびルータの使用」（P.3-10）」を参照してください。

Web セキュリティ アプライアンスの設定

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。

[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）] ページで WCCP サービスを作成します。作成する WCCP サービスによって、WCCP ルータの設定方法が決まります。WCCP サービス作成の詳細については、「WCCP サービスの追加と編集」（P.25-14）を参照してください。

（注）　システム セットアップ時に標準サービス（「web-cache」サービスとも呼ばれます）をイネーブルにし、システム セットアップ ウィザードを実行後、別個または追加の WCCP サービス グループを設定できます。

WCCP ルータの設定

Web セキュリティ アプライアンスで少なくとも 1 つの WCCP サービスを作成後、ネットワーク内の WCCP ルータを設定できます。

ルータで WCCP をイネーブルにするには、次の構文を使用します。

```
ip wccp version 2
ip wccp service_group
interface interface_type_number
ip wccp service_group redirect direction
ip wccp service_group password password
```

service_group 変数には、次の値のいずれかを入力します。

- **web-cache。**アプライアンスの WCCP サービスが標準サービスを使用する場合、「web-cache」を入力します。
- **サービス ID 番号。**アプライアンスの WCCP サービスがダイナミック サービス ID を使用する場合は、0 ～ 255 の数字を入力します。この数字は、アプライアンスで使用するサービス ID 番号に一致させる必要があります。

表 3-1 は、ルータで WCCP をイネーブルにするための WCCP 設定構文の各部分を説明しています。

表 3-1　ルータをイネーブル化するための WCCP ルータ設定構文

WCCP の設定	説明
`ip wccp version 2`	ルータで使用する WCCP のバージョンを定義します。Web セキュリティ アプライアンスと連携するには、バージョン 2 を指定します。 このコマンドは必須です。
`ip wccp service_group password password`	ルータでイネーブルにするサービス グループを指定します。また、ルータで WCCP サービスをイネーブルにします。 このコマンドは必須です。
`interface interface_type_number`	設定するインターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。*interface_type_number* 変数のインターフェイス番号を入力します。 このコマンドは必須です。
`ip wccp service_group redirect direction`	特定のインターフェイスで WCCP リダイレクションをイネーブルにします。 *direction* 変数には、次の値のいずれかを入力します。 • **in。**パケットがルータに入るときに、ルータによってリダイレクトさせたいときに `in` を使用します。 • **out。**パケットがルータを出る直前に、ルータによってリダイレクトさせたいときに `out` を使用します。 このコマンドは必須です。
`ip wccp service_group password password`	指定したサービス グループ用のルータのパスワードを設定します。 このコマンドは、アプライアンスで定義されている WCCP サービスのパスワード セキュリティがイネーブルになっている場合にのみ必要です。

次のような他のタスクを実行するように、WCCP ルータを設定することもできます。

- 特定のインターフェイスで受信するトラフィックのリダイレクトを除外するようにルータを設定します。
- ネットワークが複数の Web セキュリティ アプライアンスを使用している場合、アクセス リストを使用することで、どのトラフィックがどのアプライアンスにリダイレクトされるかを決定するルータを設定できます。Web セキュリティ アプライアンスを評価している場合、一部のネットワーク トラフィックのみをアプライアンスにリダイレクトする場合があります。

（注）　Web セキュリティ アプライアンスは、WCCP サービス グループでのマルチキャスト アドレスの使用をサポートしません。あるサービス グループで複数のルータを使用するには、そのサービス グループ内の各ルータの IP アドレスを指定し、各ルータを個別に設定する必要があります。ルータをマルチキャスト アドレスに登録することはできません。

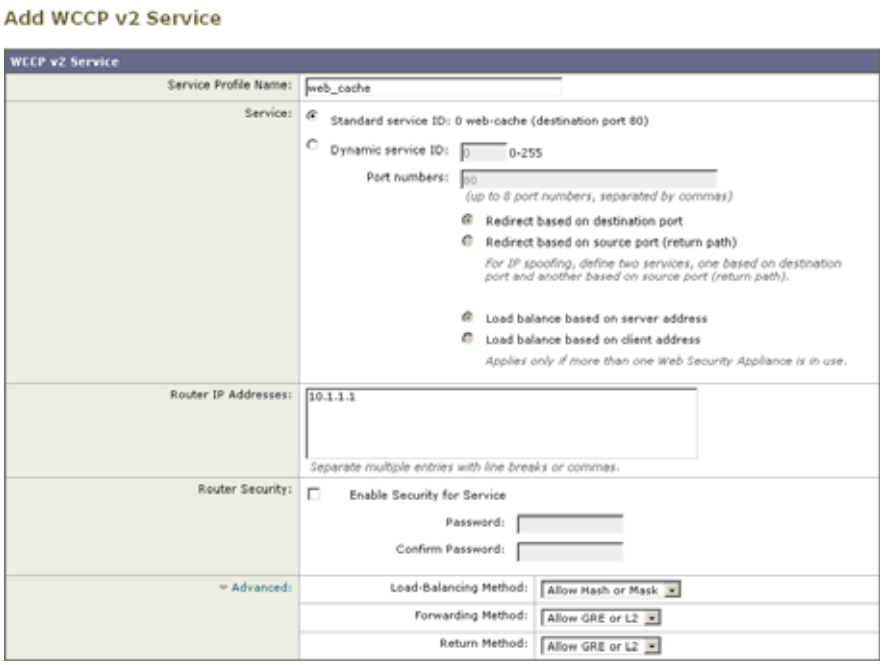
WCCP の設定例

この項では、アプライアンスに定義される WCCP サービスのいくつかの例とアプライアンスに接続するルータの設定に使用する対応する WCCP 設定を示します。

例 1

図 3-3 に示す WCCP サービスを使用しているとします。

図 3-3　WCCP サービスの例：標準サービス、パスワード不要



この例では、WCCP サービスは、標準サービス グループ（ウェルノウン サービス グループとも呼ばれます）を定義します。デフォルトで、リダイレクションの基礎は宛先ポートにあります。この例では、このサービス グループのルータで ethernet1 インターフェイスを設定することも想定します。

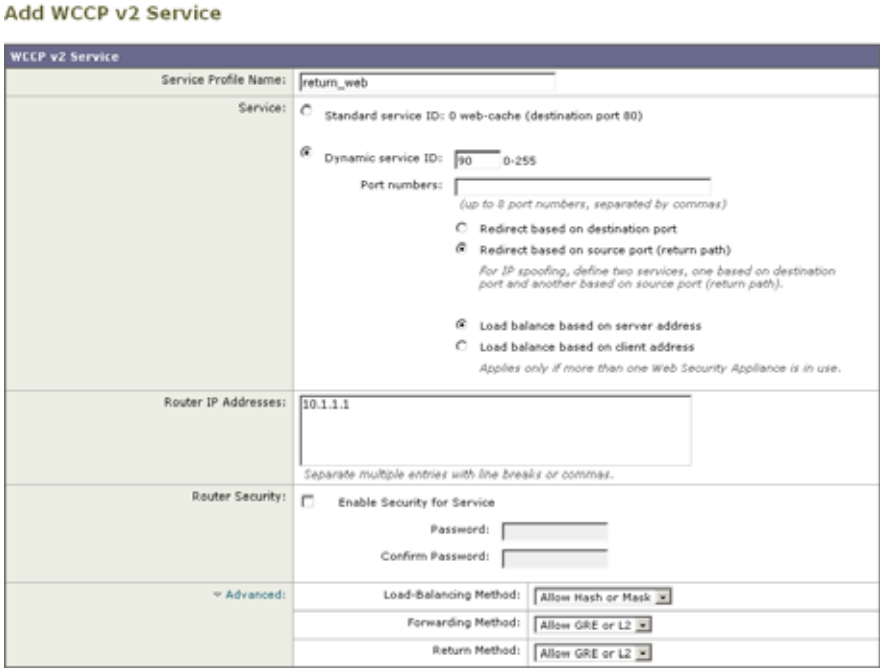
この例では、次の WCCP 設定を使用します。

```
ip wccp version 2
ip wccp web-cache
interface ethernet1
ip wccp web-cache redirect in
```

例 2

図 3-4 は、IP スプーフィングがイネーブルであり、図 3-3（P.3-8）に示す WCCP サービスが定義されている場合に作成するダイナミック サービスを示します。

図 3-4　WCCP サービスの例：IP スプーフィングのダイナミック サービス



この例では、WCCP サービスは、サービス ID 90 を持つダイナミック サービス グループを定義します。リダイレクションの基礎は送信元ポートにあります。このため、IP スプーフィングがイネーブルの場合のリターン パスに使用できます。この例では、このサービス グループのルータで ethernet0 インターフェイスを設定することも想定します。

この例では、次の WCCP 設定を使用します。

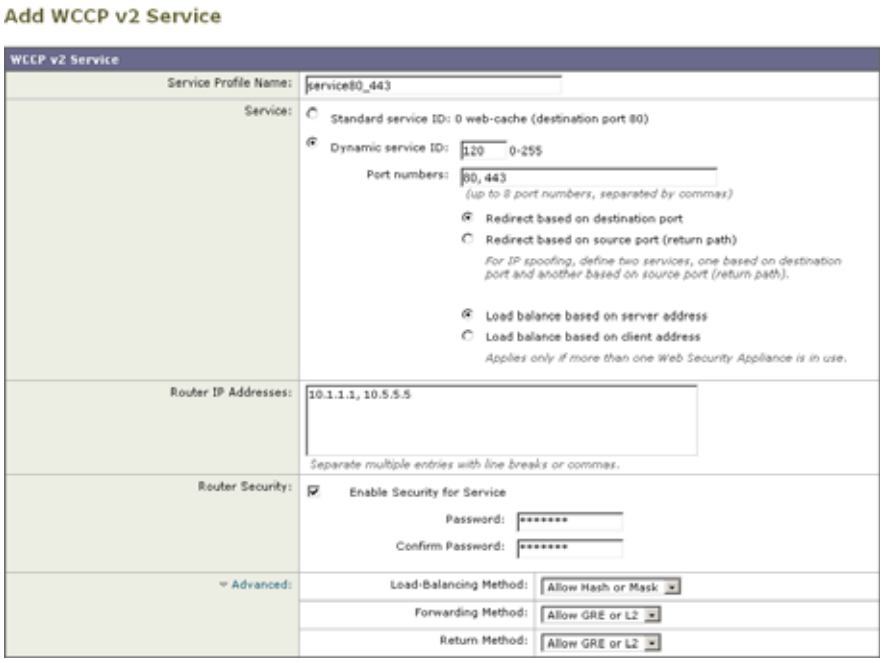
```
ip wccp version 2
ip wccp 90
interface ethernet0
ip wccp 90 redirect in
```

WCCP ルータを使用するときに IP スプーフィングをイネーブル化する方法の詳細については、「WCCP 使用時の IP スプーフィング」（P.25-14）を参照してください。

例 3

図 3-5 に示す WCCP サービスを使用しているとします。

図 3-5　　WCCP サービスの例：標準サービス、パスワード必須



この例では、WCCP サービスは、サービス ID 120 を持つダイナミック サービス グループを定義します。リダイレクションの基礎は宛先ポートにあります。このサービス グループ「admin99」のパスワードはイネーブルになっています（アプライアンス設定では非表示）。この例では、このサービス グループのルータで ethernet0 インターフェイスを設定することも想定します。

この例では、次の WCCP 設定を使用します。

```
ip wccp version 2
ip wccp 120
interface ethernet0
ip wccp 120 redirect in
ip wccp 120 password admin99
```

複数のアプライアンスおよびルータの使用

1 つ以上の WCCP ルータに 1 つ以上の Web セキュリティ アプライアンスを接続する場合、それらをまとめてクラスタと呼びます。クラスタには最大 32 のアプライアンスと 32 のルータを含めることができます。クラスタ内のすべてのアプライアンスやルータが相互に通信するように設定する必要があります。

既存のプロキシ環境での Web セキュリティ アプライアンスの使用

Web セキュリティ アプライアンスは、プロキシ対応デバイスで、既存のプロキシ環境内に容易に導入されます。ただし、既存のプロキシ サーバからダウンストリーム（つまり、クライアントの近くに）に配置することを推奨します。

システムセットアップウィザードまたは Web インターフェイスで初期セットアップした後で、既存のアップストリーム プロキシを使用するようにアプライアンスを設定できます。アップストリーム プロキシをイネーブルにするか、既存の設定を変更するには、[ネットワーク（Network）] > [プロキシ上位（Proxies Upstream）] ページを使用します。

アップストリーム プロキシを設定するときに、既存のプロキシをトランスペアレント モードにするか、明示的な転送モードにするかを指定します。

トランスペアレント アップストリーム プロキシ

トランスペアレント アップストリーム プロキシがクライアントの IP アドレスを使用してユーザ認証とアクセス制御を管理する場合、Web セキュリティ アプライアンス上で IP スプーフィングをイネーブルにし、クライアントの IP アドレスをアップストリーム プロキシに送信する必要があります。IP スプーフィングをイネーブルにするには、[セキュリティサービス（Security Services）] > [Web プロキシ（Web Proxy）] ページを使用します。

IP スプーフィングをイネーブルにし、アプライアンスを WCCP ルータに接続する場合は、少なくとも 2 つの WCCP サービスを作成する必要があります。IP スプーフィングをイネーブルにするときの WCCP サービスの設定に関する詳細については、「WCCP 使用時の IP スプーフィング」（P.25-14）を参照してください。

明示的な転送アップストリーム プロキシ

アップストリーム プロキシが明示的な転送モードの場合は、次のルールとガイドラインを考慮してください。

- アップストリーム プロキシの IP アドレスまたはホスト名、およびポートを入力する必要があります。
- アップストリーム プロキシのホスト名が複数の IP アドレスに解決されるかどうかを考慮します。Web セキュリティ アプライアンスは、起動時に IP アドレスの DNS サーバのみクエリーします。IP アドレスがそのホスト名に追加されるか、または削除される場合、新しい IP アドレスのセットにホスト名を追加し、プロキシを再起動してそのホスト名を解決する必要があります。
- アップストリーム プロキシがプロキシ認証を使用してユーザ認証またはアクセス コントロールを管理する場合、アップストリーム プロキシにクライアント ホスト ヘッダーを送信するために、X-Forwarded-For ヘッダーをイネーブルにする必要があります。X-Forwarded-For ヘッダー設定をイネーブルにするには、[セキュリティサービス（Security Services）] > [Web プロキシ（Web Proxy）] ページを使用します。
- Web セキュリティ アプライアンスが明示的な転送モードで導入されているときに、認証クレデンシャルをアップストリーム プロキシに情報を送信する場合は、`advancedproxyconfig > authentication` CLI コマンドを使用して、許可要求ヘッダーを親プロキシ サーバに転送するように Web プロキシを設定する必要があります。

（注）　デフォルトでは、Web プロキシは、セキュリティ上の理由からアップストリーム プロキシ サーバにプロキシ許可ヘッダーを転送しません。

- アップストリーム プロキシが PAC ファイルまたはログイン スクリプトを使用してクライアント トラフィックを管理する場合は、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使用して、これらのファイルを更新する必要があります。

L4 トラフィック モニタの導入

L4 トラフィック モニタ（L4TM）の導入は、Web プロキシの導入とは独立して行われます。L4 トラフィック モニタを接続し、導入する場合は、次の点を考慮します。

- **物理的な接続。**L4 トラフィック モニタをネットワークに接続する方法を選択できます。詳細については、「L4 トラフィック モニタの接続」（P.3-12）を参照してください。
- **Network Address Translation（NAT; ネットワーク アドレス変換）。**L4 トラフィック モニタを設定する場合は、出力ファイアウォールからインターネットに送信される前にできるだけ多くのネットワーク トラフィックを確認できるネットワークのポイントに接続します。L4 トラフィック モニタが、プロキシ ポートの後、およびクライアント 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が重要です。
- **L4 トラフィック モニタ アクションの設定。**L4 トラフィック モニタのデフォルト設定は、モニタのみです。セットアップ後、疑わしいトラフィックをモニタし、ブロックするように L4 トラフィックを設定する場合は、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でアクセスできるように L4 トラフィック モニタと Web プロキシが同じネットワーク上に設定されていることを確認します。

L4 トラフィック モニタの接続

次のいずれかの方法で、L4 トラフィック モニタをネットワークに接続できます。

- **ネットワーク タップ。**ネットワーク タップを使用する場合、次の通信タイプを選択できます。
  - **シンプレックス。**この通信タイプは、クライアントとアプライアンス間のすべてのトラフィックに 1 本のケーブルを使用し、アプライアンスと外部接続間のすべてのトラフィックに 1 本のケーブルを使用します。T1 ポートをネットワーク タップに接続して、すべての発信トラフィック（クライアントからインターネットへ）を受信し、T2 ポートをネットワーク タップに接続して、すべての着信トラフィック（インターネットからクライアントへ）を受信します。
  - **デュプレックス。**このモードは、すべての着信および発信トラフィックに 1 本のケーブルを使用します。半二重または全二重イーサネット接続を使用できます。T1 ポートをネットワーク タップに接続して、すべての発信トラフィックと着信トラフィックを受信します。

（注）　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。

- **L2 スイッチの SPAN/ ミラー ポート。**接続が 2 つの異なるデバイスまたは 1 つのデバイスを使用するかどうかに応じて、接続はシンプレックスまたはデュプレックス タップに類似します。
- **ハブ。**L4 トラフィック モニタをハブに接続するときは、デュプレックスを選択します。

アプライアンスをネットワークに接続する方法に関係なく、配線タイプを設定する必要があります。詳細については、「L4 トラフィック モニタの配線タイプの設定」（P.3-13）」を参照してください。

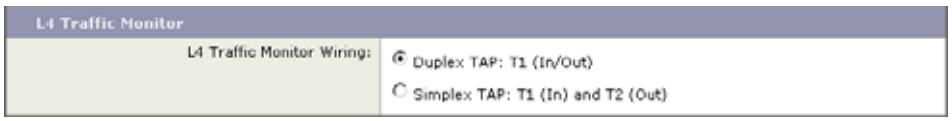
T1 および T2 ポートの詳細については、「アプライアンスのインターフェイス」（P.3-2）を参照してください。

（注）　可能な場合は、スイッチの SPAN/ミラー ポートではなくネットワーク タップを使用します。ネットワーク タップは、ハードウェアを使用してパケットを L4 トラフィック モニタに送信し、スイッチの SPAN/ミラー ポートは、ソフトウェアを使用してパケットを送信します。ハードウェア ソリューションは、ソフトウェア ソリューションよりも高パフォーマンスでパケットを送信し、処理中にパケットをドロップする可能性が低くなります。

L4 トラフィック モニタの配線タイプの設定

通常、L4 トラフィック モニタの配線タイプは、システム セットアップ中に設定されます。ただし、[ネットワーク（Network）] > [インターフェイス（Interfaces）] ページで、システム セットアップ ウィザードの実行後に配線タイプを設定できます。[設定を編集（Edit Settings）] をクリックし、T1 および T2 ポートの配線タイプを選択します。

図 3-6　　L4 トラフィック モニタの配線タイプ



4
インストールおよび構成

はじめる前に

Web セキュリティ アプライアンスを使用するには、システムセットアップウィザードを実行する必要があります。ただし、まずシステムセットアップウィザードのためのアプライアンスを準備するいくつかの手順を実行する必要があります。

仮想 Web セキュリティ アプライアンスを設定する場合、この章を続行する前に、『*Cisco Virtual Security Appliance Installation Guide*』を参照してください。

インストールのためのアプライアンスの準備に関する詳細については、Web セキュリティ アプライアンスの『*Quick Start Guide*』を参照してください。この Web セキュリティ アプライアンスのガイドおよびその他の役立つ情報は、Cisco IronPort カスタマー サポートから入手できます。

`http://www.cisco.com/web/ironport/index.html`

システムセットアップウィザードを実行する前に、次のタスクを完了してください。

- **展開。**ネットワーク内にどのようにアプライアンスを設定するかを決めます。詳細については、「導入」（P.3-1）を参照してください。
- **ラップトップのネットワーク接続。**Web セキュリティ アプライアンスと同じサブネット上の IP アドレス（192.168.42.xx）を使用するようにラップトップのネットワーク接続を設定します。詳細については、「アプライアンスへのラップトップの接続」（P.4-2）を参照してください。
- **アプライアンスの物理接続。**アプライアンスの背面パネルにある適切なポートに、イーサネットケーブルを差し込みます。詳細については、「ネットワークへのアプライアンスの接続」（P.4-2）を参照してください。
- **設定情報。**アプライアンスをネットワークにインストールする方法がわかっている場合は、IP アドレスなど、システムセットアップウィザードに必要なすべての情報を収集します。詳細については、「設定情報の収集」（P.4-3）を参照してください。
- **既存のプロキシ サーバ。**既存のプロキシ サーバを持つネットワークで Web セキュリティ アプライアンスを使用する予定の場合は、他のプロキシ サーバのダウンストリームでそれを見つけ出す必要があります。アプライアンスの初期設定を完了後、既存のプロキシ サーバで動作するように設定する必要もあります。既存のプロキシを持つネットワークへのアプライアンスの展開の詳細については、「既存のプロキシ環境での Web セキュリティ アプライアンスの使用」（P.3-11）を参照してください。

アプライアンスへのラップトップの接続

システムセットアップウィザードを初めて実行する場合は、アプライアンスをラップトップなどのコンピュータに接続する必要があります。アプライアンスに接続するには、ラップトップのサブネットがアプライアンスのサブネットと同じである必要があります。管理ポートには、M1 と M2 というラベルが付いています。Web セキュリティ アプライアンスは M1 管理ポートだけを使用します。M2 は使用しません。

アプライアンスと同じサブネット（192.168.42.xx）にあるように、ラップトップの IP アドレスを設定します。次に、アプライアンスの背面の M1 ポートにラップトップを接続します。

ネットワークへのアプライアンスの接続

アプライアンスの背面パネルにある適切なポートにイーサネット ケーブルを差し込む必要があります。アプライアンスのイーサネット ポートの詳細については、「アプライアンスのインターフェイス」（P.3-2）を参照してください。

アプライアンスの展開方法に応じて、イーサネット ケーブルを差し込む場所は次のようになります。

- **トランスペアレント モードの Web プロキシ。**すべてのトラフィックに 1 個のプロキシ ポートを使用する場合は、イーサネット ケーブルを使用して、ポート P1 をレイヤ 4 スイッチまたは WCCP ルータに接続します。トラフィックに 2 個のプロキシ ポートを使用する場合は、イーサネット ケーブルを使用して、ポート P2 をレイヤ 4 スイッチまたは WCCP ルータに接続し、ポート P1 を内部ネットワークに接続します。

  トランスペアレント モードでの Web プロキシの展開の詳細については、「トランスペアレント モードでの Web プロキシの導入」（P.3-5）を参照してください。

（注）　トランスペアレント モードでプロキシを設定し、WCCP ルータに接続する場合は、システム セットアップウィザードを実行して少なくとも 1 つの WCCP サービスを作成してからアプライアンスを設定する必要があります。WCCP サービス作成の詳細については、「WCCP サービスの追加と編集」（P.25-14）を参照してください。

- **明示的な転送モードの Web プロキシ。**すべてのトラフィックに 1 個のプロキシ ポートを使用する場合は、イーサネット ケーブルを使用して、ポート P1 をネットワーク スイッチに接続します。トラフィックに 2 個のプロキシ ポートを使用する場合は、イーサネット ケーブルを使用して、ポート P2 をネットワーク スイッチに接続し、ポート P1 を内部ネットワークに接続します。

  明示的な転送モードでの Web プロキシの展開の詳細については、「明示的な転送モードでの Web プロキシの導入」（P.3-4）を参照してください。

- **L4 トラフィック モニタ。**タップの通信タイプに従って、トラフィック モニタリング ポートをイーサネット タップに接続します。：
  - **シンプレックスを使用するイーサネット タップ。**ポート T1 をイーサネット タップに接続して、すべての発信トラフィック（クライアントからインターネットへ）を受信し、ポート T2 をイーサネット タップに接続して、すべての着信トラフィック（インターネットからクライアントへ）を受信します。
  - **デュプレックスを使用するイーサネット タップ。**ポート T1 をイーサネット タップに接続して、すべての発信トラフィックと着信トラフィックを受信します。

  L4 トラフィック モニタの展開の詳細については、「L4 トラフィック モニタの導入」（P.3-12）を参照してください。

設定情報の収集

ネットワークにアプライアンスをインストールする方法を確認したら、IP アドレスなどの必要な情報を収集して、システムセットアップウィザードに入力できます。表 4-1 に示すワークシートを使用して、特定した設定オプションを書き込むことができます。これで、システムセットアップウィザードを実行し、ワークシートに入力した情報を使用して初期設定を行うことができます。

表 4-1　システム セットアップ ワークシート

ネットワーク設定	
デフォルト システム ホスト名：	詳細については、「DNS サポート」（P.4-5）を参照してください。
DNS サーバ：	インターネットのルート DNS サーバ/組織の DNS サーバ
組織の DNS サーバ： （最大 3 つ）	1. 2. 3.
ネットワーク タイム プロトコル サーバ：	
タイム ゾーンの領域：	
タイム ゾーンの国：	
タイム ゾーン/GMT オフセット：	
ネットワーク コンテキスト	
ネットワーク上の別のプロキシの有無：	はい/いいえ
他のプロキシ IP アドレス：	
他のプロキシ ポート：	
インターフェイスの設定	
管理ポート	
IP アドレス：	
ネットワーク マスク：	
ホスト名：	
データ ポート	
IP アドレス：	
ネットワーク マスク：	
ホスト名：	
注：Web プロキシは、管理インターフェイスを共有できます。データ インターフェイスの IP アドレスと管理インターフェイスの IP アドレスを別々に設定した場合は、同じサブネットを共有できません。	
L4 トラフィック モニタ	
L4 トラフィック モニタの配線タイプ：	シンプレックス ネットワーク タップ/デュプレックス ネットワーク タップ
ルート	
管理トラフィック	

表 4-1　システム セットアップ ワークシート （続き）

デフォルト ゲートウェイ：	
スタティック ルート テーブル名：	
スタティック ルート テーブルの宛先ネットワーク：	
スタティック ルート テーブルのゲートウェイ：	
データ トラフィック	
デフォルト ゲートウェイ：	
スタティック ルート テーブル名：	
スタティック ルート テーブルの宛先ネットワーク：	
スタティック ルート テーブルのゲートウェイ：	
透過的接続設定	
デバイス タイプ	レイヤ 4 スイッチまたはデバイスなし/WCCP ルータ
WCCP v2 ルータの場合、標準サービスをイネーブルにする。	はい/いいえ
標準サービスのルータ アドレス：	
ルータ セキュリティをイネーブルにする。	いいえ/はい、パスワード： _____
注：アプライアンスを WCCP ルータに接続する際は、システムセットアップウィザードの実行後に WCCP サービスが作成されるように、Web セキュリティ アプライアンスの設定が必要になる場合があります。WCCP サービス作成の詳細については、「WCCP サービスの追加と編集」（P.25-14）を参照してください。	
管理設定	
管理者パスワード：	
電子メール システム アラーの送信先：	
SMTP リレー ホスト：	（任意）
AutoSupport:	イネーブル/ディセーブル
SensorBase ネットワーク参加：	イネーブル/ディセーブル
参加レベル：	制限付き/標準
セキュリティ サービス	
グローバル ポリシーのデフォルト アクション：	すべてのトラフィックをモニタ/すべてのトラフィックをブロック
L4 トラフィック モニタ：	モニタのみ/ブロック
許容できる使用の制御：	イネーブル/ディセーブル
評価フィルタリング：	イネーブル/ディセーブル
マルウェアおよびスパイウェアのスキャン：	Webroot をイネーブルにする/McAfee をイネーブルにする/両方をイネーブルにする
検出されたマルウェアに対する措置：	モニタのみ/ブロック
Cisco IronPort データ セキュリティ フィルタリング：	イネーブル/ディセーブル

DNS サポート

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 ホスト名と IP アドレスを DNS サーバ データベースに追加する必要があります。

仮想アプライアンスのライセンスのロード

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

システム セットアップ ウィザード

Cisco IronPort AsyncOS オペレーティング システムは、初期システム設定の手順を順を追って説明するブラウザ ベースのウィザードが用意されています。このシステムセットアップウィザードを使用して、ネットワーク設定やセキュリティ設定などの基本的な初期設定を行います。システムセットアップウィザードは、[システム管理（System Administration）] タブにあります。

初めて Web セキュリティ アプライアンスをインストールするときは、システムセットアップウィザードを実行する必要があります。システムセットアップウィザードを完了すると、アプライアンスは Web トラフィックをモニタできるようになります。ただし、システムセットアップウィザードではカバーされない、よりカスタマイズされた設定をアプライアンスに適用したい場合があります。設定オプションに関する詳細については、このガイドの他の大部分の章を参照してください。

システムセットアップウィザードを実行する前に、「はじめる前に」（P.4-1）を参照して、アプライアンスの設定に必要な情報がすべて用意されていることを確認してください。この情報を事前に準備しておくことで、初期設定の完了に必要な時間を短縮できます。また、『*Quick Start Guide*』を読み、製品のセットアップに関する情報を確認する必要もあります。

警告　**システムセットアップウィザードを実行すると、Web セキュリティ アプライアンスは完全に再設定され、管理者パスワードはリセットされます。初めてアプライアンスをインストールする場合、または既存の設定を完全に上書きする場合にのみ、システムセットアップウィザードを使用してください。アプライアンスの設定が完了した後にシステムセットアップウィザードを実行すると、クライアントによる Web へのアクセスが遮断される場合があります。初期設定を完了後、システムセットアップウィザードを実行するように選択する場合は、[システム管理（System Administration）] > [設定ファイル（Configuration File）] ページを使用して設定の概要を出力し、現在の設定ファイルをアーカイブします。**

警告　**アプライアンスには、管理インターフェイス（ポート）にデフォルト IP アドレス 192.168.42.42 が付属しています。アプライアンスをネットワークに接続する前に、ネットワーク上の他のデバイスに同じ IP アドレスが使用されていないことを確認します。**

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

工場出荷時の設定を持つ複数アプライアンスをネットワークに接続する場合は、一つずつ追加して、各アプライアンスのデフォルト IP アドレスを順に再設定してください。

システムセットアップウィザードには、設定情報を入力する次のタブが用意されています。

- **[開始（Start）]。**詳細については、「手順 1：EULA に同意してセットアップを開始する」（P.4-6）を参照してください。
- **[ネットワーク（Network）]。**詳細については、「手順 2：ネットワークの設定」（P.4-7）を参照してください。
- **[セキュリティ（Security）]。**詳細については、「手順 3：セキュリティ」（P.4-12）を参照してください。
- **[レビュー（Review）]。**詳細については、「手順 4：レビューおよびインストール」（P.4-14）を参照してください。

システムセットアップウィザードへのアクセス

システムセットアップウィザードにアクセスするには、ブラウザを開き、Web セキュリティ アプライアンスの IP アドレスを入力します。初めてシステムセットアップウィザードを実行するときは、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。

アプライアンスのログイン画面が表示されます。ユーザ名とパスワードを入力して、アプライアンスにアクセスします。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**

（注） アイドル時間が 30 分以上続くか、ログアウトしないでブラウザを閉じた場合は、セッションがタイムアウトされます。この場合、ユーザ名とパスワードを再入力する必要があります。

手順 1：EULA に同意してセットアップを開始する

ステップ 1　ページの下部にあるチェックボックスをオンにして、エンド ユーザ ライセンス契約書の条件に同意します。

ステップ 2　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。

手順 2：ネットワークの設定

ステップ 1　表 4-2 に記載された参照情報を使用して、[ステム設定（System Setting）] オプションを設定し、[次へ（Next）] をクリックします。

表 4-2　システムセットアップウィザード の [システム設定（System Setting）] オプション

オプション	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。この名前は、ネットワーク管理者が割り当てる必要があります。このホスト名は、システム アラートでアプライアンスを識別するために使用されます。
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）	ドメイン名のサービス ルックアップにインターネットのルート DNS サーバを使用するようにアプライアンスを設定します。 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ときに、このオプションを選択する場合があります。 アプライアンスでは、着信接続のための DNS ルックアップを実行するために、稼働中の DNS サーバを利用できる必要があります。アプライアンスのセット アップ時にアプライアンスが到達できる稼働中の DNS サーバを指定できない場合は、インターネットのルート DNS サーバを使用するか、または管理インターフェイスの IP アドレスを一時的に割り当てるように設定し、システムセットアップウィザードを完了できます。 DNS 設定のコンフィグレーションに関する詳細については、「DNS サーバの設定」（P.25-18）を参照してください。
DNS サーバ：（DNS Server(s):） これらの DNS サーバを使用（Use these DNS Servers）	ドメイン名のサービス ルックアップにローカルの DNS サーバを指定します。少なくとも 1 つ、最大で合計 3 つの DNS サーバを入力します。 インターネットのルート DNS サーバを使用するか、または独自の DNS サーバを指定することもできます。 DNS 設定のコンフィグレーションに関する詳細については、「DNS サーバの設定」（P.25-18）を参照してください。
NTP サーバ（NTP Server）	Network Time Protocol（NTP）サーバを使用して、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します。 デフォルトでは、Cisco IronPort タイム サーバ（time.ironport.com）が入力されます。
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。ドロップダウン メニューを使用してタイム ゾーンを見つけるか、GMT オフセットを使用してタイム ゾーンを定義します。 GMT オフセットの詳細については、「タイム ゾーンの設定」（P.26-31）を参照してください。

ステップ 2　任意で、表 4-3 に記載された参照情報を使用して、外部プロキシ サーバを設定し、[次へ（Next）] をクリックします。

（注）　システムセットアップウィザードを実行後、ネットワーク上の複数のプロキシ サーバと対話するように Web セキュリティ アプライアンスを設定できます。外部プロキシ サーバの設定の詳細については、「外部プロキシの使用の概要」（P.10-1）を参照してください。

表 4-3　システムセットアップウィザード の [ネットワーク コンテキスト（Network Context）] オプション

オプション	説明
プロキシ グループ名（Proxy group name）	プロキシ グループの名前を選択します。
アドレス（Address）	組織のネットワーク内のプロキシ サーバのアドレスを入力します。
ポート（Port）	組織のネットワーク内のプロキシ サーバのポート番号を入力します。

システムセットアップウィザードは、ユーザが表 4-3 で指定した情報を持つプロキシ グループを作成します。後でプロキシ グループを編集して、追加プロキシ サーバを含めたり、ロード バランシング オプションを設定したりできます。システム セットアップ後、追加プロキシ グループを作成することもできます。

（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。

ステップ 3　図 4-1 および表 4-4 の参照情報を使用して、[ネットワーク インターフェイスと配線（Network Interfaces and Wiring）] オプションを設定して、[次へ（Next）] をクリックします。

（注）　Web セキュリティ アプライアンスには、マシンの物理ポートに関連付けられたネットワーク インターフェイスが用意されています。

図 4-1　システム セットアップ ウィザード : [ネットワーク（Network）] タブ、[ネットワーク インターフェイスと配線（Network Interfaces and Wiring）] ページ

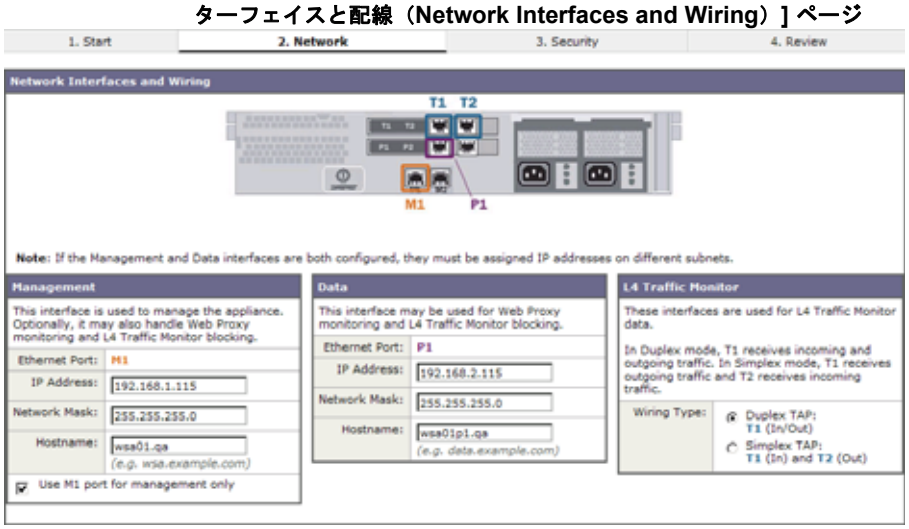


表 4-4　システムセットアップウィザードの [ネットワーク インターフェイスと配線（Network Interfaces and Wiring）] オプション

オプション	説明
管理（Management）	Web セキュリティ アプライアンスの管理に使用する IP アドレス、ネットワーク マスク、およびホスト名を入力します。管理ネットワーク上にある IP アドレスを入力します。 デフォルトで、アプライアンスは管理およびプロキシ（データ）トラフィックの両方に M1 インターフェイスを使用します（[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*オフ*にします）。 ただし、任意で、[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することで、管理トラフィック専用として M1 インターフェイスを使用できます。これは、組織が別の管理ネットワークを使用する場合に行うことがあります。これにより、プロキシ トラフィックが管理インターフェイス上のアプライアンスに確実に到達しないようにすることによって、セキュリティを強化できます。 M1 を管理トラフィック専用として使用する場合は、プロキシ トラフィックに少なくとも 1 つのデータ インターフェイスを設定する必要があります。また、管理およびデータ トラフィック用に異なるルートを定義する必要もあります。

表 4-4　システムセットアップウィザードの [ネットワーク インターフェイスと配線（Network Interfaces and Wiring）] オプション （続き）

オプション	説明
データ（Data）	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、およびホスト名を入力します。 M1 インターフェイスを管理トラフィック専用として設定する場合は、データ トラフィック用の P1 インターフェイスを設定する必要があります。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。 Web プロキシ モニタリングと任意で L4 トラフィック モニタリングのデータ インターフェイスを使用できます。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ように、このインターフェイスを設定することもできます。 **注：**システムセットアップウィザードのデータ トラフィック用の P1 ネットワーク インターフェイスのみをイネーブルにし、設定できます。P2 インターフェイスをイネーブルにする場合は、システムセットアップウィザードを終了してから、`ifconfig` コマンドを使用する必要があります。P2 インターフェイスの設定の詳細については、「ネットワーク インターフェイスの設定」（P.25-2）を参照してください。
L4 トラフィック モニタ（L4 Traffic Monitor）	「T」インターフェイスに差し込まれている有線接続を選択します。 • **デュプレックス タップ。**T1 ポートが着信トラフィックおよび発信トラフィックの両方を受信する場合、[デュプレックス タップ（Duplex TAP）] を選択します。半二重または全二重イーサネット接続を使用できます。 • **シンプレックス タップ。**T1 ポートを内部ネットワーク（クライアントからインターネットへのトラフィック フロー）に接続し、T2 ポートを外部ネットワーク（インターネットからクライアントへのトラフィック フロー）に接続する場合は、シンプレックス タップを選択します。 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。

ステップ 4　表 4-5 に記載された参照情報を使用して、[管理およびデータ トラフィックのルート（Routes for Management and Data Traffic）] オプションを設定し、[次へ（Next）] をクリックします。

（注）　このページのオプションは、[ポート M1 は管理目的でのみ使用（Use M1 port for management only）] の設定によって異なります。

表 4-5　システムセットアップウィザードの [管理とデータ用トラフィックのルート（Routes for Management and Data Traffic）] オプション

オプション	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 IP アドレスを入力します。

表 4-5　システムセットアップウィザードの [管理とデータ用トラフィックのルート（Routes for Management and Data Traffic）] オプション （続き）

オプション	説明
スタティック ルート テーブル（Static Routes Table）	任意で、1 つまたは複数の管理トラフィックやデータ トラフィックのスタティック ルートを追加できます。 スタティック ルートを追加するには、ルート、宛先ネットワーク、およびゲートウェイ IP アドレスの名前を入力し、[ルートを追加（Add Route）] をクリックします。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。 入力したスタティック ルートを削除するには、テーブルのスタティック ルート エントリの横にある [削除（Delete）] ボタンをクリックします。 スタティック ルートの詳細については、「TCP/IP トラフィック ルートの設定」（P.25-4）を参照してください。

ステップ 5　表 4-6 に記載された参照情報を使用して、透過的な接続オプションを選択し、[次へ（Next）] をクリックします。

（注）　デフォルトでは、システムセットアップウィザードを実行すると、Web プロキシはトランスペアレント モードで展開されます。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、レイヤ 4 スイッチまたは WCCP バージョン 2 ルータに接続する必要があります。

表 4-6　[トランスペアレント接続（Transparent Connection）] のオプションシステムセットアップ ウィザード

オプション	説明
レイヤ 4 スイッチもしくはデバイスなし（Layer 4 Switch or No Device）	Web セキュリティ アプライアンスがレイヤ 4 スイッチに接続されている場合、またはシステム セットアップ ウィザードを実行後、明示的な転送モードで Web プロキシを展開する場合は、このオプションを選択します。
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場合、このオプションを選択します。 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。システム セットアップ時に標準サービス（「web-cache」サービスとも呼ばれます）をイネーブルにして、システムセットアップウィザードを実行後、別個または追加の WCCP サービス グループを設定できます。 標準サービスをイネーブルにする場合は、標準サービス グループのパスワードの入力を求めるかどうかを選択します。必要に応じて、[パスワード（Password）] フィールドにパスワードを入力します。パスワードは 7 文字以下の文字列です。 WCCP サービス作成の詳細については、「WCCP サービスの追加と編集」（P.25-14）を参照してください。

ステップ 6　表 4-7 に記載された参照情報を使用して、[管理用設定（Administrative Settings）] オプションを設定し、[次へ（Next）] をクリックします。

表 4-7　システムセットアップウィザードの [管理用設定（Administrative Settings）]

オプション	説明
管理者のパスワード（Administrator Password）	パスワードを入力して、Web セキュリティ アプライアンスにアクセスします。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）	アプライアンスがアラートを送信するアカウントの電子メール アドレスを入力します。 アラートの詳細については、「アラートの管理」（P.26-18）を参照してください。
SMTP リレー ホスト経由で電子メールを送信（Send Email via SMTP Relay Host）	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を入力できます。 任意で、ポート番号も入力できます。ポート番号が定義されていない場合、AsyncOS はポート 25 を使用します。 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。 SMTP リレー ホストの設定の詳細については、「SMTP リレー ホストの設定」（P.25-17）を参照してください。
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 Cisco IronPort カスタマー サポートに送信するかどうかを選択します。
SensorBase ネットワークに参加（SensorBase Network Participation）	Cisco SensorBase ネットワークに参加するかどうかを選択します。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。 SensorBase ネットワークの詳細については、「Cisco SensorBase ネットワークへの参加」（P.2-11）を参照してください。

手順 3：セキュリティ

[セキュリティ（Security）] タブで、特定のコンポーネントをブロックするか、またはモニタするかなど、イネーブルにするセキュリティ サービスを設定できます。[セキュリティ（Security）] タブは 1 ページで構成されます。

ステップ 1　表 4-8 に記載された参照情報を使用して、[セキュリティ サービス（Security Services）] オプションを設定し、[次へ（Next）] をクリックします。

表 4-8　システムセットアップウィザードの [セキュリティ（Security）] オプション

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を完了後、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、またはモニタするかを選択します。すべてのトラフィックをブロックするように選択すると、グローバル アクセス ポリシーは、HTTP、HTTPS、FTP などのプロキシ化されたプロトコルをすべてブロックします。モニタするように選択すると、プロキシ化されたプロトコルがブロックされることはありません。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。 制限が適切に設定されたユーザ定義のアクセス ポリシーを定義し、必要に応じてグローバル アクセス ポリシーの編集が完了するまで、グローバル アクセス ポリシーのすべてのトラフィックをブロックする場合があります。
L4 トラフィック モニタ（L4 Traffic Monitor）	レイヤ 4 トラフィック モニタでレイヤ 4 トラフィックをモニタするか、またはブロックするかを選択します。 L4 トラフィック モニタは、すべてのネットワーク ポートの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します。 Web セキュリティ アプライアンスを評価する際にトラフィックをモニタしたり、アプライアンスを購入して使用する際にトラフィックをブロックしたりする場合があります。 詳細については、「L4 トラフィック モニタの設定」（P.21-2）を参照してください。
使用許可コントロール（Acceptable Use Controls）	使用許可コントロールをイネーブルにして、URL フィルタリングを使用可能にするかどうかを選択します。URL フィルタリングを使用すると、要求の URL カテゴリに基づいてユーザ アクセスを制御できます。ユーザによる特定のタイプの Web サイトへのアクセスを制限する場合は、このオプションをイネーブルにします。 詳細については、「URL フィルタ」（P.17-1）を参照してください。
レピュテーション フィルタリング（Reputation Filtering）	グローバル ポリシー グループの Web 評価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。カスタム アクセス ポリシー グループを作成する際に、Web 評価フィルタリングをイネーブルにするかどうかを選択できます。 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。 不審なアクティビティやマルウェア攻撃が発生する前に、これらのアクティビティを識別し、攻撃を阻止する場合には、このオプションをイネーブルにします。 詳細については、「Web レピュテーション フィルタの概要」（P.19-2）を参照してください。

表 4-8　システムセットアップウィザードの [セキュリティ（Security）] オプション （続き）

オプション	説明
マルウェアとスパイウェアのスキャン（Malware and Spyware Scanning）	Webroot、McAfee または Sophos を使用して、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選択します。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、またはブロックするかを選択します。 Web セキュリティ アプライアンスを評価する際にマルウェアをモニタしたり、アプライアンスを購入して使用する際にマルウェアをブロックしたりする場合があります。 システムセットアップウィザードを完了後、マルウェア スキャンを追加設定することもできます。詳細については、「ポリシーへの Web レピュテーションとアンチマルウェアの設定」（P.19-11）を参照してください。
Cisco IronPort データ セキュリティ フィルタリング（Cisco IronPort Data Security Filtering）	Cisco IronPort 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選択します。Cisco IronPort データ セキュリティ フィルタは、HTTP、HTTPS、および 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、どのデータが、どこに、どのようにして、誰によって発信されるかを制御します。 Cisco IronPort データ セキュリティ ポリシーを作成し、特定のタイプのアップロード要求をブロックする場合は、このオプションをイネーブルにします。 詳細については、「データ セキュリティと外部 DLP ポリシーの概要」（P.13-1）を参照してください。

手順 4：レビューおよびインストール

システムセットアップウィザードの最後のタブでは、設定の概要を表示します。

ステップ 1　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 2　[この設定をインストール（Install This Configuration）] をクリックします。

管理インターフェイスの IP アドレスを現在の値から変更した場合は、[この設定をインストール（Install This Configuration）] をクリックすると、現在の URL への接続が失われます。ただし、ブラウザは新しい IP アドレスに自動的にリダイレクトします。IP アドレスを現在の値から変更しなかった場合は、[システム管理（System Administration）] > [システム セットアップ（System Setup）] > [次のステップ（Next Steps）] ページが表示されます。

5
Web プロキシ サービス

Web プロキシの概要

ネットワークで Web プロキシとして Web セキュリティ アプライアンスを使用すると、次のトランスポート プロトコルを使用するネットワーク トラフィックを処理して、制御できます。

- HTTP
- FTP
- HTTPS
- SOCKS

イネーブルの場合、Web プロキシは HTTP トラフィックおよび FTP トラフィックを処理します。HTTPS トラフィックを処理するには、Web プロキシおよび HTTPS プロキシをイネーブルにする必要があります。SOCKS トラフィックを処理するには、Web プロキシおよび SOCKS プロキシをイネーブルにする必要があります。

関連トピック

- 「HTTP トラフィックの処理のイネーブル化」（P.5-2）
- 「HTTPS トラフィックの処理のイネーブル化」（P.5-2）
- 「FTP プロキシ設定値の設定」（P.5-9）
- 「SOCKS トラフィックの処理のイネーブル化」（P.6-2）

Web プロキシ サービスについて

Web プロキシは、Web 上の他のサーバの要求を行うことによって、クライアントの ワールドワイド ウェブ要求を処理するコンピュータ システムまたはソフトウェアです。Web セキュリティ アプライアンスは、Web プロキシ機能をイネーブルにすると、Web プロキシとして機能します。

Web プロキシ サービスは、内部ネットワークのクライアントから送信されるトラフィックをモニタおよび制御します。通常、Web プロキシ対応の Web セキュリティ アプライアンスはクライアントとファイアウォールの間に配置し、クライアントからサーバへのコンテンツの要求を傍受します。

HTTP トラフィックの処理のイネーブル化

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

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　[Web プロキシを有効にする（Enable Web Proxy）] を選択します。

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

関連トピック

- 「Web プロキシの設定」（P.5-3）
- 「HTTPS トラフィックの処理のイネーブル化」（P.5-2）
- 「FTP プロキシ設定値の設定」（P.5-9）
- 「SOCKS トラフィックの処理のイネーブル化」（P.6-2）

HTTPS トラフィックの処理のイネーブル化

はじめる前に

HTTPS トラフィックの処理をイネーブルにする前に、HTTP および FTP トラフィックの処理もイネーブルにする必要があります。

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

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

関連トピック

- 第 11 章「HTTPS トラフィックの処理」

Web プロキシの展開オプション

次のいずれかのタイプとして Web プロキシを設定できます。

- **トランスペアレント プロキシ。**アプライアンスをトランスペアレント プロキシとして設定すると、クライアントは Web プロキシを認識しません。Web ブラウザなどのクライアント アプリケーションは、アプライアンスに合わせて設定する必要はありません。Web ブラウザを再構成するユーザが管理者に通知せずにアプライアンスをバイパスする可能性を排除するため、トランスペアレント プロキシとしてアプライアンスを設定する必要がある場合があります。トランスペアレント プロキシとしてアプライアンスを設定するには、レイヤ 4 スイッチまたは WCCP ルータに接続する必要があります。

  トランスペアレント モードでプロキシを設定する場合にアプライアンスを設定する方法の詳細については、「透過的リダイレクションの設定」（P.25-11）を参照してください。

- **明示的な転送プロキシ。**明示的な転送プロキシ設定では、Web 上のサーバへの要求を処理するために、アプライアンスがクライアントの Web ブラウザの代わりに機能します。ユーザは、単一の Web セキュリティ アプライアンスを指すように Web ブラウザを設定する必要があります。レイヤ 4 スイッチまたは WCCP ルータがない場合、明示的な転送プロキシとしてアプライアンスを設定する必要がある場合があります。

他のプロキシ サーバが使用されているネットワークで Web セキュリティ アプライアンスを使用できます。ネットワークに別のプロキシが使用されている場合にアプライアンスを展開および設定する方法の詳細については、「既存のプロキシ環境での Web セキュリティ アプライアンスの使用」（P.3-11）を参照してください。

Web プロキシは、HTTP トランザクションとネイティブ FTP トランザクションの両方を処理します。FTP での操作の詳細については、「FTP 接続での操作」（P.5-7）を参照してください。

Web プロキシ キャッシュ

デフォルトでは、AsyncOS は Web プロキシ キャッシュを使用して、場合により Web にアクセスするユーザのパフォーマンスを向上させます。

Web プロキシおよびプロキシ キャッシュを次のように編集できます。

- **キャッシュから URL を削除する。**`webcache` CLI コマンドの `evict` サブコマンドを使用して、キャッシュから 1 つ以上の URL を削除します。
- **キャッシュしないドメインまたは URL を指定する。**`webcache` CLI コマンドの `ignore` サブコマンドを使用して、Web プロキシがプロキシ キャッシュに保存しない 1 つ以上のドメインまたは URL を指定します。キャッシュしないように指定する URL に組み込み正規表現（regex）文字を含めることができます。

各アクセス ログ ファイル エントリには、アプライアンスがクライアント要求を解決した方法を示すトランザクション結果コードが含まれます。トランザクション結果コードは、トランザクションがプロキシ キャッシュまたは宛先サーバからのものかを示します。トランザクション結果コードの詳細については、「トランザクション結果コード」（P.24-19）を参照してください。

Web プロキシの設定

このページでは、プロキシ サービスをカスタマイズするための基本および高度な設定を構成できます。

Web プロキシ設定は、HTTP または HTTPS を介す、すべての接続に適用されます。ネイティブ FTP 接続に対してプロキシ設定を構成するには、「FTP 接続での操作」（P.5-7）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）] > [Web プロキシ（Web Proxy）] ページの順に移動します。

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　[プロキシを有効にする（Enable Proxy）] フィールドが選択されていることを確認します。

ステップ 4　基本および高度な Web プロキシ設定を構成します。

表 5-1　Web プロキシの設定

プロパティ	説明
HTTP ポートからプロキシへ（HTTP Ports to Proxy）	HTTP 要求に対して Web プロキシがモニタするポートを入力します。 デフォルトは 80 および 3128 です。 WCCP を使用した展開では、HTTP および HTTPS ポートを合わせたポート エントリの最大数は 30 です。エントリ数を減らすためにポート範囲を使用できます。ポート番号およびポート範囲の両方を使用できます。例：80, 3128, 14001-14015。
キャッシュ（Caching）	キャッシングがイネーブルの場合、Web プロキシが要求と応答をキャッシュします。
プロキシモード（Proxy Mode）	Web プロキシの展開方法を選択します。 • **[トランスペアレント モード（Transparent mode）]。**クライアント アプリケーションは Web プロキシを認識しないため、プロキシに接続するように設定する必要はありません。トランスペアレント モードでは、Web プロキシは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の両方を受け入れることができます。 詳細については、「トランスペアレント モードでの Web プロキシの導入」（P.3-5）を参照してください。 • **[明示的順方向モード（Explicit forward mode）]。**Web ブラウザなどのクライアント アプリケーションは、Web プロキシを認識するため、単一の Web セキュリティ アプライアンスを指すように設定する必要があります。明示的な転送モードでは、Web プロキシは明示的に転送された接続だけを受け入れることができます。 詳細については、「明示的な転送モードでの Web プロキシの導入」（P.3-4）を参照してください。
IP スプーフィング（IP Spoofing）	要求をアップストリーム プロキシおよびサーバに送信するときに Web プロキシが IP アドレスをスプーフィングするかどうかを選択します。 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、透過的にリダイレクトされた接続のみまたはすべての接続で（透過的にリダイレクトされ、明示的に転送される）、IP スプーフィングをイネーブルにします。 IP スプーフィングがイネーブルの場合、クライアントから送信される要求はクライアントの送信元アドレスを保持し、Web セキュリティ アプライアンスではなくクライアントから送信されたように表示されます。 **注：**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、リターン パスをリダイレクトするように WCCP サービスを設定します。

表 5-1　Web プロキシの設定 （続き）

プロパティ	説明
永続的な接続タイムアウト（Persistent Connection Timeout）	トランザクションの完了後に Web プロキシがクライアントまたはサーバへの接続を開いている時間を入力します。接続を開いた状態に保つと、別の要求で Web プロキシが再び使用することができます。 たとえば、クライアントが google.com でトランザクションを完了したら、他のクライアントが google.com の要求を行わなければ、Web プロキシはサーバ google.com への接続を保持し、サーバ側の持続的なタイムアウトに指定された時間の間、開いた状態を保ちます。 • **[クライアント側（Client side）]。**クライアントからのアクティビティがないときに、Web プロキシがネットワーク上のクライアントに対して、開いた接続状態を保つ最大秒数。 • **[サーバ側（Server side）]。**ネットワーク上のすべてのクライアントからそのサーバへのアクティビティがないときに、Web プロキシが宛先サーバとの開いた接続状態を保つ最大秒数。 デフォルトでは、クライアント側とサーバ側の両方の持続的なタイムアウトは 300 秒です。 ネットワーク上のクライアントが同じサーバに頻繁に接続する場合、またはネットワークの外部サーバへの接続が比較的遅い場合、サーバ側の持続的なタイムアウト値を上げる必要がある場合があります。 シスコは、デフォルト値を維持することを推奨します。ただし、これらの値を上げたり、下げたりして、繰り返し接続を開いたり、閉じたりするのに使用されるオーバーヘッドを減らすために開いた接続状態を時間を長く保つ必要がある場合があります。持続的なタイムアウト値を上げようと考えている場合は、同時に起こる持続的な接続の最大数に達した場合に、Web Proxy の機能も軽減して、新しい接続を開きます。
使用中の接続のタイムアウト（In-Use Connection Timeout）	現在のトランザクションが完了していない場合、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さらにデータを待機する時間を入力します。 たとえば、クライアントが接続を開き、要求の半分だけを送信する場合、Web プロキシは開いている接続を閉じる前に、残りの要求のクライアント側の予約のタイムアウトで指定された時間待機します。 • **[クライアント側（Client side）]。**Web プロキシがアイドル状態のクライアントに対して開いた接続状態を保つ最大秒数。 • **[サーバ側（Server side）]。**Web プロキシがアイドル状態の宛先サーバに対して開いた接続状態を保つ最大秒数。 デフォルトでは、クライアント側とサーバ側の両方の予約のタイムアウトは 300 秒です。
同時永続的接続数（最大サーバ番号）（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状態を保つ接続（ソケット）の最大数を入力します。

表 5-1　Web プロキシの設定 （続き）

プロパティ	説明
ヘッダーを生成 （Generate Headers）	• **[X-Forwarded-For]。**HTTP の「X-Forwarded-For」のヘッダーを転送するかどうかを選択します。デフォルトは Do Not Send です。注：ネットワークにプロキシ認証を使用してユーザ認証またはアクセス コントロールを管理する明示的な転送アップストリーム プロキシが含まれる場合、X-Forwarded-For ヘッダーをイネーブルにして、クライアント ホスト ヘッダーをアップストリーム プロキシに送信する必要があります。 • **[VIA]。**クライアントからの HTTP 要求およびサーバからの HTTP 応答の HTTP の「VIA」ヘッダーを転送するかどうかを選択します。デフォルトは Send です。
受信したヘッダーの使用 （Use Received Headers）	アプライアンスがアップストリーム プロキシとして展開されており、ダウンストリーム プロキシからの IP アドレスの代わりに X-Forwarded-For ヘッダーに指定された IP アドレスを使用してクライアントを識別するようにするには、[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ます。アプライアンスが信頼できるダウンストリーム プロキシまたはロード バランサからクライアント要求を受信するときにのみ、このオプションをイネーブルにする必要があります。 このオプションをイネーブルにする場合、ダウンストリーム プロキシまたはロード バランサの IP アドレスを入力します。サブネットまたはホスト名を入力できません。[行を追加（Add Row）] をクリックして複数の IP サーバを追加します。Web プロキシは、リストに含まれないマシンからの X-Forwarded-For ヘッダーの IP アドレスを受け入れません。 **（注）** %XV のカスタム フォーマット指定子を使用してアクセス ログのダウンストリーム IP アドレスを表示し、x-request-source-ip 変数を使用して W3C アクセス ログのダウンストリーム IP アドレスを表示できます。

ステップ 5　変更を送信し、保存します。

カスタム ヘッダー

特定の出力トランザクションにカスタム ヘッダーを追加して、特定のドメインによる発信要求の特別な処理を要求できます。たとえば、YouTube for Schools との関連がある場合、カスタム ヘッダーを使用して、ネットワークから配信され、特別な処理を必要とするものとして YouTube.com にトランザクション要求を特定できます。

トラブルシューティングの目的でアクセス ログのカスタム ヘッダーを記録できます。

関連トピック

- 「[カスタム ヘッダ（Custom Header）] オプション」（P.5-34）
- 「アクセス ログおよび W3C ログのカスタム フォーマット」（P.24-31）
- 「アクセス ログのカスタム フォーマットの設定」（P.24-40）

FTP 接続での操作

Web セキュリティ アプライアンス Web プロキシは、HTTP と同様に File Transfer Protocol (FTP) のプロキシ サービスを提供します。FTP は、ネットワーク上のコンピュータ間でデータを転送するために使用されるプロトコルです。Web プロキシは、次の FTP トランザクションを処理できます。

- **FTP over HTTP。**ほとんどの Web ブラウザは FTP トランザクションをサポートしますが、このトランザクションは HTTP トランザクション内で符号化されることもあります。HTTP トランザクションに適用されるすべてのポリシーと設定オプションは、FTP over HTTP トランザクションにも適用されます。
- **ネイティブ FTP。**FTP クライアントは HTTP 接続を呼び出すことなくデータ転送に FTP を使用します。ネイティブ FTP 接続は、HTTP 接続とは異なる方法で扱われ、処理されます。

ネイティブ FTP トランザクションを処理する Web プロキシ コンポーネントは FTP プロキシと呼ばれます。

ネイティブ FTP 接続は、Web プロキシがトランスペアレントまたは明示的な転送モードで展開されている場合に提供することができます。

FTP を使用してデータを転送するコンピュータは、コンピュータ間に 2 つの接続を作成します。コントロール接続は、RETR および STOR などの FTP コマンドの送受信のほか、接続モードとファイルのプロパティなどの他の情報を伝達するために使用されます。データ接続は、データ自体の転送に使用されます。通常、コンピュータはコントロール接続にポート 21 を使用し、データ接続にランダムに割り当てられたポート（通常は 1023 より大きい数）を使用します。

FTP プロキシは、次の接続モードをサポートします。

- **パッシブ。**パッシブ モードでは、FTP サーバは、データ接続に使用するポートを選択し、FTP クライアントにこの割り当てを伝達します。パッシブ モードは通常、FTP クライアントがファイアウォールの背後にあり、着信接続（FTP サーバからなど）がブロックされるほとんどのネットワーク環境で支持されています。FTP プロキシのデフォルトは、パッシブ モードです。
- **アクティブ。**アクティブ モードでは、FTP クライアントは、データ接続に使用するポートを選択し、FTP サーバにこの割り当てを伝達します。

FTP クライアントは、パッシブ モード、アクティブ モード、または両方をサポートできる場合があります。FTP クライアントが FTP プロキシへの接続に使用するモードにかかわらず、FTP プロキシはまずパッシブ モードを使用して、FTP サーバに接続します。ただし、FTP サーバがパッシブ モードを許可しない場合、FTP プロキシはアクティブ モードを使用します。

ネイティブ FTP 接続で操作する場合、次のルールとガイドラインを考慮してください。

- ネイティブ FTP トランザクションに適用する ID グループを定義できます。
- ネイティブ FTP 接続に適用する FTP プロキシ設定を設定します。詳細については、「FTP プロキシ設定値の設定」（P.5-9）を参照してください。
- FTP サーバに接続するときに、ユーザが FTP クライアントで参照する初期メッセージを設定できます。FTP プロキシ設定を設定するときに、初期バナーを設定します。
- FTP プロキシ認証でのエラーまたはサーバ ドメイン名の悪いレピュテーションなどの理由で FTP プロキシが FTP サーバとの接続を確立できない場合、FTP プロキシが IronPort FTP 通知メッセージに表示するカスタム メッセージを定義できます。詳細については、「FTP 通知メッセージの設定」（P.16-17）を参照してください。
- FTP プロキシがネイティブ FTP トランザクションをキャッシュするために設定されている場合、匿名ユーザによってアクセスされたコンテンツのみをキャッシュします。

- FTP サーバの IP アドレスをスプーフィングするように、FTP プロキシを設定できます。データ接続（FTP サーバ）の送信元 IP アドレスがコントロール接続（FTP プロキシ）の送信元 IP アドレスと異なる場合に、FTP クライアントがパッシブ データ接続を受け入れないときにこれを実行する必要がある場合があります。
- FTP プロキシと FTP サーバとの接続が遅い場合、Cisco IronPort 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場合があります。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すると、ユーザは失敗したトランザクションを見る場合があります。
- FTP クライアントは、正式な形式（hostname:port）を使用する限り、コントロール接続に TCP ポートを指定できます。
- FTP クライアントが FTP プロキシへの接続に使用するモードにかかわらず、FTP プロキシはまずパッシブ モードを使用して、FTP サーバに接続しようとします。ただし、FTP サーバがパッシブ モードを許可しない場合、FTP プロキシはアクティブ モードを使用します。
- アクセス ログには、ユーザが最初にネイティブ FTP セッションを開始するときのエントリが含まれます。「FTP_CONNECT」（明示的な転送接続）および「FTP_TUNNEL」（トランスペアレント接続）のアクセス ログ ファイルを検索します。

ネイティブ FTP での認証の使用

FTP プロキシは、ネイティブ FTP 要求を行うことができるユーザを制御するためにユーザ認証を実行します。このユーザ認証は、ネイティブ FTP トランザクションに適用されるポリシー グループを決定します。

ただし、FTP および FTP クライアントの性質上、次のトランザクションだけがネイティブ FTP トランザクションのユーザを認証できます。

- 明示的な転送接続。
- 次のいずれかの条件による透過的にリダイレクトされた接続。
  - ユーザが Novell eDirectory または Active Directory を使用して透過的に識別される場合。
  - 認証サロゲートが IP アドレスで、ユーザが FTP トランザクションの前に HTTP トランザクションを行う場合。
  - ユーザがリモート ユーザで、セキュア モビリティ ソリューションを使用して Cisco 適応型セキュリティ アプライアンスによって識別される場合。

この制限によって、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、認証を必要としないネイティブ FTP トランザクションに少なくとも 1 つの ID とアクセス ポリシーを設定する必要がある場合があります。これにより、Web セキュリティ アプライアンスに透過的にリダイレクトされるすべての FTP 接続が作用できます。認証がすべてのポリシー グループで必要な場合、一部の透過的にリダイレクトされたネイティブ FTP トランザクションが失敗する場合があります。たとえば、クッキー認証サロゲートを使用する、透過的にリダイレクトされたネイティブ FTP トランザクションが失敗する場合があります。

FTP クライアントと通信する場合に、FTP プロキシが使用する認証形式を設定できます。FTP プロキシは、プロキシ認証で次の形式をサポートします。

- **Check Point。**次の形式を使用します。
  - ユーザ：ftp_user@proxy_user@remote_host
  - パスワード：ftp_password@proxy_password
- **Raptor。**次の形式を使用します。
  - ユーザ：ftp_user@remote_host proxy_user

  - パスワード：ftp_password
  - アカウント：proxy_password
- **No Proxy Authentication。**次の形式を使用します。
  - ユーザ：ftp_user@remote_host
  - パスワード：ftp_password

ネイティブ FTP で認証を使用する場合は、FTP クライアントが FTP プロキシで設定されているのと同じ認証設定を使用することを確認します。

FTP ユーザ名にはスペースおよび @ 文字を使用できます。ただし、これらの文字の前にはバックスラッシュ（\）を指定する必要があります。

（注）　ネイティブ FTP トランザクションに認証が必要とするときは注意してください。暗号化せずにデータ（認証クレデンシャルを含む）が回線上に直接送信されるため、FTP は本質的に安全ではありません。

トランスペアレント モードでのネイティブ FTP の操作

トランスペアレント モードで Web セキュリティ アプライアンスが展開されている場合、FTP クライアントは通常、FTP プロキシを使用するように明示的に設定されていません。ネイティブ FTP 接続は、FTP プロキシに透過的にリダイレクトされてから、処理されます。

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。このため、FTP プロキシはアクセス ポリシーに設定された IP アドレスを使用したネイティブ FTP トランザクションのみを照合します。

事前定義済みの URL カテゴリおよび Web レピュテーション フィルタは、ホスト名と IP アドレスでブロックしますが、一部のサーバでは、サーバの IP アドレスではなく、ホスト名情報だけが含まれる場合があります。たとえば、「News」に定義された URL カテゴリに cnn.com が含まれ、そのサーバの対応する IP アドレスが含まれない場合で、ブロックするようにその URL カテゴリが設定されている場合は、cnn.com へのネイティブ FTP 接続はブロックされる代わりに正常に接続されます。そのため、FTP プロキシが特定のサイトへのネイティブ FTP 接続を確実にブロックするために、カスタム URL カテゴリを作成し、ブロックするサイトのリストまたは正規表現フィールドに IP アドレスを入力します。

FTP プロキシ設定値の設定

FTP プロキシ設定は、ネイティブ FTP 接続に適用されます。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 プロキシを設定します。詳細については、「Web プロキシの設定」（P.5-3）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）] > [FTP プロキシ（FTP Proxy）] ページの順に移動し、[設定を編集（Edit Setting）] をクリックします。

ステップ 2　[FTP プロキシを有効にする（Enable FTP Proxy）] フィールドが選択されていることを確認します。

ステップ 3　基本および高度な FTP プロキシ設定を設定します。

プロパティ	説明
プロキシ リッスン ポート（Proxy Listening Port）	FTP プロキシを使用したコントロール接続の確立で使用するポート FTP クライアントを指定します。

プロパティ	説明
キャッシュ（Caching）	匿名ユーザからデータ接続のコンテンツをキャッシュするかどうかを選択します。
サーバ側 IP スプーフィング（Server Side IP Spoofing）	FTP プロキシが FTP サーバの IP アドレスをスプーフィングするかどうかを選択します。IP アドレスがコントロール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 クライアントに対してこれを実行する必要がある場合があります。
認証フォーマット（Authentication Format）	FTP クライアントと通信する場合に、FTP プロキシが使用する認証形式を選択します。詳細については、「ネイティブ FTP での認証の使用」（P.5-8）を参照してください。
パッシブモードのデータ ポート範囲（Passive Mode Data Port Range）	パッシブ モード接続で FTP プロキシを使用したデータ接続の確立に FTP クライアントが使用する TCP ポートの範囲を指定します。 デフォルトは 11000 ～ 11009 です。
アクティブ モードのデータ ポート範囲（Active Mode Data Port Range）	アクティブ モード接続で FTP プロキシを使用したデータ接続の確立に FTP サーバが使用する TCP ポートの範囲を指定します。この設定は、ネイティブ FTP および FTP over HTTP 接続の両方に適用されます。 デフォルトは 12000 ～ 12099 です。 同じ FTP サーバからのより多くの要求に対応するために、このフィールドのポート範囲を増やす必要がある場合があります。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。
ウェルカム バナー（Welcome Banner）	FTP クライアントで表示する初期メッセージを選択します。 • **[FTP サーバメッセージを（FTP server message）]。**FTP サーバ メッセージは、透過的にリダイレクトされた接続のみを表示します。ネイティブ FTP 接続が FTP プロキシに明示的に送信されると、FTP クライアントは FTP プロキシによって事前定義されたメッセージを表示します。 • **[カスタム メッセージ（Custom message）]。**すべてのネイティブ FTP 接続用に表示するメッセージを入力します。
制御接続タイムアウト（Control Connection Timeouts）	現在のトランザクションが完了していない場合、FTP プロキシがアイドル状態の FTP クライアントまたは FTP サーバからのコントロール接続でさらに通信を待機する時間を入力します。 たとえば、FTP クライアントがコントロール接続を開き、一部の要求を送信する場合、FTP プロキシは開いている接続を閉じる前に、次の要求のクライアント側のコントロール接続のタイムアウトに指定された時間を待機します。 • **[クライアント側（Client side）]。**FTP プロキシがアイドル状態のクライアントに対して開いた状態の接続を保つ最大秒数。 • **[サーバ側（Server side）]。**FTP プロキシがアイドル状態の FTP サーバに対して開いた状態のコントロール接続を保つ最大秒数。 デフォルトでは、クライアント側とサーバ側両方のコントロール接続のタイムアウトは 300 秒です。

プロパティ	説明
データ接続タイムアウト（Data Connection Timeouts）	現在のトランザクションが完了していない場合、FTP プロキシがアイドル状態の FTP クライアントまたは FTP サーバからのデータ接続でさらに通信を待機する時間を入力します。 たとえば、FTP クライアントがデータ接続を開き、要求の半分だけを送信する場合、FTP プロキシは開いている接続を閉じる前に、残りの要求のクライアント側の予備のタイムアウトに指定された時間を待機します。 • **[クライアント側（Client side）]。**FTP プロキシがアイドル状態のクライアントに対して開かれた状態のデータ接続を保つ最大秒数。 • **[サーバ側（Server side）]。**FTP プロキシがアイドル状態の FTP サーバに対して開かれた状態のデータ接続を保つ最大秒数。 デフォルトでは、クライアント側とサーバ側の両方のデータ接続のタイムアウトは 300 秒です。

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

（注）　[アプリケーションス キャンのスキップ（Application Scanning Bypass）] セクションを設定する方法の詳細については、「Web プロキシ スキャニングからのアプリケーションスキャニングのバイパス」（P.5-13）を参照してください。

特定のアドレス間のクライアント要求が Web プロキシですべての処理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。プロキシ バイパス リストは、レイヤ 4 スイッチまたは WCCP v2 ルータを使用して Web プロキシに透過的にリダイレクトされている要求に対してのみ作用します。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 Web プロキシに明示的な要求をすると、その要求は Web プロキシによって処理されます。

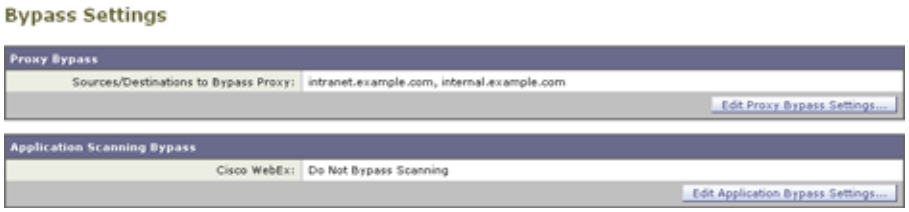
次のいずれかを実行するために、プロキシ バイパス リストを作成する必要がある場合があります。

- プロキシ サーバに接続するときに、正常に作用しなかった HTTPS ポートを使用して、Web プロパティが HTTP 非対応（または独自の）プロパティを干渉することを防ぎます。
- 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。

[セキュリティ マネージャ（Security Manager）] > [バイパス設定（Bypass Settings）] ページでプロキシ バイパス リストを定義します。

図 5-1 は、プロキシ バイパス リストの例を示します。

図 5-1　プロキシ バイパス リスト



プロキシ バイパス リストにアドレスを含めるには、[プロキシ バイパス設定を編集（Edit Proxy Bypass Settings）] をクリックします。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
- ホスト名。crm.example.com など
- ドメイン名。example.com など

（注）　ドメイン名を使用するプロキシ バイパス リストについては、L4 トラフィック モニタをイネーブルにしない場合でも、ネットワークに T1 および T2 のネットワーク インターフェイスを接続する必要があります。詳細については、「プロキシ バイパス リストの操作の概要」（P.5-12）を参照してください。

トランザクションが Web プロキシをバイパスする場合、Web 用 AsyncOS はプロキシ バイパス ログに内容を記録します。ログ方法の詳細については、「ログ サブスクリプションの使用」（P.24-7）を参照してください。

（注）　プロキシ バイパス リストに L4 トラフィック モニタに応じた既知のマルウェア アドレスであるアドレスが含まれる場合、L4 トラフィック モニタはそのアドレスの要求を参照し、その要求が継続して L4 トラフィック モニタによってブロックされます。そのアドレスへのトラフィックが常に許可されるようにするには、L4 トラフィック モニタからのアドレスもバイパスする必要があります。詳細については、「L4 トラフィック モニタが動作する仕組みについて」（P.21-1）を参照してください。

プロキシ バイパス リストの操作の概要

Web プロキシは HTTP または HTTPS 要求を受信すると、プロキシ バイパス リストに存在するかどうかを参照するために、送信元および宛先 IP アドレスの両方を確認します。存在する場合、パケットはネットワーク内のネクスト ホップに送信されます。（GRE を使用してパケットが WCCP サービスに到着した場合は、パケットがリダイレクトされたトランスペアレント リダイレクションデバイスにパケットが返送されることもあります）。

プロキシ バイパス リストはプロキシ バイパス リストの IP アドレスに要求の IP アドレスを照合させることで作用します。名前がバイパス リストに入力されると、Web プロキシは DNS を使用して IP アドレスに解決される必要があります。Web プロキシ DNS は、ドメイン名とは異なる方法でホスト名を解決します。

- **ホスト名。**ホスト名は、DNS クエリーを使用してプロキシ バイパス リストに入力されるとすぐに IP アドレスに解決されます。（ホスト名の例は www.example.com です）。

- **ドメイン名。**ドメイン名は DNS クエリーを使用して IP アドレスに解決できないので、Web プロキシは T1 および T2 ネットワーク インターフェイスを介して DNS スヌーピングを使用します。（ドメイン名の例は example.com で、www.example.com および webmail.example.com の両方に一致します）。

これらの違いにより、プロキシ バイパス リストに IP アドレスおよびホスト名だけが含まれている場合、Web プロキシは要求ヘッダーの IP アドレスをプロキシ バイパス リストの IP アドレスに容易に照合させることができます。

ただし、ドメイン名で作用するプロキシ バイパス リストでは、*L4 トラフィック モニタをイネーブルにしていなくても*、ネットワークに T1 および T2 ネットワーク インターフェイス（シンプレックス モードを使用している場合）の両方を接続するか、ネットワークに T1 ネットワーク インターフェイス（デュプレックス モードを使用している場合）のみを接続する必要があります。ただし、プロキシ バイパス リストは Web プロキシ スキャニングだけをバイパスします。これは、L4 トラフィック モニタをバイパスしません。

（注） トランスペアレント リダイレクションデバイスが WCCP ルータの場合、同じセッションで Web プロキシに他のパケットを転送させないようにする知能がある場合があります。この場合、パケットは残りのセッションに対して物理的には送信されず、残りのセッションに対して正確にバイパスしています。

プロキシ バイパス リストでの WCCP の使用

WCCP v2 ルータを使用するように Web セキュリティ アプライアンスが設定されている場合、Web セキュリティ アプライアンスで定義されたすべての WCCP サービスが同じ転送方式とリターン方式（L2 または GRE）を使用して、プロキシ バイパス リストで正常に作用することを確認する必要があります。転送およびリターン方法が一致しない場合、一部の WCCP 対応ルータは一貫性なく動作します。

詳細については、「転送方式とリターン方式の使用」（P.25-13）を参照してください。

Web プロキシ スキャニングからのアプリケーションスキャニングのバイパス

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）] ページの順に進みます。

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　バイパスするようにアプリケーションのバイパス スキャニングをイネーブルにします。

ステップ 4　変更を送信し、保存します。

プロキシの使用規約

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、一定時間が経過後にエンド ユーザ確認ページを表示することで、これを実行します。エンド ユー

ザ確認ページが表示された場合、ユーザは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にはリンクをクリックする必要があります。エンドユーザの確認ページの詳細については、「エンドユーザ確認ページ」（P.16-12）を参照してください。

Web プロキシを使用するためのクライアント アプリケーションの設定

Web ブラウザおよび他のユーザ エージェントは、ワールドワイド ウェブにアクセスするために、Web プロキシへの接続方法を認識している必要がある場合があります。明示的な転送モードで Web セキュリティ アプライアンスを展開する場合、Web プロキシを使用するように、クライアント アプリケーションを設定する*必要があります*。トランスペアレント モードでアプライアンスを展開する場合、明示的に Web プロキシを使用するためにクライアント アプリケーションを設定するかどうかを*選択*できます。

次の設定方式のいずれかを使用して、明示的に Web プロキシを使用するようにクライアント アプリケーションを設定できます。

- **手動。**手動設定では、クライアント アプリケーションごとに 3128 などの Web セキュリティ アプライアンスのホスト名とポート番号を入力する必要があります。アプライアンスが変更されると、各アプリケーションを個別に編集する必要があります。1 つのクライアント マシンでプロキシ アクセスをテストする場合に、手動でアプリケーションを設定する必要がある場合があります。シスコでは、アプライアンスの Web プロキシを使用するために手動で各クライアント アプリケーションを設定することを推奨しません。
- **Proxy Auto Config（PAC）ファイル。**Web ブラウザでは、PAC ファイルを使用するように各ブラウザを設定して、Web プロキシを検索できます。その後、PAC ファイルを編集して、アプライアンスの Web プロキシ情報を指定できます。詳細については、「PAC ファイルでの操作」（P.5-14）を参照してください。

プロキシを使用するクライアント アプリケーションの設定方法の詳細については、クライアント アプリケーションのマニュアルを参照してください。

PAC ファイルでの操作

proxy auto-config（PAC）ファイルは、所定の URL を取得するために Web ブラウザが適切なプロキシ サーバを自動的に選択できる方法を定義するテキスト ファイルです。

PAC ファイルを使用する場合、PAC ファイル情報で一度だけ各ブラウザを設定する必要があります。次に、各ブラウザを編集せずに Web プロキシ接続情報を追加、削除、または変更するために PAC ファイルを複数回編集できます。こうして中央の場所でネットワークに関するプロキシ情報を設定し、簡単に更新することができます。

（注）　ブラウザが PAC ファイルを読み終わったら、以降のブラウザ セッション用にメモリに保存します。

次の理由で、PAC ファイルを使用する必要がある場合があります。

- **集中管理。**中央の 1 つの場所で PAC ファイルを管理できます。
- **複雑なネットワーク環境。**プロキシ サーバのネットワークが複雑な場合、異なるサーバとクライアントのニーズに合わせて PAC ファイルを作成できます。

- **変化するネットワーク環境。**ネットワーク環境が今後変わる可能性がある場合は、PAC でサーバを簡単に追加、編集、または削除して、変更内容が自動的にすべてのブラウザに影響するようにします。
- **フェールオーバー。**複数のプロキシ サーバがある場合は、障害が発生する場合の冗長性を提供できます。冗長構成に PAC ファイルをプログラミングするか、障害が発生した場合に、別のプロキシ サーバを使用するように PAC ファイルを変更できます。

（注）　異なるブラウザがセカンダリ プロキシにフェールオーバーするために異なる時間を費やします。たとえば、インターネット エクスプローラには約 25 秒かかり、Firefox には約 50 秒かかります。

- **ロード バランシング。**複数のプロキシ サーバがある場合は、PAC ファイルを使用して、プロキシ サーバにアクセスする要求を指定できます。たとえば、1 つのサブネット上のユーザが特定のプロキシを使用し、異なるサブネット上のユーザが異なるプロキシを使用する必要がある場合があります。

PAC ファイル形式

PAC ファイルには、少なくとも 1 つの JavaScript 関数である FindProxyForURL（URL、ホスト）を含める必要があります。JavaScript 関数は、各 URL に使用する適切なプロキシを決めます。

たとえば、Web セキュリティ アプライアンスのホスト名が WSA.example.com の場合、次のテキストを含む PAC ファイルを作成できます。

```
function FindProxyForURL(url, host) { return "PROXY WSA.example.com:3128; DIRECT"; }
```

（注）　FindProxyForURL() 関数に指定するポートは、[セキュリティ サービス（Security Services）] > [Web プロキシ（Web Proxy）] ページで設定した Web セキュリティ アプライアンスのプロキシ ポートである必要があります。

ただし、PAC ファイルをより複雑にすることもできます。たとえば、特定のホスト名または IP アドレスの照合など、特定の条件下で直接 Web サイトに接続するようにブラウザに指示する PAC ファイルを作成し、他のあらゆるケースで、プロキシ サーバを使用するようにすることができます。イントラネット上のサーバに対して、Web サイトに直接アクセスするようにアプリケーションに指示する PAC ファイルを作成できます。

PAC ファイルの作成および使用に関する詳細については、次の場所を参照してください。

- http://en.wikipedia.org/wiki/Proxy_auto-config
- http://www.mozilla.org/catalog/end-user/customizing/enduserPAC.html
- http://wp.netscape.com/eng/mozilla/2.0/relnotes/demo/proxy-live.html

（注）　共通の規則は、PAC ファイル名に対して .pac ファイルの拡張子を使用することです。

リモート ユーザに対する PAC ファイルの作成

一部のラップトップ ユーザは、組織のネットワーク内とネットワーク外の両方からインターネットに接続します。このようなユーザの場合、ネットワーク上にいる場合は Web プロキシに接続し、ネットワーク上にいない場合は Web ブラウザに直接接続するようにブラウザに通知する PAC ファイルを作成できます。

これを実行するには、ネットワーク内で DNS 解決が可能である Web サーバで PAC ファイルがホストされ、ネットワーク外で DNS 解決が可能でないことを確認します。これは、PAC ファイルの場所の URL を入力すると、ブラウザが設定された場所で PAC ファイルを常に使用するようにするために機能します。ネットワーク外などブラウザが URL を解決できない場合、代わりにすべての Web サイトに直接アクセスしようとします。その後、ラップトップがネットワークに再接続すると、ブラウザは PAC ファイルにアクセスして、Web サイトへのアクセスに Web プロキシを使用します。

ブラウザへの PAC ファイルの指定

PAC ファイルを使用するには、アクセスする必要がある各ブラウザからアクセス可能な場所に PAC ファイルをパブリッシュする必要があります。PAC ファイルを使用するようにブラウザを設定する場合は、次のいずれかの方法を使用できます。

- **PAC ファイルの場所を入力する。**「PAC ファイルの場所の入力」（P.5-16）を参照してください。
- **PAC ファイルの場所を自動的に検出する。**「PAC ファイルの場所の自動的な検出」（P.5-16）を参照してください。

PAC ファイルの場所の入力

ファイルの正確な場所を指定することで、PAC ファイルを使用するようにブラウザを設定できます。現在の場所に応じて異なるプロキシ サーバを使用する必要がある可能性があるラップトップのユーザ用に正確な PAC ファイルの場所を入力する必要がある場合があります。

次の場所に PAC ファイルを配置できます。

- **ローカル マシン。**各クライアント マシンに PAC ファイルを配置して、それを使用するようにブラウザを設定できます。全体の組織に展開する前に PAC ファイルをテストするためにローカル PAC ファイルを使用する必要がある場合があります。ブラウザ設定にパスを入力します。入力するパスは、ブラウザ タイプによって異なります。
- **Web サーバ。**各クライアント マシンがアクセスできる Web サーバに PAC ファイルを配置できます。たとえば、Apache または Microsoft IIS Web サーバに PAC ファイルを配置できます。ブラウザ設定に URL を入力します。
- **Web セキュリティ アプライアンス。**Web セキュリティ アプライアンスに PAC ファイルを配置できます。ネットワーク内ですべてのクライアント マシンがアクセスできることを検証するために、Web セキュリティ アプライアンスに PAC ファイルを配置する必要がある場合があります。ブラウザ設定に URL を入力します。

  Web セキュリティ アプライアンスに PAC ファイルをアップロードする方法の詳細については、「Web セキュリティ アプライアンスへの PAC ファイルの追加」（P.5-17）を参照してください。

PAC ファイルの場所の自動的な検出

ブラウザが Web Proxy Autodiscovery Protocol（WPAD）をサポートする場合、PAC ファイルの場所を自動的に検出するように設定できます。WPAD は、DHCP および DNS ルックアップを使用してブラウザが PAC ファイルの場所を決定できるようにするプロトコルです。

先頭ページを取得する前に、PAC ファイルの場所を自動的に検出するように設定された Web ブラウザは、DHCP または DNS を使用して PAC ファイルを見つけようとします。そのため、WPAD を使用する場合は、DHCP サーバまたは DNS サーバ設定して、ネットワーク サーバ上の PAC ファイルに Web ブラウザの要求を送信する必要があります。ただし、すべてのブラウザが WPAD を使用した PAC ファイルの検索で DHCP をサポートしているわけではありません。

ここでは、DNS の「A」レコードで WPAD を使用する一部の一般的なガイドラインについて説明します。DHCP で WPAD を使用する場合の詳細については、次の場所を参照してください。

- http://en.wikipedia.org/wiki/Web_Proxy_Autodiscovery_Protocol
- http://www.wpad.com/draft-ietf-wrec-wpad-01.txt
- http://www.microsoft.com/technet/isa/2004/plan/automaticdiscovery.mspx

DNS で WPAD を使用する場合、ドメイン名だけが DNS を使用して PAC ファイルを一意で識別できるため、ネットワーク上の各ドメインは、ドメイン上のすべてのユーザに対して 1 つの PAC ファイルだけを使用できます。たとえば、host1.accounting.example.com および host2.finance.example.com のユーザは異なる PAC ファイルを使用できます。

ステップ 1　PAC ファイルの名前を wpad.dat に変更します。

ステップ 2　wpad.example.com など「wpad」で開始する内部的に解決可能な DNS 名を作成します。

ステップ 3　wpad.example.com などのファイルをホストする Web サイトのルート ディレクトリに wpad.dat を配置します。Web セキュリティ アプライアンスへのファイルの配置に関する詳細については、「アプライアンスへの PAC ファイルのアップロード」（P.5-20）を参照してください。

（注）　Internet Explorer 6 のバグにより、wpad.dat のコピーを作成し、ファイル名を wpad.da に変更して、Internet Explorer 6 ユーザが使用できるようにします。詳細については、http://www.microsoft.com/technet/isa/2004/ts_wpad.mspx を参照してください。

ステップ 4　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）　wpad.dat を Web セキュリティ アプライアンスに配置する場合、アプライアンスはすでにこれを実行しています。

Web セキュリティ アプライアンスへの PAC ファイルの追加

proxy auto-config（PAC）ファイルを使用して、Web プロキシを明示的に使用するようにブラウザを設定できます。PAC ファイルを Web セキュリティ アプライアンスに配置してから、2 つの方法のいずれかでブラウザを設定できます。アプライアンスに PAC ファイルの URL を入力する。または、Web Proxy Autodiscovery Protocol（WPAD）を使用して PAC ファイルを自動的に検出するようにブラウザを設定する。

アプライアンスに複数の PAC ファイルを追加できます。アプライアンスがネットワーク上の複数のドメインで使用されている場合、複数の PAC ファイルの追加が必要な場合があります。ドメイン上のすべてのブラウザで 1 つの PAC ファイルを使用できます。

アプライアンスに PAC ファイルを追加する場合、PAC ファイル要求を受信するためにアプライアンスが使用する 1 つ以上のポートを指定できます。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 PAC ファイルの URL を指定する方法の詳細については、「PAC ファイルの URL の指定」（P.5-18）を参照してください。

ブラウザが PAC ファイルを問い合わせるときに、アプライアンスは HTTP を使用してファイルを送信します。PAC ファイルは、MIME タイプの `application/x-ns-proxy-autoconfig` を使用して返されます。

（注）　アプライアンスで PAC ファイルを使用するようにブラウザが設定されている場合、URL に PAC ファイル名を含める必要があります。URL に PAC ファイル名が指定されていない場合、存在してエラーを返す場合または存在しない場合に、デフォルトによって、アプライアンスが default.pac を使用します。または、ネットワークの異なるホスト名またはドメインに使用するデフォルトの PAC ファイルを設定できます。

PAC ファイルの詳細については、「PAC ファイルでの操作」（P.5-14）を参照してください。

PAC ファイルの URL の指定

PAC ファイルを使用するようにブラウザを設定する場合、URL を使用してファイルの正確な場所を指定できます。PAC ファイルが Web セキュリティ アプライアンスをホストしている場合、表 5-2 のいずれかの形式を使用して URL を指定できます。

表 5-2　PAC ファイルの URL 形式

PAC ファイルの URL 形式	説明
http://hostname.domain:port/filename	存在する場合に、PAC ファイルの *ファイル名*が提供されます。それ以外の場合は、エラーが返されます。 これは、*ポート*がアプライアンス上に設定されたポートであり、その*ホスト名*が PAC ファイルのホスト用に設定されているアプライアンスのネットワーク インターフェイスのホスト名であることを前提としています。
http://hostname.domain:port/	存在する場合に、PAC ファイルの default.pac を提供することができます。それ以外の場合は、エラーが返されます。 これは、*ポート*がアプライアンス上に設定されたポートであり、その*ホスト名*が PAC ファイルのホスト用に設定されているアプライアンスのネットワーク インターフェイスのホスト名であることを前提としています。
http://hostname:port/filename	存在する場合に、PAC ファイルの *ファイル名*が提供されます。それ以外の場合は、エラーが返されます。 これは、*ポート*がアプライアンス上に設定されたポートであり、その*ホスト名*が PAC ファイルのホスト用に設定されているアプライアンスのネットワーク インターフェイスのホスト名であることを前提としています。

表 5-2　PAC ファイルの URL 形式 （続き）

PAC ファイルの URL 形式	説明
http://hostname:port/	存在する場合に、PAC ファイルの「default.pac」が提供されます。それ以外の場合は、エラーが返されます。 これは、*ポート*がアプライアンス上に設定されたポートであり、その*ホスト名*が PAC ファイルのホスト用に設定されているアプライアンスのネットワーク インターフェイスのホスト名であることを前提としています。
http://IPAddress:port/filename	存在する場合に、PAC ファイルの*ファイル名*が提供されます。それ以外の場合は、エラーが返されます。 これは、*ポート*がアプライアンス上に設定されたポートであり、その *IPAddress* が PAC ファイルのホスト用に設定されているアプライアンスのネットワーク インターフェイスの IP アドレスであることを前提としています。
http://IPAddress:port/	存在する場合に、PAC ファイルの「default.pac」が提供されます。それ以外の場合は、エラーが返されます。 これは、*ポート*がアプライアンス上に設定されたポートであり、その *IPAddress* が PAC ファイルのホスト用に設定されているアプライアンスのネットワーク インターフェイスの IP アドレスであることを前提としています。
http://ConfiguredHostname/filename	アプライアンスに設定され、存在する場合に、PAC ファイルの*ファイル名*が提供されます。それ以外の場合は、エラーが返されます。 これは、*ConfiguredHostname* が [セキュリティ サービス（Security Services）] >[PAC ファイル ホスティング（Proxy Auto-Configuration File Hosting）] ページの [ホスト名（Hostname）] フィールドに入力したホスト名であることを前提としています。
http://ConfiguredHostname/	*ConfiguredHostname* に設定されたデフォルトの PAC ファイル名は、ホスト名が [セキュリティ サービス（Security Services）] > [PAC ファイル ホスティング（Proxy Auto-Configuration File Hosting）] ページに設定されている場合に提供されます。これは、ポート 80 がアプライアンス上に設定されたポートであり、その*ホスト名*が PAC ファイルのホスト用に設定されているアプライアンスのネットワーク インターフェイスのホスト名であることを前提としています。ホストが設定されていない場合、エラーが返されます。

表 5-2　PAC ファイルの URL 形式 （続き）

PAC ファイルの URL 形式	説明
http://IPAddress/filename	アプライアンスに設定され、存在する場合に、PAC ファイルの *ファイル名*が提供されます。それ以外の場合は、エラーが返されます。 これは、*IPAddress* が [セキュリティ サービス（Security Services）] >[PAC ファイル ホスティング（Proxy Auto-Configuration File Hosting）] ページの [ホスト名（Hostname）] フィールドに入力した IP アドレスであることを前提としています。IP アドレスが設定されていない場合、エラーが返されます。
http://IPAddress/	IP アドレスが [セキュリティ サービス（Security Services）] > [PAC ファイル ホスティング（Proxy Auto-Configuration File Hosting）] ページで設定されたホスト名である場合に、*IPAddress* に設定されたデフォルトの PAC ファイル名が提供されます。IP アドレスが設定されていない場合、エラーが返されます。

アプライアンスへの PAC ファイルのアップロード

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（Proxy Auto-Configuration File Hosting）] ページの順に移動し、[設定の有効化と編集（Enable and Edit Settings）] をクリックします。

ステップ 2　[PAC サーバ ポート（PAC Server Ports）] フィールドに、Web セキュリティ アプライアンスが PAC ファイル要求の受信に使用する必要がある 1 つ以上のポート番号を入力します。

ステップ 3　[インターフェイス（Interface）] フィールドに、Web プロキシが PAC ファイル要求に使用するインターフェイスを選択します。データ トラフィック用に設定されたインターフェイスを選択できます。このフィールドは、複数のインターフェイスがデータ トラフィック用に設定されている場合にだけ表示されます。

ステップ 4　[PAC ファイル期限（PAC File Expiration）] セクションで、ブラウザのキャッシュに指定された分数を経過した後に PAC ファイルの終了を許可するかどうかを選択します。

ステップ 5　ローカル マシンからアプライアンスに PAC ファイルをアップロードするには、[参照（Browse）] をクリックします。

ステップ 6　PAC ファイルの場所に移動し、選択し、[開く（Open）] をクリックします。

ステップ 7　別の PAC ファイルを追加するには、[行を追加（Add Row）] をクリックし、ステップ 5 および 6 を繰り返し行います。

任意で、PAC ファイルはポート 80 などの HTTP プロキシ ポート経由で提供できます。これを可能にするには、PAC ファイルを使用し、各ホスト名でデフォルトの PAC ファイルを選択するホスト名を明示的に設定する必要があいます。指定したデフォルトの PAC ファイル名は、PAC ファイルの URL（「GET/」要求）を要求するときにブラウザに PAC ファイル名が含まれていない場合に提供されます。それ以外の場合、URL に指定されている PAC ファイル名が提供されます。PAC ファイルの URL が IP アドレスを使用する場合、設定されたホスト名として IP アドレスを入力できます。

ステップ 8　異なるホスト名にデフォルトの PAC ファイル名を設定するには、[ホスト名（Hostnames）] フィールドで Web セキュリティ アプライアンスのホスト名または IP アドレス、あるいはアプライアンスのホスト名に解決されるホスト名を入力します。次に、[プロキシ ポート（Proxy Port）] フィールドを介した「Get/」要求に対してデフォルトの PAC ファイルのデフォルトの PAC ファイル名を選択します。

たとえば、[ホスト名（Hostnames）] フィールドに *wsa.example.com* を入力し、[プロキシ ポート（Proxy Port）] フィールドを介して「Get/」要求に対するデフォルトの PAC ファイルに *pacfile1.pac* を入力する場合、http://wsa.example.com/ の要求は *pacfile1.pac* を取得し、http://wsa.example.com/default.pac の要求は *default.pac* を取得します。

ステップ 9　必要に応じて、ステップ 8 を繰り返し、Web セキュリティ アプライアンスに解決されるすべてのホスト名に対するデフォルトの PAC ファイル名を設定します。

ステップ 10　変更を送信し、保存します。

Netscape および Firefox との WPAD 互換性の概要

Netscape および Firefox ブラウザは、WPAD を使用して PAC ファイルを自動的に検出する場合にのみ DNS を使用します。そのため、Web セキュリティ アプライアンスに保存された PAC ファイルを Netscape および Firefox ブラウザが自動的に検出するようにする場合、次の手順を実行する必要があります。

1. PAC ファイルに wpad.dat の名前を付けます。
2. [セキュリティ サービス（Security Services）] > [Web プロキシ（Web Proxy）] ページの順に移動し、[HTTP ポートからプロキシへ（HTTP Ports to Proxy）] フィールドからポート 80 を削除します。
3. 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。

WPAD の詳しい使用方法については、「PAC ファイルの場所の自動的な検出」（P.5-16）を参照してください。

（注）　これらの手順は、Internet Explorer でも作用します。ただし、Internet Explorer バージョン 6 の場合、wpad.dat のコピーを作成し、wpad.da と名前を付けます。

高度なプロキシ設定

認証および DNS パラメータなどのより高度な Web プロキシ設定を設定できるように、AsyncOS には `advancedproxyconfig` CLI コマンドが含まれています。

`advancedproxyconfig` コマンドには、次のサブコマンドが含まれています。

サブコマンド	説明
Authentication	認証サーバによって認証される未処理の同時基本または NTLMSSP 認証要求の数および要求 URI に表示されるユーザ名を記録するかどうかなどの認証パラメータを設定します。ユーザの確認ページをイネーブルにするには、`authenticate` サブコマンドも使用できます。ユーザの確認ページの詳細については、「プロキシの使用規約」（P.5-13）を参照してください。 詳細については、「認証のオプション」（P.5-25）を参照してください。

サブコマンド	説明	
Caching	高度な Web プロキシ キャッシング オプションを設定します。内容はたとえば以下のとおりです。 • プロキシ キャッシュからコンテンツを取得しないために、クライアント要求を無視するかどうか • 信頼できないサーバからコンテンツをキャッシュするかどうか 「Customized Mode」を選択して別個にパラメータを設定するか、パラメータ値の定義済みセットに対して次に示すモードから選択できます。詳細については、「[キャッシング（Caching）] オプション」（P.5-30）を参照してください。	
	Safe mode	このモードでは、少ないキャッシングを使用します。クライアントが Last-Modified ヘッダー（キャッシングされるように）でエラー応答を送信する Web サーバに遭遇し、一時的なものなのでエラー応答をキャッシングする場合は、セーフ モードを使用する必要がある場合があります。または、指定したキャッシュ ライフタイムが不正なキャッシュ ヒットの原因となっていない場合に、一部の Web サーバが If-Modified-Since クエリーに正常に応答せずにオブジェクトをキャッシュしている場合は、セーフ モードを使用する必要がある場合があります。 他のモードよりも少ないキャッシングを行うことで、キャッシングに関して RFC に最も厳密に遵守します。
	Optimized mode	このモードでは、中程度のキャッシングを使用します。これは、デフォルトのモードです。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。 キャッシングに関して、セーフ モードよりも緩やか RFC に遵守し、アグレッシブより厳密に遵守します。セーフ モードより多くキャッシングを行い、アグレッシブ モードより少なくキャッシングを行います。
	Aggressive mode	このモードでは、アグレッシブ キャッシングを使用します。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 Last-Modified ヘッダーなしで認証コンテンツ、ETag の不一致、および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。 キャッシングに関して、RFC に最も緩やかに遵守します。モードのほとんどのキャッシュを実行します。
	Customized mode	このモードでは、各パラメータを個別に設定することができます。

サブコマンド	説明
CUSTOMHEADERS	特定ドメインのカスタム要求ヘッダーを管理します。これにより、特定のドメインに挿入されるカスタム ヘッダーを指定することができます。たとえば、学校のインターネット サービスを使用している学生を YouTube for Schools プログラムの一部ではない YouTube ビデオにアクセスすることから制限するために、学校は YouTube のカスタム ヘッダーを使用できます。「[カスタム ヘッダ（Custom Header）] オプション」（P.5-34）を参照してください。
DNS	DNS エラーの結果をキャッシュする時間および Web プロキシが DNS ルックアップの失敗で HTTP 302 リダイレクションを発行するかどうかなどの DNS 関連のオプションを設定します。詳細については、「[DNS] オプション」（P.5-35）を参照してください。
EUN	標準の IronPort エンドユーザ通知ページを使用するかどうか、またはカスタマイズするページを使用するかなどのエンドユーザ通知ページの設定を設定します。エンドユーザ通知ページの設定に関する詳細については、「FTP 通知メッセージの設定」（P.16-17）を参照してください。「[EUN] オプション」（P.5-36）を参照してください。
FTPOVERHTTP	匿名 FTP アクセスに使用するログイン名とパスワードおよび FTP 転送に対してアクティブ モードを許可するかどうかを設定します。FTP over HTTP トランザクションに対してのみ適用されます。「[FTPOVERHTTP] オプション」（P.5-40）を参照してください。以下の NATIVEFTP も参照してください。
HTTPS	HTTPS トランザクションで使用される URI のログ形式を設定します。URI 全体（「fulluri」）またはクエリー部分が削除された URI の一部（「stripquery」）だけを選択できます。詳細については、「[HTTPS] オプション」（P.5-40）を参照してください。
NATIVEFTP	アクティブおよびパッシブ モードに使用するポート範囲および明示的な転送接続に使用する認証タイプなどの FTP プロキシ設定を設定します。ネイティブ FTP トランザクションに対してのみ適用されます。「FTP プロキシ設定値の設定」（P.5-9）を参照してください。「[NATIVE FTP] オプション」（P.5-38）も参照してください。
PROXYCONN	AsyncOS がプロキシ接続ヘッダーを含めないユーザ エージェントを特定します。「[Proxyconn] オプション」（P.5-41）を参照してください。
SCANNING	DVS エンジンが Web トランザクションのアンチマルウェア スキャニングをどのように処理するかを設定します。「[スキャン（Scanning）] オプション」（P.5-42）を参照してください。
SOCKS	SOCKS プロキシ パラメータを設定します。「[SOCKS] オプション」（P.5-42）を参照してください。
MISCELLANEOUS	Web プロキシがレイヤ 4 スイッチからのヘルス チェックに応答するかどうか、および Web プロキシが TCP 受信ウィンドウ サイズの動的な調整を行うかどうかを設定します。 「[その他（Miscellaneous）] オプション」（P.5-43）を参照してください。

各サブメニューのコマンドは、次の表に詳細に説明されます。[デフォルト値（Default Value）] カラムでは、文字列は「hello world」などの名前または文字のリストを意味します。

認証のオプション

表 5-3 に、advancedproxyconfig CLI コマンドの認証のオプションについて説明します。

表 5-3　advancedproxyconfig CLI コマンド：認証のオプション

オプション	有効な値	デフォルト値	Web プロキシを再起動する必要があるかどうか	説明
いつ承認リクエスト ヘッダーを親プロキシに転送しますか？（When would you like to forward authorization request headers to a parent proxy?）	Never、Always、Only if not used by the WSA	Never	Yes	この設定は、Web プロキシがプロキシを含む「Proxy-Authorization」ヘッダーをアップストリーム サーバに含めるかどうかを決定します。
エンド ユーザ認証ダイアログに表示されるプロキシ承認レルムを入力（Enter the Proxy Authorization Realm to be displayed in the end user authentication dialog）	文字列	「Cisco IronPort Web Security Appliance」	No	[エンド ユーザの認証（End User Authentication）] ダイアログに表示される Proxy Authorization Realm。
要求 URI 内のユーザ名を log に残しますか？（Would you like to log the username that appears in the request URI?）	Yes、No（ブール）	No	No	イネーブルの場合、「<username>: xxxxx」が記録されます。つまり、ユーザ名が表示され、パスワードは「xxxxx」の文字列で表されます。ディセーブルの場合、ユーザ名とパスワードの両方が除去されます。実際のパスワードはこの変数の値に関係なく、表示されないことに注意してください。
グループ メンバシップ属性は Web ユーザ インターフェイスのディレクトリ参照で利用されるべきですか（使用されていない場合、空のグループと別なメンバーシップ属性が表示されます）？（Should the Group Membership attribute be used for directory lookups in the Web UI (when it is not used, empty groups and groups with different membership attributes will be displayed)?）	Yes、No（ブール）	No	No	AsyncOS がディレクトリ ルックアップを行う場合は、グループ メンバーシップ属性を使用するかどうかを選択します。 空の認証グループを表示せず、グループ メンバーシップ属性が異なっているグループを取得する場合は、[はい（Yes）] を選択します。

表 5-3　advancedproxyconfig CLI コマンド：認証のオプション （続き）

オプション	有効な値	デフォルト値	Web プロキシを再起動する必要があるかどうか	説明
高度な Active Directory 接続性チェックを使用しますか？（Would you like to use advanced Active Directory connectivity checks?）	Yes、No（ブール）	No	No	Active Directory サーバと通信する Web プロキシは通信が応答しなくなったが、まだ稼働している場合に、内部認証プロセスを自動的に再開するかどうかを選択します。
ポリシーの大文字小文字を区別しないユーザ名照合を許可しますか？（Would you like to allow case insensitive username matching in policies?）	Yes、No（ブール）	Yes	Yes	ユーザ名をポリシー グループに照合させる場合に、Web プロキシが事例を無視するべきかどうかを選択します。
LDAP グループ名での文字 * を使用したワイルドカード照合を許可しますか？（Would you like to allow wild card matching with the character * for LDAP group names?）	Yes、No（ブール）	Yes	Yes	LDAP グループ フィルタのワイルドカードとしてアスタリスクを照合させるかどうかを選択します。 このオプションがディセーブルの場合、LDAP サーバにグループ フィルタのアスタリスク（*）を使用すると、リテラル ストリングとして作用します。
クライアントで基本認証に使用する文字セットを入力してください [ISO-8859-1/UTF-8]（Enter the charset to be used for basic authentication [ISO-8859-1/UTF-8].）	ISO-8859-1、UTF-8	ISO-8859-1	No	Web プロキシが HTTP 要求で基本認証クレデンシャルを読む取る場合に使用する必要がある文字エンコーディングを選択します。ここで設定される設定は、要求コンテンツに影響しません。基本認証クレデンシャルにだけ影響します。 ネットワークで使用される Web ブラウザのほとんどが Internet Explorer、Firefox、および Safari および UTF-8 であれば ISO-8859-1 を使用します。ネットワークで使用される Web ブラウザのほとんどが Opera および Chrome であれば UTF-8 を使用します。 **注：**Web プロキシは、基本認証クレデンシャルを認証サーバに送信するときに、常に UTF-8 を使用します。

表 5-3　advancedproxyconfig CLI コマンド：認証のオプション （続き）

オプション	有効な値	デフォルト値	Web プロキシを再起動する必要があるかどうか	説明
LDAP 参照を有効にしますか？（Would you like to enable referrals for LDAP?）	Yes、No（ブール）	No	Yes	Web プロキシが言及される LDAP サーバで LDAP クエリーを実行するかどうかを選択します。 言及された LDAP サーバが Web セキュリティ アプライアンスに対して使用可能でない場合に、このオプションをディセーブルにする必要がある場合があります。
セキュア認証を有効にしますか？（Would you like to enable secure authentication?）	Yes、No（ブール）	No	Yes/No （Web プロキシは、より少ないポートまたは追加のポートを傍受する必要があるときに再起動します）	HTTPS を使用して安全に認証クレデンシャルを Web プロキシに渡すために、Web プロキシがクライアントをリダイレクトするかどうかを選択します。 この機能の詳細については、「認証クレデンシャルのセキュアな送信」（P.20-25）を参照してください。
セキュアな認証のリダイレクトポートの入力（Enter the redirect port for secure authentication.）	1 ～ 65535	443	Yes/No （Web プロキシは、より少ないポートまたは追加のポートを傍受する必要があるときに再起動します）	HTTPS を使って要求をリダイレクトするために使用するポートを入力します。1023 より大きいポートを使用することを推奨します。 このオプションの設定の詳細については、「グローバル認証設定の指定」（P.20-19）を参照してください。 **注：**このオプションは、安全な認証をイネーブルにするときにだけ表示されます。
クライアント認証をリダイレクトするホスト名の入力（Enter the hostname to redirect clients for authentication.）	文字列	アプライアンスのホスト名	No	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。 安全な認証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されたリダイレクト URL でこのホスト名を使用します。 このオプションの設定の詳細については、「グローバル認証設定の指定」（P.20-19）を参照してください。

表 5-3　advancedproxyconfig CLI コマンド：認証のオプション （続き）

オプション	有効な値	デフォルト値	Web プロキシを再起動する必要があるかどうか	説明
ユーザ クレデンシャルのサロゲート タイムアウトを入力する（Enter the surrogate timeout for user credentials.）	秒単位の時間	3600	No	この設定は、認証クレデンシャルが再度必要になるまで、サロゲート（IP アドレスまたはクッキー）をユーザ クレデンシャルにどのくらいの期間使用できるかどうかを指定します。 このオプションの設定の詳細については、「グローバル認証設定の指定」（P.20-19）を参照してください。
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する（Enter the surrogate timeout for machine credentials.）	秒単位の時間	10	No	この設定は、認証が必要になるまで、ユーザ クレデンシャルの代わりにマシン クレデンシャルが使用される IP アドレス サロゲートをどのくらいの期間使用できるかどうかを指定します。ネットワークに Network Connectivity Status Indicator（NCSI）機能を使用する Windows 7 または Windows Vista マシン上のユーザが含まれる場合に、この値を設定する必要がある場合があります。 詳細については、「Windows 7 および Windows Vista の使用」（P.20-4）を参照してください。

表 5-3　advancedproxyconfig CLI コマンド：認証のオプション （続き）

オプション	有効な値	デフォルト値	Web プロキシを再起動する必要があるかどうか	説明
リクエスト拒否オプションの再認証の入力 [disabled / embedlinkinblockpage]（Enter re-auth on request denied option [disabled / embedlinkinblockpage]?）	disabled/ embedlinkinblockpage	disabled	No	この設定は、制限が厳しい URL フィルタリング ポリシーによりユーザが Web サイトからブロックされた場合にユーザが再認証できるようにします。 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 ポリシーによりブロックされている認証済みユーザだけに適用されます。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、「ユーザに対する再認証の許可」（P.20-27）を参照してください。

表 5-3　advancedproxyconfig CLI コマンド：認証のオプション （続き）

オプション	有効な値	デフォルト値	Web プロキシを再起動する必要があるかどうか	説明
NTLMSSP 認証で NTLM ヘッダーとともに Negotiate ヘッダーを送信しますか（Would you like to send Negotiate header along with NTLM header for NTLMSSP authentication:）	1、2	1	No	Active Directory サーバで NTLM ハンドシェイクを確立するときに、Web プロキシが許容できる認証プロトコルとして「Negotiate」を送信するかどうかを選択します。次の値のいずれかを選択します。 1. Negotiate ヘッダーを送信しない（Do not send Negotiate header） 2. Negotiateヘッダーを送信する（Send Negotiate header）
ログとレポートのユーザ名と IP アドレス マスクを設定してください（Configure username and IP address masking in logs and reports:）	1、2、3	3	No	ロットおよびレポートでユーザ名および IP アドレス、またはそのいずれかをマスクするかどうかを選択します。マスクされたユーザ名は、ログに「AUTHENTICATED_USER」として表示されますが、ゲストユーザ名はマスクされません。 次のいずれかのオプションを選択します。 1. ログおよびレポートのユーザ名および IP アドレスをマスクする（Mask both user names and IP addresses in logs and reports） 2. ユーザ名のみをマスクし、ログおよびレポートの IP アドレスで置換する（Mask only usernames and replace them with IP addresses in logs and reports） 3. ログおよびレポートのユーザ名および IP アドレスを表示する（Show usernames and IP addresses in logs and reports）

[キャッシング（Caching）] オプション

[キャッシング（Caching）] サブメニューは、高度なキャッシング モードを設定するための 4 つのオプションを提供します。

表 5-4 に、advancedproxyconfig CLI コマンドの [カスタマイズ モード（Customized Mode）] オプションの [キャッシング（Caching）] オプションについて説明します。

表 5-4　advancedproxyconfig CLI コマンド : [キャッシング（Caching）] オプション

オプション	有効な値	デフォルト値	Web プロキシを再起動する必要があるかどうか	説明
ヒューリスティック型の有効期限を持つオブジェクトを、変更されない If-Modified-Since キャッシュヒットとして提供することを許可しますか?（Would you like to allow objects with a heuristic expiration time to be served as not-modified If-Modified-Since hits from cache?）	Yes、No（ブール）	Yes	No	0 = ヒューリスティックの有効期限を使用したオブジェクトへの IMS の有効期間を優先する 1 = 帯域幅の保持を優先する
クライアントの更新の際、ETAG の不一致を許可しますか?（Would you like to allow ETAG mismatch on client revalidations?）	Yes、No（ブール）	No	No	場合によっては、サーバが同じファイルの同じバージョンで別の ETags を報告することがあります。これは、たとえばクラスタ化された IIS サーバで見られます。このような場合、クライアントの再評価で Last Modified Time（LMT）の一致と ETag の一致の両方を必要とすると、多くのミスを発生させるため、指定されている場合は、LMT のみに一致するだけで十分です。 **注 :** これを 1 に設定することは、HTTP に準拠していません。
元のサーバからの認証リクエストを受けた場合のキャッシュを許可しますか ?（Would you like to allow caching when requests are authenticated by the origin server?）	Yes、No（ブール）	No	Yes	発信サーバによって認証された要求のキャッシングを許可します。

表 5-4　advancedproxyconfig CLI コマンド : [キャッシング（Caching）] オプション （続き）

オプション	有効な値	デフォルト値	Web プロキシを再起動する必要があるかどうか	説明
DNS の結果と TCP の接続先 IP と異なるサーバのキャッシュを許可しますか（trust-worthy ではなく、トランスペアレント モードのときのみ有効）？（Would you like to allow caching from servers whose DNS results do not match the TCP destination IP (not trust-worthy and applicable only in transparent modes)?）	Yes、No（ブール）	No	Yes	DNS の結果が TCP 宛先 IP に一致しないサーバからのキャッシングを許可します。
ドキュメント最終更新時間が設定されていて、実キャッシュがない場合の最大キャッシュの帰納的有効期限を入力してください（秒）（Enter the Heuristic maximum age to cache the document with Last-Modified Time but no actual caching value (in seconds):）	秒単位の時間	86400	No	実際のキャッシング値ではなく、LMT によるドキュメントをキャッシュするヒューリスティック最長期間。
ドキュメント最終更新時間が設定されていない、実キャッシュ値が無い場合の最大キャッシュの帰納的有効期限を入力してください（秒）（Enter the Heuristic maximum age to cache the document without Last-Modified Time and no actual caching value (in seconds):）	秒単位の時間	0	No	実際のキャッシング値ではなく、LMT がないドキュメントをキャッシュするヒューリスティック最長期間。

表 5-4　advancedproxyconfig CLI コマンド : [キャッシング（Caching）] オプション （続き）

オプション	有効な値	デフォルト値	Web プロキシを再起動する必要があるかどうか	説明
エラー帰納的有効期限を入力してください（HTTP_SERVICE_UNAVAIL、HTTP_GATEWAY_TIMEOUT など）（秒）（Enter the Heuristic age to cache errors (HTTP_SERVICE_UNAVAIL, HTTP_GATEWAY_TIMEOUT etc) (in seconds):）	秒単位の時間	300	No	エラー（HTTP_SERVICE_UNAVAIL、HTTP_GATEWAY_TIMEOUT など）をキャッシュするヒューリスティック経過時間。
クライアントがキャッシュからコンテンツを取得しない方針をプロキシが無視しますか？（Would you like proxy to ignore client directive to not fetch content from the cache?）	Yes、No（ブール）	No	No	キャッシュからのコンテンツを取得しないために、クライアント ディレクティブの無視をディセーブル/イネーブルにします。このイネーブル化は、HTTP 準拠ではありません。
どの再ロード リクエストがプロキシによって無視されるのか間のインターバルを入力（秒）（Enter the time interval during which reload requests must be ignored by the proxy (in seconds):）	秒単位の時間	0	No	指定された時間間隔で無視されるように、要求のリロードをディセーブル/イネーブルにします。 これは、HTTP 準拠ではなくても、一定期間要求のリロードが無視されるようにします。 帯域幅使用率を改善させるために、ゼロより大きい値を入力する必要がある場合があります。
再ロード リクエストを max-age リクエストに変換させることをプロキシに許可しますか？（Would you like to allow proxy to convert reload requests into max-age requests?）	Yes、No（ブール）	No	No	リロード要求が最大経過時間の要求に変換されます（HTTP 準拠でありませんが、帯域幅の使用率を改善する可能性があります）。これは、「ignoreReloadTime」から最大経過時間を取得します。
IMS リフレッシュ要求を送信までの時間を秒単位で指定（Time in seconds after which an explicit IMS Refresh request must be issued:）	秒単位の時間	300	No	明示的な IMS Refresh 要求が発行される秒単位の時間。

[カスタム ヘッダ（Custom Header）] オプション

表 5-5　advancedproxyconfig CLI コマンド : [カスタム ヘッダ（Custom Header）] オプション

オプション	有効な値	デフォルト値	Web プロキシを再起動する必要があるかどうか	説明
削除（Delete）	1、2、3	—	No	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（New）	ヘッダーの場合： 「header_name: header_text」形式の文字列（名前: 値のペア） ドメインの場合： 文字列（ドメイン名またはドメイン名のカンマ区切りのリスト）	—	No	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）	[新規（New）] を参照してください。	—	No	既存のヘッダーを指定する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。

[DNS] オプション

表 5-6 に、advancedproxyconfig CLI コマンドの [DNS] オプションについて説明します。

表 5-6　advancedproxyconfig CLI コマンド : [DNS] オプション

オプション	有効な値	デフォルト値	Web プロキシを再起動する必要があるかどうか	説明
DNS 参照失敗時の HTTP 307 リダイレクトに使用する URL フォーマットを入力（Enter the URL format for the HTTP 307 redirection on DNS lookup failure:）	EUN ページ変数による文字列	%P//www.%H.com/%u	No	URL format for the HTTP 307 redirection on DNS lookup failure. 有効な変数の一覧については、表 16-2「カスタマイズしたエンド ユーザ通知ページの変数」（P.6）を参照してください。
プロキシは DNS 参照失敗時に HTTP 307 リダイレクトを行いますか？（Would you like the proxy to issue a HTTP 307 redirection on DNS lookup failure?）	Yes、No（ブール）	Yes	Yes	DNS ルックアップの失敗で自動 HTTP 307 リダイレクションをディセーブル / イネーブルにします。
上位プロキシ（peer）が応答しない場合に、プロキシが自動的に DNS 結果をフェールオーバーしないようにしますか？(Would you like proxy not to automatically failover to DNS results when upstream proxy (peer) is unresponsive?)	Yes、No（ブール）	No	Yes	アップストリーム プロキシ（ピア）が応答しない場合、DNS 結果の自動フェールオーバーをディセーブル / イネーブルにします。
Web サーバの検索方法（Find web server by:）	0、1、2、3	1	Yes	アプライアンスが要求された Web サーバの場所を見つける方法を指定します。 • 0 = 順番に DNS 応答を使用 • 1 = クライアントが提供したアドレスを使用。次に、DNS を使用 • 2 = クライアントが提供したアドレスだけを使用 • 3 = クライアントが提供したアドレスをネクスト ホップ接続および Web レピュテーションに使用（警告：宛先 IP ベースのポリシーは DNS を使用）。

[EUN] オプション

表 5-7 に、advancedproxyconfig CLI コマンドの [EUN] オプションについて説明します。

表 5-7　advancedproxyconfig CLI コマンド：[EUN] オプション

オプション	有効な値	デフォルト値	Web プロキシを再起動する必要があるかどうか	説明
選択：（Choose:）	1、2、3	3	Yes	IronPort エンドユーザ通知ページまたはアップロードされたカスタマイズ済みエンドユーザ通知ページを使用するかどうかを選択します。 次のいずれかのオプションを選択します。 • 1. Refresh EUN pages • 2. Use Custom EUN pages • 3. Use Standard EUN pages 詳細については、「オンボックス エンド ユーザ通知ページの編集」（P.16-5）を参照してください。
ユーザ確認応答ページの提示をオンにしますか？（Would you like to turn on presentation of the User Acknowledgement page?）	Yes、No（ブール）	No	No	確認ページをイネーブルまたはディセーブルにします。
ユーザ確認の追跡に使用する方法を入力する（「ip」または「session」）（Enter the method to be used for tracking User Acknowledgements (“ip” or “session”).）	ip、session	ip	No	この設定は、ユーザがエンドユーザの確認ページでリンクをクリックしたユーザの後で、Web プロキシが IP アドレスまたは Web セッションのクッキーを使用してユーザを追跡する方法を指定します。 このオプションの設定の詳細については、「エンド ユーザ確認ページ」（P.16-12）を参照してください。

表 5-7　advancedproxyconfig CLI コマンド : [EUN] オプション （続き）

オプション	有効な値	デフォルト値	Web プロキシを再起動する必要があるかどうか	説明
セッション ベースの EUA による HTTPS リクエストのために実行するアクション（「bypass」または「drop」）（Action to be taken for HTTPS requests with Session based EUA (“bypass” or “drop”).）	bypass、drop	bypass	Yes	エンドユーザの確認ページがイネーブルで、セッション Cookie を使用してユーザを追跡する場合、HTTPS 要求をバイパス（パス スルー）するか、HTTPS 要求をドロップするかどうかを選択します。詳細については、「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」（P.16-15）を参照してください。 このオプションは、ユーザ確認追跡メソッドでセッション Cookie を選択する場合にのみ表示されます。
ユーザ確認応答の最大記憶時間を入力（秒）（Enter maximum time to remember User Acknowledgement (in seconds):）	30 ～ 2678400	86400	No	ユーザ確認を記録する最大時間。30 秒 ～ 1 か月（2678400）。
IP アドレスに基づくユーザ確認応答の最大アイドル タイムアウトを入力（秒）（Enter maximum idle timeout for User Acknowledgement based on IP Address (in seconds):）	30 ～ 2678400	14400	No	IP アドレスに基づくユーザ確認の最大アイドル タイムアウト。30 秒 ～ 1 か月（2678400）。

[NATIVE FTP] オプション

表 5-8 に、advancedproxyconfig CLI コマンドの [NATIVE FTP] のオプションについて説明します。

表 5-8　advancedproxyconfig CLI コマンド : [NATIVEFTP] オプション

オプション	有効な値	デフォルト値	Web プロキシを再起動する必要があるかどうか	説明
FTP プロキシを有効にしますか？（Would you like to enable FTP proxy?）	Yes、No（ブール）	Yes	Yes	FTP プロキシをイネーブルにするかどうかを選択します。
FTP プロキシがリッスンするポートの入力（Enter the ports that FTP proxy listens on.）	1 ～ 65535	8021	Yes	FTP プロキシを使用したコントロール接続の確立で使用するポート FTP クライアントを指定します。
プロキシがパッシブ FTP 接続をリッスンするポート番号の範囲を入力（Enter the range of port numbers for the proxy to listen on for passive FTP connections.）	port1-port2（文字列） 1024 ～ 65535	11000 ～ 11009	Yes	パッシブ モード接続で FTP プロキシを使用したデータ接続の確立に FTP クライアントが使用する TCP ポートの範囲を指定します。
プロキシがアクティブ FTP 接続をリッスンするポート番号の範囲を入力（Enter the range of port numbers for the proxy to listen on for active FTP connections.）	port1-port2（文字列） 1024 ～ 65535	12000 ～ 12099	Yes	アクティブ モード接続で FTP プロキシを使用したデータ接続の確立に FTP サーバが使用する TCP ポートの範囲を指定します。この設定は、ネイティブ FTP および FTP over HTTP 接続の両方に適用されます。
認証フォーマットの入力：（Enter the authentication format:）	Check Point、Raptor	Check Point	Yes	FTP クライアントと通信する場合に、FTP プロキシが使用する認証形式を選択します。詳細については、「ネイティブ FTP での認証の使用」（P.5-8）を参照してください。
キャッシュを有効にしますか？（Would you like to enable caching?）	Yes、No（ブール）	Yes	Yes	匿名ユーザからデータ接続のコンテンツをキャッシュするかどうかを選択します。

表 5-8　advancedproxyconfig CLI コマンド : [NATIVEFTP] オプション （続き）

オプション	有効な値	デフォルト値	Web プロキシを再起動する必要があるかどうか	説明
サーバ IP スプーフィングを有効にしますか ?（Would you like to enable server IP spoofing?）	Yes、No (ブール)	No	Yes	FTP プロキシが FTP サーバの IP アドレスをスプーフィングするかどうかを選択します。IP アドレスがコントロール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 クライアントに対してこれを実行する必要がある場合があります。
FTP サーバ ウェルカム メッセージをクライアントに送信しますか ?（Would you like to pass FTP server welcome message to the clients?）	Yes、No (ブール)	Yes	Yes	FTP クライアントで表示する初期メッセージを選択します。 • **[FTP サーバメッセージ（FTP server message）]。**「Yes」と入力します。[FTP サーバ メッセージ（FTP server message）] は、透過的にリダイレクトされた接続に対してのみ表示されます。ネイティブ FTP 接続が FTP プロキシに明示的に送信されると、FTP クライアントは FTP プロキシによって事前定義されたメッセージを表示します。 • **[カスタム メッセージ（Custom message）]。**「No」を入力します。次の質問ですべてのネイティブ FTP 接続を表示するために、カスタム メッセージを入力できます。
カスタム サーバ ウェルカム メッセージの入力（Enter the customized server welcome message.）	文字列	該当なし	Yes	このコマンドは、FTP サーバの初期メッセージで [いいえ（No）] と入力したときに表示されます。 すべてのネイティブ FTP 接続用に表示するカスタム メッセージを入力します。
ftp サーバ ディレクトリの最大パス サイズを入力 :（Enter the max path size for the ftp server directory:）	整数	1024	No	FTP クライアントで使用可能な FTP サーバのディレクトリ パスの最大長を入力します。

[FTPOVERHTTP] オプション

表 5-9 に、advancedproxyconfig CLI コマンドの [FTPOVERHTTP] オプションについて説明します。

表 5-9　advancedproxyconfig CLI コマンド：[FTPOVERHTTP] オプション

オプション	有効な値	デフォルト値	Web プロキシを再起動する必要があるかどうか	説明
anonymous FTP アクセスで必要なログイン名を入力してください：(Enter the login name to be used for anonymous FTP access:)	文字列	anonymous	No	匿名 FTP ログイン名。
anonymous FTP アクセスで必要なパスワードを入力してください：(Enter the password to be used for anonymous FTP access:)	文字列	proxy@	No	匿名 FTP ログイン パスワード。

[HTTPS] オプション

表 5-10 に、advancedproxyconfig CLI コマンドの [HTTPS] オプションについて説明します。

表 5-10　advancedproxyconfig CLI コマンド：[HTTPS] オプション

オプション	有効な値	デフォルト値	Web プロキシを再起動する必要があるかどうか	説明
HTTPS URI のログ形式：(HTTPS URI Logging Style:)	fulluri または stripquery	fulluri	Yes	URI 全体（fulluri）またはクエリー部分が削除された URI の一部（stripquery）を記録できます。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。

表 5-10　advancedproxyconfig CLI コマンド : [HTTPS] オプション （続き）

オプション	有効な値	デフォルト値	Web プロキシを再起動する必要があるかどうか	説明
認証目的で、認証されていない透過的 HTTPS リクエストを復号化しますか?（Would you like to decrypt unauthenticated transparent HTTPS requests for authentication purpose?）	Yes、No (ブール)	Yes	No	Web プロキシが IP ベースのサロゲートを持つ ID を使用して認証された HTTP 要求を受信する前に、透過的にリダイレクトされた HTTPS トランザクションを処理する方法を選択します。次のオプションのいずれかを選択します。 • **Yes.** 認証の目的で HTTPS 要求を複合化します。 • **No.**HTTPS 要求を拒否します。
ハンドシェイク中に HTTPS サーバがクライアントの証明書を求めるときに実行するアクション：（Action to be taken when HTTPS servers ask for client certificate during handshake:）	1、2	2	Yes	SSL ハンドシェイク時にクライアント証明書を問い合わせるときに、HTTPS プロキシが HTTPS サーバに応答する方法を選択します。 • 1. Pass through the transaction • 2. Reply with certificate unavailable **（注）** HTTPS サーバがクライアント証明書を要求したときを把握するためにプロキシ ログを読み取ることができます。

[Proxyconn] オプション

AsyncOS がプロキシ接続ヘッダーを含めないユーザ エージェントを特定します。

表 5-11　advancedproxyconfig CLI コマンド : [Proxyconn] オプション

オプション	有効な値	デフォルト値	Web プロキシを再起動する必要があるかどうか	説明
新規（New）	正規表現	—	No	ユーザ エージェントを照合する正規表現。 例： Mozilla/.* Gecko/.* Firefox/ は、すべての FireFox バージョンに一致します。
削除（Delete）	1、2、3[...]	—	No	削除するユーザ エージェントを表す整数。このオプションは、設定されたユーザ エージェントの番号付きリストを返します。

[スキャン（Scanning）] オプション

はじめる前に

- マルウェア スキャニングの結果をイネーブルにすると、Web プロキシのパフォーマンスに大きな影響が生じることに注意してください。
- スキャニング オプションを編集する前の適応型スキャニングをディセーブルにします。

表 5-12　advancedproxyconfig CLI コマンド : [スキャン（Scanning）] オプション

オプション	有効な値	デフォルト値	Web プロキシを再起動する必要があるかどうか	説明
コンテンツ タイプにかかわらず、プロキシですべてのコンテンツに対してマルウェア スキャンを実行しますか? (Would you like the proxy to do malware scanning all content regardless of content type?)	Yes、No (ブール)	No	No	DVS エンジンがコンテンツの種類に関係なく、すべての応答コンテンツをスキャンするかどうかを選択します。

[SOCKS] オプション

表 5-13　advancedproxyconfig CLI コマンド : [SOCKS] のオプション

オプション	有効な値	デフォルト値	Web プロキシを再起動する必要があるかどうか	説明
SOCKS プロキシを有効にしますか? (Would you like to enable SOCKS proxy?)	Yes、No (ブール)	N	Yes	—
プロキシ ネゴシエーション タイムアウト（Proxy Negotiation Timeout.）	1 ～ 60	60	Yes	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 トンネル タイムアウト（UDP Tunnel Timeout.）	1 ～ 60	60	Yes	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。

表 5-13　advancedproxyconfig CLI コマンド : [SOCKS] のオプション （続き）

オプション	有効な値	デフォルト値	Web プロキシを再起動する必要があるかどうか	説明
SOCKS 制御ポート（SOCKS Control Ports.）	ポート範囲は、1 ～ 65535 です。	1080	Yes	SOCKS 要求を受け入れるポート。デフォルトは 1080 です。
UDP リクエスト ポート（UDP Request Ports.）	ポート範囲は、1 ～ 65535 です。	16000 ～ 16100	Yes	SOCKS サーバがリスンする必要がある UDP ポート。デフォルトは 16000 ～ 16100 です。

[その他（Miscellaneous）] オプション

表 5-14　advancedproxyconfig CLI コマンド : [その他（Miscellaneous）] オプション

オプション	有効な値	デフォルト値	Web プロキシを再起動する必要があるかどうか	説明
L4 スイッチからのヘルスチェックに応答しますか（WSA が L4 トランスペアレント モードである場合常に有効）?（Would you like proxy to respond to health checks from Layer 4 switches (always enabled if WSA is in L4 transparent mode)?）	Yes、No (ブール)	No	Yes	レイヤ 4 スイッチからのヘルスチェックに応答するサポートをイネーブル/ディセーブルにします（WSA が L4 トランスペアレント モードの場合は、常にイネーブルにされています）。レイヤ 4 スイッチは、応答していることを確認するためにプロキシでダイレクトされた「HEAD / HTTP/1.0」要求を発行します。
プロキシで TCP の受信ウィンドウ サイズの動的な適応を実行しますか?（Would you like proxy to perform dynamic adjustment of TCP receive window size?）	Yes、No (ブール)	Yes	Yes	TCP 受信ウィンドウ サイズの動的な調整をディセーブル/イネーブルにします。
HTTPS 応答のキャッシュを有効にしますか?（Enable caching of HTTPS responses?）	Yes、No (ブール)	No	No	Webセキュリティ アプライアンスが Web キャッシュで HTTPS 応答を保存するかどうかを選択します。

表 5-14　advancedproxyconfig CLI コマンド : [その他（Miscellaneous）] オプション （続き）

オプション	有効な値	デフォルト値	Web プロキシを再起動する必要があるかどうか	説明
上位プロキシの無応答のチェックの最小アイドルタイムアウトを入力（秒）（Enter minimum idle timeout for checking unresponsive upstream proxy (in seconds).）	秒単位の時間	10	No	アップストリーム プロキシがまだ使用不可の状態であるかを確認するまで、Web プロキシが待機する最小時間。
上位プロキシの無応答のチェックの最大アイドルタイムアウトを入力（秒）（Enter maximum idle timeout for checking unresponsive upstream proxy (in seconds).）	秒単位の時間	86400	No	アップストリーム プロキシがまだ使用不可の状態であるかを確認するまで、Web プロキシが待機する最大時間。
プロキシのモード：（Mode of the proxy:）	1、2、3	2	Yes	次のいずれかのオプションを使用して、Web プロキシの展開方法を選択します。 • 1. Explicit forward mode only • 2. Transparent mode with L4 Switch or no device for redirection • 3. Transparent mode with WCCP v2 Router for redirection 詳細については、「導入の概要」（P.3-1）を参照してください。

表 5-14　advancedproxyconfig CLI コマンド : [その他（Miscellaneous）] オプション （続き）

オプション	有効な値	デフォルト値	Web プロキシを再起動する必要があるかどうか	説明
プロキシによるクライアント IP のスプーフィング：(Spoofing of the client IP by the proxy:)	1、2、3	1	No	次のいずれかのオプションを使用してアップストリーム プロキシおよびサーバに要求を送信するときに Web プロキシが IP アドレスをスプーフィングするかどうかを選択します。 • 1. Disable • 2. Enable for all requests • 3. Enable for transparent requests only IP スプーフィングがイネーブルの場合、クライアントから送信される要求はクライアントの送信元アドレスを保持し、Web セキュリティ アプライアンスではなくクライアントから送信されたように表示されます。 **（注）** 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、リターン パスをリダイレクトするように WCCP サービスを設定します。
HTTP X-Forwarded-For ヘッダーを通過させますか?(Do you want to pass HTTP X-Forwarded-For headers?)	Yes、No (ブール)	Yes	No	Web プロキシが受信した要求に含まれる「X-Forwarded-For」ヘッダーを保持するかどうかを選択します。 [いいえ（No）] に設定すると、Web プロキシからダウンストリーム プロキシ サーバに入力される要求から「X-Forwarded-For」ヘッダーを削除します。ダウンストリーム プロキシ サーバのヘッダーにクライアント IP アドレスが含まれ、ネットワーク外のサーバに IP アドレスを公開しない場合は、これを実行する場合があります。

表 5-14　advancedproxyconfig CLI コマンド : [その他（Miscellaneous）] オプション （続き）

オプション	有効な値	デフォルト値	Web プロキシを再起動する必要があるかどうか	説明
HTTP ポートにおける HTTP 以外のリクエストのトンネルを許可しますか？（Would you like to permit tunneling of non-http requests on http ports?）	Yes、No（ブール）	Yes	No	Web プロキシがモニタするように設定されているポート 80 などのポートの非 HTTP トラフィックを許可するかどうかを選択します。このオプションは、Web プロキシがトランスペアレント モードにある場合に適用されます。 このオプションをイネーブルにすると、通常 HTTP トラフィックに使用されるポートの非 HTTP トラフィックをトンネリングするアプリケーションをブロックします。 **（注）** トランザクションがこの設定にブロックされている場合、トランザクションの ACL の決定タグは BLOCK_ADMIN_TUNNELING として記録されます。
SSL ポートにおける SSL 以外のトランザクションのトンネルをブロックしますか？（Would you like to block tunneling of non-SSL transactions on SSL Ports?）	Yes、No（ブール）	No	No	Web プロキシは SSL ポートで非 SSL トラフィックをブロックするかどうかを選択します。 デフォルトで（この機能がディセーブルの場合）、クライアントが設定された SSL ポートに接続しようとし、サーバとの SSL ハンドシェイクが失敗すると、Web プロキシがトランザクションをトンネリングします。
プロキシで受信接続の IP アドレスの代わりに X-Forwarded-For ヘッダーの値を記録しますか？（Would you like proxy to log values from X-Forwarded-For headers in place of incoming connection IP addresses?）	Yes、No（ブール）	No	No	アクセス ログに、着信接続の IP アドレスの代わりに X-Forwarded-For ヘッダー値を含めるかどうかを選択します。

表 5-14　advancedproxyconfig CLI コマンド : [その他（Miscellaneous）] オプション （続き）

オプション	有効な値	デフォルト値	Web プロキシを再起動する必要があるかどうか	説明
プロキシでキャッシュからのコンテンツをスロットルしますか？（Do you want proxy to throttle content served from cache?）	Yes、No (ブール)	Yes	No	Web プロキシが Web サーバから提供されたコンテンツだけでなく、Web キャッシュから提供されたコンテンツに帯域幅制御をユーザごとに適用するかどうかを選択します。帯域幅制限が適用されたアプリケーション タイプに適用されます。
X-Forwarded-For ヘッダーからのクライアント IP アドレスをプロキシに使用させますか？（Would you like the proxy to use client IP addresses from X-Forwarded-For headers?）	Yes、No (ブール)	No	No	Web プロキシが信頼され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 X-Forwarded-For ヘッダーのクライアント IP アドレスを受け入れるかどうかを選択します。 「Yes」を選択する場合、Web プロキシが信頼するダウンストリーム プロキシまたはロード バランサの IP アドレスを入力します。Web プロキシは、リストに含まれないマシンからの X-Forwarded-For ヘッダーの IP アドレスを受け入れません。複数の IP アドレスはカンマで区切って指定します。サブネットまたはホスト名を入力できません。 **（注）** %XV のカスタム フォーマット指定子を使用してアクセス ログのダウンストリーム IP アドレスを表示し、x-request-source-ip 変数を使用して W3C アクセス ログのダウンストリーム IP アドレスを表示できます。

6
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。アクセス ポリシーと同等の SOCKS ポリシーが 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 ポリシーでどのトランザクションで管理されるかを指定できます。アクセス ポリシーと同様に、SOCKS ポリシーがトランザクションに適用された後、ルーティング ポリシーがトラフィックのルーティングを管理できます。

コメント

- SOCKS プロトコルは、直接転送接続のみをサポートしています。
- SOCKS プロキシは、アップストリーム プロキシをサポートしていません（アップストリーム プロキシに転送されません）。
- SOCKS プロキシは、Application Visibility and Control（AVC）、Data Loss Prevention（DLP）、およびマルウェア検出に使用されるスキャニング サービスをサポートしていません。
- SOCKS プロキシは、ポリシー追跡をサポートしていません。
- SOCKS プロキシは、SSL トラフィックを復号化できません。これは、クライアントからサーバにトンネリングします。

SOCKS トラフィックの処理をイネーブルにし、設定する方法

	作業	追加情報
ステップ 1	Web プロキシをイネーブルにします。	「HTTP トラフィックの処理のイネーブル化」（P.5-2）
ステップ 2	SOCKS プロキシをイネーブルにします。	「SOCKS トラフィックの処理のイネーブル化」（P.6-2）
ステップ 3	SOCKS プロキシを設定します。	「SOCKS プロキシの設定」（P.6-2）

	作業	追加情報
ステップ 4	（任意）SOCKS ポリシーで使用するための ID を追加します。	「ID の作成」（P.8-18）
ステップ 5	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。	「SOCKS ポリシーの設定」（P.6-3）

SOCKS トラフィックの処理のイネーブル化

ステップ 1　[セキュリティ サービス（Security Services）] > [SOCKS プロキシ（SOCKS 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　[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 [実行（Submit）] および [確定する（Commit）] します。

次の項目に戻る

- 「SOCKS トラフィックの処理をイネーブルにし、設定する方法」（P.6-1）

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）] ページの順に移動します。

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　[SOCKS プロキシを有効にする （Enable SOCKS Proxy）] が選択されていることを確認します。

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（SOCKS Proxy）	イネーブル
SOCKS 制御ポート（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 リクエストポート（UDP Request Ports）	SOCKS サーバがリスンする必要がある UDP ポート。デフォルトは 16000 ～ 16100 です。
プロキシ ネゴシエーション タイムアウト（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 トンネル タイムアウト（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。

次の項目に戻る

- 「SOCKS トラフィックの処理をイネーブルにし、設定する方法」（P.6-1）

SOCKS ポリシーの設定

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）] ページの順に進みます。

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。

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。正しい照合が確実に行われるように、ポリシーを慎重に並べます。

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。

詳細オプション	説明
プロキシ ポート（Proxy Ports）	ブラウザに設定されたポート。 オプションで、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：**このグループ ポリシーに関連付けられた ID がこの詳細設定で ID メンバーシップを定義すると、SOCKS ポリシー グループ レベルではこの設定を設定することはできません。

詳細オプション	説明
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：**このポリシー グループに関連付けられた ID によってアドレスでそのメンバーシップが定義されている場合は、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。 時間に基づいたポリシーの作成の詳細については、「時間ベースのポリシーの使用」（P.7-9）を参照してください。 時間範囲の作成の詳細については、「時間範囲の作成」（P.7-10）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。

ロギング

ここでは、第 24 章「ロギング」を SOCKS トラフィック固有の情報で補足します。

トランザクション結果コード

結果コード	説明
UDP_MISS	オブジェクトは発信サーバから取得されました。

ログ フィールド、フォーマット指定子、およびフィールド値

W3C ログ フィールド	フォーマット指定子	フィールド値	説明
x-elapsed-time	%e	97	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。

7
ポリシー

ポリシーの概要

ポリシーは、ユーザ、グループ、およびその他の基準に基づいてトランザクションを制御する方法です。ポリシーの例：

- マーケティング グループのユーザは、競合他社の Web サイトにアクセスできますが、他のユーザはアクセスできません。
- 購買部のコンピュータなど、顧客に対応するマシンのゲスト ユーザは、銀行サイトにアクセスできませんが、従業員はアクセスできます。
- ユーザはギャンブル サイトにアクセスできません。ユーザがギャンブル サイトを表示しようとすると、代わりに組織のポリシーを説明する Web ページが表示されます。
- もう存在していない特定のサイトにアクセスしようとするすべてのユーザは別のサイトにリダイレクトされます。
- IT 部門以外のすべてのユーザは、マルウェアの可能性があるサイトへのアクセスがブロックされますが、IT 部門のユーザは、これらのサイトへテスト目的でアクセスでき、ダウンロードするコンテンツが有害なオブジェクトであるかどうかスキャンされます。
- ストリーミング メディアに対するすべての要求は、業務時間内はブロックされますが、業務時間外は許可されます。
- ソフトウェア更新プログラムなど、特定のユーザ エージェントからのすべての要求は、認証なしに許可されます。
- 2 MB を超えるすべての Excel スプレッドシート ファイルのアップロードはブロックされます。
- Web レピュテーションが低いサイトへのデータのアップロードはブロックされます。
- マルウェアに感染したデータのアップロードはブロックされます。

関連項目

- 「ポリシー タイプ」（P.7-2）
- 「ポリシー グループの使用」（P.7-5）

- 「ポリシーのトレース」（P.7-13）

ブロックと許可の決定

Web セキュリティ アプライアンスは、デフォルトでは高い許容性があります。つまり、ポリシー グループで明確にブロックされない限り、要求は許可されます。

ファイル タイプ

AsyncOS は、まずファイル ヘッダーの情報を調べてファイル タイプを識別します。保証される場合、そのファイルをスキャンします。ヘッダーがファイルを 1 つのタイプ（たとえば、PDF）として識別し、AsyncOS がスキャンを通じて実際には別のタイプ（たとえば、実行可能ファイル）と判定した場合、実際のファイル タイプがポリシーで許可される場合であっても、AsyncOS はトランザクションをブロックします。これは、ファイル タイプの誤認によって、セキュリティ上の脅威が存在する可能性があるためです。

ポリシー	ファイル タイプ（ヘッダーにより識別）	ファイル タイプ（スキャンにより判定）	結果
ファイル タイプ *X* をブロックする	*X*	N/A（ファイルがスキャンされない）	ブロック
ファイル タイプ *X* を許可する	*X*	*X*	許可
ファイル タイプ *X* を許可し、ファイル タイプ *Y* を許可する	*X*	*Y*	ブロック

ポリシー タイプ

Web セキュリティ アプライアンスは、複数のポリシーのタイプを使用して、組織のポリシーおよび要件を適用します。

- **ID。**「あなたは誰ですか。」
- **復号化ポリシー。**「復号化しますか、復号化しませんか。」
- **ルーティング ポリシー。**「どこからコンテンツを取得しますか。」
- **アクセス ポリシー。**「トランザクションを許可しますか、ブロックしますか。」
- **Cisco IronPort データ セキュリティ ポリシー。**「データのアップロードをブロックしますか。」Cisco IronPort データ セキュリティ ポリシーのアクションは、Web セキュリティ アプライアンスで定義されます。
- **外部 DLP（データ消失防止）ポリシー。**「データのアップロードをブロックしますか。」外部 DLP ポリシーのアクションは、外部 DLP アプライアンスで定義されます。
- **発信マルウェア スキャン ポリシー。**「悪意のあるデータのアップロードをブロックしますか。」
- **SaaS アプリケーション認証ポリシー。**「このユーザの SaaS アプリケーションへのアクセスを許可しますか。」

ポリシーを併用して、クライアントが Web にアクセスする際に必要な動作または予期する動作を作成します。

ポリシーを定義するには、ポリシー グループを作成します。ポリシー グループを作成すると、各グループの制御設定を定義できます。ポリシー グループの使用方法の詳細については、「ポリシー グループの使用」（P.7-5）を参照してください。

すべてのポリシー タイプには、別のポリシーによってカバーされない Web トランザクションに適用するデフォルトの設定とルールを保持するグローバル ポリシー グループが含まれています。グローバル ポリシーの詳細については、「ポリシー グループの使用」（P.7-5）を参照してください。

ID

ID は、要求を行うユーザを識別するポリシーです。これは、認証が必要かどうかを定義できる唯一のポリシーです。ID は、「あなたは誰ですか。」という質問に対処します。ただし、ID は Web へのアクセスが*許可されている*ユーザのリストを指定するものでは*ありません*。使用する ID を指定したら、他のポリシー タイプで許可されるユーザを指定します。

他のポリシーを作成する場合は、すべてに ID を指定する必要があります。

[Web セキュリティ マネージャ（Web Security Manager）] > [アイデンティティ（Identities）] ページで ID を設定します。ID の詳細については、「ID」（P.8-1）を参照してください。

復号化ポリシー

復号化ポリシーによって、HTTPS 接続が復号化されるか、パススルーされるか、ドロップされるかが決まります。これらは、「復号化しますか、復号化しませんか。」という質問に対処します。

アプライアンスは、復号化ポリシーを使用して HTTPS 要求を評価します。HTTPS 要求に適用される復号化ポリシー グループは、アプライアンスが接続をドロップするか、復号化せずにパススルーするか、接続を復号化し、その後復号化された要求と応答を定義済みのアクセス ポリシー グループに対して評価するかを決定します。

[Web セキュリティ マネージャ（Web Security Manager）] > [復号化ポリシー（Decryption Policies）] ページで復号化ポリシー グループを設定します。復号化ポリシー グループの詳細については、「HTTPS トラフィックの処理」（P.11-1）を参照してください。

ルーティング ポリシー

ルーティング ポリシーは、クライアント要求を別のプロキシに渡すか、または宛先サーバに渡すかを決定します。これらは、「どこからコンテンツを取得しますか。」という質問に対処します。

このポリシー タイプを使用して、ロード バランシングやフェールオーバーに設定されているアップストリーム プロキシ グループを選択できます。

[Web セキュリティ マネージャ（Web Security Manager）] > [ルーティング ポリシー（Routing Policies）] ページでルーティング ポリシーを設定します。ルーティング ポリシーの詳細については、「外部プロキシの使用」（P.10-1）を参照してください。

アクセス ポリシー

アクセス ポリシーは、HTTP および復号化された HTTPS トランザクションを許可するか、ブロックするかを決定します。これらは、「トランザクションを許可しますか、ブロックしますか。」という質問に対処します。

アクセス ポリシーは、アプライアンスが HTTP および 復号化された HTTPS 要求のための Web 上のサービス、アプリケーション、オブジェクトへのアクセスを制御する方法を決定します。アプライアンスは、アクセス ポリシーを使用して、HTTP 要求および復号化するように指定された HTTPS 要求を評価し、スキャンします。

[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）] ページでアクセス ポリシー グループを設定します。アクセス ポリシー グループの詳細については、「トランザクション要求のブロック、許可、またはリダイレクト」（P.9-1）を参照してください。

Cisco IronPort データ セキュリティ ポリシー

Cisco IronPort データ セキュリティ ポリシーは、Web セキュリティ アプライアンスで定義されたロジックを使用して、データの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。これらは、「データのアップロードをブロックしますか。」という質問に対処します。

Web プロキシは、Cisco IronPort データ セキュリティ ポリシーを使用して、要求本文にデータを含む HTTP 要求および復号化された HTTPS 要求を評価し、スキャンします。

[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 グループを設定します。データ セキュリティ ポリシー グループの詳細については、「データ セキュリティと外部 DLP ポリシー」（P.13-1）を参照してください。

外部 DLP ポリシー

外部 DLP（データ消失防止）ポリシーは、外部 DLP サーバに保存されたロジックを使用して、データの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。これらは、「データのアップロードをブロックしますか。」という質問に対処します。

Web プロキシは、外部 DLP ポリシーを使用して、要求本文にデータが含まれる HTTP 要求および復号化された HTTPS 要求を評価し、外部 DLP サーバに送信してスキャンします。

[Web セキュリティ マネージャ（Web Security Manager）] > [外部データ消失防止（External Data Loss Prevention）] ページで、外部 DLP ポリシー グループを設定します。外部 DLP ポリシー グループの詳細については、「データ セキュリティと外部 DLP ポリシー」（P.13-1）を参照してください。

Outbound Malware Scanning ポリシー

Outbound Malware Scanning ポリシーは、悪意のあるデータを含むデータの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。これらは、「悪意のあるデータのアップロードをブロックしますか。」という質問に対処します。

Web プロキシは、Outbound Malware Scanning ポリシーを使用して、要求本文にデータを含む HTTP 要求および復号化 HTTPS 要求のマルウェアをスキャンします。

[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）] ページで、Outbound Malware Scanning ポリシー グループを設定します。Outbound Malware Scanning ポリシー グループの詳細については、「Outbound Malware Scanning」（P.12-1）を参照してください。

SaaS アプリケーション認証ポリシー

SaaS アプリケーション認証ポリシーは、サービス（SaaS）アプリケーションとしてのソフトウェアへのアクセスをユーザに許可するかどうかを決定します。これらは、「このユーザの SaaS アプリケーションへのアクセスを許可しますか。」という質問に対処します。

SaaS アプリケーション認証ポリシーは、アプライアンスが WebEx などの設定済み SaaS アプリケーションへのユーザのアクセスを制御する方法を決定します。Cisco SaaS アクセス コントロールをイネーブルにすると、ユーザはネットワーク認証のユーザ クレデンシャルを使用して、設定済み SaaS アプリケーションにログインします。つまり、ユーザがすべての SaaS アプリケーションおよびネットワーク アクセスに同じユーザ名とパスワードを使用することを意味します。

[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、SaaS アプリケーション認証ポリシー グループを設定します。SaaS アプリケーション認証ポリシー グループの詳細については、「SaaS アプリケーションへのアクセスの制御」（P.15-1）を参照してください。

ポリシー グループの使用

ポリシー グループは、ユーザの特定のカテゴリにアクセプタブル ユース ポリシーを適用する管理者が定義した設定です。ポリシー グループを作成すると、各グループの制御設定を定義できます。

適切なアクセス コントロールを実行するために必要な数だけユーザ定義のポリシー グループを作成できます。Web セキュリティ アプライアンスは、ポリシー テーブルにポリシー グループをまとめて表示します。

すべてのポリシーには、どのユーザ定義ポリシー グループも適用されない場合にトランザクションに適用されるデフォルトのグローバル ポリシー グループが含まれています。グローバル ポリシー グループは、別のポリシーによってカバーされない Web トランザクションに適用するデフォルトの設定とルールを保持します。このグループはポリシー テーブルの末尾の行に表示され、一致が見つからない場合、Web プロキシはそのルールの末尾の行を適用します。

ポリシー グループの作成

宛先サイトの URL カテゴリのクライアント サブネットなど、複数の条件の組み合わせに基づいてポリシー 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。複数の条件を定義した場合、クライアント要求は、ポリシー グループと一致するために、すべての条件を満たす必要があります。

ポリシー グループの設定に使用するオプションにより、グローバル ポリシー設定の例外を指定し、ユーザ グループに対するサービスへのアクセスを制御できます。

さまざまなポリシー グループの作成方法の詳細については、次の項を参照してください。

- 「ID の作成」（P.8-18）
- 「アクセス ポリシーの作成」（P.9-5）
- 「復号ポリシーの作成」（P.11-17）
- 「ルーティング ポリシーの作成」（P.10-5）
- 「データ セキュリティおよび外部 DLP ポリシーの作成」（P.13-6）

ポリシー テーブルの使用

ポリシー テーブルには、ポリシー グループの順序付きリストと各フィルタリング コンポーネントに設定する設定が含まれています。行にポリシー グループ、カラムに制御設定が表示されます。定義できる制御設定は、ポリシー タイプによって異なります。

図 7-1（P.7-6）は、アクセス ポリシー テーブルを示します。

図 7-1　　アクセス ポリシー テーブル

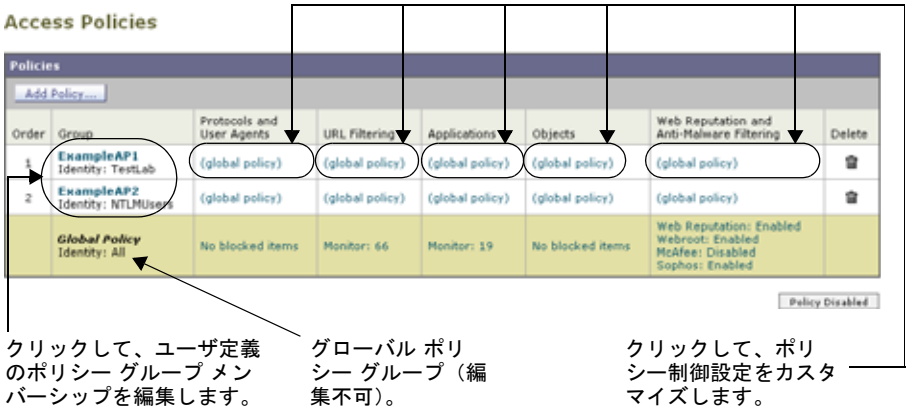
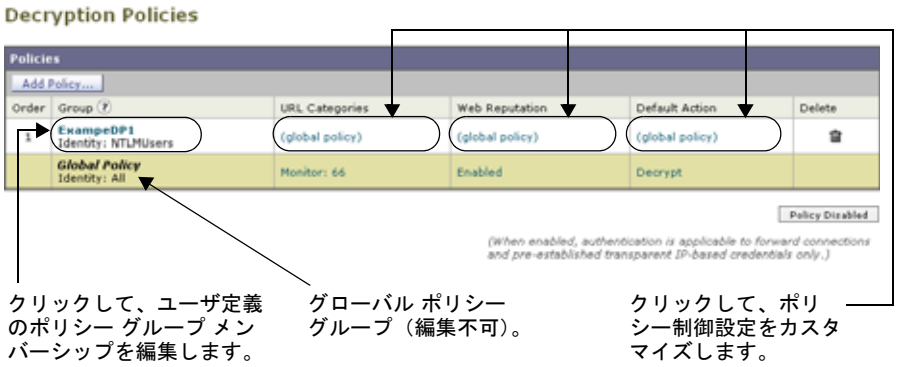


図 7-2 は、復号化ポリシー テーブルを示します。

図 7-2　　復号化ポリシー テーブル



作成するポリシー グループは、ポリシー テーブルに新しい行として追加されます。新しいポリシー グループは、上書きされるまで各制御設定のグローバル ポリシー設定を継承しています。ポリシー グループを編集するには、各行のリンクをクリックします。

グループ ポリシーを作成または設定する際に、次のコンポーネントを定義します。

- **ポリシー グループ メンバーシップ。**ポリシー グループに属するユーザをグループ化する方法を定義します。ユーザ定義ポリシー グループの場合、クライアントの IP アドレス、認証グループまたはユーザ名、あるいは、URL カテゴリなどのさまざまなプロパティによってグループ化できます。ポリシーに定義できるプロパティは、ポリシー タイプによって異なります。

  ポリシー グループ名をクリックして、クライアント IP アドレスおよび認証要件などのグループ メンバーシップの要件を編集します。メンバーシップの要件を設定できるページが表示されます。

（注）　グローバル ポリシーの場合、グローバル ID グループのメンバーシップの要件だけを定義できます。グローバル アクセス、復号化、またはルーティング グループの要件は定義できません。グローバル アクセス、復号化、およびルーティング グループは、常にすべての ID に一致します。

ポリシー グループ メンバーシップの詳細については、「ポリシー グループ メンバーシップ」（P.7-7）を参照してください。

- **ポリシー グループの制御設定。**グループ内のユーザがインターネットを使用できる方法を定義します。定義できる制御設定はポリシー タイプによって異なります。たとえば、ルーティング ポリシーの場合、コンテンツを取得するプロキシ グループを定義し、アクセス ポリシーの場合、Web レピュテーション、アンチマルウェア スキャンなどの Web セキュリティ アプライアンス機能を使用して、クライアント要求を許可するかどうかを決定できます。

  設定する制御設定の下にあるグループ ポリシー行のリンク（[URL カテゴリ（URL Categories）] または [ルーティング先（Routing Destination）] など）をクリックします。テーブル内のリンクをクリックすると、そのポリシー グループを設定できるページが表示されます。

  各ポリシー タイプの制御設定の構成の詳細については、次の項を参照してください。

  - 「HTTP およびネイティブ FTP トラフィックの制御」（P.9-8）
  - 「HTTPS トラフィックの制御」（P.11-20）
  - 「ルーティング ポリシーの作成」（P.10-5）
  - 「Cisco IronPort データ セキュリティ ポリシーを使用したアップロード要求の制御」（P.13-9）
  - 「外部 DLP ポリシーを使用したアップロード要求の制御」（P.13-16）

ポリシー グループ メンバーシップ

すべてのポリシー グループがそれを適用するトランザクションを定義します。クライアントがサーバに要求を送信するときに、Web プロキシは、要求を受信し、評価し、どのポリシー グループに属しているかを判定します。Web プロキシは、クライアント要求のポリシー グループのメンバーシップに基づいて、設定されたポリシー制御設定をクライアント要求に適用します。

トランザクションは、イネーブルになっている各ポリシー タイプのポリシー グループに属します。ポリシー タイプがユーザ定義のポリシー グループではない場合、各トランザクションはそのポリシー タイプのグローバル ポリシー グループに属します。

ルーティング ポリシー、復号化ポリシー、アクセス ポリシー、データ セキュリティ ポリシー、および外部 DLP ポリシーのポリシー グループ メンバーシップは ID と任意の追加基準に基づいています。これは *Web プロキシが他のポリシー タイプを評価する前に ID グループを評価する*ことを意味します。Web セキュリティ アプライアンス では、ID レベルまたは非 ID ポリシー レベルのいずれかで、いくつかのメンバーシップの基準を定義できます。詳細については、「ポリシー グループ メンバーシップのルールとガイドライン」（P.7-9）を参照してください。

サブネット 10.1.1.0/24 で ID を定義し、その ID を使用してアクセス ポリシーを作成するとします。アクセス ポリシーのメンバーシップは、デフォルトで ID に指定されたすべての IP アドレスに適用されます。次に、アドレス 10.1.1.0-15 など、ID で定義されたアドレスのサブセットに適用するように、アクセス ポリシーのメンバーシップの設定を選択できます。

各ポリシー タイプのメンバーシップの定義に関する詳細については、次の項を参照してください。

- 「ID グループ メンバーシップの評価」（P.8-4）
- 「アクセス ポリシー グループ メンバーシップの評価」（P.9-4）

- 「復号ポリシー グループ メンバーシップの評価」（P.11-15）
- 「ルーティング ポリシー グループのメンバーシップの評価」（P.10-4）
- 「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」（P.13-5）

ユーザの認証とユーザの許可

Web セキュリティ アプライアンスは、ユーザを認証する場所とユーザを許可する場所を分離します。

*認証*は、Web プロキシがユーザを安全に識別するメカニズムです。これは次の質問に答えます。

- ユーザは誰ですか。
- ユーザは本当に自分がユーザであると申し立てている人ですか。

*許可*は、Web プロキシがユーザの Web サイトへのアクセス レベルを決定するメカニズムです。これは次の質問に答えます。

- このユーザに、この Web サイトの閲覧を許可しますか。
- このユーザに、接続を復号化することなく、この HTTPS サーバへの接続を許可しますか。
- このユーザに、Web サーバへの直接接続を許可しますか、あるいはまず他のプロキシ サーバへの接続を要求しますか。
- このユーザに、このデータのアップロードを許可しますか。

Web プロキシは、ユーザが誰かを認証した*後に*、ユーザのインターネット リソースへのアクセスを許可できます。Web プロキシは、ID グループを評価する時点でユーザを認証し、他のすべてのポリシー グループのタイプを評価する時点でユーザを許可します。これは、ID グループは要求しているクライアントを示しますが、そのクライアントが要求を行うことを許可されているかどうかは示していないことを意味します。

認証と許可を分離することにより、ユーザのグループを識別する単一の ID グループを作成し、ID 内のグループのユーザのサブセットに異なるアクセス レベルを許可する複数のポリシー グループを作成できます。

たとえば、認証シーケンスですべてのユーザをカバーする 1 つの ID グループを作成できます。その後、シーケンスの認証レルムごとにアクセス ポリシー グループを作成できます。この ID を使用して、ID 内のすべてのユーザに対して同じアクセス レベルを持つ 1 つの復号化ポリシーを作成できます。

認証および許可に失敗した場合の操作

認証または許可に失敗したユーザに対して、Web にアクセスする別の機会を与えることができます。Web セキュリティ アプライアンスの設定方法は、失敗の内容によって異なります。

- **認証。**認証に失敗した場合、ユーザにゲスト アクセスを許可できます。認証は次の状況で失敗する可能性があります。
  - 新規採用者が電子メールでクレデンシャルを提供されましたが、それらがまだ認証サーバに登録されていない場合。
  - ビジターがオフィスに来場し、制限されたインターネット アクセスを許可する必要があるが、ビジターが企業のユーザ ディレクトリに存在しない場合。

  ゲスト アクセスの設定の詳細については、「認証に失敗したユーザへのゲスト アクセスの許可」（P.8-10）を参照してください。

- **許可。**ユーザは正しく認証されていると思われますが、該当するアクセス ポリシーによって Web へのアクセスが許可されません。この場合、ユーザに追加の特権クレデンシャルを使用する再認証を許可することもできます。これを行うには、「Enable Re-Authentication Prompt If End User Blocked by URL Category or User Session Restriction」グローバル認証設定をイネーブルにします。詳細については、「ユーザに対する再認証の許可」（P.20-27）を参照してください。

すべての ID の使用

設定済み ID グループとして [すべての ID（All Identities）] を指定するポリシー グループを作成できます。定義上、すべての要求は、成功してユーザ定義またはグローバル ID が割り当てられるか、認証に失敗して終了するか（また、認証に失敗したユーザにはゲスト アクセスは提供されない）のいずれかであるため、[すべての ID（All Identities）] は有効なすべてのクライアント要求に適用されます。

[すべての ID（All Identities）] を使用するポリシー グループを作成する場合、少なくとも 1 つの拡張オプションを設定し、ポリシー グループとグローバル ポリシー グループを区別する必要があります。

通常、ポリシーに [すべての ID（All Identities）] を使用すると同時に、特定のユーザ エージェントや宛先など、拡張オプションを設定します（カスタム URL カテゴリを使用）。これにより、特定のケースを例外扱いとする複数のルールを作成するのではなく、特定のケースを例外扱いとする単一のルールを作成できます。たとえば、メンバーシップをすべてのイントラネット ページの [すべての ID（All Identities）] とカスタム URL カテゴリに適用するアクセス ポリシー グループを作成できます。その後、アクセス ポリシーの制御設定を設定して、アンチマルウェア フィルタリングと Web レピュテーション スコアをディセーブルにできます。

ポリシー グループ メンバーシップのルールとガイドライン

ポリシー グループのメンバーシップを定義する場合は、次のルールとガイドラインを考慮してください。

- Web プロキシは、他のポリシー タイプを評価する前に ID グループを評価します。
- ID グループで定義されたサブネットのメンバーシップ基準は、ID グループを使用してポリシー グループをさらに絞り込むことができます。
- ID グループで定義された拡張メンバーシップ基準（プロキシ ポート、URL カテゴリ、およびユーザ エージェント）は、ID グループを使用してポリシー グループに定義できません。
- ID グループはできるだけ幅広く定義します。次に、他のポリシー タイプの ID グループを使用し、必要に応じてさらにメンバーシップを絞り込むことができます。
- 少数の、より一般的な復号化およびルーティング ポリシーをできるだけ多く定義します。
- 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。他の目的で、アクセス ポリシー、復号化 ポリシー、ルーティング ポリシー、データ セキュリティ ポリシー、または外部 DLP ポリシー グループの URL カテゴリによってメンバーシップを定義します。ほとんどの場合、これによりパフォーマンスを向上させることができます。

時間ベースのポリシーの使用

Web セキュリティ アプライアンスには、業務時間などの時間範囲を指定し、これらの時間範囲を使用して Web へのアクセスを定義するなど、時間ベースのポリシーを作成する方法が用意されています。時間範囲に基づいてポリシー グループのメンバーシップを定義し、時間範囲に基づいて URL フィルタリングのアクションを指定できます。

次のタスクを実行するために時間範囲を使用する場合があります。

- 業務時間内にストリーミング メディアなどの高帯域幅のサイトへのアクセスをブロックしたり、ゲームなどの職務に関係のないサイトへのアクセスをブロックしたりできます。
- 他のプロキシが修理されている深夜過ぎに、トランザクションを特定の外部プロキシにルーティングできます。
- 大規模なファイルを週末にダウンロードできます。

[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 Ranges）] ページで、時間範囲を定義します。「業務時間」や「週末シフト」などの時間範囲を作成できます。その後、次の場合に時間範囲を使用できます。

- ルーティング、アクセス、または復号化ポリシーのポリシー グループ メンバーシップ。
- アクセス ポリシーの URL フィルタリングの設定。

時間範囲を定義するときは、曜日と時刻を指定できます。トランザクションが任意の日の指定された時刻内に発生する場合、トランザクションは指定された時間範囲に一致します。1 つの時間範囲内に複数の日付と時刻の組み合わせを定義できます。たとえば、月曜日から金曜日の 08:00 ～ 17:00、または土曜日の 09:00 ～ 13:00 に発生するトランザクションに適用する時間範囲を定義できます。

ポリシーおよび URL フィルタリング アクションは、定義された時間範囲内または定義された時間範囲外に定義できます。

（注） 時間ベースのポリシー グループのメンバーシップは、ルーティング、アクセス、および復号化ポリシーのみに定義でき、ID には定義できないため、ユーザを認証する必要がある時点を定義する時間ベースのポリシーは作成できません。認証要件は ID グループで定義されますが、時間ベースのポリシーは、他のポリシー グループ タイプで定義されます。（バグ #41723）

時間範囲の作成

ステップ 1　[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 Ranges）] に移動します。

ステップ 2　[時間範囲の追加（Add Time Range）] をクリックします。

ステップ 3　[時間範囲名（Time Range Name）] フィールドに、一意のわかりやすい名前を入力します。

ステップ 4　[タイム ゾーン（Time Zone）] セクションで、Web セキュリティ アプライアンス上のタイム ゾーン設定を使用するか、または別のタイム ゾーンを設定するかを選択します。

ステップ 5　[時間値（Time Values）] セクションで、この時間範囲に含める曜日と時刻を指定する少なくとも 1 つの行を定義します。

a. [曜日（Day of the Week）] セクションで、少なくとも 1 つの日を選択します。

b. [時間（Time of Day）] セクションで、[終日（All Day）] を選択するか、または [から（From）] フィールドと [まで（To）] フィールドを使用して一日の時間範囲を入力します。

各時間範囲は開始時刻が含まれ、終了時刻は除外されます。たとえば、8:00 ～ 17:00 を入力する場合、8:00:00 ～ 16:59:59 に一致しますが 17:00: 00 には一致しません。

深夜は、開始時刻が 00:00、終了時刻が 24:00 として指定する必要があります。

（注）　トランザクションは、[時間値（Time Values）] セクションの行に一致するように指定された日付*および*時刻に発生する必要があります。これは [曜日（Day of Week）] と [時刻（Time of Day）] の値が 1 つの行内で相互に「AND」関係にあることを意味します。

ステップ 6　任意で、[行を追加（Add Row）] をクリックして、時間値を追加する行を作成できます。

（注）　時間範囲に複数の時間値の行が含まれている場合、トランザクションは時間範囲に一致する任意の定義された時間値内に発生する可能性があります。これは、1 つの時間範囲の複数の時間値の行が相互に「OR」関係にあることを意味します。

ステップ 7　変更を送信し、保存します。

ユーザ エージェント ベースのポリシーの使用

Web セキュリティ アプライアンスは、Web ブラウザなどのクライアント アプリケーション（ユーザ エージェント）による、クライアント要求を行なうための Web へのアクセスを定義するポリシーを作成できます。ユーザ エージェントに基づいてポリシー グループのメンバーシップを定義し、ユーザ エージェントに基づいて制御設定を指定できます。

次のタスクを実行するためにユーザ エージェントを指定する場合があります。

- 特定のユーザ エージェントを認証から除外できます。認証クレデンシャルの入力をユーザに要求する処理を行えないクライアント アプリケーションに、この操作を実行する場合があります。実行方法の詳細については、「ユーザ エージェントの認証の免除」（P.7-12）を参照してください。
- 定義する特定のユーザ エージェントからのアクセスをブロックできます。

次の場所でユーザ エージェントを設定できます。

- ID を含むすべてのポリシー タイプのポリシー グループのメンバーシップ。
- アクセス ポリシーのアプリケーション制御設定。

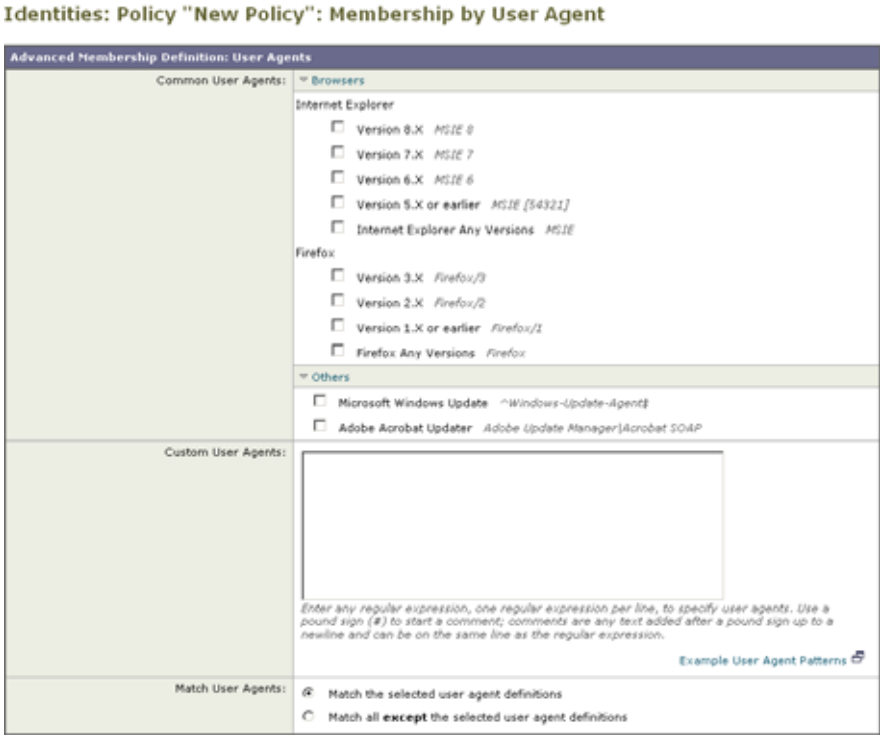
（注）　アプライアンスがトランスペアレント モードで展開される場合、ユーザ エージェント情報は復号化ポリシーに使用できません。

ポリシー グループ メンバーシップのユーザ エージェントの設定

任意のポリシー タイプのポリシー グループのメンバーシップを定義する場合、[詳細（Advanced）] セクションを展開して、ユーザ エージェントなどの追加の基準によってメンバーシップを定義できます。[ユーザ エージェント（User Agent）] リンクをクリックすると、ユーザ エージェントによってメンバーシップを定義できる [ユーザ エージェントによるメンバーシップ（Membership by User Agent）] ページが表示されます。

図 7-3（P.7-12）は、ID ポリシー グループの [ユーザ エージェントによるメンバーシップ（Membership by User Agent）] ページを示します。

図 7-3　ユーザ エージェントによるポリシー グループ メンバーシップの定義



このページで、必要な数だけユーザ エージェントを選択できます。Web インターフェイスには、チェックボックスを使用して選択できるより一般的なユーザ エージェントの一部が含まれています。必要なユーザ エージェントを定義する正規表現を入力することもできます。

[共通ユーザ エージェント（Common User Agents）] で選択するユーザ エージェントの場合、AsyncOS for Web はユーザ エージェントを定義するために正規表現を作成します。ただし、ブラウザ タイプごとに [すべてのバージョン（Any Versions）] オプションを選択する場合、AsyncOS for Web は、各バージョンの式の代わりに、そのブラウザのすべてのバージョンを表す単一の正規表現を作成します。複数の式の代わりに単一の正規表現を作成するとパフォーマンスが向上します。

たとえば、Firefox の [バージョン 2.x（Version 2.X）] および [バージョン 1.x もしくはそれ以前（Version 1.X or earlier）] を選択する場合、AsyncOS for Web は次の正規表現を使用します。

```
Firefox/2
Firefox/1
```

ただし、[すべての Firefox のバージョン（Firefox Any Versions）] を選択する場合、AsyncOS は次の正規表現を使用します。

```
Firefox
```

また、定義するユーザ エージェントに一致するか、または定義したユーザ エージェント以外の他のすべてのユーザ エージェントに一致するポリシー グループ メンバーシップを設定できます。

ユーザ エージェントの認証の免除

ステップ 1　免除するユーザ エージェントに基づくメンバーシップを持つ ID ポリシー グループを作成します。

（注）　ID ポリシー グループに認証を要求しないでください。

ID の作成に関する詳細については、「ID の作成」（P.8-18）を参照してください。

ステップ 2　認証を必要とする他のすべての ID ポリシー グループの上に ID ポリシー グループを配置します。

ステップ 3　変更を送信し、保存します。

ポリシーのトレース

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は、特定のクライアント要求をトレースし、Web プロキシが要求を処理する方法を詳細を示すツールが含まれています。Web プロキシは、コミット済みのすべてアクセス、復号化、Cisco IronPort データ セキュリティ ポリシー、Outbound Malware Scanning に対する要求を評価し、Web レピュテーション スコアなどの他の属性を計算します。

ポリシー トレース ツールにより、管理者はエンド ユーザが Web プロキシの動作に関する質問を行うときにトラブルシューティングできます。このツールは、エンド ユーザによって行われたかのようにクライアント要求をシミュレートし、Web プロキシの動作を説明します。特に、Web セキュリティ アプライアンスで使用可能な多くの拡張機能を組み合わせた場合、強力なトラブルシューティングまたはデバッグ ツールとなります。

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。

デフォルトで、Web プロキシは HTTP GET 要求をシミュレートします。ただし、[要求の詳細（Request Details）] セクションでファイルのアップロードを指定する場合、Web プロキシは HTTP POST 要求をシミュレートします。

（注）　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でも、ポリシー トレース ツールは明示的に要求を行います。

[システム管理（System Administration）] > [ポリシー トレース（Policy Trace）] ページで、ポリシーをトレースできます。

ステップ 1　[システム管理（System Administration）] > [ポリシー トレース（Policy Trace）] ページに移動します。

ステップ 2　[URL] フィールドに、シミュレートするクライアント要求の URL を入力します。

ステップ 3　任意で、[クライアント IP アドレス（Client IP Address）] フィールドに、シミュレートするマシンの IP アドレスを入力します。

（注）　IP アドレスを指定しない場合、AsyncOS は localhost を使用します。

ステップ 4　任意で、[ユーザ（User）] 領域に次の認証要件を入力して、認証ユーザをシミュレートできます。

- **[ユーザ名（User Name）]。**認証ユーザのユーザ名を入力します。
- **[認証レルム（Authentication Realm）]。**認証レルムを選択します。

（注）　ここで入力するユーザに対して認証が機能するためには、ユーザはあらかじめ Web セキュリティ アプライアンスを介して正常に認証されている必要があります。

ステップ 5　任意で、[詳細（Advanced）] セクションを展開して、トレースするより具体的なユーザ要求をシミュレートするために追加設定を設定できます。

高度な設定は、シミュレートされるトランザクション要求の詳細と上書きされるトランザクション応答の詳細に分割されます。

ステップ 6　必要に応じて、シミュレートするトランザクション要求情報を設定します。表 7-1 は、ユーザが設定できる要求側の高度な設定を示しています。

表 7-1　要求のポリシー トレースの高度な設定

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（Time of Request）	要求でシミュレートする曜日と時間帯を指定します。
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（Object Size）	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 Type）	MIME タイプを入力します。
アンチマルウェア スキャンの判定（Anti-malware Scanning Verdicts）	Webroot、McAfee、または Sophos スキャンの判定を上書きするかどうかを選択します。

ステップ 7　任意で、表 7-2 の参照情報を使用して、トランザクション応答の上書きを設定します。低 Web レピュテーション スコアなど、別のレスポンス値がトランザクションに割り当てられたポリシーにどのように影響するかをシミュレートするために、トランザクション応答の詳細を上書きする場合があります。

表 7-2　応答上書きのポリシー トレースの高度な設定

設定	説明
URL カテゴリ（URL Category）	トランザクション応答の URL カテゴリを上書きするかどうかを選択します。
アプリケーション（Application）	Application Visibility and Control エンジンが検出可能なアプリケーションを選択します。
オブジェクトのサイズ（Object Size）	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 Type）	MIME タイプを入力します。

表 7-2　応答上書きのポリシー トレースの高度な設定 （続き）

設定	説明
Web レピュテーション スコア（Web Reputation Score）	Web レピュテーション スコア（-10.0 ～ 10.0）を入力します。
アンチマルウェア スキャンの判定（Anti-malware Scanning Verdicts）	Webroot、McAfee、または Sophos スキャンの判定を上書きするかどうかを選択します。

ステップ 8　[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 ツールは [結果（Results）] 領域に結果を表示します。

8
ID

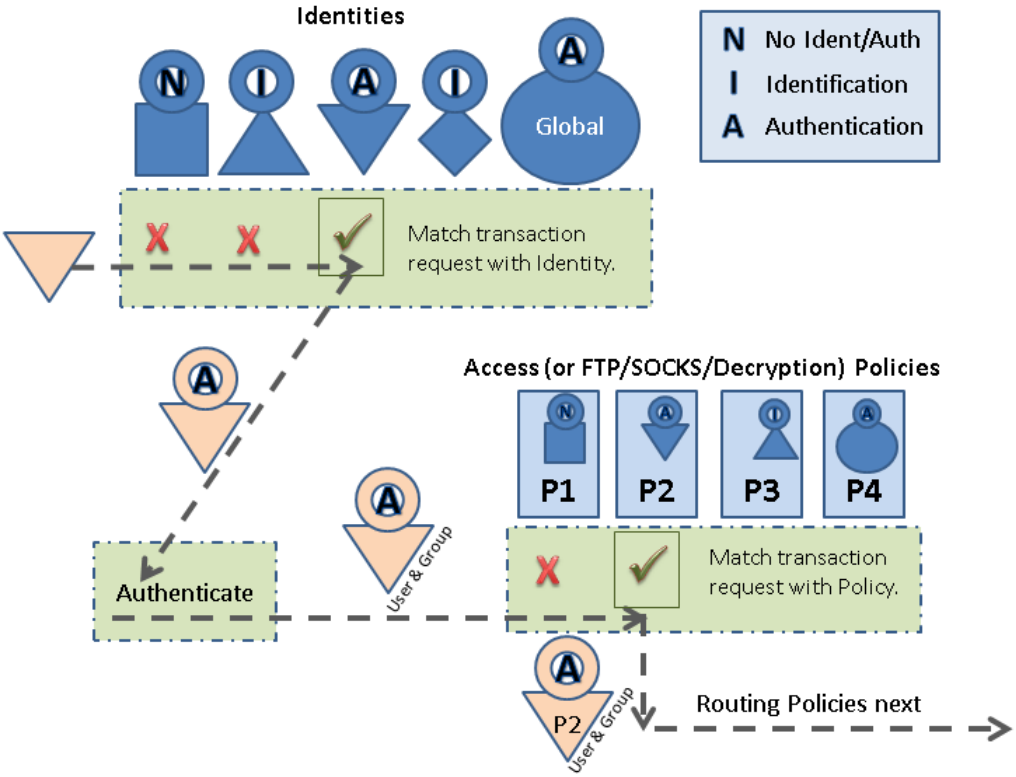
ID の概要

ID は次の目的で使用されます。

- ポリシーのアプリケーションに対するトランザクション要求をグループ化します。
- ID グループのメンバーの識別または認証の必要性を明示します。

AsyncOS は、処理するすべてのトランザクションに ID を割り当てます。グローバル ID は、ユーザ定義 ID のメンバーシップとして不適格なすべてのトランザクションに適用されます。ユーザが作成する ID は、アクセス ポリシー（SOCKS ポリシーを含む）および復号化ポリシーの設定で使用することもできます。

下図に AsyncOS がトランザクションを処理する例を示します。



これらのトランザクションの特性は、以下の ID グループの定義に使用できます。

- サブネット：トランザクション要求を行うクライアントのサブネット。
- プロトコル：要求されたトランザクションが使用するプロトコル。
- ポート：クライアントが要求を行うポート。

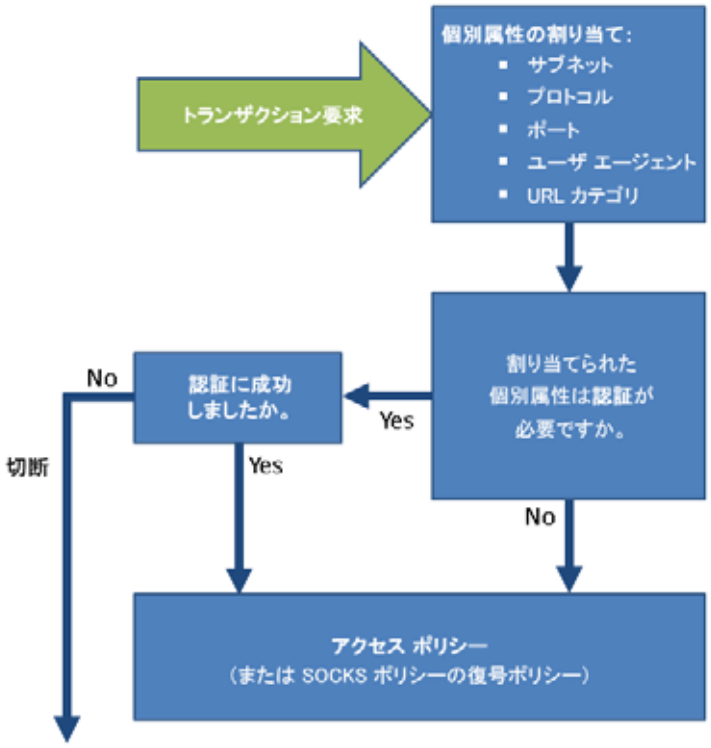
（注） アプライアンスが明示的に転送モードで展開されている場合、またはクライアントがアプライアンスに明示的に要求を転送する場合、ポート別の ID の定義は最もよく機能します。クライアント要求が透過的にアプライアンスにリダイレクトされる場合、ポート別の ID の定義は要求の一部を誤って拒否することがあります。

- ユーザ エージェント：Internet Explorer または Firefox など、要求を行うユーザ エージェント（クライアント アプリケーション）。
- URL カテゴリ：クライアントによって要求された URL に関連付けられた URL カテゴリ。

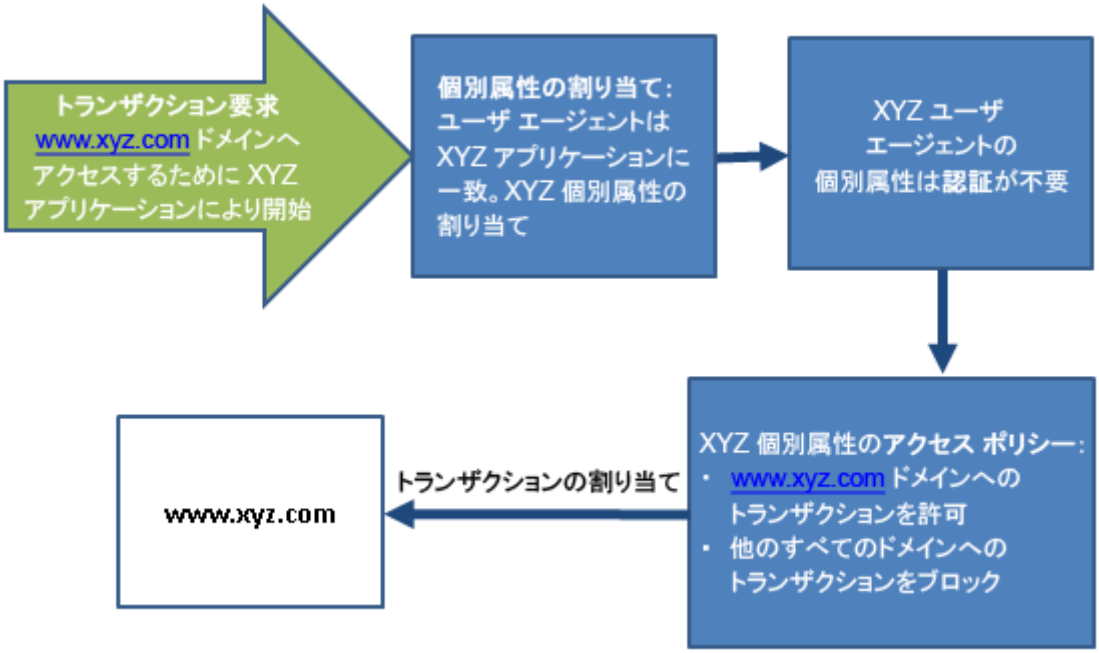
次に、例を示します。

- ID は、認証をサポートしないユーザ エージェントから出される要求に使用できます。
- ID は、特定のサブネットのクライアントによって開始されたソーシャル ネットワーキング サイトのトランザクション要求に使用できます。

下図に、ID フローの例を示します。



アクセス ポリシー（SOCKS ポリシーを含む）および復号化ポリシーのメンバーシップの要件として作成する ID を使用できます。たとえば、エンド ユーザが XYZ ドメインでヘルプ ファイルにアクセスし、認証を必要としないかまたはサポートしていない XYZ アプリケーションを使用することがわかっている場合、XYZ アプリケーション（ユーザ エージェント）用の ID を作成することがあります。XYZ の ID は認証が必要ありません。また、グループ メンバーとして XYZ ID を持つトランザクションを定義し、XYZ ドメイン内の URL にのみアクセスできるアクセス ポリシーを作成できます。



次のタイプのユーザまたはマシンをグループ化することがあります。

- **テスト ラボのマシン アドレスのグループ。**この ID を持つルーティング ポリシーを作成できるので、これらのマシンからの要求は宛先サーバから直接取得されます。
- **すべてのレルムの認証シーケンスに基づくすべての認証済みユーザ。**この ID を使用して、単一のアクセス ポリシーを作成したり、認証レルムごとに異なるアクセス ポリシーを作成し、各レルムのユーザに異なる制御設定を設定したりできます。
- **特定のプロキシ ポート上の Web セキュリティ アプライアンスにアクセスするユーザ。**特定のプロキシ ポート上のアプライアンスへの明示的な接続の要求に対して、特定の外部プロキシからコンテンツを取得するこの ID を使用して、ルーティング ポリシーを作成できます。
- **ユーザ定義の URL カテゴリ内の Web サイトにアクセスしようとするすべてのサブネットは認証が必要ありません。**この ID を使用して、認証から特定の宛先への要求を免除するアクセス ポリシーを作成できます。Windows Update サーバに対して、この処理を実行することがあります。

[Web セキュリティ マネージャ（Web Security Manager）] > [アイデンティティ（Identities）] ページで ID を定義します。ID の作成に関する詳細については、「ID の作成」（P.8-18）を参照してください。

ID グループ メンバーシップの評価

クライアントがサーバに要求を送信するときに、Web プロキシは、要求を受信し、評価し、どの ID グループに属しているかを判定します。

クライアント要求が一致する ID グループを判定するために、Web プロキシは、きわめて特殊なプロセスを実行して ID グループ メンバーシップの基準と照合します。このプロセスでは、グループ メンバーシップの次の要素が考慮されます。

- **サブネット。**クライアント サブネットは、ポリシー グループのサブネットのリストに一致する必要があります。
- **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 のいずれか。
- **ポート。**要求のプロキシ ポートは、ポートの ID グループの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。

  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 ID グループのメンバーシップを定義することがあります。
- **ユーザ エージェント。**要求を行うユーザ エージェントは、ユーザ エージェントの ID グループの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）。認証を処理できないユーザ エージェントをユーザ エージェント別にグループ化し、認証を必要としない ID を作成することがあります。
- **URL カテゴリ。**要求 URL の URL カテゴリは、URL カテゴリの ID グループの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）。URL カテゴリに基づいて別の認証グループを作成し、Web サイトの分類に応じてユーザに適用する場合、宛先 URL カテゴリ別にグループ化することがあります。
- **認証要件** ID グループが認証を必要とする場合、クライアントの認証クレデンシャルは、ID グループの認証要件に一致する必要があります。ID グループにおける認証の動作の詳細については、「認証が ID グループに影響を与える仕組みについて」（P.8-5）を参照してください。

この項では、アプライアンスがクライアント要求を ID グループと照合する方法の概要を説明します。アプライアンスがクライアント要求を正確に照合する方法の詳細については、「クライアント要求と ID グループとの照合」（P.8-8）を参照してください。

Web プロキシは、ID ポリシー テーブルの各 ID グループを順番に読み取ります。次に、クライアント要求のステータスを最初の ID グループのメンバーシップの基準と比較します。一致する場合、Web プロキシは ID グループをトランザクションに割り当てます。

一致しない場合、Web プロキシは、クライアント要求を次の ID グループと比較します。クライアント要求がユーザ定義の ID グループに一致するまで、またはユーザ定義の ID グループに一致しない場合、グローバル ID ポリシーに一致するまで、このプロセスを続行します。Web プロキシがクライアント要求を ID グループまたはグローバル ID ポリシーと照合すると、ID グループをトランザクションに割り当てます。

比較プロセス中どの時点でもユーザが認証に失敗した場合、Web プロキシは要求を終了します。ID グループにおける認証の動作の詳細については、「認証が ID グループに影響を与える仕組みについて」（P.8-5）を参照してください。

Web プロキシがクライアント要求に ID を割り当てた後で、その要求をその他のポリシー グループ タイプに対して評価します。詳細については、以下の項を参照してください。

- 「アクセス ポリシー グループ メンバーシップの評価」（P.9-4）
- 「復号ポリシー グループ メンバーシップの評価」（P.11-15）
- 「ルーティング ポリシー グループのメンバーシップの評価」（P.10-4）
- 「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」（P.13-5）

認証が ID グループに影響を与える仕組みについて

ID グループの認証要件を定義する際に、ID グループに適用する認証レルムまたはシーケンスを選択できます。

（注）　非 ID ポリシー グループの ID を使用する場合、承認されたユーザを指定できます。

ID グループの作成および順序付けの際に、次のルールとガイドラインを考慮してください。

- **ID グループの順序。**認証を必要としないすべての ID グループが認証を必要とする ID グループより上位にくる必要があります。
- **クッキー ベースの認証。**アプライアンスがクッキー ベースの認証サロゲートを使用するように設定されている場合、アプライアンスは HTTP 要求を介した HTTPS および FTP のクライアントからクッキー情報を取得しません。このため、クッキーからユーザ名を取得できません。HTTP 要求を介した HTTPS および FTP が ID グループに照合される仕組みは、他の要因によって異なります。詳細については、「認証が HTTP 要求を介した HTTPS および FTP に影響を与える仕組みについて」（P.8-6）を参照してください。
- **ID の一意性。**ID グループ メンバーシップの要件が ID グループごとに一意であることを確認します。2 つの ID グループで完全に同一のメンバーシップが必要な場合、クライアント要求が下位の ID グループに一致することはありません。非 ID ポリシーがより下位の ID グループを使用する場合、クライアント要求がそのポリシーに一致することはありません。
- **グローバル ID ポリシー。**デフォルトで、認証レルムを作成する場合、グローバル ID ポリシーは認証が必要ありません。グローバル ID ポリシーの認証が必要になるようにする場合は、認証レルム、認証シーケンス、または全レルム シーケンスをグローバル ID ポリシーに割り当てます。

Web プロキシが、クライアント要求を異なる ID ポリシー テーブルの ID グループと照合する方法を示すいくつかの例については、「ID ポリシー テーブルの例」（P.8-24）を参照してください。

認証が HTTP 要求を介した HTTPS および FTP に影響を与える仕組みについて

Web プロキシが HTTP 要求を介した HTTPS および FTP を ID と照合する方法は、要求のタイプ（Web プロキシに明示的に転送されたか、透過的にリダイレクトされたかのいずれか）および認証サロゲートのタイプによって異なります。

- **認証サロゲートなし。**Web プロキシは、HTTP 要求を照合する場合と同じ方法で、HTTP 要求を介した HTTPS および FTP を ID グループと照合します。この操作が行われる仕組みを示す略図については、図 8-1（P.8-9）を参照してください。
- **IP ベースの認証サロゲートおよび明示的要求。**Web プロキシは、HTTP 要求を照合する場合と同じ方法で、HTTP 要求を介した HTTPS および FTP を ID グループと照合します。この操作が行われる仕組みを示す略図については、図 8-1（P.8-9）を参照してください。
- **IP ベースの認証サロゲートおよび透過的要求。**Web プロキシは、HTTP 要求を照合する場合と同じ方法で、HTTP 要求を介した FTP を ID グループと照合します。ただし、HTTPS 要求の場合、以前の HTTP 要求から入手できる認証情報を持つクライアントから HTTPS 要求が送信されたかどうかによって動作が異なります。
  - **以前の HTTP 要求から入手できる情報。**Web プロキシは、HTTP 要求を照合する場合と同じ方法で、HTTPS 要求を ID グループと照合します。HTTPS 要求は IP アドレスに関連付けられた ID として扱われます。
  - **以前の HTTP 要求から入手できる情報なし。**Web プロキシにクライアントのクレデンシャル情報が存在しない場合、HTTPS プロキシの設定方法に応じて、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。

  この操作が行われる仕組みを示す略図については、図 8-1（P.8-9）を参照してください。
- **クッキー ベースの認証サロゲートおよび透過的要求。**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。この場合、HTTP 要求を介した HTTPS および FTP は他のメンバーシップの基準に従って ID グループと照合しますが、*ID グループで認証が必要な場合*でも、Web プロキシがクライアントに認証を要求することはありません。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、非認証要求が非 ID ポリシー グループに対して評価されたときに、「すべての ID」を指定し、「すべてのユーザ」を適用する非 ID グループに一致します。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。この操作が行われる仕組みを示す略図については、図 8-2（P.8-10）を参照してください。
- **クッキー ベースの認証サロゲートおよび明示的要求。**クレデンシャルの暗号化がイネーブルかどうかに応じて、動作が異なります。
  - **クレデンシャルの暗号化がイネーブルの場合。**動作は、前述したとおり、透過的要求によるクッキー ベース認証と同じです。「イネーブルのクレデンシャルの暗号化による HTTPS サイトと FTP サイトへのアクセス」（P.20-27）も参照してください。
  - **クレデンシャルの暗号化がディセーブルの場合。**Web プロキシはサロゲートを使用しません。HTTP 要求を介した HTTPS および FTP は、HTTP 要求と同じように ID グループに認証され、照合されます。この操作が行われる仕組みを示す略図については、図 8-1（P.8-9）を参照してください。

表 8-1 に、以前の情報をまとめて示します。

表 8-1　HTTP 要求を介した HTTPS および FTP と ID との照合

サロゲート タイプ	明示的要求	透過的要求
サロゲートなし	HTTP 要求を介した HTTPS および FTP は、HTTP 要求と同じように照合されます。	該当なし
IP ベース	HTTP 要求を介した HTTPS および FTP は、HTTP 要求と同じように照合されます。	HTTP 要求を介した FTP は、HTTP 要求と同じように照合されます。 HTTPS 要求は、次のいずれかの条件の下で HTTP 要求と同じように照合されます。 • 以前の HTTP 要求は、IP ベースのサロゲートを持つ ID を使用して認証されました。 • 以前の HTTP 要求は認証されませんでしたが、HTTPS プロキシが最初の HTTPS 要求を復号化するように設定されます。 それ以外の場合、以前の HTTP 要求が認証されなかった状態で、HTTPS プロキシが要求を拒否するように設定されている場合、HTTPS 要求は失敗します。
Cookie ベース	クライアントは認証が要求されません。 **注：**クレデンシャルの暗号化がディセーブルの場合、サロゲートは使用されず、HTTPS 要求は、HTTP 要求と同じように照合されます。	クライアントは認証が要求されません。

認証スキームが ID グループに影響を与える仕組みについて

レルムまたはシーケンスごとではなく、ID グループごとに認証スキームを定義します。これは、NTLM レルムを含む同じ NTLM レルムまたはシーケンスを使用し、それを NTLMSSP、Basic、または「Basic または NTLMSSP」認証スキームのいずれかを使用する ID グループで使用できることを意味します。

Web プロキシは、トランザクションの開始時にクライアント アプリケーションをサポートするスキームと通信します。現在使用中の ID グループはサポートするスキームを決定します。Web プロキシが Basic および NTLMSSP の両方をサポートすることをクライアント アプリケーションに通知するときに、クライアント アプリケーションはトランザクションで使用するスキームを選択します。

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。これにより、次の条件がすべて当てはまる場合、ユーザが認証をパスしない状態が発生することがあります。

- ID グループが LDAP レルムと NTLM レルムの両方を含むシーケンスを使用する。
- ID グループが「Basic または NTLMSSP」認証スキームを使用する。
- 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。
- ユーザが LDAP レルムにのみ存在する。

このような状態が発生した場合、Web プロキシは、クライアントの要求に応じ、NTLMSSP スキームを使用して、この ID グループのユーザを認証します。ただし、LDAP サーバは NTLMSSP をサポートしないので、指定した LDAP サーバにのみ存在するユーザは、この ID グループの認証を渡すことができません。

このため、LDAP レルムと NTLM レルムの両方を含む認証シーケンスを使用する必要がある場合は、ID グループの認証スキームを設定する際に、URL にアクセスしようとする可能性のあるクライアントアプリケーションを考慮してください。場合によっては、ID グループの唯一の認証スキームとして Basic を選択することもあります。

クライアント要求と ID グループとの照合

図 8-1（P.8-9）は、ID が以下を使用するよう設定されている場合、Web プロキシがクライアント要求を ID グループに対して評価する方法を示します。

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

図 8-2（P.8-10）は、ID が認証サロゲートとしてクッキーを使用し、クレデンシャルの暗号化がイネーブルになり、要求が明示的に転送されるように設定されているときに、Web プロキシがクライアント要求を ID グループに対して評価する方法を示します。

図 8-1　ID のポリシー グループ フロー図：サロゲートなしおよび IP ベースのサロゲート

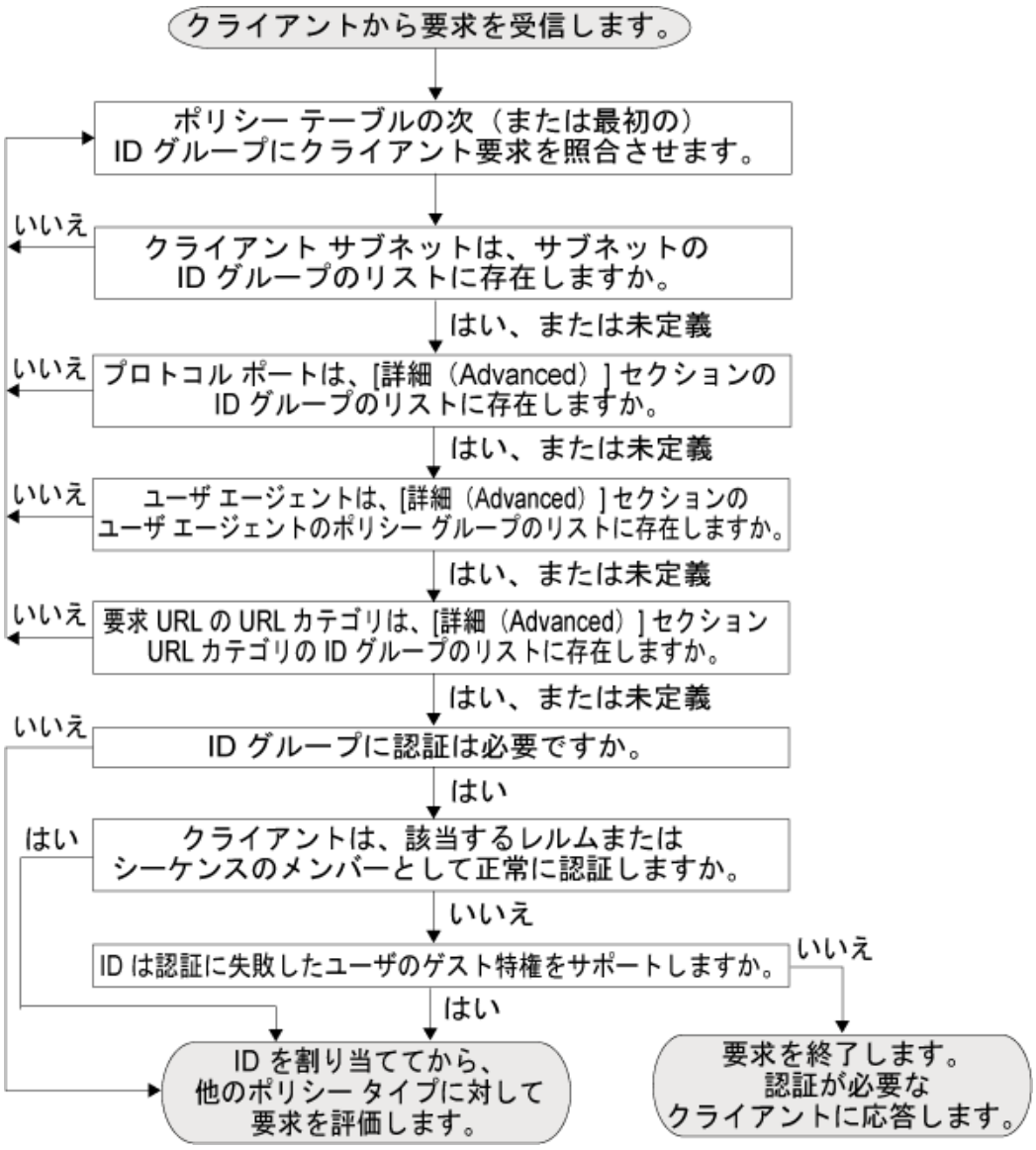
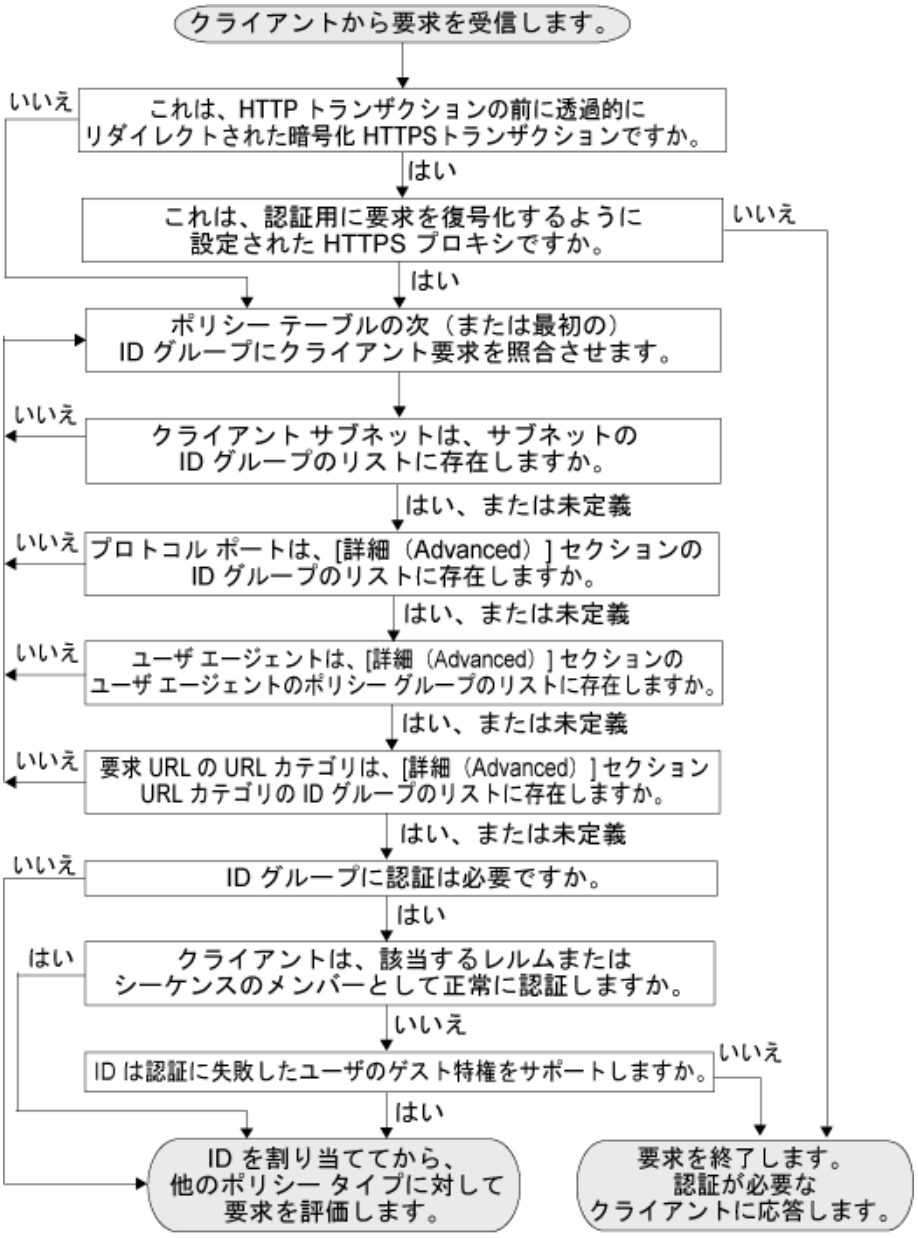


図 8-2　ID のポリシー グループ フロー図：クッキー ベースのサロゲート



認証に失敗したユーザへのゲスト アクセスの許可

無効なクレデンシャルにより認証に失敗したユーザへの制限付きアクセスを許可できます。デフォルトでは、クライアントが無効な認証クレデンシャルを渡したときに、Web プロキシは、基本的にすべてのインターネット リソースへのアクセスをブロックしながら、有効なクレデンシャルを要求し続けます。ただし、ゲスト アクセスを許可した場合、最初にクライアントが無効な認証クレデンシャルを渡したときに、ユーザはゲストとして扱われ、Web プロキシが再度認証を要求することはありません。

次のような場合に、ユーザにゲスト アクセスを許可することがあります。

- ビジターがオフィスに来場し、制限されたインターネット アクセスを許可する必要があるが、ビジターが企業のユーザ ディレクトリに存在しない場合。
- 別のブランチ ロケーション（または被買収企業）の従業員が本社に出社し、インターネット アクセスが必要な場合。ブランチ ロケーション（または被買収企業）のユーザ ディレクトリと本社のユーザ ディレクトリは異なるため、この従業員のクレデンシャルは本社では機能しません。
- 新規採用者が電子メールでクレデンシャルを提供されましたが、それらがまだ認証サーバに登録されていない場合。
- ユーザが Windows ドメイン アカウントの代わりにローカル アカウントを使用して Windows ワーク ステーションにログインし、インターネットへのアクセスが必要な場合。

組織の認証サーバ管理者は、ユーザ ディレクトリにゲスト ユーザ アカウントを作成できます。この場合、Web セキュリティ アプライアンスを介してゲスト アクセスを許可れば、管理者はすべてのビジターにゲスト クレデンシャルを伝達しなくても済みます。

認証に失敗したユーザにゲスト アクセスを許可するには、認証を必要とする ID を作成し、さらにゲスト特権を付与します。次に、この ID を使用して別のポリシーを作成し、そのポリシーをゲスト ユーザに適用します。認証に失敗したユーザがゲスト アクセスを許可された場合、ユーザはこの ID に対してゲスト アクセスを指定するポリシー グループで定義されたリソースにアクセスできます。

次の*いずれか*の条件が当てはまる場合、認証に失敗したユーザは、すべてのトランザクションが*ブロックされています*。

- ID にゲスト特権が付与されていない。
- ユーザはゲスト特権が付与された ID に一致しない。

次の条件が*すべて*当てはまる場合、認証に失敗したユーザは、トランザクションが*許可されています*。

- ユーザはゲスト特権を持つ ID に一致する。
- 非 ID ポリシー グループはこの ID を使用し、ゲスト ユーザに適用する。

たとえば、ゲスト ユーザに固有のアクセスまたは復号化ポリシーを作成できます。

（注） ID がゲスト アクセスを許可し、その ID を使用するユーザ定義のポリシー グループがない場合、認証に失敗したユーザはそのポリシー タイプのグローバル ポリシーに一致します。たとえば、MyIdentity がゲスト アクセスを許可し、MyIdentity を使用するユーザ定義のアクセス ポリシーがない場合、認証に失敗したユーザはグローバル アクセス ポリシーに一致します。ゲスト ユーザをグローバル ポリシーに一致させたくない場合は、ゲスト ユーザに適用され、すべてのアクセスをブロックするグローバル ポリシー上にポリシー グループを作成します。

Web プロキシがユーザのゲスト アクセスを許可する場合、ユーザをゲストとして識別し、アクセス ログに記録します。Web プロキシが IP アドレスまたはユーザ名によってユーザを識別するかどうかを指定できます。アクセス ログ、レポート、エンド ユーザ確認ページでは、ゲスト ユーザのエントリは次のいずれかの形式をとります。

- (unauthenticated)*IP_address*
- (unauthenticated)*username_entered*

認証プロトコルまたはスキームを使用する ID のゲスト アクセスをイネーブルにできます。

ステップ 1　ID グループを定義し、[ゲストのサポート（Support Guest）] 特権オプションをイネーブルにします。

ステップ 2　アクセス ポリシー、復号化 ポリシー、ルーティング ポリシー、データ セキュリティ ポリシー、または外部 DLP データ ポリシーを作成し、ステップ 1 で作成した ID を選択します。

ステップ 3　アクセス ポリシー、復号化 ポリシー、ルーティング ポリシー、データ セキュリティ ポリシー、または外部 DLP データ ポリシーのグループ メンバーシップで、復号化、ルーティング、セキュリティ、または外部 DLP ポリシー は、ステップ 1 の ID に対して [ゲスト（認証に失敗したユーザ）（Guests (users failing authentication)）] を選択します。

ステップ 4　変更を送信し、保存します。

（注）　制限付き URL フィルタリングのため、認証されたユーザが Web サイトからブロックされている場合は、認証を再要求するように Web Proxy を設定できます。これを行うには、「Enable Re-Authentication Prompt If End User Blocked by URL Category or User Session Restriction」グローバル認証設定をイネーブルにします。詳細については、「ユーザに対する再認証の許可」（P.20-27）を参照してください。

ユーザの透過的識別

慣例上、認証ユーザ名によって識別されたユーザはユーザ名とパスワードを入力するように要求されています。その後、ユーザが入力するクレデンシャルは認証サーバによって検証され、Web プロキシが認証済みユーザ名に基づくトランザクションに適切なポリシーを適用します。

ただし、認証済みユーザ名によってユーザを透過的に（つまり、エンド ユーザに情報の入力を要求することなしに）識別するように、Web セキュリティ アプライアンスを設定できます。ID は、別の信頼できるソースから取得したユーザ クレデンシャルを取得する方法です。AsyncOS for Web は、ユーザ名を提供する信頼できるソースによってユーザ名が認証されていることを前提としています。

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適用するために、認証ベースのポリシーを使用する。

ユーザの透過的識別は、Web プロキシがユーザ名を取得し、ID グループを割り当てる方法にのみ影響を与えます。Web プロキシは、ユーザ名を取得して ID を割り当てると、ID を割り当てた方法に関係なく、通常どおり他のすべてのポリシーを適用します。

ユーザを透過的に識別するには、次の基本的な手順を実行します。

1. 透過的ユーザ ID をサポートする、認証レルムを少なくとも 1 つ定義します。詳細については、「透過的ユーザ ID について」（P.8-12）を参照してください。
2. ユーザを透過的に識別する ID グループを成し、上記の手順で作成した認証レルムを指定します。

（注）　Secure Mobility を使用すれば、リモート ユーザを透過的にすることも識別できます。詳細については、「リモート ユーザの透過的な識別」（P.14-3）を参照してください。

透過的ユーザ ID について

以下の認証サーバのいずれかを使用して、ユーザを透過的に識別できます。

- **Active Directory エージェント。**NTLM 認証レルムを作成し、透過的ユーザ ID をイネーブルにします。また、別の Active Directory エージェント ユーティリティを展開する必要があります。シスコでは、Cisco Context Directory Agent を推奨します。詳細については、「Active Directory による透過的ユーザ ID」（P.8-14）を参照してください。
- **Novell eDirectory。**Novell eDirectory をサポートする LDAP 認証レルムを作成します。詳細については、「Novell eDirectory による透過的なユーザ ID」（P.8-15）を参照してください。

AsyncOS for Web は、Novell eDirectory または Active Directory エージェントのいずれかと連携して、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持します。AsyncOS for Web は、Novell eDirectory サーバおよび Active Directory エージェントと定期的に通信して、ユーザ名マッピングへの現在の IP アドレスを保持します。

透過的ユーザ ID がイネーブルの場合、次の手順に従います。

1. クライアントが Web サイトの要求を行います。
2. Web セキュリティ アプライアンスがクライアント要求を受信し、この要求から IP アドレスを取得します。
3. AsyncOS for Web が、クライアント要求にユーザ名を割り当てるために、Web セキュリティ アプライアンスに保存されているユーザ名マッピングへの IP アドレスをチェックします。透過的ユーザ ID と Active Directory との一致が見つからない場合、AsyncOS for Web は Active Directory エージェントにアクセスして一致するユーザ名を見つけます。
4. ユーザ名と IP アドレスが一致することを前提として、AsyncOS for Web は Novell eDirectory サーバまたは Active Directory サーバからユーザ グループを取得します。
5. 必要に応じて、AsyncOS for Web がトランザクションにポリシーを適用します。

IP アドレスがユーザ名に一致しない場合、トランザクションの処理方法を設定できます。エンド ユーザのゲスト 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。図 8-3 は、透過的ユーザ ID 用の ID を設定する際にユーザ アクセスを許可する場所を示します。

図 8-3　　ゲスト アクセスの許可：透過的ユーザ ID

デフォルトで、ユーザ名マッピングへの現在の IP アドレスは 600 秒ごとに更新されます。`tuiconfig` CLI コマンドを使用して、この時間間隔を変更できます。詳細については、「CLI を使用した透過的ユーザ ID の設定」（P.8-17）を参照してください。

（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、「ユーザに対する再認証の許可」（P.20-27）を参照してください。

Active Directory による透過的ユーザ ID

Active Directory は、Web セキュリティ アプライアンスなど、他のサーバによって簡単に照会される方法でユーザ ログイン イベント情報を記録することはありません。ただし、シスコは、Active Directory によって認証されたユーザのユーザ名マッピングへの IP アドレスを保持するために、Active Directory セキュリティ イベント ログを照会する Cisco Context Directory Agent を提供しています。Active Directory エージェント（Cisco Context Directory Agent などを含む）は、一種の ID リポジトリとして機能します。

AsyncOS for Web は Active Directory エージェントと通信して、ユーザ名マッピングへの IP アドレスのローカル コピーを保持します。AsyncOS for Web が IP アドレスをユーザ名に関連付ける必要がある場合は、まず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」（P.8-14）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ときは、次のルールとガイドラインを考慮してください。

- Active Directory による透過的ユーザ ID は NTLM 認証レルムでのみ動作します。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。
- 任意で、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 番めのインスタンスをインストールできます。この場合、各 Active Directory エージェントは他方のエージェントとは関係なく、ユーザ名マッピングへの IP アドレスを保持します。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 サーバのセキュリティ 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。このため、Active Directory エージェントからの更新がない場合に AsyncOS がユーザ マッピングへの IP アドレスをキャッシュする時間のタイムアウト値を定義できます。詳細については、「CLI を使用した透過的ユーザ ID の設定」（P.8-17）を参照してください。
- Active Directory エージェントは、ユーザ名が一意であることを確認するために、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のみ検索します。ネストされたグループは検索しません。

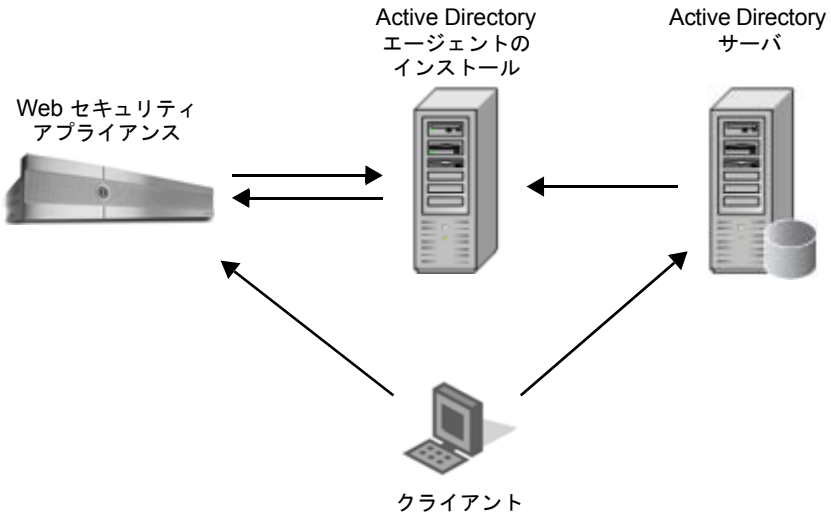
Web セキュリティ アプライアンスに情報を提供する Active Directory エージェントの設定

AsyncOS for Web OS は、直接 Active Directory からクライアントの IP アドレスを取得できないため、Active Directory エージェントからユーザ名マッピング情報への IP アドレス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、フォレスト内のすべての 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、このマシンはネットワーク上の Web セキュリティ アプライアンスにできるだけ近いところに置く必要があります。小規模なネットワーク環境では、直接 Active Directory サーバに Active Directory エージェントをインストールすることもできます。

図 8-4 は、ネットワークに Active Directory エージェントがインストールされる場所を示します。

図 8-4　　Active Directory エージェントのワークフロー



（注） Web セキュリティ アプライアンスとの通信に使用する Active Directory エージェントのインスタンスは、適応型セキュリティ アプライアンスおよびその他の Web セキュリティ アプライアンスをサポートします。

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

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

（注） Web セキュリティ アプライアンスと Active Directory エージェントは、RADIUS プロトコルを使用して相互に通信します。アプライアンスとエージェントは、ユーザのパス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。

Novell eDirectory による透過的なユーザ ID

AsyncOS for Web は、ユーザ名マッピングへの IP アドレスを保持するために Novell eDirectory サーバと通信します。ユーザが Novell クライアントを介してクライアント マシンにログインする際に、Novell クライアントは Novell eDirectory サーバに対してユーザを認証します。認証が成功すると、クライアント マシンの IP アドレスがワーク ステーションにログインしたユーザの属性（[ネットワーク アドレス（NetworkAddress）] フィールド）として、Novell eDirectory サーバに記録されます。

Novell eDirectory を使用してユーザを透過的に識別するときは、次のルールとガイドラインを考慮してください。

- Novell クライアントが各クライアント マシンにインストールされ、エンド ユーザがそれを使用して Novell eDirectory サーバに対して認証する必要があります。
- Novell クライアントのログインで使用する Novell LDAP ツリーは、認証レルムに設定された LDAP ツリーと同一である必要があります。
- Novell クライアントが複数の Novell 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 Novell の LDAP 認証レルムを使用して認証シーケンスを作成します。
- Novell eDirectory の LDAP 認証レルムするときは、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。
- Novell eDirectory は、ユーザがログインするときに、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。これを実行する方法の詳細については、次の Novell サポート記事を参照してください。
  `http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7004564&sliceId=1&docTypeID=DT_TID_1_1&dialogID=100407203&stateId=0%200%20100405493?`

（注）　Novell eDirectory バージョン 8.6、8.7、および 8.8 は、NetworkAddress 属性を更新するように設定できます。

- Novell eDirectory の照会時に、AsyncOS for Web は、ユーザが属する上位の親グループのみ検索します。ネストされたグループは検索しません。
- Novell eDirectory のユーザの [ネットワーク アドレス（Network Address）] フィールドを使用して、ユーザが以前にログインしたワークステーションの IP アドレスを取得できます。

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ときは、ユーザ名マッピングへの IP アドレスが Web セキュリティ アプライアンス上で DHCP リースよりも頻繁に更新されることを確認します。`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 ID の設定」（P.8-17）を参照してください。
- ユーザ名マッピングへの IP アドレスが Web セキュリティ アプライアンス上で更新される前に、エンド ユーザがある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する場合、Web プロキシはそのクライアントを以前のユーザとして記録します。
- 透過的ユーザ ID が失敗したときに、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 ID 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する場合、AsyncOS for Web はシーケンスに表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 ID を設定する場合、認証サロゲートは IP アドレスとする必要があります。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。

- ユーザを透過的に識別するように ID を設定する場合、AsyncOS for Web は、すべてのレルムが透過的ユーザ ID をイネーブルにしているシーケンスのみ表示します。
- %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 の値は、ユーザ名がクライアント 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取得されたことを示します （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 Secure Mobility Solution を使用して Cisco ASA から取得されたことを示します）。

透過的ユーザ ID の設定

ステップ 1　Novell eDirectory サーバで LDAP 認証レルムを作成します。バージョン 3 を使用し、「Novell eDirectory をサポート」するようにレルムを設定します。

ステップ 2　Novell eDirectory を使用して、ユーザを透過的に識別する ID グループを定義します。

a. [識別と認証（Identification and Authentication）] セクションで、[ユーザを透過的に識別（Identify Users Transparently）] を選択します。

b. Novell eDirectory をサポートする LDAP 認証レルムを選択します。

c. 必要に応じて、他の ID オプションをすべて設定します。

ステップ 3　透過的ユーザ ID 用の ID を使用するポリシーを作成します。

関連項目

- 「LDAP 認証」（P.20-31）
- 「LDAP 認証レルムの追加」（P.20-11）
- 「ID の作成」（P.8-18）

CLI を使用した透過的ユーザ ID の設定

AsyncOS for Web には、透過的ユーザ ID で使用する次の CLI コマンドが用意されています。

- **tuiconfig。**このコマンドを使用して、透過的ユーザ ID に関連付けられたいくつかの設定を構成できます。このコマンドは、バッチ モードで使用できます。
  - **AD エージェントのマッピング タイムアウトを設定します。**エージェントからの更新がない場合に Active Directory エージェントから取得した IP アドレスに対して、AsyncOS がユーザ マッピングへの IP アドレスをキャッシュする時間のタイムアウト値を入力します。
  - **Novell eDirectory のマッピング タイムアウトを設定します。**サーバからの更新がない場合に Novell eDirectory サーバから取得した IP アドレスに対して、AsyncOS がユーザ マッピングへの IP アドレスをキャッシュする時間のタイムアウト値を入力します。
  - **AD エージェントのクエリー待ち時間を設定します。**Active Directory エージェントからの応答を待機する時間（秒単位）を入力します。クエリーがタイムアウト値より長くかかる場合、透過的ユーザ ID 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。

  - **Novell eDirectory のクエリー待ち時間を設定します。**Novell eDirectory サーバからの応答を待機する時間（秒単位）を入力します。クエリーがタイムアウト値より長くかかる場合、透過的ユーザ ID 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。

- **tuistatus。**このコマンドには、次のサブ コマンドが用意されています。
  - **adagentstatus。**このコマンドは、すべての Active Directory エージェントの現在のステータスと 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。**このコマンドは、Active Directory エージェントから取得した、Web セキュリティ アプライアンス上に保存されたユーザ名マッピングへの IP アドレスのすべてのエントリを表示します。Active Directory エージェントに保存されたエントリは表示されません。

ID の作成

宛先サイトの URL カテゴリのクライアント サブネットなど、複数の基準の組み合わせに基づいて ID を作成できます。ID メンバーシップには、少なくとも 1 つの基準を定義する必要があります。複数の基準を定義する場合、クライアント要求は ID を照合するためにすべての基準を満たす必要があります。

Web プロキシがクライアント要求を ID と照合する方法の詳細については、「ID グループ メンバーシップの評価」（P.8-4）と「クライアント要求と ID グループとの照合」（P.8-8）を参照してください。

[Web セキュリティマネージャ（Web Security Manager）] > [アイデンティティ（Identities）] ページで ID グループ メンバーシップを定義します。

（注）　認証レルムまたはシーケンスを削除して、削除されたレルムまたはシーケンスに依存する ID をディセーブルにします。

ステップ 1　[Web セキュリティマネージャ（Web Security Manager）] > [アイデンティティ（Identities）] ページに移動します。

ステップ 2　[アイデンティティを追加（Add Identity）] をクリックします。

ステップ 3　ID グループの名前と説明（任意）を入力します。

（注）　各 ID 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　[上に挿入（Insert Above）] フィールドで、ポリシー テーブル内の ID グループを配置する場所を選択します。

複数の ID グループを設定する場合は、各グループの論理的な順序を指定します。適切に照合が行われるように、ID グループを慎重に順序付けます。認証を必要とする最初のポリシー グループの上に、認証を必要としないグループを配置します。認証が ID グループに影響を与える仕組みの詳細については、「認証が ID グループに影響を与える仕組みについて」（P.8-5）を参照してください。

ステップ 5　[ユーザの場所別にメンバーを定義（Define Members by User Location）] セクションで、ローカル ユーザ、リモート ユーザ、またはローカル ユーザとリモート ユーザの両方を適用する ID を設定します。

ここで選択した設定は、この ID 使用可能な認証の設定に影響を与えます。

（注）　このセクションは、Secure Mobility がイネーブルの場合にのみ表示されます。詳細については、「セキュア モビリティの実現の概要」（P.14-1）を参照してください。

ステップ 6　[サブネット別にメンバーを定義（Define Members by Subnet）] フィールドで、この ID が適用され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。複数のアドレスを指定する場合は、カンマで区切ります。

（注）　このフィールドにアドレスを入力しない場合、ID グループがすべての IP アドレスに適用されます。たとえば、認証を必要とするように IP を設定し、その他の設定を定義しない場合、ID は認証を必要とするデフォルトの ID ポリシーと同じように動作します。

ステップ 7　[プロトコル別にメンバーを定義（Define Members by Protocol）] セクションで、この ID を適用するプロトコルを選択します。

（注）　[HTTP/HTTPS のみ（HTTP/HTTPS Only）] は、FTP over HTTP および HTTP CONNECT を使用してトンネリングするその他のプロトコルを含む基礎となるプロトコルとして、HTTP または HTTPS を使用するすべての要求に適用されます。

ステップ 8　[識別と認証（Identification and Authentication）] セクションで、次のオプションのいずれかを選択します。

- **[ID または認証なし（No Identification or Authentication）]。**ユーザは、基本的に IP アドレスによって識別されます。ステップ 15 に進みます。
- **[ユーザを透過的に識別（Identify Users Transparently）]。**ユーザは、ユーザ名マッピングへの現在の IP アドレスによって識別されます。このオプションは、少なくとも 1 つの認証レルムが透過的ユーザ ID をサポートするように定義されているときに使用できます。ステップ 10 に進みます。
- **[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）]。**ユーザは、Cisco 適応型セキュリティ アプライアンス（ASA）から受信したユーザ名マッピングへの現在の IP アドレスによって識別されます。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いて、Cisco 適応型セキュリティ アプライアンスと統合され、ステップ 5 でリモート ユーザが選択されている場合に表示されます。ステップ 11 に進みます。

  （注）　（セキュリティ管理アプライアンスによる展開の場合）セキュリティ管理アプライアンス上で ID を設定する際に、透過的ユーザ ID をサポートする認証レルムを持つ Web セキュリティ アプライアンスが管理対象アプライアンスとして追加されたときにこのオプションが表示されます。

- **[ユーザの認証（Authenticate Users）]。**ユーザは入力された認証クレデンシャルによって識別されます。このオプションは、少なくとも 1 つの認証レルムが定義されているときに表示されます。ステップ 9 に進みます。

ステップ 9　ユーザを認証するように ID を設定します。

a.　[レルムまたはシーケンスを選択（Select a Realm or Sequence）] フィールドで、定義済みの認証レルムまたはシーケンスを選択します。

b. NTLM 認証レルムを含む NTLM 認証レルムまたはシーケンスを選択した場合は、[スキームを選択（Select a Scheme）] フィールドで認証スキームを選択します。

c. 無効な認証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には、[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。

詳細については、「認証に失敗したユーザへのゲスト アクセスの許可」（P.8-10）を参照してください。

（注）　異なるタイプのポリシー グループで ID を使用する場合、認証済みのユーザまたはユーザのグループを指定できます。詳細については、「他のポリシー グループの ID の設定」（P.8-22）を参照してください。

d. ステップ 12 に進みます。

ステップ 10　透過的ユーザ ID を使用するように ID を設定します。

a. [レルムまたはシーケンスを選択（Select a Realm or Sequence）] フィールドで、透過的ユーザ ID をサポートする定義済みの認証レルム（Novell eDirectory をサポートする LDAP 認証レルム、または透過的ユーザ ID に対してイネーブルになっている NTLM 認証レルムのいずれか）を選択します。透過的ユーザ ID をサポートするレルムのみを含むシーケンスを選択することもできます。

b. 透過的ユーザ ID が失敗したときにトランザクションを処理する方法（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表示するかのいずれか）を選択します。

Web プロキシが、指定した IP アドレスから現在ログインしているユーザを判定できない場合、つまり、IP アドレスがユーザ マッピングへの IP アドレスに存在しない場合、透過的ユーザ ID が失敗する可能性があります。

c. 透過的ユーザ ID が失敗したため認証プロンプトが表示され、無効なクレデンシャルによって認証に失敗したときに、ユーザにゲスト アクセスを許可するかどうかを選択します。

透過的ユーザ ID の詳細については、「ユーザの透過的識別」（P.8-12）を参照してください。

d. ステップ 12 に進みます。

ステップ 11　Cisco 適応型セキュリティ アプライアンス（ASA）と統合することで、透過的ユーザ ID を使用するように ID を設定します。

a. [レルムまたはシーケンスを選択（Select a Realm or Sequence）] フィールドで、定義済みの認証レルムまたはシーケンスを選択します。

b. NTLM 認証レルムを含む NTLM 認証レルムまたはシーケンスを選択した場合は、[スキームの選択（Select a Scheme）] フィールドで認証スキームを選択します。

（注）　異なるタイプのポリシー グループで ID を使用する場合、認証済みのユーザまたはユーザのグループを指定できます。詳細については、「他のポリシー グループの ID の設定」（P.8-22）を参照してください。

c. ステップ 12 に進みます。

ステップ 12　[認証サロゲート（Authentication Surrogate）] セクションで設定を表示します。

ステップ 13　ユーザが正常に認証された後で、クライアントの認証に使用されるトランザクションをユーザに関連付ける方法（IP アドレスによるか、クッキーを使用するかのいずれか）を選択します。表 8-2 に示すオプションのいずれかを選択します。

表 8-2　サロゲート タイプ

サロゲート タイプ	説明
IP アドレス	Web プロキシは、特定の IP アドレスで認証されたユーザを追跡します。透過的ユーザ ID を実現するには、IP ベースの認証を選択します。
永続的なクッキー	Web プロキシは、アプリケーションごとの各ユーザに永続的なクッキーを生成することにより、特定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 cookie	Web プロキシは、アプリケーションごと、ドメインごとの各ユーザにセッション Cookie を生成することにより、特定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提供する場合、クッキーは上書きされます）。アプリケーションを終了するとクッキーは削除されます。
サロゲートなし	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、すべての新しい TCP 接続の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。

次の場合に、IP ベースの認証を使用することがあります :

- クライアント マシン上に 1 人だけユーザが存在し、ユーザがシングル サイン オン動作を実現できるようにしたい場合。
- 透過的ユーザ ID を使用したい場合。
- MSN Messenger など、クッキーベースのサロゲートでは動作しないアプリケーションで機能する ID を作成した場合。

多くのユーザが共有する Citrix サーバやキオスクなど、1 台のマシン上に複数のユーザが存在する場合、クッキー ベースの認証を選択する場合があります。

他の設定やさまざまなタイプの要求によってサポートされる認証サロゲートの詳細については、「認証ユーザの追跡」（P.20-29）を参照してください。

（注）　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。詳細については、「グローバル認証設定の指定」（P.20-19）を参照してください。

ステップ 14　[明示的な転送要求（Explicit Forward Request）] フィールドで、透過的要求に使用するサロゲートを明示的要求にも使用するかどうかを選択します。

クレデンシャルの暗号化をイネーブルにすると、このフィールドは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。

ステップ 15　任意で、[詳細（Advanced）] セクションを展開して、追加メンバーシップの要件を定義します。

表 8-3　ID グループの拡張オプション

拡張オプション	説明
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 ポートによるポリシー グループのメンバーシップを定義するには、[プロキシ ポート（Proxy Ports）] フィールドに 1 つまたは複数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。 **注：**シスコでは、アプライアンスが明示的に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のみ、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。
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、ユーザ定義のカテゴリと定義済みの URL カテゴリの両方のメンバーシップが除外されます。つまり、[追加（Add）] カラム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。
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。 ユーザ エージェント ベースのポリシーの作成の詳細については、「ユーザ エージェント ベースのポリシーの使用」（P.7-11）を参照してください。

ステップ 16　変更を送信し、保存します。

（注）　ID への変更をコミットした場合、エンド ユーザは再認証される必要があります。

他のポリシー グループの ID の設定

すべての非 ID ポリシー グループは、そのポリシー グループのメンバーシップの一部として、少なくとも 1 つの ID グループを指定します。複数の ID グループを使用するように非 ID ポリシー グループを設定し、ポリシー グループを使用して Web へのアクセスを許可するユーザまたはユーザのグループを指定できます。

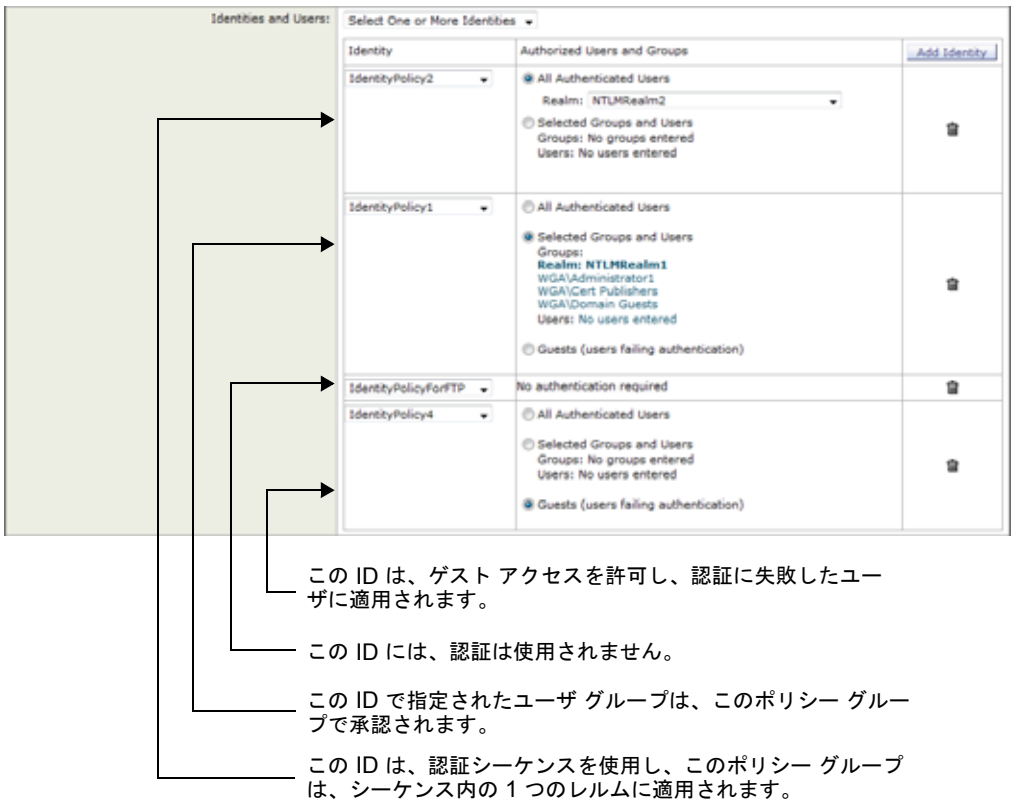
次のような状況で、1 つのポリシー グループに複数の ID グループを指定する場合があります。

- HTTP トランザクション用に定義された ID グループとネイティブ FTP トランザクション用に定義された別の ID グループが存在する場合。HTTP トランザクションとネイティブ FTP トランザクションの両方に適用する単一の非 ID ポリシー グループを作成できます。
- 認証レルムごとに別個の ID グループを定義する場合。複数の認証レルムのユーザに同じアクセス コントロール設定を定義する 1 つのアクセス ポリシー グループを作成します。

（注）　すべての ID を指定し、認証済みユーザを設定することもできます。

図 8-5 は、複数の ID を使用するポリシー グループを示します。

図 8-5　　ポリシー グループ内の複数の ID



（注）　ID グループがディセーブルになると、その ID グループは それを使用した非 ID ポリシー グループから（ディセーブルではない）*削除されます*。ID グループが再びイネーブルになったときに、以前に ID を使用した非 ID ポリシー グループがイネーブルになった ID を自動的に取り込むことはありません。ID グループは、削除された認証レルムまたはシーケンスによってディセーブルになります。

ステップ 1　新しいグループ ポリシーを作成するか、アクセス ポリシー、復号化 ポリシー、ルーティング ポリシー、データ セキュリティ ポリシー、または外部 DLP データ ポリシーの既存のポリシー グループのメンバーシップを編集します。

ステップ 2　[ID とユーザ（Identities and Users）] セクションまで下方にスクロールします。

ステップ 3　ドロップダウン メニューから次のオプションのいずれかを選択します。

- **[1 つ以上の ID を選択（Select One or More Identities）]。**このオプションでは、特定の ID グループを設定できます。ステップ 4 に進みます。
- **[すべての ID（All Identities）]。**このオプションでは、すべての設定済み ID グループを指定します。ステップ 5 に進みます。

ステップ 4　[アイデンティティ（Identity）] カラムで、このグループ ポリシーに適用する ID グループを選択します。

ステップ 5　認証を必要とする ID を選択すると、このポリシー グループで承認されているユーザを指定できます。これらのユーザは認証する必要があります。[承認済みユーザとグループ（Authorized Users and Groups）] カラムで、次のオプションのいずれかを選択します。

- **[すべての認証済みユーザ（All authenticated users）]。**このポリシー グループの ID を設定して、デフォルトで ID グループのすべての*認証済み*ユーザに適用できます。ID グループが認証シーケンスを指定する場合、このグループ ポリシーを設定して、シーケンスの 1 つの認証レルムまたはすべてのレルムに適用できます。
- **[選択されたグループとユーザ（Selected Groups and Users）]。**このグループ ポリシーの ID を設定して、特定のユーザに適用できます。グループ オブジェクトまたはユーザ オブジェクトによってユーザを定義できます。グループまたはユーザのいずれかのリンクをクリックし、開いたページでグループまたはユーザ情報を入力します。
  NTLM 認証レルムを使用して ID にユーザのグループを追加する場合、[グループの編集（Edit Groups）] ページには、組み込みグループを除き、一致する最初の 500 件のエントリが表示されます。
- **[ゲスト（認証に失敗したユーザ）（Guests (users failing authentication)）]。**ID グループがゲスト アクセスを許可する場合、このポリシー グループを設定して、この ID で認証に失敗したすべてのユーザに適用できます。詳細については、「認証に失敗したユーザへのゲスト アクセスの許可」（P.8-10）を参照してください。
- **[すべてのユーザ（認証済みユーザおよび未認証ユーザ）（All users (authenticated and unauthenticated users)）]。**このグループ ポリシーを設定して、すべての ID グループのすべてのユーザに適用できます。このオプションは、[すべての ID（All Identities）] を選択した場合にのみ表示されます。このポリシー グループをすべてのユーザに適用する場合、少なくとも 1 つの拡張オプションを指定して、このポリシー グループとグローバル ポリシーを区別する必要があります。

ステップ 6　（任意）[アイデンティティを追加（Add Identity）] をクリックして、このグループ ポリシーに別の ID グループを追加します。

[すべての ID（All Identities）] ではなく特定の ID グループを設定した場合は、追加の ID グループを追加できます。

ステップ 7　別の ID グループを追加する場合は、ステップ 4 と 5 を繰り返します。

ステップ 8　変更を送信し、保存します。

ID ポリシー テーブルの例

この項では、ID ポリシー テーブルで定義されている ID グループのサンプルを示し、Web プロキシが各 ID ポリシー テーブルを使用してさまざまなクライアント要求を評価する方法について説明します。

例 1

表 8-4 は、3 つのユーザ定義の ID グループを持つ ID ポリシー テーブルを示します。最初の ID グループは、特定のサブネットに適用され、認証は必要ありません。2 番めの ID グループは、すべてのサブネットに適用され、[プロキシ & 変換（Proxies & Translators）] カテゴリの URL を要求し、RealmA で認証する必要があります。3 番めの ID グループは、すべてのサブネットに適用され、定義された拡張オプションがないので RealmA で認証する必要があります。グローバル ID ポリシーは、すべてのサブネット（定義上）に適用され、認証は必要ありません。

表 8-4　　ポリシー テーブルの例 1

順序	サブネット	認証の必要の有無	レルムまたはシーケンス	拡張オプション
1	10.1.1.1	No	該当なし	なし
2	All	Yes	RealmA	URL カテゴリは [プロキシ & 変換（Proxies & Translators）] です
3	All	Yes	RealmA	なし
グローバル ID ポリシー	All（デフォルト）	No	該当なし	該当なし（デフォルトでなし）

Web プロキシは、クライアントのサブネットおよび要求の URL カテゴリに応じて、このシナリオの ID グループへのクライアント要求に別々に一致します。

- **任意の URL のサブネット 10.1.1.1 上の任意のクライアント。**サブネット 10.1.1.1 上のクライアントが任意の URL の要求を送信する場合、Web プロキシは最初の ID グループを評価し、クライアント サブネットが最初の ID グループのサブネットに一致することを判定します。次に、認証が必要ないこと、および拡張オプションは設定されていないことを判定し、最初の ID グループをトランザクションに割り当てます。
- **[プロキシ & 変換（Proxies & Translators）] URL カテゴリ内の URL の 10.1.1.1 以外のサブネット上の任意のクライアント。**10.1.1.1 以外のサブネット上のクライアントが [プロキシ & 変換（Proxies & Translators）] カテゴリの URL の要求を送信する場合、Web プロキシは最初の ID グループを評価し、クライアントのサブネットがサブネットの最初の ID グループのリストに表示されていないことを判定します。その結果、2 番めの ID グループを評価し、クライアントのサブネットがサブネット上の 2 番めの ID グループのリストにあることを判定します。次に、要求の URL が 2 番めの ID グループの詳細セクションで URL カテゴリと一致することを判定します。次に、2 番めの ID グループは認証が必要であることを判定し、RealmA で定義された認証サーバによってユーザを認証しようとします。ユーザが RealmA に存在する場合、Web プロキシは 2 番めの ID グループをトランザクションに割り当てます。ユーザが RealmA に存在しない場合、AsyncOS は、クライアントの認証の失敗によりクライアント要求を終了します。
- **[プロキシ & 変換（Proxies & Translators）] URL カテゴリ内の任意の URL の 10.1.1.1 *以外の* サブネット上の任意のクライアント。**10.1.1.1 以外のサブネット上のクライアントが URL の要求を送信する場合、Web プロキシは最初の ID グループを評価し、クライアントのサブネットがサブネットの最初の ID グループのリストに表示されていないことを判定します。その結果、2 番めの ID グループを評価し、クライアントのサブネットがサブネット上の 2 番めの ID グループのリストにあることを判定します。次に、要求の URL が 2 番めの ID グループの詳細セクションで URL カテゴリと一致*しない*ことを判定します。その結果、3 番めの ID グループを評価し、クライアントのサブネットがサブネット上の 3 番めの ID グループのリストにあることを判定します。3 番めの ID グループに拡張オプションが何も設定されていない場合は、認証要件との比較を続けます。次に、3 番めの ID グループは認証が必要であることを判定し、RealmA で定義された認証サーバに

よってユーザを認証しようとします。ユーザが RealmA に存在する場合、Web プロキシは 3 番めの ID グループをトランザクションに割り当てます。ユーザが RealmA に存在しない場合、Web プロキシは、クライアントの認証の失敗によりクライアント要求を終了します。

このシナリオでは、すべてのサブネットに適用されるユーザ定義の ID グループ（3 番めのグループ）に拡張オプションが設定されていないため、ほとんどのクライアント要求がグローバルな ID グループに一致せず、認証が必要になることに注意してください。最初または 2 番めの ID グループに一致しないネットワーク上のクライアントは 3 番めの ID グループに一致します。アプライアンスがクッキーベースの認証を使用するトランスペアレント モードの場合の HTTPS 要求は、この例外です。認証が必要な場合であっても、10.1.1.1 以外のサブネット上の任意のクライアントがグローバル ID グループに一致します。

例 2

表 8-5 は、2 つのユーザ定義の ID グループを持つポリシー テーブルを示します。最初の ID グループは、すべてのサブネットに適用され、認証を必要とし、認証に RealmA を指定します。2 番めの ID グループは、すべてのサブネットに適用され、認証を必要とし、認証に RealmB を指定します。どの ID グループも拡張オプションは何も設定されていません。グローバル ID グループはすべてのサブネットに適用され、認証を必要とし、認証に全レルム シーケンスを指定します。

表 8-5　ポリシー テーブルの例 2

順序	サブネット	認証の必要の有無	レルムまたはシーケンス	拡張オプション
1	すべて	Yes	RealmA	なし
2	すべて	Yes	RealmB	なし
グローバル ID ポリシー	すべて	Yes	すべてのレルム	該当なし（デフォルトでなし）

このシナリオでは、クライアントが URL の要求を送信し、Web プロキシが最初の ID グループを評価し、ID グループがすべてのサブネットに適用されることを判定し、拡張オプションは何も設定されていません。次に、ID グループが認証を必要とし、ID グループに指定されている唯一のレルムが RealmA であることを判定します。このため、*任意のサブネット上のクライアントが認証に合格するには、RealmA に存在する必要があります。*

RealmA に存在するクライアントが URL の要求を送信すると、クライアントは認証に合格し、Web プロキシが最初の ID グループをトランザクションに割り当てます。RealmA に存在*しない*クライアントが URL の要求を送信すると、クライアントは認証に失敗し、Web プロキシは要求を終了します。

RealmB 内のクライアントが URL の要求の送信する場合、Web プロキシは、クライアント要求を 2 番めの ID グループと照合*しない*ことに注意してください。これは、以前の ID グループが 2 番めの ID グループの同じサブネット（およびまったく同じ拡張オプション、この例では「なし」）にすでに適用され、認証が必要ではあるが、代わりに RealmA から行う必要があるためです。RealmB のクライアントは、2 番めの ID グループを「通り抜け」ません。

RealmB のユーザに、RealmA のユーザに適用される設定とは異なるアクセス ポリシー、復号化ポリシー、ルーティング ポリシーを設定する場合は、次の手順を実行します。

ステップ 1　RealmA および RealmB の両方を含む認証シーケンスを作成します。業務上のニーズに応じて、シーケンスのレルムの順序を選択できます。

ステップ 2　ID グループを 1 つ作成し、それを RealmA および RealmB 内にユーザが存在する可能性のあるサブネットに設定します。この例では、すべてのサブネットに対して ID グループを設定します。

ステップ 3　ステップ 1 で定義したシーケンスを使用するように ID グループを設定します。

ステップ 4　アクセス ポリシーなど、同じタイプの 2 つのユーザ定義のポリシー グループを作成し、両方がステップ 3 で定義した認証シーケンスを持つ ID グループを使用するように設定します。

ステップ 5　最初のポリシー グループを、RealmA などの 1 つのレルムのユーザにのみ適用するように設定します。これを実行するには、シーケンスに特定のレルムを指定するか、認証グループを使用するか、または特定のユーザ名を入力します。

ステップ 6　2 番めのポリシー グループを、RealmB などの 1 つのレルムのユーザにのみ適用するように設定します。これを実行するには、シーケンスに特定のレルムを指定するか、認証グループを使用するか、または特定のユーザ名を入力します。

このようにアプライアンスを設定する場合、URL の要求を送信する任意のクライアントは、ID レベルで認証に合格するために、シーケンス内のいずれかのレルム（RealmA または RealmB）に存在する必要があります。クライアント要求に ID が割り当てられると、Web プロキシは、クライアント要求を他のポリシー タイプと比較し、アクセス ポリシー グループなどの一致するポリシー グループを決定し、これらの制御設定に適用します。この例では、Web プロキシは、ステップ 5 で設定したポリシー グループを持つ RealmA のユーザを照合し、ステップ 6 で設定したポリシー グループを持つ RealmB のユーザを照合します。

9

トランザクション要求のブロック、許可、またはリダイレクト

トランザクション要求のブロック、許可、またはリダイレクトの概要

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し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。**Web プロキシは、中断のない接続を寄与化します。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場合があります。
- **ブロック。**Web プロキシは、接続を許可せずに、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。**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。組織が内部サイトへのリンクを公開したが、サイトの場所が公開以降に変更された場合や、Web サーバを制御する権限がない場合は、アプライアンスでトラフィックをリダイレクトします。

通常、さまざまなタイプのポリシーが、トランスポート プロトコルに基づいてトラフィックを制御します。

	ポリシー タイプ				
プロトコル	**アクセス**	**復号化**	**FTP**	**SOCKS**	**コメント**
HTTP	X				
HTTPS	X	X			復号化ポリシーはアクセス ポリシーに優先します。
FTP	X		X		FTP ポリシーはアクセス ポリシーに優先します。
SOCKS				X	

AsyncOS を設定し、トランザクション要求の次の特性に基づいて、トランザクション要求をブロック、許可、またはリダイレクトできます。

- AsyncOS によってトランザクション要求に割り当てられる **ID**

- トランザクションが従う**プロトコル**
- 要求を受信した**プロキシ ポート**
- 要求の発信元である**サブネット**
- 要求が行われた**時間範囲**
- 宛先 Web サイトの **URL カテゴリ**
- 要求を行う**ユーザ エージェント**（アプリケーション）

AsyncOS for Web は、その Web プロキシおよび DVS エンジンとともに複数の Web セキュリティ機能を使用して、Web トラフィックを制御し、Web ベースの脅威からネットワークを保護し、組織のアクセプタブル ユース ポリシーを実施します。どの HTTP 接続が許可されるか、またはブロックされるかを指定するポリシーを定義できます。

アプライアンスが HTTP 要求を処理するように設定するには、次のタスクを実行します。

ステップ 1　**Web プロキシをイネーブルにします。**HTTP トラフィックを許可またはブロックするには、まず、Web プロキシをイネーブルにします。通常、Web プロキシは、初期セットアップ中にシステム セットアップ ウィザードを使用してイネーブルにします。詳細については、「Web プロキシの設定」（P.5-3）を参照してください。

ステップ 2　**アクセス ポリシー グループを作成して設定します。**Web プロキシがイネーブルになった後、アクセス ポリシー グループを作成して、各ユーザからの各要求の処理方法を決定します。詳細については、「アクセス ポリシー グループ」（P.9-2）を参照してください。

アクセス ポリシー グループ

アクセス ポリシーで、Web プロキシが HTTPS および FTP 接続を処理し、ネットワーク ユーザの HTTP 要求を復号化する方法を定義します。指定したユーザのグループに、異なるアクションを適用できます。また、Web プロキシが HTTP トランザクションのために、どのポートをモニタするかを指定できます。

（注）　HTTP PUT および POST 要求は、Outbound Malware Scanning、Cisco IronPort Data Security、および外部 DLP ポリシーによって処理されます。詳細については、「データ セキュリティと外部 DLP ポリシーの概要」（P.13-1）および「Outbound Malware Scanning」（P.12-1）を参照してください。

Web プロキシは、モニタ対象ポートまたは復号化された HTTPS 接続で HTTP 要求を受信すると、要求をアクセス ポリシー グループと比較して、適用するアクセス ポリシー グループを決定します。アクセス ポリシー グループに要求を割り当てた後は、要求の処理方法を決定できます。アイデンティティ グループ メンバーシップの評価の詳細については、「ポリシー グループ メンバーシップ」（P.7-7）を参照してください。

Web プロキシは、HTTP 要求、または復号化された HTTPS 接続で、次のアクションをどれでも実行できます。

- **許可。**Web プロキシは、中断のない接続を寄与化します。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場合があります。
- **ブロック。**Web プロキシは、接続を許可せずに、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。**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。組織が内部サイトへのリンクを公開したが、サイトの場所が公開以降に変更された場合や、Web サーバを制御する権限がない場合は、アプライアンスでトラフィックをリダイレクトします。トラフィックのリダイレクトの詳細については、「トラフィックのリダイレクト」（P.17-20）を参照してください)。

（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実行する最終アクションです。アクセス ポリシーに設定できるモニタ アクションは最終アクションではありません。詳細については、「モニタ アクションについて」（P.9-3）を参照してください。

Web プロキシは、HTTP 要求または復号化された HTTPS 要求にアクセス ポリシーを割り当てた後、その要求を、ポリシー グループの設定済み管理設定と比較し、適用するアクションを決定します。複数のセキュリティ コンポーネントを設定して、特定のポリシー グループに対する、HTTP 要求および復号化された HTTPS 要求の処理方法を決定できます。設定できるセキュリティ コンポーネント、および Web プロキシがアクセス グループを使用して HTTP トラフィックを制御する方法の詳細については、「HTTP およびネイティブ FTP トラフィックの制御」（P.9-8）を参照してください。

モニタ アクションについて

Web プロキシは、トランザクションと管理設定を比較するときに、設定を順番に評価します。各管理設定を指定して、アクセス ポリシーに対して次のいずれかの操作を実行できます。

- モニタ
- 許可
- ブロック
- リダイレクト

モニタ以外のすべての操作は、Web プロキシがトランザクションに適用する最終アクションです。最終アクションにより、Web プロキシは、残りの管理設定とトランザクションの比較を停止します。

モニタ アクションは中間アクションです。Web プロキシは、トランザクションを他の管理設定と比較し続け、適用する最終アクション決定します。

たとえば、アクセス ポリシーが、疑わしいユーザ エージェントを*モニタ*するように設定されている場合、Web プロキシは、ユーザ エージェントからの要求に関する最終決定を下しません。特定の URL カテゴリの妨げになるようにアクセス ポリシーが設定されている場合は、その URL カテゴリへのすべての要求が、サーバのレピュテーション スコアに関係なく、サーバからコンテンツを取得する前に*ブロック*されます。

（注）　管理設定がモニタと一致し、トランザクションが最終的に許可されると、Web プロキシは、モニタされた設定をアクセス ログに記録します。たとえば、URL が、モニタされた URL カテゴリと一致すると、Web プロキシは URL カテゴリをアクセス ログに記録します。

図 9-3（P.9-10）は、アクセス ポリシーの管理設定を評価するときに、Web プロキシが使用する順序を示しています。フロー ダイアグラムは、トランザクションに適用されるアクションが最終アクション、つまり、許可、ブロック、リダイレクトのみであることを示しています。

（注）　図 11-5（P.11-22）は、復号化ポリシーの管理設定を評価するときに Web プロキシが使用する順序を示し、図 13-3（P.13-11）は、Cisco IronPort データ セキュリティ ポリシーの管理設定を評価するときの順序を示します。

アクセス ポリシー グループ メンバーシップの評価

Web プロキシは、クライアント要求に ID を割り当てた後、この要求を他のポリシー タイプと比較して要求を評価し、タイプごとに属するポリシー グループを特定します。HTTPS プロキシがイネーブルである場合は、アクセス ポリシーに対して HTTP 要求および*復号化*された HTTPS 要求が適用されます。HTTPS プロキシがイネーブルでない場合、デフォルトでは、アクセス ポリシーに対して HTTP 要求およびすべての HTTPS 要求が評価されます。

Web プロキシは、クライアント要求のポリシー グループのメンバーシップに基づいて、設定されたポリシー制御設定をクライアント要求に適用します。

クライアント要求が一致するポリシー 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。このプロセスでは、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。ID グループ メンバーシップの評価に関する詳細については、「ID グループ メンバーシップの評価」（P.8-4）を参照してください。
- **権限を持つユーザ。**割り当てられた ID に認証が必要な場合、ユーザは、グループ ポリシーに一致するために、アクセス ポリシー グループ内の権限を持つユーザのリストに含まれている必要があります。権限を持つユーザのリストには、任意の指定したグループまたはユーザ、または ID がゲスト アクセスを許可する場合はゲスト ユーザを指定できます。
- **高度なオプション。**アクセス ポリシー グループ メンバーシップの複数の高度なオプションを設定できます。オプションの一部（プロキシ ポートや URL カテゴリなど）は、ID 内でも定義できます。高度なオプションを ID 内で設定すると、アクセス ポリシー グループ レベルでは設定できなくなります。

このセクションでは、Web プロキシがクライアント要求とアクセス ポリシー グループを照合する方法についての概要を示します。Web プロキシがクライアント要求を正確に照合する仕組みに関する詳細については、「クライアント要求のアクセス ポリシー グループとの照合」（P.9-4）を参照してください。

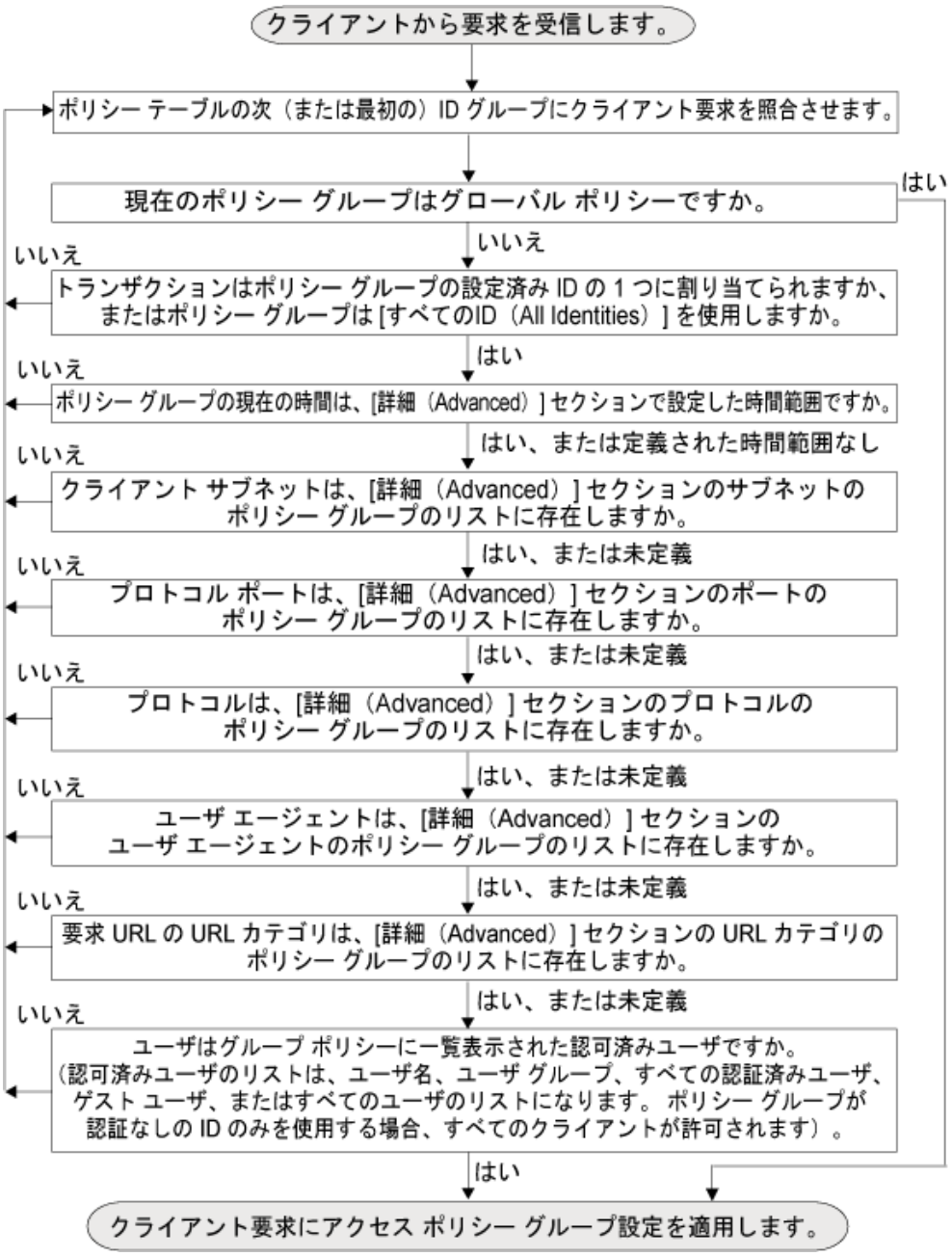
Web プロキシは、ポリシー テーブルの各ポリシー グループを順番に読み取ります。クライアント要求の状態を、最初のグループ ポリシーのメンバーシップ基準と比較します。一致した場合、Web プロキシは、そのポリシー グループのポリシー設定を適用します。

一致しない場合、Web プロキシは、クライアント要求を次のポリシー グループと比較します。ユーザ定義のポリシー グループにクライアント要求が一致するまでこのプロセスを継続します。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、クライアント要求をポリシー 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。

クライアント要求のアクセス ポリシー グループとの照合

図 9-1（P.9-5）は、Web プロキシがアクセス ポリシー グループに対してクライアント要求を評価する方法を示します。

図 9-1　アクセス ポリシーのポリシー グループ フロー ダイアグラム



アクセス ポリシーの作成

宛先サイトの 1 つ以上のアイデンティティや URL カテゴリなど、複数の条件の組み合わせに基づいてアクセス 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。複数の条件を定義した場合、クライアント要求は、ポリシー グループと一致するために、すべての条件を満たす必要があります。ただし、クライアント要求が一致するのは、設定されたアイデンティティのうち、1 つだけである必要があります。

Web プロキシがクライアント要求をポリシー グループと照合する方法の詳細については、「アクセス ポリシー グループ メンバーシップの評価」（P.9-4）および「クライアント要求のアクセス ポリシー グループとの照合」（P.9-4）を参照してください。

ポリシー グループ メンバーシップは、[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）] ページの順に進みます。

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 グループ名を入力し、必要に応じて [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、慎重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。

この方法の詳細については、「他のポリシー グループの ID の設定」（P.8-22）を参照してください。

ステップ 6　必要に応じて、[詳細（Advanced）] セクションを拡大し、追加メンバーシップの要件を定義します。

表 9-1　アクセス ポリシー グループの高度なオプション

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。組み込むプロトコルを選択します。 「All others」は、このオプションの上記に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した場合、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、アウトバウンド マルウェア スキャン、データ セキュリティ、または外部 DLP ポリシーの 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：**このグループ ポリシーに関連付けられた ID がこの拡張設定によって ID を定義する場合、これは非 ID ポリシー グループ レベルでは設定できません。
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：**このポリシー グループに関連付けられた ID によってアドレスでそのメンバーシップが定義されている場合は、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）	定義された時間範囲でポリシー 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。[時間範囲（Time Range）] フィールドから時間の範囲を選択します。次に、このポリシー グループが、指定した時間の範囲内と範囲外のどちらを適用するかを選択します。 時間ベースのポリシーの作成の詳細については、「時間ベースのポリシーの使用」（P.7-9）を参照してください。 時間範囲の作成の詳細については、「時間範囲の作成」（P.7-10）を参照してください。

表 9-1　アクセス ポリシー グループの高度なオプション （続き）

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：**このグループ ポリシーに関連付けられた ID がこの拡張設定によって ID を定義する場合、これは非 ID ポリシー グループ レベルでは設定できません。
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。 ユーザ エージェント ベースのポリシーの作成の詳細については、「ユーザ エージェント ベースのポリシーの使用」（P.7-11）を参照してください。 **注：**このグループ ポリシーに関連付けられた ID がこの拡張設定によって ID を定義する場合、これは非 ID ポリシー グループ レベルでは設定できません。
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。詳細については、「セキュア モビリティの実現の概要」（P.14-1）を参照してください。

ステップ 7　変更を送信します。

ステップ 8　アクセス ポリシー グループの管理を設定して、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。

新しいアクセス ポリシー グループは、各管理設定のオプションを設定するまでは、グローバル ポリシー グループ設定を自動的に継承します。詳細については、「HTTP およびネイティブ FTP トラフィックの制御」（P.9-8）を参照してください。

ステップ 9　変更を送信し、保存します。

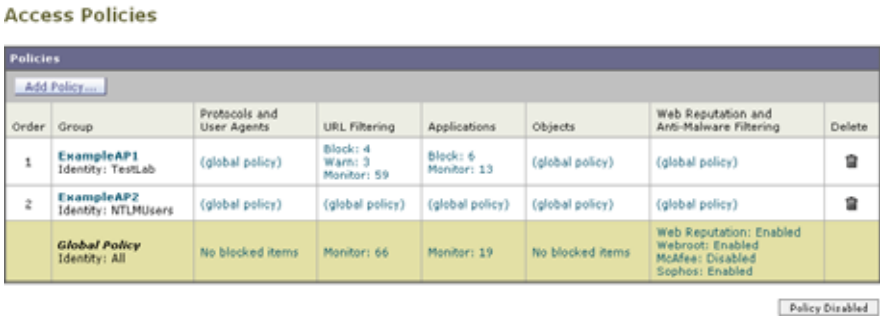
HTTP およびネイティブ FTP トラフィックの制御

Web プロキシによってアクセス ポリシー グループに HTTP 要求、ネイティブ FTP 要求、または復号化された HTTPS 要求が割り当てられた後、要求は、そのポリシー グループの管理設定を継承します。アクセス 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許可するか、ブロックするか、またはリダイレクトするかが決定されます。

[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、アクセス ポリシー グループの管理を設定します。

図 9-2 は、アクセス ポリシー グループの管理を設定する場所を示します。

図 9-2　セキュア アクセス ポリシーの作成



次の設定で、要求に実行するアクションを決定できます。

- **プロトコルとユーザエージェント（Protocols and User Agents）。**詳細については、「プロトコルおよびユーザ エージェント」（P.9-10）を参照してください。
- **URL カテゴリ（URL Categories）。**詳細については、「URL カテゴリ」（P.9-11）を参照してください。
- **アプリケーション（Applications）。**詳細については、「アプリケーション」（P.9-12）を参照してください。
- **オブジェクト（Objects）。**詳細については、「オブジェクトのブロック」（P.9-12）を参照してください。
- **Web レピュテーションおよびマルウェア対策フィルタ（Web Reputation and Anti-Malware Filtering）。**詳細については、「「Web レピュテーションおよびアンチマルウェア」（P.9-13）」を参照してください。

アクセス グループが要求に割り当てられた後、ポリシー グループの管理設定が評価され、要求を許可するか、ブロックするか、またはリダイレクトするかが決定されます。要求にアクセス グループを割り当てる方法の詳細については、「ポリシー グループ メンバーシップ」（P.7-7）を参照してください。

図 9-3（P.9-10）は、Web プロキシが特定のアクセス ポリシーを要求に割り当てた後に、その要求で実行するアクションを決定する方法を示します。

図 9-3　アクセス ポリシーのアクション適用

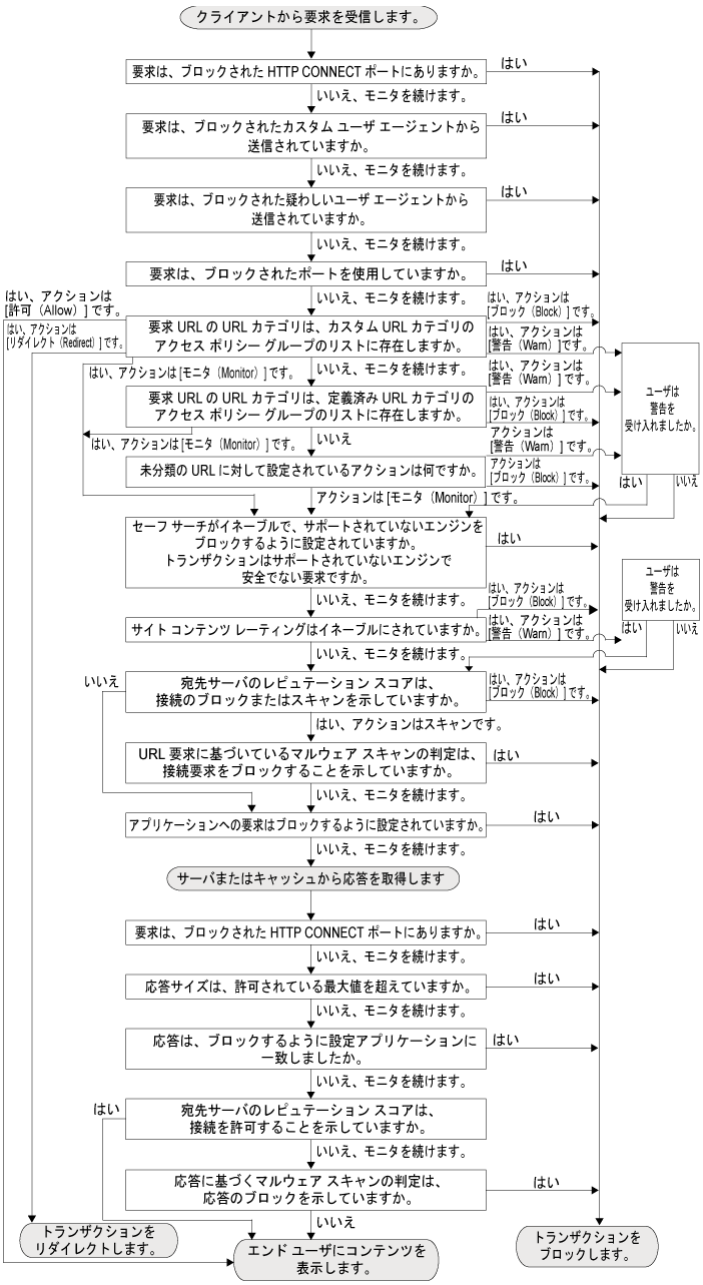


図 9-3（P.9-10）は、宛先サーバの Web レピュテーション スコアに関連する 2 つの決定ポイントを示します。サーバの Web レピュテーション スコアが評価されるのは 1 回だけですが、その結果は、決定フローの 2 つのポイントで適用されます。

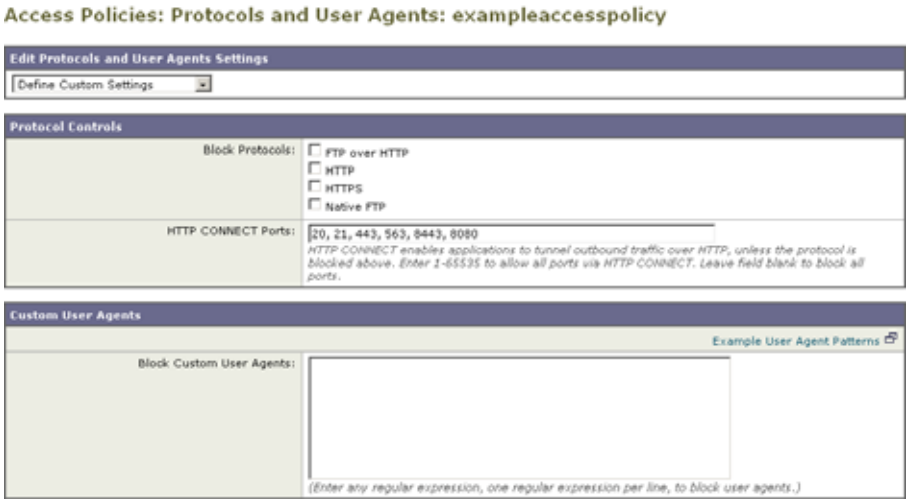
プロトコルおよびユーザ エージェント

[アクセス ポリシー（Access Policies）] > [ユーザ エージェント（Protocols and User Agents）] ページの [プロトコルとユーザエージェント（Protocols and User Agents）] 設定を使用して、ポリシー グループによるプロトコルへのアクセスを制御したり、ユーザ エージェントとも呼ばれる特定のクライ

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）のブロックを設定したりできます。また、特定のポートで 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。

ユーザ エージェントのブロックの詳細については、「特定のアプリケーションおよびプロトコルのブロック」（P.9-13）を参照してください。

図 9-4　　プロトコルとユーザ エージェントの制御の設定



（注）　HTTPS プロキシがイネーブルの場合、HTTPS トランザクションへのアクセスは、復号化ポリシーのみを使用して制御できます。このページのアクセス ポリシーを設定して、HTTPS 接続をブロックすることはできません。

URL カテゴリ

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、カテゴリ別にコンテンツをモニタするか、またはブロック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 サイトのトラフィックを許可するか、モニタするか、ブロックするか、警告するか、またはリダイレクトするかを選択することもできます。カスタム URL カテゴリを使用し、宛先に基づいてブロック リストと許可リストを作成できます。

URL フィルタリング エンジンのイネーブル化については、「URL フィルタリング エンジンの設定」（P.17-4）を参照してください。アクセス ポリシーの URL カテゴリの設定については、「アクセス ポリシー グループの URL フィルタの設定」（P.17-10）を参照してください。

また、[アクセス ポリシー（Access Policies）] > [URL カテゴリ（URL Categories）] ページを使用して、安全な検索とサイト コンテンツ評価を実施することにより、アダルト コンテンツをフィルタリングできます。詳細については、「「アダルト コンテンツのフィルタリング」（P.17-18）」を参照してください。

アプリケーション

[アクセス ポリシー（Access Policies）] > [アプリケーションの表示およびコントロール（Application Visibility and Control）] ページを使用して、Web プロキシを設定し、アプリケーション タイプ別に、または特定の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、ファイル転送など、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に制御を適用できます。

Cisco IronPort Web 使用率制御には、Application Visibility and Control エンジン（AVC エンジン）が含まれているため、特定のアプリケーション タイプをより精密に制御できます。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、アプリケーションで使用される Web トラフィックを深く理解し、管理できるように、Web トラフィックを検査します。

AVC エンジンのイネーブル化については、「AVC エンジンのイネーブル化」（P.18-3）を参照してください。アクセス ポリシーのアプリケーション設定の詳細については、「アプリケーション制御の設定について」（P.18-3）を参照してください。

オブジェクトのブロック

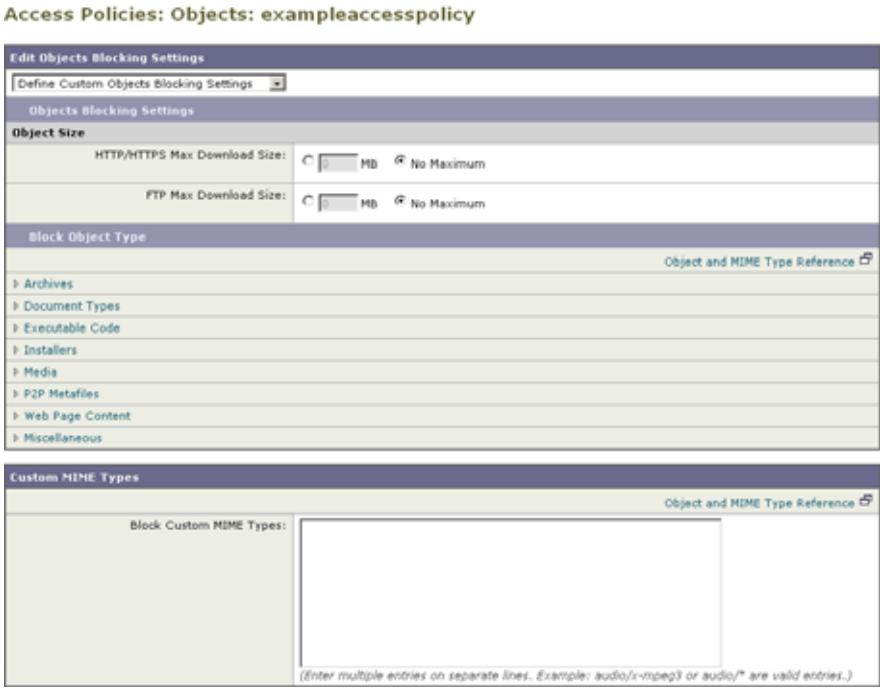
[アクセス ポリシー（Access Policies）] > [オブジェクト（Objects）] ページの設定を使用して、ファイル サイズやファイル タイプなどのファイル特性に基づいて、ファイルのダウンロードをブロックするように Web プロキシを設定できます。

（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。

特定のオブジェクトまたは MIME タイプのブロックの詳細については、「特定のアプリケーションおよびプロトコルのブロック」（P.9-13）を参照してください。

（注）　[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場合があります。すべての Microsoft Office ファイルを確実に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。

図 9-5　オブジェクト タイプのブロック



Web レピュテーションおよびアンチマルウェア

Web レピュテーションおよびアンチマルウェア フィルタリング ポリシーは、コンポーネントごとのグローバル設定を継承します。特定のポリシー グループのフィルタリングとスキャンをカスタマイズするには、[Web レピュテーションおよびマルウェア対策設定（Web Reputation and Anti-Malware Settings）] プルダウン メニューを使用して、マルウェア スキャンの判定に基づいてマルウェア カテゴリのモニタリングまたはブロックをカスタマイズしたり、Web レピュテーション スコアしきい値をカスタマイズしたりできます。

詳細については、「アクセス ポリシーの Web レピュテーションとアンチマルウェア設定」（P.19-11）を参照してください。

特定のアプリケーションおよびプロトコルのブロック

使用するポートに基づいて、特定の種類のアプリケーションをアプライアンスが管理する方法を設定できます。

- **ポート 80。**Web セキュリティ アプライアンスがアクセス ポリシーを使用してこれらのアプリケーションを管理する方法を制御できますが、これは、ポート 80 での HTTP トンネリング経由でアプリケーションにアクセスした場合に限られます。
- **80 以外のポート。**L4 トラフィック モニタを使用して、他のポートでこれらのアプリケーションをブロックできます。

[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）] ページを使用して、より詳細な（ポリシー別）レベルで、これらのタイプのアプリケーションのアクセスとモニタを管理します。よりグローバルにアクセスとモニタを管理するには、L4 トラフィック モニタを使用します。

ポート 80 でのブロッキング

ポート 80 を使用するタイプのアプリケーションへのアクセスをブロックするには、[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）] ページを使用します。[アクセス ポリシー（Access Policies）] ページには、アクセスをブロックする複数の方法が用意されています。次に示す特定のグループ ポリシーの列のいずれかをクリックすると、アクセスをブロックできます。

- Protocols and User Agents
- URL Categories
- Objects

「Chat and Instant Messaging」や「Peer File Transfer」などの定義済みの URL カテゴリへのアクセスをブロックしたり、独自のカスタム URL カテゴリを作成したりできます。「エージェント パターン」またはシグネチャに基づいて、特定のアプリケーションをブロックできます。

追加のアクセス ポリシー グループを作成して、さまざまなアクセス ポリシーに、これらの方法の一部またはすべてを適用できます。追加のアクセス ポリシー グループの作成方法の詳細については、「アクセス ポリシーの作成」（P.9-5）を参照してください。

ポリシー：プロトコルおよびユーザ エージェント

正規表現を使用し、パターンに基づいて、特定のユーザ エージェントをブロックするルールを作成できます。

さまざまなアクセス ポリシーのエージェント パターンに同様に基づいて、アプリケーションへのアクセスをブロックします。

- **ユーザ定義のポリシー**：[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、必要なポリシーの [プロトコルとユーザ エージェント（Protocols and User Agents）] 列の値をクリックします。[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。
- **グローバル ポリシー**：[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、グローバル ポリシーの [プロトコルとユーザ エージェント（Protocols and User Agents）] 列の値をクリックします。

[アクセス ポリシー：プロトコルとユーザ エージェント：*Policy_Name*（Access Policies: Protocols and User Agents: *Policy_Name*）] ページが表示されたら、このページの [ブロックするユーザ エージェント（Block Custom User Agents）] セクションにユーザ エージェント パターン（シグネチャと呼ばれます）を追加します。

図 9-6　ブロックするエージェント パターンの入力

（注）　[ユーザ エージェント パターンの例（Example User Agent Patterns）] リンクをクリックすると、ユーザ エージェント パターンの例のリストが表示されます。

表 9-2 は、一般的なパターンのリストを示します。

表 9-2　一般的なアプリケーション エージェント パターン

アプリケーション	設定での検索	HTTP ヘッダー	シグニチャ
AOL Messenger	要求ヘッダー	User-Agent	Gecko/
BearShare	応答ヘッダー	Server	BearShare
BitTorrent	要求ヘッダー	User-Agent	BitTorrent
eDonkey	要求ヘッダー	User-Agent	e2dk
Gnutella	要求ヘッダー	User-Agent	Gnutella Gnucleus
Kazaa	要求ヘッダー	P2P-Agent	Kazaa Kazaaclient:
Kazaa	要求ヘッダー	User-Agent	KazaClient Kazaaclient:
Kazaa	要求ヘッダー	X-Kazaa-Network	KaZaA
Morpheus	応答ヘッダー	Server	Morpheus
MSN Messenger	要求ヘッダー	User-Agent	MSN Messenger
Trillian	要求ヘッダー	User-Agent	Trillian/
Windows Messenger	要求ヘッダー	User-Agent	MSMSGS
Yahoo Messenger	要求ヘッダー	Host	msg.yahoo.com
Yahoo Messenger	要求ヘッダー	User-Agent	ymsgr

これは、包括的なリストではありません。シグニチャは変わる場合があり、新しいアプリケーションが開発されるためです。次の Web サイトなど、さまざまな Web サイトには、追加のシグニチャが掲載されています。

- http://www.user-agents.org/
- http://www.useragentstring.com/pages/useragentstring.php
- http://www.infosyssec.com/infosyssec/security/useragentstrings.shtml

（注）　Cisco IronPort では、これらのどの Web サイトのユーザ エージェントのリストも保持、確認、サポートしていません。

ポリシー：URL カテゴリ

定義済みの「Chat and Instant Messaging」および「Peer File Transfer」カテゴリなど、ブロックする URL のカテゴリを指定できます。まだ定義済みのカテゴリに含まれていない URL を追加する場合は、特定のカスタム URL カテゴリを追加することもできます。そして、ブロックした URL のリストにカスタム カテゴリを追加できます。

URL カテゴリの使用の詳細については、「URL カテゴリ」（P.9-11）を参照してください。

ポリシー：オブジェクト

[アクセス ポリシー：オブジェクト：グローバル ポリシー（Access Policies: Objects: Global Policy）] ページを使用して、一部のピアツーピア ファイルを直接ブロックできます。

[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、必要なポリシーの [オブジェクト（Objects）] 列の値をクリックします。

[ブロックするオブジェクトタイプ（Block Object Type）] セクションで、[P2P メタファイル（P2P Metafiles）] グループのボックスを選択します。カスタム MIME（Multipurpose Internet Mail Extensions）タイプを、[カスタム MIME タイプ（Custom MIME Types）] フィールドに入力して追加できます。たとえば、`application/x-zip` シグネチャを入力すると、ZIP アーカイブ ファイルがブロックされます。

80 以外のポートでのブロック

これらのアプリケーションが 80 以外のポートを使用している場合は、特定のサーバへのアクセスをブロックしたり、クライアントが接続する必要のある IP アドレスへのアクセスをブロックしたりできます。他のポートでこれらのアプリケーションを管理するには、L4 トラフィック モニタを使用します。L4 トラフィック モニタで、特定のポートでのアクセスを制限できます。ただし、制限はグローバルであるため、そのポートのすべてのトラフィックに適用されます。

10
外部プロキシの使用

外部プロキシの使用の概要

Web セキュリティ アプライアンスは、プロキシ対応デバイスで、既存のプロキシ環境内に容易に導入されます。ただし、既存のプロキシ サーバからダウンストリーム（つまり、クライアントの近くに）に配置することを推奨します。

アプライアンスは、複数の既存のアップストリーム プロキシと連携させるように設定できます。[ネットワーク（Network）] > [プロキシ上位（Proxies Upstream）] ページを使用して、アップストリーム プロキシを定義したり、既存の設定を変更したりします。プロキシ グループを定義し、複数のプロキシへの接続時に、ロード バランシングおよびフェールオーバー機能を使用するようにアプライアンスを設定できます。

プロキシ グループを定義したら、ルーティング ポリシーを作成して、クライアントまたはプロキシ グループのメンバーが指定したサーバに Web プロキシが接続されるかどうかどうかを判別します。

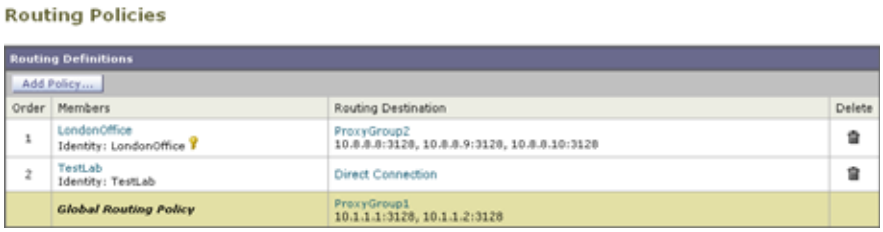
トランザクションのルーティングにルーティング ポリシーを使用する方法については、「アップストリーム プロキシへのトラフィックのルーティング」（P.10-1）を参照してください。外部プロキシの定義の詳細については、「外部プロキシ情報の追加」（P.10-3）を参照してください。

アップストリーム プロキシへのトラフィックのルーティング

Web プロキシがキャッシュからの応答を配信しない場合、クライアント要求を直接宛先サーバまたはネットワークの外部プロキシに送信できます。ルーティング ポリシーを使用して、トランザクションをいつどこに送信するかを指定するルールを作成します。ルーティング ポリシーはクライアント要求を（プロキシ グループで定義された）別のプロキシまたは宛先サーバに渡すかを判別します。「どこからコンテンツを取得しますか?」という内容の質問がされます。高度に分散化されたネットワークを所有している場合は、ルーティング ポリシーを作成する必要がある場合があります。

図 10-1 は、[Web セキュリティ マネージャ（Web Security Manager）] > [ルーティング ポリシー（Routing Policies）] ページのルーティング ポリシーを示します。

図 10-1　ルーティング ポリシー



プロキシ グループに複数の外部プロキシを定義する場合、Web プロキシはグループで定義された異なるプロキシに要求を配布させるロード バランシング技術を使用できます。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）。**Web プロキシは、トランザクションをグループ内にある 1 つの外部プロキシに送信します。一覧表示されている順序でプロキシに接続しようとします。1 つの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しようとします。
- **最少の接続。**Web プロキシは、グループ内の異なるプロキシ間でアクティブな要求がどのくらいあるかを追跡し、現在最も少ない接続数の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。**Web プロキシはハッシュ関数を使用して、グループ内のプロキシに要求を配布します。ハッシュ関数は入力値としてプロキシ ID および URL を使用して、同じ URL の要求が同じ外部プロキシに常に送信されるようにします。
- **最も長い間使われていない。**すべてのプロキシが現在アクティブの場合、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、異なるプロキシ グループのメンバーであることによって、プロキシが受信したトランザクションも考慮することを除いて、ラウンドロビンに類似しています。つまり、プロキシが複数のプロキシ グループに一覧表示されている場合、「最も長い間使われていない」オプションがそのプロキシに対して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。**Web プロキシは、一覧表示された順序でグループ内のすべてのプロキシ間でトランザクションを平等に循環させます。

ルーティング ポリシーの作成の詳細については、「ルーティング ポリシーの作成」（P.10-5）を参照してください。

（注）　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、すべての ID および FTP 要求にだけ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 サーバまたはプロキシのすべてが FTP 接続をサポートするプロキシ グループに直接接続します。

URL カテゴリ メンバーシップ基準でルーティング ポリシーを使用した HTTPS サイトへのアクセス

透過的にリダイレクトされた HTTP 要求では、Web プロキシは宛先サーバに連絡して、サーバ名および所属する URL カテゴリを判別する必要があります。これにより、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ときに、宛先サーバに連絡していないので、HTTPS 要求の URL カテゴリを知ることはできません。Web プロキシが URL カテゴリを認識できなければ、メンバーシップ基準として URL カテゴリを使用するルーティング ポリシーにトランスペアレント HTTPS 要求を照合させることができません。

結果として、透過的にリダイレクトされた HTTPS トランザクションだけが、URL カテゴリでルーティング ポリシー グループのメンバーシップ基準を定義しないルーティング ポリシーに一致します。すべてのユーザ定義のルーティング ポリシーが URL カテゴリによるメンバーシップを定義する場合、トランスペアレント 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 グループに一致します。

外部プロキシ情報の追加

外部プロキシ情報を定義するには、プロキシ グループを作成します。プロキシグループは、グループ内のプロキシに要求を配布するときに使用するプロキシのリスト、接続情報およびロード バランシング技術を定義するオブジェクトです。複数のプロキシ グループを作成し、そのグループ内の複数のプロキシを定義できます。

Web 用 AsyncOS では、同じプロキシ グループに同じプロキシ サーバ情報を複数回入力できます。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で等しくない負荷分散を可能にする必要がある場合があります。

（注）　システムセットアップウィザード では 1 つの既存のプロキシだけを指定できます。AsyncOS では、システムセットアップウィザード で入力する情報を使用して 1 つのプロキシでプロキシ グループを作成します。初期セットアップ後に Web インターフェイスに追加のプロキシを指定できます。

プロキシ グループの作成

ステップ 1　[ネットワークへ移動（Navigate to Network）] > [上位プロキシ（Upstream Proxies）] の順に進み、[グループを追加（Add Group）] をクリックします。

ステップ 2　[名前（Name）] フィールドにプロキシ グループの名前を入力します。

ステップ 3　[プロキシ サーバ（Proxy Servers）] セクションで、少なくとも 1 つの外部プロキシを定義します。

- **a.** [プロキシ アドレス（Proxy Address）] フィールドに、プロキシ サーバのホスト名または IP アドレスを入力します。
- **b.** [ポート（Port）] フィールドに、プロキシへのアクセスに使用するポート番号を入力します。
- **c.** [再接続の試行（Reconnection Attempts）] フィールドに、無視するまで Web プロキシがプロキシ サーバへの接続を試行する回数を入力します。
- **d.** オプションで、[行を追加（Add Row）] をクリックして、別のプロキシ サーバを定義できます。

ステップ 4　[ロード バランシング（Load Balancing）] フィールドでは、グループに複数のプロキシが含まれている場合にプロキシにトランザクションを配布するの Web プロキシが使用するメソッドを選択します。

ロード バランシングのオプションの詳細については、「アップストリーム プロキシへのトラフィックのルーティング」（P.10-1）を参照してください。

ステップ 5　[失敗のハンドリング（Failure Handling）] フィールドでは、グループ内のすべてのプロキシが失敗する場合に、Web プロキシがトランザクションを処理する方法を選択します。

ステップ 6　変更を送信し、保存します。

ルーティング ポリシー グループのメンバーシップの評価

Web プロキシは、クライアント要求に ID を割り当てた後、この要求を他のポリシー タイプと比較して要求を評価し、タイプごとに属するポリシー グループを特定します。失敗した認証によって終了しない要求は、ルーティング ポリシーに対して評価され、どこからデータを取得するかを判別します。

Web プロキシが要求に対してルーティング ポリシー グループを割り当てると、ポリシー グループに設定されたロケーション、つまり設定されたプロキシ グループまたはサーバから直接コンテンツを取得します。

クライアント要求が一致するポリシー 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。このプロセスでは、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。ID グループ メンバーシップの評価に関する詳細については、「ID グループ メンバーシップの評価」（P.8-4）を参照してください。
- **権限を持つユーザ。**割り当てられた ID で認証が必要な場合、ユーザはポリシー グループと照合するために、ルーティング ポリシー グループの認可済みユーザのリストに含まれている必要があります。
- **詳細オプション。**ルーティング 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。オプションの一部（プロキシ ポートや URL カテゴリなど）は、ID 内でも定義できます。詳細オプションが ID に設定されている場合、ルーティング ポリシー グループ レベルには設定できません。

この項では、アプライアンスがクライアント要求をルーティング ポリシー グループに対して照合する方法についての概要を示します。アプライアンスがクライアント要求を照合する方法の詳細については、「ルーティング ポリシー グループへのクライアント要求の照合」（P.10-4）を参照してください。

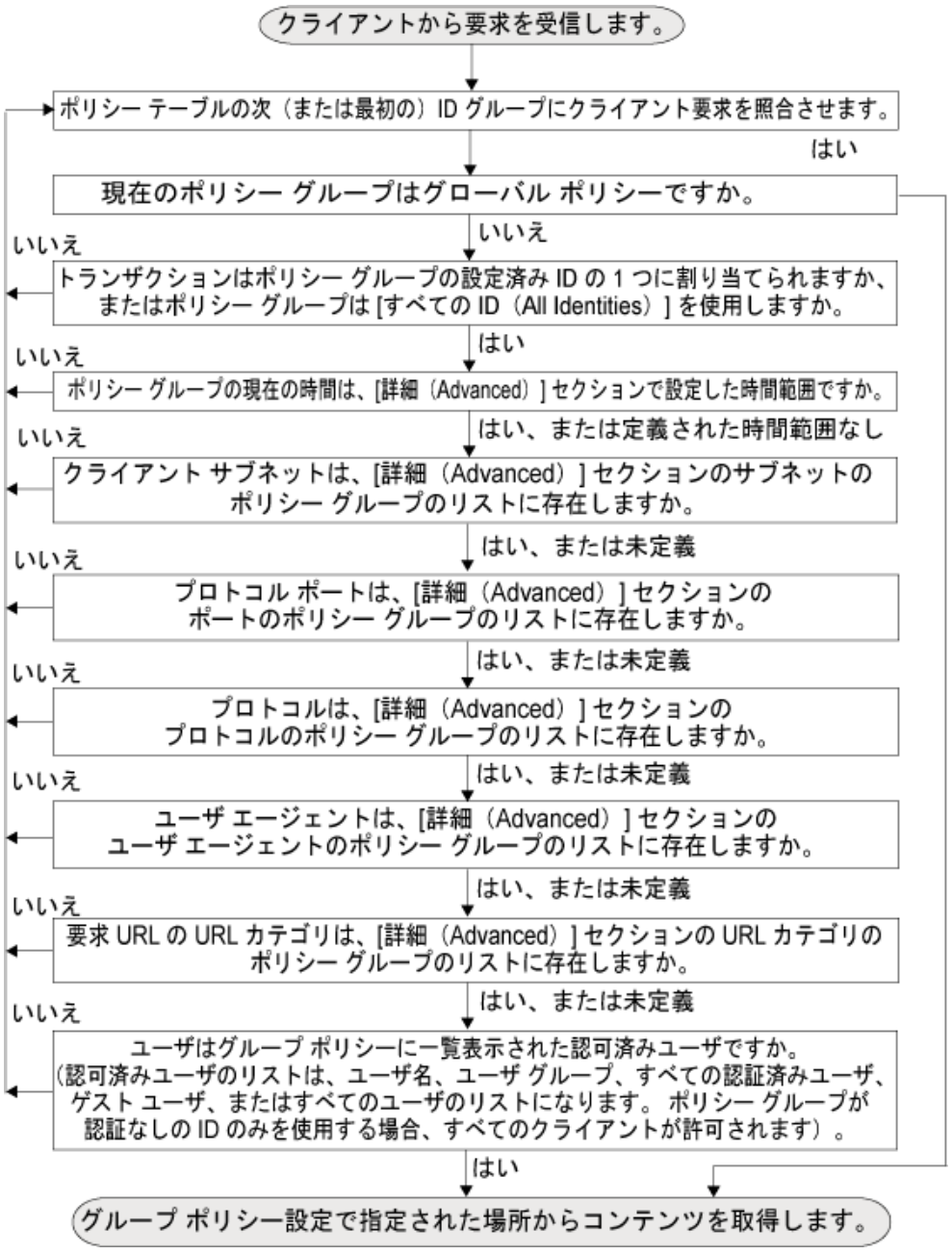
Web プロキシは、ポリシー テーブルの各ポリシー グループを順番に読み取ります。クライアント要求の状態を、最初のグループ ポリシーのメンバーシップ基準と比較します。一致した場合、Web プロキシは、そのポリシー グループのポリシー設定を適用します。

一致しない場合、Web プロキシは、クライアント要求を次のポリシー グループと比較します。ユーザ定義のポリシー グループにクライアント要求が一致するまでこのプロセスを継続します。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、クライアント要求をポリシー 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。

ルーティング ポリシー グループへのクライアント要求の照合

図 10-2（P.10-5）は、Web プロキシがルーティング ポリシー グループに対してクライアント要求を評価する方法を示します。

図 10-2　ルーティング ポリシーのポリシー グループ フロー ダイアグラム



ルーティング ポリシーの作成

Web プロキシへのアクセスに使用される ID またはポートなどの複数の条件の組み合わせに基づいてルーティング 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。複数の条件を定義した場合、クライアント要求は、ポリシー グループと一致するために、すべての条件を満たす必要があります。

アプライアンスがクライアント要求をポリシー グループと照合する方法の詳細については、「ルーティング ポリシー グループのメンバーシップの評価」（P.10-4）および「ルーティング ポリシー グループへのクライアント要求の照合」（P.10-4）を参照してください。

[Web セキュリティ マネージャ（Web Security Manager）] > [ルーティング ポリシー（Routing Policies）] ページでポリシー グループ メンバーシップを定義します。

ステップ 1　[Web セキュリティ マネージャ（Web Security Manager）] > [ルーティング ポリシー（Routing Policies）] ページの順に進みます。

ステップ 2　[グループを追加（Add Group）] 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 グループ名を入力し、必要に応じて [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、慎重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。

この方法の詳細については、「他のポリシー グループの ID の設定」（P.8-22）を参照してください。

ステップ 6　必要に応じて、[詳細（Advanced）] セクションを拡大し、追加メンバーシップの要件を定義します。

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。

表 10-1 で、ポリシー グループを定義できる詳細オプションについて説明します。

表 10-1　　ポリシー グループの詳細オプション

詳細オプション	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。組み込むプロトコルを選択します。 「All others」は、このオプションの上記に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した場合、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、アウトバウンド マルウェア スキャン、データ セキュリティ、または外部 DLP ポリシーの 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：**このグループ ポリシーに関連付けられた ID がこの拡張設定によって ID を定義する場合、これは非 ID ポリシー グループ レベルでは設定できません。
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：**このポリシー グループに関連付けられた ID によってアドレスでそのメンバーシップが定義されている場合は、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）	定義された時間範囲でポリシー 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。[時間範囲（Time Range）] フィールドから時間の範囲を選択します。次に、このポリシー グループが、指定した時間の範囲内と範囲外のどちらを適用するかを選択します。 時間ベースのポリシーの作成の詳細については、「時間ベースのポリシーの使用」（P.7-9）を参照してください。 時間範囲の作成の詳細については、「時間範囲の作成」（P.7-10）を参照してください。

表 10-1　ポリシー グループの詳細オプション （続き）

詳細オプション	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 :** このグループ ポリシーに関連付けられた ID がこの拡張設定によって ID を定義する場合、これは非 ID ポリシー グループ レベルでは設定できません。
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。 ユーザ エージェント ベースのポリシーの作成の詳細については、「ユーザ エージェント ベースのポリシーの使用」（P.7-11）を参照してください。 **注 :** このグループ ポリシーに関連付けられた ID がこの拡張設定によって ID を定義する場合、これは非 ID ポリシー グループ レベルでは設定できません。
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。詳細については、「「セキュア モビリティの実現の概要」（P.14-1）」を参照してください。

ステップ 8　変更を送信します。

ステップ 9　ルーティング ポリシー グループ制御設定を設定して、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。

新しいポリシー グループは、各管理設定のオプションを設定するまでは、グローバル ポリシー グループ設定を自動的に継承します。詳細については、「「アップストリーム プロキシへのトラフィックのルーティング」（P.10-1）」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。

11
HTTPS トラフィックの処理

HTTPS トラフィックの処理の概要

HTTPS トラフィックは暗号化されます。Web プロキシは、「中間者」として機能し、暗号化された HTTPS トラフィックをパススルーできますが、コンテンツが復号化されない限り、アクセス ポリシー内に含まれるコンテンツ ベースのルールを適用できません。たとえば、実行可能ファイルをブロックすることも、マルウェアをスキャンすることもできません。HTTPS プロキシは、HTTPS トラフィックを復号化し、アクセス ポリシーに渡して、コンテンツ ベースのポリシーを適用することができます。その後、Web プロキシは、復号化された HTTPS コンテンツにアクセス ポリシーを適用します。

HTTPS プロキシがイネーブルの場合、アクセス ポリシー内の HTTPS 固有のルール（「HTTPS トラフィックをブロックする」など）はディセーブルになります。Web プロキシは、HTTP 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。

復号化ポリシーで、モニタ、ドロップ、パス スルー、または復号化の対象となる HTTPS 接続が指定されます。

（注）　**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。シスコでは、管理者が Web セキュリティ アプライアンスこの機密情報の取り扱いに注意することを推奨します。

ログに保存する URI テキストの量は、`advancedproxyconfig` CLI コマンドと `HTTPS` サブ コマンドを使用して構成できます。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。ログに保存する URI テキストの量は、

advancedproxyconfig CLI コマンドと HTTPS サブ コマンドを使用して設定できます。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。

作業	コメント
HTTPS プロキシをイネーブルにする	[HTTPS プロキシを有効にする（Enable HTTPS proxy）] を選択すると、HTTPS トラフィックの復号化と処理がイネーブルになります。
証明書と秘密キーを生成またはアップロードする	証明書と秘密キーにより、コンテンツを復号化するために必要な信頼性が提供されます。
信頼された証明書とブロックされた証明書を管理する	長期にわたって、信頼された証明書とブロックされた証明書のリストを管理します。
無効な証明書と失効した証明書の処理を設定する	無効な、または失効した証明書を使用する HTTPS 接続をドロップ、復号化、またはモニタするかどうかを指定します。
復号化ポリシーを作成する	HTTPS 接続をモニタ、ドロップ、パススルー、または復号化するタイミングを指定します。

復号化ポリシー

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。

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。

- **[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。
- **[ドロップ（Drop）]。**アプライアンスは接続をドロップします。サーバに接続要求を渡しません。アプライアンスは接続をドロップしたことをユーザに通知しません。組織が許容する使用ポリシーをユーザがバイパスできるサードパーティ プロキシへの接続をドロップすることができます。
- **[通過（Pass through）]。**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。有名な銀行や金融機関などの信頼できるセキュア サイトへの接続をパス スルーできます。
- **[復号（Decrypt）]。**アプライアンスは、接続を許可しますが、トラフィックの内容を検査します。トラフィックを復号化、プレーン テキスト HTTP 接続であるかのように、復号化されたトラフィックにアクセス ポリシーを適用します。接続を復号化し、アクセス ポリシーを適用することにより、トラフィックをスキャンしてマルウェアを検出できます。gmail や hotmail などのサードパーティ電子メール プロバイダーへの接続を復号化できます。アプライアンスが HTTPS トラフィックを復号化する方法の詳細については、「証明書」（P.11-3）を参照してください。

Monitor 以外のすべてのアクションは、Web プロキシがトランザクションに適用する最終アクションです。最終アクションは、Web プロキシが他の管理設定に対してトランザクションを評価することを停止する操作です。

たとえば、復号化ポリシーが、無効なサーバ証明書をモニタするように設定されている場合、Web プロキシは、サーバにある証明書が無効である場合の HTTPS トランザクションの処理方法についての最終決定を行いません。復号化ポリシーが、Web レピュテーション スコアが低いサーバをブロックするように設定されている場合は、レピュテーション スコアが低いサーバに対する要求がすべて、URL カテゴリ操作を考慮せずにドロップされます。

（注）　シスコでは、一般的な復号化ポリシー グループを少数作成して、すべてのユーザ、またはネットワーク上の少数の大規模なグループのユーザに適用することを推奨しています。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。アクセス ポリシー グループの詳細については、「トランザクション要求のブロック、許可、またはリダイレクト」（P.9-1）を参照してください。

図 11-5（P.11-22）は、復号化ポリシーの管理設定を評価するときに、Web プロキシが使用する順序を示しています。図 9-3（P.9-10）は、アクセス ポリシーの管理設定を評価するときに、Web プロキシが使用する順序を示しています。

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と秘密キー ファイルは、PEM 形式である必要があります。

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。組織に使用中の証明書とキーがない場合や、新しい一意の証明書とキーが必要な場合には、証明書とキーを生成できます。
- **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。ネットワーク上のクライアントのマシンにすでにルート証明書がある場合は、証明書とキー ファイルをアップロードできます。
  アップロードする証明書とキー 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。DER 形式の証明書またはキーの PEM 形式への変換の詳細については、「証明書およびキー形式の変換」（P.A-9）を参照してください。

（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」が含まれていることが必要です。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。

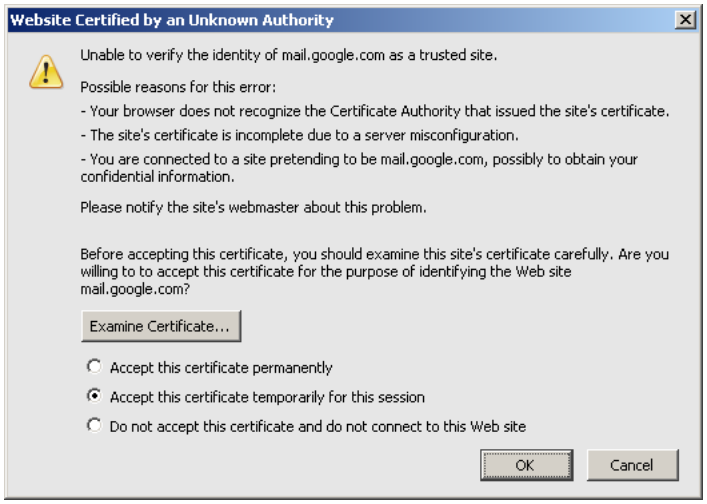
証明書およびキーを生成またはアップロードする方法の詳細については、「HTTPS プロキシのイネーブル化」（P.11-13）を参照してください。

ただし、通常は、アプライアンスで生成またはアップロードす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 アプリケーションに認識されていません。大部分の Web ブラウザではデフォルトで、ユーザが HTTPS 要求を送信すると、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 アプリケーションから表示されます。通常、エラー メッセージの内容は、信頼できる認証局によって Web サイトのセキュリティ証明書が発行されていないか、Web サイトが未知の認証局によって認証されているということです。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）　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。組織が独自のルート認証局を使用する場合は、中間証明書をアップロードすることもできますが、セキュリティ上の理由から、ルート証明書は Web セキュリティ アプライアンスにアップロードしないでください。

図 11-1（P.11-4）は、ユーザが Netscape Navigator を使用して HTTPS 要求を送信したときのエラー メッセージの例を示します。

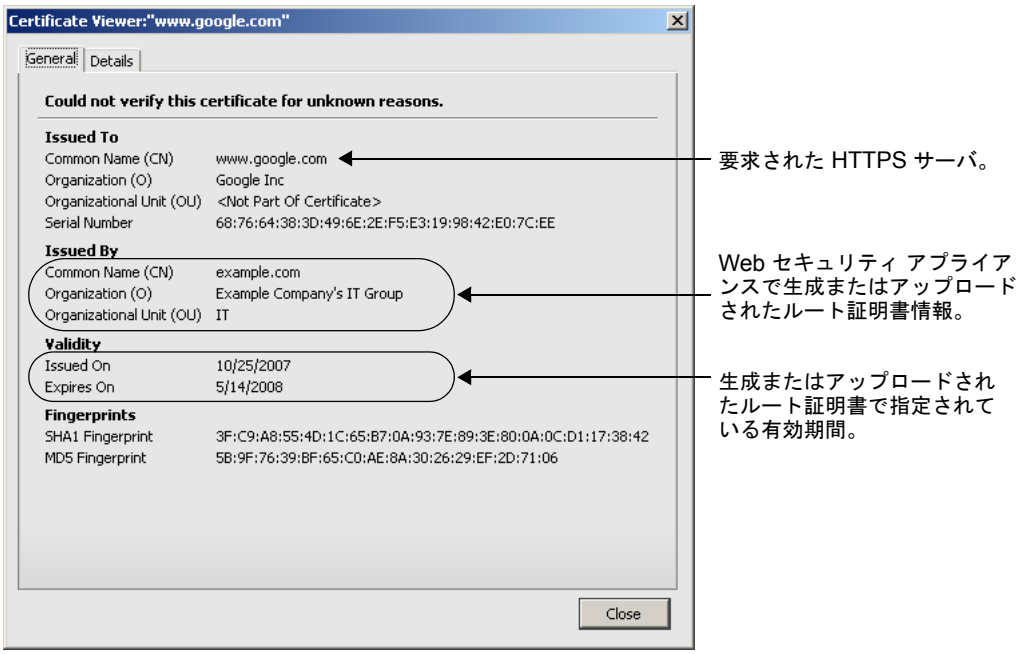
図 11-1　不明な認証局エラー メッセージ



通常、ユーザは証明書を確認し、証明書の情報を使用して、この Web サイトとの安全な接続を許可するかどうかを選択できます。図 11-1 では、[証明書の検証（Examine Certificate）] をクリックすると、証明書の内容を表示できます。

図 11-2（P.11-5）は、アプライアンスが発行したルート証明書の例を示しています。

図 11-2　Web セキュリティ アプライアンスが発行した証明書



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。アプリケーションが使用しているルート証明書を確実に配布するには、[セキュリティ サービス（Security Services）] > [HTTPS プロキシ（HTTPS Proxy）] ページからルート証明書をダウンロードします。[設定の編集（Edit Settings）] をクリックして、[証明書のダウンロード（Download Certificate）] リンクをクリックし、生成またはアップロードされた証明書をダウンロードします。

  他の人がアプライアンスにルート証明書をアップロードしており、クライアント マシンに確実に同じルート証明書が配布されるようにする場合は、アプライアンスからルート証明書をダウンロードします。

（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。

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。

- 次の条件を満たす明示的な要求
  - 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
- 次の条件を満たす透過的な要求
  - 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

AVC エンジンによる復号化

HTTPS プロキシは、Web アプリケーションに対して HTTPS 接続を復号化できます。これにより、AVC エンジンが、HTTPS を使用する Web アプリケーションをより正確に検出およびブロックできるようになります。これらの Web アプリケーションでは、Web ブラウザ、またはインスタント メッセージ アプリケーションなどの他のクライアント アプリケーションを使用する場合があります。

ただし、HTTPS 接続が復号化されるときにすべてのアプリケーションが適切に機能するようにするには、信頼できるルート認証局として、署名用ルート証明書をネットワークのすべてのクライアント マシンに追加します。たとえば、Windows マシンでは、Yahoo Instant Messenger、MSN Messenger、および Google Talk などの多くのインスタント メッセージ クライアント アプリケーションが機能するように、Internet Explorer にルート証明書をインストールする必要があります。

AOL Instant Messenger による復号化

ほとんどの AOL Instant Messenger（AIM）クライアント アプリケーションでは、信頼できる証明書のリストにルート証明書を追加できません。署名用アプライアンス ルート証明書を AIM クライアント アプリケーションに追加できないため、AIM サーバへの HTTPS 接続が復号化されると、AIM ユーザは AIM にログインできません。AIM サーバの復号化は、AIM サーバと同じレピュテーション スコアを持つサーバへのトラフィックを復号化するように Web レピュテーション フィルタが設定されている場合、または、すべてのトラフィックを復号化するように復号化ポリシーが設定されている場合に発生する可能性があります。

ユーザが AIM にログインできるようにするには、AIM サーバへの HTTPS トラフィックが復号化されずに、パススルーするようにする必要があります。

（注） ユーザが AIM にログインすると、すべてのインスタント メッセンジャ トラフィックが HTTP を使用し、設定されたアクセス ポリシーの対象となります。

HTTPS トラフィックを AIM サーバにパススルーするには：

ステップ 1　カスタム URL カテゴリの先頭位置にカスタム URL カテゴリを作成し、次のアドレスを入力します。

- aimpro.premiumservices.aol.com
- bos.oscar.aol.com
- kdc.uas.aol.com
- buddyart-d03c-sr1.blue.aol.com
- 205.188.8.207
- 205.188.248.133

- 205.188.13.36
- 64.12.29.131

ステップ 2　復号化ポリシーを作成し、ステップ 1 で作成されたカスタム URL カテゴリを、ポリシー グループ メンバーシップの一部として使用します。設定されている他の復号化ポリシーに応じて、リストの先頭にこの復号化ポリシーを配置できます。

ステップ 3　すべてのトラフィックがカスタム URL カテゴリにパススルーするように復号化ポリシーを設定します。

ステップ 4　パススルーを、復号化ポリシーのデフォルト アクションとして選択します。

ステップ 5　変更を送信し、保存します。

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。

関連トピック

- 「証明書の検証と HTTPS の復号化の管理」（P.11-7）
- 「無効な証明書の処理の設定」（P.11-11）
- 「証明書失効ステータスのチェックのオプション」（P.11-12）
- 「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」（P.11-12）

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（Drop）]。**アプライアンスは、接続をドロップし、クライアントに通知しません。これは、最も制限レベルの高いオプションです。
- **[復号（Decrypt）]。**アプライアンスは、接続を許可しますが、トラフィックの内容を検査します。トラフィックを復号化、プレーン テキスト HTTP 接続であるかのように、復号化されたトラフィックにアクセス ポリシーを適用します。

- **[モニタ（Monitor）]。**アプライアンスは接続をドロップしませんが、代わりに、サーバ要求を復号化ポリシー グループと比較し続けます。無効なサーバ証明書をモニタしているときは、証明書内のエラーが維持されたまま、エンド ユーザに渡されます。これは、最も制限レベルの低いオプションです。

関連項目

- 「証明書」（P.11-3）

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。証明書の通常名は「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 ユーザが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。

HTTPS 証明書の検証およびコンテンツの復号化のイネーブル化

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

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　アプライアンスが HTTPS プロキシとして動作するポートを指定します。ポート番号が複数ある場合は、カンマで区切ります。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。アプライアンスが HTTP プロキシとして動作するポートの指定については、「Web プロキシの設定」（P.5-3）を参照してください。

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。

関連項目

- 「ルート証明書およびキーのアップロード」（P.11-9）
- 「証明書およびキーの生成」（P.11-10）

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 証明書の検証およびコンテンツの復号化のイネーブル化」（P.11-8）。

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

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。

（注）　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 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。また、秘密キー 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 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 証明書の検証およびコンテンツの復号化のイネーブル化」（P.11-8）。

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

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。Web セキュリティ アプライアンスは、入力したデータを含む証明書を生成し、キーを生成します。

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）[証明書署名要求をダウンロード（Download Certificate Signing Request）] リンクをクリックします。これで、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、保存します。

関連項目

- 「ルート証明書およびキーのアップロード」（P.11-9）。

復号化オプションの設定

はじめる前に

- 「HTTPS 証明書の検証およびコンテンツの復号化のイネーブル化」（P.11-8） 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）] ページに移動します。

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。

無効な証明書の処理の設定

はじめる前に

- 「HTTPS 証明書の検証およびコンテンツの復号化のイネーブル化」（P.11-8）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）] ページに移動します。

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応答を定義します。

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	**（注）**　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。これは、「中央者攻撃」の間、またはサーバが別の URL に要求をリダイレクトしたときに発生する可能性があります。たとえば、http://mail.google.com は http://www.gmail.com にリダイレクトされます。Web プロキシがホスト名の照合を実行できるのは、明示的な転送モードで展開されている場合のみです。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、署名を検証または復号化できないなどの問題が発生しました。

証明書エラーのタイプ	説明
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。
プロキシ応答タイプ	**説明**
ドロップ	接続をドロップします。
復号化	コンテンツを復号化して、HTTP 接続であるかのようにアクセス ポリシーを適用します。
モニタ	この証明書エラーに基づいて、決定的なアクションを実行しないでください。検証サービスを続行します。

無効なサーバ証明書の処理の詳細については、「証明書」（P.11-3）を参照してください。

ステップ 4　変更を送信し、保存します。

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特定するために、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 アプライアンスが、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。

関連トピック

- 「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」（P.11-12）
- 「無効な証明書の処理の設定」（P.11-11）

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」（P.11-13）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、表 11-1 に示すように設定します。

表 11-1　OCSP 設定フィールド

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

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、[セキュリティ サービス（Security Services）] > [HTTPS プロキシ（HTTPS Proxy）] ページで 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、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 メンバーシップが HTTPS で定義されており、一部のアクセス ポリシーが HTTPS をブロックしている場合は、HTTPS プロキシを有効にすると、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。

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。

（注）　カスタムルート権限証明書のインポートについては、「信頼できるルート証明書」（P.11-23）を参照してください。

HTTPS プロキシをイネーブルにするには：

ステップ 1　[セキュリティ サービス（Security Services）] > [HTTPS プロキシ（HTTPS Proxy）] ページに移動し、[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）　WCCP を使用した展開では、HTTP および HTTPS ポートを合わせたポート エントリの最大数は 30 です。エントリ数を減らすためにポート範囲を使用できます。ポート番号およびポート範囲の両方を使用できます。例：443, 3128, 14001-14015。

ステップ 5　[HTTPS 透過的要求（HTTPS Transparent Request）] セクションで、IP ベースのサロゲートでアイデンティティを使用して認証された HTTP 要求の前に受信する、リダイレクトされた HTTPS トランザクションを Web プロキシが透過的に処理する方法を選択します。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。

詳細については、「認証が HTTP 要求を介した HTTPS および FTP に影響を与える仕組みについて」（P.8-6）を参照してください。

（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 6　[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。

この設定をイネーブルにすると、HTTPS を使用するアプリケーションを検出する Web プロキシの精度が向上します。この設定は、復号化ポリシーで設定されている Web レピュテーション フィルタによる「パススルー」決定より優先されます。ただし、URL カテゴリの決定は適用されます。

（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。

ステップ 7　変更を送信し、保存します。

関連項目

- 「証明書」（P.11-3）
- 「AVC エンジンによる復号化」（P.11-6）

復号ポリシー グループ メンバーシップの評価

Web プロキシは、クライアント要求に ID を割り当てた後、この要求を他のポリシー タイプと比較して要求を評価し、タイプごとに属するポリシー グループを特定します。

Web プロキシは、クライアント要求のポリシー グループのメンバーシップに基づいて、設定されたポリシー制御設定をクライアント要求に適用します。

クライアント要求が一致するポリシー グループを特定するために、Web プロキシは、グループ メンバーシップの次の要素について考慮します。

- **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。ID グループ メンバーシップの評価に関する詳細については、「ID グループ メンバーシップの評価」（P.8-4）を参照してください。
- **権限を持つユーザ。**割り当てられた ID に認証が必要な場合、ユーザは、グループ ポリシーに一致するために、復号化ポリシー グループ内の権限を持つユーザのリストに含まれている必要があります。
- **高度なオプション。**復号化ポリシー グループ メンバーシップの複数の高度なオプションを設定できます。オプションの一部（プロキシ ポートや URL カテゴリなど）は、ID 内でも定義できます。高度なオプションを ID 内で設定すると、復号化ポリシー グループ レベルでは設定できなくなります。

このセクションでは、アプライアンスがクライアント要求と復号化ポリシー グループを照合する方法についての概要を示します。アプライアンスがクライアント要求を照合する方法の詳細については、「クライアント要求の復号ポリシー グループとの照合」（P.11-16）を参照してください。

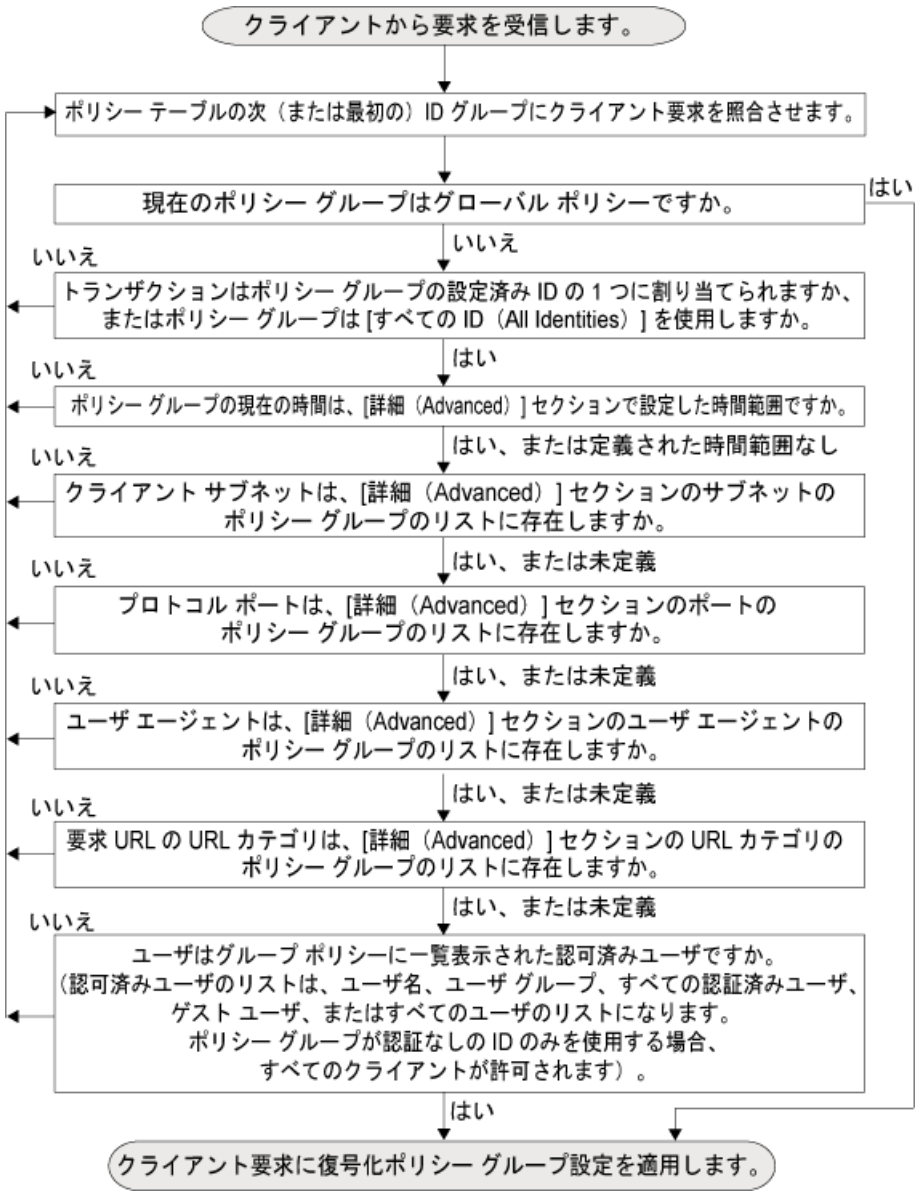
Web プロキシは、ポリシー テーブルの各ポリシー グループを順番に読み取ります。クライアント要求の状態を、最初のグループ ポリシーのメンバーシップ基準と比較します。一致した場合、Web プロキシは、そのポリシー グループのポリシー設定を適用します。

一致しない場合、Web プロキシは、クライアント要求を次のポリシー グループと比較します。ユーザ定義のポリシー グループにクライアント要求が一致するまでこのプロセスを継続します。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、クライアント要求をポリシー 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。

クライアント要求の復号ポリシー グループとの照合

図 11-3（P.11-16）は、Web プロキシが復号化ポリシー グループに対してクライアント要求を評価する方法を示します。

図 11-3　復号化ポリシーのポリシー グループ フロー ダイアグラム



復号ポリシーの作成

宛先サイトのアイデンティティや URL カテゴリなど、複数の条件の組み合わせに基づいて復号化ポリシー 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。複数の条件を定義した場合、クライアント要求は、ポリシー グループと一致するために、すべての条件を満たす必要があります。

アプライアンスがクライアント要求をポリシー グループと照合する方法の詳細については、「復号ポリシー グループ メンバーシップの評価」（P.11-15）および「クライアント要求の復号ポリシー グループとの照合」（P.11-16）を参照してください。

ポリシー グループ メンバーシップは、[Web セキュリティ マネージャ（Web Security Manager）] > [復号化ポリシー（Decryption Policies）] ページで定義します。

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

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

ステップ 3　[ポリシー名（Policy Name）] フィールドにポリシー グループ名を入力し、必要に応じて [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、慎重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。

（注）　アイデンティティに認証が必要な場合は、ユーザが HTTPS サーバに接続しようとしたときに認証情報が表示されないことがあります。HTTPS と認証の連携方法の詳細については、「認証が HTTP 要求を介した HTTPS および FTP に影響を与える仕組みについて」（P.8-6）を参照してください。

この方法の詳細については、「他のポリシー グループの ID の設定」（P.8-22）を参照してください。

ステップ 6　必要に応じて、[詳細（Advanced）] セクションを拡大し、追加メンバーシップの要件を定義します。

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。

表 11-2 は、復号化ポリシー グループに設定できる高度なオプションの説明です。

表 11-2　復号化ポリシー グループの高度なオプション

高度なオプション	説明
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透過的にアプライアンスにリダイレクトされる場合にプロキシ ポートでポリシー グループ メンバーシップを定義すると、一部の要求が拒否される場合があります。 **注：**このグループ ポリシーに関連付けられた ID がこの拡張設定によって ID を定義する場合、これは非 ID ポリシー グループ レベルでは設定できません。
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：**このポリシー グループに関連付けられた ID によってアドレスでそのメンバーシップが定義されている場合は、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）	定義された時間範囲でポリシー 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。[時間範囲（Time Range）] フィールドから時間の範囲を選択します。次に、このポリシー グループが、指定した時間の範囲内と範囲外のどちらを適用するかを選択します。 時間ベースのポリシーの作成の詳細については、「時間ベースのポリシーの使用」（P.7-9）を参照してください。 時間範囲の作成の詳細については、「時間範囲の作成」（P.7-10）を参照してください。
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：**このグループ ポリシーに関連付けられた ID がこの拡張設定によって ID を定義する場合、これは非 ID ポリシー グループ レベルでは設定できません。

表 11-2　復号化ポリシー グループの高度なオプション （続き）

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。 ユーザ エージェント ベースのポリシーの作成の詳細については、「ユーザ エージェント ベースのポリシーの使用」（P.7-11）を参照してください。 **注：**このグループ ポリシーに関連付けられた ID がこの拡張設定によって ID を定義する場合、これは非 ID ポリシー グループ レベルでは設定できません。
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。詳細については、「セキュア モビリティの実現の概要」（P.14-1）を参照してください。

ステップ 8　変更を送信します。

ステップ 9　復号化ポリシー グループの管理を設定して、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。

新しいポリシー グループは、各管理設定のオプションを設定するまでは、グローバル ポリシー グループ設定を自動的に継承します。詳細については、「HTTPS トラフィックの制御」（P.11-20）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。

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。

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。たとえば、透過 HTTPS トランザクションでは、AsyncOS が、HTTPS クライアント ヘッダー内のユーザ名にアクセスできないため、ユーザ名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 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。

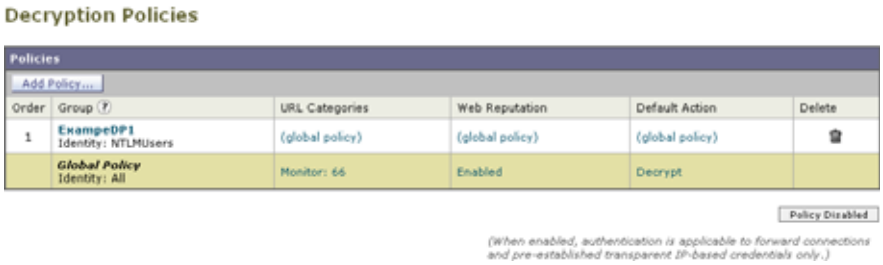
HTTPS トラフィックの制御

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で、アプライアンスが接続を復号化するか、ドロップするか、またはパススルーするかが決定されます。アプライアンスが HTTPS 要求で実行可能な処理の詳細については、「HTTPS トラフィックの処理の概要」（P.11-1）を参照してください。

[Web セキュリティ マネージャ（Web Security Manager）] > [復号化ポリシー（Decryption Policies）] ページで、復号化ポリシー グループの管理を設定します。

図 11-4 は、復号化ポリシー グループの管理を設定する場所を示します。

図 11-4　　復号化ポリシー テーブル



次の設定で、HTTPS 接続で実行するアクションを決定できます。

- **URL カテゴリ。**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。URL フィルタの使用方法の詳細については、「URL フィルタ」（P.17-1）を参照してください。URL カテゴリの設定の詳細については、「復号化ポリシー グループの URL フィルタの設定」（P.17-12）を参照してください。

（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。**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。Web レピュテーション スコアの使用方法の詳細については、「復号化ポリシーの Web レピュテーション」（P.19-4）を参照してください。
- **デフォルト アクション。**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。

復号化ポリシー グループが HTTPS 要求に割り当てられた後、ポリシー グループの管理設定が評価され、HTTPS 接続要求を復号化するか、ドロップするか、またはパススルーするかが決定されます。HTTPS 要求に復号化ポリシー グループを割り当てる方法の詳細については、「ポリシー グループ メンバーシップ」（P.7-7）を参照してください。

図 11-5（P.11-22）は、アプライアンスが特定の復号化ポリシーを HTTPS 要求に割り当てた後に、その要求で実行するアクションを決定する方法を示します。

図 11-5　復号化ポリシー アクションの適用

図 11-5 は、宛先サーバの Web レピュテーション スコアに関連する 2 つの決定ポイントを示します。サーバの Web レピュテーション スコアが評価されるのは 1 回だけですが、その結果は、決定フローの 2 つのポイントで適用されます。

たとえば、Web レピュテーション スコアのドロップ アクションは、定義済みの URL カテゴリに定義されているあらゆるアクションに優先することに注意してください。

（注）　設定されたデフォルト アクションが HTTPS 要求の処理に影響するのは、Web レピュテーション フィルタリングがイネーブルでない場合、または、イネーブルであるが、サーバに割り当てられたスコアがなく、スコアのないサーバのアクションがモニタすることである場合のみです。

特定の 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。

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。

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　[信頼済み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 [実行（Submit）] して [確定する（Commit）] します。

[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。

関連項目

- 「HTTPS プロキシのイネーブル化」（P.11-13）

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　[信頼済み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 [実行（Submit）] して [確定する（Commit）] します。

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。たとえば、「GET https://ftp.example.com」です。

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。

12
Outbound Malware Scanning

この章の構成は、次のとおりです。

Outbound Malware Scanning の概要

マルウェアは広範囲にわたり、かつ永続的であり、困ったことに、通常はネットワーク内のコンピュータへのアクセスを検出します。ユーザは、プロジェクトでコラボレートし、生産性を向上させるために、顧客やパートナーとの連携がますます増加しています。このようなコラボレーションの増大によって、情報セキュリティの専門家は、誤って感染した主要パートナーから社内システムにマルウェアを感染させ、その結果レピュテーションに悪影響を及ぼす事態を防ぐための方法を究明するという課題を突きつけられています。

Web セキュリティ アプライアンスは、ネットワーク内のコンピュータでアクティブ化しているマルウェアがネットワークから漏出し、顧客やパートナーに影響を与えるのを防止できるアウトバウンド マルウェア スキャン機能を提供します。

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出る際にリアル タイムでスキャンします。Cisco IronPort DVS エンジンとの連携により、Web セキュリティ アプライアンスを使用してユーザが無意識のうちに悪意のあるデータをアップロードするのを防止できます。

悪意のあるデータがネットワークから漏出しないようにするために、Web セキュリティ アプライアンスには アウトバウンド マルウェア スキャン ポリシー グループが用意されています。マルウェアをスキャンするアップロード、スキャンに使用するアンチマルウェア 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します。

アンチマルウェア スキャンの詳細については、「アンチマルウェア スキャンの概要」（P.19-4）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

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 サイトがエンド ユーザにブロック ページを表示するわけではありません。たとえば、Web 2.0 の Web サイトは、静的 Web ページの代わりに Javascript を使用して動的コンテンツを表示し、ブロック ページを表示することはありません。ユーザは、悪意のあるデータをアップロードしないように適切にブロックされますが、この情報が Web サイトを通じて通知されない場合があります。

ポリシー グループ

アウトバウンド マルウェア スキャン ポリシーは、Web プロキシが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）に対する HTTP 要求および復号化された 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を含む HTTP または復号化された HTTPS 要求です。

Web プロキシがアップロード要求を受信すると、要求を アウトバウンド マルウェア スキャン 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に、要求をモニタするか、ブロックするかを判定するポリシー グループの設定済み制御設定と要求を比較します。アウトバウンド マルウェア スキャン ポリシーが要求をモニタするように判定した場合、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まります。

アウトバウンド マルウェアに基づいて要求をブロックするように アウトバウンド マルウェア スキャン ポリシーを設定する方法の詳細については、「アウトバウンド マルウェア スキャン ポリシーを使用したアップロード要求の制御」（P.12-7）を参照してください。

（注）　サイズがゼロ（0）バイトのファイルをアップロードしようとするアップロード要求は、アウトバウンド マルウェア スキャン ポリシーに対して評価されません。

アウトバウンド マルウェア スキャン ポリシー グループ メンバーシップの評価

各クライアント要求は ID に割り当てられ、他のポリシー タイプに対して評価されて、タイプごとに属するポリシー グループが判定されます。Web プロキシは、アウトバウンド マルウェア スキャン 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 グループのメンバーシップに基づいて、設定されたポリシー制御設定をクライアント要求に適用します。

クライアント要求が一致するポリシー 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。このプロセスでは、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、認証に失敗し、ゲスト アクセスが許可されるか、または認証に失敗し、終了します。ID グループ メンバーシップの評価に関する詳細については、「ID グループ メンバーシップの評価」（P.8-4）を参照してください。
- **権限を持つユーザ。**割り当てられた ID で認証が必要な場合、ユーザは、アウトバウンド マルウェア スキャン ポリシー グループの権限を持つユーザのリストに含まれ、グループ ポリシーに一致する必要があります。権限を持つユーザのリストには、任意の指定したグループまたはユーザ、または ID がゲスト アクセスを許可する場合はゲスト ユーザを指定できます。
- **拡張オプション。**アウトバウンド マルウェア スキャン ポリシー グループ メンバーシップに対して複数の拡張オプションを設定できます。一部のオプション（プロキシ ポートおよび URL カテゴリなど）は、ID 内に定義することもできます。ID 内に拡張オプションを設定する場合、アウトバウンド マルウェア スキャン 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 アウトバウンド マルウェア スキャン ポリシー グループと照合する方法の概要を説明します。Web プロキシがクライアント要求を正確に照合する仕組みに関する詳細については、「クライアント要求と アウトバウンド マルウェア スキャン ポリシー グループとの照合」（P.12-3）を参照してください。

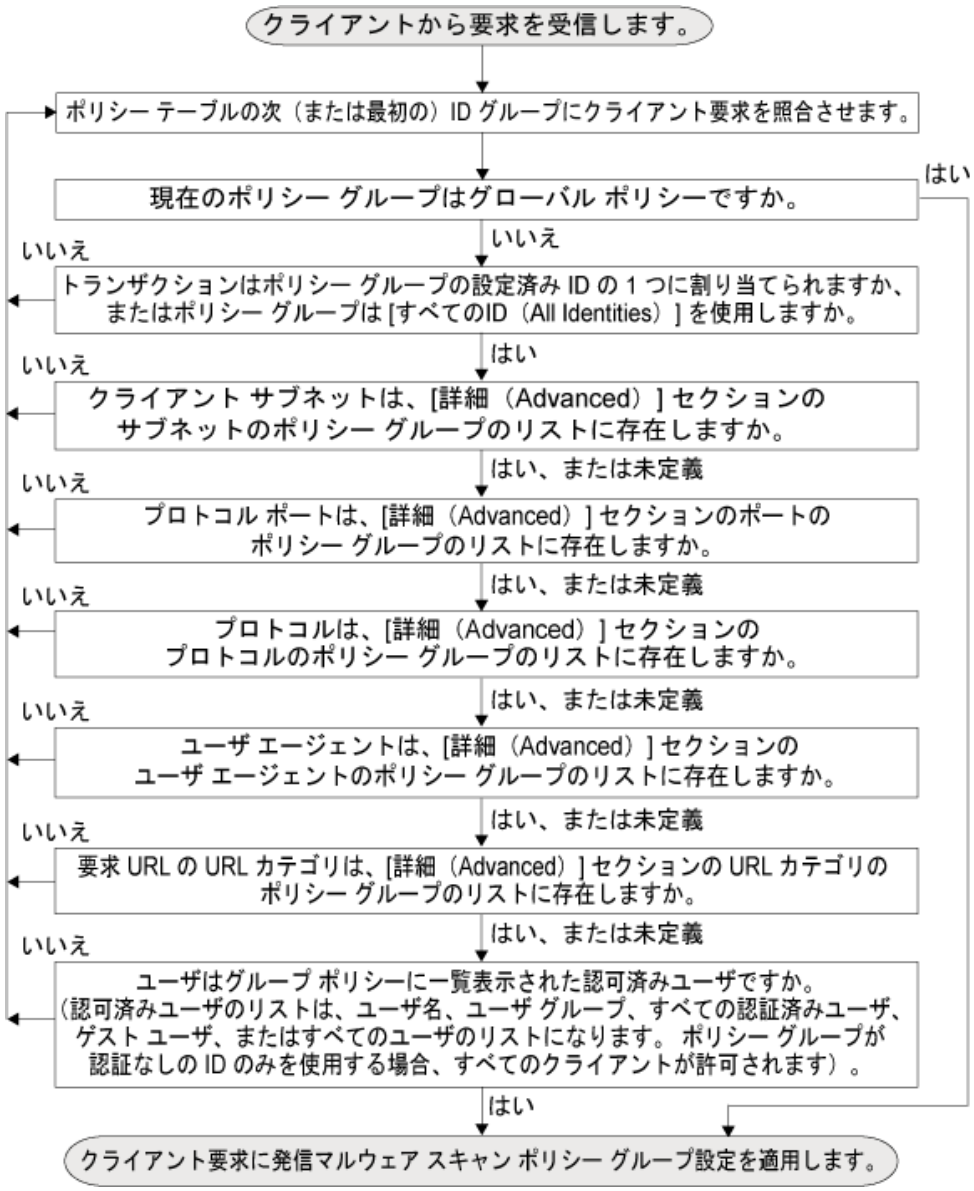
Web プロキシは、ポリシー テーブルの各ポリシー グループを順番に読み取ります。次に、アップロード要求のステータスを最初のポリシー グループのメンバーシップの基準と比較します。一致した場合、Web プロキシは、そのポリシー グループのポリシー設定を適用します。

一致しない場合、Web プロキシは、アップロード要求を次のポリシー グループと比較します。アップロード要求がユーザ定義のポリシー グループに一致するまで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。アップロード要求がポリシー グループまたはグローバル ポリシー グループと一致すると、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。

クライアント要求と アウトバウンド マルウェア スキャン ポリシー グループとの照合

図 12-1（P.12-4）は、Web プロキシがアップロード要求を アウトバウンド マルウェア スキャン グループに対して評価する方法を示します。

図 12-1　アウトバウンド マルウェア スキャン ポリシーのポリシー グループ フロー図



ポリシーアウトバウンド マルウェア スキャンの作成

宛先サイトの URL カテゴリの 1 つまたは複数の ID など、複数の条件の組み合わせに基づいて アウトバウンド マルウェア スキャン 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。複数の条件を定義する場合、アップロード要求はポリシー グループに一致するすべての条件を満たしている必要があります。ただし、アップロード要求は設定された ID の 1 つのみと一致するが必要です。

Web プロキシがアップロード要求をポリシー グループと照合する方法の詳細については、「アウトバウンド マルウェア スキャン ポリシー グループ メンバーシップの評価」（P.12-2）と「クライアント要求と アウトバウンド マルウェア スキャン ポリシー グループとの照合」（P.12-3）を参照ください。

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）] ページに移動し、[ポリシーを追加（Add Policy）] をクリックします。

ステップ 2　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 3　[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、各グループの論理的な順序を指定する必要があります。ポリシー グループが正しく照合されるように、慎重に順序を指定してください。

ステップ 4　[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 つまたは複数の ID グループを選択します。

詳細については、「他のポリシー グループの ID の設定」（P.8-22）を参照してください。

ステップ 5　必要に応じて、[詳細（Advanced）] セクションを拡大し、追加メンバーシップの要件を定義します。

ステップ 6　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。

表 12-1 は、アウトバウンド マルウェア スキャン ポリシー グループに設定できる拡張オプションについて説明します。

表 12-1　アウトバウンド マルウェア スキャン ポリシー グループの拡張オプション

拡張オプション	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。組み込むプロトコルを選択します。 「All others」は、このオプションの上記に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した場合、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、アウトバウンド マルウェア スキャン、データ セキュリティ、または外部 DLP ポリシーの 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に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のみ、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：**このグループ ポリシーに関連付けられた ID がこの拡張設定によって ID を定義する場合、これは非 ID ポリシー グループ レベルでは設定できません。
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 として定義されている可能性のあるアドレスを使用するように選択するか、またはここで特定のアドレスを入力できます。 **注：**このグループ ポリシーに関連付けられた ID がアドレスによってメンバーシップを定義している場合、このグループ ポリシーでは、ID で定義された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。
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：**このグループ ポリシーに関連付けられた ID がこの拡張設定によって ID を定義する場合、これは非 ID ポリシー グループ レベルでは設定できません。

表 12-1　アウトバウンド マルウェア スキャン ポリシー グループの拡張オプション （続き）

拡張オプション	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。 ユーザ エージェント ベースのポリシーの作成の詳細については、「ユーザ エージェント ベースのポリシーの使用」（P.7-11）を参照してください。 **注：**このグループ ポリシーに関連付けられた ID がこの拡張設定によって ID を定義する場合、これは非 ID ポリシー グループ レベルでは設定できません。
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。詳細については、「「セキュア モビリティの実現の概要」（P.14-1）」を参照してください。

ステップ 7　変更を送信します。

ステップ 8　アウトバウンド マルウェア スキャン 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 アウトバウンド マルウェア スキャン ポリシー グループは、各制御設定のオプションを設定するまで、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。詳細については、「「アウトバウンド マルウェア スキャン ポリシーを使用したアップロード要求の制御」（P.12-7）」を参照してください。

ステップ 9　変更を送信し、保存します。

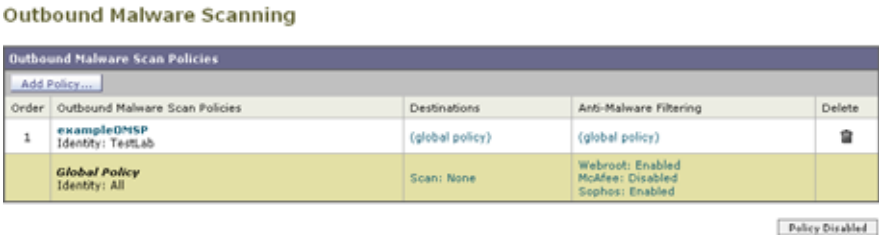
アウトバウンド マルウェア スキャン ポリシーを使用したアップロード要求の制御

各アップロード要求は、アウトバウンド マルウェア スキャン 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。アウトバウンド マルウェア スキャン ポリシー グループの制御設定は、アップロード要求のマルウェアをスキャンするかどうかを判定し、スキャンした場合、ブロックするマルウェアのタイプを決定します。

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すべての情報が提供されます。DLP エンジンは、要求をスキャンし、Web プロキシに判定（ブロックするか、モニタするかのいずれか）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）。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。

図 12-2 は、アウトバウンド マルウェア スキャン ポリシー グループの制御設定を設定できる場所を示します。

図 12-2　アウトバウンド マルウェア スキャン 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）] > [発信マルウェア スキャン（Outbound Malware Scanning）] ページに移動します。

ステップ 2　[接続先（Destinations）] カラムで、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　[接続先設定の編集セクション（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。

図 12-3　Outbound Malware Scanning ポリシーの宛先スキャンの設定

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。

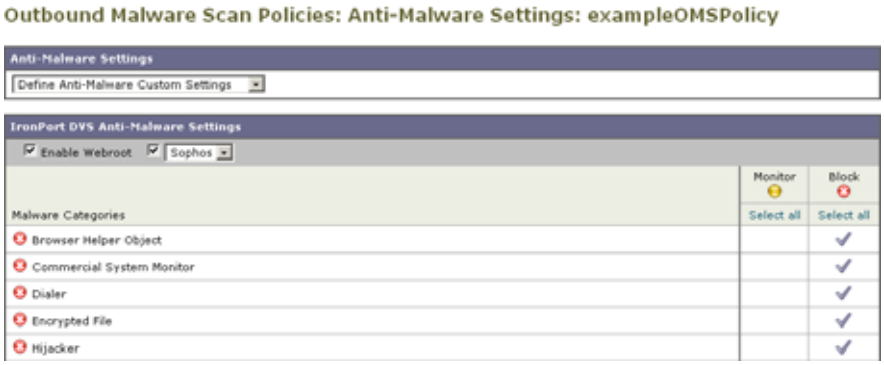
- **[どのアップロードもスキャンしない（Do not scan any uploads）]。**DVS エンジンはアップロード要求をスキャンしません。すべてのアップロード要求はアクセス ポリシーに対して評価されます。
- **[すべてのアップロードをスキャンする（Scan all uploads）]。**DVS エンジンはすべてのアップロード要求をスキャンします。アップロード要求は、DVS エンジンの スキャンの判定に応じて、ブロックされるか、またはアクセス ポリシーに対して評価されます。
- **[指定したカスタム URL カテゴリへのアップロードをスキャン（Scan uploads to 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。アップロード要求は、DVS エンジンの スキャンの判定に応じて、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）] カラムで、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、ドロップダウン メニューから [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。

図 12-4　アウトバウンド マルウェア スキャン ポリシーのアンチマルウェア設定



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 グルーでイネーブルにするアンチマルウェア スキャン エンジンを選択します。

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。

ステップ 9　[マルウェア カテゴリ（Malware Categories）] セクションで、マルウェア スキャンの判定に基づいてさまざまなマルウェア カテゴリをモニタするか、ブロックするかどうかを選択します。

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するか、またはシステムが一時的なエラー状態に陥ると、URL トランザクションが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や AsyncOS のアップグレードが行われている間は、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 スキャンの判定である SV_TIMEOUT および SV_ERROR 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、保存します。

ロギング

アクセス ログは、DVS エンジンがアップロード要求のマルウェアをスキャンする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の DVS エンジン アクティビティの値が含まれています。表 12-2 の任意のフィールドを W3C またはアクセス ログに追加して、この DVS エンジン アクティビティをより容易に検索することもできます。

表 12-2　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 エンジンがアップロード要求をマルウェアであると指定し、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 となります。

ただし、DVS エンジンがアップロード要求をマルウェアであると指定し、マルウェアのアップロード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するアクセス ポリシーによって決まります。

DVS エンジンがアップロード要求のマルウェアをスキャンしたかどうかを判定するには、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するか、または W3C あるいはアクセス ログに追加した表 12-2 に示されるフィールドの結果を確認します。

詳細については、「「スキャン判定情報について」（P.24-24）」を参照してください。

13
データ セキュリティと外部 DLP ポリシー

データ セキュリティと外部 DLP ポリシーの概要

情報化時代では、組織のデータが組織の最も大切な財産の 1 つです。組織では多額の費用をかけ、従業員、顧客、パートナーがデータを利用できるようにしています。データは Web と電子メールを通して絶え間なく行き交っています。このようにデータ アクセスが増加したため、機密情報や占有情報の悪意、偶然、または過失による消失をどのように防止するかの答えを見つけ出すことは、情報セキュリティの専門家にとって難問となっています。

Web セキュリティ アプライアンスは、データの安全を確保するために、次の機能を提供します。

- **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、および 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、どのデータが、どこに、どのようにして、誰によって発信されるかを制御します。
- **サードパーティ製のデータ消失防止（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、保護する代表的なサードパーティ製コンテント アウェア DLP システムを統合します。Web プロキシは、プロキシ サーバがコンテンツ スキャンを外部システムにオフロードできる軽量 HTTP ベース プロトコルである Internet Content Adaptation Protocol（ICAP）を使用します。Web プロキシは、コンテンツ スキャンを専用外部システムにオフロードすることにより、パフォーマンスへの影響を最小限に抑えて他の Web プロキシ機能を自由に実行できるようにすると同時に、他の製品の詳細なコンテンツ スキャンを活用できます。

Cisco IronPort データセキュリティ フィルタおよび外部 DLP システムと連携することにより、Web セキュリティ アプライアンス は情報と知的財産の保護を可能にし、ユーザによる意図しない機密データのアップロードを防止することで、規制と組織のコンプライアンスを履行します。ネットワークから発信できるデータの種類を定義します。

ネットワークから発信されるデータを制限するために、Web セキュリティ アプライアンスは次のポリシー グループのタイプを提供します。

- **Cisco IronPort データ セキュリティ ポリシー。**Cisco IronPort データ セキュリティ フィルタをイネーブルにすると、ビジネス ポリシーを強制するために Cisco IronPort データ セキュリティ ポリシーを作成できます。たとえば、ユーザによる Excel や zip ファイルの送信を禁止するデータ セキュリティ ポリシーを作成できます。詳細については、「「データ セキュリティ ポリシー グループ」（P.13-3）」を参照してください。
- **外部 DLP ポリシー。**外部 DLP システムと連携するようにアプライアンスを設定した場合、コンテンツをスキャンし、要求をブロックするかどうかを判定する外部 DLP システムにネットワークから発信されるデータを渡すために外部 DLP ポリシーを作成できます。詳細については、「「外部 DLP ポリシー グループ」（P.13-4）」を参照してください。

組織のニーズによっては、データ セキュリティと外部 DLP ポリシーの両方を使用する場合があります。たとえば、Cisco IronPort データ セキュリティ ポリシーを使用して、レピュテーション スコアが低い Web サイトへのデータのアップロードをブロックする場合があります。これにより、データは詳細なコンテンツ スキャンのために外部 DLP システムに送信されないため、全体的なパフォーマンスの向上が図れます。

最小サイズ以下のアップロード要求のバイパス

多くの Web サイトはインタラクティブです。つまり、ユーザはデータを送信すると同時にデータを受信します。ユーザは、Web サイトへのログイン時または単純な形式のデータの送信時にデータを送信する場合があります。多くの Web トラフィックは、比較的小さな POST 要求で構成されますが、多くの行をログ ファイルに取り込む可能性があります。これにより、ログ内に多くの「ノイズ」が生成され、ユーザが個人の電子メール アカウントを使用して会社ファイルをアップロードするなど、真のデータ セキュリティ違反を見つけ、問題に対処するのが困難になります。

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、それを下回る場合は Cisco IronPort データセキュリティ フィルタまたは外部 DLP サーバによってアップロード要求がスキャンされない本文の最小要求サイズを定義できます。

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 フィルタを適用します。
- **`externaldlpconfig`。**設定済みの外部 DLP サーバに適用します。

デフォルトで、本文の最小要求サイズは、両方の CLI コマンド共、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を行う本文の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および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 サーバでスキャンされます（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バイパスできます。詳細については、「図 13-3（P.13-11）」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

Cisco IronPort データセキュリティ フィルタまたは外部 DLP サーバがアップロード要求をブロックすると、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。ただし、すべての Web サイトがエンド ユーザにブロック ページを表示するわけではありません。たとえば、Web 2.0 の Web サイトは、静的 Web ページの代わりに javascript を使用して動的コンテンツを表示し、ブロック ページを表示することはありません。ユーザは、データ セキュリティ違反が発生しないように適切にブロックされますが、この情報が Web サイトを通じて通知されない場合があります。

データ セキュリティと外部 DLP ポリシーの使用

Cisco IronPort データ セキュリティ ポリシーと外部 DLP ポリシーは、Web プロキシが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）のための HTTP 要求および復号化された HTTPS 接続を処理する方法を定義します。ただし、Cisco IronPort データ セキュリティ ポリシーは、Web セキュリティ アプライアンスで定義されたロジックを使用し、外部 DLP ポリシーは DLP システムで定義されたロジックを使用します。アップロード要求は、要求本文にコンテンツを含む HTTP または復号化された HTTPS 要求です。

Web プロキシがアップロード要求を受信すると、要求をデータ セキュリティおよび外部 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、外部 DLP ポリシーの前に 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に、要求に対して何を行うかを決定するポリシー グループの設定済み制御設定と要求を比較します。

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。詳細については、「データ セキュリティ ポリシー グループ」（P.13-3）および「外部 DLP ポリシー グループ」（P.13-4）を参照してください。

（注）　サイズがゼロ（0）バイトのファイルをアップロードしようとするアップロード要求は、Cisco IronPort データ セキュリティまたは外部 DLP ポリシーでは評価されません。

データ セキュリティ ポリシー グループ

アプライアンス自体の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　**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。**アプライアンスのアップロード要求をスキャンするには、まず 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。通常、Cisco IronPort データセキュリティ フィルタ機能は、システム セットアップ ウィザードを使用して、初期設定時にイネーブルになります。それ以外の場合は、[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）] ページに移動して、イネーブルにします。

ステップ 2　**データ セキュリティ ポリシー グループを作成および設定します。**Cisco IronPort データセキュリティ フィルタ機能をイネーブルにした後、データ セキュリティ ポリシー グループを作成および設定して、各ユーザからのアップロード要求を処理する方法を決定します。

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。設定可能なセキュリティ コンポーネントと Web プロキシがデータ セキュリティ ポリシー グループを使用してアップロード要求を制御する方法の詳細については、「Cisco IronPort データ セキュリティ ポリシーを使用したアップロード要求の制御」（P.13-9）を参照してください。

Web プロキシがアップロード要求を制御設定と比較する場合、設定を順番に評価します。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。

- **ブロック（Block）**：Web プロキシは、接続を許可せずに、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、残りのデータ セキュリティ ポリシーのセキュリティ 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 またはアクセス ポリシー 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けて、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 ポリシーでは、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は Block アクションだけです。最終アクションとは、Web プロキシがトランザクションと他のすべての制御設定との比較を中止するアクションです。Monitor および Allow アクションは中間のアクションです。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。

図 13-3（P.13-11）は、Cisco IronPort データ セキュリティ ポリシーの制御設定を評価するときに Web プロキシが使用する順序を示します。フロー図は、トランザクションに適用されるアクションは、最終アクションである Block とアクセス ポリシーに対する評価でしかないことを示しています。

考えられるアクセス ポリシーのアクションの詳細については、「アクセス ポリシー グループ」（P.9-2）を参照してください。アクセス ポリシーの Monitor アクションの詳細については、「モニタ アクションについて」（P.9-3）を参照してください。

外部 DLP ポリシー グループ

外部 DLP システム上の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　**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 アプライアンス上で定義する必要があります。このタスクは、[ネットワーク（Network）] > [外部 DLP サーバ（External DLP Servers）] ページで実行します。詳細については、「「外部 DLP システムの定義」（P.13-13）」を参照してください。

ステップ 2　**外部 DLP ポリシー グループを作成および設定します。**外部 DLP システムを定義したら、外部 DLP ポリシー グループを作成および設定し、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。

アップロード要求が外部 DLP ポリシーに一致する場合、Web プロキシは、スキャンのために Internet Content Adaptation Protocol（ICAP）を使用して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 Allow に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、該当するアクセス ポリシーによって決まります。

外部 DLP ポリシー グループの設定方法の詳細については、「外部 DLP ポリシーを使用したアップロード要求の制御」（P.13-16）を参照してください。

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は ID に割り当てられ、他のポリシー タイプに対して評価されて、タイプごとに属するポリシー 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 グループのメンバーシップに基づいて、設定されたポリシー制御設定をクライアント要求に適用します。

クライアント要求が一致するポリシー 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。このプロセスでは、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。ID グループ メンバーシップの評価に関する詳細については、「ID グループ メンバーシップの評価」（P.8-4）を参照してください。
- **権限を持つユーザ。**割り当てられた ID で認証が必要な場合、ユーザは、データ セキュリティまたは外部 DLP ポリシー グループの権限を持つユーザのリストに含まれ、グループ ポリシーに一致する必要があります。権限を持つユーザのリストには、任意の指定したグループまたはユーザ、または ID がゲスト アクセスを許可する場合はゲスト ユーザを指定できます。
- **拡張オプション。**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拡張オプションを設定できます。オプションの一部（プロキシ ポートや URL カテゴリなど）は、ID 内でも定義できます。ID 内に拡張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 ポリシー グループの両方と照合する方法の概要について説明します。Web プロキシがクライアント要求を正確に照合する仕組みに関する詳細については、「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」（P.13-5）を参照してください。

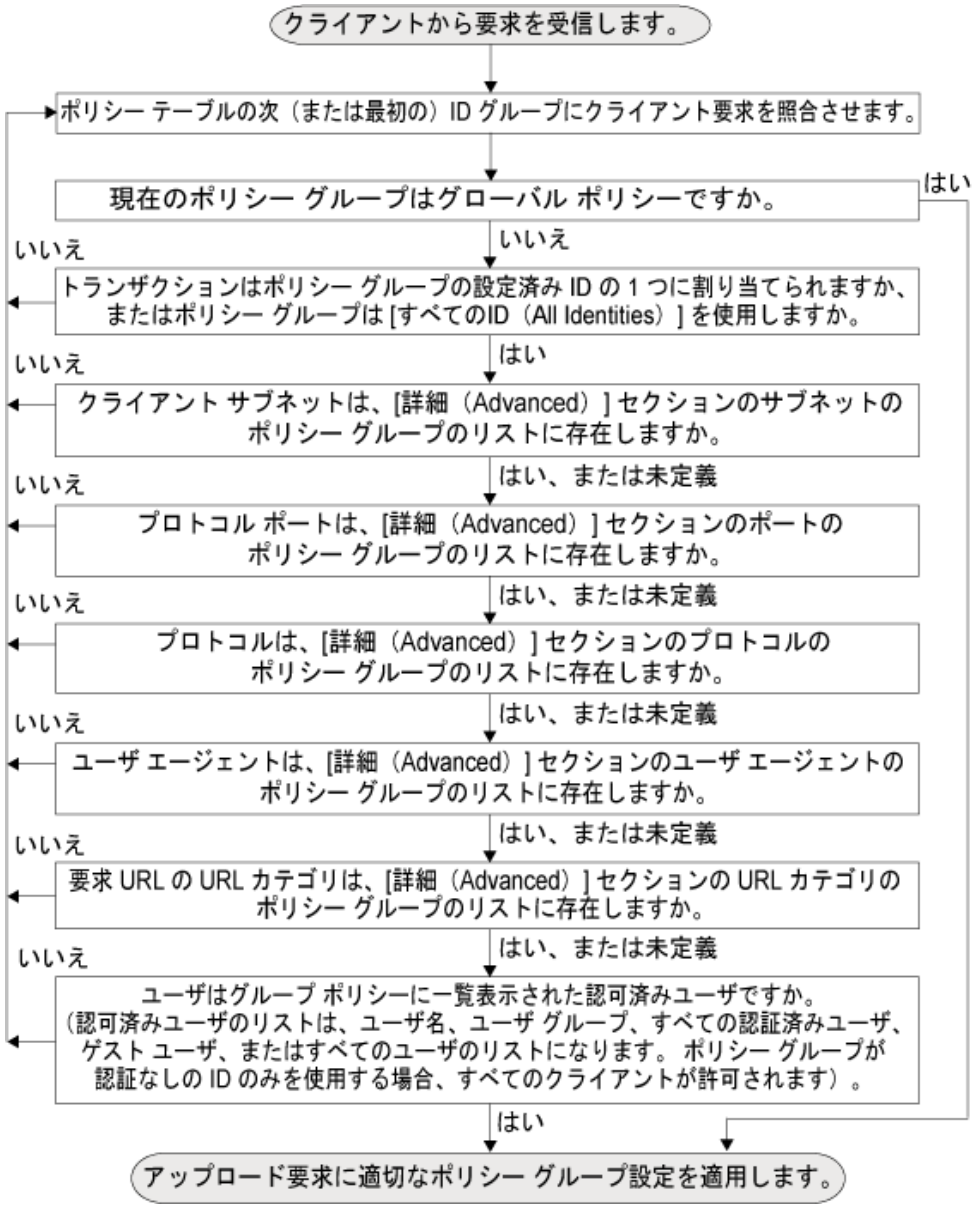
Web プロキシは、ポリシー テーブルの各ポリシー グループを順番に読み取ります。次に、アップロード要求のステータスを最初のポリシー グループのメンバーシップの基準と比較します。一致した場合、Web プロキシは、そのポリシー グループのポリシー設定を適用します。

一致しない場合、Web プロキシは、アップロード要求を次のポリシー グループと比較します。アップロード要求がユーザ定義のポリシー グループに一致するまで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。アップロード要求がポリシー グループまたはグローバル ポリシー グループと一致すると、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。

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

図 13-1（P.13-6）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 ポリシー グループに対して評価する方法を示します。

図 13-1　データ セキュリティおよび外部 DLP ポリシーのポリシー グループ フロー図



データ セキュリティおよび外部 DLP ポリシーの作成

宛先サイトの URL カテゴリの 1 つまたは複数の 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。複数の条件を定義する場合、アップロード要求はポリシー グループに一致するすべての条件を満たしている必要があります。ただし、アップロード要求は設定された ID の 1 つのみと一致するが必要です。

Web プロキシがアップロード要求をポリシー グループと照合する方法の詳細については、「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」（P.13-5）と「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」（P.13-5）を参照ください。

[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）] ページでデータ セキュリティ ポリシー グループのメンバーシップを定義します。[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）] ページで外部 DLP ポリシー グループのメンバーシップを定義します。

ステップ 1　[Web セキュリティ マネージャ（Web Security Manager）] > [Cisco IronPort データ セキュリティ（Cisco IronPort Data Security）] ページまたは [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）] ページに移動します。

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

ステップ 3　[ポリシー名（Policy Name）] フィールドにポリシー グループ名を入力し、必要に応じて [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、慎重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。

この方法の詳細については、「他のポリシー グループの ID の設定」（P.8-22）を参照してください。

ステップ 6　必要に応じて、[詳細（Advanced）] セクションを拡大し、追加メンバーシップの要件を定義します。

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。

表 13-1 は、データ セキュリティおよび外部 DLP ポリシー グループに設定できる拡張オプションについて説明します。

表 13-1　データ セキュリティおよび外部 DLP ポリシー グループの拡張オプション

拡張オプション	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。組み込むプロトコルを選択します。 「All others」は、このオプションの上記に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した場合、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、アウトバウンド マルウェア スキャン、データ セキュリティ、または外部 DLP ポリシーの 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：**このグループ ポリシーに関連付けられた ID がこの拡張設定によって ID を定義する場合、これは非 ID ポリシー グループ レベルでは設定できません。
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：**このグループ ポリシーに関連付けられた ID がアドレスによってメンバーシップを定義している場合、このグループ ポリシーでは、ID で定義された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。
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：**このグループ ポリシーに関連付けられた ID がこの拡張設定によって ID を定義する場合、これは非 ID ポリシー グループ レベルでは設定できません。

表 13-1　データ セキュリティおよび外部 DLP ポリシー グループの拡張オプション （続き）

拡張オプション	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。 ユーザ エージェント ベースのポリシーの作成の詳細については、「ユーザ エージェント ベースのポリシーの使用」（P.7-11）を参照してください。 **注：**このグループ ポリシーに関連付けられた ID がこの拡張設定によって ID を定義する場合、これは非 ID ポリシー グループ レベルでは設定できません。
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。詳細については、「「セキュア モビリティの実現の概要」（P.14-1）」を参照してください。

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、Web プロキシがアップロード要求を処理する方法を定義するための制御設定を設定します。

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を設定するまで、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。詳細については、「「Cisco IronPort データ セキュリティ ポリシーを使用したアップロード要求の制御」（P.13-9）」を参照してください。

ステップ 10　外部 DLP ポリシー グループを作成する場合は、Web プロキシがアップロード要求を処理する方法を定義するための制御設定を設定します。

新しい外部 DLP ポリシー グループは、カスタム設定を設定するまで、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。詳細については、「「外部 DLP ポリシーを使用したアップロード要求の制御」（P.13-16）」を参照してください。

ステップ 11　変更を送信し、保存します。

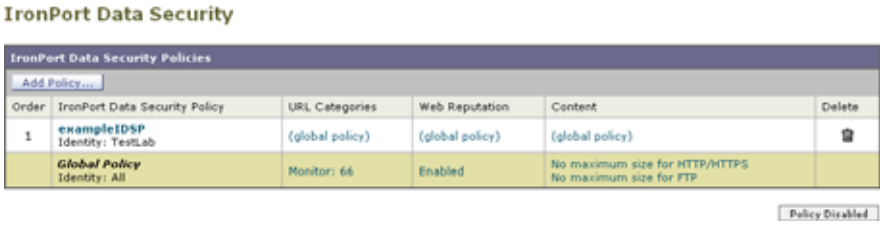
Cisco IronPort データ セキュリティ ポリシーを使用したアップロード要求の制御

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は、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 ポリシーに対して評価するかを決定します。

[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）] 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。

図 13-2 は、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できる場所を示します。

図 13-2　セキュアな Cisco IronPort データ セキュリティ ポリシーの作成



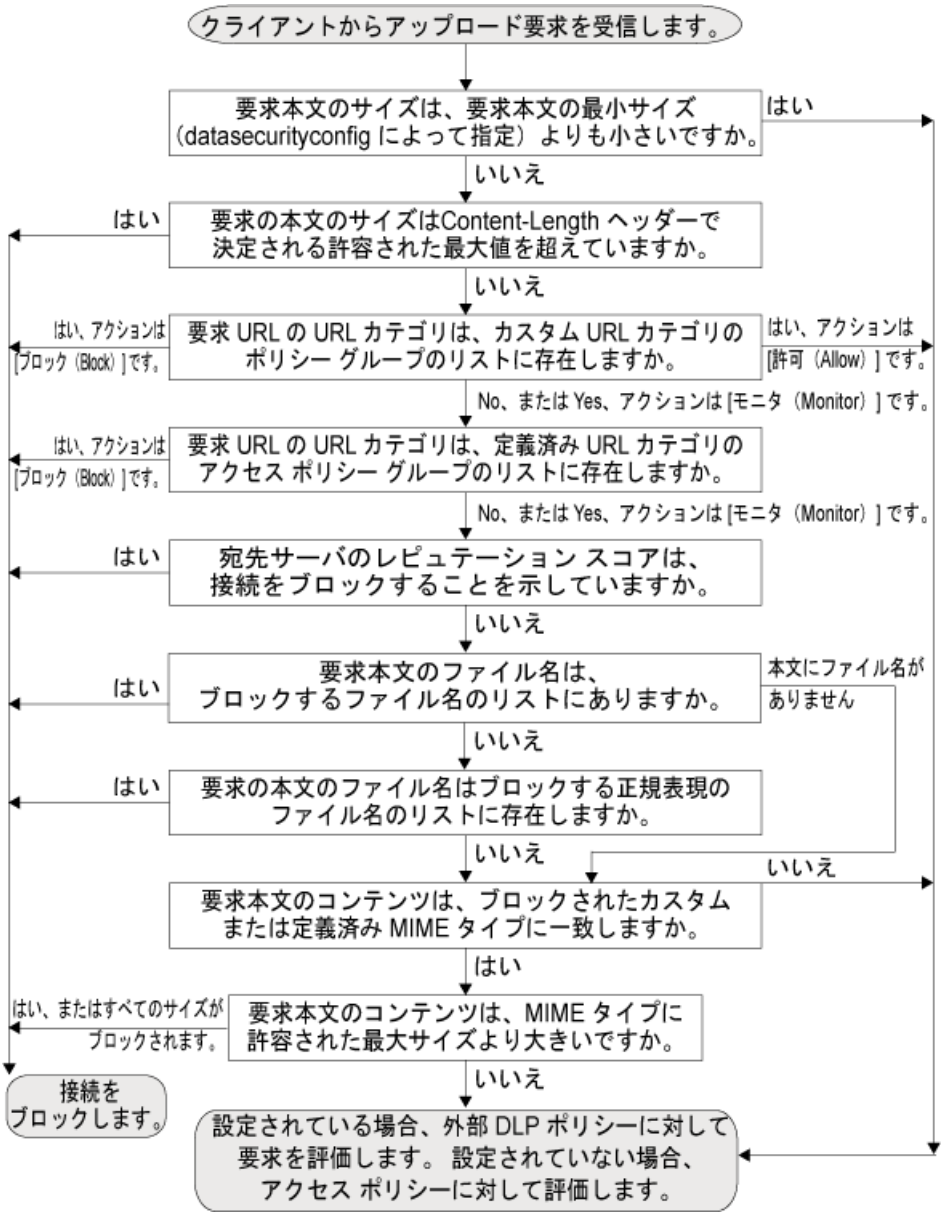
アップロード要求で実行するアクションを決定するために次の設定を設定できます。

- **URL カテゴリ（URL Categories）。**詳細については、「URL カテゴリ」（P.13-11）を参照してください。
- **Web レピュテーション（ReputationWeb）。**詳細については、「Web レピュテーション」（P.13-12）を参照してください。
- **コンテンツ（Content）。**詳細については、「コンテンツのブロッキング」（P.13-12）を参照してください。

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ると、ポリシー グループの制御設定は要求をブロックするか、またはアクセス ポリシーに対して評価するかを決定するかどうかが評価されます。データ セキュリティ ポリシー グループをアップロード要求に割り当てる方法の詳細については、「ポリシー グループ メンバーシップ」（P.7-7）を参照してください。

図 13-3（P.13-11）は、特定のデータ セキュリティ ポリシーを要求に割り当てた後で、アプライアンスがアップロード要求で実行するアクションを決定する方法を示します。

図 13-3　データ セキュリティ ポリシーのアクションの適用



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、または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 カテゴリで Web サイトのトラフィックを許可するか、モニタするか、またはブロックするかを選択することもできます。

URL カテゴリの使用方法の詳細については、「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」（P.17-14）を参照してください。

Web レピュテーション

Web レピュテーション設定はグローバル設定を継承します。特定のポリシー グループの 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ために、[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できます。

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。定義上、すべての正のスコアがすべてモニタされます。

Web レピュテーション スコアの設定の詳細については、「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」（P.19-4）を参照してください。

コンテンツのブロッキング

[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）] ページ上の設定を使用して、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 [オブジェクト スキャン制限（Object Scanning Limits）] フィールドで設定）の両方より大きい場合、アップロード要求はブロックされますが、この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、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 タイプをサイズでブロックする場合、[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 [オブジェクト スキャン制限（Object Scanning Limits）] フィールドの値と同じ値を最大ファイル サイズとして指定できます。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際にアーカイブされたファイルのコンテンツを確認しません。アーカイブされたファイルは、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。コンテンツではブロックできません。

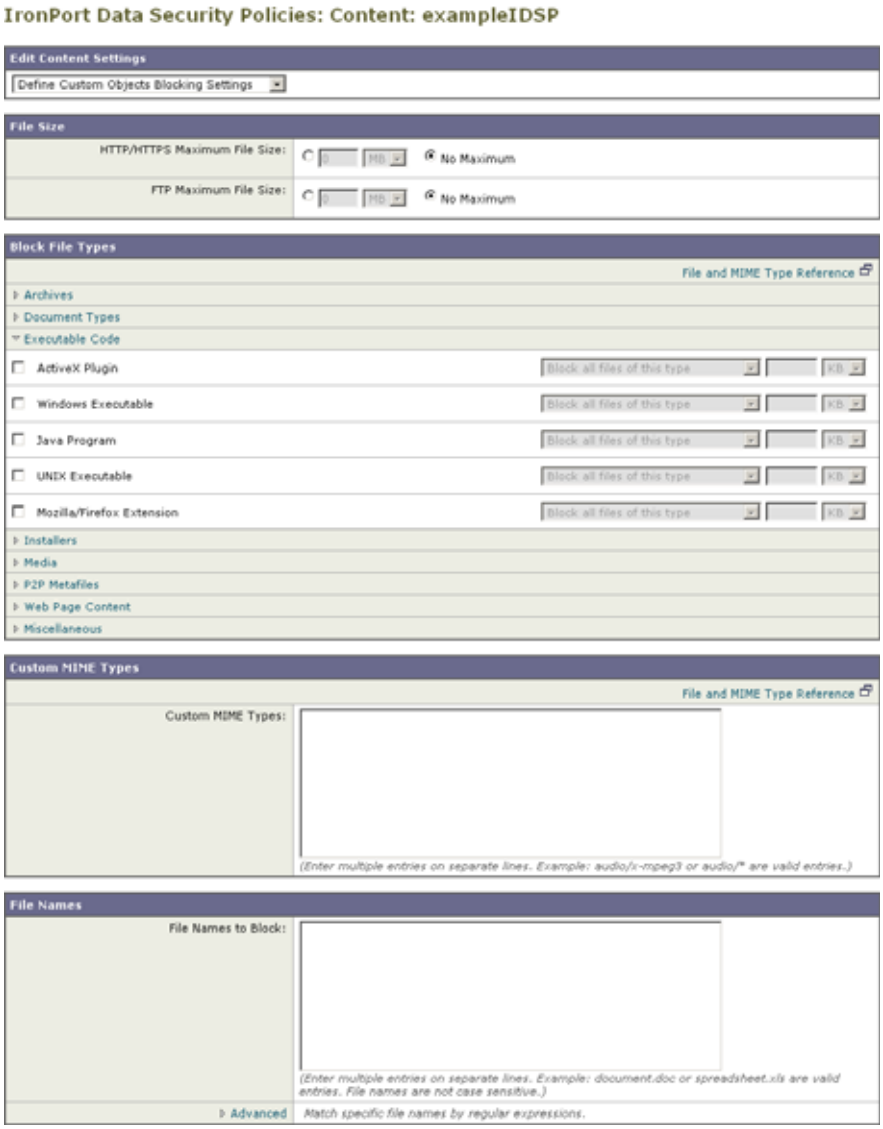
（注）　一部の MIME タイプのグループでは、1 つのタイプをブロックすると、グループ内のすべての MIME がブロックされます。たとえば、application/x-java-applet をブロックすると、application/java および application/javascript など、すべての MIME タイプがブロックされます。

- **[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。正規表現の使用方法の詳細については、「正規表現」（P.17-24）を参照してください。

（注）　8 ビット ASCII 文字を使用するファイル名のみを入力します。Web プロキシは、8 ビット ASCII 文字を使用するファイル名のみ照合します。

図 13-4（P.13-13）は、コンテンツ制御設定を設定する [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）] ページを示します。

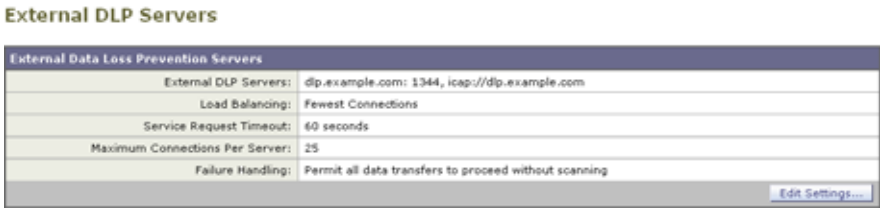
図 13-4　Cisco IronPort データ セキュリティ ポリシーの設定



外部 DLP システムの定義

Web セキュリティ アプライアンスは、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。[ネットワーク（Network）] > [外部 DLP サーバ（External DLP Servers）] ページで、すべての DLP システムとの統合に影響を与える DLP システムとグローバル設定を定義します。

図 13-5　[ネットワーク（Network）] > [外部 DLP サーバ（External DLP Servers）] ページ



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。たとえば、Web プロキシはラウンドロビンまたはハッシュ関数を使用して各 DLP システムにアクセスできます。

（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）] ページに移動します。

ステップ 2　[設定を編集（Edit Settings）] をクリックします。

図 13-6　外部 DLP サーバの設定

ステップ 3　表 13-2 の情報を入力します。

表 13-2　外部 DLP サーバの設定

設定	説明
外部 DLP サーバの編集（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 アドレスとポート。**DLP システムにアクセスするためのホスト名または IP アドレスと TCP ポート。 • **再接続の試行。**Web プロキシが失敗するまで DLP システムへの接続を試行する回数。 • **DLP サービスの URL。**特定の DLP サーバに固有の ICAP クエリー URL。Web プロキシには、外部 DLP サーバに送信する、この ICAP 要求で入力する情報が含まれています。URL は、ICAP プロトコル icap:// で始まる必要があります。
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、Web プロキシが別の DLP サーバにアップロード要求を配布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）。**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。リストされている順序で、DLP サーバへの接続を試行します。1 つの 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 1 つに接続しようとします。 • **最少の接続。**Web プロキシは、別の DLP サーバにアクティブな要求の数を記録し、現在提供している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。**Web プロキシは、ハッシュ関数を使用して、DLP サーバに要求を配布します。ハッシュ関数は、同じ URL の要求が常に同じ DLP サーバに送信されるように、プロキシ ID および URL を入力として使用します。 • **ラウンド ロビン。**Web プロキシは、アップロード要求をすべての DLP サーバ間にリストされた順序で均等に循環させます。
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。この時間を超えると、ICAP 要求は失敗し、障害処理設定に応じて、アップロード要求はブロックされるか、または許可されます。 デフォルト値は 60 秒です。
ICAP DLP 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た各外部 DLP サーバへの同時 ICAP 要求接続の最大数を指定します。このページの障害処理設定は、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。
失敗のハンドリング（Failure Handling）	DLP サーバがタイムリーな応答に失敗したときに、アップロード要求がブロックされるか、または許可されるか（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せずに許可する」）です。

ステップ 4　任意で、新しく追加された [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 サーバ情報を入力して、別の DLP サーバを追加できます。

ステップ 5　[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の外部 DLP サーバ間の接続をテストできます。

ステップ 6　変更を送信し、保存します。

外部 DLP ポリシーを使用したアップロード要求の制御

各アップロード要求は、外部 DLP 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。外部 DLP ポリシー グループの制御設定は、スキャンのためにアップロード要求を外部 DLP システムに送信するかどうかを決定します。

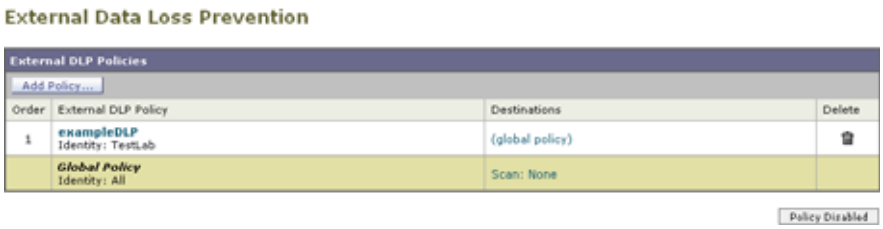
Web プロキシがアップロード要求ヘッダーを受信すると、スキャンのために要求を外部 DLP システムに送信する必要があるかどうかを決定するために必要なすべての情報が提供されます。DLP システムは、要求をスキャンし、Web プロキシに判定（ブロックするか、モニタするかのいずれか）を返します（要求はアクセス ポリシーに対して評価されます）。必要に応じて、DLP システムによって提供されるブロック ページがエンド ユーザに表示されます。

（注）　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適用される場合、外部 DLP システムが要求をスキャンすると同時に、Web プロキシはポリシー グループの制御設定をアップロード要求に対して評価します。DLP システムがスキャンを完了する前に、データ セキュリティ ポリシー設定が要求をブロックする場合、Web プロキシは要求をブロックし、DLP システムによって ICAP セッションを終了します。

[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）] ページで、外部 DLP ポリシー グループの制御設定を設定します。

図 13-7 は、外部 DLP ポリシー グループの制御設定を設定できる場所を示します。

図 13-7　外部 DLP ポリシーの作成

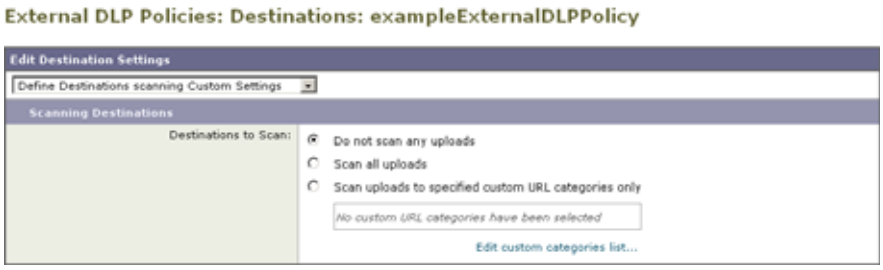


ステップ 1　[Web セキュリティ マネージャ（Web Security Manager）] > [外部データ漏洩防止（External Data Loss Prevention）] ページに移動します。

ステップ 2　設定するポリシー グループの [接続先（Destinations）] カラムの下にある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）] 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（まだ選択されていない場合）。

図 13-8　外部 DLP ポリシーの宛先スキャンの設定



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はアクセス 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 スキャンの判定に応じて、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）]。**特定のカスタム URL カテゴリに分類されるアップロードは、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 スキャンの判定に応じて、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、保存します。

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された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。詳細については、「「スキャン判定情報について」（P.24-24）」を参照してください。

アクセス ログに加えて、Web セキュリティ アプライアンスは Cisco IronPort データ セキュリティおよび外部 DLP ポリシーをトラブルシュートするために次のログ ファイル タイプを提供します。

- **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。
- **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ます。これにより、外部 DLP サーバとの接続性または統合の問題をトラブルシュートできます。

次のテキストは、データのログ エントリのサンプルを示します。

```
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
```

表 13-3 は、[データ セキュリティ ログ（Data Security Log）] フィールドについて説明します。

表 13-3　[データ セキュリティ ログ（Data Security Log）] フィールド

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`	送信元 IP アドレス
`-`	ユーザ名
`-`	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、設定された本文の最小要求サイズ（デフォルトで 4096 バイト）より小さいテキスト/プレーン ファイルは含まれません。本文の最小要求サイズの設定の詳細については、「最小サイズ以下のアップロード要求のバイパス」（P.13-2）を参照してください。
`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）　POST 要求などのサイトへのデータ転送がいつ外部 DLP サーバによってブロックされたかについては、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てください。

14
セキュア モビリティの実現

セキュア モビリティの実現の概要

今日、ユーザとその所有デバイスは、オフィス、自宅、空港、カフェといったさまざまな場所からインターネットに接続するなど、さらにモバイル化が進んでいます。従来、ネットワーク内のユーザはセキュリティの脅威から保護されていましたが、従来のネットワーク境界外のユーザはアクセプタブル ユース ポリシーが適用されずにマルウェアから最小限しか保護されないため、データ損失のリスクが高まっています。

雇用主は、従業員やパートナーが場所やデバイスを問わずに作業できるフレキシブルな作業環境の創出を望んでいますが、同時に、企業の利益と資産をインターネット ベースの脅威から常時保護したいと考えています。

従来のネットワーク セキュリティ ソリューションやコンテンツ セキュリティ ソリューションは、ユーザと資産をネットワーク ファイアウォールで保護する点では理想的でしたが、ユーザまたはデバイスがネットワークに接続していない場合や、セキュリティ ソリューションを介してデータがルーティングされない場合には効果がありません。

シスコは Cisco AnyConnect Secure Mobility を提供することで、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。Secure Mobility は、ボーダレス ネットワークのセキュリティと制御を復元する、複数のシスコ製品にまたがる機能のコレクションです。Secure Mobility と連携するシスコ製品には、Cisco IronPort Web セキュリティ アプライアンス、Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス、および Cisco AnyConnect セキュア モビリティ クライアントがあります。

Secure Mobility を使用すれば、モバイルおよびリモート ユーザは、ネットワーク内で接続されたローカル ユーザであるかのようにシームレスな体験を行い、常にリスクから保護されます。

Secure Mobility が Web セキュリティ アプライアンス上でイネーブルになっている場合、リモート ユーザとローカル ユーザを区別できます。これにより、次のタスクを実行できます。

- リモート ユーザの ID およびその他のポリシーを作成します。
- リモート トラフィックのレポートを表示します。
- リモート ユーザのシングル サインオン（SSO）をイネーブルにします。

シングル サイン オンのイネーブル化の詳細については、「リモート ユーザの透過的な識別」（P.14-3）を参照してください。

リモート ユーザの操作

Secure Mobility がイネーブルの場合、ID およびその他のポリシーを設定し、場所に応じて次のように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（バーチャル プライベート ネットワーク）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。ユーザは、自宅オフィス、喫茶店、ホテルなどにいる場合があります。Cisco 適応型セキュリティ アプライアンスおよび 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、物理的またはワイヤレスでネットワークに接続されます。

リモートおよびローカル ユーザに対して別個のポリシーを作成する場合があります。たとえば、ユーザが社外にいる（リモート ユーザの）場合はアート サイトやエンタテインメント サイトへのアクセスを許可し、ユーザが社内にいる（ローカル ユーザの）場合はアクセスをブロックするアクセス ポリシーを作成できます。

[セキュリティ サービス（Security Services）] > [AnyConnect] ページで Secure Mobility をイネーブルにした場合、次のいずれかの方法を使用してリモート ユーザを識別します。

- **IP アドレスによる関連付け：**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。通常、Cisco 適応型セキュリティ アプライアンスは、VPN 機能を使用して接続しているデバイスに、これらの IP アドレスを割り当てます。Web セキュリティ アプライアンスは、設定されているいずれかの IP アドレスからトランザクションを受信すると、そのユーザをリモート ユーザと見なします。
- **Cisco ASA との統合：**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 適応型セキュリティ アプライアンスを指定します。Cisco 適応型セキュリティ アプライアンスは、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 プロキシが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判定します。Cisco 適応型セキュリティ アプライアンスと統合してユーザを判定する場合、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。

  シングル サイン オンのイネーブル化の詳細については、「リモート ユーザの透過的な識別」（P.14-3）を参照してください。

セキュア モビリティのイネーブル化

常時接続セキュリティを使用してリモート ユーザを保護するには、まず Web セキュリティ アプライアンスで Secure Mobility 機能をイネーブルにする必要があります。Secure Mobility がイネーブルの場合、ID を作成するときにリモート ユーザとローカル ユーザを区別できます。

（注） また、CLI を使用して Secure Mobility を設定することもできます。詳細については、「「CLI を使用したセキュア モビリティの設定」（P.14-5）」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）] > [Anyconnect セキュア モビリティ（AnyConnect Secure Mobility）] ページに移動し、[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　[AnyConnect セキュア モビリティを有効化（Enable AnyConnect Secure Mobility）] フィールドがイネーブルであることを確認します。

IP アドレスによるか、1 つ以上の Cisco 適応型セキュリティ アプライアンスを統合することにより、リモート ユーザの識別方法を設定します。詳細については、「リモート ユーザの操作」（P.14-2）を参照してください。

ステップ 4　IP アドレスによってリモート ユーザを識別するには、[IP 範囲（IP Range）] オプションを選択し、[IP 範囲（IP Range）] フィールドに IP アドレスの範囲を入力し、ステップ 10 に進みます。それ以外の合は、ステップ 5 に進みます。

ステップ 5　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により、リモート ユーザを識別するには、[Cisco ASA 統合（Cisco ASA Integration）] オプションを選択します。

ステップ 6　[ASA ホスト名（ASA Host Name）] または [IP アドレス（IP Address）] フィールドに Cisco 適応型セキュリティ アプライアンスのホスト名または IP アドレス、[ポート（Port）] フィールドに ASA へのアクセスに使用するポート番号を入力して、少なくとも 1 つの Cisco 適応型セキュリティ アプライアンスを設定します。Cisco ASA のデフォルト ポート番号は 11999 です。

ステップ 7　クラスタ内に複数の Cisco 適応型セキュリティ アプライアンスが設定されている場合は、[行を追加（Add Row）] をクリックし、クラスタの各 ASA を設定します。2 つの Cisco 適応型セキュリティ アプライアンスが高可用性に設定されている場合、*アクティブな* Cisco 適応型セキュリティ アプライアンスに対して 1 つのホスト名または IP アドレスのみを入力します。

ステップ 8　[ASA アクセス パスワード（ASA Access Password）] フィールドで、ステップ 6 と 7 で指定する Cisco 適応型セキュリティ アプライアンスのアクセス パスワードを入力します。アクセス パスワードは、少なくとも 8 文字で、20 文字以内にする必要があります。使用可能な文字は次のとおりです。

0 ～ 9、a ～ z、A ～ Z、.、,、:、;、_、/、-

（注）　ここで入力するパスワードは、指定された Cisco 適応型セキュリティ アプライアンスに設定されたアクセス パスワードと一致する必要があります。

ステップ 9　任意で、[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た Cisco 適応型セキュリティ アプライアンスに接続できるかどうかを確認します。

ステップ 10　変更を送信し、保存します。

リモート ユーザの透過的な識別

Web セキュリティ アプライアンスが Cisco 適応型セキュリティ アプライアンスを統合すると、認証されたユーザ名によりユーザを透過的に（つまりエンド ユーザに要求せずに）識別するように設定できます。リモート ユーザのシングル サイン オンを実現するために、この設定が必要となる場合があります。

（注）　Novell eDirectory および Active Directory を使用してユーザを透過的に識別することもできます。詳細については、「ユーザの透過的識別」（P.8-12）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）] > [AnyConnect セキュア モビリティ（AnyConnect Secure Mobility）] ページで Secure Mobility をイネーブルにします。

詳細については、「セキュア モビリティのイネーブル化」（P.14-2）を参照してください。

ステップ 2　リモート ユーザに適用する ID グループを作成します。

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、[リモート ユーザ（Remote Users）] 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。

c. 必要に応じて、他の ID オプションをすべて設定します。

ID の作成の詳細については、「ID の作成」（P.8-18）を参照してください。

ステップ 3　リモート ユーザの ID を使用するポリシーを作成します。

ロギング

アクセス ログは、各トランザクションがローカル ユーザによって行われたか、リモート ユーザによって行われたかを示します。また、既存のアクセス ログにカスタム フォーマット指定子（%l）を追加したり、W3C アクセス ログに同等の W3C フィールド（auth-user-type）を追加することもできます。

アクセス ログに加えて、Web セキュリティ アプライアンスは Secure Mobility の潜在的な問題のトラブルシューティングのために次のログを表示します。

- **ユーザ検出サービス（UDS）ログ。**UDS ログは、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。
- **AnyConnect セキュア モビリティ デーモン ログ。**AnyConnect セキュア モビリティ デーモン ログは、ステータス チェックを含む、Web セキュリティ アプライアンスと AnyConnect クライアント間の対話を記録します。

CLI を使用したセキュア モビリティの設定

表 14-1 は、Secure Mobility を設定およびモニタするために使用できる CLI コマンドについて説明します。

表 14-1　セキュア モビリティの CLI コマンド

コマンド	説明
musconfig	このコマンドを使用して Secure Mobility をイネーブルにし、IP アドレスによるか、または 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、リモート ユーザの識別方法を設定します。 **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。 Secure Mobility のイネーブル化および設定の詳細については、「セキュア モビリティのイネーブル化」（P.14-2）を参照してください。
musstatus	このコマンドを使用して、Web セキュリティ アプライアンスが適応型セキュリティ アプライアンスと統合されたときに、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 アプライアンスの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。Web セキュリティ アプライアンスを介してトラフィックが渡されたリモート クライアントの数として定義されます。 • リモート クライアントの合計数。

15
SaaS アプリケーションへのアクセスの制御

SaaS アクセス コントロールの概要

組織内にソフトウェア アプリケーションを所有し、管理するのではなく、ソフトウェアをサービス（SaaS）アプリケーションとして使用するように選択する組織がますます増加しています。通常、SaaS アプリケーションは、ネットワーク内のオンプレミスではなく「クラウド内」にあります。SaaS アプリケーションの使用には、コスト削減などの多くの潜在的な利点がありますが、特に SaaS アプリケーションへのアクセスの制御を管理する必要がある IT 管理者には課題もあります。

シスコは、SaaS アプリケーションへのアクセスの制御やセキュリティ ポリシーの適用に必要なシームレスかつ安全な制御を IT 管理者に提供する SaaS アクセス コントロール機能を提供します。SaaS アクセス コントロールにより、IT 管理者は SaaS アプリケーションにアクセスする必要があるユーザの認証と許可を容易に制御することができます。

Cisco SaaS アクセス コントロールをイネーブルにすると、ユーザはネットワーク認証のユーザ クレデンシャルを使用して、設定済み SaaS アプリケーションにログインします。つまり、ユーザがすべての SaaS アプリケーションおよびネットワーク アクセスに同じユーザ名とパスワードを使用することを意味します。ユーザが透過的にサインインするか（シングル サイン オン機能）、認証ユーザ名とパスワードの入力を求めるプロンプトを表示するか選択できます。

Cisco SaaS アクセス コントロールを使用して SaaS アプリケーションの適切なアクセス制御を行うことにより、次のことができます。

- SaaS アプリケーションにアクセス可能なユーザとアクセスする場所を制御します。
- パスワードを 1 つ覚えるだけで済むので、エンド ユーザのユーザビリティが向上します。
- ユーザが組織に雇用されなくなった時点で、すべて SaaS アプリケーションのへのアクセスをすばやくディセーブルにします。これは、「ゼロデイ失効」とも呼ばれています。
- 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します。

SaaS アクセス コントロールの動作について

SaaS アクセス コントロール ソリューションは、Security Assertion Markup Language（SAML）を使用して、SaaS アプリケーションへのアクセスを許可します。SAML バージョン 2.0 に厳密に準拠している SaaS アプリケーションで動作します。

SAML は、異なるセキュアなネットワーク（セキュリティ ドメインとも呼ばれています）間で認証および許可データを交換するための XML ベースの標準です。SAML が解決する主な問題は、異なるセキュリティ ドメイン間のシングル サイン オンです。通常 SAML は、Web ブラウザを使用してネットワーク（別のドメイン）にアクセスするユーザが 1 つのドメインに存在する場合に使用されます。これは、Web ブラウザ シングル サイン オンとも呼ばれています。

Web ブラウザ シングル サイン オンを実行するには、SAML ダイアログが次の用語を使用して各ドメインのエンティティによって組み込まれている必要があります。

- **ID プロバイダー。**ID プロバイダーは、SAML アサーションを生成するエンティティです。ID プロバイダーは、SAML アサーションを生成する前にエンド ユーザを認証すると想定されます。Web セキュリティ アプライアンスは ID プロバイダーです。
- **Service Provider（サービス プロバイダー）。**サービス プロバイダーは、SAML アサーションを消費するエンティティです。Web セキュリティ アプライアンス上に設定する SaaS アプリケーションは、サービス プロバイダーです。サービス プロバイダーは、ID プロバイダーに依存してエンド ユーザを識別し、SAML アサーションのサービス プロバイダーにその ID を通信します。サービス プロバイダーは、アサーションに基づいてアクセス コントロールを決定します。

SAML アサーションは、SAML 要求および応答内の ID プロバイダーとサービス プロバイダー間で渡される情報のコンテナです。アサーションには、サービス プロバイダーがアクセス コントロールを決定するために使用するステートメント（認証ステートメントや許可ステートメントなど）が含まれています。アサーションは <saml:Assertion> タグで始まります

SAML ダイアログはフローと呼ばれ、フローは次のいずれのプロバイダーでも開始できます。

- **サービス プロバイダーが開始するフロー。**サービス プロバイダーはアクセスを要求するエンド ユーザに問い合わせを行い、それによりユーザに ID を提供する ID プロバイダーにアクセスすることで SAML ダイアログを開始します。サービス プロバイダーが開始するフローの場合、エンド ユーザは http://www.serviceprovider.com/<*URI*> などのサービス プロバイダーのドメインを含む URL を使用してサービス プロバイダーにアクセスします。
- **ID プロバイダーが開始するフロー。**ID プロバイダーはエンド ユーザに代わってアクセスを要求するサービス プロバイダーに問い合わを行うことにより、SAML ダイアログを開始します。ID プロバイダーが開始するフローの場合、エンド ユーザは http://saas.example.com/<*URI*> などのローカル ドメインを含む URL を使用してサービス プロバイダーにアクセスします。

SaaS アプリケーションは、サービス プロバイダーが開始するフローをサポートするか、ID プロバイダーが開始するフローをサポートするかを定義します。たとえば、Salesforce は、ID プロバイダーが開始するフローをサポートし、Google Apps はサービス プロバイダーが開始するフローをサポートし、Cisco WebEx は両方をサポートします。

SaaS アプリケーションによってサポートされるフロー タイプによって、エンド ユーザがアプリケーションにアクセスする方法が決まります。詳細については、「「シングル サイン オン URL について」（P.15-5）」を参照してください。

（注）　この項は、SAML の包括的な説明を提供するものではなく、ID およびセキュリティ プロバイダーが相互に通信する方法を示すものではありません。詳細については、http://docs.oasis-open.org/security/saml/v2.0/ に記載された SAML ついての説明を参照してください。

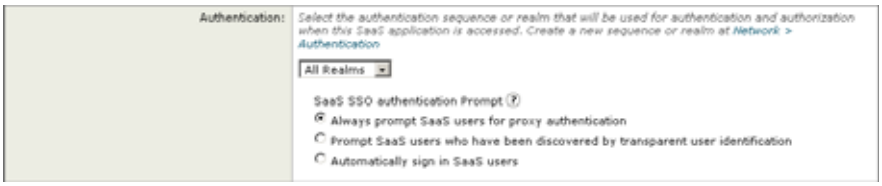
SaaS ユーザの認証

ユーザが SaaS アプリケーションにアクセスするときに、ユーザが SaaS アプリケーションにサインインする方法を選択できます。

- 常にユーザにローカル認証クレデンシャルの入力を求めるプロンプトを表示します。
- Web プロキシが透過的ユーザ ID を使用してユーザ名を取得した場合、ユーザにローカル認証クレデンシャルの入力を求めるプロンプトを表示します。
- ローカル認証クレデンシャルを使用して、ユーザが SaaS アプリケーションに自動的にサインインします。

図 15-1 は、SaaS アプリケーション認証ポリシーで SaaS ユーザがサインインする方法を設定する場所を示します。

図 15-1　SaaS ユーザとしての自動サインイン



ユーザが自動的にサインインにするように SaaS アプリケーション認証ポリシーを設定する場合、Web プロキシは、クレデンシャルを再度入力するようにユーザに求めるプロンプトを表示せずに、あらかじめユーザに関連付けられた認証クレデンシャルを使用した SaaS アプリケーションへのユーザのログインを試行します。これらのクレデンシャルは、ユーザが手動で入力するか、または透過的ユーザ ID を使用して取得できます。

ただし、ユーザは Web ブラウザに認証クレデンシャルを入力するように要求される場合があります。ユーザがユーザ クレデンシャルの入力を求められた場合、フィールドに設定されたフォームがユーザ クレデンシャルを入力できる Web ブラウザに表示されます。これは、次の状況で発生します。

これは、次のいずれかの理由により、認証情報がユーザに関連付けられていない場合に発生します。

- ユーザが Web を閲覧するために認証が必要ない場合。
- ユーザが他の Web サイトにアクセスする前に、あかかじめシングル サインオン URL に接続している場合。
- ユーザが IP ベースの認証サロゲートを使用する ID で認証され、Web セキュリティ アプライアンス上で「Client IP Idle Timeout」または「Surrogate Timeout」値の期限が切れ、タイムアウト有効期限以降、他の Web サイトにアクセスする前に、ユーザがシングル サインオン URL に接続されている場合。
- ユーザがクッキー ベースの認証サロゲートを使用する ID で認証され、「Surrogate Timeout」値の期限が切れ、タイムアウト有効期限以降、他の Web サイトにアクセスする前に、ユーザがシングル サインオン URL に接続されている場合。

シングル サインオン URL の詳細については、「シングル サイン オン URL について」（P.15-5）を参照してください。

（注）　ユーザがすでに Web セキュリティ アプライアンスによって認証されているが、SaaS アプリケーションに接続する許可を受けていない場合、ユーザは認証クレデンシャルの入力を強制される場合もあります。ユーザがポリシーの認証レルムに対して認証されていない場合、またはポリシーの認証レルムリストされているユーザの 1 人ではない場合に発生することがあります。

ユーザが認証を求められる場合、認証クレデンシャルはセキュアな HTTPS 接続を使用して Web プロキシに送信されます。アプライアンスはデフォルトで、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 接続を作成します。ほとんどのブラウザでは、証明書が無効であることがユーザに警告されます。無効な証明書のメッセージがユーザに表示されないようにするには、組織で使用する証明

書とキーのペアをアップロードします。証明書とキーのアップロードの詳細については、「クレデンシャルの暗号化と SaaS アクセス コントロールで使用する証明書およびキーのアップロード」（P.20-26）を参照してください。

（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ときに、すべてのユーザに対して明示的な転送要求を使用しシングル サイン オン動作を実行するには、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）] 設定を選択する必要があります。

認証要件

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になる場合があります。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。

したがって、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す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。認証コンテキストの設定を使用して SaaS アプリケーション認証ポリシーを作成するときに、この値を設定します。ただし、管理者は認証コンテキストの設定として、通常 [自動（Automatic）] を選択します。

SaaS アプリケーション認証ポリシーの作成の詳細については、「SaaS アプリケーション認証ポリシーの作成」（P.15-8）を参照してください。

SaaS アクセス コントロールのイネーブル化

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。アプライアンスと SaaS アプリケーションで行う設定が相互に適正に一致することが非常に重要です。

SaaS アクセス コントロールをイネーブルにすると、Web セキュリティ アプライアンスと SaaS アプリケーションへの接続を同時に開いたままにするのが最も簡単です。両方のコンポーネントの間を行き来して、両方の情報をコピー アンド ペーストします。

（注）　特定の SaaS アプリケーションの SaaS アクセス コントロールの設定方法の詳細については、技術営業担当者にお問い合わせいただくか、cisco.com Web サイトでホワイト ペーパー、ナレッジ ベース記事、ビデオ チュートリアルなどの追加情報をご覧ください。

SaaS アクセス コントロールを使用するには、次の手順を実行します。

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します。**詳細については、「「アプライアンスの ID プロバイダーとしての設定」（P.15-6）」を参照してください。
2. **SaaS アプリケーションを、シングル サイン オンに設定します。**SaaS アプリケーションを設定する場合、[セキュリティ サービス（Security Services）] > [SaaS のアイデンティティ プロバイダー（Identity Provider for SaaS）] ページで使用する証明書をアップロードする必要もあります。詳細については、SaaS アプリケーションのマニュアルを参照してください。
3. **各 SaaS アプリケーションに対して、1 つ以上の SaaS アプリケーション認証ポリシーを作成します。**詳細については、「「SaaS アプリケーション認証ポリシーの作成」（P.15-8）」を参照してください。

シングル サイン オン URL について

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、アプライアンスはシングル サインオン URL（SSO URL）を作成します。

管理者がこの URL を使用する方法は、フロー タイプによって異なります。

- **ID プロバイダーが開始するフロー。**管理者は、この SaaS アプリケーションにアクセスするエンドユーザがシングル サインオン URL を利用できるようにする必要があります。たとえば、管理者は、この URL をリンクとして含む内部 Web ページを作成できます。ユーザがログインすると、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。
- **サービス プロバイダーが開始するフロー。**管理者は、SaaS アプリケーションでこの URL を設定する必要があります。SaaS アプリケーションは、ポリシー グループの [SaaS SSO Authentication Prompt（SaaS SSO 認証プロンプト）] 設定に応じて、シングル サインオン URL を使用してブラウザ セッションをリダイレクトします。
  - **常に SaaS ユーザにプロキシ認証を要求します。**Web セキュリティ アプライアンスページには、ユーザがローカル認証クレデンシャルを入力できる場所が表示されます。有効なクレデンシャルを入力後、ユーザは SaaS アプリケーションにログインします。
  - **SaaS ユーザとして透過的にサインインします。**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。

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。変更を送信すると、[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 を確認できます。

シングル サイン オン URL の形式は次のとおりです。

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

したがって、アプライアンスの ID プロバイダーのドメイン名が idp.example.com、SaaS アプリケーション認証ポリシーのアプリケーション名が GoogleApps の場合、シングル サインオン URL は次のようになります。

http://idp.example.com/SSOURL/GoogleApps

複数のアプライアンスによる SaaS アクセス コントロールの使用

SaaS アクセス コントロールを持つ複数の Web セキュリティ アプライアンスを使用する場合は、次の手順を実行する必要があります。

- 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。
- 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。
- [セキュリティ サービス（Security Services）] > [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。次に、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。

アプライアンスの ID プロバイダーとしての設定

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。証明書とキーはアップロードするか、または生成できます。

SAML アサーションの署名に使用する証明書とキーを選択したら、各 SaaS アプリケーションに証明書をアップロードする必要があります。この操作を実行するには、[署名証明書（Signing Certificate）] 領域で [証明書をダウンロード（Download Certificate）] リンクを使用します。証明書のアップロードにより、SaaS アプリケーション（サービス プロバイダー）は、サービス プロバイダーと Web セキュリティ アプライアンス（ID プロバイダー）間の信頼関係を確立するために Web セキュリティ アプライアンスの公開キーを保持できるようになります。

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は、次のルールとガイドラインを考慮してください。

- ID プロバイダーのドメイン名は、ネットワーク内で解決可能である必要があります。たとえば、「example.com」という組織内で、「http://idp.example.com/」への透過的要求はルーティング可能なネットワークである必要があり、ネットワーク境界内の Web セキュリティ アプライアンスに到達できる必要があります。
- SaaS アクセス コントロールを持つ複数の Web セキュリティ アプライアンスを使用する場合は、各アプライアンスに同じ ID プロバイダーのドメイン名を入力し、各アプライアンスに同じ ID プロバイダーのエンティティ ID を入力する必要があります。詳細については、「複数のアプライアンスによる SaaS アクセス コントロールの使用」（P.15-5）を参照してください。
- アプライアンスに証明書とキーを生成またはアップロード後、Web セキュリティ アプライアンスが通信する各 SaaS アプリケーションに同じ証明書をアップロードする必要があります。アプライアンスから証明書をダウンロードすることにより、この操作を実行できます。
- 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、構成する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 オンに設定する際に使用する必要があります。Web セキュリティ アプライアンスと SaaS アプリケーションへの接続を同時に開いたままにするのが最も簡単です。両方のコンポーネントの間を行き来して、両方の情報をコピー アンド ペーストします。
- アプライアンスは、[アイデンティティ プロバイダーのドメイン名（Identity Provider Domain Name）] フィールドに入力した値と SaaS ポリシーで設定した SaaS アプリケーション名に基づいて、各 SaaS アプリケーションのシングル サイン オン（SSO）ログイン URL を構築します。詳細については、「シングル サイン オン URL について」（P.15-5）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）] > [SaaS のアイデンティティ プロバイダー（Identity Provider for SaaS）] ページに移動します。

ステップ 2　[設定を編集（Edit Settings）] をクリックします。

ステップ 3　[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、Web セキュリティ アプライアンスに ID プロバイダー インスタンスとしてアクセスするために仮想ドメイン名を入力します。

ID プロバイダーのドメイン名は、ネットワーク内で解決可能である必要があります。たとえば、「example.com」という組織内では、「http://idp.example.com/」への透過的要求はルーティング可能なネットワークである必要があり、ネットワーク境界内の Web セキュリティ アプライアンスに到達できる必要があります。

（注）　SaaS アクセス コントロールを持つ複数の Web セキュリティ アプライアンスを使用する場合は、各 Web セキュリティ アプライアンスに同じ ID プロバイダーのドメイン名を入力する必要があります。アプライアンスを 1 つだけ使用している場合、アプライアンスのホスト名を ID プロバイダーのドメイン名として使用できます。詳細については、「複数のアプライアンスによる SaaS アクセス コントロールの使用」（P.15-5）を参照してください。

ステップ 4　[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、通信するすべての SaaS アプリケーションに対する ID プロバイダーとして、この Web セキュリティ アプライアンスを識別するために使用するテキストを入力します。

文字列ベースの URI 形式が推奨されますが、任意の一意の文字列を入力できます。URI 文字列は、ネットワークにアクセス可能である必要はありません。SaaS アプリケーションをシングル サイン オンに設定する際に同じ値を使用する必要があるため、ここで入力する値を記録します。

（注）　SaaS アクセス コントロールを持つ複数の Web セキュリティ アプライアンスを使用する場合は、各 Web セキュリティ アプライアンスに同じ ID プロバイダーのエンティティ ID を入力する必要があります。詳細については、「複数のアプライアンスによる SaaS アクセス コントロールの使用」（P.15-5）を参照してください。

ステップ 5　アプライアンスがセキュアな接続（SAML フロー内で）を使用して通信するときに使用する署名付き証明書を設定します。証明書を設定するには、次の方法のいずれかを使用できます。

- **アップロードされた証明書およびキー。**6 に進みます。
- **生成された証明書およびキー。**7 に進みます。

（注）　アプライアンスがアップロードされた証明書とキー ペアおよび生成された証明書とキー ペアの両方を所有する場合、[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 ペアのみを使用します。

ステップ 6　ルート証明書とキーをアップロードするには、次の手順を実行します。

a. [アップロードされた証明書とキーを使用（Use Uploaded Certificate and Key）] をクリックします。

b. [証明書（Certificate）] フィールドで [ブラウズ（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。

（注）　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。

c. [キー（Key）] フィールドで [ブラウズ（Browse）] をクリックし、秘密キー ファイルに移動します。秘密キーが暗号化されていないこと。

（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。また、秘密キー 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。

d. [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情報は、[SaaS シングル サインオンのアイデンティティ プロバイダー設定を編集（Edit Identity Provider Settings for SaaS Single Sign on）] ページに表示されます。

（注）　証明書およびキーをアップロードした後で、生成された証明書をダウンロードし、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できます。この操作を実行するには、生成されたキー領域で、[証明書をダウンロード（Download Certificate）] リンクを使用します。

e. 8 に進みます。

ステップ 7　証明書とキーを生成するには、次の手順を実行します。

a. [生成された証明書とキーを使用（Use Generated Certificate and Key）] オプションをクリックします。

b. [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。

c. [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。

d. [生成（Generate）] をクリックします。Web セキュリティ アプライアンスは、入力したデータを含む証明書を生成し、キーを生成します。

生成された証明書情報は、[SaaS シングル サインオンのアイデンティティ プロバイダー設定を編集（Edit Identity Provider Settings for SaaS Single Sign on）] ページに表示されます。

（注）　証明書およびキーを生成した後で、生成された証明書をダウンロードし、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できます。この操作を実行するには、生成されたキー領域で、[証明書をダウンロード（Download Certificate）] リンクを使用します。

e. 任意で、[証明書署名要求をダウンロード（Download Certificate Signing Request）] リンクを使用して、証明書署名要求（CSR）をダウンロードし、それを認証局（CA）に送信できます。CA から署名付き証明書を受信したら、[ブラウズ（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。アプライアンスで証明書の生成後、いつでもこの操作を実行できます。

ステップ 8　変更を送信し、保存します。

SaaS アプリケーション認証ポリシーの作成

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 アプリケーションをシングル サイン オンを設定すると、Web セキュリティ アプライアンスが SaaS アプリケーションと通信し、Web ブラウザのシングル サイン オンをイネーブルにできるように、SaaS アプリケーション認証ポリシーを作成できます。

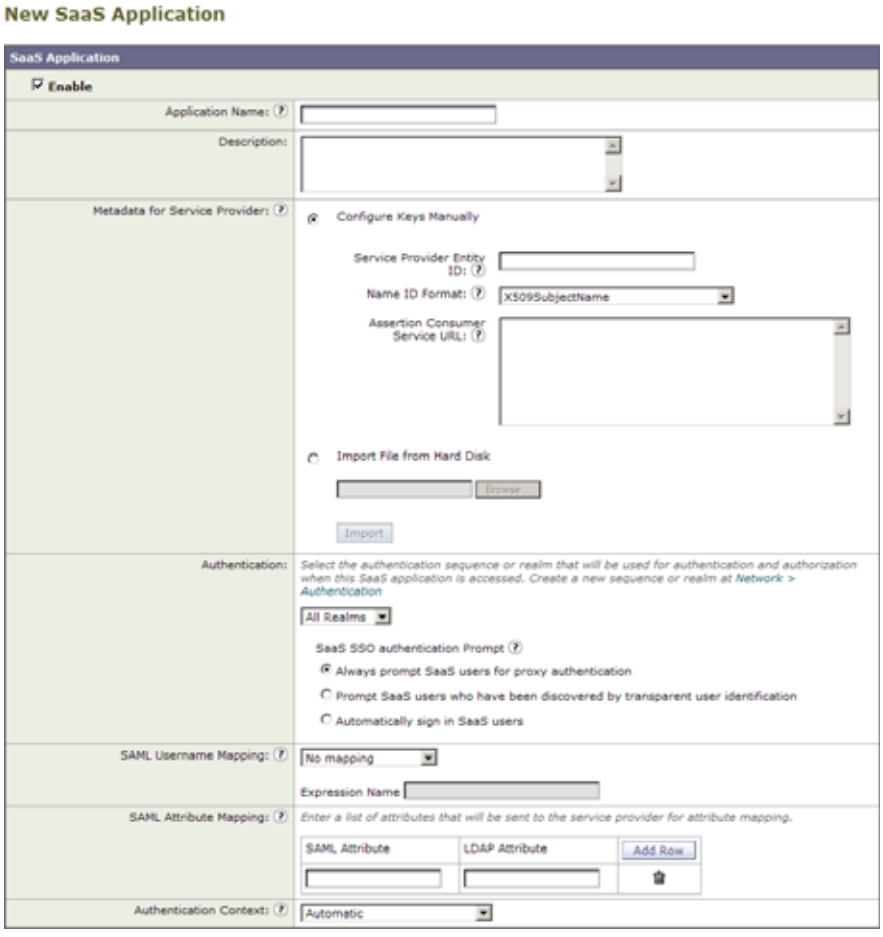
SaaS アプリケーション認証ポリシーで SaaS アプリケーション情報を設定する場合、次のルールとガイドラインを考慮してください。

- アサーション コンシューマ サービスの場所を指す URL は、ネットワーク内で解決可能である必要があります。
- アプライアンスは、アプライアンスの [アイデンティティプロバイダーのドメイン名（Identity Provider Domain Name）] フィールドに入力した値と SaaS ポリシーで設定した SaaS アプリケーション名に基づいて、各 SaaS アプリケーションのシングル サイン オン（SSO）ログイン URL を構築します。詳細については、「シングル サイン オン URL について」（P.15-5）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）] > [SaaS ポリシー（SaaS Policies）] ページに移動します。

ステップ 2　[アプリケーションの追加（Add Applications）] をクリックして、特定の SaaS アプリケーションに対して新しいポリシーを作成します。

図 15-2　SaaS アプリケーション認証ポリシーの作成



ステップ 3　表 15-1 で定義されている設定を構成します。

表 15-1　SaaS アプリケーション認証ポリシーの設定

プロパティ	説明
アプリケーション名（Application Name）	このポリシー グループの 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、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。 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 を生成できます。詳細については、「シングル サイン オン URL について」（P.15-5）を参照してください。
説明（Description）	任意で、この SaaS アプリケーション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）	このグループ 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 アプリケーションが提供するメタデータ 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、SAML を使用して 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するために、メタデータを使用します。メタデータを設定するため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。 メタデータ情報を手動で設定する場合は、次の値を設定します。 • **サービス プロバイダーのエンティティ ID。** SaaS アプリケーションがそれ自身をサービス 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。** アプライアンスが、サービス プロバイダーに送信する SAML アサーションでユーザを識別するために使用する形式を入力します。ここで入力する値は、SaaS アプリケーションで設定された対応する設定に一致する必要があります。 • **アサーション コンシューマ サービスの場所。** Web セキュリティ アプライアンスが、作成した SAML アサーションを送信する URL を入力します。使用する URL が適切かどうか確認するには、SaaS アプリケーションのマニュアルを参照してください。これはログイン URL とも呼ばれます。 **注：** 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、このファイルについては 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。
認証（Authentication）	Web プロキシがこの 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使用する認証レルムまたは認証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。 [SaaS SSO 認証プロンプト（SaaS SSO Authentication Prompt）] セクションで、ユーザが SaaS アプリケーションにサインインする方法を選択します。営業や人事データなど機密データを保存するアプリケーションで、ユーザにクレデンシャルの入力を求める場合があり、機密データを保存しないアプリケーションにユーザが透過的にサインインできるようにする場合があります。 詳細については、「SaaS ユーザの認証」（P.15-2）を参照してください。

表 15-1　SaaS アプリケーション認証ポリシーの設定 （続き）

プロパティ	説明
ユーザ名 ID マッピング（User Name Identifier 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表示する方法を指定します。 ネットワーク（マッピングなし）内で使用されるユーザ名を渡すか、または次のいずれかの方法を使用して内部ユーザ名を別の形式に変更できます。 • **固定ルール マッピング。**サービス プロバイダーに送信されるユーザ名は、内部ユーザ名の前または後に固定文字列を追加し内部ユーザ名に基づきます。内部ユーザ名に固定文字列と %s を入力します。 • **LDAP クエリー。**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。属性名を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、`<user>@<domain>.com` と入力できます。
属性マッピング オプション（Attribute Mapping Options）	任意で、SaaS アプリケーションによって要求される場合、LDAP 認証サーバから内部ユーザに関する SaaS アプリケーションの追加情報を提供できます。各 LDAP サーバ属性を SAML 属性にマッピングします。 たとえば、LDAP 属性の「mail」を SAML 属性の「Email」にマッピングできます。
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指定します。現在、Web プロキシが「PasswordProtectedTransport」を使用していますが、通常、管理者は「Automatic」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する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になる場合があります。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、保存します。

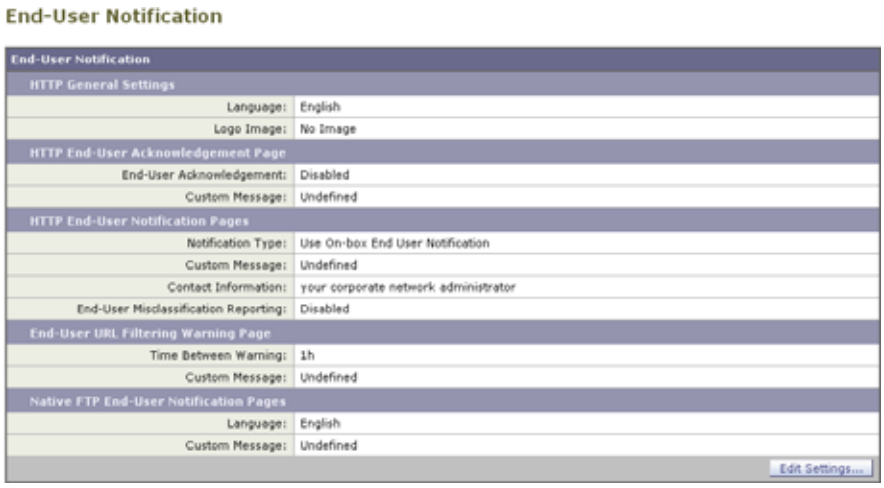
16
エンド ユーザへの通知

エンド ユーザへの組織のポリシーの通知

Web セキュリティ アプライアンスは、組織が Web にアクセスするためのポリシーを実装し、適用するのに役立ちます。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。Web ユーザは、Web サイトへのアクセスがブロックされた理由、およびユーザがブロックされた理由を示す Web ページを参照します。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。Web プロキシは、URL 要求をブロックした理由に応じてさまざまなエンド ユーザ通知ページを表示できます。アプライアンスに保存されている所定のエンド ユーザ通知ページを使用したり　独自のオフボックスを定義できます。

[セキュリティ サービス（Security Services）] > [ユーザ通知（End-User Notification）] ページでエンド ユーザ通知ページを設定します。図 16-1 は、エンド ユーザの通知設定を設定する場所を示します。

図 16-1　[セキュリティ サービス（Security Services）] > [ユーザ通知（End-User Notification）] 通知ページ



次のタイプの通知ページおよび設定を設定できます。

- **オンボックス エンド ユーザ通知ページ。**Web プロキシは、URL 要求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ページを表示します。ユーザはこれらのページをカスタマイズできます。詳細については、「「オンボックス エンド ユーザ通知ページの使用」（P.16-4）」を参照してください。
- **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。詳細については、「「エンド ユーザ通知ページをオフボックスに定義」（P.16-9）」を参照してください。
- **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および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 ユーザ確認ページが表示された場合、ユーザは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にはリンクをクリックする必要があります。言語とロゴの設定は、エンド ユーザ確認ページと通知ページに適用されます。詳細については、「「エンド ユーザ確認ページ」（P.16-12）」を参照してください。
- **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。警告ページが表示された場合、ユーザは要求した元のサイトにアクセスするためにリンクをクリックできます。言語とロゴの設定は、エンド ユーザ URL フィルタリング警告ページと通知ページに適用されます。詳細については、「「ユーザの警告と続行の許可」（P.17-22）」を参照してください。
- **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。詳細については、「「FTP 通知メッセージの設定」（P.16-17）」を参照してください。

- **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。詳細については、「通知ページの一般設定のコンフィギュレーション」（P.16-3）」を参照してください。

通知ページの一般設定のコンフィギュレーション

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 ユーザ通知ページのみのロゴを設定できます。ロゴの設定は、すべての HTTP 通知ページに適用されます。

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）] ページに移動します。

ステップ 2　[設定を編集（Edit Settings）] をクリックします。

ステップ 3　[HTTP/HTTPS] セクションの下の [一般設定（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。次のいずれかの言語を選択できます。

- 英語
- フランス語
- ドイツ語
- イタリア語
- スペイン語
- 日本語
- 韓国語
- ポルトガル語
- ロシア語
- タイ語
- 中国語（繁体字）
- 中国語（簡体字）

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、または [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 ファイルを指定できます。

（注）　カスタム ロゴの使用に関する詳細については、「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」（P.16-18）を参照してください。

ステップ 5　変更を送信し、保存します。

オンボックス エンド ユーザ通知ページの使用

オンボックス エンド ユーザ通知ページを選択すると、Web プロキシは元のページをブロックした理由に応じてさまざまなページを表示します。ただし、個々のページを組織に固有のページにカスタマイズすることもできます。

次の機能をカスタマイズできます:

- カスタム メッセージ
- 連絡先情報
- エンド ユーザが誤って分類されたページをシスコにレポートできるようにする

Web セキュリティ アプライアンスに保存されているオンボックス エンド ユーザ通知ページを手動で編集することもできます。実行方法の詳細については、「オンボックス エンド ユーザ通知ページの編集」（P.16-5）を参照してください。

オンボックス エンド ユーザ通知ページの設定

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）] 通知ページに移動し、[設定を編集（Edit Settings）] をクリックします。

ステップ 2　[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（Use On Box End User Notification）] を選択します。

ステップ 3　オンボックス エンド ユーザ通知ページ設定を設定します。

表 16-1 は、ユーザがオンボックス エンド ユーザ通知ページに設定できる設定について説明します。

表 16-1　オンボックス エンド ユーザ通知ページの設定

設定	説明
カスタムメッセージ（Custom Message）	各通知ページで指定する追加テキストを含めるかどうかを選択します。 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。 HTML タグを小文字で組み込み、テキストを書式設定できます。サポートされている 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」（P.16-18）を参照してください。 カスタム メッセージの使用に関する詳細については、「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」（P.16-18）を参照してください。

表 16-1　オンボックス エンド ユーザ通知ページの設定 （続き）

設定	説明
連絡先情報（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するかどうかを選択します。 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）	ユーザが誤って分類された URL をシスコにレポートできるかどうかを選択します。 このオプションをイネーブルにすると、不審なマルウェアまたは URL フィルタによってブロックされたサイトのオンボックス エンド ユーザ通知ページに追加のボタンが表示されます。このボタンにより、ユーザはページが誤って分類されていると確信できるページをレポートできるようになります。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。 ユーザがこのボタンを押すと、ブロックされた要求に関するデータが Web セキュリティ アプライアンスに送信されます。AsyncOS は、フィードバック ログに情報を記録し、データを要約し、それをシスコに転送します。 この機能は、管理者および Cisco IronPort カスタマー サポート プロセスの効率向上に役立ちます。また、誤分類のレポートは URL フィルタリングの有効性を向上させます。 未分類の URL と誤って分類された URL のシスコへのレポートの詳細については、「未分類の URL と誤って分類された URL の報告」（P.17-3）を参照してください。

ステップ 4　[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、別個のブラウザ 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）　（「オンボックス エンド ユーザ通知ページの編集」（P.16-5）の説明に従って）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 5　変更を送信し、保存します。

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」（P.16-8）」を参照してください。

表 16-2 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ます。

表 16-2　カスタマイズしたエンド ユーザ通知ページの変数

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	No
%A	ARP アドレス	Yes
%b	User-agent 名	No
%B	BLOCK-SRC または BLOCK-TYPE などのブロックした理由	No
%c	エラー ページの担当者	Yes
%C	Set-Cookie 全体：ヘッダー行、または空の文字列	No
%d	クライアント IP アドレス	Yes
%D	ユーザ名	No
%e	エラー ページの電子メール アドレス	Yes
%E	エラー ページのロゴの URL	No
%f	ユーザ フィードバック セクション	No
%F	ユーザ フィードバックの URL	No
%g	Web カテゴリ名（使用可能な場合）	Yes
%G	許可された最大ファイル サイズ（MB 単位）	No
%h	プロキシのホスト名	Yes
%H	URL のサーバ名	Yes
%i	16 進数値としてのトランザクション ID	Yes
%I	管理 IP アドレス	Yes
%j	URL カテゴリ警告ページのカスタム テキスト	No
%k	エンド ユーザ確認通知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	No
%K	レスポンス ファイル タイプ	No
%l	WWW-Authenticate：ヘッダー行	No
%L	Proxy-Authenticate：ヘッダー行	No
%M	「GET」または「POST」などの要求方式	Yes
%n	マルウェア カテゴリ名（使用可能な場合）	No
%N	マルウェア脅威名（使用可能な場合）	No
%o	Web レピュテーションの脅威タイプ（使用可能な場合）	No
%O	Web レピュテーションの脅威の理由（使用可能な場合）	No
%p	Proxy-Connection HTTP ヘッダーの文字列	Yes
%P	プロトコル	Yes
%q	ID ポリシー グループ名	Yes
%Q	非 ID ポリシーのポリシー グループ名	Yes
%r	リダイレクト URL	No

表 16-2　カスタマイズしたエンド ユーザ通知ページの変数 （続き）

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、空の文字列を出力し、true の場合、スペースを出力するので、単独で使用するには便利ではありません。代わりに、条件変数として使用します。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」（P.16-8）を参照してください。 再認証の詳細については、「ユーザに対する再認証の許可」（P.20-27）を参照してください。	No
%S	プロキシの署名	No。常に FALSE に評価
%t	UNIX 秒 + ミリ秒のタイムスタンプ	Yes
%T	日付	Yes
%u	URI の一部を構成する URL（サーバ名を除く URL）	Yes
%U	要求の完全な URL	Yes
%v	HTTP プロトコルのバージョン	Yes
%W	管理 WebUI ポート	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。	Yes
%Y	設定されている場合、管理者のカスタム テキスト文字列、そうでない場合、空の文字列	No
%y	エンド ユーザ確認ページのカスタム テキスト	Yes
%z	Web レピュテーション スコア	Yes
%Z	DLP メタデータ	Yes
%%	通知ページのパーセント記号（%）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。

このディレクトリには、エンド ユーザ通知ページのサポートされる各言語のサブ ディレクトリがあります。

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。

ルールとガイドラインの一覧については、「オンボックス エンド ユーザ通知ページの編集用のルールとガイドライン」（P.16-8）を参照してください。

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ときに、カスタム エンド ユーザ通知ページ オプションが現在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 プロキシが再起動されるまで、新しいファイルは有効になりません。

ステップ 9　変更を保存し、SSH クライアントを閉じます。

オンボックス エンド ユーザ通知ページの編集用のルールとガイドライン

オンボックス エンド ユーザ通知ページを編集するときは、以下のルールとガイドラインを使用します。

- 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」（P.16-18）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るファイル名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 コントロール 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。

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 ボックスのエンド ユーザ通知ページを編集するときに、現在の状態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するために、条件変数を含めることができます。たとえば、再認証を提供する場合（%R）、リダイレクト URL（%r）を含むカスタマイズしたオンボックス エンド ユーザ通知ページを作成できます。この例では、%R から条件変数を作成します。

表 16-3 は、さまざまな条件変数のフォーマットについて説明します。

表 16-3　エンド ユーザ通知ページでの条件変数の作成

条件変数のフォーマット	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。

表 16-3　エンド ユーザ通知ページでの条件変数の作成 （続き）

条件変数のフォーマット	説明
%!*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、次のテキストは、再認証が提供されるかどうかを確認するために条件変数として %R を使用し、再認証 URL を提供するために標準変数として %r を使用する HTML コードです。

```
%?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
```

表 16-2（P.16-6）に記載されている変数は条件変数として使用できます。ただし、条件ステートメントで使用する最適な変数は、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、TRUE に評価されたり、評価されなっかりする変数です。たとえば、%t 変数（UNIX 秒 + ミリ秒のタイムスタンプ）は常に TRUE に評価されるため、それに基づく if-then ステートメントの作成はほとんど意味がありません。

エンド ユーザ通知ページをオフボックスに定義

すべての通知ページを指定したカスタム URL に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。さまざまな理由でさまざまなブロック ページを表示するため、またはサードパーティ製のロギング ツールを使用してブロック イベントを記録するために、この操作が必要となる場合があります。

通知ページを URL にリダイレクトする場合、デフォルトで、AsyncOS は元のページをブロックした理由に関係なく、ブロックされたすべての Web サイトを URL にリダイレクトします。ただし、AsyncOS は、パラメータをリダイレクト URL に追加されたクエリー文字列として渡すため、ユーザがブロックされた理由を説明する独自のページを確認でき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」（P.16-10）を参照してください。

ユーザがブロックされた Web サイトのそれぞれの理由を示すページを表示するようにしたい場合は、リダイレクト URL のクエリー文字列を解析できる Web サーバで CGI スクリプトを構築します。次に、サーバは別のリダイレクトを実行して該当するページに移動できます。

ルールとガイドライン

通知ページのカスタム URL を入力する場合は、次のルールとガイドラインを考慮してください。

- 任意の HTTP または HTTPS URL を使用できます。

- URL は特定のポート番号を指定できます。
- URL は疑問符の後に引数をと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 を入力した場合、

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

および次のアクセス 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、次のリダイレクトされた 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
```

表 16-4 は、AsyncOS がクエリー文字列に含めるパラメータについて説明します。

表 16-4　リダイレクトされた URL のエンド ユーザ通知パラメータ

パラメータ名	説明
Time	トランザクションの日付と時刻。
ID	トランザクション ID。
Client_IP	クライアントの IP アドレス。
User	要求を行うユーザクライアントのユーザ名（該当する場合）。
Site	HTTP 要求の宛先ホスト名。
URI	HTTP 要求で指定された URL パス。
Status_Code	要求の HTTP ステータス コード。
Decision_Tag	DVS エンジンがトランザクションを処理した方法を示すアクセス ログ エントリで定義されている ACL デシジョン タグ。 ACL デシジョン タグの詳細については、「ACL デシジョン タグ」（P.24-20）を参照してください。

表 16-4　リダイレクトされた URL のエンド ユーザ通知パラメータ （続き）

パラメータ名	説明
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。 さまざまな URL カテゴリの一覧については、「URL カテゴリについて」（P.17-26）を参照してください。 **注：**AsyncOS for Web は、定義済みおよびユーザ定義の URL カテゴリの両方に URL カテゴリ名全体を送信します。カテゴリ名の URL エンコードを実行するため、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。 マルウェア カテゴリの詳細については、「マルウェア スキャンの判定値」（P.24-42）を参照してください。
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	ユーザが制限付き 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、ユーザが再度認証を取得するためにクリックできる URL。[URL カテゴリまたはユーザセッション制限によってエンドユーザがブロックされた場合に、再認証メッセージの表示を有効化する（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、ブロックされた 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、このパラメータを使用します。 このパラメータを使用するには、CGI スクリプトが次の手順を実行することを確認します。 1. `Reauth_Url` パラメータの値を取得します。 2. URL エンコードされた値をデコードします。 3. 値を Base64 でデコードし、実際の再認証 URL を取得します。 4. リンクまたはボタンなどの何らかの方法でデコードされた URL をエンド ユーザ通知ページに組み込みます。同時に、リンクをクリックし、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みます。 詳細については、「「ユーザに対する再認証の許可」（P.20-27）」を参照してください。

（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。

エンド ユーザ通知ページのカスタム URL へのリダイレクト

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）] 通知ページに移動し、[設定を編集（Edit Settings）] をクリックします。

ステップ 2　[通知タイプ（Notification Type）] フィールドで、[カスタム URL へのリダイレクト（Redirect to Custom URL）] を選択します。

ステップ 3　[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。

（注）　[カスタム URL のプレビュー（Preview Custom URL）] リンクをクリックすることで、入力する URL をプレビューするかどうかを選択できます。

ステップ 4　変更を送信し、保存します。

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。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、一定時間が経過後にエンド ユーザ確認ページを表示することで、これを実行します。エンド ユーザ確認ページが表示された場合、ユーザは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にはリンクをクリックする必要があります。

エンド ユーザ確認ページを使用して、組織のネットワークからワールドワイド ウェブ参照するための条件にユーザが明示的に同意するように強制する場合があります。Web ユーザには Web トランザクションがセキュリティ目的でフィルタリングされ、モニタリングされていることがわからないので、この操作は Web プロキシがトランスペアレント モードのときに役立つ場合があります。

エンド ユーザ確認ページを表示するようにアプライアンスを設定すると、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適用されます。これにより、ユーザが初めて Web サイトに最初にアクセスしようとしたとき、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るようになります。

Web プロキシは、認証がユーザ名を使用できるようにした場合、ユーザ名によってユーザを追跡します。ユーザ名が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。

表 16-5 は、エンド ユーザ確認ページをイネーブルにするときに設定可能な設定について説明します。

表 16-5　エンド ユーザ確認ページの設定

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。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、[確認応答の時間間隔（Time Between Acknowledgements）] に入力した時間、そのユーザがプロキシを確認するのを考慮します。この設定は、ユーザ名で追跡されるユーザ、および IP アドレスまたはセッション Cookie で追跡されるユーザに適用されます。30 ～ 2678400 秒（1 か月）の任意の値を指定できます。デフォルトは 1 日（86400 秒）です。 [確認応答の時間間隔（Time Between Acknowledgements）] を変更し、確定すると、Web プロキシは Web プロキシを確認済みのユーザにも新しい値を使用します。
非アクティビティ タイムアウト：（Inactivity Timeout）	[非アクティビティ タイムアウト：（Inactivity Timeout）] では、ユーザが確認済みと見なされる前に、IP アドレスまたはセッション Cookie（未認証ユーザのみ）によって追跡され、確認されたユーザがアイドル状態を維持する時間を指定します。30 ～ 2678400 秒（1 か月）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。

表 16-5　エンド ユーザ確認ページの設定

設定	説明
サロゲートタイプ（Surrogate Type）	[サロゲートタイプ（Surrogate Type）] では、Web プロキシがユーザを追跡するためにを使用する方式を指定します。 • **IP Address.**[IP アドレス（IP Address）] を選択すると、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、新しい確認が非アクティブのため、または設定された時間間隔により 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、ユーザが Web アクセスできるようになります。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の期限が切れない限り、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。 • **Session Cookie。**[セッションクッキー（Session Cookie）] を選択すると、Web プロキシは、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、クッキーを使用してセッションを追跡するときに、ユーザの Web ブラウザにクッキーを送信します。ユーザは、[確認応答の時間間隔（Time Between Acknowledgements）] の値の期限が切れ、割り当てられた時間より長い時間にわたって非アクティブになるか、または Web ブラウザを閉じるまで、Web にアクセスできます。ブラウザ以外の HTTP クライアント アプリケーションがマルウェア クライアントなど、エンド ユーザの確認なしに Web にアクセスするの防止するために、セッション Cookie を使用する場合があります。 ユーザがブラウザ以外の HTTP クライアント アプリケーションを使用している場合、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する必要があります。ユーザが別の Web ブラウザ アプリケーションを開く場合、Web プロキシが別の Web ブラウザにセッション Cookie を送信するために、ユーザは再度エンド ユーザ確認プロセスを経由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。これらの問題の回避策の詳細については、「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」（P.16-15）を参照してください。
カスタム メッセージ（Custom message）	カスタム メッセージは、すべてのエンド ユーザ 確認ページ上に表示されるように入力したテキストです。一部の単純な HTML タグを組み込んでテキストを書式設定できます。たとえば、テキストの色とサイズを変更したり、イタリック体で表示させることができます。詳細については、「「通知ページのカスタム テキスト」（P.16-18）」を参照してください。 **（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。CLI では実行できません。

エンド ユーザ確認ページをイネーブルにする場合は、次のルールとガイドラインを考慮してください。

- 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および 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 ブラウザを閉じてから再起動するか、別の Web ブラウザ アプリケーションを開くときにエンド 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。これらの問題の回避策の詳細については、「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」（P.16-15）を参照してください。
- 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 ユーザ確認ページには最初に要求された URL にユーザをリダイレクトするリンクにドメイン名のみが含まれます。最初に要求された URL のドメイン名の後にテキストが含まれている場合、このテキストは切り捨てられます。
- エンド ユーザ確認ページがユーザに表示されると、そのトランザクションのアクセス ログ エントリには ACL デシジョン タグとして OTHER が表示されます。これは、最初に要求した URL がブロックされ、代わりにユーザにはエンド ユーザ確認ページが表示されたためです。

エンド ユーザ確認ページによる 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。ユーザに使用可能なユーザ名がない限り、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。

ただし、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。

- **HTTPS。**Web プロキシは、ユーザがクッキーを使用してエンド 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クッキーを取得できません。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ときに、HTTPS 要求をバイパス（パス スルー）するか、または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 要求に対して実行するアクション（「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クッキーを送信することはないので、Web プロキシはクッキーを取得できません。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://」を使用してカスタム URL カテゴリ（引用符なし）を作成し、このカスタム URL カテゴリのエンド ユーザ確認ページからユーザを免除する ID ポリシー定義してこの操作を実行します。

エンド ユーザ確認ページの設定

Web インターフェイスまたはコマンドライン インターフェイスのエンド ユーザ確認ページをイネーブルにし、設定できます。ただし、Web インターフェイスのエンド ユーザ確認ページを設定する場合、各ページに表示されるカスタム メッセージを含めることができます。フォントの色やサイズなど、カスタム メッセージに一部の単純な HTML タグを追加できます。

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）] > [ユーザ通知（End-User Notification）] ページに移動します。

ステップ 2　[設定を編集（Edit Settings）] をクリックします。

ステップ 3　[エンドユーザ確認応答ページ（End-User Acknowledgement Page）] セクションで、[エンド ユーザによる、確認応答ページのクリックを必須とする（Require end-user to click through acknowledgement page）] フィールドをイネーブルにします。この機能によるカスタム メッセージの処理方法の詳細については、「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」（P.16-18）を参照してください。

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に使用する時間間隔を入力します。

30 ～ 2678400 秒（1 か月）の任意の値を指定できます。デフォルトは 1 日（86400 秒）です。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　[非アクティビティ 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 秒（1 か月）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）] に [IP アドレス（IP Address）] または [セッション クッキー（Session Cookie）] 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。

HTML タグを小文字で組み込み、テキストを書式設定できます。サポートされている 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」（P.16-18）を参照してください。

次に例を示します。

インターネットにアクセスする 前に 、次の内容を確認してください。

ステップ 8　[確認応答ページのカスタマイズをプレビュー（Preview Acknowledgment Page Customization）] リンクをクリックして、別個のブラウザ ウィンドウで現在のエンド 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、保存します。

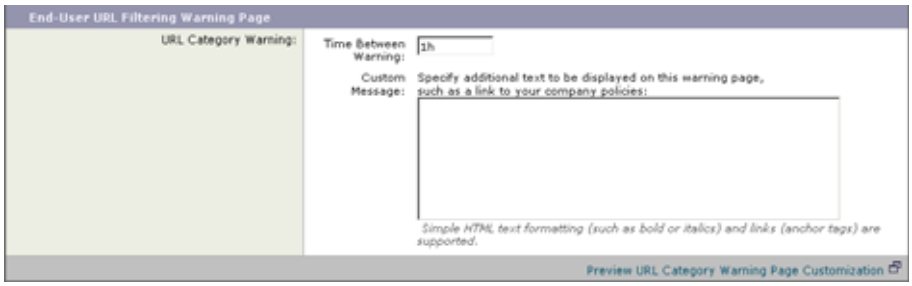
エンド ユーザ URL フィルタリング警告ページの設定

[セキュリティ サービス（Security Services）] > [ユーザ通知（End-User Notification）] 通知ページで、エンド ユーザ URL フィルタリング警告ページを設定できます。フォントの色やサイズなど、カスタム メッセージに一部の単純な HTML タグを追加できます。

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）] 通知ページに移動し、[設定の編集（Edit Settings）] をクリックします。

ステップ 2　[エンドユーザ URL フィルタの警告ページ（End-User URL Filtering Warning Page）] セクションまでスクロール ダウンします。

図 16-2　エンド ユーザ URL フィルタリング警告ページ設定の編集



ステップ 3　[警告の時間間隔（Time Between Warning）] フィールドで、Web プロキシがユーザごとの各 URL カテゴリ用にエンド ユーザ URL フィルタリング警告ページを表示する間に使用する時間間隔を入力します。

ユーザがエンド ユーザ URL フィルタリング警告ページで [継続（Continue）] リンクをクリックすると、Web プロキシは、ここで入力した時間中ユーザが警告を確認するのを考慮します。この設定は、ユーザ名で追跡されるユーザ、および IP アドレスで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 4　[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。

組織の利用規定に対してテキストを含めたり、利用規定を詳しく説明するページへのリンクを含めたりする必要がある場合があります。

HTML タグを小文字で組み込み、テキストを書式設定できます。サポートされている 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」（P.16-18）を参照してください。

次に例を示します。

インターネットにアクセスする 前に 、次の内容を確認してください。

ステップ 5　[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）] リンクをクリックして、別個のブラウザ 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 6　変更を送信し、保存します。

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）] > [ユーザ通知（End-User Notification）] 通知ページに移動し、[設定を編集（Edit Settings）] をクリックします。

ステップ 2　[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 3　[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 4　[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 5　変更を送信し、保存します。

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されるカスタム 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

一部の HTML タグを使用して、オンボックス エンド ユーザ通知、およびエンド ユーザ確認ページのテキストを書式設定できます。タグは小文字で、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。

```
インターネットにアクセスする<i>前に</i>、次の内容を確認してください。
```

 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">警告：</span>インターネットにアクセスする<i>前に</i>、次の内容を確認する必要があります。
```

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 パスおよびドメイン名のすべての組み合わせとオンボックス エンド ユーザ通知、エンド ユーザ確認、およびエンド 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`

次のすべての URL もすべてのスキャンから免除されるように扱われます。

`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>/` の場合、ホスト上のディレクトリ パスの下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スキャンから免除されます。

たとえば、`http://www.example.com/gallery2/` という URL が埋め込まれている場合、`http://www.example.com/gallery2/main.php` などの URL も免除として扱われます。

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もあります。

通知ページのタイプ

インターネットにアクセスするユーザが目的のサーバにアクセスできない場合があります。デフォルトで、Web プロキシは、ユーザがされたこと、およびブロックされた理由をユーザに知らせる通知ページを表示します。この項では、ユーザがインターネットへのアクセス中に表示される可能性のあるすべての通知ページの一覧を示し、説明します。

通知ページを表示する可能性のある理由には、次のようなものがあります。

- エンド ユーザ通知ページがイネーブルになっている場合で、ユーザがアクセス ポリシーに違反した方法でインターネットにアクセスした場合。
- エンド ユーザが誤って分類されたページをシスコにレポートできるようにエンド ユーザ通知ページが設定されている場合で、ユーザが誤って分類されたページをレポートした場合。
- エンド ユーザ確認ページがイネーブルになっている場合で、タイムアウトの期限が切れた後にユーザが最初にインターネットにアクセスした場合。
- Web セキュリティ アプライアンスが、DNS の障害またはサーバの使用不能など、外部エラーによってサーバにアクセスできなかった場合。

ほとんどの通知ページは、管理者または Cisco IronPort カスタマー サポートが潜在的な問題をトラブルシューティングするのに役立つ可能性のあるさまざまなコードのセットを表示します。一部のコードはシスコ社内でのみ使用されます。通知ページに表示される可能性のあるさまざまなコードは、表 16-2（P.16-6）に一覧で示された、カスタマイズされた通知ページに含めることができる変数と同じです。

表 16-6 は、ユーザが直面する可能性のあるさまざまな通知ページについて説明します。

表 16-6　通知ページのタイプ

ファイル名および通知の件名	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、 ありがとうございました	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（Notification）] ページ。	誤分類のレポートが送信されました。フィードバックいただき、ありがとうございました。
ERR_ADAPTIVE_SECURITY ポリシー：全般	ユーザが Adaptive Scanning 機能によってブロックされたときに表示される [ブロック（Block）] ページ。	コンテンツがセキュリティ リスクになると判定されたため、組織のセキュリティ ポリシーに基づき、この Web サイトの *<URL>* がブロックされました。
ERR_ADULT_CONTENT ポリシーの確認	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。次のリンクをクリックして、このコンテンツ タイプ用のインターネットの使用を管理する組織のポリシーを読み、同意していることを確認します。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。この種類の Web ページに引き続きアクセスする場合は、このステートメントを確認するように定期的に要求されます。 このステートメントに同意し、インターネットにアクセスするには、ここをクリックします。
ERR_AVC ポリシー：アプリケーションの制御	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（Block）] 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。
ERR_BAD_REQUEST Bad Request	無効なトランザクション要求によって生成された [エラー（Error）] ページ。	システムはこの要求を処理できません。非標準ブラウザが無効な HTTP 要求を生成した可能性があります。 標準ブラウザを使用している場合は、要求を再試行します。
ERR_BLOCK_DEST ポリシー：宛先	ユーザがブロックされた Web サイトのアドレスにアクセスしようとしたときに表示される [ブロック（Block）] 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。

表 16-6　通知ページのタイプ（続き）

ファイル名および 通知の件名	通知の説明	通知テキスト
ERR_BROWSER セキュリティ：ブラウザ	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ときに表示される [ブロック（Block）] 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。「<*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。 <*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供してください。 非標準ブラウザを使用している場合で、誤って分類されたと確信する場合、次のボタンを使用してこの誤分類をレポートします。
ERR_BROWSER_CUSTOM ポリシー：ブラウザ	トランザクション要求がブロックされたユーザ エージェントから発信されたときに表示される [ブロック（Block）] 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。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。
ERR_CERT_INVALID 無効な証明書	要求された HTTPS サイトが無効な証明書を使用しているときに表示される [ブロック（Block）] ページ。	サイト <*ホスト名*> が無効な証明書を提供したため、セキュア セッションは確立できません。
ERR_CONTINUE_UNACKNOWLEDGED ポリシーの確認	ユーザが警告アクションが割り当てられていたカスタム URL カテゴリにあるサイトを要求したときに表示される [警告（Warning）] 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。次のリンクをクリックして、このコンテンツ タイプ用のインターネットの使用を管理する組織のポリシーを読み、同意していることを確認します。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。この種類の Web ページに引き続きアクセスする場合は、このステートメントを確認するように定期的に要求されます。 このステートメントに同意し、インターネットにアクセスするには、ここをクリックします。
ERR_DNS_FAIL DNS の障害	要求された URL に無効なドメイン名が含まれているときに表示される [エラー（Error）] 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）が失敗しました。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。 入力したインターネット アドレスのスペルをチェックしてください。スペルが正しい場合、後でこの要求を試行してください。

表 16-6　通知ページのタイプ （続き）

ファイル名および 通知の件名	通知の説明	通知テキスト
ERR_EXPECTATION_FAILED 予測の失敗	トランザクション要求が HTTP 417「Expectation Failed」応答をトリガーするときに表示される [エラー（Error）] ページ。	システムはこのサイト <*URL*> の要求を処理できません。非標準ブラウザが無効な HTTP 要求を生成した可能性があります。 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。
ERR_FILE_SIZE ポリシー：ファイル サイズ	要求されたファイルが許容される最大ファイル サイズより大きいときに表示される [ブロック（Block）] ページ。	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。
ERR_FILE_TYPE ポリシー：ファイル タイプ	要求されたファイルがブロックされたファイル タイプであると表示される [ブロック（Block）] ページ。	ファイル タイプ「<*ファイル 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 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。
ERR_FILTER_FAILURE フィルタの障害	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）] に設定されているときに表示される [エラー（Error）] 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*> の要求は拒否されました。 後で要求を再試行してください。
ERR_FOUND 検出	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 <*リダイレクトされた URL*> にリダイレクトされます。
ERR_FTP_ABORTED FTP 中断	FTP over HTTP トランザクション要求が HTTP 416「Requested Range Not Satisfiable」応答をトリガーするときに表示される [エラー（Error）] ページ。	ファイル <*URL*> の要求が成功しませんでした。FTP サーバ <*ホスト名*> が予期せずに接続を終了しました。 後で要求を再試行してください。
ERR_FTP_AUTH_REQUIRED FTP 認可の要求	FTP over HTTP トランザクション要求が FTP 530「Not Logged In」応答をトリガーするときに表示される [エラー（Error）] ページ。	認証は FTP サーバ <*ホスト名*> によって行われる必要があります。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する必要があります。 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。通常、匿名ユーザとしてこのサーバに接続する場合は、後で再試行してください。
ERR_FTP_CONNECTION_FAILED FTP 接続の失敗	FTP over HTTP トランザクション要求が FTP 425「Can't open data connection」応答をトリガーするときに表示される [エラー（Error）] ページ。	システムが FTP サーバ <*ホスト名*> と通信できません。FTP サーバが一時的または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。 入力したアドレスのスペルをチェックしてください。スペルが正しい場合、後でこの要求を試行してください。

表 16-6　通知ページのタイプ （続き）

ファイル名および 通知の件名	通知の説明	通知テキスト
ERR_FTP_FORBIDDEN FTP の禁止	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るときに表示される [エラー（Error）] ページ。	アクセスは FTP サーバ *<ホスト名>* によって拒否されました。ユーザ ID には、このドキュメントにアクセスする権限がありません。
ERR_FTP_NOT_FOUND FTP が検出されない	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るときに表示される [エラー（Error）] ページ。	ファイル *<URL>* が見つかりませんでした。アドレスが間違っているか、または廃止されています。
ERR_FTP_SERVER_ERR FTP サーバ エラー	FTP をサポートしないサーバにアクセスしようとする FTP over HTTP トランザクションに表示される [エラー（Error）] 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。FTP サーバが一時的または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。 有効なアドレスかどうか確認してください。スペルが正しい場合、後でこの要求を試行してください。
ERR_FTP_SERVICE_UNAVAIL FTP サービス使用不可	使用できない FTP サーバにアクセスしようとする FTP over HTTP トランザクションに表示される [エラー（Error）] ページ。	システムが FTP サーバ *<ホスト名>* と通信できません。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。 有効なアドレスかどうか確認してください。スペルが正しい場合、後でこの要求を試行してください。
ERR_GATEWAY_TIMEOUT ゲートウェイのタイムアウト	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（Error）] 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。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。 入力したインターネット アドレスのスペルをチェックしてください。スペルが正しい場合、後でこの要求を試行してください。
ERR_IDS_ACCESS_FORBIDDEN IDS アクセスの禁止	設定済みの Cisco IronPort 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するときに表示される [ブロック（Block）] 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。ファイルの詳細： *<ファイルの詳細>*
ERR_INTERNAL_ERROR Internal Error	内部エラーがある場合に表示される [エラー（Error）] ページ。	ページ *<URL>* の要求を処理する際の内部システム エラー。 この要求を再試行してください。 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供してください。

表 16-6　通知ページのタイプ （続き）

ファイル名および 通知の件名	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	ファイルのダウンロード時にマルウェアが検出されたときに表示される [ブロック（Block）] ページ。	コンピュータまたは組織のセキュリティ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、この Web サイト <*URL*> がブロックされました。 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。
ERR_MALWARE_SPECIFIC_OUTGOING セキュリティ：マルウェアの検出	ファイルのアップロード時にマルウェアが検出されたときに表示される [ブロック（Block）] ページ。	受信側端末のネットワーク セキュリティに有害なマルウェアがファイルに含まれていることが判明したため、組織のポリシーに基づき、URL（<*URL*>）へのファイルのアップロードがブロックされました。 マルウェア名：<*マルウェアの名*> マルウェア テゴリ：<*マルウェア 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 クライアントに表示される [ブロック（Block）] メッセージ。	530 ログインが拒否されました
ERR_NO_MORE_FORWARDS これ以上転送なし	アプライアンスがネットワーク上の Web プロキシと他のプロキシ サーバ間で転送ループを検出したときに表示される [エラー（Error）] ページ。Web プロキシはループを切断し、このメッセージをクライアントに表示します。	ページ <*URL*> の要求は失敗しました。 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ためにポート番号を指定する必要があります。
ERR_POLICY ポリシー：全般	要求が何らかのポリシー設定によってブロックされるときに表示される [ブロック（Block）] 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。
ERR_PROTOCOL ポリシー：プロトコル	使用するプロトコルに基づいて要求がブロックされるときに表示される [ブロック（Block）] 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。
ERR_PROXY_AUTH_REQUIRED プロキシ認可の要求	ユーザが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（Notification）] 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、認証が必要になります。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する必要があります。
ERR_PROXY_PREVENT_MULTIPLE_LOGIN 別のマシンからログイン済み	誰かが別のマシンの 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 にアクセスしようとしたときに表示される [ブロック（Block）] 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。 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、別のユーザ名とパスワードを入力します。
ERR_PROXY_REDIRECT Redirect	[リダイレクション（Redirection）] ページ。	この要求は、リダイレクトされています。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。

表 16-6　通知ページのタイプ （続き）

ファイル名および 通知の件名	通知の説明	通知テキスト
ERR_PROXY_UNACKNOWLEDGED ポリシーの確認	エンド ユーザ確認ページ。 詳細については、「エンド ユーザ確認ページ」(P.16-12)」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、次の内容を確認してください。 Web トランザクションは、危険なコンテンツを検出し、組織のポリシーを適用するために、自動的にモニタされ、処理されます。次のリンクをクリックすることで、このモニタリングに同意し、ユーザが参照するサイトに関するデータが記録される場合があることを承認します。モニタリング システムの存在を承認するように定期的に要求されます。インターネット アクセスに関する以下の組織のポリシーに責任を負います。 このステートメントに同意し、インターネットにアクセスするには、ここをクリックします。
ERR_PROXY_UNLICENSED プロキシのライセンスなし	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（Block）] 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 アクセスは使用不能です。 *<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供してください。 **（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、ポートに設定された IP アドレスを入力します。
ERR_RANGE_NOT_SATISFIABLE 範囲が不適切	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（Error）] ページ。	システムはこの要求を処理できません。非標準ブラウザが無効な HTTP 要求を生成した可能性があります。 標準ブラウザを使用している場合は、要求を再試行します。
ERR_REDIRECT_PERMANENT 永続的リダイレクト	内部リダイレクション ページ。	ページ *<URL>* は *<リダイレクトされた URL>* にリダイレクトされます。
ERR_REDIRECT_REPEAT_REQUEST Redirect	内部リダイレクション ページ。	要求を繰り返します。
ERR_SAAS_AUTHENTICATION SaaS ポリシー：アクセス拒否	ユーザが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（Notification）] ページ。これは、SaaS アプリケーションへのアクセスに便利です。	組織のポリシーに基づき、*<URL>* へのアクセス要求がログイン クレデンシャルを入力する必要があるページにリダイレクトされました。認証に成功し、適切な特権が付与されている場合、アプリケーションへのアクセスが許可されます。

表 16-6　通知ページのタイプ （続き）

ファイル名および 通知の件名	通知の説明	通知テキスト
ERR_SAAS_AUTHORIZATION SaaS ポリシー：アクセス拒否	ユーザがアクセス権限のない SaaS アプリケーションにアクセスしようとしたときに表示される [ブロック（Block）] ページ。	権限を持つユーザではないため、組織のポリシーに基づき、SaaS 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。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たユーザのユーザ名とパスワードを入力します。
ERR_SAML_PROCESSING SaaS ポリシー：アクセス拒否	SaaS アプリケーションにアクセスするために、内部プロセスがシングル サインオン URL を処理しようとして失敗した場合に表示される [エラー（Error）] 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。
ERR_SERVER_NAME_EXPANSION サーバ名の拡張	自動的に URL を拡張し、ユーザを更新された URL に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>* は省略形で表示され、*<リダイレクトされた URL>* にリダイレクトされます。
ERR_URI_TOO_LONG URI が長すぎる	URL の長さが長すぎるときに表示される [ブロック（Block）] ページ。	要求された URL が長すぎるため、処理にできませんでした。これは、ネットワークへの攻撃を表す場合があります。 *<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供してください。
ERR_WBRS セキュリティ：マルウェアのリスク	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 フィルタがサイトをブロックするときに表示される [ブロック（Block）] ページ。	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セキュリティ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、この Web サイト *<URL>* がブロックされました。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。 *脅威のタイプ*：%o *脅威の理由*：%O
ERR_WEBCAT ポリシー：URL フィルタリング	ユーザがブロックされた URL カテゴリの Web サイトにアクセスしようとするときに表示される [ブロック（Block）] ページ。	Web カテゴリ「*<カテゴリ 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 Web サイト *<URL>* へのアクセスがブロックされました。
ERR_WWW_AUTH_REQUIRED WWW 認可の要求	要求されたサーバが続行するためにユーザに認証クレデンシャルの入力を要求する場合に表示される [通知（Notification）] ページ。	要求された Web サイト *<ホスト名>* にアクセスするために認証が要求されます。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する必要があります。

17
URL フィルタ

URL: フィルタの概要

Web 用 AsyncOS により、管理者は特定の HTTP または HTTPS 要求の Web サーバ カテゴリをベースにしたユーザ アクセスを制御することができます。たとえば、ギャンブル関連の Web サイトに対するすべての HTTP 要求をブロックしたり、Web ベースの電子メール Web サイトに対するすべての HTTPS 要求を復号化することができます。

ポリシー グループを使用して、不適切または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ア ポリシーを作成できます。各ポリシー グループのカテゴリ ブロッキングを設定する場合、実際にブロック、ドロップ、許可、または復号化するサイトは、選択するサイトによって異なります。

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 IronPort Web 使用コントロール 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 フィルタリングです。プレフィックスとキーワードによってカテゴリが判別されない場合は、Dynamic Content Analysis エンジンによるリアルタイム応答コンテンツ分析を使用します。これには、80 を超える定義済みの URL カテゴリが含まれます。このエンジンは、エンドユーザと管理者がデータベースのカテゴリ化に今後含めるため、誤って分類された URL と未分類の URL をシスコに報告できるようにします。詳細については、「「Dynamic Content Analysis エンジン」（P.17-2）」を参照してください。

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:

- **ポリシー グループのメンバーシップの定義。**要求 URL の URL カテゴリ別にポリシー グループのメンバーシップを定義できます。

- **HTTP、HTTPS、および FTP 要求へのアクセスの制御。**アクセス ポリシーを使用して URL カテゴリ別に HTTP 要求および FTP 要求を許可またはブロックすることを選択できます。また復号化ポリシーを使用して URL カテゴリ別に HTTPS 要求をパススルー、ドロップ、または復号化することができます。Cisco IronPort データ セキュリティ ポリシーを使用して URL カテゴリ別にアップロード要求をブロックするかどうかも選択できます。詳細については、「「URL カテゴリを使用したトランザクションのフィルタリング」（P.17-10）」を参照してください。

URL フィルタリング エンジンに付いている定義済み URL カテゴリに加え、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ができます。詳細については、「「カスタム URL カテゴリの作成および編集」（P.17-16）」を参照してください。

Dynamic Content Analysis エンジン

Dynamic Content Analysis エンジンは、クライアント要求の URL だけを使用して分類に失敗したトランザクションを分類するために応答時間に呼び出されるスキャン エンジンです。組織のトラフィックがインターネット上のより新しいサイトにアクセスし、そのためまだ分類されていない場合、Dynamic Content Analysis をイネーブルにする必要がある場合があります。

[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）] ページで Cisco IronPort Web 使用コントロール をイネーブルにする場合、Dynamic Content Analysis エンジンをイネーブルにします。

Dynamic Content Analysis エンジンが URL を分類したら、一時的なキャッシュにカテゴリの判定と URL を保存します。これにより、これ以降のトランザクションが以前の応答のスキャンを活用でき、応答時間ではなく、要求時間で分類されるため、全体的なパフォーマンスが向上します。

Dynamic Content Analysis エンジンは、アクセス ポリシーのみで Web サイトへのアクセスを制御するときに URL を分類します。ポリシー グループのメンバーシップを判別するとき、または復号化または Cisco IronPort 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ときに、URL を分類しません。これは、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で機能するためであり、応答がサーバからダウンロードされる前に要求時間で実行されなければならない決定では使用できません。

Dynamic Content Analysis 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場合があります。ただし、ほとんどのトランザクションは Cisco IronPort Web 使用コントロール URL カテゴリ データベースを使用して分類されるため、Dynamic Content Analysis エンジンは通常、トランザクションのわずかな割合にのみ呼び出されます。

（注）　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 が定義済みの URL カテゴリでポリシー メンバーシップを定義し、アクセス ポリシーで同じ URL カテゴリのアクションを実行することができます。この場合、ID およびアクセス 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が、サーバ応答を受信した後で Dynamic Content Analysis エンジンで分類することができます。このシナリオでは、Cisco IronPort Web 使用コントロール は Dynamic Content Analysis エンジンからのカテゴリの判定を無視し、URL は残りのトランザクションに対して「未分類」を保持します。ただし、これ以降のトランザクションは、引き続き新規のカテゴリの判定を活用できます。

未分類の URL

未分類の URL は、定義済みの URL カテゴリまたは*付属*のカスタム URL カテゴリに一致しない 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場合、カスタム URL カテゴリはポリシー グループ メンバーシップに選択されている場合にだけ含まれていると見なされます。

一致しないカテゴリに分類されたすべてのトランザクションが [レポート（Reporting）] > [URL カテゴリ（URL Categories）] ページで「Uncategorized URL」として報告されます。未分類の URL の多くが内部ネットワーク内で要求から Web サイトに生成されます。内部トランザクションのこのタイプが誤ってレポート データを拡張し、URL フィルタリング エンジンの影響を誤って伝えることがあるので、カスタム URL カテゴリを使用して内部 URL をグループ化し、すべての要求を内部 Web サイトに許可することを推奨します。これは、「Uncategorized URL」として報告される Web トランザクションの数を減らし、「URL Filtering Bypassed」統計情報の一部として内部トランザクションを報告します。

詳細については、「フィルタリングおよび未分類のデータの概要」（P.17-24）を参照してください。

カスタム URL カテゴリの作成の詳細については、「カスタム URL カテゴリの作成および編集」（P.17-16）を参照してください。

URL カテゴリへ URL の照合

URL フィルタリング エンジンがクライアント要求の URL に URL カテゴリを照合する場合、まずポリシー グループに*含まれる*カスタム URL カテゴリに対して URL を評価します。要求の URL が付属のカスタム カテゴリに一致しない場合、URL フィルタリング エンジンは定義済みの URL カテゴリと比較します。URL が含まれていたカスタム URL カテゴリまたは定義済みの URL カテゴリに一致しない場合、要求は分類されません。

（注）　ポリシー グループのメンバーシップを判別する場合、カスタム URL カテゴリはポリシー グループ メンバーシップに選択されている場合にだけ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 と誤って分類された URL の報告」（P.17-3）の URL に移動します。

未分類の URL の詳細については、「未分類の URL」（P.17-2）を参照してください。

未分類の URL と誤って分類された URL の報告

Cisco IronPort Web 使用コントロール を使用して、未分類の URL と誤って分類された URL をシスコに報告できます。シスコは複数の URL を同時に送信できる URL 送信ツールを Web サイトに提供します。

`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 [送信された 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 に対して割り当てられた 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 カテゴリのデータベースによって判別されます。Web セキュリティ アプライアンスは情報を収集し、各 URL フィルタリング エンジンの個別のデータベースを維持します。フィルタリング カテゴリ データベースは、Cisco Ironport アップデート サーバ（`https://update-manifests.ironport.com`）からアップデートを定期的に受信します。サーバ アップデートは自動化され、更新間隔はアプライアンスとは対照的にサーバによって設定されます。データベース への更新は定期的に行われ、管理者の介入が必要とされません。

Cisco IronPort Web 使用コントロール は Web レピュテーション フィルタ（WBRS）データベースと一部のデータベース コンポーネントを共有します。この共有情報のため、シスコでは SensorBase ネットワークに全面的に参加することを推奨します。その理由は、Cisco IronPort Web 使用コントロール が Dynamic Content Analysis エンジンによって動的に分類されたすべての URL（それ以外の場合は分類されないすべての URL を含む）を検証および分類することを可能にして、全体的な効果を高めるからです。

更新間隔と Cisco IronPort アップデート サーバの詳細については、「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」（P.26-43）を参照してください。

URL カテゴリ データベースには、さまざまな要素、シスコ内およびインターネットからのデータ ソースが含まれます。折にふれて考慮される要素の 1 つは、最初のものから大幅に変更されたオープン ディレクトリ プロジェクトの情報です。

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 と誤って分類された URL の報告」（P.17-3）の URL に移動します。

URL フィルタリング エンジンの設定

定義済みカテゴリ設定をポリシー グループに適用し、カスタム設定をネットワーク トランザクションを管理するように設定するには、次のセクションを参照してください。デフォルトでは、Cisco IronPort Web 使用コントロール URL フィルタリング エンジンがシステム セットアップ ウィザードでイネーブルです。

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）] ページに移動します。

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

ステップ 3　[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。

（注）　Application Visibility and Control 設定の詳細については、第 18 章「アプリケーションの可視性と制御について」を参照してください。

ステップ 4　Dynamic Content Analysis エンジンをイネーブルにするかどうかを選択します。

Dynamic Content Analysis エンジンの詳細については、「Dynamic Content Analysis エンジン」（P.17-2）を参照してください。

ステップ 5　URL フィルタリング エンジンを利用できないときに、Web プロキシが使用する必要がある [モニタ（Monitor）] または [ブロック（Block）] のデフォルトのアクションを選択します。デフォルトは [モニタ（Monitor）] です。

ステップ 6　変更を送信し、保存します。

URL カテゴリのセットに対する更新の管理

Cisco IronPort Web 使用率制御の事前定義された 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更新されることがあります。

URL カテゴリ セットへの更新は、「URL カテゴリ データベース」（P.17-4）で説明されるように、新しい URL を追加し、誤分類された URL をリマップする変更とは違います。カテゴリ セットの更新は、既存のポリシーの設定を変更するので、ユーザからのアクションが必要になります。

URL カテゴリ セットの更新は、製品のリリース間で生じる可能性があり、AsyncOS のアップグレードは必要ありません。各アップデートについての情報は、http://www.cisco.com/en/US/products/ps10164/prod_release_notes_list.html から入手できます。

次のアクションを実行してください。

実行する時期	詳細については次のセクションを参照
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 セットの更新の影響について」（P.17-5） • 「URL カテゴリ セットの更新の制御」（P.17-8） • 「新規および変更されたカテゴリのデフォルト設定の選択」（P.17-9） • 「カテゴリおよびポリシー変更に関するアラートを確実に受信する」（P.17-9）
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」（P.17-9） • 「URL カテゴリ セットの更新とレポート」（P.23-12） ここでは、URL カテゴリ セットの変更がレポートおよび Web 追跡のデータにどのように影響するかについて説明します。 • URL カテゴリ セット アップデートから生じるポリシー変更は、GUI ログに記録されます。詳細については、「ロギング」の章を参照してください。

URL カテゴリ セットの更新の影響について

URL カテゴリ セットの更新では、既存のアクセス ポリシー、復号化ポリシーおよび Cisco IronPort 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。

- 「ポリシー グループ メンバーシップの URL カテゴリ セット変更の影響」（P.17-5）
- 「ポリシーのアクションのフィルタリングでの URL カテゴリ セット更新の影響」（P.17-6）

ポリシー グループ メンバーシップの URL カテゴリ セット変更の影響

このセクションは、URL カテゴリに定義できるメンバーシップによるすべてのポリシー タイプおよび ID に適用されます。

ポリシー グループのメンバーシップが URL カテゴリに定義されている場合、カテゴリ セットへの変更は次の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が削除されたカテゴリの場合、ポリシーまたは ID はディセーブルになります。
- 任意のポリシーのメンバーシップが変化する URL カテゴリによって定義される場合、そしてこれにより ACL リストが変更される場合、Web プロキシが再起動します。プロキシの再起動の影響については、「コミット時の Web プロキシ再起動のチェック」（P.2-10）を参照してください。

ポリシーのアクションのフィルタリングでの URL カテゴリ セット更新の影響

URL カテゴリ セットの更新は、次のようにポリシーの動作を変更できます。

表 17-1　URL カテゴリ セットの更新の影響

変更	ポリシーおよび ID への影響
新しいカテゴリが追加される	各ポリシーでは、新しく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）] で指定されたアクションです。
カテゴリが削除される	削除されたカテゴリに関連付けられたアクションが削除されます。 ポリシーが削除されたカテゴリにのみ依存している場合、ポリシーはディセーブルになります。 ポリシーが削除されたカテゴリにのみ依存している ID に依存している場合、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る	既存のポリシーの動作に変更はありません。
カテゴリが分割される	1 つのカテゴリは、複数の新しいカテゴリになることがあります。 たとえば、1 つの「Arts and Entertainment」カテゴリが「Arts」と「Entertainment」の 2 つのカテゴリになることがあります。 新しいカテゴリの両方に、元のカテゴリに関連付けられたアクションが含まれます。

表 17-1　URL カテゴリ セットの更新の影響

変更	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る	ポリシーの元のすべてのカテゴリに同じアクションが割り当てられている場合、マージされたカテゴリに元のカテゴリと同じアクションが含まれます。元のすべてのカテゴリが「Use Global Setting」に設定されている場合、マージされたカテゴリも「Use Global Setting」に設定されます。 元のカテゴリにさまざまなアクションが割り当てられたポリシーがある場合は、マージされたカテゴリに割り当てられたアクションは、そのポリシーの [分類されてないURL（Uncategorized URLs）] 設定によって異なります。 • [分類されてないURL（Uncategorized URLs）] が [ブロック（Block）] に設定されている場合（またはグローバル設定が [ブロック（Block）] の場合は [グローバル設定を使用（Use Global Settings）]）、元のカテゴリで最も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）] 以外の他のアクションに設定されている場合（またはグローバル設定が [ブロック（Block）] 以外の他のアクションに設定されている場合は [グローバル設定を使用（Use Global Settings）]）、元のカテゴリで最も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可能性があります。 ポリシーのメンバーシップが URL カテゴリで定義され、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）] 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、グローバル ポリシーの値が不足している項目に使用されます。 制限性の順序は次のとおりになります（すべてのアクションはすべてのポリシー タイプで使用できません）。 • ブロック（Block） • ドロップ（Drop） • 復号（Decrypt） • 警告（Warn） • 時間ベース（Time-based） • モニタ（Monitor） • パススルー（Pass Through） 詳細については、「マージされたカテゴリ - 例」（P.17-7）を参照してください。 注：マージされたカテゴリに基づく時間ベースのポリシーは、元のカテゴリのいずれか 1 つと関連付けられたアクションを採用します。（時間ベース ポリシーでは、最も厳しい、または最も緩いアクションがない可能性があります）。

マージされたカテゴリ - 例

ポリシーの [URL フィルタ（URL Filtering）] ページの設定に基づいたマージされたカテゴリの例は、次のとおりです。

表 17-2　カテゴリがマージする場合の出力例

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（Block）	ブロック（Block）	（該当なし）	ブロック（Block）
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（Block）	モニタ（Monitor） そのため、元のカテゴリでは最も緩いアクションを使用します。	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） そのため、元のカテゴリでは最も厳しいアクションを使用します。	ブロック（Block）
ブロック（Block）	• 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） そのため、元のカテゴリでは最も緩いアクションを使用します。	モニタ（Monitor）
メンバーシップが URL カテゴリに定義されているポリシーの場合： モニタ（Monitor）	このカテゴリのアクションはこのポリシーに指定されませんが、このカテゴリのグローバル ポリシーの値はブロック（Block）です。	分類されてない URL（Uncategorized URLs）のアクションはこのポリシーに指定されませんが、分類されてない URL（Uncategorized URLs）のグローバル ポリシーの値はモニタ（Monitor）です。	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 セットの更新が自動的に行われます。ただし、これらの更新が既存のポリシー設定を変更する可能性があるため、URL カテゴリ セットの更新を含む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。

更新をディセーブルにすると、[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。「URL カテゴリ セットの手動の更新」（P.17-9）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」（P.26-43）を参照してください。

すべての自動更新をディセーブルにするには、「Web インターフェイスからのアップデートおよびアップグレード設定値の設定」（P.26-41）または「CLI からのアップデートおよびアップグレード設定値の設定」（P.26-42）を参照してください。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。

URL カテゴリ セットの手動の更新

（注）　処理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 カテゴリの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）] ページに移動します。

ステップ 2　更新を利用できるかどうかを判別します。

[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 IronPort Web Usage Controls - Web Categorization Categories List」項目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の選択

URL カテゴリ セットの更新は既存のポリシーの動作を変更することがあります。URL カテゴリ セットの更新時に対応できるようにポリシーを設定する場合に、特定の変更に対してデフォルト設定を指定する必要があります。

新しいカテゴリが追加される場合、または既存のカテゴリが新しいカテゴリにマージされる場合、各ポリシーのこれらのカテゴリのデフォルトのアクションは、そのポリシーの [分類されてない URL（Uncategorized URLs）] に影響されます。必要に応じて設定を選択するには、「ポリシーのアクションのフィルタリングでの URL カテゴリ セット更新の影響」（P.17-6）の新規およびマージされたカテゴリの情報を確認します。

既存の設定を確認したり、変更を行うには、各アクセス ポリシー、復号化ポリシー、および Cisco IronPort データ セキュリティ ポリシーの [URL フィルタ（URL Filtering）] リンクをクリックし、[分類されてない URL（Uncategorized URLs）] で選択した設定をオンにします。

カテゴリおよびポリシー変更に関するアラートを確実に受信する

カテゴリ セットの更新は 2 つのタイプのアラート（カテゴリ変更に関するアラート、およびカテゴリ セットの変更の結果として変更またはディセーブルにされたポリシーに関するアラート）をトリガーします。

URL カテゴリ セットの更新に関するアラートを受信することを確認するには、[システム管理（System Administration）] > [アラート（Alerts）] に進み、[システム（System）] カテゴリで警告レベルのアラートを受信するようにします。アラートについての詳細は、「アラートの管理」（P.26-18）を参照してください。

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する場合は、次を内容を実行する必要があります。

- カテゴリのマージ、追加、および削除の後でポリシーの目標を達成するように、ポリシーと ID を確認し、

- ポリシーと ID を変更して新しいカテゴリを活用すること、スプリット カテゴリの追加された詳細度を考慮します。

ポリシーと ID を確認するには、「URL カテゴリ セットの更新の影響について」（P.17-5）の情報を使用します。

URL カテゴリを使用した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 エンジンでは、アクセス、復号化、およびデータ 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 フィルタリングを設定するには、[URL カテゴリ（URL Categories）] カラムの下のポリシー テーブルで、編集するポリシー グループのリンクをクリックします。ポリシー テーブルの詳細については、「ポリシー テーブルの使用」（P.7-6）を参照してください。

ポリシー グループの URL カテゴリを設定する際には、定義されている場合も、カスタム URL カテゴリのアクションおよび定義済み URL カテゴリを設定できます。カスタム URL カテゴリの詳細については、「カスタム URL カテゴリの作成および編集」（P.17-16）を参照してください。

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。

- **アクセス ポリシー。**「アクセス ポリシー グループの URL フィルタの設定」（P.17-10）を参照してください。
- **復号化ポリシー。**「復号化ポリシー グループの URL フィルタの設定」（P.17-12）を参照してください。
- **Cisco IronPort 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」（P.17-14）を参照してください。

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）] ページの順に進みます。

ステップ 2　[URL フィルタ（URL Filtering）] カラムの下のポリシー テーブルで、編集するポリシー グループのリンクをクリックします。

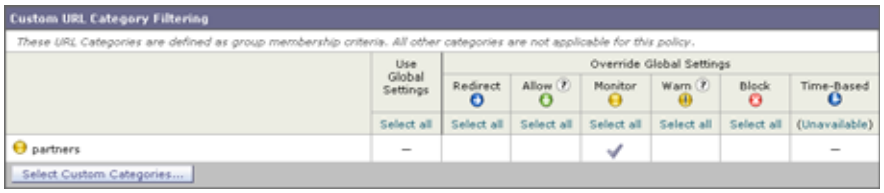
ステップ 3　オプションで、[カスタム URL カテゴリのフィルタリング（Custom URL Category Filtering）] セクションで、このポリシーに対してアクションを実行するカスタム URL カテゴリを追加できます。

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 エンジンがクライアント要求に対して照合するカスタム URL カテゴリを選択します。URL フィルタリング エンジンは、含まれるカスタム URL カテゴリに対してクライアント要求を比較し、除外されたカスタム URL カテゴリを無視します。URL フィルタリング エンジンは、定義済みの URL カテゴリの前に含まれるカスタム 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　[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、含まれる各カスタム URL カテゴリに対するアクションを選択します。表 17-3 で、各処理について説明します。

表 17-3　アクセス ポリシーの URL カテゴリ フィルタリング

アクション	説明
グローバル設定を使用（Use Global Settings）	グローバル ポリシー グループのこのカテゴリに対してアクションを使用します。これは、ユーザ定義のポリシー グループに対するデフォルト アクションです。 ユーザ定義のポリシー グループのみに適用されます。 **注：**カスタム URL カテゴリがグローバル アクセス ポリシーで除外された場合は、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（Redirect）	最初の宛先がこのカテゴリの URL であるトラフィックを、指定する場所にリダイレクトします。このアク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。 トラフィックのリダイレクトの詳細については、「トラフィックのリダイレクト」（P.17-20）を参照してください）。
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、これ以降のすべてのフィルタリングおよびマルウェア スキャンをバイパスします。 信頼できる Web サイトに対してだけ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場合があります。
モニタ（Monitor）	Web プロキシは、要求を許可またはブロックしません。代わりに、Web レピュテーション フィルタリングなどの他のポリシー グループ制御設定に対してクライアント要求を評価し続けます。
警告（Warn）	Web プロキシは最初に要求をブロックし、警告ページを表示しますが、警告ページのハイパーテキスト リンクをクリックして、ユーザの続行を許可します。 詳細については、「「ユーザの警告と続行の許可」（P.17-22）」を参照してください。
ブロック（Block）	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、指定した時間範囲内の要求をブロックまたはモニタします。 時間に基づいた URL フィルタリング アクションの作成の詳細については、「時間ベースの URL フィルタの作成」（P.17-23）を参照してください。

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、各カテゴリの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（Block）
- 時間ベース（Time-Based）

これらのアクションの詳細は、表 17-3 を参照してください。

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 URL カテゴリに分類されない Web サイトに対するクライアント要求に行うアクションを選択します。この設定は、URL 更新による新規およびマージされたカテゴリのデフォルト アクションも決定します。詳細については、「ポリシーのアクションのフィルタリングでの URL カテゴリ セット更新の影響」（P.17-6）を参照してください。

ステップ 7　変更を送信し、保存します。

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）] ページに移動します。

ステップ 2　[URL カテゴリ（URL Categories）] カラムの下のポリシー テーブルで、編集するポリシー グループのリンクをクリックします。

ステップ 3　オプションで、[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、このポリシーに対してアクションを実行するカスタム URL カテゴリを追加できます。

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 エンジンがクライアント要求に対して照合するカスタム URL カテゴリを選択します。URL フィルタリング エンジンは、含まれるカスタム URL カテゴリに対してクライアント要求を比較し、除外されたカスタム URL カテゴリを無視します。URL フィルタリング エンジンは、定義済みの URL カテゴリの前に含まれるカスタム 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　各カスタムおよび定義済み URL カテゴリのアクションを選択します。表 17-4 で、各処理について説明します。

表 17-4　復号化ポリシーの URL カテゴリ フィルタリング

アクション	説明
グローバル設定を使用（Use Global Settings）	グローバル復号化ポリシー グループでこのカテゴリに対してアクションを使用します。これは、ユーザ定義のポリシー グループに対するデフォルト アクションです。 ユーザ定義のポリシー グループのみに適用されます。 カスタム URL カテゴリがグローバル復号化ポリシーで除外された場合は、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。
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。有名な銀行や金融機関などの信頼できるセキュア サイトへの接続をパス スルーできます。
モニタ（Monitor）	Web プロキシは、要求を許可またはブロックしません。代わりに、Web レピュテーション フィルタリングなどの他のポリシー グループ制御設定に対してクライアント要求を評価し続けます。
復号（Decrypt）	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。gmail や hotmail などのサード パーティ電子メール プロバイダーへの接続を復号化できます。 アプライアンスが HTTPS トラフィックを復号化する方法の詳細については、「証明書」（P.11-3）を参照してください。
ドロップ（Drop）	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。ネットワーク上のユーザが組織の利用規定をバイパスすることを許可するサードパーティ プロキシへの接続をドロップする必要がある場合があります。

（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ように選択してから、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ように選択します。

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 URL カテゴリに分類されない Web サイトに対するクライアント要求に行うアクションを選択します。

この設定は、URL 更新による新規およびマージされたカテゴリのデフォルト アクションも決定します。詳細については、「ポリシーのアクションのフィルタリングでの URL カテゴリ セット更新の影響」（P.17-6）を参照してください。

表 17-4 に示されているすべてのリストを選択できます。

ステップ 6　変更を送信し、保存します。

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）] > [Cisco IronPort データ セキュリティ ポリシー（Cisco IronPort Data Security）] ページの順に進みます。

ステップ 2　[URL カテゴリ（URL Categories）] カラムの下のポリシー テーブルで、編集するポリシー グループのリンクをクリックします。

ステップ 3　オプションで、[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、このポリシーに対してアクションを実行するカスタム URL カテゴリを追加できます。

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 エンジンがクライアント要求に対して照合するカスタム URL カテゴリを選択します。URL フィルタリング エンジンは、含まれるカスタム URL カテゴリに対してクライアント要求を比較し、除外されたカスタム URL カテゴリを無視します。URL フィルタリング エンジンは、定義済みの URL カテゴリの前に含まれるカスタム 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　[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、各カスタム URL カテゴリのアクションを選択します。表 17-5 で、各処理について説明します。

表 17-5　Cisco IronPort データ セキュリティ ポリシーの URL カテゴリ フィルタリング

アクション	説明
グローバル設定を使用（Use Global Settings）	グローバル ポリシー グループのこのカテゴリに対してアクションを使用します。これは、ユーザ定義のポリシー グループに対するデフォルト アクションです。 ユーザ定義のポリシー グループのみに適用されます。 カスタム URL カテゴリがグローバル Cisco IronPort データ セキュリティ ポリシーで除外された場合は、ユーザ定義の Cisco IronPort 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 Cisco IronPort データ セキュリティ 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。
許可（Allow）	このカテゴリの Web サイトにアップロード要求を常に許可します。カスタム URL カテゴリに対してのみ適用されます。 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 サイトに対してだけ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場合があります。
モニタ（Monitor）	Web プロキシは、要求を許可またはブロックしません。代わりに、Web レピュテーション フィルタリングなどの他のポリシー グループ制御設定に対してアップロード要求を評価し続けます。
ブロック（Block）	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、各カテゴリの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（Block）

これらのアクションの詳細は、表 17-5 を参照してください。

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 URL カテゴリに分類されない Web サイトに対するアップロード要求に行うアクションを選択します。この設定は、URL 更新による新規およびマージされたカテゴリのデフォルト アクションも決定します。詳細については、「ポリシーのアクションのフィルタリングでの URL カテゴリ セット更新の影響」（P.17-6）を参照してください。

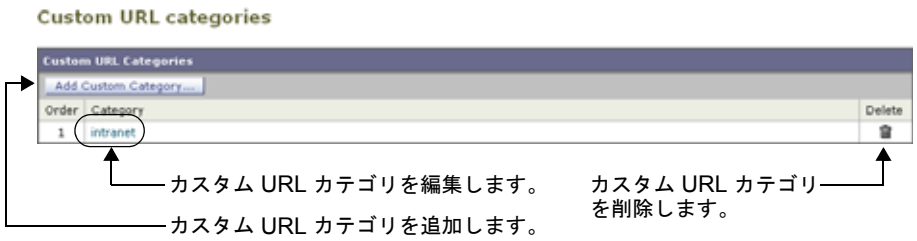
ステップ 7　変更を送信し、保存します。

カスタム URL カテゴリの作成および編集

Web セキュリティ アプライアンスには、デフォルトで多数の定義済み URL カテゴリ（Web-based Email など）が用意されています。ただし、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。内部サイトや確実に信頼できる外部サイトのグループには、カスタム URL カテゴリを作成することを推奨します。

[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）] ページで、カスタム URL カテゴリを作成、編集、および削除します。

図 17-1　　[カスタム URL カテゴリ（Custom URL Categories）] ページ



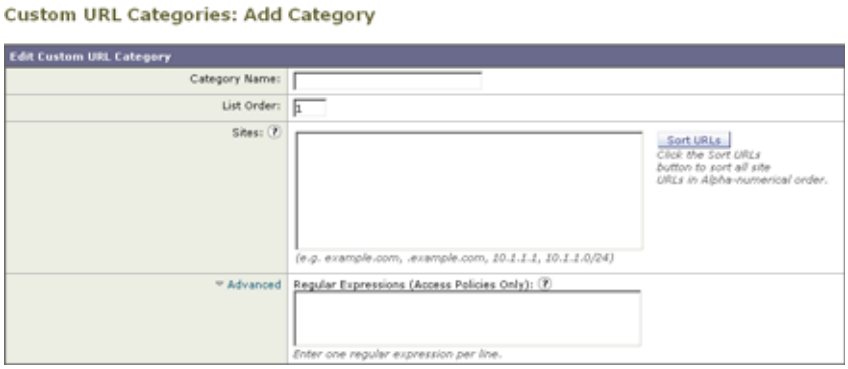
（注）　Web セキュリティ アプライアンスでは、先頭に「c_」が付加されたカスタム URL カテゴリ名の最初の 4 文字が、アクセス ログで使用されます。Sawmill for IronPort を使用してアクセス ログを解析する場合は、カスタム URL カテゴリの名前に注意してください。カスタム URL カテゴリの最初の 4 文字にスペースが含まれていると、Sawmill for IronPort はアクセス ログ エントリを正しく解析できません。Sawmill for IronPort を使用してアクセス ログを解析する場合は、この最初の 4 文字に、サポートされている文字のみを使用してください。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。この方法の詳細については、「アクセス ログおよび W3C ログのカスタム フォーマット」（P.24-31）を参照してください。

複数のカスタム URL カテゴリを作成し、各カテゴリに同じ URL を含めることができます。カスタム URL カテゴリの順序は重要です。リストの上位にあるカテゴリが、下位にあるカテゴリよりも優先されます。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 Cisco IronPort Data Security ポリシー グループに入れ、各カテゴリに異なるアクションを定義した場合は、より上位にあるカスタム URL カテゴリのアクションが有効となります。

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）] ページに移動します。

ステップ 2　カスタム URL カテゴリを作成するには、[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。

図 17-2　　カスタム URL カテゴリの作成



ステップ 3　カスタム URL カテゴリに対して表 17-6 に設定を入力します。

表 17-6　　カスタム URL カテゴリの設定

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）	このカテゴリに配置するカスタム URL カテゴリのリストの順序を選択します。最上位の URL カテゴリに対して「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 などのホスト名の一部を入力すると、www.example.com も一致します。
詳細：正規表現（Advanced: Regular Expressions）	入力するパターンと一致する複数の Web サーバを指定するための正規表現を入力できます。 **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）] フィールドの入力内容と一致した場合は、ここで入力した式との比較は行われません。 Web セキュリティ アプライアンスの正規表現の使用方法の詳細については、「正規表現」（P.17-24）を参照してください。

ステップ 4　任意で、[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）　アドレスをソートすると、元の順序を取得できません。

ステップ 5　変更を送信し、保存します。

アダルト コンテンツのフィルタリング

一部の Web 検索および 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。これは、安全でない可能性があるコンテンツがユーザに到達することを制限しながら、google.com や youtube.com などのサイトへのアクセスを許可する場合に必要になる場合があります。たとえば、学区が youtube.com の教育ビデオへのアクセスを許可し、生徒が不適切なコンテンツにアクセスするのをブロックする場合です。

Web 用 AsyncOS はアダルト コンテンツをフィルタリングするために、次の機能を提供します。

- **セーフ サーチの実施。**検索エンジンの多くは、Web 上の不適切なコンテンツを成人向けとして分類するフィルタリング技術機能をサポートしています。このフィルタリング機能がイネーブルの場合、ユーザに表示される前に、成人向けと分類されたコンテンツが検索結果からフィルタリングされます。この機能は、一般的にセーフ サーチと呼ばれています。ただし、ほとんどの検索エンジンでは、この機能はエンド ユーザによってイネーブルおよびディセーブルにされています。出力の検索要求がセーフ 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。エンド ユーザではなく、ネットワーク上の管理者への制御が提供されます。これは、検索エンジンを使用してユーザが利用規定をバイパスすることを防ぐために必要となる場合があります。
- **サイト コンテンツ レーティングの実施。**ユーザが生成した写真やビデオを提供する多くのコンテンツ共有サイトは、成人向けとして一部のコンテンツを分類します。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、または両方を実行して、これらのサイトのアダルト コンテンツへのユーザによるアクセスをブロックできます。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。

アクセス ポリシー レベルでこの機能をイネーブルにすることで、異なるユーザに対してセーフ サーチとサイト コンテンツ レーティングを実施します。すべての検索エンジンまたはコンテンツ共有 Web サイトはサポートされていませんが、Web 用 AsyncOS は URL フィルタリング エンジンの更新中に追加の検索エンジンおよび Web サイトをサポートできます。[アクセス ポリシー（Access Policies）] > [URL フィルタ（URL Filtering）] > [policyname] ページでは、各機能で現在サポートされている検索エンジンと Web サイトを常に示します。サポートされている検索エンジンおよびコンテンツ共有 Web サイトのリストは AVC エンジンの更新とともに増加する可能性があります。

セーフ サーチとサイト コンテンツ レーティングを実施する場合は、次のルールとガイドラインに留意してください。

- セーフ サーチとサイト コンテンツ レーティング機能を使用するには、Web 用 AsyncOS が Cisco IronPort Web 使用コントロール に含まれている URL フィルタリング エンジンを使用する必要があります。
- セーフ サーチ機能は、厳密なセーフ サーチを実施する。
- セーフ サーチとサイト コンテンツ レーティングを実施するために、URL および Web クッキーまたはいずれかを書き換え、セーフ モードをオンにして、AVC エンジンが特定の Web サイトで実行されるセーフ モード機能を利用します。そのため、ユーザ エクスペリエンスがサイトの機能によって決まります。ただし、craigslist.org など Web サイトがセーフ モード機能を提供しない場合は、AVC エンジンは Web サイトの既知の有害なセクションを識別し、必要に応じてサイトをブロックまたは警告します。

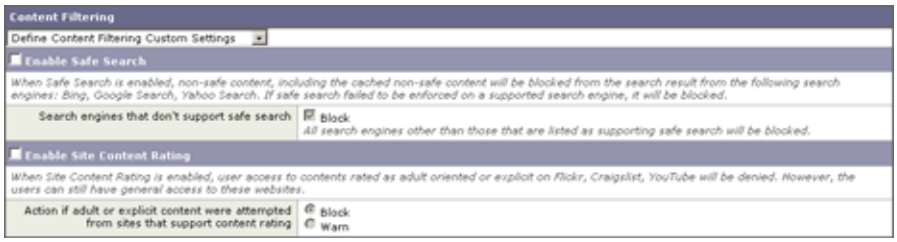
- サポートされている検索エンジンの 1 つの URL またはサポートされているコンテンツ レーティング Web サイトが [許可（Allow）] アクションが適用されているカスタム URL カテゴリに含まれている場合、セーフ サーチまたはコンテンツ レーティング機能がディセーブルの場合に、ユーザはその URL にアクセスできます。つまり、検索結果がブロックされず、すべてのコンテンツが表示されます。
- Web セキュリティ アプライアンス セーフ サーチ機能で現在サポートされていない検索エンジンからユーザをブロックするかどうかを選択できます。
- youtube.com に固有の制限により、Web プロキシはサードパーティ Web サイトから YouTube の組み込みビデオをブロックできません。
- サイト コンテンツ レーティング機能を設定する場合、アダルト コンテンツからユーザをブロックするか、またはユーザがリンクをクリックして警告メッセージを許可した後にアダルト コンテンツの表示を許可するエンド ユーザの URL フィルタリング警告ページを提供するかどうかを選択できます。詳細については、「「ユーザの警告と続行の許可」（P.17-22）」を参照してください。
- 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イネーブルにされているアクセス ポリシーは、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 レーティングの実施。

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）] ページの順に進みます。

ステップ 2　[URL カテゴリ（URL Categories）] カラムで、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 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できます。

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 サイトからすべてのアダルト コンテンツをブロックするか、またはエンドユーザ URL フィルタギング警告ページを表示するかどうかを選択します。

ステップ 8　変更を送信し、保存します。

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 ログは各エントリの山カッコ内に安全なブラウジング スキャンの判定を含みます。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 ログまたは 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

表 17-7 は、安全なブラウジング スキャンの判定値について説明します。

表 17-7　安全なブラウジング スキャンの判定値

値	説明
ensrch	最初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	最初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	最初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に適用されていました。
err	最初のクライアント要求が安全でなく、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エラーによって適用されませんでした。
-	機能がバイパスされたか（たとえば、トランジションがカスタム URL カテゴリで許可された）、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 サーチまたはサイト コンテンツ レーティング機能がクライアント要求に適用されていません。

ロギングの詳細については、「ログ ファイルへのアクセス」（P.24-17）を参照してください。

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りブロックされた要求には、アクセス ログの次のいずれか ACL 決定タグを使用します。

- BLOCK_SEARCH_UNSAFE
- BLOCK_CONTENT_UNSAFE
- BLOCK_UNSUPPORTED_SEARCH_APP
- BLOCK_CONTINUE_CONTENT_UNSAFE

ACL 決定タグの詳細については、「ACL デシジョン タグ」（P.24-20）を参照してください。

トラフィックのリダイレクト

Web セキュリティ アプライアンスを使用して特定の Web サイトへのトラフィックをモニタおよびブロックするとともに、ユーザを異なる Web サイトにリダイレクトするために使用することもできます。最初の宛先がカスタム URL カテゴリの URL であるトラフィックを指定する場所にリダイレクトするように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、アプライアンス上のトラフィックをリダイレクトできます。

組織が内部サイトへのリンクを公開したが、サイトの場所が公開以降に変更された場合や、Web サーバを制御する権限がない場合は、アプライアンスでトラフィックをリダイレクトします。

アクセス ポリシー グループの URL カテゴリを設定するときに、カスタム URL カテゴリを別の場所にリダイレクトするようにアプライアンスを設定します。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。

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。カスタム URL カテゴリの作成の詳細については、「カスタム URL カテゴリの作成および編集」（P.17-16）を参照してください。

（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、無限ループに注意してください。たとえば、http://A.example.com 宛てのトラフィックを http://B.example.com にリダイレクトし、http://B.example.com 宛てのトラフィックを http://A.example.com に不注意にリダイレクトしてしまった場合、無限ループが作成されます。この場合、アプライアンスは 2 つの URL 間でトラフィックの無制限にリダイレクトします。

ロギングとレポーティング

トラフィックをリダイレクトする場合、最初に要求された Web サイトのアクセス ログ エントリには REDIRECT_CUSTOMCAT で始まる ACL タグがあります。アクセス ログ（通常は次の行）の後半に、ユーザがリダイレクトされた 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は、「Allowed」としてリダイレクトされたトランザクションを表示します。

アクセス ポリシーのトラフィックのリダイレクト

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）] ページの順に進みます。

ステップ 2　[URL カテゴリ（URL Categories）] カラムで、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。

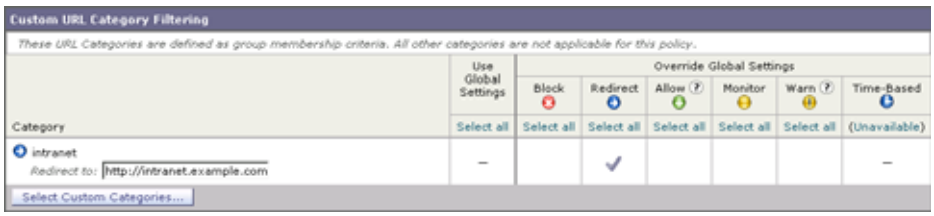
ステップ 3　[カスタム URL カテゴリのフィルタリング（Custom URL Category Filtering）] セクションで、[カスタム カテゴリの選択（Select Custom Categories）] をクリックします。

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 カテゴリの「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）] カラムをクリックします。

ステップ 7　カスタム カテゴリの [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する URL を入力します。



ステップ 8　変更を送信し、保存します。

ユーザの警告と続行の許可

Web セキュリティ アプライアンスを使用して特定の Web サイトへのトラフィックをブロックするとともに、組織の利用規定にサイトが適合せず、選択した場合は続行を許可することをユーザに警告するために使用することもできます。ユーザが特定のサイトにアクセスできないようにすることを組織が望みながら、これらのサイトへのアクセスを法律でブロックできない場合などは、ユーザに警告し、続行することを許可する必要がある場合があります。

次のいずれかの方法を使用して、ユーザを警告し、続行を許可できます。

- 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。
- サイト コンテンツ レーティング機能をイネーブルにし、ブロックせずにアダルト コンテンツにアクセスするユーザを警告します。サイト コンテンツ レーティング機能の詳細については、「アダルト コンテンツのフィルタリング」（P.17-18）を参照してください。

警告および続行するように設定された URL にユーザがアクセスすると、このカテゴリまたはコンテンツのサイトへのアクセスについての警告に関する IronPort 通知ページが最初に表示されます。エンド ユーザ URL フィルタリング警告ページには、次の要素が含まれます。

- シスコによって提供されるデフォルトの警告テキスト
- Web セキュリティ アプライアンス管理者によって提供されるシスコのカスタム テキスト（任意）
- 呼び出されたアクセス ポリシーおよび警告されている URL カテゴリまたは安全なブラウジング スキャンの判定を記載する通知コード
- 最初に要求された URL へのハイパーテキスト リンク

認証によってユーザ名が利用可能な場合は、ユーザ名でアクセス ログ内のユーザが追跡され、ユーザ名が使用できない場合は、IP アドレスで追跡されます。

警告および続行機能を使用する場合、エンド ユーザの URL フィルタリング警告に影響する次の設定を設定できます。

- **[警告の時間間隔（Time Between Warning）]。**[警告の時間間隔（Time Between Warning）] は、Web プロキシがユーザ 1 人あたりの各 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させる頻度を決めます。ユーザがエンドユーザ URL フィルタリング警告ページで続行リンクをクリックすると、Web プロキシは [警告の時間間隔（Time Between Warning）] で入力する時間の警告を認識したと見なします。この設定は、ユーザ名で追跡されるユーザ、および IP アドレスで追跡されるユーザに適用されます。30 ～ 2678400 秒（1 か月）の任意の値を指定できます。デフォルトは 1 時間（3600 秒）です。
- **カスタム メッセージ。**カスタム メッセージは、エンド ユーザ URL フィルタリング警告ページごとに表示されるユーザが入力するテキストです。組織の利用規定に対してテキストを含めたり、利用規定を詳しく説明するページへのリンクを含めたりする必要がある場合があります。一部の単純な HTML タグを組み込んでテキストを書式設定できます。たとえば、テキストの色とサイズを変更したり、イタリック体で表示させることができます。詳細については、「「通知ページのカスタム テキスト」（P.16-18）」を参照してください。

[セキュリティ サービス（Security Services）] > [ユーザ通知（End-User Notification）] ページで、これらの設定を設定します。詳細については、「「エンド ユーザ URL フィルタリング警告ページの設定」（P.16-16）」を参照してください。

（注）　警告および続行機能は、HTTP および復号化された HTTPS トランザクションでのみ作用します。これはネイティブ FTP トランザクションでは作用しません。

ユーザを警告するときのユーザ エクスペリエンス

URL フィルタリング エンジンが特定の要求をユーザに警告するときに、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。たたし、すべての Web サイトがエンド ユーザに対して警告ページを表示しません。たとえば、一部の Web 2.0 Web サイトは、静的な Web ページの代わりに JavaScript を使用して動的なコンテンツを表示し、Web プロキシから警告ページを表示することはありません。この場合、ユーザはサイトへのアクセスを続行するチャンスは与えられず、[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。

時間ベースの URL フィルタの作成

Web セキュリティ アプライアンスが日時別に特定のカテゴリの URL の要求をどのように処理するかを設定できます。たとえば、ブログまたはフォーラムなどソーシャル ネットワーク サイトへの業務時間内のアクセスをブロックできます。

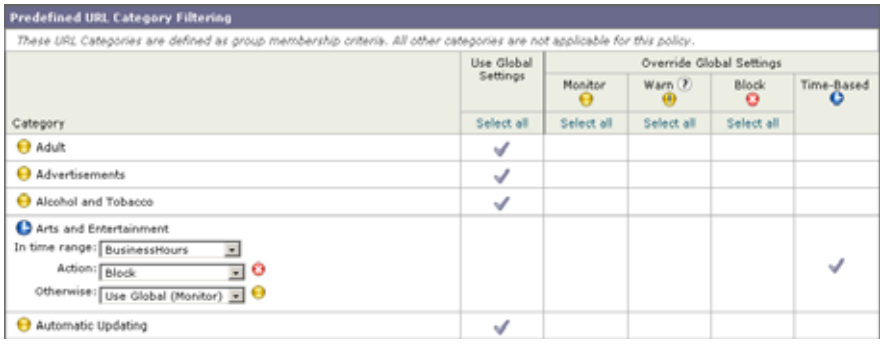
時間別に URL フィルタリング アクションを定義するには、最初に少なくとも 1 つの時間範囲を定義する必要があります。時間範囲の詳細については、「時間ベースのポリシーの使用」（P.7-9）を参照してください。

ステップ 1　[Web セキュリティ マネージャ（Web Security Manager）] > [アクセス ポリシー（Access Policies）] ページの順に進みます。

ステップ 2　[URL カテゴリ（URL Categories）] カラムの下のポリシー テーブルで、編集するポリシー グループのリンクをクリックします。

ステップ 3　時間範囲に基づいて設定するカスタムまたは定義済みの URL カテゴリの時間ベースを選択します。

図 17-3　時間ベースの URL フィルタリング アクションの定義



[URL カテゴリの時間ベース（Time-Based for the URL category）] を選択すると、アクションを選択できるカテゴリ名の下に追加のフィールドが表示されます。

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。

時間範囲の定義の詳細については、「時間範囲の作成」（P.7-10）を参照してください。

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にこの URL カテゴリのトランザクションを実行させるアクションを選択します。

ステップ 6　[でなければ（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を実行させ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。

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）] ページは、一致した上位の URL カテゴリとブロックした上位の URL カテゴリに関する情報を含む URL 統計情報の総合的な表示を提供します。また、このページは帯域幅の軽減と Web トランザクションのカテゴリ固有のデータを表示します。モニタリングおよびレポート機能の詳細については、「レポート」（P.22-1）を参照してください。

フィルタリングおよび未分類のデータの概要

[レポート（Reporting）] > [URL カテゴリ（URL Categories）] ページで URL 統計情報を表示するには、次のデータを解釈する方法を理解することが重要です。

- **バイパスされた URL フィルタリング**：このデータは、URL フィルタリングの前に発生するポリシー、ポート、および admin ユーザ エージェントのブロックを表します。
- **未分類の URL**：このデータは、URL フィルタリング エンジンが照会されるが、カテゴリが一致しないすべてのトランザクションを表します。

アクセス ログ ファイル

アクセス ログ ファイルは、各エントリのスキャンの判定情報セクションの各トランザクションに対して URL カテゴリを記録します。アクセス ログの詳細については、「ログ ファイルへのアクセス」（P.24-17）を参照してください。各 URL カテゴリのリストについては、「URL カテゴリについて」（P.17-26）を参照してください。

正規表現

正規表現は、テキスト文字列のパターンに照合させるために使用される通常の印刷可能文字および特殊文字を含むパターン マッチングの記述です。たとえば、「welcome」などのテキスト文字列は「welcome」または「welcomemyfriend」に一致します。一致が発生すると、機能が true を返します。一致しなかった場合は、false を返します。アクションは、パターン マッチング表現が true の場合にだけ実行されます。

Web セキュリティ アプライアンスは POSIX 拡張正規表現構文を使用します（IEEE POSIX 1003.2 で詳しく説明されています）。ただし、フォワード スラッシュからエスケープするためのアプライアンスのバックワード スラッシュはサポートしていません。正規表現でフォワード スラッシュを使用する必要がある場合は、バックワード スラッシュなしでフォワード スラッシュを入力します。

（注）　技術的には、Web 用 AsyncOS は Flex 正規表現アナライザを使用します。正規表現を読み取る方法の詳細については、http://flex.sourceforge.net/manual/Patterns.html を参照してください。

次の場所で正規表現を使用できます。

- **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ときに、正規表現を使用して、入力するパターンに一致する複数の Web サーバを指定できます。カスタム URL カテゴリの作成の詳細については、「カスタム URL カテゴリの作成および編集」（P.17-16）を参照してください。
- **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と、正規表現を使用して Skype または Microsoft Internet Explorer などの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。ユーザ エージェントをブロックする正規表現の使用に関する詳細については、「ポリシー：プロトコルおよびユーザ エージェント」（P.9-14）を参照してください。

（注）　広範な文字の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。そのため、正規表現は慎重に適用する必要があります。

正規表現の形成

正規表現は、一般的に表現に「一致」する単語を使用するルールです。特定の URL の宛先または Web サーバの照合に適用できます。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みます。

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

この例では、サーバ [0-9] は、ドメイン example.com の server0、server1、server2、...、server9 に一致します。

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

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

冗長な正規表現の文字列は Web セキュリティ アプライアンスで CPU 使用率が高くなる原因になるため、使用しないようにしてください。冗長な正規表現は、「.*」で開始または終了します。

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

正規表現の文字テーブル

表 17-8 は、正規表現を形成するために一般的に使用される文字について説明します。

表 17-8　正規表現の文字の説明

文字	説明
.	任意の単一文字と一致します。
*	直前の正規表現の 0 回または複数回の発生に一致します。 次に例を示します。 [0-9]* は任意の数字に一致します。 「.*」は、文字の任意の文字列に一致します。
^	正規表現の先頭文字として行の先頭に一致します。

表 17-8　正規表現の文字の説明 （続き）

文字	説明
$	正規表現の末尾の文字として行の末尾に一致します。
+	直前の正規表現の 1 回または複数回の発生に一致します。
?	直前の正規表現の 0 回または 1 回の発生に一致します。
|	直前の正規表現または次の正規表現に一致します。次に例を示します。 x|y が x または y に一致します。 abc|xyz は abc または xyz の文字列に一致します。
[ ]	カッコで囲まれた文字または数字に一致します。 次に例を示します。 [a-z] は a と z 間の文字に一致します。 [r-u] は文字 r、s、t、または u に一致します。 [0-3] は 0、1、2、3 の 1 桁の数字に一致します。
{ }	以前のパターンに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 の 1 ～ 3 の発生に一致します。
( )	正規表現のグループ文字。 次に例を示します。 (abc) * は abc または abcabcabc に一致します。
“...”	引用符で囲まれた文字を文字どおり解釈します。
\	エスケープ文字。

（注）　特殊文字のリテラル バージョンを照合するために、文字の前にバックスラッシュ「\」を付ける必要があります。たとえば、ピリオド「.」に正確に一致させるには、正規表現は「\.example\.com」のように「\」を使用する必要があります。ただし、フォワード スラッシュからエスケープするためのアプライアンスのバックワード スラッシュはサポートしていません。正規表現でフォワード スラッシュを使用する必要がある場合は、バックワード スラッシュなしでフォワード スラッシュを入力します。

URL カテゴリについて

ここでは、Cisco IronPort Web 使用コントロール の URL カテゴリを示します。テーブルには、アクセス ログ ファイル エントリの Web レピュテーション フィルタリングおよびアンチマルウェア スキャン セクションに表示される可能性がある省略された URL カテゴリ名も含まれます。

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 と誤って分類された URL の報告」（P.17-3）の URL に移動します。

（注）　アクセス ログでは、Cisco IronPort Web 使用コントロール の URL カテゴリの省略形には、各省略形の前にプレフィックス「IW_」が含まれ、「art」カテゴリが「IW_art」になります。

表 17-9 は、リリース時点での Cisco IronPort Web 使用コントロール の URL カテゴリについて説明します。このリストへのリビジョンの場所を含む URL カテゴリ セットの更新については、「URL カテゴリのセットに対する更新の管理」（P.17-5）を参照してください。

表 17-9　Cisco IronPort Web 使用コントロール　の URL カテゴリの説明について

URL カテゴリ	省略形	コード	説明	URL の例
Adult	adlt	1006	成人向けですが、ポルノとは限りません。成人向けクラブ（ストリップ クラブ、スインガー クラブ、エスコート サービス、ストリッパー）、セックスに関する一般的な情報、非ポルノ性サイト、性器ピアス、成人向け商品またはグリーティング カード、健康や病気の文脈に含まれないセックスに関する情報。	www.adultentertainmentexpo.com www.adultnetline.com
Advertisements	adv	1027	Web ページに付随して表示されることの多いバナー広告やポップアップ広告、広告コンテンツを提供するその他の広告に関連する Web サイト。広告に関連するサービスと販売は「Business and Industry」に分類されます。	www.adforce.com www.doubleclick.com
Alcohol	alc	1077	楽しみとしてのアルコール、ビールやワインの製造、カクテルのレシピ、酒類販売者、ワイナリ、ブドウ園、ビール醸造所、アルコール販売業者。アルコール依存は「Health and Nutrition」に分類されます。バーとレストランは「Dining and Drinking」に分類されます。	www.samueladams.com www.whisky.com
Arts	art	1002	ギャラリーと展示会、芸術家と芸術、写真、文学と書籍、芸能と劇場、ミュージカル、バレエ、博物館、設計、建築。映画とテレビは「Entertainment」に分類されます。	www.moma.org www.nga.gov
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
Auctions	auct	1088	オンライン オークションおよびオフライン オークション、競売場、案内広告。	www.craigslist.com www.ebay.com
Business and Industry	busi	1019	マーケティング、商業、企業、ビジネス手法、労働力、人材、運輸、給与、セキュリティとベンチャー キャピタル、オフィス用品、産業機器（プロセス用機器）、機械と機械系、加熱装置、冷却装置、資材運搬機器、包装装置、製造、立体処理、金属製作、建築と建築物、旅客輸送、商業、工業デザイン、建築、建築資材、出荷と貨物（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、優先サービス、荷高と貨物のマッチング、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、移動と保管）。	www.freightcenter.com www.staples.com

表 17-9　Cisco IronPort Web 使用コントロール （続き）の URL カテゴリの説明について

URL カテゴリ	省略形	コード	説明	URL の例
Chat and Instant Messaging	chat	1040	Web ベースのインスタント メッセージングおよびチャット ルーム。	www.icq.com www.meebo.com
Cheating and Plagiarism	plag	1051	不正行為を助長し、学期末論文（盗用したもの）などの書物を販売したりします。	www.bestessays.com www.superiorpapers.com
Child Abuse Content	cprn	1064	世界的な規模の不法な児童性的虐待コンテンツ。	—
Computer Security	csec	1065	企業ならびにホーム ユーザ向けにセキュリティ商品とサービスを提供します。	www.computersecurity.com www.symantec.com
Computers and Internet	comp	1003	ハードウェア、ソフトウェア、ソフトウェア サポートなどのコンピュータとソフトウェアに関する情報、ソフトウェア エンジニア向けの情報、プログラミングとネットワーキング、Web サイトの設計、一般的な Web およびインターネット、コンピュータ サイエンス、コンピュータ グラフィックスおよびクリップアート。「Freeware and Shareware」は別のカテゴリになっています。	www.xml.com www.w3.org
Dating	date	1055	デート、出会い系サイト、結婚紹介所。	www.eharmony.com www.match.com
Digital Postcards	card	1082	デジタル ポストカードと E カードの送信が可能です。	www.all-yours.net www.delivr.net
Dining and Drinking	food	1061	飲食施設、レストラン、バー、酒場、パブ、レストランのガイドとレビュー。	www.hideawaybrewpub.com www.restaurantrow.com
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行す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
Education	edu	1001	学校、カレッジ、大学、教材、教員の人材などの教育関連、技術訓練および職業訓練、オンライン研修、教育に関する問題とポリシー、金融支援、学校助成金、基準と試験。	www.education.com www.greatschools.org
Entertainment	ent	1093	映画の詳細やディスカッション、音楽やバンド、テレビ、セレブやファンの Web サイト、娯楽関係のニュース、セレブのゴシップ、娯楽スポット。「Arts」カテゴリと比較してください。	www.eonline.com www.ew.com
Extreme	extr	1075	性暴力または犯罪的な性質のサイト、暴力および暴力的行為、悪趣味なサイト（死体画像などのむごたらしい写真が載っていることが多い）、犯罪現場の写真、犯罪や事故の犠牲者、過剰にわいせつな情報、衝撃的な Web サイト。	www.car-accidents.com www.crime-scene-photos.com
Fashion	fash	1076	衣類とファッション、美容室、化粧品、アクセサリ、宝石、香水、身体の改造に関する写真や文、タトゥーとピアス、モデル事務所。皮膚に関する商品は「Health and Nutrition」に分類されます。	www.fashion.net www.findabeautysalon.com

表 17-9　Cisco IronPort Web 使用コントロール （続き）の URL カテゴリの説明について

URL カテゴリ	省略形	コード	説明	URL の例
File Transfer Services	fts	1071	主要な目的が、ダウンロード サービスの提供とホスティング ファイルの共有のファイル転送サービス。	www.rapidshare.com www.yousendit.com
Filter Avoidance	filt	1025	匿名の cgi、php、glype プロキシ サービスを含む、検出できない、または匿名 Web の使用を拡大および助長します。	www.bypassschoolfilter.com www.filterbypass.com
Finance	fnnc	1015	会計実務、会計、課税、税金、銀行、保険、投資、国家経済、すべての保険の種類、クレジット カード、退職後のプランと相続プラン、ローン、抵当権を含む個人金融などの金融が主体のサイト。株式は「Online Trading」に分類されます。	finance.yahoo.com www.bankofamerica.com
Freeware and Shareware	free	1068	フリー ソフトウェアおよびシェアウェア ソフトウェアのダウンロードを提供します。	www.freewarehome.com www.shareware.com
Gambling	gamb	1049	カジノとオンライン ギャンブル、ギャンブルの胴元と賭け率、ギャンブルに関する助言、ギャンブル コンテキストでの競争の厳しいレース、スポーツ ギャンブル、株式に幅広く賭けるサービス。ギャンブル依存を扱う Web サイトは「Health and Nutrition」に分類されます。政府運営の宝くじは「Lotteries」に分類されます。	www.888.com www.gambling.com
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、コンバット ゲーム、スポーツ ゲーム、ダウンロード可能なゲーム、ゲームのレビュー、ゲーム攻略サイト、ロールプレイング ゲームなどのコンピュータ ゲームとインターネット ゲーム。	www.games.com www.shockwave.com
Government and Law	gov	1011	政府 Web サイト、国際関係、政府と選挙に関係するニュースと情報、弁護士、法律事務所、法律関係の出版物、法関連の資料、裁判所、訴訟事件表、弁護士会、法律および裁判所による決定などの法律の分野に関係する情報、公民権に関する問題、入国管理、特許と著作権、法執行と矯正行政、犯罪報告、法執行、犯罪統計、武力、軍事基地、軍組織、反テロリズムなどの軍隊。	www.usa.gov www.law.com
Hacking	hack	1050	Web サイト、ソフトウェア、コンピュータのセキュリティを迂回する方法について記載しているサイト。	www.hackthissite.org www.gohacking.com
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、性同一性を基に、憎悪、不寛容、差別を助長する Web サイト。人種差別を扇動するサイト、性差別、人種差別の神学、人種差別の音楽、ネオナチ組織、特定民族至上主義、ホロコースト否定論。	www.kkk.com www.nazi.org

表 17-9　Cisco IronPort Web 使用コントロール （続き）の URL カテゴリの説明について

URL カテゴリ	省略形	コード	説明	URL の例
Health and Nutrition	hlth	1009	ヘルス ケア、病気と障がい、医療、病院、医師、医薬品、メンタル ヘルス、精神医学、薬理学、エクササイズとフィットネス、身体障がい、ビタミンとサプリメント、健康のコンテキスト内でのセックス（病気とヘルス ケア）、たばこの摂取、アルコールの摂取、薬の摂取、健康のコンテキスト内でのギャンブル（病気とヘルス ケア）、一般的な食物、食物と飲料、料理とレシピ、食糧と栄養、健康、ダイエット、レシピと料理の Web サイトを含む料理、代替医療。	www.health.com www.webmd.com
Humor	lol	1079	ジョーク、スケッチ、コミック、その他のユーモラスなコンテンツ。気分を害する可能性のある成人向けユーモアは「Adult」に分類されます。	www.humor.com www.jokes.com
Illegal Activities	ilac	1022	窃盗、不正行為、電話ネットワークへの不法アクセスなどの犯罪を助長するサイト、コンピュータ ウィルス、テロリズム、爆弾、無秩序、殺人や自殺を描写したものやその実行方法を記述した Web サイト。	www.ekran.no www.thedisease.net
Illegal Downloads	ildl	1084	ソフトウェアまたは他の情報、シリアル番号、キージェネレータ、および著作権侵害でソフトウェアの保護を迂回するツールをダウンロードできる機能を提供するサイト。動画共有は「Peer File Transfer」に分類されます。	www.keygenguru.com www.zcrack.com
Illegal Drugs	drug	1047	気晴らしのためのドラッグ、ドラッグ摂取の道具、ドラッグの購入と製造に関する情報。	www.cocaine.org www.hightimes.com
Infrastructure and Content Delivery Networks	infr	1018	コンテンツ配信インフラストラクチャおよびダイナミックに生成されるコンテンツ、セキュリティ保護されているため、これ以上分類できないか、保護されていないため分類が困難である Web サイト。	www.akamai.net www.webstat.net
Internet Telephony	voip	1067	インターネットを使用した電話サービス。	www.evaphone.com www.skype.com
Job Search	job	1004	キャリアに関する助言、レジュメの書き方とインタビューのスキル、職業紹介サービス、職業データバンク、終身雇用職業紹介所、人材派遣会社、企業の Web サイト。	www.careerbuilder.com www.monster.com
Lingerie and Swimsuits	ling	1031	肌着と水着、特にモデルが登場するもの。	www.swimsuits.com www.victoriassecret.com
Lotteries	lotr	1034	宝くじ、コンテストおよび国が運営する宝くじ。	www.calottery.com www.flalottery.com
Mobile Phones	cell	1070	ショート メッセージ サービス（SMS）、着信音と携帯電話のダウンロード。携帯電話会社の Web サイトは「Business and Industry」カテゴリに含まれます。	www.cbfsms.com www.zedge.net

表 17-9　Cisco IronPort Web 使用コントロール （続き）の URL カテゴリの説明について

URL カテゴリ	省略形	コード	説明	URL の例
Nature	natr	1013	天然資源、生態学および保護、森林、荒地、植物、花、森林保護、森林、荒地、林業活動、森林管理（植林、森林保護、保護、収穫、森林状態、間伐、山焼き）、農業活動（農業、ガーデニング、園芸、造園、作付け、雑草防除、用水、剪定、収穫）、公害に関する問題（大気質、有害廃棄物、公害防止、リサイクル、廃棄物管理、水質、環境浄化産業）、動物、ペット、家畜、動物学、生物学、植物学。	www.enature.com www.nature.org
News	news	1058	ニュース、ヘッドライン、新聞、テレビ局、雑誌、天気、スキー場の状態。	www.cnn.com news.bbc.co.uk
Non-Governmental Organizations	ngo	1087	クラブ、圧力団体、コミュニティ、非営利組織および労働組合などの非政府組織。	www.panda.org www.unions.org
Non-sexual Nudity	nsn	1060	ヌーディズムおよび裸体、裸体主義、ヌーディストキャンプ、芸術的裸体。	www.artenuda.com www.naturistsociety.com
Online Communities	comm	1024	アフィニティ グループ、特殊な関心のグループ、Web ニュースグループ、メッセージ ボード。「Professional Networking」または「Social Networking」として分類された Web サイトは除外します。	www.igda.org www.ieee.org
Online Storage and Backup	osb	1066	バックアップ、共有、ホスティング用オフサイトおよびピアツーピア ストレージ。	www.adrive.com www.dropbox.com
Online Trading	trad	1028	オンライン仲買、ユーザが株式をオンラインでトレードできる Web サイト、株式市場に関係する情報、株式、担保、投資信託、ブローカ、株価分析および解説、株式審査、株式チャート、IPO、株式分割。株式に幅広く賭けるサービスは「ギャンブル」に分類されます。他の金融サービスは「金融」に分類されます。	www.tdameritrade.com www.scottrade.com
Organizational Email	pem	1085	業務上の電子メール アクセスに使用する Web サイト（多くは Outlook Web アクセス）。	—
Parked Domains	park	1092	広告ネットワークから有料のリストを使用して、ドメインからのトラフィックを金銭化したり、利益を求めてドメイン名の販売を希望する「不法占拠者」が所有する Web サイト。これらは有料の広告リンクを返す、偽の検索 Web サイトも含みます。	www.domainzaar.com www.parked.com
Peer File Transfer	p2p	1056	ピアツーピア ファイル要求の 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
Personal Sites	pers	1081	私的な個人の Web サイト、個人的なホームページ サーバ、個人的なコンテンツを持つ Web サイト、特定のテーマを持たない個人ブログ。	www.karymullis.com www.stallman.org
Photo Searches and Images	img	1090	イメージ、画像、およびクリップ アートの保管と検索を促進します。	www.flickr.com www.photobucket.com

表 17-9　Cisco IronPort Web 使用コントロール （続き）の URL カテゴリの説明について

URL カテゴリ	省略形	コード	説明	URL の例
Politics	pol	1083	政治家の Web サイト、政党、政治、選挙、民主主義、投票に関するニュースと情報。	www.politics.com www.thisnation.com
Pornography	porn	1054	明白に性的な文章または描写。明示的なアニメーションや漫画、一般的に明白な描写、他のフェティッシュ情報、明示的なチャット ルーム、セックス シミュレータ、ストリップ ポーカー、成人向け映画、わいせつなアート、明白な Web ベースの E メールなどがあります。	www.redtube.com www.youporn.com
Professional Networking	pnet	1089	キャリアまたは専門的な開発を目的とするソーシャル 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
Real Estate	rest	1045	不動産の検索をサポートする情報、オフィスと商業スペース、不動産一覧、賃貸、アパート、住宅、住宅建設などの不動産一覧。	www.realtor.com www.zillow.com
Reference	ref	1017	市と州のガイド、地図、時刻、参照先、辞書、ライブラリ。	www.wikipedia.org www.yellowpages.com
Religion	rel	1086	宗教に関するコンテンツ、宗教に関する情報、宗教上のコミュニティ	www.religionfacts.com www.religioustolerance.org
SaaS and B2B	saas	1080	オンライン ビジネス サービス向け Web ポータル、オンライン ミーティング。	www.netsuite.com www.salesforce.com
Safe for Kids	kids	1057	幼児を対象に、特に承認されたサイト。	kids.discovery.com www.nickjr.com
Science and Technology	sci	1012	航空宇宙科学、電子工学、工学、数学、その他の類似の主題、宇宙開発、気象学、地理学、環境、エネルギー（化石、原子力、再生可能）、通信（電話、遠距離通信）。	www.physorg.com www.science.gov
Search Engines and Portals	srch	1020	インターネット上の情報への検索エンジンと他の初期アクセス ポイント。	www.bing.com www.google.com
Sex Education	sxed	1052	セックス、性の健康、避妊、妊娠を扱う、事実に基づく Web サイト。	www.avert.org www.scarleteen.com
Shopping	shop	1005	物々交換、オンラインでの購入、クーポンとフリーオファー、一般的なオフィス消耗品、オンライン カテゴリ、オンライン モール。	www.amazon.com www.shopping.com
Social Networking	snet	1069	ソーシャル 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
Social Science	socs	1014	社会に関係する科学と歴史、考古学、人類学、文化考、歴史学、言語学、地理学、哲学、心理学、女性学。	www.archaeology.org www.anthropology.net
Society and Culture	scty	1010	家族と親族、民族性、社会組織、家系、高齢者、育児。	www.childcare.gov www.familysearch.org

表 17-9　Cisco IronPort Web 使用コントロール （続き）の URL カテゴリの説明について

URL カテゴリ	省略形	コード	説明	URL の例
Software Updates	swup	1053	ソフトウェア パッケージの更新をホスティングする Web サイト。	www.softwarepatch.com www.versiontracker.com
Sports and Recreation	sprt	1008	プロとアマチュアのすべてのスポーツ、レクリエーション活動、釣り、ファンタジー スポーツ、公共公園、アミューズメント パーク、親水公園、テーマ パーク、動物園、水族館、温泉。	www.espn.com www.recreation.gov
Streaming Audio	aud	1073	インターネット ラジオおよびオーディオ フィードなどのリアルタイムのストリーミング オーディオのコンテンツ。	www.live-radio.net www.shoutcast.com
Streaming Video	vid	1072	インターネット テレビ、Web キャスト、ビデオ共有などのリアルタイムのストリーミング ビデオ。	www.hulu.com www.youtube.com
Tobacco	tob	1078	たばこ専門 Web サイト、たばこ製造業、パイプと喫煙用商品（不法ドラッグ使用のため販売されているものではない）。たばこ依存に関しては「Health and Nutrition」に分類されます。	www.bat.com www.tobacco.org
Transportation	trns	1044	個人輸送、車とバイクに関する情報、新車と中古車およびバイクの購入、カー クラブ、ボート、飛行機、レクレーショナル ビークル（RV）、その他の類似項目。車とバイクのレースは「Sports and Recreation」に分類されます。	www.cars.com www.motorcycles.com
Travel	trvl	1046	ビジネス旅行と個人旅行、トラベル情報、トラベル リソース、旅行代理店、休暇利用のパック旅行、船旅、宿泊施設、旅行に関する輸送、航空券の予約、航空運賃、レンタカー、別荘。	www.expedia.com www.lonelyplanet.com
Unclassified	—	—	シスコのデータベースに存在しない Web サイトは、レポートのために未分類として記録されます。入力ミスした URL が含まれます。	—
Weapons	weap	1036	銃販売者、銃のオークション、銃に分類される広告、銃の装飾品、銃のショー、銃のトレーニングなどの通常兵器の購入または使用に関連する情報、銃に関する一般的な情報、他の武器とグラフィック ハンティング サイトも含まれることがあります。政府軍の Web サイトは「Government and Law」に分類されます。	www.coldsteel.com www.gunbroker.com
Web Hosting	whst	1037	Web サイトのホスティング、帯域幅サービス。	www.bluehost.com www.godaddy.com
Web Page Translation	tran	1063	言語間での Web ページの変換。	babelfish.yahoo.com translate.google.com
Web-based Email	mail	1038	公開された 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 サービスにアクセスするための Web サイトは、「Organizational Email」に分類されます。	mail.yahoo.com www.hotmail.com

18
アプリケーションの可視性と制御について

アプリケーションの制御の概要

Salesforce.com や Google Apps などのブラウザ ベースのアプリケーション プラットフォームか、または企業ネットワークの内部および外部で広く使用できる転送として Web プロトコルを使用する Cisco WebEx などのリッチ メディア アプリケーションかにかかわらず、Web は企業内でアプリケーションを配信するユビキタス プラットフォームになりました。

Cisco IronPort Web 使用率制御には、Application Visibility and Control エンジン（AVC エンジン）が含まれているため、管理者は、特定のアプリケーション タイプをより精密に制御できるようになります。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、アプリケーションで使用される Web トラフィックを深く理解し、管理できるように、Web トラフィックを検査します。アプリケーション制御によって、たとえば URL フィルタリングのみを使用した場合と比較して、より細かく Web トラフィックを制御できます。

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なくても、ネットワーク上で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。

アプリケーション制御によって、次のアプリケーション タイプへの可視性と制御が提供されます。

- 回避アプリケーション（アノニマイザや暗号化トンネルなど）。
- コラボレーション アプリケーション（Cisco WebEx、インスタント メッセージなど）。
- リソースを大量消費するアプリケーション（ストリーミング メディアなど）。

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、次の手順を実行します。

1. AVC エンジンをイネーブルにします。詳細については、「「AVC エンジンのイネーブル化」（P.18-3）」を参照してください。
2. アクセス ポリシーでアプリケーション管理設定を定義します。詳細については、「「アプリケーション制御の設定について」（P.18-3）」を参照してください。

AVC エンジンを使用して、アプリケーション タイプごとに、または特定のアプリケーションをブロックまたは許可できます。また、特定のアプリケーション タイプをより細かく制御できます。たとえば、次のタスクを実行できます。

- **輻輳を制御するためにアプリケーション タイプが消費する帯域幅を制限します。**詳細については、「「帯域幅の制御」（P.18-8）」を参照してください。

- **インスタント メッセージのトラフィックを許可しますが、インスタント メッセンジャを使用したファイル共有は禁止します。**詳細については、「「インスタント メッセージ トラフィックの制御」（P.18-11）」を参照してください。
- **検索エンジンと、ユーザが生成したコンテンツのサイトで安全な検索を実行します。**詳細については、「「アダルト コンテンツのフィルタリング」（P.17-18）」を参照してください。
- **一部のコンテンツ共有サイトのアダルト コンテンツへのアクセスを制限します。**詳細については、「「アダルト コンテンツのフィルタリング」（P.17-18）」を参照してください。

AVC エンジンは、Cisco Ironport アップデート サーバから動的に新しいアプリケーションおよびアプリケーション タイプのサポートなどの更新を受信できます。詳細については、「「AVC エンジン アップデート」（P.18-2）」を参照してください。

また、[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 アクティビティも調べることができます。詳細については、「「AVC アクティビティの表示」（P.18-11）」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 エンジンがトランザクションをブロックすると、Web プロキシによってエンド ユーザにブロック ページが送信されます。ただし、すべての Web サイトがエンド ユーザにブロック ページを表示するわけではありません。たとえば、Web 2.0 の Web サイトは、静的 Web ページの代わりに Javascript を使用して動的コンテンツを表示し、ブロック ページを表示することはありません。ユーザは、悪意のあるデータのダウンロードを適切にブロックされていますが、この情報が常に Web サイトで通知されるとは限りません。

AVC エンジン アップデート

AVC は、AVC エンジンを含む、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。AVC エンジン アップデートには、新しいアプリケーション タイプとアプリケーションのサポートが含まれる場合があります。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向けの更新されたサポートも含まれます。AsyncOS のバージョンが変わる際に AVC エンジンを更新すると、サーバのアップグレードを必要とせずに、Web セキュリティ アプライアンスの柔軟性が保たれます。

AVC エンジン アップデートは、Cisco Security Intelligence Operations（SIO）センターによって維持されます。Cisco SIO は、必要に応じてシグニチャを更新し、変化する市場に対応します。

AVC エンジンは、新しいアプリケーションおよびアプリケーション タイプのサポートを受けられるため、AsyncOS for Web によって、グローバル アクセス ポリシーの次のデフォルト アクションが割り当てられます。

- 新しいアプリケーション タイプのデフォルト設定はモニタリングです。
- 特定アプリケーション内のブロック ファイル転送などの新しいアプリケーション動作のデフォルト設定は、モニタリングです。
- 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設定は、そのアプリケーション タイプのデフォルト設定です。

AVC エンジンのイネーブル化

Cisco IronPort Web 使用コントロール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）] ページに移動します。

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

ステップ 3　[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　[使用許可コントロール サービス（Acceptable Use Controls Service）] エリアで、Cisco IronPort Web 使用コントロールを選択してから、[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、保存します。

アプリケーション制御の設定について

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。

- **アプリケーション タイプ。**1 つまたは複数のアプリケーションを含むカテゴリです。たとえば、インスタント メッセージは、Google Talk、AOL Instant Messenger を含むアプリケーション タイプです。
- **アプリケーション。**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です。たとえば、YouTube はメディア アプリケーション タイプに含まれるアプリケーションです。
- **アプリケーション動作。**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。たとえば、ユーザは Yahoo Messenger などのアプリケーションの使用中にファイルを転送できます。すべてのアプリケーションに、設定可能なアプリケーション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。[アクセス ポリシー：アプリケーションの表示およびコントロール：*policyname*（Access Policies: Applications Visibility and Control: *policyname*）] ページ、略して「Applications Visibility and Control ページ」が表示されます。

Applications Visibility and Control ページには、現在の AVC エンジンのシグニチャに従って設定可能な現在のアプリケーションが表示されます。設定できる特定のアプリケーションに関係なく、Applications Visibility and Control ページでは、アプリケーションの設定に関する次のビューを使用できます。

- **参照ビュー。**アプリケーション タイプを参照できます。参照ビューを使用して、特定のタイプの複数のアプリケーションを同時に設定できます。詳細については、「参照ビューの使用」（P.18-4）」を参照してください。
- **検索ビュー。**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、検索ビューを使用できます。詳細については、「検索ビューの使用」（P.18-5）」を参照してください。

両方のビューで、同じ管理設定のほとんどを設定できます。ただし、アプリケーション タイプの帯域幅制御の制限を設定できるのは、参照ビューのみです。

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。

- **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。**このアクションは、中間アクションです。Web プロキシは、トランザクションを他の管理設定と比較し続け、適用する最終アクション決定します。詳細については、「モニタ アクションについて」（P.9-3）を参照してください。
- **制限。**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。

参照ビューの使用

図 18-1 は、ユーザ定義アクセス ポリシーの Applications Visibility and Control ページの参照ビューを示しています。

図 18-1　ユーザ定義アクセス ポリシーのアプリケーションの設定：参照ビュー

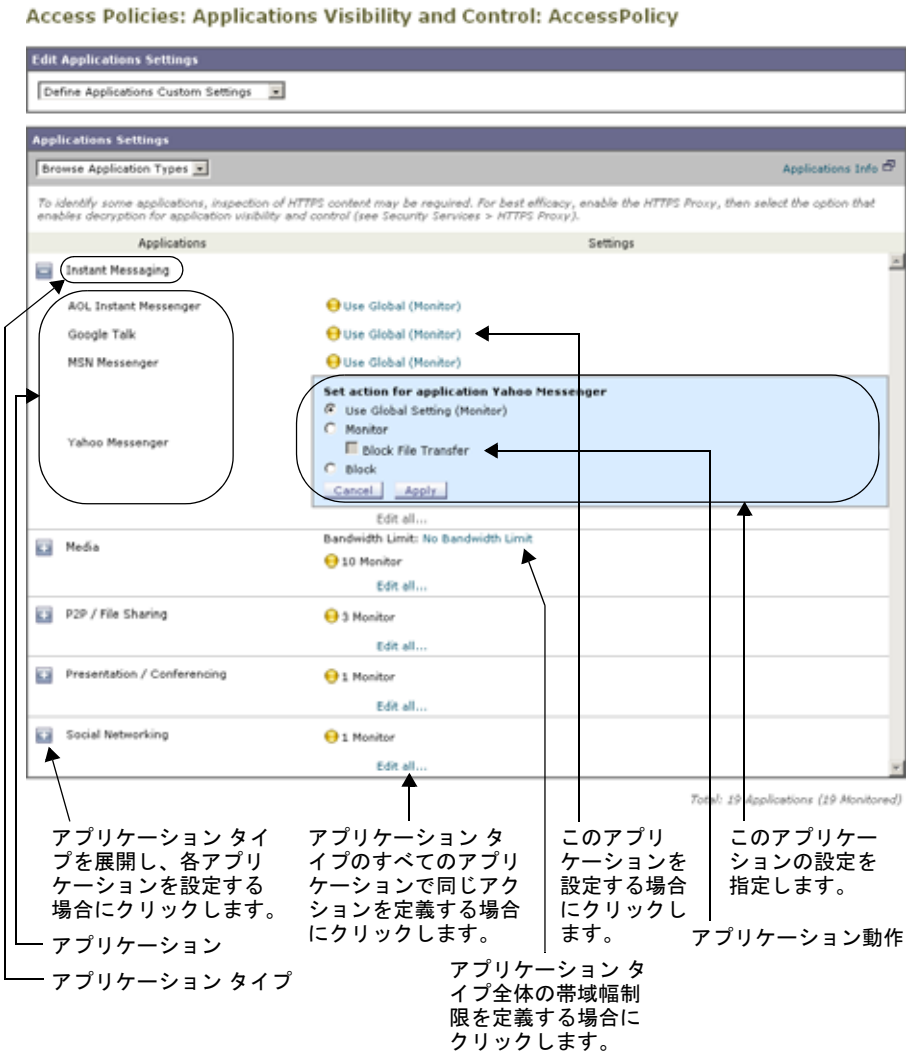
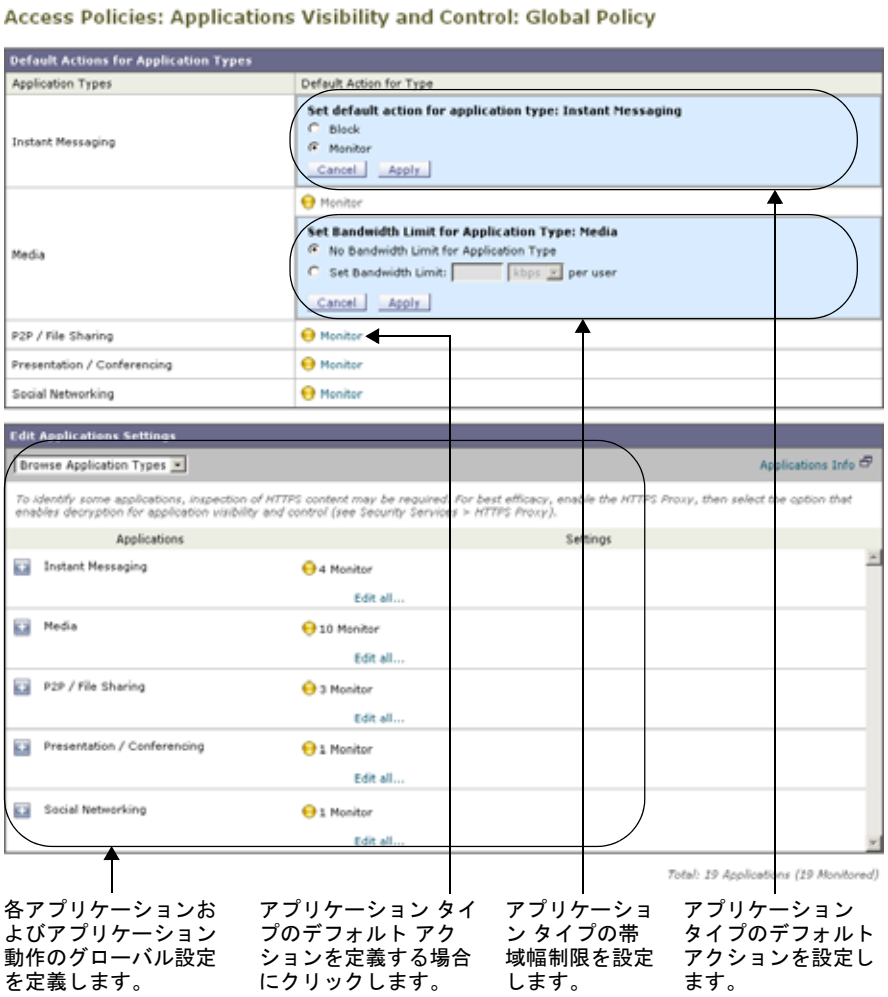


図 18-2 は、グローバル アクセス ポリシーの Applications Visibility and Control ページの参照ビューを示しています。

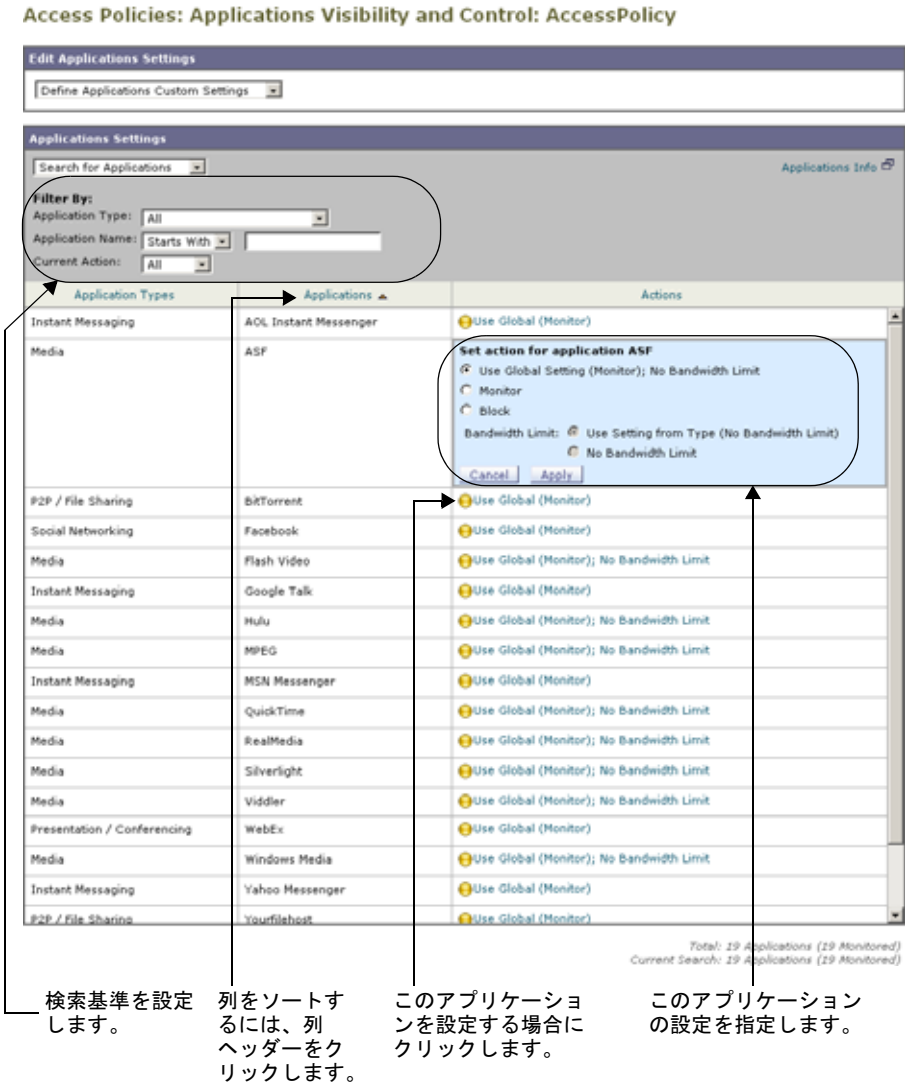
図 18-2　グローバル アクセス ポリシーのアプリケーションの設定：参照ビュー



検索ビューの使用

図 18-3 は、ユーザ定義アクセス ポリシーの Applications Visibility and Control ページの検索ビューを示しています。

図 18-3　ユーザ定義アクセス ポリシーのアプリケーションの設定：検索ビュー



ルールとガイドライン

アプリケーション制御の設定時には、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の動作は、AVC エンジンのアップデート中の AsyncOS for Web のアップグレードに応じて変わる可能性があります。
- アプリケーション タイプが参照ビュー内で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のリストが表示され、アクションがグローバル ポリシーから継承されたか、または現在のアクセス ポリシーで設定されているのかどうかは示されません。アプリケーションのアクションに関する情報を調べるには、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。各アプリケーション タイプのデフォルト アクションを設定すると、Application Visibility and Control エンジンアップデートで導入された新しいアプリケーションが自動的にデフォルト アクションを継承します。
- 参照ビューでアプリケーション タイプの「edit all」リンクをクリックすると、同じアプリケーション タイプのすべてのアプリケーションに同じアクションをすばやく設定できます。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のみです。アプリケーション動作を設定するには、同じタイプのすべてのアプリケーションを同時に編集するのではなく、アプリケーションを個別に編集する必要があります。
- 検索ビューでは、アクション列で表をソートすると、最終アクションに基づいて並べ替えられます。たとえば、「Use Global (Block)」が「Block」の後に並べられます。
- 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

- 「証明書」（P.11-3）
- 「AVC エンジンによる復号化」（P.11-6）

アクセス ポリシー グループのアプリケーション管理設定

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）] ページの順に進みます。

ステップ 2　ポリシーの表で、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は、[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。この方法の詳細については、図 18-2（P.18-5）を参照してください。

ステップ 4　ユーザ定義アクセス 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（[ブラウズ（Brows）]）または検索ビュー（[検索（Search）]）を選択します。

ステップ 6　各アプリケーションおよびアプリケーション動作のアクションを設定します。

各ビューの使用の詳細については、「参照ビューの使用」（P.18-4）と「検索ビューの使用」（P.18-5）を参照してください。

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。詳細については、「「帯域幅の制御」（P.18-8）」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。

帯域幅の制御

AVC エンジンで管理者は、特定のアプリケーション タイプが使用する帯域幅の量を制御できます。アプリケーション タイプには、帯域幅制御をサポートしていないものもあります。

次の帯域幅制限を定義できます。

- **全体の帯域幅制限。**サポートされるアプリケーション タイプについて、ネットワークのすべてのユーザの全体的な制限を定義します。全体の帯域幅制限は、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。また、Web キャッシュからのトラフィックは制限しません。全体の帯域幅制限を定義すると、ストリーミング メディア サイトなどのトラフィックの多いサイトに使用されるネットワーク トラフィックの量を制限できます。詳細については、「「全体の帯域幅制限の設定」（P.18-8）」を参照してください。
- **ユーザの帯域幅制限。**アプリケーション タイプごとに、ネットワークの特定の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を定義すると、使用率の高いユーザがアクセプタブル ユース ポリシーを適用するために消費するトラフィック量を制限できます。詳細については、「「ユーザの帯域幅制限の設定」（P.18-8）」を参照してください。

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すると、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。

（注）　帯域幅制限を定義すると、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 プロキシにより、各アプリケーションのトランザクションに遅延が生じ、サーバへの低速リンクのように見えます。

全体の帯域幅制限の設定

全体の帯域幅制限は、ネットワーク内のすべてのユーザに関して、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。

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）] ページに移動します。

ステップ 2　[制限値（Limit to）] オプションを選択します。

ステップ 3　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 4　変更を送信し、保存します。

ユーザの帯域幅制限の設定

ユーザの帯域幅制限は、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て定義します。アクセス ポリシーでユーザの帯域幅制御の次のタイプを定義できます。

- **アプリケーション タイプのデフォルトの帯域幅制限。**グローバル アクセス ポリシーでは、1 つのアプリケーション タイプのすべてのアプリケーションのデフォルト帯域幅制限を定義できます。詳細については、「「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」（P.18-9）」を参照してください。
- **アプリケーション タイプの帯域幅制限。**ユーザ定義アクセス 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。帯域幅制限を排除するか、または別の帯域幅制限値を設定できます。詳細については、「「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」（P.18-9）」を参照してください。
- **アプリケーションの帯域幅制限。**ユーザ定義アクセス ポリシーまたはグローバル アクセス ポリシーでは、アプリケーション タイプの帯域幅制限を適用するか、または制限を適用しない（アプリケーション タイプの制限を排除する）ことを選択できます。アプリケーションの帯域幅制限を排除して、アプリケーション タイプに設定された帯域幅制限からアプリケーションを免除することができます。詳細については、「「アプリケーションの帯域幅制御の設定」（P.18-10）」を参照してください。

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）] ページの順に進みます。

ステップ 2　ポリシーの表で、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「Bandwidth Limit」の横にあるリンクをクリックします。

ステップ 4　「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。これを実行する方法の詳細については、図 18-2（P.18-5）を参照してください。

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。

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。

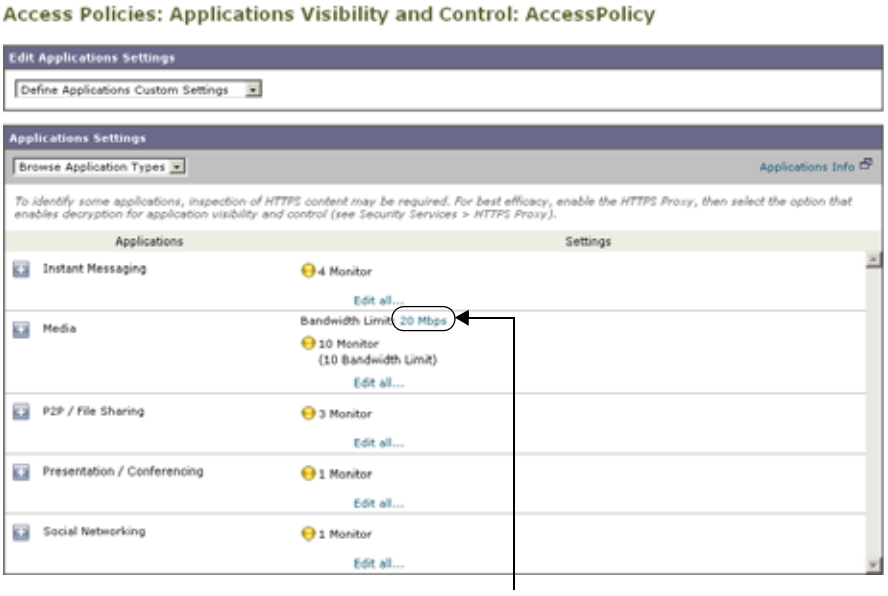
ステップ 1　[Web セキュリティ マネージャ（Web Security Manager）] > [アクセス ポリシー（Access Policies）] ページの順に進みます。

ステップ 2　ポリシーの表で、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。

（注）　参照ビューを使用していることを確認します。検索ビューに切り替えないでください。

図 18-4　　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



ステップ 4　編集するアプリケーション タイプの「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　[完了（Done）] をクリックします。

ステップ 7　変更を送信し、保存します。

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）] ページの順に進みます。

ステップ 2　ポリシーの表で、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を含むアプリケーション 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）] を選択してから、アプリケーション タイプに定義されている帯域幅制限を使用するか、または制限を使用しないことを選択します。

（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 タイプに帯域幅制限が定義されていない場合は適用されません。

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、保存します。

インスタント メッセージ トラフィックの制御

AVC エンジンを使用して、HTTP 上で実行される一部のインスタント メッセンジャ（IM）のトラフィックに管理設定を適用できます。IM トラフィックのブロックやモニタを実行でき、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とも呼ばれます）をブロックすることもできます。たとえば、特定の IM サービス プロバイダーとの IM セッションを許可しながら、そのセッション内のファイル転送をブロックすることができます。

AVC エンジンは、ネイティブ IM トラフィックを制御しません。

IM トラフィックは、アクセス ポリシーの Applications Visibility and Control ページにあるインスタント メッセンジャ アプリケーション設定を指定して制御します。

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）] ページの順に進みます。

ステップ 2　ポリシーの表で、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　[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 4　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 5　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 6　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、ブロックするアプリケーション動作を選択します。

ステップ 7　[完了（Done）] をクリックします。

ステップ 8　変更を送信し、保存します。

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 タイプについての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。個々のアプリケーションおよびアプリケーション タイプをクリックすると、それぞれの情報を確認できます。モニタリングおよびレポート機能の詳細については、「レポート」（P.22-1）を参照してください。

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 スキャン判定情報のセクションには、表 18-1 に示すフィールドが含まれます。

表 18-1　アプリケーション可視性制御のロギング情報

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	%Xu	x-avc-type
アプリケーション動作	%Xb	x-avc-behavior

アクセス ログの詳細については、「ログ ファイルへのアクセス」（P.24-17）を参照してください。

19
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、複数のセキュリティ コンポーネントを使用して、さまざまな Web ベースのマルウェアの脅威からエンド ユーザを保護します。

- **アンチマルウェア スキャン。**Cisco IronPort DVS™ エンジンは、アプライアンスに結合された複数のアンチマルウェア 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。詳細については、「「アンチマルウェア スキャンの概要」（P.19-4）」を参照してください。
- **Web レピュテーション フィルタ。**これは、Web サーバの動作を分析し、URL ベースのマルウェアが含まれている可能性を判断するためのレピュテーション スコアを URL に割り当てるセキュリティ機能です。詳細については、「「Web レピュテーション フィルタの概要」（P.19-2）」を参照してください。

マルウェアからエンド ユーザを保護するために、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、ポリシーごとにアンチマルウェアおよび Web レピュテーションの設定値を設定します。詳細については、「Web レピュテーションおよびアンチマルウェア フィルタのイネーブル化」（P.19-9）および「ポリシーへの Web レピュテーションとアンチマルウェアの設定」（P.19-11）を参照してください。

各ポリシー グループでアンチマルウェアおよび Web レピュテーション設定値を設定できますが、アクセス ポリシーを設定する場合、ブロックするコンテンツを判別するときに、Web 用 AsyncOS がアンチマルウェア スキャンと Web レピュテーション スコアの最良の組み合わせを選択するようにすることもできます。詳細については、「「Adaptive Scanning について」（P.19-9）」を参照してください。

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 サーバの動作を分析し、Web ベース Reputation Score（WBRS）を URL に割り当てて、URL ベースのマルウェアを含む可能性があるかを判別するセキュリティ機能です。この機能は、エンドユーザのプライバシーや企業の機密情報を危険にさらす URL ベースのマルウェアを防ぐために役立ちます。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、疑わしいアクティビティを特定して、マルウェア攻撃を未然に防ぎます。

Web レピュテーション フィルタは、特にマルウェア ライターに屈した正規の Web サイトからユーザを保護するために、マルウェアのまん延した動的な性質に対処するように設計されています。

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 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、統計的に有意な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。特定のドメインが登録されていた期間、Web サイトがホストされている場所、Web サーバがダイナミック IP アドレスを使用しているかどうかなどのデータを使用して、特定の URL の信頼性が判定されます。

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、またはクライアント IP アドレスなどの個人識別情報を収集しません。

Web レピュテーション フィルタの操作について

Web レピュテーション スコアは URL 要求で実施するアクションに関連付けられます。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。

- **アクセス ポリシー。**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。**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。

各ポリシー グループを特定の Web レピュテーション スコアへのアクションを関連付けるように設定できます。

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 レピュテーション設定値を設定する場合、設定を手動で設定するか、Web 用 AsyncOS が Adaptive Scanning を使用して最良のオプションを選択するようにできます。

Adaptive Scanning がイネーブルの場合、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。Adaptive Scanning の詳細については、「Adaptive Scanning について」（P.19-9）を参照してください。

表 19-1 は、Adaptive Scanning がディセーブルのときに編集できるアクセス ポリシーのデフォルトの Web レピュテーション スコアについて説明します。

表 19-1　アクセス ポリシーのデフォルトの Web レピュテーション スコア

スコア	アクション	説明	例
-10 ～ -6.0	ブロック	不正なサイト。要求がブロックされ、さらなるマルウェア スキャンは実行されません。	• URL は、ユーザの許可なしで情報をダウンロードします。 • URL ボリュームによる突然のスパイク。 • URL が人気あるドメインの誤植です。
-5.9 ～ 5.9	スキャン	判別不能なサイト。さらなるマルウェア スキャンに対して、要求が DVS エンジンに渡されます。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。 • プラスの Web レピュテーション スコアを持つネットワーク オーナーの IP アドレス。
6.0 ～ 10.0	許可	優れたサイト。要求が許可されます。マルウェア スキャンは必要ありません。	• URL には、ダウンロード可能なコンテンツがありません。 • 長い歴史がある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存在するドメイン。 • 評価が低い URL へのリンクがありません。

たとえばデフォルトで、+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。ただし、+3 などの HTTP 要求の弱いスコアは、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。非常に評価が低い HTTP 要求の URL がブロックされます。

復号化ポリシーの Web レピュテーション

表 19-2 は、復号化ポリシーのデフォルトの Web レピュテーション スコアについて説明します。

表 19-2　復号化ポリシーのデフォルトの Web レピュテーション スコア

スコア	アクション	説明
-10 ～ -9.0	ドロップ	不正なサイト。要求がエンド ユーザに通知なしでドロップされます。 このコマンド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。 アプライアンスが HTTPS トラフィックを復号化する方法の詳細については、「証明書」（P.11-3）を参照してください。
6.0 ～ 10.0	パススルー	優れたサイト。要求は、検査または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

表 19-3 は、Cisco IronPort データ セキュリティのデフォルトの Web レピュテーション スコアについて説明します。

表 19-3　Cisco IronPort データ セキュリティ ポリシーのデフォルトの Web レピュテーション スコア

スコア	アクション	説明
-10 ～ -6.0	ブロック	不正なサイト。トランザクションがブロックされ、さらなるスキャニングは実行されません。
-5.9 ～ 0.0	モニタ	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、コンテンツの確認（ファイル タイプとサイズ）に進みます。 **（注）**　スコアがないサイトがモニタされます。

アンチマルウェア スキャンの概要

Web セキュリティ アプライアンスのアンチマルウェア機能は、ゼロデイ脅威を含む Web ベースのマルウェアの脅威を識別し、停止するためにアプライアンスに統合された複数のアンチマルウェア スキャン エンジンと併用して Cisco IronPort DVS™ エンジンを使用するセキュリティ コンポーネントです。DVS エンジンは、Webroot™、McAfee、および Sophos アンチマルウェア スキャン エンジンに使用します。

DVS エンジンの詳細については、「Cisco IronPort DVS™（Dynamic Vectoring and Streaming）エンジン」（P.19-5）を参照してください。

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、アンチマルウェア スキャンをイネーブルにしてから、グローバル設定値を設定して、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。詳細については、「Web レピュテーションおよびアンチマルウェア フィルタのイネーブル化」（P.19-9）および「ポリシーへの Web レピュテーションとアンチマルウェアの設定」（P.19-11）を参照してください。

Cisco IronPort DVS™（Dynamic Vectoring and Streaming）エンジン

Cisco IronPort Dynamic Vectoring and Streaming（DVS）エンジンは、商業上侵略的なアドウェア アプリケーションから、悪意のあるトロイの木馬、システム モニタ、およびフィッシング攻撃の幅広い Web ベースのマルウェアに対して保護を提供する Web トラフィックを検査します。

Cisco IronPort DVS エンジンは、マルウェアのリスクを判別するのに 1 つ以上のスキャン エンジンを使用できます。アプライアンスと共に購入した機能によって、次のスキャン エンジンをイネーブルにできます。

- **Webroot。**Webroot の自動化されたスパイウェア検出システムは、毎日のように何百万ものサイトをインテリジェントにスキャンすることで、インターネット上の既存および新規のスパイウェアの脅威を迅速に特定します。Webroot はシグニチャ データベースを使用して、インターネットの脅威の検出を支援します。詳細については、「Webroot スキャン」（P.19-7）を参照してください。
- **McAfee。**McAfee スキャン エンジンは、マルウェア情報とヒューリスティック分析のシグニチャ データベースを使用して、既存および新規のマルウェアの脅威を検出できます。詳細については、「McAfee スキャン」（P.19-7）を参照してください。
- **Sophos。**Sophos スキャン エンジンは、シグニチャ データベースを使用して、既存および新規のマルウェアの脅威を検出できます。詳細については、「Sophos スキャン」（P.19-8）を参照してください。

スキャン エンジンはトランザクションを検査して、DVS エンジンに渡すためのマルウェア スキャンの判定を判別します。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。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またはブロックするかどうかを決めます。マフウェア スキャンの判定の詳細については、「マルウェア スキャンの判定値」（P.24-42）を参照してください。

すべてのスキャン エンジンをグローバルにイネーブルにできますが、各アクセスまたは発信マルウェア スキャン ポリシーに対して Sophos または McAfee スキャン エンジンをイネーブルにできます（同時に両方をイネーブルにすることはできません）。同様に、各アクセスまたは発信マルウェア スキャン ポリシーに対して Sophos または McAfee で Webroot スキャン エンジンをイネーブルにすることもできます。クライアント マシンに 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、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。

場合によっては、DVS エンジンが 1 つの URL に対して複数の判定を判別する場合もあります。DVS が複数の判定を処理する方法の詳細については、「複数のマルウェアの判定の操作」（P.19-6）を参照してください。

DVS エンジンの操作について

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る URL のトランザクションでアンチマルウェア 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 がマルウェアを含む可能性を計算し、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る URL スコアを割り当てます。

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す場合、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。Webroot または Sophos、またはその両方、あるいは McAfee スキャン エンジンとの組み合わせによる DVS エンジンは、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 ポリシーの設定からの情報を使用して、クライアントへのコンテンツをブロックまたは配信するかどうかを判別します。

Webroot および Sophos または McAfee の両方をイネーブルにすると、DVS エンジンはパフォーマンスと効果を最適化するためのコンテンツをスキャンする方法を判別します。

複数のマルウェアの判定の操作

場合によっては、DVS エンジンが 1 つの URL に対して複数のマルウェアの判定を判別する場合もあります。イネーブルにされた一方または両方のスキャン エンジンから複数の判定を取得できます。

- **異なるスキャン エンジンによるさまざまな判定。**Webroot および Sophos または McAfee の両方をイネーブルにすると、各スキャン エンジンは同じオブジェクトで異なるマルウェアの判定を返す可能性があります。
- **同じスキャン エンジンからの異なる判定。**スキャン エンジンは、オブジェクトに複数の感染が含まれている場合に、1 つのオブジェクトに対して複数の判定を返す可能性があります。たとえば zip ファイルには、異なる種類のマルウェアに感染した複数のファイルが含まれる可能性があります。

1 つの URL に対して複数の判定が行われると、イネーブル化された一方または両方のスキャン エンジンが複数のマルウェアの判定を返すかどうかに応じて、アプライアンスが異なるアクションを実行します。

異なるスキャン エンジン

1 つの URL に対して複数の判定が両方のイネーブル化されたスキャン エンジンから行われると、アプライアンスは最も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す場合、DVS エンジンは常に要求をブロックします。最も厳しい判定だけが記録され、レポートされます。

同じスキャン エンジン

1 つの URL に対して複数の判定が同じスキャン エンジンから行われると、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。最上位の判定だけが記録され、レポートされます。次のテキストは、最上位から最下位の優先順位で考えられるマルウェア スキャンの判定を示します。

- 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
- Adware
- 暗号化ファイル
- スキャン不可
- その他のマルウェア

McAfee スキャン エンジンがスキャンされたオブジェクトでアドウェアおよびウィルスの両方を検出し、アプライアンスがアドウェアをブロックし、ウィルスをモニタするように設定されているとします。上記のリストに従って、優先順位が高いウィルスはアドウェアよりカテゴリを判定します。そのため、アプライアンスはオブジェクトをモニタし、レポートとログのウィルスとして判定を報告します。アドウェアをブロックするように設定されている場合でも、オブジェクトをブロックしません。

Webroot スキャン

Webroot スキャン エンジンは DVS エンジンに送信するために、オブジェクトを検査してマルウェア スキャンの判定を判別します。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ることを Webroot が疑うと、アプライアンスの設定に応じて、アプライアンスが要求をモニタまたはブロックします。Webroot の評価が要求をクリアすると、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 データベースと比較します。

DVS エンジンが Web トラフィックを処理するためにマルウェア スキャンの判定を使用する方法の詳細については、「Cisco IronPort DVS™（Dynamic Vectoring and Streaming）エンジン」（P.19-5）を参照してください。

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、DVS エンジンが要求をモニタまたはブロックするかどうかを判別できるように、マルウェア スキャンの判定を DVS エンジンに渡します。

McAfee ウィルス スキャン エンジンは次の方法を使用して、マルウェア スキャンの判定を判別します。

- 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

DVS エンジンが Web トラフィックを処理するためにマルウェア スキャンの判定を使用する方法の詳細については、「Cisco IronPort DVS™（Dynamic Vectoring and Streaming）エンジン」（P.19-5）を参照してください。

ウィルス シグニチャ パターンの照合

McAfee は、データベース内のウィルス定義をスキャン エンジンで使用して、特定のウィルス、ウィルスのタイプ、またはその他の潜在的に望ましくないソフトウェアを検出します。ファイル内のウィルス シグニチャを検索します。

McAfee をイネーブルにすると、McAfee ウィルス スキャン エンジンはこの方法を常に使用して、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

Web 上には新しい脅威が毎日のように現れます。シグネチャは未知であるため、ウィルス シグニチャを使用するだけでは、新しいウィルスまたはその他のマルウェアは検出できません。ただし、ヒューリスティック分析を使用することで McAfee ウィルス スキャン エンジンは、現在未知のウィルスやマルウェアの新しいクラスを事前に検出できます。

ヒューリスティック分析は、新しいウィルスとマルウェアの検出に特定のルールではなく、一般的なルールを使用する手法です。McAfee スキャン エンジンがヒューリスティック分析を使用すると、オブジェクトのコードを確認し、一般的なルールを適用し、どの程度オブジェクトがウィルス様になるかを決めます。

ヒューリスティック分析を使用すると、McAfee がウィルス シグニチャ データベースを更新する前に、ウィルスとマルウェアを取り込む可能性を高めます。ただし、偽陽性（ウィルスとして指定されたコンテンツの消去）を報告する可能性も高めます。また、アプライアンスのパフォーマンスに影響する場合があります。

McAfee をイネーブルにすると、オブジェクトのスキャンでヒューリスティック分析もイネーブルにするかどうかも選択できます。

McAfee カテゴリ

表 19-4 は、McAfee の判定およびマルウェア スキャン判定カテゴリにどのように対応するかを示します。

表 19-4　McAfee 判定のアプライアンス 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	トロイの木馬
ジョーク ファイル	Adware
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	Adware
望ましくないソフトウェア パッケージ	Adware
暗号化ファイル	暗号化ファイル

マルウェア スキャン判定の一覧については、「マルウェア スキャンの判定値」（P.24-42）を参照してください。

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、DVS エンジンが要求をモニタまたはブロックするかどうかを判別できるように、マルウェア スキャンの判定を DVS エンジンに渡します。クライアント マシンに 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、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。

DVS エンジンが Web トラフィックを処理するためにマルウェア スキャンの判定を使用する方法の詳細については、「Cisco IronPort DVS™（Dynamic Vectoring and Streaming）エンジン」（P.19-5）を参照してください。

Adaptive Scanning について

Adaptive Scanning は、Web レピュテーションとコンテンツ タイプを関連付け、アンチマルウェア スキャン エンジンが Web 要求を処理する現在の脅威のプロファイルに基づいて決定する論理層です。

Adaptive Scanning は、リスクの高いコンテンツを識別し、使用可能なアンチマルウェア サービスの最良の組み合わせを自動的に選択することで効果を高めます。既知のマルウェアとして特定されているコンテンツを自動的にブロックできます。Adaptive Scanning 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「Outbreak Heuristics」アンチマルウェア カテゴリを適用します。アプライアンスにアンチマルウェア設定を行う場合に、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。

Adaptive Scanning のイネーブル化はマルウェアを除外するための効果を高めますが、アプライアンス パフォーマンスを多少低下させる原因となります。

Adaptive Scanning を使用するには、Web レピュテーション フィルタをイネーブルにします。

Adaptive Scanning をイネーブルにすると、アクセス ポリシーに設定できる Web レピュテーションとアンチマルウェア設定がわずかに異なります。

- 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。
- 各アクセス ポリシーでアンチマルウェア スキャンをイネーブルにすることができますが、イネーブルにするアンチマルウェア スキャン エンジンを選択することはできません。Adaptive Scanning は、各 Web 要件で最適なエンジンを選択します。

（注）　Adaptive Scanning がイネーブルにされておらず、アクセス ポリシーに特定の Web レピュテーションとアンチマルウェア設定が設定されている場合は、Adaptive Scanning をイネーブルにすると、既存の Web レピュテーションとアンチマルウェア設定が上書きされます。

Web レピュテーションおよびアンチマルウェア フィルタのイネーブル化

Web レピュテーション フィルタ、DVS エンジン、および Webroot、McAfee、および Sophos スキャン エンジンは、システム設定のときにデフォルトでイネーブルにされます。システム設定後に、いつでも Web レピュテーションとアンチマルウェア フィルタをイネーブルにし、グローバル設定値を設定できます。

Web レピュテーションとアンチマルウェア フィルタがイネーブルにされた後、ポリシー グループで Web レピュテーションとアンチマルウェア設定値を設定できます。詳細については、「ポリシーへの Web レピュテーションとアンチマルウェアの設定」（P.19-11）」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）] > [Web レピュテーションおよびマルウェア対策（Web Reputation and Anti-Malware）] ページに移動します。

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

ステップ 3　必要に応じて Web レピュテーションとアンチマルウェア設定値を設定します。表 19-5 は、設定可能な設定値を示します。

表 19-5　Web レピュテーションとアンチマルウェア フィルタ設定 の設定

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）	Adaptive Scanning 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だけ Adaptive Scanning をイネーブルにできます。 詳細については、「「Adaptive Scanning について」（P.19-9）」を参照してください。
オブジェクトスキャン制限（Object Scanning Limits）	最大要求/応答サイズを指定します。 指定する [最大オブジェクト サイズ（Maximum Object Size）] 値は、Cisco IronPort データ セキュリティ フィルタまたは Webroot スキャン エンジンなど Web セキュリティ アプライアンス上のセキュリティ コンポーネントによってスキャンされる可能性がある要求および応答の全サイズに適用されます。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、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。ヒューリスティック スキャンの詳細については、「McAfee スキャン」（P.19-7）を参照してください。 **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、偽陽性になり、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、Threat Risk Threshold（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は URL 一致シーケンスの結果を評価し、Threat Risk Rating（TRR）を割り当てます。この値は、TRT 設定に関連付けられています。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：**90 より低い値に TRT 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ます。シスコは、90 の TRT のデフォルト値を変えない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、保存します。

ポリシーへの Web レピュテーションとアンチマルウェアの設定

Web レピュテーションとアンチマルウェア フィルタがアプライアンスでイネーブルの場合、ポリシー グループの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たマルウェア カテゴリのモニタリングまたはブロックをイネーブルにできます。次のポリシー グループにアンチマルウェア設定値を設定できます。

- **アクセス ポリシー。**設定できる設定は、Adaptive Scanning がイネーブルにされているかによって異なります。詳細については、「「アクセス ポリシーの Web レピュテーションとアンチマルウェア設定」（P.19-11）」を参照してください。
- **発信マルウェア スキャン ポリシー。**発信マルウェア スキャン ポリシーでアンチマルウェア設定値を設定する手順の詳細については、「アウトバウンド マルウェア スキャン ポリシーを使用したアップロード要求の制御」（P.12-7）を参照してください。

次のポリシー グループに 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。**設定できる設定は、Adaptive Scanning がイネーブルにされているかによって異なります。詳細については、「「アクセス ポリシーの Web レピュテーションとアンチマルウェア設定」（P.19-11）」を参照してください。
- **復号化ポリシー。**詳細については、「「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」（P.19-15）」を参照してください。
- **Cisco IronPort データ セキュリティ ポリシー。**詳細については、「「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」（P.19-15）」を参照してください。

アクセス ポリシーの Web レピュテーションとアンチマルウェア設定

Adaptive Scanning がイネーブルの場合、Adaptive Scanning をオフにすると、アクセス ポリシーに設定できる Web レピュテーションとアンチマルウェア設定はわずかに異なります。詳細については、「「Adaptive Scanning について」（P.19-9）」を参照してください。

（注）　配置にセキュリティ管理アプライアンスが含まれ、この機能を Configuration Master に設定する場合、このページのオプションは Adaptive Security が関連する設定マスターでイネーブルにされているかどうかによって異なります。[Web] > [ユーティリティ（Utilities）] > [セキュリティ サービスの表示（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。

Adaptive Scanning がイネーブルにされている Web レピュテーションおよびアンチマルウェア設定値の設定

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）] ページの順に進みます。

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

ステップ 3　「Web Reputation and Anti-Malware Settings」セクションの下で、選択されていない場合に、[Web レピュテーションおよびアンチマルウェア カスタム設定を定義（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 レピュテーション設定およびアンチマルウェア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。Adaptive Scanning は各 Web 要求の最適な Web レピュテーション スコアのしきい値を選択します。

ステップ 5　[Cisco IronPort DVS マルウェア対策設定（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 6　ポリシーのアンチマルウェア設定を必要に応じて指定します。表 19-6 は、Adaptive Scanning がイネーブルの場合に、アクセス ポリシーに対して設定できるアンチマルウェア設定について説明します。

表 19-6　アクセス ポリシーのアンチマルウェア設定：Adaptive Scanning がイネーブルの場合

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 要求ヘッダーに指定されたユーザ 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 [追加のスキャン（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。Adaptive Scanning は、各 Web 要件で最適なエンジンを選択します。
マルウェア カテゴリ（Malware Categories）	各種のマルウェア カテゴリを、マルウェア スキャンの判定に基づいてモニタするかブロックするかを選択します。各カテゴリの詳細については、「マルウェアのカテゴリについて」（P.19-18）を参照してください。
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：**Outbreak Heuristics のカテゴリは、スキャン エンジンを実行する前に Adaptive Scanning によってマルウェアとして識別される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するか、またはシステムが一時的なエラー状態に陥ると、URL トランザクションが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や AsyncOS のアップグレードが行われている間は、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 スキャンの判定である SV_TIMEOUT および SV_ERROR 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 7　変更を送信し、保存します。

Adaptive Scanning がディセーブルにされている Web レピュテーションおよびアンチマルウェア設定値の設定

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）] ページの順に進みます。

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

ステップ 3　「Web Reputation and Anti-Malware Settings」セクションの下で、選択されていない場合に、[Web レピュテーションおよびアンチマルウェア カスタム設定を定義（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 レピュテーション設定およびアンチマルウェア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）] セクションで設定値を設定します。詳細については、「アクセス ポリシーの Web レピュテーション スコアのしきい値の設定」（P.19-14）を参照してください。

ステップ 5　[Cisco IronPort DVS マルウェア対策設定（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 6　ポリシーのアンチマルウェア設定を必要に応じて指定します。表 19-7 は、Adaptive Scanning がディセーブルの場合に、アクセス ポリシーに対して設定できるアンチマルウェア設定について説明します。

表 19-7　アクセス ポリシーのアンチマルウェア設定：Adaptive Scanning がディセーブルの場合

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 要求ヘッダーに指定されたユーザ 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。Webroot 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。
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。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。
マルウェア カテゴリ（Malware Categories）	各種のマルウェア カテゴリを、マルウェア スキャンの判定に基づいて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。各カテゴリの詳細については、「マルウェアのカテゴリについて」（P.19-18）を参照してください。
その他のカテゴリ（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するか、またはシステムが一時的なエラー状態に陥ると、URL トランザクションが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や AsyncOS のアップグレードが行われている間は、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 スキャンの判定である SV_TIMEOUT および SV_ERROR 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 7　変更を送信し、保存します。

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の設定が指定されます。ただし、組織のニーズに適合させるために Web レピュテーション スコアのしきい値設定を変更できます。

各ポリシー グループの Web レピュテーション フィルタ設定値を設定します。

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

Adaptive Scanning がディセーブルの場合に、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。

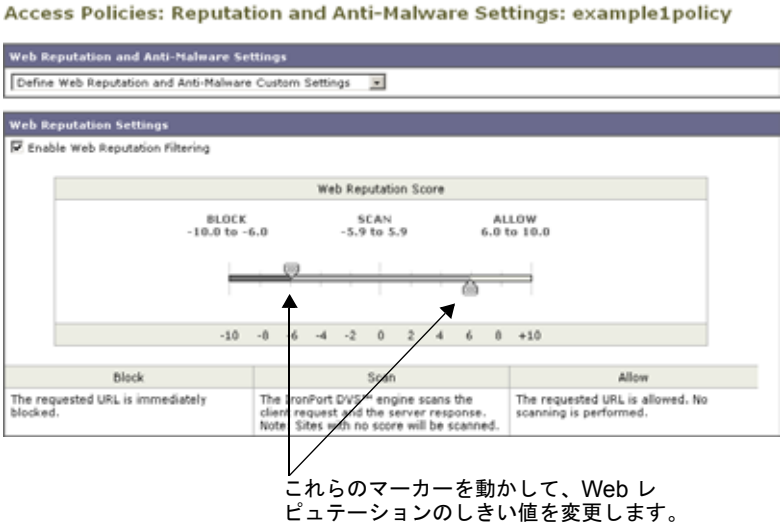
ステップ 1　[Web セキュリティ マネージャ（Web Security Manager）] > [アクセス ポリシー（Access Policies）] ページの順に進みます。

ステップ 2　[Web レピュテーションおよびマルウェア対策フィルタ（Web Reputation and Anti-Malware Filtering）] カラムで、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 レピュテーションおよびマルウェア対策設定（Web Reputation and Anti-Malware Settings）] セクションで、すでに選択されていない場合は、ドロップ ダウン メニューからの「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 レピュテーション設定およびアンチマルウェア設定を指定できます。

図 19-1　アクセス ポリシーに対する Web レピュテーション フィルタの設定



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）] チェックボックス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、保存します。

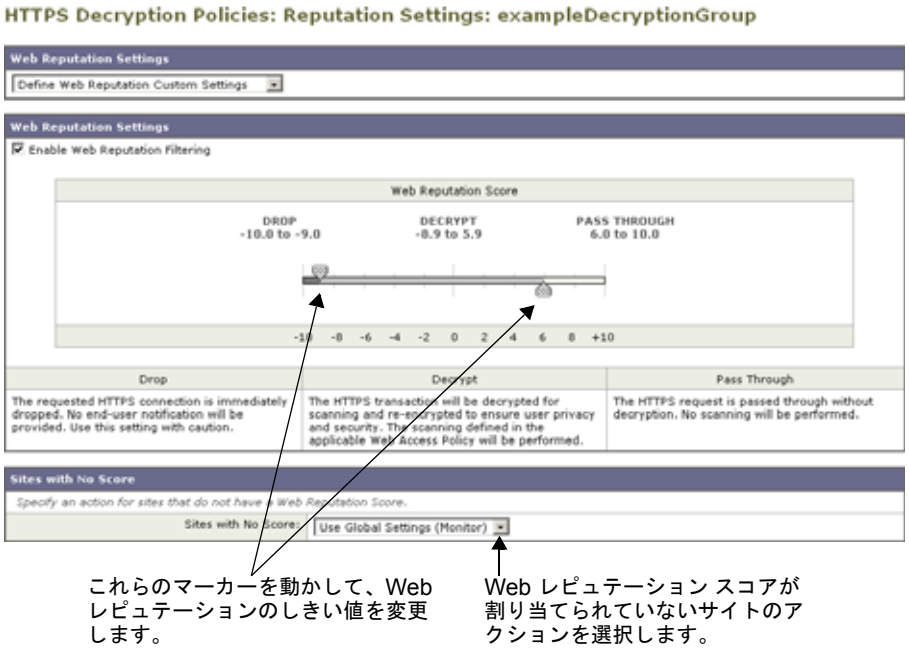
復号化ポリシー グループの Web レピュテーション フィルタの設定

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）] ページに移動します。

ステップ 2　[Web レピュテーション（Web Reputation）] カラムで、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、すでに選択されていない場合は、ドロップ ダウン メニューからの「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 グループから Web レピュテーション設定を上書きすることができます。

図 19-2　復号化ポリシーに対する Web レピュテーション フィルタ設定



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で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。

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

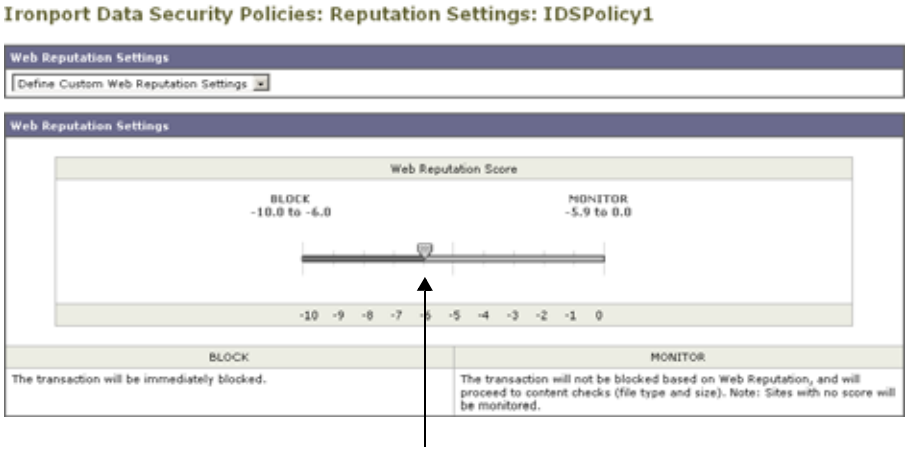
Cisco IronPort データ セキュリティ ポリシーの Web レピュテーションのしきい値には、負またはゼロの値のみ設定できます。定義上、すべての正のスコアがすべてモニタされます。

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）] ページの順に進みます。

ステップ 2　[Web レピュテーション（Web Reputation）] カラムで、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、すでに選択されていない場合は、ドロップ ダウン メニューからの「Define Web Reputation Custom Settings」を選択します。

図 19-3　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 フィルタ設定



これにより、グローバル ポリシー グループから 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のアクションの範囲を変更します。

これらのアクションの詳細については、「データ セキュリティ ポリシー グループ」（P.13-3）を参照してください。

ステップ 5　変更を送信し、保存します。

データベース テーブルの維持

Webroot、Sophos、および McAfee データベースは、Cisco Ironport アップデート サーバ（`https://update-manifests.ironport.com`）からアップデートを定期的に受信します。サーバ アップデートは自動化され、アップデート間隔はアプライアンスではなくサーバによって設定されます。データベース テーブルへのアップデートは、管理者の介入なしで自動的に実行されます。

更新間隔と Cisco IronPort アップデート サーバの詳細については、「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」（P.26-43）を参照してください。

Web レピュテーション データベース

Web セキュリティ アプライアンスは、情報を収集し、集約トラフィック統計情報、要求属性、さまざまなタイプの要求が処理される方法に関する情報が含まれるフィルタリング データベースを維持します。また、アプライアンスは 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設定できます。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、収集情報が Web レピュテーション スコアの作成に使用されます。

（注）　詳細については、「Cisco SensorBase ネットワークへの参加」（P.2-11）を参照してください。

ロギング

アクセス ログ ファイルは、Web レピュテーション フィルタによって返された情報とトランザクションごとの DVS エンジンを記録します。アクセス ログのスキャンの判定情報セクションには、トランザクションに適用される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含まれます。たとえば、一部のフィールドは DVS エンジンに渡される Web レピュテーション スコアまたはマルウェア スキャン判定 Sophos を表示します。

アクセス ログ ファイルのスキャン判定情報セクションに関する詳細については、「スキャン判定情報について」（P.24-24）を参照してください。

アクセス ログ ファイルの読み取り方法の詳細については、「ログ ファイルへのアクセス」（P.24-17）を参照してください。Web レピュテーション処理について説明するアクセス ログ エントリの例については、「Web レピュテーション フィルタの例」（P.24-28）を参照してください。

Adaptive Scanning のロギング

Adaptive Scanning がイネーブルの場合、表 19-8 のフィールドを使用して、Adaptive Scanning Engine がトランザクションにどのように影響するかどうかについて詳細に知ることができます。

表 19-8　Adaptive Scanning のロギング情報

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	Adaptive Scanning から返されたアンチマルウェア名。トランザクションがブロックされなかった場合、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。

Adaptive Scanning Engine 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 の決定タグを使用します。

- BLOCK_AMW_RESP
- MONITOR_AMW_RESP

キャッシング

マルウェアのスキャンで AsyncOS がキャッシュを使用する方法についての注

- オブジェクト全体がダウンロードされたときにだけ、AsyncOS が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 はサーバまたは Web キャッシュから取得されるかどうかに関わらず、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。
- シグニチャが更新されると、AsyncOS が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

表 19-9 は、Web セキュリティ アプライアンスがブロックできるさまざまなマルウェアのカテゴリを示します。

表 19-9　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
Adware	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。アドウェア アプリケーションの中には、別々のプロセスを同時に実行して互いをモニタさせて、変更を永続化するものがあります。変異型の中には、マシンが起動されるたびに自らが実行されるようにするものがあります。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、ユーザがブラウザ検索オプション、デスクトップ、およびその他の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、ユーザの完全で有効な承諾なしに、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、ユーザの完全で有効な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。
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。フィッシングは、ソーシャル エンジニアリングと技術的欺瞞の両方を使用して個人データや金融口座の認証情報を盗み出す、オンライン ID 盗難の一種です。
PUA	望ましくないアプリケーションのこと。PUA は、悪質ではないが好ましくないと見なされるアプリケーションです。

表 19-9　マルウェアのカテゴリについて （続き）

マルウェアのタイプ	説明
システム モニタ	システム モニタには、次のいずれかのアクション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。これらのインストールは、通常はユーザに気付かれることなく行われます。また、トロイのダウンローダはリモート ホストまたはサイトからダウンロード命令を取得するので、インストールごとにペイロードが異なる場合があります。
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。ウィルスとは異なり、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つか、または感染したマシンをスキャンして銀行サイト、オークション サイト、あるいはオンライン支払サイトに関係するユーザ名とパスワードを探します。
ウィルス	ウィルスは、ユーザが気付かない間にコンピュータにロードされ、ユーザの意思に反して実行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、通常は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。

20
認証

認証の概要

認証は、ユーザのアイデンティティを確認する動作です。Web セキュリティ アプライアンスで認証を使用すると、各ユーザまたはユーザ グループによる Web へのアクセスを制御できます。これにより、組織のポリシーを適用し、法規制を遵守することができます。認証を有効にすると、Web セキュリティ アプライアンスが、宛先サーバへのアクセスを許可する前に、ネットワークのクライアントを認証します。

Web セキュリティ アプライアンスは、次の認証プロトコルをサポートしています。

- **Lightweight Directory Access Protocol（LDAP）。**アプライアンスは、標準の LDAP サーバ認証とセキュア LDAP 認証をサポートしています。基本認証方式を使用できます。LDAP 設定オプションの詳細については、「LDAP 認証」（P.20-31）を参照してください。
- **NT LAN Manager（NTLM）。**アプライアンスは、アプライアンスと Microsoft Windows ドメイン コントローラ間の認証を有効にする NTLM をサポートしています。NTLMSSP 認証方式または基本認証方式を使用できます。NTLM 設定オプションの詳細については、「NTLM 認証」（P.20-33）を参照してください。

認証を有効にするには、少なくとも 1 つの認証レルムを作成する必要があります。認証レルムは、特定の設定による単一の認証プロトコルをサポートする一連の認証サーバ（または単一のサーバ）です。認証レルムの詳細については、「認証レルム」（P.20-10）を参照してください。

複数のレルムを作成すると、レルムをグループ化して認証シーケンスにすることができます。認証シーケンスは認証レルムのグループで、クライアントを認証するために Web セキュリティ アプライアンスが使用する順に並べられています。認証シーケンスの詳細については、「認証シーケンスの使用」（P.20-15）を参照してください。

一部の認証オプションは、どのレルムにも依存しないグローバル レベルで設定します。詳細については、「「グローバル認証設定の指定」（P.20-19）」を参照してください。

認証レルムと認証シーケンスを作成して、1 つ以上の認証サーバを使用してネットワークのクライアントを認証するように Web セキュリティ アプライアンスを設定できます。複数の認証サーバを使用する場合のアプライアンスの動作の詳細については、「認証レルムが複数の場合のアプライアンスの動作」（P.20-17）を参照してください。

認証レルムと、必要に応じて認証シーケンスも作成した後、認証レルムまたは認証シーケンスに基づいてアイデンティティを作成または編集できます。ただし、認証レルムまたは認証シーケンスを削除した場合は、その認証レルムまたは認証シーケンスに依存する ID グループはすべてディセーブルになります。認証とアイデンティティの併用の詳細については、「認証が ID グループに影響を与える仕組みについて」（P.8-5）を参照してください。

クライアント アプリケーションのサポート

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、トランザクションに認証が必要な場合は、Web プロキシが、認証クレデンシャルを要求しているクライアント アプリケーションに応答します。ただし、一部のクライアントは認証をサポートしておらず、これらのクライアントには、ユーザ名とパスワードの入力をユーザに求める方法がありません。これらのアプリケーションは、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は使用できません。

次のリストに、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は機能しないアプリケーションの例を示します。

- 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

（注）　ユーザが、これらのクライアント アプリケーションのいずれかを使用して特定の URL にアクセスする必要がある場合は、認証が必要でないカスタム URL カテゴリに基づいてアイデンティティを作成し、認証を必要とする他のすべてのアイデンティティより上に配置します。これを行うと、クライアント アプリケーションに認証が求められません。

アップストリーム プロキシ サーバの使用

Web セキュリティ アプライアンスをアップストリーム プロキシ サーバに接続できます。アップストリーム プロキシ サーバは、別の Web セキュリティ アプライアンスまたはサードパーティのプロキシである場合もあります。Web セキュリティ アプライアンスがアップストリーム プロキシ サーバに接続されている場合、認証を有効にすることができるかどうかは、認証タイプによって異なります。

- **NTLMSSP：**ユーザの認証に NTLMSPP 認証を使用している場合は、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 サーバのいずれかでのみ認証を有効にする必要があります。両方では有効にしないでください。シスコでは、Web セキュリティ アプライアンスを設定して認証を使用することを推奨しています。これにより、ユーザ認証に基づいてポリシーを作成できます。

  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 による認証を使用すると、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要求の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。

- **基本：**ユーザの認証に基本認証を使用する場合は、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、またはアプライアンスとアップストリーム プロキシ サーバの両方で認証を有効にすることができます。ただし、Web セキュリティ アプライアンスとアップストリーム プロキシ サーバの両方が基本認証を使用する場合は、ダウンストリーム Web セキュリティ アプライアンスでクレデンシャル暗号化機能をイネーブルにしないでください。クレデンシャル暗号化がダウンストリーム アプライアンスでイネーブルである場合は、クライアント要求が失敗します。これは、Web プロキシがクライアントから「Authorization」HTTP ヘッダーを受信するが、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です。

ユーザの認証

ユーザが Web セキュリティ アプライアンス経由で Web にアクセスすると、ユーザ名とパスワードを入力するプロンプトが表示される場合があります。Web プロキシは、設定されたアイデンティティおよびアクセス ポリシー グループに応じて、一部のユーザに認証クレデンシャルを要求します。ユーザは、組織の認証サーバによって認識されたクレデンシャルのユーザ名とパスワードを入力する必要があります。

Web プロキシが NTLM 認証レルムで NTLMSPP 認証を使用する場合、シングル サイン オンが適切に設定されていれば、ユーザは通常、ユーザ名とパスワードの入力を求められません。ただし、認証を求められた場合、ユーザは、ユーザ名の前に自分の Windows ドメイン名を入力する必要があります。たとえば、jsmith というユーザが、MyDomain という Windows ドメインに属する場合は、ユーザ名のフィールドに次のテキストを入力する必要があります。

```
MyDomain\jsmith
```

ただし、Web プロキシが NTLM 認証レルムに基本認証を使用する場合は、Windows ドメインの入力を省略できます。ユーザが Windows ドメインを入力しない場合は、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。

（注） Web プロキシが LDAP 認証レルムで認証を使用する場合は、ユーザは Windows ドメイン名を入力しないようにしてください。

認証の失敗への対処

ユーザが、認証に失敗したために Web からブロックされる場合があります。次のリストでは、認証失敗の原因と、実行できる修正アクションを説明しています。

- **クライアント アプリケーションが認証を実行できない。**一部のクライアントが認証を実行できないか、必要なタイプの認証を実行できません。クライアント アプリケーションが原因で認証に失敗した場合は、ユーザ エージェントに基づいてアイデンティティ ポリシーを定義し、認証の要求

から除外することができます。または、カスタム URL カテゴリに基づいてアイデンティティ ポリシーを定義し、特定の URL へのアクセス時に、すべてのクライアントを認証の要求から除外することができます。

- **認証サーバを使用できない。**ネットワーク接続が切断された場合、またはサーバに問題が発生している場合は、認証サーバを利用できない可能性があります。この問題を回避するには、「Action if Authentication Service Unavailable」グローバル認証設定を指定します。詳細については、「「グローバル認証設定の指定」（P.20-19）」を参照してください。
- **クレデンシャルが無効である。**クライアントが無効な認証クレデンシャルを渡すと、Web プロキシは、有効なクレデンシャルを要求し続け、デフォルトで Web へのアクセスを実質的にブロックします。しかし、認証に失敗したユーザには、制限付きアクセスを許可できます。詳細については、「「認証に失敗したユーザへのゲスト アクセスの許可」（P.8-10）」を参照してください。

（注）　認証されたユーザが、URL フィルタリングによる制限により Web サイトからブロックされている場合、または複数のマシンに同時にログインできない場合は、認証を再度要求するように Web プロキシを設定できます。これを行うには、「Enable Re-Authentication Prompt If End User Blocked by URL Category or User Session Restriction」グローバル認証設定をイネーブルにします。詳細については、「「ユーザに対する再認証の許可」（P.20-27）」を参照してください。

Windows 7 および Windows Vista の使用

Windows 7 および Windows Vista のマシンには、ネットワーク接続状態インジケータ（NCSI）という機能があります。ネットワーク上のクライアントが NCSI を使用し、Web セキュリティ アプライアンスが NTLMSPP 認証を使用する場合は、比較的小さいタイムアウト値をマシン クレデンシャルで使用するように、アプライアンスを設定する必要があります。これを行うには、`advancedproxyconfig > authentication` CLI コマンドを使用します。

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。

NCSI が Windows マシンで実行しているときは、HTTP 要求を実行してネットワーク接続をチェックします。NCSI を実行しているマシンが認証を求められた場合（要求には、認証を必要とするアイデンティティ ポリシーが割り当てられます）、NCSI は、ユーザのクレデンシャルの代わりにマシンのクレデンシャルを使用して認証します。

アイデンティティ ポリシーが IP ベースのサロゲートを使用する場合は、ユーザ自身のクレデンシャルの代わりにマシンのクレデンシャルを使用して識別されるため、ユーザからの以降の要求に、誤ったポリシーが割り当てられる可能性があります。

CLI コマンド `advancedproxyconfig > authentication` を使用すると、認証を再度要求する前に、IP アドレスのサロゲートをマシン クレデンシャルに使用する期間を指定するできます。Web プロキシは、ユーザ クレデンシャルとマシン クレデンシャルを区別します。

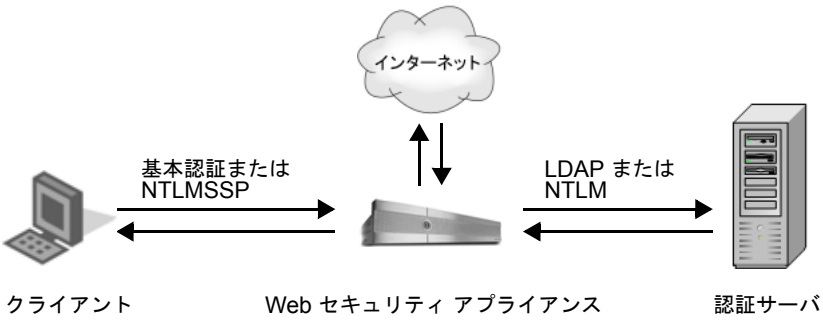
認証の機能

Web にアクセスするユーザを認証するために、Web セキュリティ アプライアンスは外部認証サーバに接続します。認証サーバには、ユーザとそれに対応するパスワードのリストが含まれ、ユーザは階層構造で整理されています。ネットワークのユーザが正常に認証されるためには、有効な認証クレデンシャル（認証サーバに保存されているユーザ名およびパスワード）をユーザが提供する必要があります。

ユーザが、認証を必要とする Web セキュリティ アプライアンス経由で Web にアクセスすると、Web プロキシはクライアントに認証クレデンシャルを要求します。Web プロキシは、クライアントと認証サーバの両方と通信して、ユーザを認証し、要求を処理します。

図 20-1 は、Web セキュリティ アプライアンスがクライアントおよび認証サーバと通信する方法を示します。

図 20-1　Web セキュリティ アプライアンスの認証



Web セキュリティ アプライアンスは、次の認証プロトコルをサポートしています。

- **Lightweight Directory Access Protocol（LDAP）。**Web プロキシは、LDAP バインド操作を使用して、LDAP 互換認証サーバに照会します。アプライアンスは、標準の LDAP サーバ認証とセキュア LDAP 認証をサポートしています。

  LDAP 設定オプションの詳細については、「LDAP 認証」（P.20-31）を参照してください。

- **NT LAN Manager（NTLM）。**Web プロキシは、Microsoft 独自のプロトコルである NTLM を使用して、Microsoft Active Directory に存在するユーザを認証します。NTLM プロトコルでは、クライアントと Active Directory サーバ間でメッセージのチャレンジ/レスポンス シーケンスを使用します。クライアント側では、NTLMSSP 認証方式または基本認証方式を使用できます。

  NTLM 設定オプションの詳細については、「NTLM 認証」（P.20-33）を参照してください。

上記のプロトコルに加え、Web セキュリティ アプライアンスは、次のクライアント側認証方式をサポートしています。

- **基本。**クライアント アプリケーションが、要求時に、ユーザ名およびパスワードの形式で認証クレデンシャルを提供できます。LDAP サーバまたは Active Directory サーバで基本認証方式を使用できます。
- **NTLMSSP。**クライアント アプリケーションが、チャレンジとレスポンスの形式で認証情報を提供できます。NTLM プロトコルでネットワーク リソースにアクセスするクライアントが、バイナリ メッセージ形式を使用して認証されます。NTLMSPP 認証方式は、Active Directory サーバでのみ使用できます。Web プロキシが NTLMSSP を使用する場合は、ほとんどのクライアント アプリケーションで認証に Windows ログイン クレデンシャルを使用できるため、ユーザが自分のクレデンシャルを再入力する必要はありません。これは「シングル サインオン」と呼ばれます。

詳細については、「「基本認証方式と NTLMSPP 認証方式」（P.20-6）」を参照してください。

表 20-1 では、Web セキュリティ アプライアンスとクライアントの間、および Web セキュリティ アプライアンスと認証サーバの間で設定できるさまざまな認証シナリオについて説明しています。

表 20-1　Web セキュリティ アプライアンスの認証シナリオ

クライアントから Web セキュリティ アプライアンスへ	Web セキュリティ アプライアンスから認証サーバへ	認証サーバ タイプ
基本	LDAP	LDAP サーバ
基本	LDAP	LDAP を使用する Active Directory サーバ

表 20-1　Web セキュリティ アプライアンスの認証シナリオ （続き）

クライアントから Web セキュリティ アプライアンスへ	Web セキュリティ アプライアンスから認証サーバへ	認証サーバ タイプ
基本	NTLM	NTLM を使用する Active Directory サーバ
NTLMSSP	NTLM	NTLM を使用する Active Directory サーバ

また、Web プロキシの展開も、表 20-1 に記載された各シナリオで認証が機能する仕組みに影響します。詳細については、「Web プロキシの展開が認証に及ぼす影響」（P.20-7）」を参照してください。

基本認証方式と NTLMSPP 認証方式

ID グループを設定して認証を使用する場合は、基本認証方式または NTLMSSP 認証方式を選択します。認証方式は、ユーザ エクスペリエンスと、ユーザのパスワードのセキュリティに影響します。

表 20-2 では、基本認証方式と NTLMSPP 認証方式の違いについて説明しています。

表 20-2　基本認証方式と NTLMSPP 認証方式

認証方式	ユーザ エクスペリエンス	セキュリティ
基本	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、入力したクレデンシャルを記憶するかどうかを尋ね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 アプライアンスの間でのパケット キャプチャにより、ユーザ名とパスワードが開示されます。 **注：**保護された認証クレデンシャルをクライアントが送信するように、Web セキュリティ アプライアンスを設定できます。詳細については、「認証クレデンシャルのセキュアな送信」（P.20-25）」を参照してください。
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、次の状況では、クライアントが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）で*保護され*て送信されます。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。 3 ウェイ ハンドシェイクの詳細については、「明示的な転送展開、NTLM 認証」（P.20-9）を参照してください。

Web プロキシの展開が認証に及ぼす影響

Web プロキシは、Web プロキシの展開と認証プロトコルのタイプに応じて、異なる方法でクライアントおよび認証サーバと通信します。

表 20-3 は、さまざまな認証プロトコルおよび展開のタイプで考えられる認証方式のリストです。

表 20-3　認証方式

Web プロキシの展開	クライアントから Web セキュリティ アプライアンスへ	Web セキュリティ アプライアンスから認証サーバへ
明示的な転送	基本	LDAP または NTLM の基本
トランスペアレント	基本	LDAP または NTLM の基本
明示的な転送	NTLM	NTLMSSP
トランスペアレント	NTLM	NTLMSSP

ここでは、これらの認証方式を、さらに詳しく説明します。

明示的な転送展開、基本認証

クライアントが Web ページ要求を、明示的な転送モードで展開された Web セキュリティ アプライアンスに明示的に送信する場合、Web プロキシは 407 HTTP 応答「Proxy Authentication Required」でクライアントに応答できます。このステータスは、Web リソースにアクセスするには、有効な認証クレデンシャルの入力が必要であることをクライアントに通知します。

認証プロセスは、次の手順で構成されます。

1. クライアントが、Web ページへの接続要求を Web プロキシに送信します。
2. Web プロキシが 407 HTTP 応答「Proxy Authentication Required」で応答します。
3. ユーザがクレデンシャルを入力し、クライアント アプリケーションが、Base64 で（暗号化なし）で符号化されたクレデンシャルを含む「Proxy-Authorization」HTTP ヘッダーを持つ元の要求を再送信します。
4. Web プロキシがクレデンシャルを確認し、要求された Web ページを返します。

表 20-4 は、明示的な転送基本認証を使用した場合のメリットとデメリットを示します。

表 20-4　明示的な転送基本認証の利点と欠点

利点	欠点
• RFC ベース • 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 • 最小限のオーバーヘッド • HTTPS（CONNECT）要求で使用できる	• すべての要求でクリア テキスト（Base64）としてパスワードが送信される • シングル サインオンなし

トランスペアレント展開、基本認証

407 HTTP 応答「Proxy Authentication Required」が許可されるのは、プロキシ サーバからの場合のみです。ただし、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、その存在を、ネットワークのクライアント アプリケーションが認識できません。したがって、Web プロキシは 407 応答を返すことができません。

この問題に対処するために、認証プロセスが次の手順で実行されます。

1. クライアントが Web ページに要求を送信し、Web プロキシが透過的に代行受信します。
2. Web プロキシが HTTP 307 応答を使用して、ローカル Web サーバとしてマスカレードする Web プロキシにクライアントをリダイレクトします。

（注）　このトランザクションは、「TCP_DENIED/307」としてアクセス ログに記録されます。

3. クライアントが、リダイレクトされた URL に要求を送信します。
4. Web プロキシが 401 HTTP 応答「Authorization required」を送信します。
5. ユーザにクレデンシャルの入力が求められ、ユーザが入力します。
6. クライアントが要求を再度送信しますが、このときは、クレデンシャルが「Authorization」HTTP ヘッダーに含まれます。
7. Web プロキシがクレデンシャルを確認し、IP アドレス別に、または Cookie を使用してユーザを追跡してから、最初に要求されたサーバにクライアントをリダイレクトします。

（注）　IP アドレスまたは Cookie を使用して、認証されたユーザを追跡するように、Web プロキシを設定できます。

8. クライアントが最初の Web ページを再度要求した場合は、Web プロキシが、要求を透過的に代行受信し、IP アドレスまたは Cookie でユーザを確認し、要求されたページを返します。

（注）　クライアントが別の Web ページを要求し、Web プロキシが IP アドレスでユーザを追跡した場合は、Web プロキシが IP アドレスでユーザを確認し、要求されたページを返します。

表 20-5 は、トランスペアレント基本認証と、IP ベースのクレデンシャルのキャッシュを使用する利点と欠点のリストです。

表 20-5　トランスペアレント基本認証と IP キャッシュの利点と欠点

利点	欠点
• すべての主要なブラウザで使用できる • 認証をサポートしないユーザ 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 • 比較的低いオーバーヘッド • 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	• 認証クレデンシャルが、ユーザではなく、IP アドレスに関連づけられる（Citrix および RDP 環境で、またはユーザが IP アドレスを変更した場合は使用できない） • 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

表 20-6 は、トランスペアレント基本認証と、Cookie ベースのクレデンシャルのキャッシュを使用する利点と欠点のリストです。

表 20-6　トランスペアレント基本認証と Cookie キャッシュの利点と欠点

利点	欠点
• すべての主要な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	• Cookie はドメイン固有であるため、新規の各 Web ドメインには認証プロセス全体が必要 • Cookie がイネーブルであることが必要 • 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

明示的な転送展開、NTLM 認証

Web プロキシは、サード パーティのチャレンジ/レスポンス システムを使用して、ネットワークのユーザを認証します。

認証プロセスは、次の手順で構成されます。

1. クライアントが、Web ページへの接続要求を Web プロキシに送信します。
2. Web プロキシが 407 HTTP 応答「Proxy Authentication Required」で応答します。
3. クライアントが要求を繰り返し、NTLM「ネゴシエート」メッセージに「Proxy-Authorization」HTTP ヘッダーを含めます。
4. Web プロキシが 407 HTTP 応答と、クライアントからのネゴシエート メッセージに基づく NTLM「チャレンジ」メッセージで応答します。
5. クライアントが要求を繰り返し、チャレンジ メッセージへの応答を含めます。

（注） クライアントが、パスワードに基づくアルゴリズムを使用してチャレンジを変更し、Web プロキシへのチャレンジ応答を送信します。

6. Web プロキシが Active Directory サーバに認証情報を渡します。その後、Active Directory サーバが、チャレンジ文字列を正しく変更されたかどうかに基づいて、クライアントが正しいパスワードを入力したことを確認します。
7. チャレンジ応答が成功すると、Web プロキシが、要求された Web ページを返します。

（注） *同じ TCP 接続でのその他の要求は、Active Directory サーバによって再度認証される必要はありません。*

表 20-7 は、明示的な転送 NTLM 認証を使用した場合のメリットとデメリットを示します。

表 20-7　明示的な転送 NTLM 認証の利点と欠点

利点	欠点
• 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は、Active Directory 環境での真のシングル サインオンを実現	• 中程度のオーバーヘッド：新しい各接続に再認証が必要 • 主に Windows のみ、および主要なブラウザのみでサポート

トランスペアレント展開、NTLM 認証

トランスペアレント NTLM 認証は、トランスペアレント基本認証に似ていますが、Web プロキシが、基本の代わりに NTLMSSP を使用してクライアントと通信します。ただし、トランスペアレント NTLM 認証では、認証クレデンシャルがクリア テキストとして認証サーバに送信されません。

詳細については、「「トランスペアレント展開、基本認証」（P.20-8）」を参照してください。

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じです。ただし、パスワードが認証サーバに送信されず、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るという点で、トランスペアレント NTLM 認証の方が優れています。トランスペアレント基本認証の利点と欠点の詳細については、表 20-5（P.20-8）表 20-6（P.20-9）を参照してください。

認証レルム

認証レルムは、特定の設定による単一の認証プロトコルをサポートする一連の認証サーバ（または単一のサーバ）です。

認証の設定時には、次の作業を行うことができます。

- レルムに 3 つまでの認証サーバを含める。
- 0 個以上の LDAP レルムを作成する。
- 0 ～ 10 個の NTLM のレルムを作成する。
- 複数のレルムに認証サーバを含める。
- 認証シーケンスに 1 個以上のレルムを含める。
- 異なるプロトコルのレルムを単一の認証シーケンスに含める。ただし、1 つの NTLM レルムだけがシーケンスで NTLMSSP を使用できる。
- レルムまたはシーケンスを ID グループに割り当てる。

認証レルムは、[ネットワーク（Network）] > [認証（Authentication）] ページの [認証レルム（Authentication Realms）] セクションで作成、編集、および削除を行います。

複数のレルムを作成すると、それらを認証シーケンスとして並べることができます。詳細については、「「認証シーケンスの使用」（P.20-15）」を参照してください。

LDAP 認証レルムの追加

ステップ 1　[ネットワーク（Network）] > [認証（Authentication）] に移動します。

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　認証レルムに名前を付けます。

すべてのシーケンス名とレルム名は一意であり、英数字またはスペースのみを含んでいる必要があります。また、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が、各アプライアンスで定義されているものと同じプロパティを持つことを確認します。

ステップ 4　[認証プロトコルとスキーマ（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 パージョン（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 では、LDAP バージョン 3 が必要です。 この LDAP サーバがトランスペアレント ユーザ ID で使用する Novell eDirectory をサポートするかどうかを選択します。
LDAP サーバ（LDAP Server）	LDAP サーバの IP アドレスまたはホスト名、およびポート番号を入力します。最大 3 台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。たとえば、「ldap.example.com」のように指定します。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、ここに、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てください。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、ユーザを認証する必要があるのはローカル ドメイン コントローラのみであることがわかっている場合は、ローカル ドメイン コントローラを使用する場合があります。 **注：**複数の認証サーバをレルムで設定した場合、アプライアンスは、最大 3 台の認証サーバで認可しようとした後、そのレルム内のトランザクションの認証に失敗します。

設定	説明
LDAP 永続的接続（LDAP Persistent Connections） （[詳細（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。接続が使用できない場合は、新しい接続が開かれます。 • **[永続的接続の使用（Use persistent connections）]。**既存の接続を使用して、指定された数の要求に使用します。最大値に到達すると、LDAP サーバへの新しい接続を確立します。 • **[永続的接続を使用しない（Do not use persistent connections）]。**必ず、LDAP サーバへの新しい接続を作成します。
ユーザ認証：（User Authentication）	次のフィールドの値を入力します。 **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で、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` という形式の 1 つ以上のコンポーネントで構成されます。たとえば、「`dc=companyname, dc=com`」のように入力します。 **ユーザ名属性（User Name Attribute）** 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 ディレクトリで一意の ID。 • **[custom]。**「`UserAccount`」などのカスタム ID。 **ユーザ フィルタのクエリー（User Filter Query）** ユーザのフィルタのクエリーは、ユーザのベース DN を見つける LDAP 検索フィルタです。これは、ユーザ ディレクトリがベース DN の下の階層にある場合、またはそのユーザのベース DN のユーザ固有コンポーネントにログイン名が含まれていない場合に必要です。 次の値のいずれかを選択します。 • **[none]。**すべてのユーザを抽出します。 • **[custom]。**ユーザの特定のグループを抽出します。

設定	説明
クエリー クレデンシャル（Query Credentials）	認証サーバが匿名クエリーを受け入れるかどうかを選択します。 認証サーバが匿名クエリーを受け入れる場合は、[サーバは、匿名の質問に対応します（Server Accepts Anonymous Queries）] を選択します。 認証サーバが匿名クエリーを受け入れない場合は、[バインド DN を使用（Use Bind DN）] を選択し、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ている必要があります。 • **[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のリストです。 cn=administrator,cn=Users,dc=domain,dc=com sAMAccountName=jdoe,cn=Users,dc=domain,dc=com. Active Directory サーバを LDAP サーバとして使用している場合は、「DOMAIN\username」というバインド DN ユーザ名を入力することもできます。
グループ認証（Group Authorization）	LDAP グループの認可をイネーブルにするかどうかを選択します。LDAP グループの認可をイネーブルにすると、グループ オブジェクトまたはユーザ オブジェクト別にユーザをグループ化できます。

ステップ 6　[テスト開始（Start Test）] をクリックします。

ステップ 7　変更を送信し、保存します。

関連トピック

- 「ユーザの透過的識別」（P.8-12）
- 「LDAP グループの認可」（P.20-31）
- 「認証レルムのテスト」（P.20-18）。

NTLM 認証レルムの追加

はじめる前に

- Web セキュリティ アプライアンス で読み取られた現在時刻と、Active Directory サーバで読み取られた現在時刻を比較します。その差が、Active Directory サーバの「Maximum tolerance for computer clock synchronization」オプションで指定された時間を超えていないことを確認します。ネットワーク タイム プロトコル（NTP）を使用して、Web セキュリティ アプライアンスの現在時刻を指定する場合、デフォルトのタイム サーバは time.ironport.com です。
- ネットワークが NetBIOS を使用する場合は、`setntlmsecuritymode` CLI コマンドを使用して、NTLM セキュリティ モードが「domain」に設定されていることを確認します。そうしないと、NetBIOS ドメイン名を提供できません。

- Active Directory エージェントを使用してトランスペアレント ユーザ ID を設定する場合は、Active Directory サーバにアクセスできる、少なくとも 1 台のコンピュータに Active Directory エージェントがインストールされていることを確認します。

ステップ 1　[ネットワーク（Network）] > [認証（Authentication）] に移動します。

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　認証レルムに名前を付けます。

すべてのシーケンス名とレルム名は一意であり、英数字またはスペースのみを含んでいる必要があります。また、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が、各アプライアンスで定義されているものと同じプロパティを持つことを確認します。

ステップ 4　[認証プロトコルとスキーマ（Authentication Protocol and Scheme(s)）] フィールドで [NTLM] 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。

複数の認証サーバをレルムで設定した場合、アプライアンスは、最大 3 台の認証サーバで認可しようとした後、そのレルム内のトランザクションの認証に失敗します。

ステップ 6　アプライアンスをドメインに結合します。

a.　Active Directory アカウントを、次のように設定します。

設定	説明
Active Directory のドメイン（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）	ネットワークが 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）	Active Directory ドメイン内の場所を指定します。ここで、AsyncOS が Active Directory のコンピュータ アカウント（「マシン信頼アカウント」とも呼ばれます）を作成し、ドメイン上でコンピュータを一意的に識別します。 Active Directory 環境で、コンピュータ オブジェクトが特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たコンテナ内に、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.　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使用されるだけで、保存されません。

自分のコンピュータにログインするときにユーザが自分の sAMAccountName ユーザ名を入力したことを確認します。

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）トランスペアレント ユーザ ID を設定します。

設定	説明
Active Directory エージェントを使用した透過的ユーザ識別を有効にする（Enable Transparent User Identification using Active Directory agent）	プライマリ Active 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 Active 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　[テスト開始（Start Test）] をクリックします。

ステップ 10　変更を送信し、保存します。

関連項目

- 「ユーザの透過的識別」（P.8-12）。
- 「認証レルムのテスト」（P.20-18）

認証レルムの削除

レルムを削除すると、Web セキュリティ アプライアンスは自動的に、そのレルムを使用したシーケンスからそのレルムを削除します。また、削除されたレルムに依存するアイデンティティ ポリシー グループはすべてディセーブルになります。

ステップ 1　[ネットワーク（Network）] > [認証（Authentication）] ページで、レルム名に対応するゴミ箱のアイコンをクリックします。

ステップ 2　[削除（Delete）] をクリックして、レルムを削除することを確認します。

ステップ 3　変更を保存します。

認証シーケンスの使用

複数のレルムを作成すると、レルムをグループ化して認証シーケンスにすることができます。認証シーケンスは認証レルムのグループで、クライアントを認証するために Web セキュリティ アプライアンスが使用する順に並べられています。

認証シーケンスの設定時には、次の作業を行うことができます。

- 複数の認証シーケンスを作成する。
- 認証シーケンスに 1 個以上のレルムを含める。
- 異なるプロトコルのレルムを単一の認証シーケンスに含める。
- レルムまたはシーケンスを ID グループに割り当てる。

認証シーケンスは、[ネットワーク（Network）] > [認証（Authentication）] ページの [レルム シーケンス（Realm Sequences）] セクションで作成します。[レルム シーケンス（Realm Sequences）] セクションは、複数のレルムを作成するときにだけ表示されます。

2 番めのレルムを作成した後、自動的に [レルム シーケンス（Realm Sequences）] セクションが表示され、「All Realms」という名前のデフォルトの認証シーケンスが含まれています。[すべてのレルム（All Realms）] シーケンスには自動的に、ユーザが定義する各レルムが含まれます。[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、レルムを削除することはできません。[すべてのレルム（All Realms）] シーケンスは削除できません。

（注） 複数の NTLM 認証レルムを定義すると、AsyncOS は、どのシーケンスにも 1 つの NTLM 認証レルムを含む NTLMSSP のみを使用します。[すべてのレルム（All Realms）] シーケンスを含め、すべてのシーケンスの NTLMSSP に使用する NTLM 認証レルムを選択できます。複数の NTLM レルムで NTLMSSP を使用するには、各レルムに対して個別のアイデンティティを定義します。

認証シーケンスの作成

複数の認証レルムを定義すると、認証シーケンスを作成できます。

ステップ 1　[ネットワーク（Network）] > [認証（Authentication）] ページで [シーケンスを追加（Add Sequence）] をクリックします。

ステップ 2　[レルム シーケンス（Name for Realm Sequence）] フィールドにシーケンス名を入力します。

（注） すべてのシーケンス名とレルム名は一意であり、英数字またはスペースのみを含んでいる必要があります。また、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が、各アプライアンスで定義されているものと同じプロパティを持つことを確認します。

ステップ 3　[基本スキームのレルム シーケンス（Realm Sequence for Basic Scheme）] エリアの最初の行で、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 4　[基本スキームのレルム シーケンス（Realm Sequence for Basic Scheme）] エリアの 2 番めの行で、シーケンスに含める次のレルムを選択します。

ステップ 5　（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、[行を追加（Add Row）] をクリックします。

（注） その行のゴミ箱のアイコンをクリックすると、シーケンスからレルムを削除できます。

ステップ 6　NTLM realm を定義した後は、[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 7　変更を送信し、保存します。

認証シーケンスの削除

認証シーケンスを削除すると、削除したシーケンスに依存するアクセス ポリシー グループはすべてディセーブルになります。

ステップ 1　[ネットワーク（Network）] > [認証（Authentication）] ページで、シーケンス名に対応するゴミ箱のアイコンをクリックします。

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

ステップ 3　変更を保存します。

認証レルムが複数の場合のアプライアンスの動作

複数の認証サーバや、認証プロトコルの異なる複数の認証サーバに対してクライアントを認証するように、Web セキュリティ アプライアンスを設定できます。複数の認証サーバに対して認証するようにアプライアンスを設定した場合も、クライアントにクレデンシャルが要求されるのは 1 回だけです。これは、異なるプロトコルに対して認証するようにアプライアンスを設定した場合にも当てはまります。

組織が、同じまたは異なる認証プロトコルを使用する認証サーバを持つ他の組織を買収した場合は、異なるレルムに対して認証するように ID グループを設定できます こうすると、すべてのユーザ用の 1 つの ID グループを作成し、このグループに、各認証サーバのレルムを含む認証シーケンスを割り当てることができます。

複数のレルムを含む認証シーケンスを ID グループに割り当てて、クライアントが Web 要求を送信すると、アプライアンスは次のアクションを実行します。

1. アプライアンスがクライアントからクレデンシャルを取得します。
2. クライアントが NTLMSSP クレデンシャルを提供しており、シーケンスの [NTLMSSP スキームのレルム（Realm for NTLMSSP Scheme）] フィールドで NTLM レルムが選択されている場合は、アプライアンスが、指定された NTLM レルムで定義された認証サーバに対してクライアントを認証しようとします。
3. クライアントが基本クレデンシャルを提供した場合は、アプライアンスが、[基本スキームのレルム シーケンス（Realm Sequence for Basic Scheme）] セクションの最初のレルムで定義された認証サーバに対してクライアントを認証しようとします。
4. 基本クライアント クレデンシャルが、最初の基本レルムで定義されているサーバのユーザに一致しない場合は、シーケンスの次の基本レルムの認証サーバに対して認証しようとします。
5. アプライアンスは、認証が成功するか、認証レルムがなくなるまで、次の基本レルムのサーバに対してクライアントを認証しようとし続けます。
6. 認証が成功すると、アプライアンスはアクセス ポリシーを割り当てて、サーバの応答をクライアントに渡します。
7. アプライアンスが、シーケンス内のすべての認証レルムに対してクライアントを認証できない場合は、クライアントが宛先サーバへの接続を許可されません。代わりに、クライアントにエラー メッセージが表示されます。

ヒント　最適なパフォーマンスを得るには、1 つのレルムで認証されるように、サブネット上のクライアントを設定してください。

認証レルムのテスト

認証の設定をテストすると、Web セキュリティ アプライアンスは最初に、ユーザがレルムに入力した設定が有効な形式であることを確認します。たとえば、文字列が必要なフィールドに、現在は数値が含まれている場合は、そのエラーが通知されます。

すべてのフィールドに有効な値が含まれる場合、アプライアンスは、認証プロトコルに応じて異なる手順を実行します。複数の認証サーバがレルムに含まれる場合、アプライアンスは、各サーバに順番にテスト プロセスを実行します。

アプライアンスは、レルム内のすべてのサーバをテストし、サーバごとに、できるだけ多くのエラーを特定します。レルム内の各サーバのテスト結果が報告されます。

LDAP テスト

アプライアンスは、LDAP 認証の設定をテストする場合に、次の手順を実行します。

1. LDAP サーバが、指定された LDAP ポートで確実にリッスンしているようにします。
2. セキュア LDAP を選択した場合は、LDAP サーバが確実にセキュア LDAP をサポートするようにします。
3. 指定したベース DN、ユーザ名属性、ユーザ フィルタ クエリーを使用して LDAP クエリーを実行します。
4. レルムにバインド パラメータが含まれる場合は、バインド パラメータで LDAP クエリーを作成して検証します。
5. グループ認可が指定されている場合は、サーバからグループを取得して、指定したグループ属性が有効であることを保証します。

NTLM テスト

アプライアンスは、NTLM 認証の設定をテストする場合に、次の手順を実行します。

1. 指定した Active Directory サーバが到達可能であることを保証し、クエリーに応答します。
2. Active Directory ドメインの DNS ルックアップが確実に成功するようにします。これは、Active Directory ドメインが WINS ドメイン名ではなく、DNS ドメイン名である必要があるためです。
3. アプライアンスのシステム時刻と Active Directory サーバのシステム時刻の差が 3 分以内であるようにします。
4. Kerberos チケットを生成して、ユーザ クレデンシャルを検証します。
5. Active Directory ドメインに Web セキュリティ アプライアンスを追加するための適切な権限がユーザにあるかどうかを検証します。

6. ドメイン内のグループを取得できるかどうかを検証します。

グローバル認証設定の指定

一部の認証設定は、定義したどのレルムからも独立しています。たとえば、基本認証方式を使用している場合でも、クライアントが Web セキュリティ アプライアンスに認証クレデンシャルをセキュアな方法で送信するかどうかを設定できます。詳細については、「認証クレデンシャルのセキュアな送信」（P.20-25）」を参照してください。

（注）　指定できるグローバル認証設定は、Web プロキシの展開に応じて変わります。明示的な転送モードより、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、より詳細に設定できます。

ステップ 1　[ネットワーク（Network）] > [認証（Authentication）] ページで [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 2　[グローバル認証設定を編集（Global Authentication Settings）] セクションを、表 20-8 で定義されているように編集します。

表 20-8　グローバル認証設定

設定	説明
認証サービスが使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）]。**処理が、ユーザが認証されたかのように続行されます。 • **[ユーザ認証に失敗したら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）	ユーザに、アイデンティティ ポリシーのゲスト アクセスを許可する場合は、この設定により、Web プロキシがアクセス ログでユーザをゲストとして識別し、記録する方法が決定されます。 ユーザのゲスト アクセス許可の詳細については、「認証に失敗したユーザへのゲスト アクセスの許可」（P.8-10）を参照してください。

表 20-8　グローバル認証設定 （続き）

設定	説明
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）	この設定は、制限 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 URL フィルタリング ポリシーまたはユーザ セッションの制限が原因でブロックされた認証済みユーザだけに適用されます。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、「ユーザに対する再認証の許可」（P.20-27）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前に、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たディレクトリ グループが含まれます。 デフォルト値は、推奨された設定です。基本認証トークン TTL より大きい [Surrogate Timeout] 設定が指定されている場合は、サロゲート タイムアウト値が優先され、サロゲート タイムアウトの期限後に Web プロキシが認証サーバに連絡します。

設定できる残りの認証設定は、トランスペアレント モードと明示的な転送モードのどちらで Web プロキシが展開されているかにより異なります。

ステップ 3　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、表 20-9 にある設定を編集します。

表 20-9　トランスペアレント プロキシ モードの認証設定

設定	説明
クレデンシャルの暗号化（Credential Encryption）	この設定で、暗号化された HTTPS 接続経由でクライアントが 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、基本認証方式の場合に特に役立ちます。これは、ユーザのクレデンシャルがプレーン テキストで送信されるためです。 詳細については、「認証クレデンシャルのセキュアな送信」（P.20-25）を参照してください。
HTTPS リダイレクト ポート（HTTPS Redirect Port）	HTTPS 接続でユーザを認証するための要求のリダイレクトに使用する TCP ポートを指定します。 これは、どのポートで、クライアントが HTTPS を使用して Web プロキシへの接続を開始するかを指定します。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、SaaS アクセス コントロールの使用時に SaaS ユーザが認証を求められている場合に発生します。

表 20-9　トランスペアレント プロキシ モードの認証設定 （続き）

設定	説明
リダイレクト ホスト名（Redirect Hostname）	Web プロキシが着信接続をリッスンするネットワーク インターフェイスの短いホスト名を入力します。 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での認証を設定する場合は、Web プロキシが、ユーザを認証するためにクライアントに送信され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。**クライアントと Web セキュリティ アプライアンスが DNS 解決可能である 1 つの単語のホスト名を入力できます。これにより、ブラウザ側の設定なしで、クライアントが Internet Explorer での真のシングル 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、プロキシでルックアップを実行して、`proxy.mycompany.com` を解決できます。 • **完全修飾ドメイン名（FQDN）。**このフィールドに、FQDN または IP アドレスを入力することもできます。ただし、これを行って、Internet Explorer および Firefox での真のシングル サインオンを実現する場合は、FQDN または IP アドレスが、クライアント ブラウザでクライアントの信頼済みサイト リストに確実に追加されているように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）	この設定は、Web プロキシが、認証クレデンシャルをクライアントに再度要求する前に待機する時間を指定します。Web プロキシは、クレデンシャルを再度要求するまでは、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。 ブラウザなどのユーザ エージェントでは一般に、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をキャッシュします。
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 アドレスが認証サロゲートとして使用される場合は、この設定で、クライアントがアイドル状態のときに Web プロキシが認証クレデンシャルをクライアントに再度要求する前に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は、この設定には効果がなくなり、サロゲート タイムアウトへの到達後にクライアントは認証を求められます。 この設定を使用して、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下させることができます。

表 20-9　トランスペアレント プロキシ モードの認証設定 （続き）

設定	説明
クレデンシャル キャッシュ オプション:（Credential Cache Options:） キャッシュ サイズ（Cache Size）	認証キャッシュに保管され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が安全に使用できます。デフォルト値は、推奨された設定です。
ユーザ セッション制限（User Session Restrictions）	この設定は、認証されたユーザが複数の IP アドレスからインターネットに同時にアクセスすることを許可するかどうかを指定します。 1 台のマシンへのアクセスを制限して、ユーザが、認可されていないユーザと認証クレデンシャルを共有することを防止できます。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）] の設定を使用して、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ように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。この値で、ユーザが別の IP アドレスでマシンにログインできるまでに待機する必要がある時間が決定されます。制限タイムアウト値は、サロゲート タイムアウト値より大きい値である必要があります。 `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（Advanced）	クレデンシャルの暗号化または SaaS 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）と、ここでアップロードするデジタル証明書のどちらをアプライアンスが使用するかを選択できます。 デジタル証明書およびキーをアップロードするには、[ブラウズ（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。 詳細については、「クレデンシャルの暗号化と SaaS アクセス コントロールで使用する証明書およびキーのアップロード」（P.20-26）を参照してください。

ステップ 4　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、表 20-10 にある設定を編集します。

表 20-10　明示的な転送プロキシ モードの認証設定

設定	説明
クレデンシャルの暗号化（Credential Encryption）	この設定で、暗号化された HTTPS 接続経由でクライアントが 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有効にすると、認証のために Web プロキシにクライアントを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、基本認証方式の場合に特に役立ちます。これは、ユーザのクレデンシャルがプレーン テキストで送信されるためです。 詳細については、「認証クレデンシャルのセキュアな送信」（P.20-25）」を参照してください。
HTTPS リダイレクト ポート（HTTPS Redirect Port）	HTTPS 接続でユーザを認証するための要求のリダイレクトに使用する TCP ポートを指定します。 これは、どのポートで、クライアントが HTTPS を使用して Web プロキシへの接続を開始するかを指定します。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、SaaS アクセス コントロールの使用時に SaaS ユーザが認証を求められてい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。 上記の認証モードをイネーブルにすると、Web プロキシは、ユーザを認証するためにクライアントに送信され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。**クライアントと Web セキュリティ アプライアンスが DNS 解決可能である 1 つの単語のホスト名を入力できます。これにより、ブラウザ側の設定なしで、クライアントが Internet Explorer での真のシングル 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、プロキシでルックアップを実行して、`proxy.mycompany.com` を解決できます。 • **完全修飾ドメイン名（FQDN）。**このフィールドに、FQDN または IP アドレスを入力することもできます。ただし、これを行って、Internet Explorer および Firefox での真のシングル サインオンを実現する場合は、FQDN または IP アドレスが、クライアント ブラウザでクライアントの信頼済みサイト リストに確実に追加されているように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。

表 20-10　明示的な転送プロキシ モードの認証設定 （続き）

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）	この設定は、Web プロキシが、認証クレデンシャルをクライアントに再度要求する前に待機する時間を指定します。Web プロキシは、クレデンシャルを再度要求するまでは、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。 ブラウザなどのユーザ エージェントでは一般に、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をキャッシュします。
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 アドレスが認証サロゲートとして使用される場合は、この設定で、クライアントがアイドル状態のときに Web プロキシが認証クレデンシャルをクライアントに再度要求する前に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は、この設定には効果がなくなり、サロゲート タイムアウトへの到達後にクライアントは認証を求められます。 この設定を使用して、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下させることができます。
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）	認証キャッシュに保管され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が安全に使用できます。デフォルト値は、推奨された設定です。

表 20-10　明示的な転送プロキシ モードの認証設定 （続き）

設定	説明
ユーザ セッション制限（User Session Restrictions）	この設定は、認証されたユーザが複数の IP アドレスからインターネットに同時にアクセスすることを許可するかどうかを指定します。 1 台のマシンへのアクセスを制限して、ユーザが、認可されていないユーザと認証クレデンシャルを共有することを防止できます。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）] の設定を使用して、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ように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。この値で、ユーザが別の IP アドレスでマシンにログインできるまでに待機する必要がある時間が決定されます。制限タイムアウト値は、サロゲート タイムアウト値より大きい値である必要があります。 `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（Advanced）	クレデンシャルの暗号化または SaaS 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）と、ここでアップロードするデジタル証明書のどちらをアプライアンスが使用するかを選択できます。 デジタル証明書およびキーをアップロードするには、[ブラウズ（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。 詳細については、「クレデンシャルの暗号化と SaaS アクセス コントロールで使用する証明書およびキーのアップロード」（P.20-26）」を参照してください。

ステップ 5　変更を送信し、保存します。

認証クレデンシャルのセキュアな送信

Web を使用してクライアントを識別するために認証を使用する場合は、クライアント アプリケーションが Web プロキシにクレデンシャルを送信し、Web プロキシがそれを認証サーバに渡します。クレデンシャルがクライアントから Web プロキシに渡される方法は、使用される認証方式によって異なります。

- **NTLMSSP。**クレデンシャルは常に、Web プロキシにセキュアな方法で渡されます。クレデンシャルは、Active Directory サーバで指定されたキーを使用して暗号化され、HTTP で送信されます。
- **基本。**デフォルトでは、クレデンシャルが Web プロキシに、セキュアでない方法で渡されます。符号化されていますが、暗号化されておらず、HTTP で送信されます。ただし、保護された認証クレデンシャルをクライアントが送信するように、Web セキュリティ アプライアンスを設定できます。これは、LDAP、および NTLM の両方の基本認証で機能します。

クレデンシャルの暗号化を基本認証で使用するようにアプライアンスを設定した場合は、Web プロキシがクライアントを Web プロキシ自身にリダイレクトしますが、このときは、HTTPS を使用した暗号化済み接続を使用します。クライアント アプリケーションは、アプライアンスへの要求の転送方法（明示的またはトランスペアレント）、およびクライアント アプリケーションで設定されている HTTPS 要求の転送方法（Web プロキシを使用するかどうか）に応じて、GET または CONNECT を要求します。

次に、セキュア HTTPS 接続を使用して、クライアントが認証クレデンシャルを送信します。アプライアンスはデフォルトで、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 接続を作成します。ほとんどのブラウザでは、証明書が無効であることがユーザに警告されます。無効な証明書のメッセージがユーザに表示されないようにするには、組織で使用する証明書とキーのペアをアップロードします。証明書とキーをアップロードする場合、秘密キーは*暗号化されていない*ことが必要です。証明書とキーのアップロードの詳細については、「クレデンシャルの暗号化と SaaS アクセス コントロールで使用する証明書およびキーのアップロード」（P.20-26）を参照してください。

クレデンシャルの暗号化を使用するようにアプライアンスを設定するには、グローバル認証設定の [クレデンシャルの暗号化（Credential Encryption）] 設定をイネーブルにします。詳細については、「「グローバル認証設定の指定」（P.20-19）」を参照してください。また `advancedproxyconfig > authentication` CLI コマンドを使用することもできます。詳細については、「「高度なプロキシ設定」（P.5-21）」を参照してください。

クレデンシャルの暗号化と SaaS アクセス コントロールで使用する証明書およびキーのアップロード

クレデンシャルの暗号化がイネーブルであるか、SaaS アクセス コントロールで使用する場合、アプライアンスはデジタル証明書を使用して、クライアント アプリケーションとの接続をセキュアに確立します。Web セキュリティ アプライアンスはデフォルトで、インストールされている「Cisco IronPort Web セキュリティ アプライアンス デモ証明書」を使用します。ただし、クライアント アプリケーションは、この証明書を認識するようにはプログラミングされていないため、アプリケーションが自動的に認識するデジタル証明書をアプライアンスにアップロードできます。

証明書およびキーをアップロードするには、[ネットワーク（Network）] > [認証（Authentication）] ページの [詳細（Advanced）] セクションを使用します。

アップロードする証明書と秘密キーのペアの取得の詳細については、「証明書の取得」（P.26-32）を参照してください。

（注）　[ネットワーク（Network）] > [認証（Authentication）] ページにアップロードする証明書とキーはすべて、クレデンシャルの暗号化のためのクライアントとのセキュアな接続の確立、および SaaS アクセス コントロールを使用した SaaS ユーザの認証にのみ使用されます。証明書およびキーは、Web セキュリティ アプライアンス Web インターフェイスへの接続時にセキュア HTTPS セッションを確立するためには使用されません。Web インターフェイスへの HTTPS 接続用の証明書とキーのペアのアップロードの詳細については、「サーバのデジタル証明書のインストール」（P.26-32）を参照してください。

SaaS アクセス コントロールの詳細については、「SaaS ユーザの認証」（P.15-2）を参照してください。

イネーブルのクレデンシャルの暗号化による HTTPS サイトと FTP サイトへのアクセス

クレデンシャルの暗号化は、Web プロキシが HTTPS 接続を使用して、認証のためにクライアントを Web プロキシ自身にリダイレクトしているため、機能します。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、クライアントが FTP over HTTPS 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は、Cookie を使用してユーザを追跡することはできません。

- **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 サイトの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。

このため、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。

（注）　認証は、クレデンシャルの暗号化がイネーブルで、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は、HTTPS 要求や FTP over HTTP 要求に対して機能しません。したがって、この設定で、HTTPS 要求と FTP over HTTP 要求が一致するのは、認証を必要としないアクセス ポリシーのみです。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。

ユーザに対する再認証の許可

AsyncOS for Web は、Web サイトにアクセスしようとしているユーザに応じて、さまざまなカテゴリの Web サイトにアクセスできないようにユーザをブロックできます。この場合、ユーザは正常に認証されますが、該当するアクセス ポリシーの設定済み URL フィルタリングにより、特定の Web サイトへのアクセスを許可されません。許可されなかった場合でも、認証されたユーザに Web にアクセスする機会を再度与えることができます。

（注）　再認証が許可されるのは、認証されたユーザのみです。認証されていないユーザには許可されません。

これは、複数のユーザが使用するが、デフォルトのアカウントがアクセスを制限されている共用ワークステーションで実行できます。ワークステーションのデフォルトのアカウントが、制限 URL フィルタリングにより Web サイトからブロックされている場合、ユーザは、権限がより強力な別の認証クレデンシャルを入力できます。

これを行うには、「Enable Re-Authentication Prompt If End User Blocked by URL Category or User Session Restriction」グローバル認証設定をイネーブルにします。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。Web プロキシは、該当する ID グループで定義された認証レルムに対してクレデンシャルを評価し、新しいクレデンシャルでより強力なアクセス権が付与される場合は、要求されたページがブラウザに表示されます。詳細については、「「グローバル認証設定の指定」（P.20-19）」を参照してください。

（注）　Web プロキシは、該当する ID グループで定義された認証レルムに対してのみ、新しいクレデンシャルを評価します。他のすべての ID グループに対しては比較しません。

より強力な権限のユーザが認証され、アクセスを許可されると、Web プロキシは、設定されている認証サロゲートに応じてさまざまな期間だけ、このような特権ユーザのアイデンティティをキャッシュします。

- **セッション Cookie。**特権ユーザのアイデンティティが、ブラウザを閉じるか、セッションがタイム アウトになるまで使用されます。
- **永続的な Cookie。**特権ユーザのアイデンティティが、サロゲートがタイムアウトするまで使用されます。
- **IP アドレス。**特権ユーザのアイデンティティが、サロゲートがタイムアウトするまで使用されます。
- **サロゲートなし。**デフォルトでは、Web プロキシが、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、Web プロキシが新しい*要求*ごとに認証を要求します。したがって、NTLMSSP を使用すると、認証サーバの負荷が増大します。ほとんどのブラウザは、特権ユーザのクレデンシャルをキャッシュし、ブラウザが閉じられるまで、ユーザに再入力を求めることなく認証します。Web プロキシがトランスペアレント モードで展開され、[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）] 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ません。

（注）　ユーザ定義のエンドユーザ通知ページで再認証を使用するには、リダイレクト URL を解析する CGI スクリプトが、Reauth_URL パラメータを解析して使用する必要があります。詳細については、「「エンド ユーザ通知ページをオフボックスに定義」（P.16-9）」を参照してください。

Internet Explorer での再認証の使用

再認証をイネーブルにし、クライアントが Microsoft Internet Explorer を使用する場合は、Internet Explorer で再認証が正常に機能するように、特定の設定を確認する必要があります。Internet Explorer での既知の問題により、再認証は、次の条件下では正常に機能しません。

- Internet Explorer が、Web セキュリティ アプライアンスをプロキシとして使用するように設定されている。
- Web セキュリティ アプライアンスが NTLMSPP 認証を使用している。
- Web セキュリティ アプライアンスが、認証サロゲート用の Cookie を使用しているが、クレデンシャルの暗号化用に設定されていない。
- Web プロキシが明示的な転送モードで展開されている、またはトランスペアレント モードで展開されており、該当する ID グループで [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）] オプションがイネーブルである。

サイトにアクセスするために認証が必要な場合は、問題が発生します。また、初めてサイトを要求している場合、またはサイトにアクセスしようとして再認証している場合にも発生する可能性があります。

これらの問題を回避するには、[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イネーブルにします。

PAC ファイルによる再認証の使用

再認証をイネーブルにし、PAC ファイルを使用するようにクライアント アプリケーションを設定すると、PAC ファイルで再認証が正常に機能するように、特定の設定を確認する必要があります。

再認証は、次の条件下では正常に機能しません。

- クライアント ブラウザが PAC ファイルを使用するように設定され、PAC ファイルが、内部 Web サーバの Web プロキシをバイパスするように設計されている。Web プロキシに要求を明示的に送信するようブラウザに指示するのではなく、宛先サーバに要求を直接送信するようにブラウザに指示する。
- Web セキュリティ アプライアンスが、認証サロゲートの IP アドレスを使用するか、サロゲートを使用しない。また、クレデンシャルの暗号化がイネーブルでない。
- Web プロキシが明示的な転送モードで展開されている、またはトランスペアレント モードで展開されており、該当する ID グループの [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）] オプションがイネーブルである。

問題が発生するのは、再認証で、クライアントが認証のために Web プロキシにリダイレクトされる必要があるにもかかわらず、PAC ファイルによって、すべての要求が内部 Web サーバ（Web セキュリティ アプライアンスを含む）にバイパスされるためです。

このような問題を回避するには、PAC ファイルを編集して、ホストの IP アドレスが x.x.x.x の場合に関数 FindProxyForURL() が 「PROXY x.x.x.x:80」を返すようにします。戻りで指定するポート番号は、他の宛先に対して設定されているポートと同じである必要があります。

（注）　Web セキュリティ アプライアンスが認証のために 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。詳細については、「Internet Explorer での再認証の使用」(P.20-28)」を参照してください。

認証ユーザの追跡

表 20-11 は、認証サロゲートが明示的な転送要求の他の設定で、どの認証サロゲートがサポートされるかを説明しています。

表 20-11　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	Yes	Yes	Yes	該当なし	該当なし	該当なし
IP ベース	Yes	Yes	Yes	Yes	Yes	Yes
Cookie ベース	Yes	Yes***	Yes***	Yes	No/Yes**	Yes***

表 20-12 は、認証サロゲートがトランスペアレント要求の他の設定で、どの認証サロゲートがサポートされるかを説明しています。

表 20-12　トランスペアレント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	該当なし	該当なし	該当なし	該当なし	該当なし	該当なし
IP ベース	Yes	No/Yes*	No/Yes*	Yes	No/Yes*	No/Yes*
Cookie ベース	Yes	No/Yes**	No/Yes**	Yes	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。**トランザクションが認証をバイパスします。
- **HTTPS トランザクション。**トランザクションがドロップされます。ただし、認証のために最初の 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のために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 の各要求は認証をバイパスするため、認証は要求されません。アイデンティティ ポリシー グループおよび非アイデンティティ ポリシー グループに HTTPS 要求が割り当てられる方法の詳細については、「認証が HTTP 要求を介した HTTPS および FTP に影響を与える仕組みについて」（P.8-6）を参照してください。

*** 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。

認証のバイパス

一部のインスタント メッセージのアプリケーションまたはアプレットなど、一部のクライアント アプリケーションおよびサーバでは、認証が適切に処理されません。たとえば、NTLMSSP にまったく対応しないクライアントもあれば、認証の標準に従わないクライアントもあります。これらのアプリケーションまたはサーバの間のトランザクションを Web プロキシが処理すると、認証が失敗することがあります。

これらの制限は、影響を受けるクライアントとサーバの認証をバイパスすると、回避できます。

ステップ 1　拡張プロパティを設定して、影響を受ける Web サイトを含むカスタム URL カテゴリを作成します。

ステップ 2　影響を受けるクライアント アプリケーションおよびステップ 1 で作成したカスタム URL カテゴリにだけ適用される ID グループを作成します。

ステップ 3　このアイデンティティを、認証を必要とする他のすべてのアイデンティティの前に配置します。

ステップ 4　認証を必要としないようにアイデンティティを設定します。

ステップ 5　必要に応じて、他のポリシー グループでアイデンティティを使用します。

LDAP 認証

LDAP（Lightweight Directory Access Protocol）サーバ データベースは、従業員ディレクトリのリポジトリです。これらのディレクトリには、従業員の名前とともに、電話番号、電子メール アドレス、および個々の従業員固有の情報など、さまざまなタイプの個人的なデータが含まれます。LDAP データベースは、属性と値を含むオブジェクトで構成されます。各オブジェクト名は、識別名（DN）と呼ばれます。検索が開始される LDAP サーバの場所は、ベース識別名またはベース DN と呼ばれます。

アプライアンスは、標準の LDAP サーバ認証とセキュア LDAP 認証をサポートしています。LDAP のサポートにより、インストールが確立され、ユーザの認証に LDAP サーバ データベースを使用し続けることができます。

セキュア LDAP の場合、アプライアンスは、SSL を介して LDAP 接続をサポートします。SSL プロトコルは、機密性を確保するための業界標準のプロトコルです。SSL では、認証局（CA）の署名付き証明書とともにキー暗号化アルゴリズムを使用して、アプライアンスのアイデンティティを確認する方法を LDAP サーバに提供します。

（注）　AsyncOS for Web は、基本認証方式を使用する場合、7 ビット ASCII 文字のパスワードのみをサポートします。パスワードに 7 ビット ASCII 以外の文字が含まれる場合、基本認証は失敗します。

Active Directory パスワードの変更

Active Directory LDAP ユーザが自分のアカウント パスワードを変更した後、Active Directory LDAP サーバは、Active Directory サーバの設定に応じて、これらのユーザを現在または以前のパスワードで認証します。

ユーザが新しいパスワードでのみ認証できるようにする場合は、Active Directory サーバを再起動するか、古いパスワードで Active Directory サーバがタイムアウトされるまで待ちます。

LDAP グループの認可

LDAP ディレクトリに保存されているユーザ グループ メンバーシップ情報を使用して、ユーザのグループにグループ ポリシーを適用できます。これを行うには、LDAP 認証レルムでグループの認可をイネーブルにし、次の LDAP オブジェクト タイプのいずれかを使用してユーザをグループ化します。

- **グループ オブジェクト。**グループ メンバーシップ情報は、グループ オブジェクトに保存される場合があります。このオブジェクトには、グループに属するすべてのユーザのリストである属性（「member」など）があります。グループ オブジェクトに、ユーザが定義する必要があるすべてのユーザが含まれている場合は、認可されたユーザをグループ オブジェクトで定義してください。認可されたユーザをグループ オブジェクトで定義する方法の詳細については、表 20-13（P.20-32）を参照してください。
- **ユーザ オブジェクト。**グループ メンバーシップ情報は、ユーザ オブジェクトに保存される場合があります。このオブジェクトには、ユーザが属するすべてのグループのリストである属性（「memberOf」など）があります。認証サーバがグループ オブジェクトにメンバ情報を保存しない場合、またはグループ オブジェクトがない場合は、認可されたユーザをユーザ オブジェクトで定義できます。認可されたユーザをユーザ オブジェクトで定義する方法の詳細については、表 20-14（P.20-33）を参照してください。

（注）　ユーザ オブジェクトには、特殊文字を含めることはできません。

グループの認可を LDAP 認証レルムに設定する場合は、必ず、LDAP サーバのグループ オブジェクトを一意的に識別してください。グループ DN の検索で複数のエントリが返される場合、Web セキュリティ アプライアンスは、最初に返されたエントリだけを使用します。次のフィールドを使用して、グループ オブジェクトを一意的に識別します。

- Base DN
- グループ名が格納されている属性
- オブジェクトがグループかどうかを特定するクエリー文字列

Active Directory サーバに対する、ユーザ オブジェクトに基づくグループの認可を含む LDAP 認証レルムを作成すると、ユーザ オブジェクトには、ユーザが属するプライマリ グループ（「Domain Users」など）が含まれません。定義された他のグループのみが含まれます。したがって、次の条件下では、ポリシー グループが、このようなユーザに一致しない可能性があります。

- アイデンティティ ポリシー グループで、ユーザ属性に基づくグループの認証を行う LDAP レルムが指定されている。
- 非アイデンティティ ポリシー グループがアイデンティティ ポリシー グループを使用しており、プライマリ グループが、認可されたグループとして Active Directory サーバで設定されている。

表 20-13 は、グループ オブジェクト設定について説明しています。

表 20-13　LDAP グループの認可：グループ オブジェクト設定

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のリストである 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 メンバを指定する、LDAP ディレクトリで一意の ID。 • **[custom]。**「`UserInGroup`」などのカスタム ID。
グループ名を含む属性（Attribute that Contains the Group Name）	ポリシー グループの設定で使用できるグループ名を指定する LDAP 属性を選択します。 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]。**「`FinanceGroup`」などのカスタム ID。
オブジェクトがグループかどうかを判別するクエリ文字列（Query String to Determine if Object is a Group）	LDAP オブジェクトがユーザ グループを表すかどうかを特定する 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]。**「`objectclass=person`」などのカスタム フィルタ。 **注：**クエリーによって、ポリシー グループで使用できる認証グループのセットが定義されます。

表 20-14 は、ユーザ オブジェクト設定について説明しています。

表 20-14　LDAP グループの認可：ユーザ オブジェクト設定

ユーザ オブジェクト設定	説明
ユーザ オプ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のリストであ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 メンバを指定する、LDAP ディレクトリで一意の ID。 • **[custom]。**「`UserInGroup`」などのカスタム ID。
グループメンバーシップ属性は DN です。（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、以降の設定を指定する必要があります。
グループ名を含む属性（Attribute that Contains the Group Name）	グループ メンバーシップ属性が DN である場合は、これで、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]。**「`FinanceGroup`」などのカスタム ID。
オブジェクトがグループかどうかを判別するクエリ文字列（Query String to Determine if Object is a Group）	LDAP オブジェクトがユーザ グループを表すかどうかを特定する 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]。**「`objectclass=person`」などのカスタム フィルタ。 **注：**クエリーによって、Web Security Manager ポリシーで使用できる認証グループのセットが定義されます。

NTLM 認証

NT LAN Manager（NTLM）は、アプライアンスと Microsoft Windows ドメイン コントローラの間で発生する、暗号化されたチャレンジ/レスポンス シーケンスでユーザを認証します。NTLM チャレンジ/レスポンス ハンドシェイクは、データが設定される前の、Web ブラウザがアプライアンスに接続しようとしたときに発生します。

NTLM 認証レルムを設定すると、認証方式を指定する必要がなくなります。代わりに、ID グループでレルムを使用するときに方式を選択します。これにより、アイデンティティごとに異なる方式を選択できます。ID グループを作成または編集するときに、次の方式の 1 つを選択できます。

- NTLMSSP の使用
- 基本認証または NTLMSSP の使用
- 基本認証の使用

（注）　AsyncOS for Web は、基本認証方式を使用する場合、7 ビット ASCII 文字のパスワードのみをサポートします。パスワードに 7 ビット ASCII 以外の文字が含まれる場合、基本認証は失敗します。

複数の Active Directory ドメインに対するユーザ認証

NTLM レルムは、1 つの Active Directory ドメインに参加するように設定されます。ただし、次の条件が存在する場合は、Web プロキシも同じまたは異なるフォレストのドメインに対してユーザを認証できます。

- すべての Active Directory ドメインが同じフォレストにある場合は、フォレスト内のすべてのドメイン間の信頼関係が必要です。
- 別のフォレストにある Active Directory ドメインが存在する場合は、Web セキュリティ アプライアンスが参加するドメインに、ユーザが属するドメインとの間に少なくとも 1 方向の信頼が必要です。

AsyncOS では、最大 10 の NTLM 認証レルムを作成できます。Web プロキシが、別のフォレストとの相互信頼関係を持たない異なる Active Directory フォレストのユーザを認証する必要がある場合は、複数の NTLM レルムを作成できます。

（注）　複数の NTLM レルムを作成するには、1 つの NTLM レルムのクライアントの IP アドレスが、別の NTLM レルムのクライアント IP アドレスと重複していないことが必要です。

ポリシー グループのメンバーシップをグループ名で定義すると、Web インターフェイスには、ドメインに参加させたときに AsyncOS がコンピュータ アカウントを作成したドメインの Active Directory グループのみが表示されます。異なるドメインのユーザのポリシー グループを作成するには、Web インターフェイスに手動でドメインとグループ名を入力します。

（注）　シスコでは、必要に応じて、いくつかの NTLM レルムとして作成することを推奨します。複数の NTLM レルムを作成すると、より多くのメモリが認証で必要になります。

サポートされる認証文字

ここに示すのは、Web セキュリティ アプライアンスが、LDAP サーバや Active Directory サーバと通信する場合にサポートされる文字の一覧です。認証が正しく機能するように、認証サーバが、この一覧に含まれる、サポートされる文字のみを使用することを確認してください。

たとえば、アプライアンスは表 20-15 に従って、次の Active Directory のユーザ名でユーザを検証できます。

```
jsmith#123
```

また、アプライアンスは表 20-15 に従って、次の Active Directory のユーザ名でユーザを検証できます。

```
jsmith+
```

Active Directory サーバでサポートされる文字

表 20-15 は、Web セキュリティ アプライアンスが、Active Directory サーバの [ユーザ名（User Name）] フィールドでサポートする文字の一覧です。

表 20-15　サポートされる Active Directory サーバ文字：[ユーザ名（User Name）] フィールド

サポートされる文字	サポートされない文字
A...Z a...z 0 1 2 3 4 5 6 7 8 9 ` ~ ! # $ % ^ & ( ) _ - { } ' . @ space	/ \ [ ] : ; | = , + * ? < > "

（注）　Web セキュリティ アプライアンスは、Web を参照しているエンド ユーザの場合はパーセント（%）文字をサポートします。ただし、NTLM 認証レルムを作成するときに、パーセント（%）文字を含むユーザ名を使用して、Active Directory ドメインに参加させることはできません。

表 20-16 は、Web セキュリティ アプライアンスが、Active Directory サーバの [パスワード（Password）] フィールドでサポートする文字の一覧です。

表 20-16　サポートされる Active Directory サーバ文字：[パスワード（Password）] フィールド

サポートされる文字	サポートされない文字
A...Z a...z 0 1 2 3 4 5 6 7 8 9 ` ~ ! # $ ^ & ( ) _ - { } ' . / [ ] : | * ? @ + \ , ; " = < > space	該当なし

表 20-17 は、Web セキュリティ アプライアンスが、Active Directory サーバの [ロケーション（Location）] フィールドでサポートする文字の一覧です。NTLM 認証レルムを設定するときは、[ロケーション（Location）] フィールドに場所の文字列を入力します。

表 20-17　サポートされる Active Directory サーバ文字：[ロケーション（Location）] フィールド

サポートされる文字	サポートされない文字
A...Z a...z 0 1 2 3 4 5 6 7 8 9 ` ~ ! # $ ^ & ( ) _ - { } ' . / [ ] : | * ? @ space	+ \ , ; " = < > （注）　アプライアンスでは、バックスラッシュ（\）文字でエスケープしても、これらの文字はサポートされません。

表 20-18 は、Web セキュリティ アプライアンスが、Active Directory サーバの [グループ（Group）] フィールドでサポートする文字の一覧です。

表 20-18　サポートされる Active Directory サーバ文字：[グループ（Group）] フィールド

サポートされる文字	サポートされない文字
A...Z a...z 0 1 2 3 4 5 6 7 8 9 ` ~ ! # $ % ^ & ( ) _ - { } ' . @ space	/ \ [ ] : ; | = , + * ? < > "

（注）　バックスラッシュ（\）文字を使用できるのは、ドメイン名と、ユーザ名またはグループ名の間の区切り文字として、または Active Directory サーバの場所を示す文字列で複数の組織単位（OU）間の区切り文字としてのみです。ドメイン名、ユーザ名、グループ名、または場所名の一部として使用することはできません。

LDAP サーバでサポートされる文字

表 20-19 は、Web セキュリティ アプライアンスが、LDAP サーバの [ユーザ名（User Name）] フィールドでサポートする文字の一覧です。

表 20-19　サポートされる LDAP サーバ文字：[ユーザ名（User Name）] フィールド

サポートされる文字	サポートされない文字
A...Z a...z 0 1 2 3 4 5 6 7 8 9 ` ~ ! # $ % ^ & ( ) _ - { } ' . @ （注）　アプライアンスは、バックスラッシュ（\）文字でエスケープした場合にのみ、「(」および「)」文字をサポートします。	/ \ [ ] : ; | = , + * ? < > "

表 20-20 は、Web セキュリティ アプライアンスが、LDAP サーバの [パスワード（Password）] フィールドでサポートする文字の一覧です。

表 20-20　サポートされる LDAP サーバ文字：[パスワード（Password）] フィールド

サポートされる文字	サポートされない文字
A...Z a...z 0 1 2 3 4 5 6 7 8 9 ` ~ ! # $ % ^ & ( ) _ - { } @ ' . / \ [ ] : | = * ? < > " , ; + space	該当なし

表 20-21 は、Web セキュリティ アプライアンスが、LDAP サーバの [グループ（Group）] フィールドでサポートする文字の一覧です。

表 20-21　サポートされる LDAP サーバ文字：[グループ（Group）] フィールド

サポートされる文字	サポートされない文字
A...Z a...z 0 1 2 3 4 5 6 7 8 9 ` ~ ! # $ % ^ & ( ) _ - { } @ ' . / \ [ ] : | = * ? < > " space （注）　アプライアンスは、バックスラッシュ（\）文字でエスケープした場合にのみ、「(」および「)」文字をサポートします。	, ; +

表 20-22 は、Web セキュリティ アプライアンスが、LDAP サーバの [カスタム ユーザ フィルタ クエリ（Custom User Filter Query）] フィールドでサポートする文字の一覧です。

表 20-22　サポートされる LDAP サーバ文字 : [カスタム ユーザ フィルタ クエリ（Custom User Filter Query）] フィールド

サポートされる文字	サポートされない文字
A...Z a...z 0 1 2 3 4 5 6 7 8 9 ` ~ ! # $ % ^ & ( ) _ - { } ' . space	@ / \ [ ] : | = * ? < > " , ; +

表 20-23 は、Web セキュリティ アプライアンスが、LDAP サーバの [カスタム グループ フィルタ クエリ（Custom Group Filter Query）] フィールドでサポートする文字の一覧です。

表 20-23　サポートされる LDAP サーバ文字 : [カスタム グループ フィルタ クエリ（Custom Group Filter Query）] フィールド

サポートされる文字	サポートされない文字
A...Z a...z 0 1 2 3 4 5 6 7 8 9 ` ~ ! # $ % ^ & ( ) _ - { } @ ' . / \ [ ] : | = * ? < > " space	, ; +

21
L4 トラフィック モニタ

L4 トラフィック モニタについて

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 ポート間の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。また、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間で Phone Home を行おうとすると、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。

L4 トラフィック モニタが動作する仕組みについて

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、着信トラフィックと発信トラフィックを許可するかどうかを決定します。

Web の宛先は、すべて次のカテゴリのいずれかに分類されます。

- **既知の許可されたアドレス。**Allow List プロパティのリストに記載されている 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。
- **リストに記載されていないアドレス。**マルウェア サイトであるかも、既知の許可されたアドレスであるかもわからない IP アドレス。これらは、Allow List または Additional Suspected Malware Addresses プロパティのリストに記載されておらず、L4 トラフィック モニタ データベースのリストにも既知のマルウェア サイトとして記載されていません。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。**これらのアドレスは、「グレイリスト」アドレスとしてログ ファイルに表示されます。次のような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*および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*および 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 アドレス。**これらのアドレスは、「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ます。次のようなアドレスが該当します。

- L4 トラフィック モニタ データベースが既知のマルウェア サイトと判定し、Allow List に記載されていない IP アドレスまたはホスト名。
- Additional Suspected Malware Addresses プロパティのリストに記載*されず*、Allow List のリストにも記載されていない、不明瞭であると判定*されない IP アドレス*。

（注）　[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）] ページで、Allow List and the Additional Suspected Malware Addresses プロパティを定義できます。

L4 トラフィック モニタは、不正なアクティビティ用のネットワーク ポートをリッスンし、モニタします。ネットワーク上のすべてのトラフィックに対して、次のいずれかのアクションを実行します。

- **許可。**既知の許可されたアドレスおよびリストに記載されていないアドレスとの間のトラフィックを常に許可します。
- **モニタ。**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との間でないすべての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、不明瞭なアドレスとの間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 アドレスとの間のトラフィックをブロックします。

L4 トラフィック モニタ データベース

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。また、データベース テーブルは、次の URL にある Cisco IronPort アップデート サーバから定期的に更新を受信します。

```
https://update-manifests.ironport.com
```

更新間隔と Cisco IronPort アップデート サーバの詳細については、「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」（P.26-43）を参照してください。

L4 トラフィック モニタの設定

L4 トラフィック モニタは、システム セットアップ ウィザードを使用して初期システム セットアップの一部としてイネーブルにできます。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。

（注）　正しいクライアント IP アドレスをモニタするには、ネットワーク アドレス変換（NAT）が行われる前にファイアウォール内で必ず L4 トラフィック モニタを設定する必要があります。L4 トラフィック モニタの展開の詳細については、「L4 トラフィック モニタの導入」（P.3-12）を参照してください。

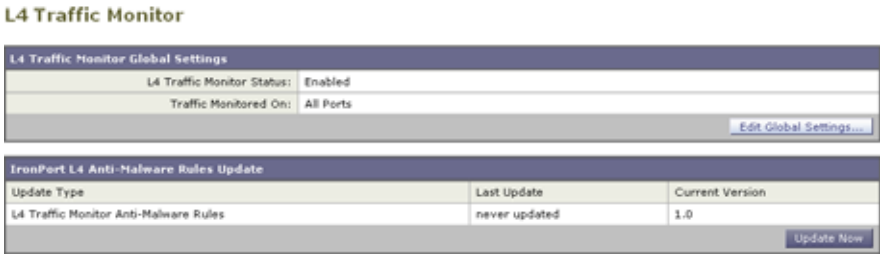
次の設定値を設定できます。

- **グローバル L4 トラフィック モニタの設定。**初期設定後、L4 トラフィック モニタをイネーブルまたはディセーブルに設定し、モニタ対象の TCP ポートを設定できます。[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）] ページを使用します。詳細については、「L4 トラフィック モニタ グローバル設定のコンフィグレーション」（P.21-3）を参照してください。
- **L4 トラフィック モニタ ポリシー。**L4 トラフィック モニタをイネーブルにする場合、管理トラフィック用に特定のポリシーを設定します。[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）] ページを使用します。詳細については、「L4 トラフィック モニタのポリシーの設定」（P.21-4）を参照してください。

L4 トラフィック モニタ グローバル設定のコンフィグレーション

[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）] ページで、L4 トラフィック モニタ グローバル設定を設定し、L4 トラフィック モニタ アンチマルウェア ルールを更新できます。

図 21-1　[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）] ページ



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）] ページに移動します。

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

ステップ 3　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する必要があります。

- **すべてのポート。**不正なアクティビティに関して TCP ポート 65535 をすべてをモニタします。
- **プロキシ** ポートを除くすべての**ポート。**不正なアクティビティに関して、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 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 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、保存します。

L4 トラフィック モニタ アンチマルウェア 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）] ページに移動します。

ステップ 2　[今すぐ更新（Update Now）] をクリックします。

Web セキュリティ アプライアンスは、コンポーネント アップデート サーバにポーリングし、L4 トラフィック モニタ アンチマルウェア ルールを更新します。コンポーネント アップデート サーバの詳細については、「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」（P.26-43）を参照してください。

L4 トラフィック モニタのポリシーの設定

L4 トラフィック モニタがイネーブルの場合、設定した TCP ポート上でトラフィックを管理する方法を設定できます。この設定により、TCP ポート上のトラフィックで次のアクションを実行できます。

- 許可
- モニタ
- ブロック

L4 トラフィック モニタがトラフィックを処理する方法の詳細については、「L4 トラフィック モニタが動作する仕組みについて」（P.21-1）を参照してください。

L4 トラフィック モニタがとるアクションは、設定する L4 トラフィック モニタのポリシーによって異なります。

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）] ページに移動します。

ステップ 2　[設定を編集（Edit Settings）] をクリックします。

ステップ 3　[L4 トラフィック モニタ ポリシー（L4 Traffic Monitor Policies）] ページで、表 21-1 の説明に従って L4 トラフィック モニタのポリシーを設定します。

表 21-1　L4 トラフィック モニタのポリシー

プロパティ	説明
許可リスト（Allow List）	L4 トラフィック モニタがクライアントの接続を常に許可するアドレスを入力します。該当するアドレスがない場合は入力せず、ある場合は 1 つまたは複数のアドレスを入力します。 複数入力する場合は、スペースまたはカンマで区切ります。「有効な形式」（P.21-6）で、使用できる有効なアドレス形式のリストを確認できます。 **（注）** example.com などのドメイン名の一部を入力すると、www.example.com や hostname.example.com も一致します。 このリストに含まれるすべての宛先への接続は常に許可され、トラフィックのログは作成されません。アプライアンスは、L4 トラフィック モニタ アンチマルウェア ルールまたは同じページに記載されている追加のマルウェアと疑われるアドレスに対して宛先を確認しません。 たとえば、IP アドレス 10.1.1.1 が [許可リスト（Allow List）] フィールドと [追加するサスペクト マルウェア アドレス（Additional Suspected Malware Addresses）] フィールドの両方に表示されている場合、L4 トラフィック モニタは 10.1.1.1 への要求を常に許可します。 **（注）** 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許可されたリストに含めないでください。さもないと、L4 トラフィック モニタは、どんなトラフィックもブロックしません。
サスペクト マルウェア アドレスに対するアクション：（Actions for Suspected Malware Addresses）	既知のマルウェア アドレス宛てのトラフィックをモニタするか、またはブロックするかを選択します。既知のマルウェア アドレスの定義については、「L4 トラフィック モニタが動作する仕組みについて」（P.21-1）を参照してください。 • **Monitor :** L4 トラフィック モニタ データベース内のエントリに一致するドメインと IP アドレスへのすべてのトラフィックをスキャンします。[モニタ（Monitor）] オプションは、不審なトラフィックをブロックしません。この設定は、ユーザ エクスペリエンスに影響を与えることなく、感染したクライアントを識別するために役立ちます。 • **Block :** アプライアンスの管理リストおよびブロック リスト データベースのエントリに一致するドメインおよび IP アドレスへのすべてのトラフィックをスキャンし、検出されたすべてのトラフィックをブロックします。この設定は、感染したクライアントを識別し、標準以外のポートを介したマルウェア攻撃を阻止するのに役立ちます。 不審なマルウェア トラフィックをブロックするように選択する場合、不明瞭なアドレスを常にブロックするかどうかを選択することもできます。デフォルトで、不明瞭なアドレスはモニタされます。 不明瞭なアドレスの定義については、「L4 トラフィック モニタが動作する仕組みについて」（P.21-1）を参照してください。

表 21-1　L4 トラフィック モニタのポリシー （続き）

プロパティ	説明
追加するサスペクト マルウェア アドレス (任意) (Additional Suspected Malware Addresses (Option))	L4 トラフィック モニタがマルウェアの可能性があると見なす既知のアドレスを入力します。該当するアドレスがない場合は入力せず、ある場合は 1 つまたは複数のアドレスを入力します。「有効な形式」（P.21-6）で、使用できる有効なアドレス形式のリストを確認できます。 不審なマルウェア アドレスをブロックするように選択した場合、L4 トラフィック モニタは、これらを既知のマルウェア アドレスまたは不明瞭なアドレスと判定するかどうかに応じて、これらのアドレスをブロックするか、またはモニタします。不明瞭なアドレスと既知のマルウェア アドレスの定義については、「L4 トラフィック モニタが動作する仕組みについて」（P.21-1）を参照してください。 不審なマルウェア アドレスをモニタするように選択した場合、これらのアドレスをモニタします。 **（注）** 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。このようなタイプの誤ったレポートを回避するために、[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。

（注） L4 トラフィック モニタがブロックを実行するように設定する場合は、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。

ステップ 4　変更を送信し、保存します。

有効な形式

Allow List または Additional Suspected Malware Addresses プロパティにアドレスを追加する場合、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。

- **IP アドレス。**たとえば、10.1.1.0 と入力します。
- **CIDR アドレス。**たとえば、10.1.1.0/24 と入力します。
- **ドメイン名。**たとえば、example.com のように指定します。example.com などのドメイン名の一部を入力すると、www.example.com や hostname.example.com も一致します。
- **ホスト名。**たとえば、crm.example.com のように指定します。

L4 トラフィック モニタ 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。時間、日、週、または月などの時間範囲を指定して、これらの表示をインタラクティブに更新できます。さらに、これらの表示ページを印刷したり、未処理データをファイルにエクスポートしたりすることもできます。

次の表示およびレポート ツールを使用して、L4 トラフィック モニタ アクティビティの結果を表示できます。

表 21-2　L4 トラフィック モニタのスキャン データ

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、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 レポートでクライアント 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、クライアントの IP アドレスが正しく記録され、表示されるように IP スプーフィングをイネーブルにします。

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。L4 トラフィック モニタ ログの詳細については、「トラフィック モニタ ログ」（P.24-43）を参照してください。

22
レポート

レポーティングの概要

レポーティング機能は、個々のセキュリティ機能から情報を収集し、Web トラフィック パターンやセキュリティ リスクのモニタに使用できるデータを記録します。レポートをリアルタイムで実行して所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、スケジュールを作成してレポートを定期的に実行したりすることができます。

Web セキュリティ アプライアンスは、概要レポートを生成してネットワークで起きていることを把握できるだけでなく、特定のドメイン、ユーザ、またはカテゴリのトラフィックの詳細を、ドリルダウンして確認できます。

また、レポーティング機能を使用して、raw データをファイルにエクスポートすることもできます。詳細については、「レポート ページからのレポートの印刷とエクスポート」（P.22-7）を参照してください。

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 jsmith などの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認識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。

レポートでユーザ名を認識できないようにするには、次の手順を実行します。

ステップ 1　[クライアント アクティビティ（Client Activity）] > [レポート（Reporting）] ページに移動し、[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）] の下で、[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、保存します。

レポート ページ

Web セキュリティ アプライアンスは、次のレポートを表示します。

- 概要（Overview）
- ユーザ（Users）
- Web サイト（Web Sites）
- URL カテゴリ（URL Categories）
- アプリケーションの表示（Application Visibility）
- マルウェア対策（Anti-Malware）
- 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）
- L4 トラフィック モニタ（L4 Traffic Monitor）
- ユーザの場所別のレポート（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)

これらの各レポートの詳細については、「Web セキュリティ アプライアンスのレポート」（P.23-1）を参照してください。

[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。このセクションでは、これらのオプションについて説明し、各レポート ページに表示される情報を示します。

レポート ページは、システム アクティビティのカラフルな概要を説明し、システム データを表示するための複数のオプションをサポートします。たとえば、データを更新し、ソートして、リソースの使用率と Web トラフィック アクティビティにリアルタイムで確認できます。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。

- **レポートで表示する時間範囲を変更します。**詳細については、「「時間範囲の変更」（P.22-3）」を参照してください。
- **特定のクライアントとドメインを検索します。**詳細については、「「データの検索」（P.22-3）」を参照してください。
- **チャートに表示するデータを選択します。**「チャート化するデータの選択」（P.22-4）を参照してください。
- **カラムを選択およびソートします。**詳細については、「「レポート ページのカラムの使用」（P.22-4）」を参照してください。
- **レポートを外部ファイルにエクスポートします。**詳細については、「「レポート ページからのレポートの印刷とエクスポート」（P.22-7）」を参照してください。

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 コンポーネントに表示されるデータを更新できます。このオプションでは、直近の時間または週など、定義済みの時間範囲の更新を行い、特定の開始時刻から特定の終了時刻までのカスタム時間範囲を定義することができます。

（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 ページを通して使用されます。

図 22-1 は、[URL カテゴリ（URL Categories）] レポートの [時間範囲（Time Range）] フィールドを示します。

図 22-1　　データの時間範囲の選択

表 22-1 に示す任意の時間範囲を選択できます。

表 22-1　　設定可能な時間範囲

時間範囲	データが返される間隔
時（Hour）	60 分間と、追加で最大 5 分間。
日（Day）	1 時間間隔で直近の 24 時間（その時点の 1 時間未満を含む）。
週（Week）	1 日間隔で直近の 7 日間（その時点の 1 日未満を含む）。
1ヶ月（30 日）（Month (30 days)）	1 日間隔で直近の 30 日間（その時点の 1 日未満を含む）。
昨日（Yesterday）	時間帯が定義された Web セキュリティ アプライアンスを使用した直近の 24 時間（00:00 ～ 23:59）。
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）　すべてのレポートは、グリニッジ標準時（GMT）オフセットとして表示されるシステムに設定されたタイム ゾーンに基づい日付と時刻情報を表示します。ただし、データのエクスポートでは、全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 GMT で時刻が表示されます。

データの検索

一部のレポートは、特定のデータ ポイントを検索できるフィールドを備えています。たとえば、[URL カテゴリ（URL Categories）] レポートでは、特定の URL カテゴリを検索し、[ユーザ（Users）] レポートでは、ユーザ名または IP アドレスによって特定のユーザを検索できます。データを検索するときに、レポートは検索する特定のデータ セットのレポート データを調整します。

入力する文字列に完全に一致する値や入力する文字列で始まる値を検索できます。

次のレポート ページは、検索フィールドを備えています。

- **ユーザ（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 カテゴリ（URL Categories）。**URL カテゴリを検索します。
- **アプリケーションの表示（Application Visibility）。**AVC エンジンがモニタし、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。

図 22-2 は、[URL カテゴリ（URL Categories）] レポートの検索フィールドを示します。

図 22-2　URL カテゴリの検索

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。

通常、チャートのオプションは、レポート内のテーブルのカラムの見出しと同じです。これらの見出しの説明については、「レポート ページのカラムの使用」（P.22-4）を参照してください。

チャートには、関連付けられたテーブルに表示するように選択した項目（行）数に関係なく、テーブル カラムの使用可能なすべてのデータが反映されます。

チャート化するデータを選択するには、次の手順を実行します。

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。

レポート ページのカラムの使用

各ページには、そのページのデータを表示するニーズだけに当てはまるデータをカラムごとにソートするように設定できるインタラクティブなカラムの見出しが用意されています。

（注） レポート ページによっては、一部のカラムを使用できないことがあります。利用可能なカラムを表示するには、各レポート ページの [カラム（Columns）] リンクをクリックします。

表 22-2 は、レポートの使用時に利用可能なカラムについて説明します。

表 22-2　　レポートのカラムの説明

カラム名	説明
ドメインまたはレルム（Domain or Realm）	テキスト形式で表示されるユーザのドメインまたはレルム。
ユーザ ID またはクライアント IP（User ID or Client IP）	テキスト形式で表示されるユーザ名またはクライアント IP アドレス。
使用帯域幅（Bandwidth Used）	特定のユーザまたはアクションによって使用される帯域幅の量。帯域幅の単位は、バイトまたは % で表示されます。
ブロック機能によって節約された帯域幅（Bandwidth Saved by Blocking）	特定のトランザクションのブロックのため節約された帯域幅の量。帯域幅単位はバイトで表示されます。
滞留時間（Time Spent）	Web ページに費やされた時間。各 URL カテゴリでユーザが費やした時間。ユーザを調査する目的で使用されます。URL のトラッキング時には、その特定の URL に各ユーザが費やした時間。 費やされた時間を計算するため、AsyncOS はアクティブ ユーザごとに、1 分間のアクティビティに対して 60 秒という時間を割り当てます。この 1 分間の終わりに、各ユーザが費やした時間は、そのユーザが訪れた各ドメイン間で均等に配分されます。たとえば、あるユーザがアクティブな 1 分間に 4 つの異なるドメインに進んだ場合、そのユーザは各ドメインで 15 分ずつ費やしたと見なされます。 経過時間の値に関して、以下の注意事項を考慮してください。 • アクティブ ユーザは、アプライアンスを介して HTTP トラフィックを送信し、Web サイトにアクセスした、すなわち AsyncOS が「ページ ビュー」と見なす動作を行ったユーザ名または IP アドレスとして定義されています。 • AsyncOS では、クライアント アプリケーションが開始する要求とは逆に、ユーザが開始する HTTP 要求としてページ ビューを定義します。AsyncOS はヒューリスティック アルゴリズムを使用して、可能な限り効果的にユーザ ページ ビューを識別します。 単位は時間：分形式で表示されます。
許可された URL カテゴリ（Allowed URL Category）	許可されたカテゴリの数とタイプ。単位はトランザクション タイプで表示されます。
モニタされた URL カテゴリ（Monitored URL Category）	モニタリングされているカテゴリの数とタイプ。単位はトランザクション タイプで表示されます。
警告された URL カテゴリ（Warned URL Category）	警告が発行されたカテゴリの数とタイプ。単位はトランザクション タイプで表示されます。
URL カテゴリによるブロック（Blocked by URL Category）	URL カテゴリが原因でブロックされたトランザクション。単位はトランザクション タイプで表示されます。

表 22-2　レポートのカラムの説明 （続き）

カラム名	説明
アプリケーションまたはアプリケーション タイプによるブロック（Blocked by Application or Application Type）	アプリケーション タイプが原因でブロックされたアプリケーション。単位はトランザクション タイプで表示されます。
Web レピュテーションによるブロック（Blocked by Web Reputation）	Web レピュテーションのためブロックされたトランザクション。単位はトランザクション タイプで表示されます。
マルウェア対策によるブロック（Blocked by Anti-Malware）	Anti-Malware によってブロックされたトランザクション。単位はトランザクション タイプで表示されます。
その他のブロックされたトランザクション（Other Blocked Transactions）	ブロックされた他のすべてのトランザクション。単位はトランザクション タイプで表示されます。
帯域幅制限のあるトランザクション（Transactions with Bandwidth Limit）	帯域幅の制限があるトランザクションの数。
帯域幅制限のないトランザクション（Transactions without Bandwidth Limit）	帯域幅の制限がないトランザクションの数。
ブロックされたトランザクション（アプリケーション別）（Transactions Blocked by Application）	特定のアプリケーション タイプによってブロックされたトランザクションの数。
警告されたトランザクション（Warned Transactions）	ユーザに警告が発せられたすべてのトランザクション。単位はトランザクション タイプで表示されます。
完了したトランザクション（Transactions Completed）	ユーザが完了したトランザクション。単位はトランザクション タイプで表示されます。
ブロックされたトランザクション（Transactions Blocked）	ブロックされたすべてのトランザクション。単位はトランザクション タイプで表示されます。
総トランザクション（Total Transactions）	発生したトランザクションの合計数。

レポート ページのカラムの設定

レポートに表示するカラムを設定するには、次の手順を実行します。

ステップ 1　[レポート（Reporting）] > [Report_Name] を選択します。

ステップ 2　レポートの右下隅に表示される [カラム（Columns）] リンクをクリックします。

ステップ 3　ポップアップ ウィンドウの各カラムの横にあるチェックボックスをオンにして、表示する各カラムを選択し、[完了（Done）] をクリックします。

レポーティング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

レポーティング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 [印刷用（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）でエクスポートできます。このデータを、ほとんどスケジュール設定されたレポートに CSV で保存することもできます。

CSV エクスポートには未処理データだけが含まれているため、Web ベースのレポート ページからエクスポートしたデータには、そのデータを Web ベースのレポートに表示する場合でも、パーセンテージなどの計算されたデータが含まれない可能性があります。

（注）　[Web トラッキング（Web Tracking）] ページが検索結果を返した後に、[Web トラッキング（Web Tracking）] ページからのデータを PDF にのみ出力し、エクスポートできます。実行するには、[印刷可能なダウンロード（Printable Download）] リンクを使用します。このリンクから、現在のページに表示されるデータ、または最大 1,000 件のトランザクションのデータを含む PDF を作成し、あるいはすべてのデータを CSV ファイルにエクスポートできます。詳細を表示する場合、最大 100 件の関連トランザクションのデータが PDF に含まれます。冒頭の 3000 文字が関連トランザクションごとに表示されます。

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て、データにアクセスし、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
```

表 22-3　raw データ エントリの表示

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。
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。この問題の回避策するには、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。

中央集中型レポーティングのイネーブル化

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。デフォルトで、Web セキュリティ アプライアンスはレポート（ローカル レポーティング）を保持します。ただし、中央集中型レポーティングをイネーブルにすることで、セキュリティ管理アプライアンスがレポートを保持するように Web セキュリティ アプライアンスを設定でき

ます。セキュリティ管理アプライアンスが複数の Web セキュリティ アプライアンスを管理する場合、中央集中型レポーティングをイネーブルにする場合があります。これにより、すべての Web セキュリティ アプライアンスにまたがって Web トラフィックの中央集中型表示が可能になります。

（注）　中央集中型レポーティングをイネーブルにした場合、[システム容量（System Capacity）] レポートと [システム ステータス レポート（System Status Report）] レポートのみ 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。Web セキュリティ アプライアンスには、その他のレポートのデータが保存されなくなります。

中央集中型レポーティングをイネーブルにするには、次の手順を実行します。

ステップ 1　[セキュリティ サービス（Security Services）] > [レポート（Reporting）] ページに移動し、[設定を編集（Edit Settings）] をクリックします。

ステップ 2　[集中型レポート（Centralized Reporting）] を選択します。

ステップ 3　変更を送信し、保存します。

レポートのスケジューリング

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。スケジュールされたレポートは、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。また、指定した日数（2 ～ 100 日）または指定した月数（2 ～ 12 ヵ月）のデータを含めることもできます。

レポートの実行時間にかかわらず、直前の時間間隔（過去 1 時間、1 日、1 週間、または 1 ヵ月）のデータのみが含まれます。たとえば、日次レポートを午前 1 時に実行するようにスケジュールを設定した場合、レポートには前日の 00:00 から 23:59 までのデータが含まれます。

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（Overview）
- ユーザ（Users）
- Web サイト（Web Sites）
- URL カテゴリ（URL Categories）
- アプリケーションの表示（Application Visibility）
- マルウェア対策（Anti-Malware）
- 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）
- L4 トラフィック モニタ（L4 Traffic Monitor）
- ユーザの場所別のレポート（Reports by User Location）
- システム容量（System Capacity）

各レポートに表示されるデータの詳細については、「Web セキュリティ アプライアンスのレポート」（P.23-1）を参照してください。

スケジュール設定されたレポートの追加

さまざまなレポートのレポーティングをスケジュールするには、[レポート（Reporting）] > [定期レポート（Scheduled Reports）] ページを使用します。

スケジュール設定されたレポートを作成するには、次の手順を実行します。

ステップ 1　[レポート（Reporting）] > [定期レポート（Scheduled Reports）] ページに移動し、[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。同じ名前の複数のレポートを作成することを防止するため、わかりやすいタイトルを使用することを考慮します。

ステップ 4　レポートに含まれ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、raw データを CSV ファイルとして保存することもできます。

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カラムなど、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、毎日、毎週、または毎月、および何時にレポートを行うかを選択します。

ステップ 8　[電子メール（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、保存します。

スケジュール設定されたレポートの編集

レポートを編集するには、[レポート（Reporting）] > [定期レポート（Scheduled Reports）] ページでリストからレポート タイトルを 選択し、設定を変更してから、変更を送信し、保存します。

スケジュール設定されたレポートの削除

レポートを削除するには、[レポート（Reporting）] > [定期レポート（Scheduled Reports）] ページに移動し、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。スケジュール設定されたレポートをすべて削除する場合は、[すべて（All）] チェックボックスをオンにし、**削除**を実行して変更を**確定**します。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

[レポート（Reporting）] > [アーカイブ レポート（Archived Reports）] ページの [今すぐレポートを生成（Generate Report Now）] オプションを使用すると、各レポート タイプのオンデマンド データ表示を生成できます。

ステップ 1　[レポート（Reporting）] > [アーカイブ レポート（Archived Reports）] ページに移動します。

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 タイプを選択し、必要に応じてタイトルを編集します。同じ名前の複数のレポートを作成することを防止するため、わかりやすいタイトルを使用することを考慮します。

ステップ 4　レポートに含まれ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、raw データを CSV ファイルとして保存することもできます。

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カラムなど、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 Reports）] 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　変更を保存します。

アーカイブ済みのレポート

[レポート（Reporting）] > [アーカイブ レポート（Archived Reports）] 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 タイトル（Report Title）] カラムのレポート名はインタラクティブとなっていて、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。また、インタラクティブなカラム見出しを使用して、各カラム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 要求は、P1 インターフェイスでサービスされます。
- SNMP は、デフォルトで**オフ**になります。
- SNMP SET 動作（コンフィギュレーション）は実装されません。
- AsyncOS は SNMPv1、v2、および v3 をサポートしています。
- このサービスをイネーブルにするには、パスワード認証と DES 暗号化を伴う SNMPv3 の使用が必須です （SNMPv3 の詳細については、RFC 2571 ～ 2575 を参照してください）。SNMP システム ステータスのモニタリングをイネーブルにするには、少なくとも 8 文字の SNMPv3 パスフレーズ

を設定する必要があります。最初に SNMPv3 パスフレーズを入力するときは、確認のためにそのパスフレーズを再入力する必要があります。次に snmpconfig コマンドを実行するときは、コマンドにこのフレーズが「記憶」されています。

- SNMPv3 ユーザ名は v3get です。

```
> snmpwalk -v 3 -l AuthNoPriv -u v3get -a MD5 ironport 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

シスコは、電子メールと Web セキュリティ アプライアンスに、次の「エンタープライズ」MIB および「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、IronPort 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 センサーが温度、ファン スピード、および電源モジュール ステータスを報告します。

表 22-4 に、どのモデルでどのハードウェア派生オブジェクトをモニタリングに使用できるかを示します。表示されている数字は、モニタできるオブジェクトのインスタンスの数です。たとえば、S350 アプライアンスの 4 つのファンの用 RPM を照会できます。

表 22-4　アプライアンスごとのハードウェア オブジェクトの数

モデル	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

表 22-5 に、ハードウェア トラップが送信される温度およびハードウェアの条件を示します。

表 22-5　ハードウェア トラップ：温度およびハードウェアの条件

モデル	高温（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	ステータス変更	ステータス変更	ステータス変更

ステータス変更トラップは、ステータスが変更されると送信されます。ファン障害および高温トラップは、5 秒ごとに送信されます。その他のトラップは、障害条件アラーム トラップです。これらのトラップは、ステータスが（良好から障害へ）変更されたときに一度だけ送信されます。ハードウェア ステータス テーブルにポーリングを送信して、致命的な状況になる前に潜在的なハードウェア障害を識別することを推奨します。重大値の 10 % 以内の温度を不安原因と考えることができます。

障害条件アラーム トラップは、個々のコンポーネントの致命的な障害を示しますが、システム全体の障害の原因になるとは限りません。たとえば、S650 アプライアンスで 1 つのファンまたは電源モジュールに障害が発生しても、アプライアンスは動作し続けます。

SNMP トラップ

SNMP には、1 つまたは複数の条件が満たされたときに管理アプリケーション（通常は、SNMP 管理コンソール）に知らせるためのトラップ（または通知）を送信する機能が備わっています。トラップとは、トラップを送信するシステムのコンポーネントに関するデータを含むネットワーク パケットです。トラップは、SNMP エージェント（この場合は IronPort 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。トラップ ターゲットの入力を求められたときに、複数のトラップ ターゲットを指定するには、カンマで区切った IP アドレスを 10 個まで入力できます。

CLI の例

次の例では、snmpconfig コマンドを使用して、ポート 161 の「PublicNet」インターフェイスで SNMP をイネーブルにしています。バージョン 3 のパスフレーズが入力され、確認のために再入力されています。システムは、バージョン 1 および 2 要求を処理するように設定されており、これらのバージョン 1 および 2 からの GET 要求に対してコミュニティ ストリング public が入力されています。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)

[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>
```

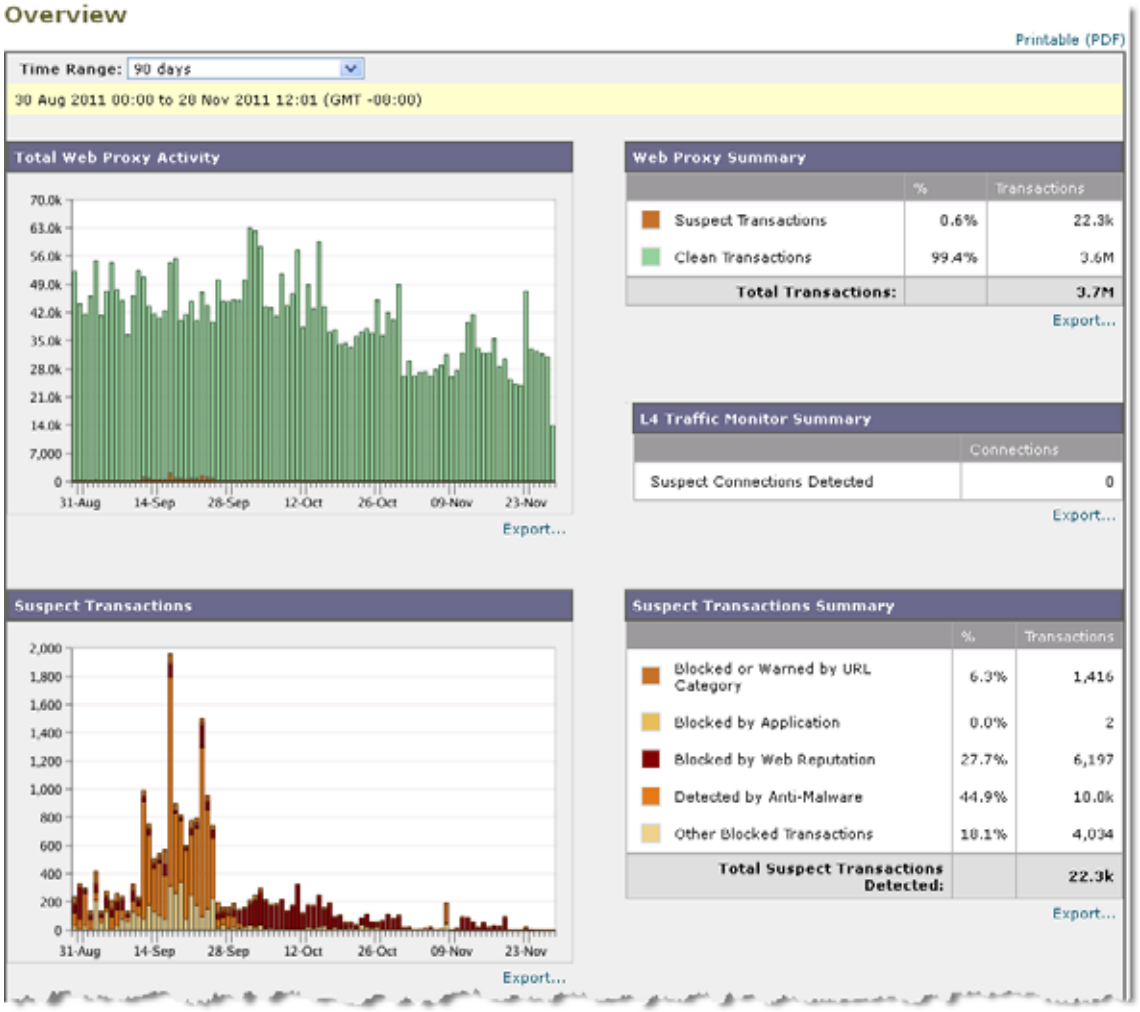
23
Web セキュリティ アプライアンスのレポート

[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。

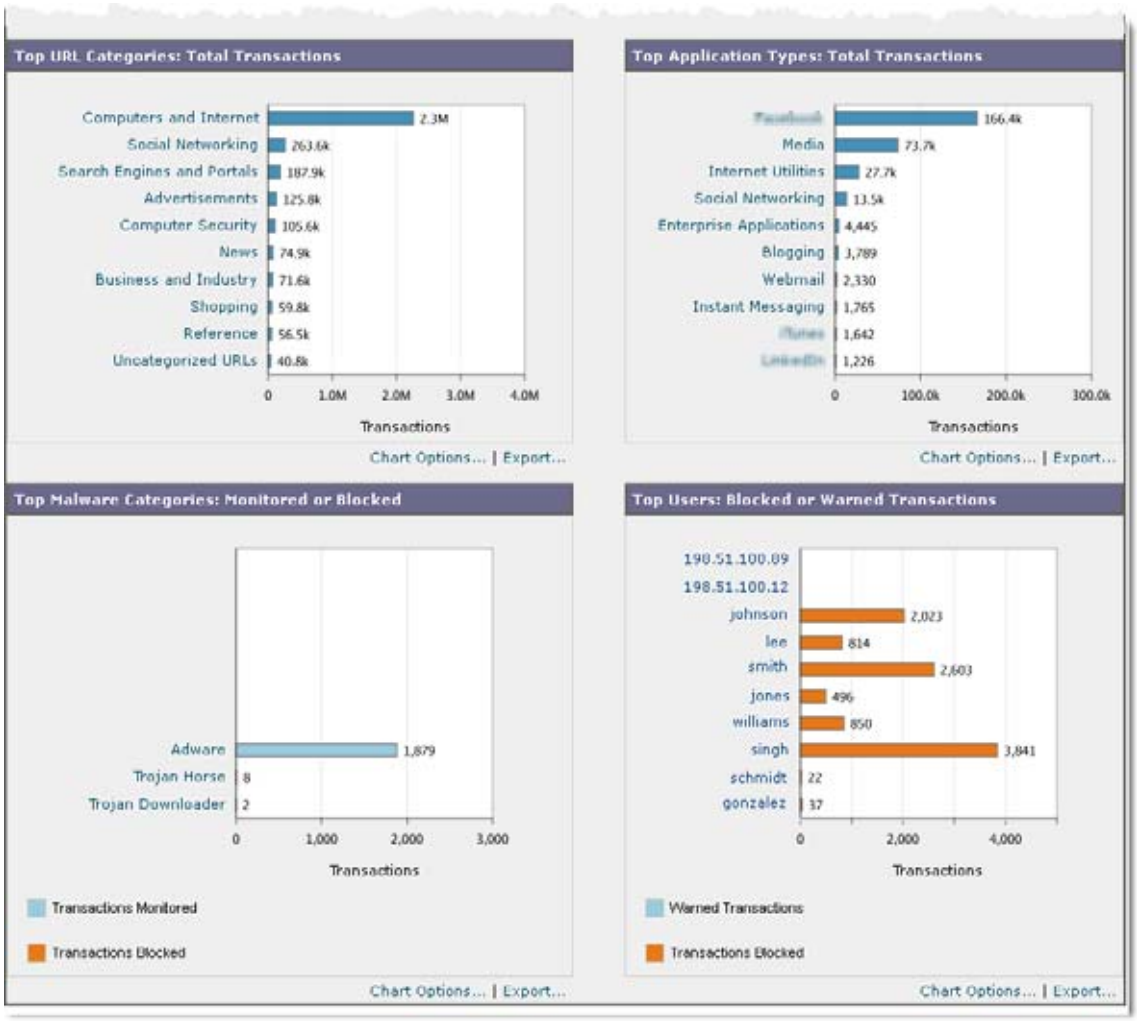
図 23-1 に、[概要（Overview）] ページを示します。

図 23-1　[概要（Overview）] ページ



（次のページに続く）

（前ページからの続き）



[概要（Overview）] ページの上部には、URL とユーザの使用量に関する統計情報、Web プロキシ アクティビティ、および各種トランザクション サマリーが表示されます。トランザクション サマリーには、さらに詳細なトレンド情報が示されます。たとえば、疑わしいトランザクションと、そのグラフの隣にそれらのトランザクションがブロックされた数、およびブロックされた方法が表示されます。

[概要（Overview）] ページの下半分は、使用状況に関する情報に使用されます。つまり、表示されている上位 URL カテゴリ、ブロックされている上位アプリケーション タイプおよびカテゴリ、これらのブロックまたは警告を生成している上位ユーザが表示されます。

表 23-1 で、[概要（Overview）] ページに表示される情報について説明します。

表 23-1　[概要（Overview）] ページのコンポーネント

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。詳細については、「時間範囲の変更」（P.22-3）を参照してください。
Web プロキシ アクティビティ総数（Total Web Proxy Activity）	このセクションでは、Web プロキシのアクティビティを表示します。このセクションには、トランザクションの実際の数（縦の目盛り）、および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）	このセクションでは、疑わしい Web プロキシ アクティビティまたは正常な Web プロキシ アクティビティの比率を、トランザクションの総数も含めて表示できます。
L4 トラフィック モニタの概要（L4 Traffic Monitor Summary）	このセクションでは、L4 トラフィック モニタによってモニタされ、ブロックされる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）	このセクションでは、さまざまなセキュリティ コンポーネントが疑わしいトランザクションと分類した Web トランザクションを表示できます。 このセクションには、トランザクションの実際の数（縦の目盛り）、および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。
疑わしいトランザクションの概要（Suspect Transactions Summary）	このセクションでは、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。また、検出されてブロックされたトランザクションのタイプ、およびそのトランザクションが実際にブロックされた回数を確認できます。
総トランザクション数別上位 URL カテゴリ（Top URL Categories by Total Transactions）	このセクションには、ブロックされた上位 10 の URL カテゴリが表示されます （縦の目盛りで URL カテゴリ、横の目盛りでそのカテゴリの要求がブロックされた回数）。 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。こうした更新によるレポート結果への影響については、「URL カテゴリ セットの更新とレポート」（P.23-12）を参照してください。
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、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 （縦の目盛りでアプリケーション タイプ、横の目盛りでそのタイプのアプリケーションの要求がブロックされた回数）。
検出された上位マルウェア カテゴリ（Top Malware Categories Detected）	このセクションには、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）	このセクションには、ブロックされたトランザクションまたは警告が発行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。 レポートで、ユーザ名を認識できないようにすることができます。実行方法の詳細については、「レポートでのユーザ名の使用」（P.22-1）を参照してください。

[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。

図 23-2 は、[ユーザ（Users）] ページを示しています。

図 23-2　[ユーザ（Users）] ページ

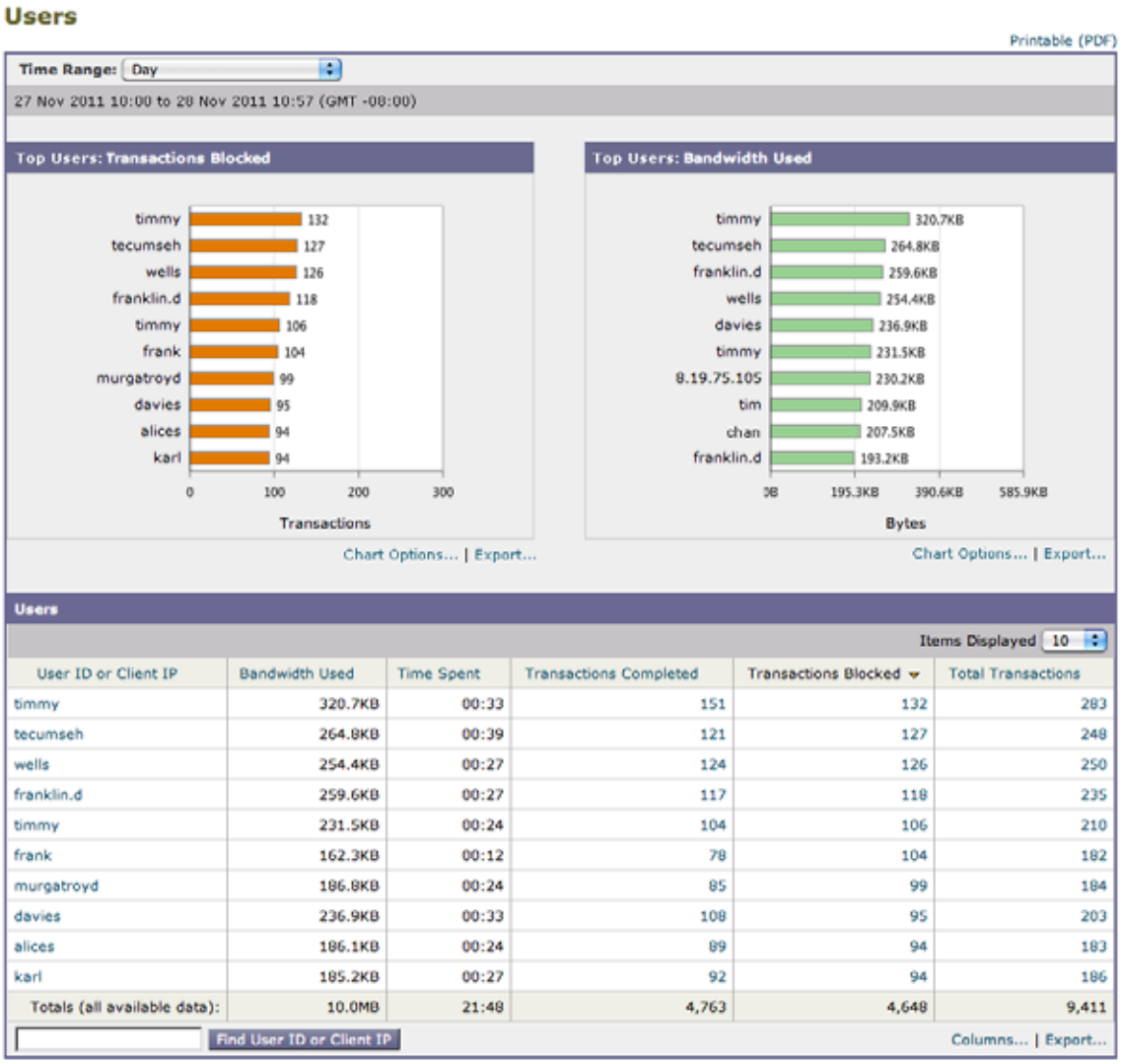


表 23-2 で、[ユーザ（Users）] ページに表示される情報について説明します。

表 23-2　[ユーザ（Users）] レポート ページのコンポーネント

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。詳細については、「時間範囲の変更」（P.22-3）を参照してください。
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）	このセクションには、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。 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。レポートで、ユーザ名を認識できないようにすることができます。実行方法の詳細については、「レポートでのユーザ名の使用」（P.22-1）を参照してください。
使用した帯域幅別上位ユーザ（Top Users by Bandwidth Used）	このセクションには、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）で表示されます。
ユーザ テーブル（Users Table）	[ユーザ テーブル（Users Table）] は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。カラム見出しをクリックしてテーブルをソートし、表示するデータ カラムを選択できます。詳細については、「レポート ページのカラムの使用」（P.22-4）を参照してください。 セクションに 10 人以上のユーザが含まれている場合、[表示された項目（Items Displayed）] メニューを使用して表示するユーザ数を設定できます。 [ユーザ ID またはクライアント IP アドレスの検索（Find User ID or Client IP Address）] フィールドで、特定のユーザのデータを検索できます。詳細については、「データの検索」（P.22-3）を参照してください。 テーブル内のユーザをクリックして、より詳細な情報を検索できます。この情報は、[ユーザの詳細（User Details）] ページに表示されます。詳細については、「[ユーザの詳細（User Details）] ページ」（P.23-6）を参照してください。

[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。

[ユーザの詳細（User Details）] ページでは、ネットワーク上の個々のユーザのアクティビティを調査することができます。ユーザ レベルの調査を実行し、ユーザが閲覧しているサイト、直面しているマルウェア脅威、アクセスしている URL カテゴリ、およびユーザがこれらのサイトで費やしている時間などを調べる必要がある場合、この情報を表示する場合があります。

ユーザの [ユーザの詳細（User Details）] ページを表示するには、[レポート（Reporting）] > [ユーザ（Users）] ページの [ユーザ テーブル（Users Table）] でユーザをクリックします。表 23-3 で、[ユーザの詳細（User Details）] ページに表示される情報について説明します。

表 23-3　[ユーザ（Users）] > [ユーザの詳細（User Details）] レポート ページのコンポーネント

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。詳細については、「時間範囲の変更」（P.22-3）を参照してください。
総トランザクション数別 URL カテゴリ（URL Categories by Total Transactions）	このセクションには、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。 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。こうした更新によるレポート結果への影響については、「URL カテゴリ セットの更新とレポート」（P.23-12）を参照してください。
総トランザクション数別トレンド（Trend by Total Transaction）	このグラフには、ユーザが Web にいつアクセスしたかが表示されます。 たとえば、1 日の特定の時刻に Web トラフィックに大きなスパイクが存在するかどうか、また、それらのスパイクがいつ発生したかが、このグラフからわかります。[時間範囲（Time Range）] ドロップダウン リストを使用すると、このグラフを拡張し、このユーザが Web を閲覧していた時間を表示するきめ細かさを増減できます。
一致した URL カテゴリ（URL Categories Matched）	このセクションには、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関して、指定した時間範囲内の一致したすべての URL カテゴリが表示されます。カラム見出しを使用して、データをソートできます。セクションに 10 以上のカテゴリが含まれている場合、[表示された項目（Items Displayed）] メニューを使用して表示する URL カテゴリを設定できます。 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。こうした更新によるレポート結果への影響については、「URL カテゴリ セットの更新とレポート」（P.23-12）を参照してください。 このセクションで、[URL カテゴリの検索（Find URL Category）] フィールドで特定の URL カテゴリに適用するデータを検索することもできます。詳細については、「データの検索」（P.22-3）を参照してください。
一致したドメイン（Domains Matched）	このセクションでは、このユーザがアクセスした特定のドメインまたは IP アドレスを確認できます。また、ユーザがこれらのカテゴリで費やした時間、およびカラム ビューで設定したその他のさまざまな情報も参照できます。セクション下部のテキスト フィールドにドメインまたは IP アドレスを入力し、[ドメインまたは IP の検索（Find Domain or IP）] をクリックします。ドメインまたは IP アドレスは正確に一致している必要はありません。

表 23-3　[ユーザ（Users）] > [ユーザの詳細（User Details）] レポート ページのコンポーネント （続き）

セクション	説明
一致したアプリケーション（Applications Matched）	このセクションで、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を検索できます。たとえば、Flash ビデオを多用するサイトにユーザがアクセスしている場合は、[アプリケーション（Application）] カラムにそのアプリケーション タイプが表示されます。 セクション下部のテキスト フィールドにアプリケーション名を入力し、[アプリケーションの検索（Find Application）] をクリックします。アプリケーションの名前は正確に一致している必要はありません。
検出されたマルウェア脅威（Malware Threats Detected）	このテーブルでは、特定のユーザがトリガーしている上位のマルウェア脅威を確認できます。[マルウェア脅威（Malware Threats）] セクション下部のテキスト フィールドにマルウェア脅威の名前を入力し、[マルウェア脅威の検索（Find Malware Threat）] をクリックします。マルウェア脅威の名前は正確に一致している必要はありません。
一致したポリシー（Policies Matched）	このセクションでは、この特定のユーザに適用されている特定のポリシーを検索できます。 このセクションで、[ポリシーの検索（Find Policy）] フィールドで特定のポリシーに適用するデータを検索することもできます。詳細については、「データの検索」（P.22-3）を参照してください。

（注）　クライアント レポートで、ユーザ名の末尾にアスタリスク（*）が表示されることがあります。たとえば、クライアント レポートに「jsmith」と「jsmith*」の両方のエントリが表示される場合があります。アスタリスク（*）が付いているユーザ名は、ユーザの指定したユーザ名が認証サーバで確認されていないことを示しています。この状況は、認証サーバがその時点で使用できず、かつ認証サービスを使用できないときもトラフィックを許可するようにアプライアンスが設定されている場合に発生します。

[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。このページでは、特定の時間範囲内にアクセスされたリスクの高い Web サイトをモニタできます。

図 23-3 は、[Web サイト（Web Sites）] ページを示します。

図 23-3　[Web サイト（Web Sites）] ページ

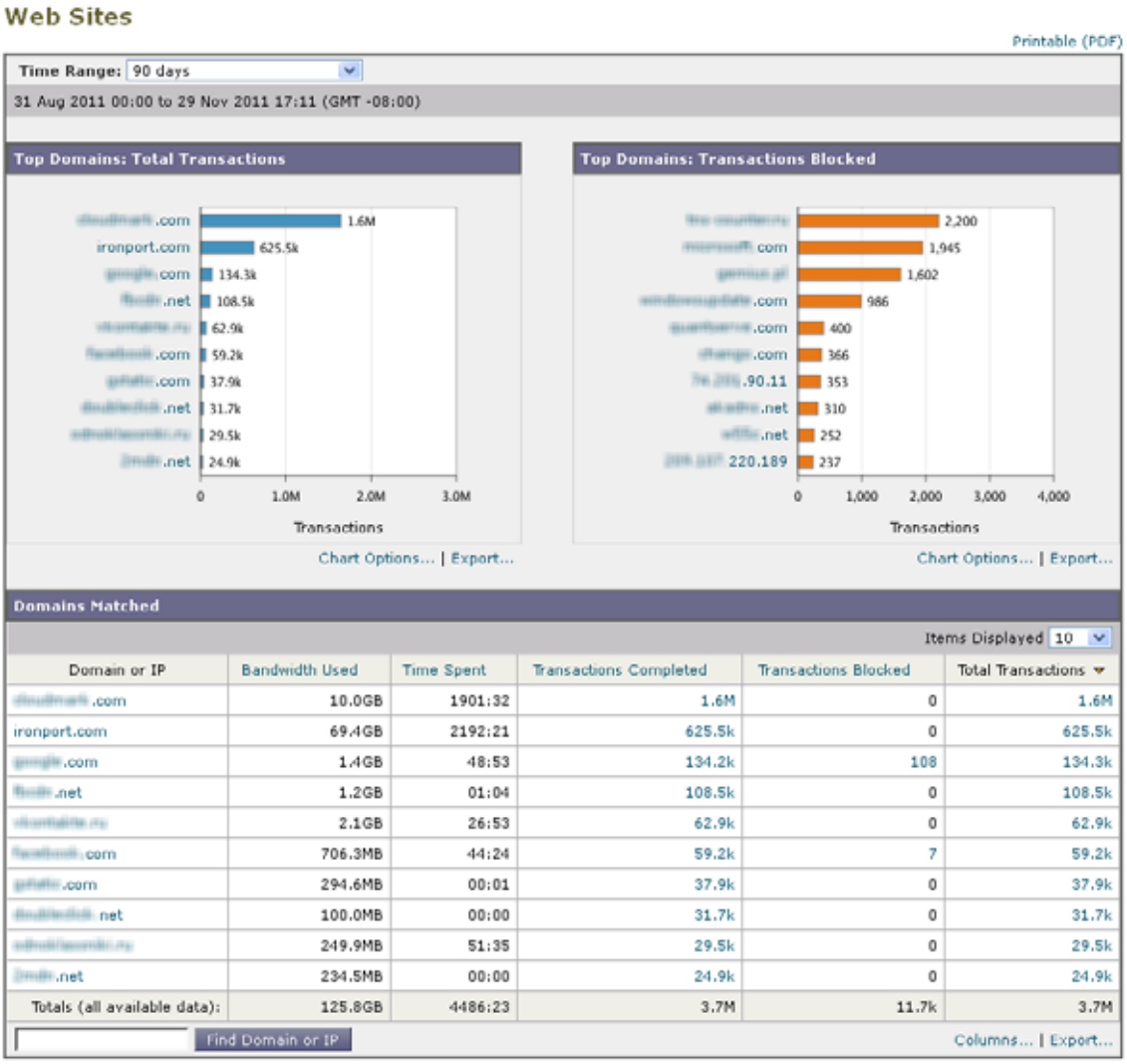


表 23-4 で、[Web サイト（Web Sites）] ページに表示される情報を説明します。

表 23-4　[Web サイト（Web Sites）] レポート ページのコンポーネント

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。詳細については、「時間範囲の変更」（P.22-3）を参照してください。
総トランザクション数別上位ドメイン（Top Domains 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ドメインがグラフ形式で表示されます。

表 23-4　[Web サイト（Web Sites）] レポート ページのコンポーネント （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ドメイン（Top Domains by Transactions Blocked）	このセクションには、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。たとえば、ユーザがあるドメインにアクセスしたが、特定のポリシーが適用されていたために、ブロック アクションがトリガーされたとします。このドメインはブロックされたトランザクションとしてこのグラフに追加され、ブロック アクションをトリガーしたドメイン サイトが表示されます。
一致したドメイン（Domains Matched）	このセクションでは、サイト上で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。このテーブルでは、特定のドメインをクリックすることで、そのドメインに関するさらに詳細な情報にアクセスできます。[Web トラッキング（Web Tracking）] ページに [プロキシ サービス（Proxy Services）] タブが表示され、トラッキング情報と、特定のドメインがブロックされた理由を確認できます。 カラム見出しを使用してデータをソートし、表示するカラムを選択できます。詳細については、「レポート ページのカラムの使用」（P.22-4）を参照してください。 セクションに 10 以上のドメインが含まれている場合、[表示された項目（Items Displayed）] メニューを使用して表示するドメイン数を設定できます。 特定のドメインをクリックすると、そのドメインの上位ユーザ、そのドメインでの上位トランザクション、一致した URL カテゴリ、および検出されたマルウェアの脅威が表示されます。[時間範囲（Time Range）] ドロップダウン リストを使用して、特定の時間範囲（時間、日、または週）でドメインの使用状況が表示されるようにこのテーブルを変更できます。

[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。

（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。こうした更新によるレポート結果への影響については、「URL カテゴリ セットの更新とレポート」（P.23-12）を参照してください。

図 23-4 は、[URL カテゴリ（URL Categories）] ページを示します。

図 23-4　[URL カテゴリ（URL Categories）] ページ

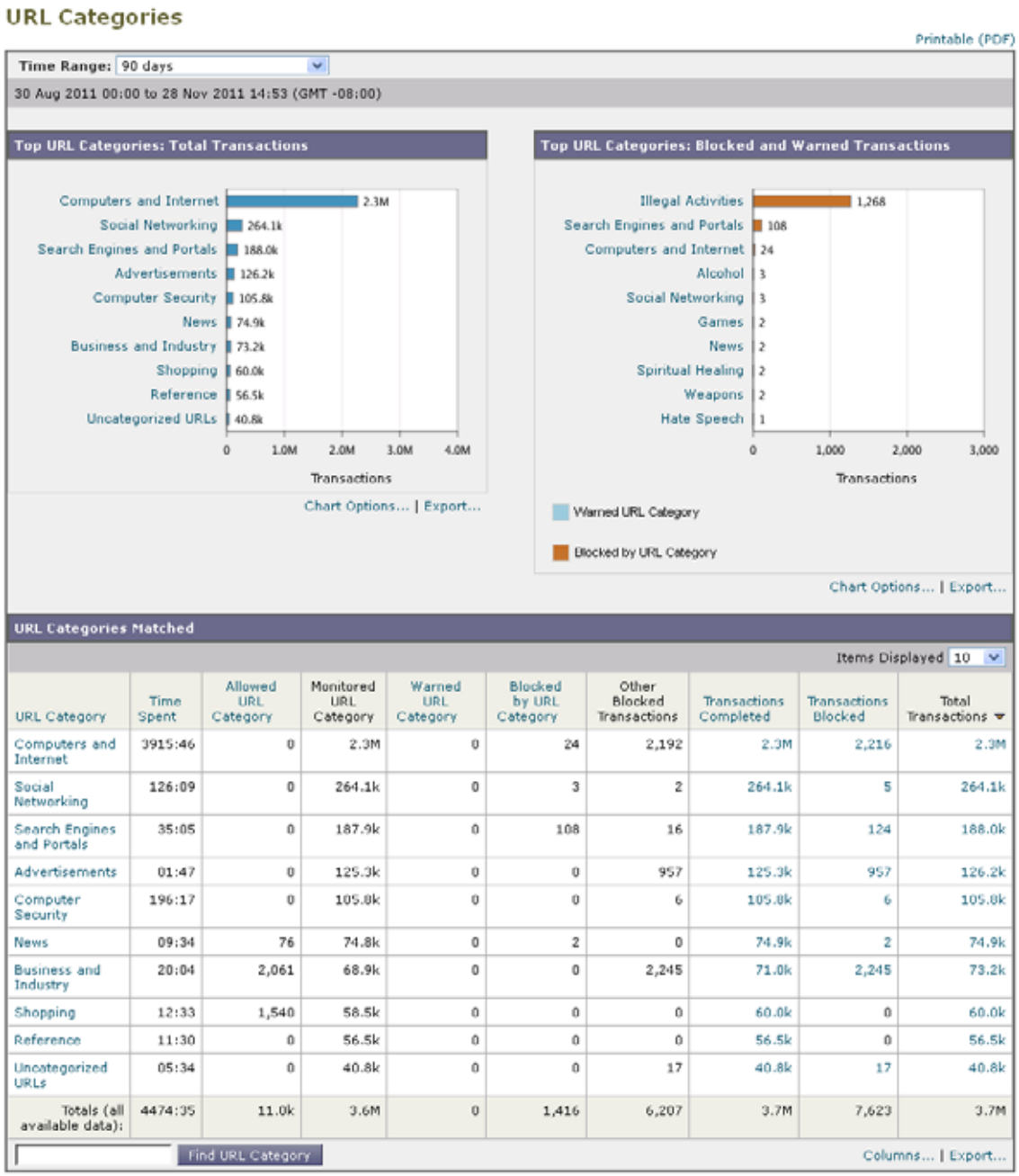


表 23-5 で、[URL カテゴリ（URL Categories）] ページに表示される情報を説明します。

表 23-5　[URL カテゴリ（URL Categories）] レポート ページのコンポーネント

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。詳細については、「時間範囲の変更」（P.22-3）を参照してください。
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。

表 23-5　[URL カテゴリ（URL Categories）] レポート ページのコンポーネント （続き）

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）	このセクションには、トランザクションごとに発生するブロック アクション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。たとえば、ユーザがある URL にアクセスしたが、特定のポリシーが適用されているために、ブロック アクションまたは警告がトリガーされたとします。この URL は、ブロックまたは警告されたトランザクションとしてこのグラフに追加されます。
一致した URL カテゴリ（URL Categories Matched）	[一致した URL カテゴリ（URL Categories Matched）] セクションには、指定した時間範囲内における URL カテゴリ別のトランザクションの処理、使用された帯域幅、各カテゴリで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。詳細については、「カスタム URL カテゴリの作成および編集」（P.17-16）を参照してください。 • 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。「未分類の URL と誤って分類された URL の報告」（P.17-3）を参照してください。 • 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。多くの場合、疑わしいコンテンツを含む URL とマルウェアの相関性は高く、今後のフィルタで検出される可能性が高くなります。URL フィルタリングで判定できない場合は、他のダウンストリーム フィルタで悪質なトラフィックが検出されるように、システム パイプラインが設定されます。

URL カテゴリ セットの更新とレポート

「URL カテゴリのセットに対する更新の管理」（P.17-5）で説明されているように、Web セキュリティ アプライアンスでは一連の定義済み URL カテゴリが定期的かつ自動的に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。

古いカテゴリと新しいカテゴリの間で重複した箇所がある場合、有効な統計情報を得るために、より注意深くレポート結果を検証する必要が生じることがあります。たとえば、調査対象のタイム フレーム内に「Instant Messaging」カテゴリと「Web-based Chat」カテゴリが「Chat and Instant Messaging」という 1 つのカテゴリにマージされていた場合、「Instant Messaging」および「Web-based Chat」カテゴリに対応するサイトへのマージ前のアクセスは「Chat and Instant Messaging」の合計数にカウントされません。同様に、インスタント メッセージング サイトまたは Web ベース チャット サイトへのマージ後のアクセスは、「Instant Messaging」または「Web-based Chat」カテゴリの合計数には含まれません。

[URL カテゴリ（URL Categories）] ページとその他のレポーティング ページの併用

[URL カテゴリ（URL Categories）] ページの利点の 1 つは、[アプリケーションの表示（Application Visibility）] ページおよび [ユーザ（Users）] ページと組み合わせて使用して、特定のユーザだけでなく、特定のユーザがアクセスを試みているアプリケーションまたは Web サイトのタイプも調査できることです。

たとえば、[URL カテゴリ（URL Categories）] ページで、サイトからアクセスされたすべての URL カテゴリの詳細を表示する、人事部門向けの概要レポートを生成できます。同じページの [URL カテゴリ（URL Categories）] インタラクティブ テーブルでは、URL カテゴリ「Streaming Media」に関するさらに詳しい情報を収集できます。[ストリーミング メディア（Streaming Media）] カテゴリ リンクをクリックすると、特定の [URL カテゴリ（URL Categories）] レポート ページが表示されます。このページには、ストリーミング メディア サイトにアクセスしている上位ユーザが表示されるだけでなく（[総トランザクション数のカテゴリ別上位ユーザ（Top Users by Category for Total Transactions）] セクション）、YouTube.com や QuickPlay.com などのアクセスされたドメインも表示されます（[一致したドメイン（Domains Matched）] インタラクティブ テーブル）。

この時点で、特定のユーザに関するさらに詳しい情報を得られます。たとえば、特定のユーザによる使用が突出しているので、そのユーザのアクセス先を正確に確認する必要があるとします。ここから、[ユーザ（Users）] テーブルのユーザをクリックすることができます。このアクションにより [ユーザの詳細（User Details）] ページが表示され、そのユーザのトレンドを確認し、そのユーザの Web での行動を正確に把握できます。

さらに詳しい情報が必要な場合は、インタラクティブ テーブルで [完了したトランザクション（Transactions Completed）] リンクをクリックして、Web トラッキングの詳細を表示できます。これにより、[Web トラッキング（Web Tracking）] ページに 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が表示され、ユーザがサイトにアクセスした日付、完全な URL、その URL で費やされた時間などについて、実際の詳細情報を確認できます。

[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。

図 23-5 は、[アプリケーションの表示（Application Visibility）] ページを示します。

図 23-5　[アプリケーションの表示（Application Visibility）] ページ

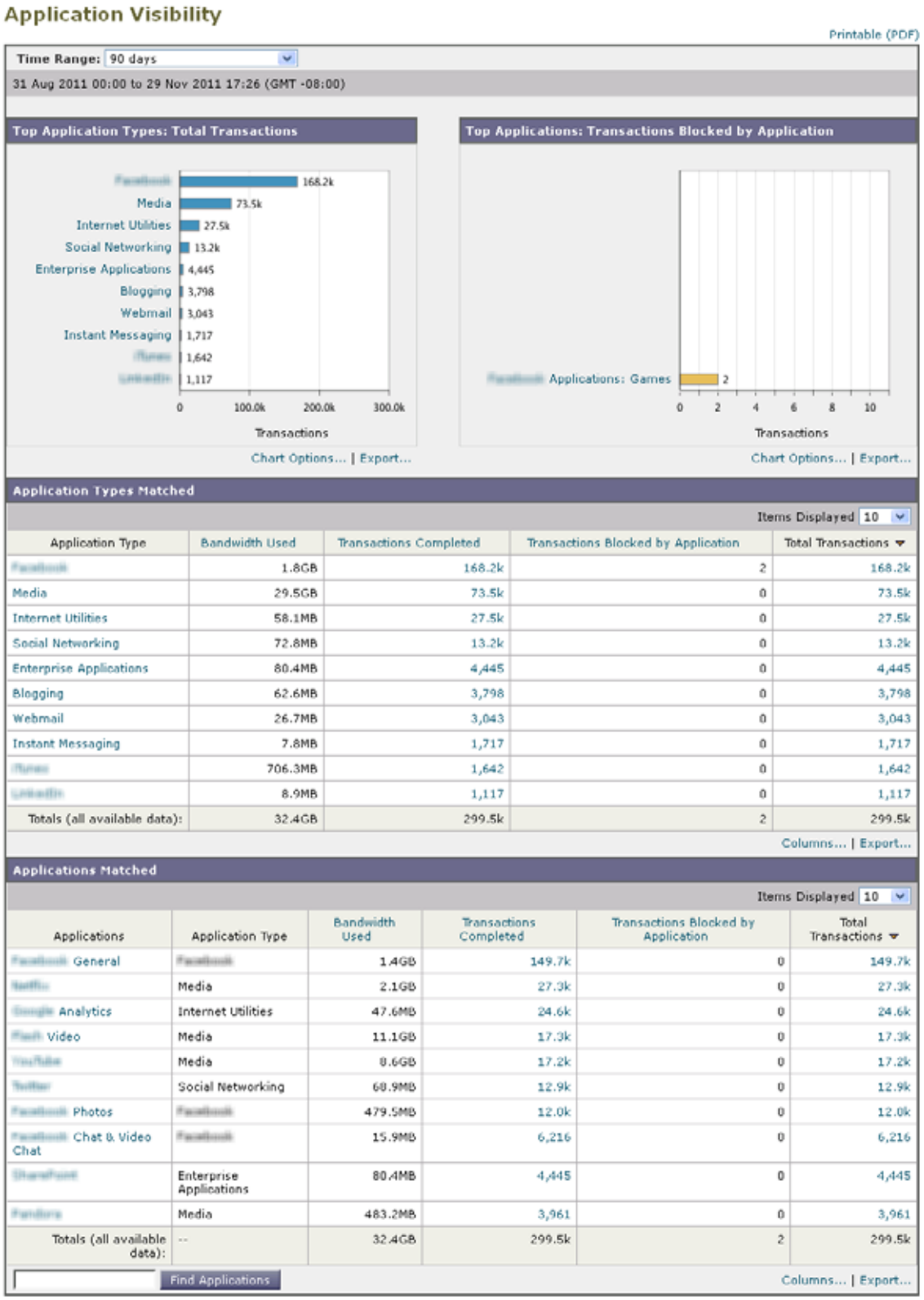


表 23-6 で、[アプリケーションの表示（Application Visibility）] ページに表示される情報を説明します。

表 23-6　[アプリケーションの表示（Application Visibility）] レポート ページのコンポーネント

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。詳細については、「時間範囲の変更」（P.22-3）を参照してください。
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。たとえば、Yahoo Instant Messenger などのインスタント メッセージング ツール、Presentation というアプリケーション タイプが表示されます。
ブロックされたトランザクション数別上位アプリケーション（Top Applications by Blocked Transactions）	このセクションには、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。たとえば、ユーザが Google Talk などの特定のアプリケーションを起動しようとし、設定済みポリシーによって、ブロック アクションがトリガーされました。このアプリケーションは、ブロックまたは警告されたトランザクションとしてこのグラフに追加されます。
一致したアプリケーション タイプ（Application Types Matched）	[一致したアプリケーション タイプ（Application Types Matched）] テーブルでは、[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 タイプに関するさらに詳しい情報を表示できます。[アプリケーション（Applications）] カラムで、詳細を表示するアプリケーションをクリックできます。
一致したアプリケーション（Applications Matched）	[一致したアプリケーション（Applications Matched）] セクションには、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。 カラム見出しをクリックしてテーブルをソートし、表示するデータ カラムを選択できます。詳細については、「レポート ページのカラムの使用」（P.22-4）を参照してください。 セクションに 10 以上のアプリケーションが含まれている場合、[表示された項目（Items Displayed）] メニューを使用して表示するアプリケーション数を設定できます。 [アプリケーションの検索（Find Application）] フィールドで、特定のアプリケーションのデータを検索できます。詳細については、「データの検索」（P.22-3）を参照してください。

[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。

図 23-6 は、[マルウェア対策（Anti-Malware）] ページを示します。

図 23-6　[マルウェア対策（Anti-Malware）] ページ

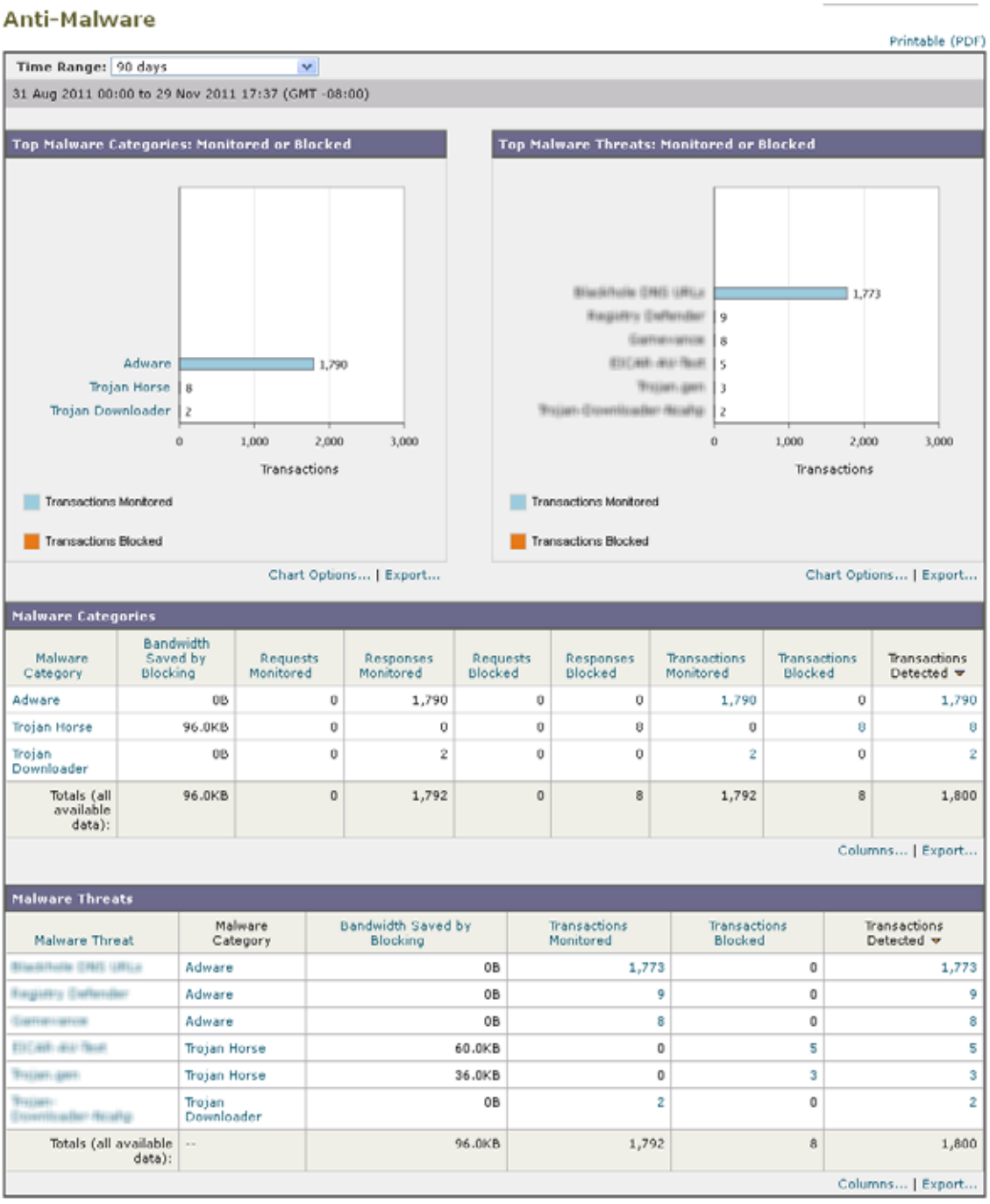


表 23-7 で、[マルウェア対策（Anti-Malware）] ページに表示される情報を説明します。

表 23-7　[マルウェア対策（Anti-Malware）] レポート ページのコンポーネント

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。詳細については、「時間範囲の変更」（P.22-3）を参照してください。
検出された上位マルウェア カテゴリ（Top Malware Categories Detected）	このセクションには、DVS エンジンによって検出された上位マルウェア カテゴリが表示されます。この情報はグラフ形式で表示されます。
検出された上位マルウェア脅威（Top Malware Threats Detected）	このセクションには、DVS エンジンによって検出された上位マルウェア脅威が表示されます。この情報はグラフ形式で表示されます。
マルウェア カテゴリ（Malware Categories）	[マルウェア カテゴリ（Malware Categories）] テーブルには、[検出された上位マルウェア脅威（Top Malware Threats Detected）] セクションに表示されている個々のマルウェア カテゴリに関する詳細情報が表示されます。 このテーブル内のリンクをクリックすると、個々のマルウェア カテゴリおよびネットワークでの検出場所に関するさらに詳しい情報が表示されます。
マルウェア脅威（Malware Threats）	[マルウェア脅威（Malware Threats）] テーブルには、[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個々のマルウェアの脅威に関する詳細情報が表示されます。 「Outbreak」のラベルと番号が付いている脅威は、他のスキャン エンジンとは別に、Adaptive Scanning 機能によって特定された脅威です。 **（注）** [マルウェア脅威（Malware Threats）] でテーブルを昇順にソートすると、リストの最上部に [名前のないマルウェア（Unnamed Malware）] が表示されます。

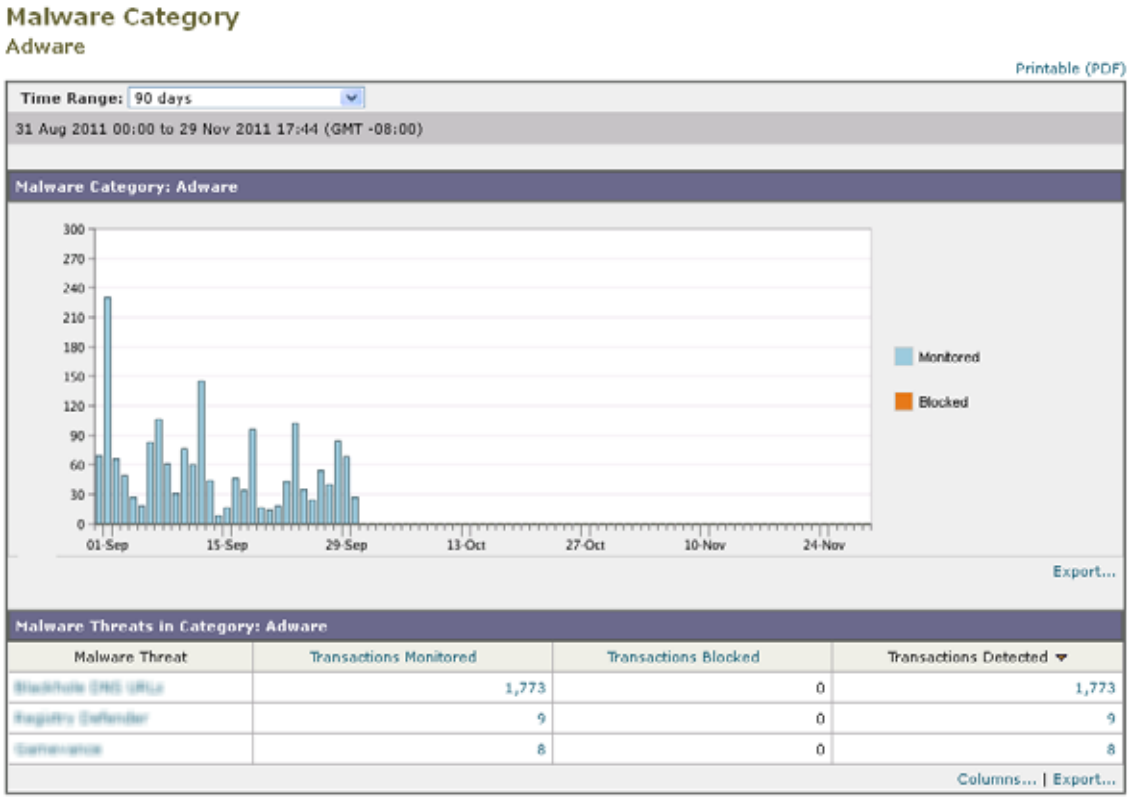
[マルウェア カテゴリ（Malware Category）] レポート ページ

[マルウェア カテゴリ（Malware Category）] レポート ページでは、個々のマルウェア カテゴリとネットワークでのその動作に関する詳細情報を表示できます。

ステップ 1　[レポート（Reporting）] > [マルウェア対策（Anti-Malware）] ページに移動します。

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。

図 23-7　[マルウェア カテゴリ（Malware Category）] レポート ページ



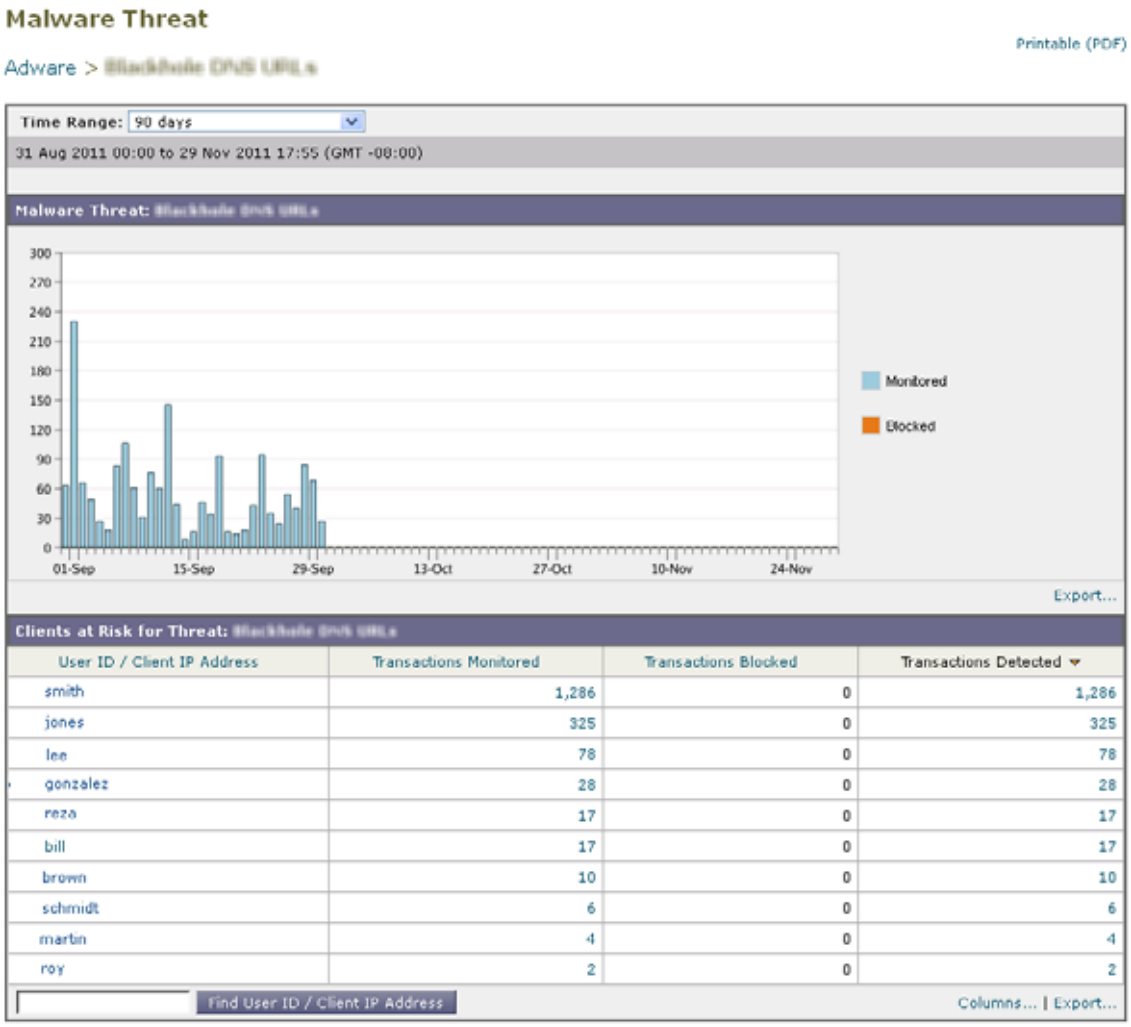
[マルウェア脅威（Malware Threats）] レポート ページ

[マルウェア脅威（Malware Threats）] レポート ページには、特定の脅威にさらされているクライアント、および感染した可能性があるクライアントのリストが表示され、[クライアントの詳細（Client Detail）] ページへのリンクがあります。レポート上部のトレンド グラフには、指定した時間範囲内で脅威に関してモニタされたトランザクションおよびブロックされたトランザクションが表示されます。下部のテーブルには、指定した時間範囲内で脅威に関してモニタされたトランザクションおよびブロックされたトランザクションの実際の数が表示されます。

ステップ 1　[レポート（Reporting）] > [マルウェア対策（Anti-Malware）] ページに移動します。

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。

図 23-8　[マルウェア脅威（Malware Threats）] レポート ページ



[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）] ページでは、システム管理者が最も多くブロックまたは警告を受けているユーザを確認できます。このページで収集された情報から、管理者はユーザ リンクをクリックして、そのユーザが多数のブロックや警告を受けている原因、およびネットワーク上の他のユーザよりも多く検出されている原因となっているユーザの行動を確認できます。

さらに [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。マルウェア サイトに頻繁に接続するコンピュータは、マルウェアに感染している可能性があります。これらのマルウェアは中央のコマンド/コントロール サーバに接続しようとするので、除去しなければなりません。

図 23-9 に [クライアント マルウェア リスク（Client Malware Risk）] ページを示します。

図 23-9　[クライアント マルウェア リスク（Client Malware Risk）] ページ

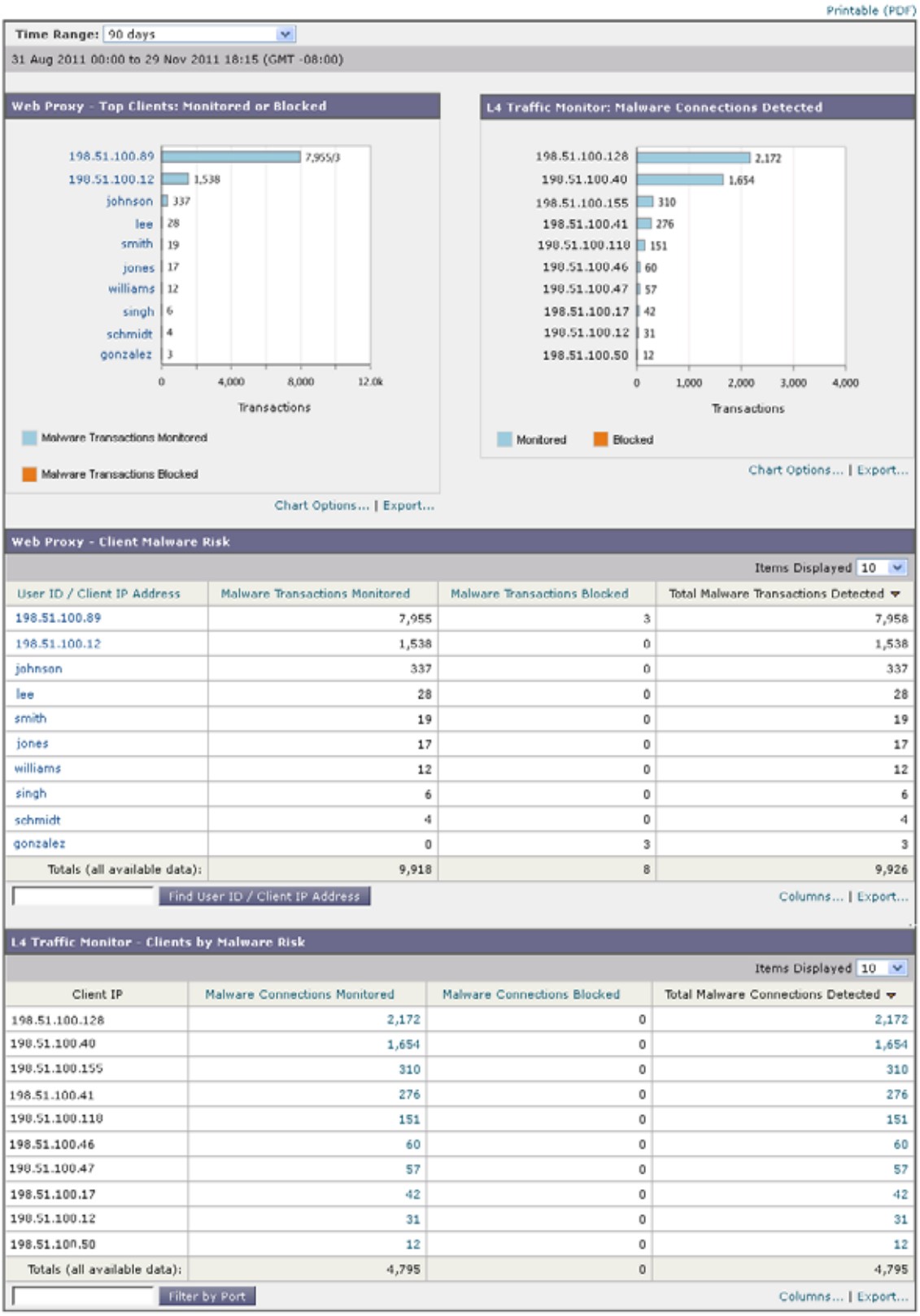


表 23-8 で [クライアント マルウェア リスク（Client Malware Risk）] ページの情報について説明します。

表 23-8　[クライアント マルウェア リスク（Client Malware Risk）] レポート ページの内容

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。詳細については、「時間範囲の変更」（P.22-3）を参照してください。
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。
L4 トラフィック モニタ：検出されたマルウェア接続（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。 このチャートは「[L4 トラフィック モニタ（L4 Traffic Monitor）] ページ」（P.23-25）の [上位クライアント IP（Top Client IPs）] チャートと同じです。詳細およびチャート オプションについてはこの項を参照してください。
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。 このテーブルの各ユーザをクリックして、各ユーザの詳細情報が記載された [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）] ページを開くことができます。詳細については、「[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」（P.23-23）を参照してください。 テーブルで任意のリンクをクリックすると、個々のユーザと、マルウェアのリスクをトリガーしているそのユーザのアクティビティをさらに詳しく表示できます。たとえば [ユーザ ID/クライアント IP アドレス（User ID / Client IP Address）] カラムのリンクをクリックすると、そのユーザの [ユーザ（User）] ページに移動します。
L4 トラフィック モニタ：マルウェア リスク別クライアント（L4 Traffic Monitor: Clients by Malware Risk）	このテーブルには、組織内でマルウェア サイトに頻繁にアクセスしているコンピュータの IP アドレスが表示されます。 このテーブルは「[L4 トラフィック モニタ（L4 Traffic Monitor）] ページ」（P.23-25）の [クライアント ソース IP（Client Source IPs）] テーブルと同じです。テーブルの操作についてはこの項を参照してください。

[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）] ページでは、[クライアント マルウェア リスク（Client Malware Risk）] ページの [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）] テーブルのエントリに、指定した時間範囲の特定のクライアントに対するすべての Web アクティビティとマルウェア リスク の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）] ページに移動します。

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）] カラムのユーザをクリックします。

このページのアイテムの詳細については、「[ユーザの詳細（User Details）] ページ」（P.23-6）を参照してください。

[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。

図 23-10 は、[Web レピュテーション フィルタ（Web Reputation Filters）] ページを示します。

図 23-10　[Web レピュテーション フィルタ（Web Reputation Filters）] ページ

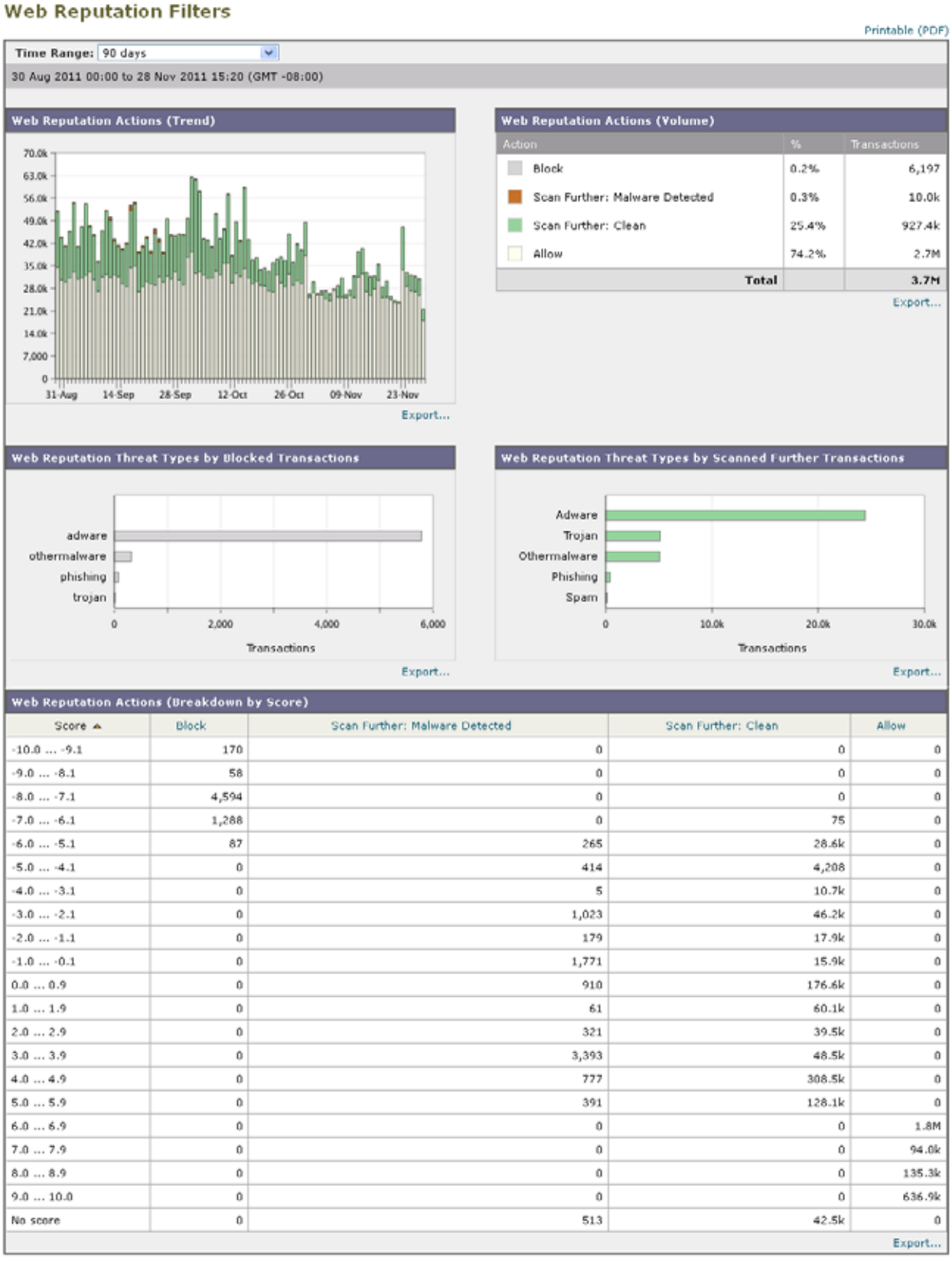


表 23-9 で、[Web レピュテーション フィルタ（Web Reputation Filters）] ページに表示される情報を説明します。

表 23-9　[Web レピュテーション フィルタ（Web Reputation Filters）] レポート ページのコンポーネント

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。詳細については、「時間範囲の変更」（P.22-3）を参照してください。
Web レピュテーション アクション（トレンド）（Web Reputation Actions (Trend)）	このセクションには、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。このセクションでは、時間の経過に伴う Web レピュテーション アクションの潜在的なトレンドを確認できます。
Web レピュテーション アクション（ボリューム）（Web Reputation Actions (Volume)）	このセクションには、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の比率で表示されます。
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）	このセクションには、低レピュテーション スコアの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）	このセクションには、トランザクションをスキャンするように指定されたレピュテーション スコアに基づく脅威タイプが表示されます。モニタされるトランザクションとブロックされるトランザクションの両方が表示されます。
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)）	このインタラクティブ テーブルには、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

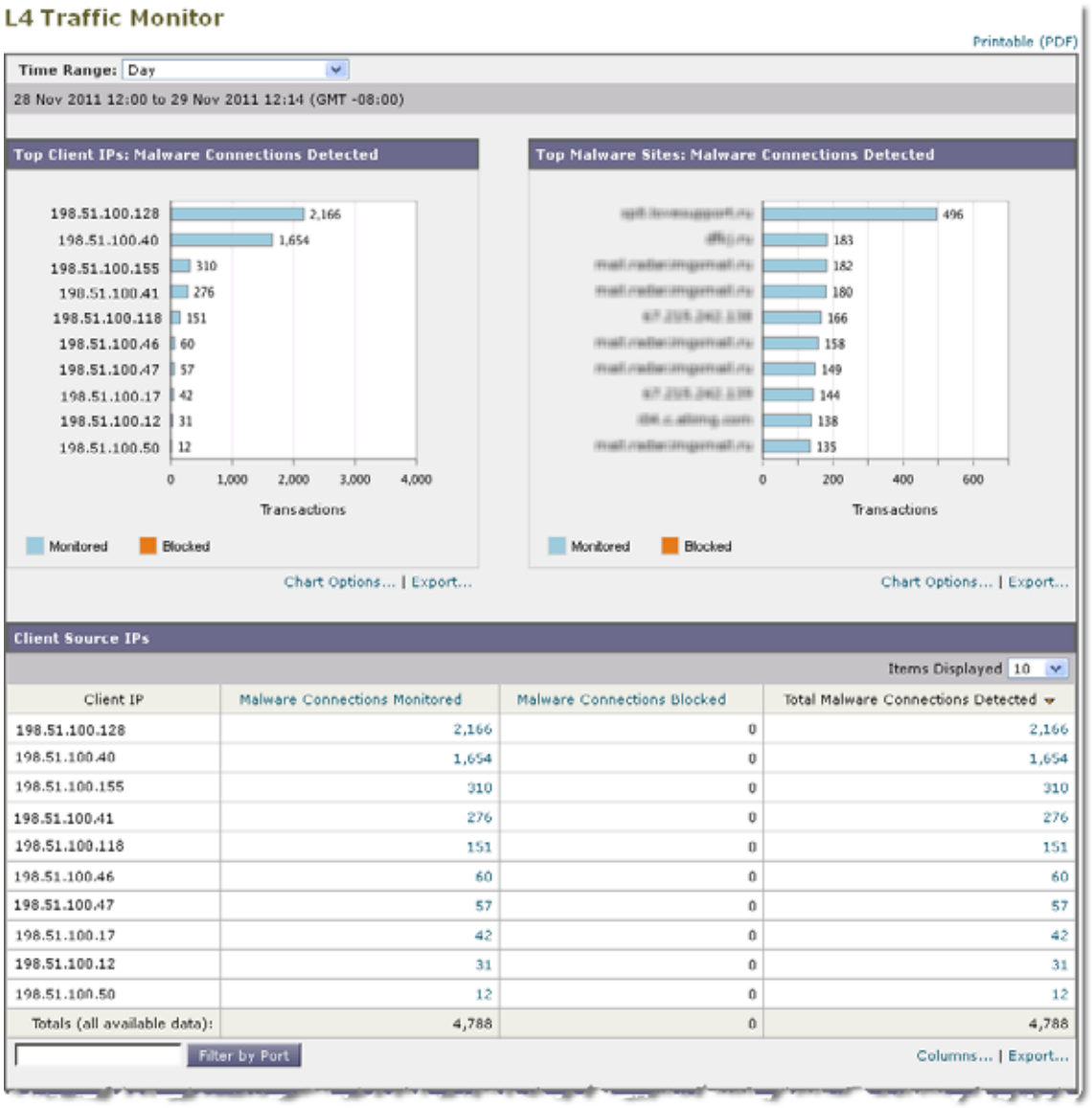
[レポート（Reporting）] > [L4 トラフィック モニタ（L4 Traffic Monitor）] ページは、指定した時間範囲内に L4 トラフィック モニタが検出したマルウェア ポートとマルウェア サイトに関する情報を表示する、セキュリティ関連のレポーティング ページです。マルウェア サイトに頻繁にアクセスしているクライアントの IP アドレスも表示されます。

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、着信トラフィックと発信トラフィックを許可するかどうかを決定します。

このレポートのデータを使用して、ポートまたはサイトをブロックするかどうかを判断したり、特定のクライアント IP アドレスが著しく頻繁にマルウェア サイトに接続している理由（たとえば、その IP アドレスに関連付けられたコンピュータが、中央のコマンド/コントロール サーバに接続しようとするマルウェアに感染しているなど）を調査したりできます。

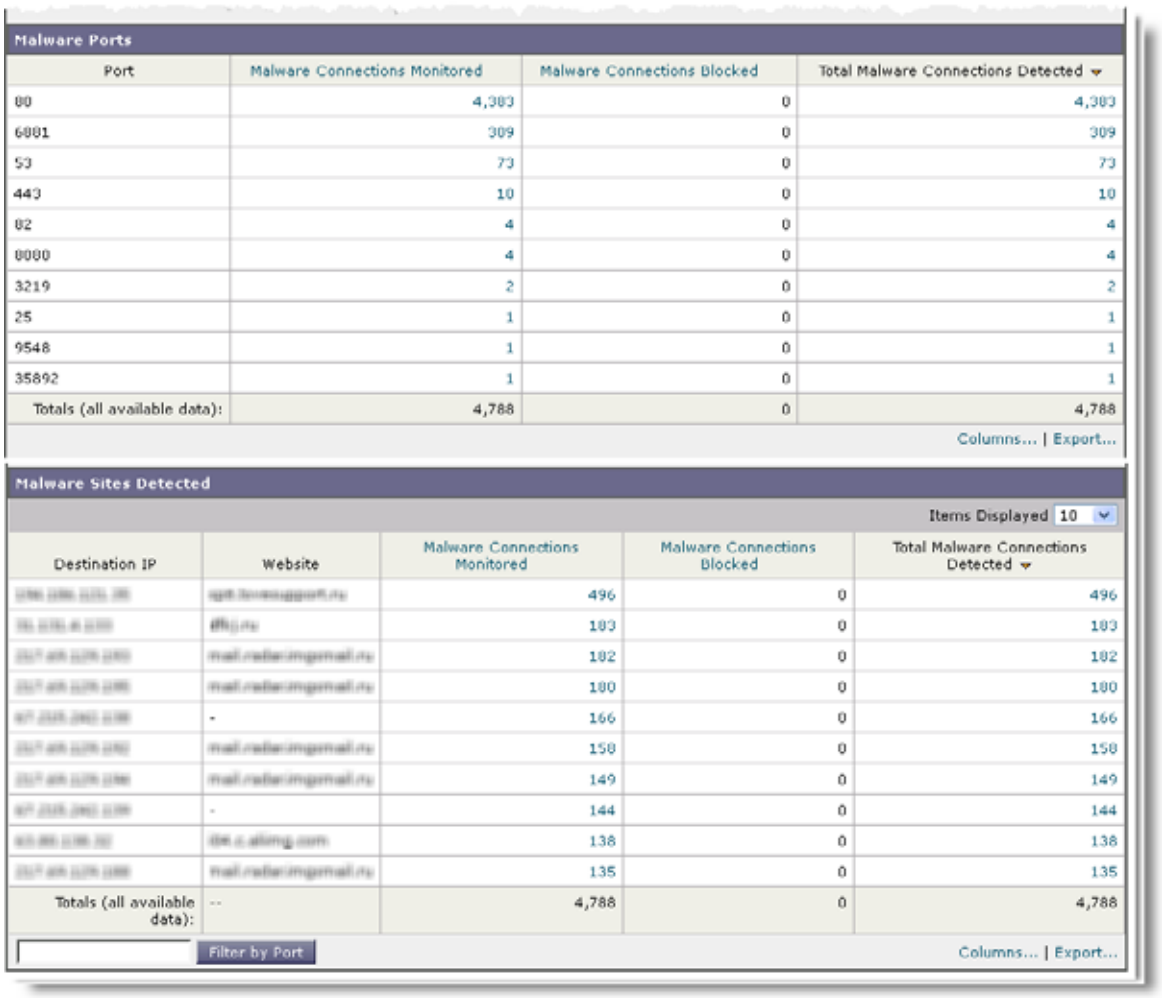
図 23-11 に [L4 トラフィック モニタ（L4 Traffic Monitor）] ページを示します。

図 23-11　[L4 トラフィック モニタ（L4 Traffic Monitor）] ページ



（次のページに続く）

（前ページからの続き）



Malware Ports

Port	Malware Connections Monitored	Malware Connections Blocked	Total Malware Connections Detected
80	4,303	0	4,303
6881	309	0	309
53	73	0	73
443	10	0	10
82	4	0	4
8080	4	0	4
3219	2	0	2
25	1	0	1
9548	1	0	1
35892	1	0	1
Totals (all available data):	4,788	0	4,788

Columns... | Export...

Malware Sites Detected

Items Displayed 10

Destination IP	Website	Malware Connections Monitored	Malware Connections Blocked	Total Malware Connections Detected
[redacted]	[redacted]	496	0	496
[redacted]	[redacted]	103	0	103
[redacted]	[redacted]	102	0	102
[redacted]	[redacted]	100	0	100
[redacted]	-	166	0	166
[redacted]	[redacted]	150	0	150
[redacted]	[redacted]	149	0	149
[redacted]	-	144	0	144
[redacted]	[redacted]	138	0	138
[redacted]	[redacted]	135	0	135
Totals (all available data):	--	4,788	0	4,788

Filter by Port

Columns... | Export...

表 23-10 で [L4 トラフィック モニタ（L4 Traffic Monitor）] ページに表示される情報を説明します。

表 23-10　[L4 トラフィック モニタ（L4 Traffic Monitor）] レポート ページの内容

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。詳細については、「時間範囲の変更」（P.22-3）を参照してください。
上位クライアント IP（Top Client IPs）	このセクションには、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 アドレスがグラフ形式で表示されます。 チャートの下の [チャート オプション（Chart Options）] リンクをクリックすると、表示を総合的な [検出されたマルウェア接続] から [モニタされたマルウェア接続（Malware Connections Monitored）] または [ブロックされたマルウェア接続（Malware Connections Blocked）] に変更できます。 このチャートは、「[クライアント マルウェア リスク（Client Malware Risk）] ページ」（P.23-19）の [L4 トラフィック モニタ：検出されたマルウェア接続（L4 Traffic Monitor: Malware Connections Detected）] チャートと同じです。
上位マルウェア サイト（Top Malware Sites）	このセクションには、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。 チャートの下の [チャート オプション（Chart Options）] リンクをクリックすると、表示を総合的な [検出されたマルウェア接続] から [モニタされたマルウェア接続（Malware Connections Monitored）] または [ブロックされたマルウェア接続（Malware Connections Blocked）] に変更できます。
クライアント ソース IP（Client Source IPs）	このテーブルには、組織内でマルウェア サイトに頻繁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。 特定のポートのデータだけを含めるには、テーブル下部のボックスにポート番号を入力し、[ポート別にフィルタ（Filter by Port）] をクリックします。この機能を使用して、マルウェアがどのポートを使用してマルウェア サイトへ「誘導」しているかを判断できます。 各接続のポートや宛先ドメインなどの詳細情報を表示するには、テーブル内のエントリをクリックします。たとえば、ある特定のクライアント IP アドレスの [ブロックされたマルウェア接続（Malware Connections Blocked）] が高い数値を示している場合、そのカラムの数値をクリックすると、ブロックされた各接続のリストが表示されます。このリストは、[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）] タブに検索結果として表示されます。リストの詳細については、「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」（P.23-36）を参照してください。 このテーブルは、「[クライアント マルウェア リスク（Client Malware Risk）] ページ」（P.23-19）の [L4 トラフィック モニタ：マルウェア脅威別クライアント（L4 Traffic Monitor: Clients by Malware Risk）] テーブルと同じです。

表 23-10　[L4 トラフィック モニタ（L4 Traffic Monitor）] レポート ページの内容 （続き）

セクション	説明
マルウェア ポート（Malware Ports）	このテーブルには、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。 詳細を表示するには、テーブル内のエントリをクリックします。たとえば、[検出された上位マルウェア接続（Total Malware Connections Detected）] の数値をクリックすると、そのポートの各接続の詳細情報が表示されます。このリストは、[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）] タブに検索結果として表示されます。リストの詳細については、「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」（P.23-36）を参照してください。
検出されたマルウェア サイト（Malware Sites Detected）	このテーブルには、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。 特定のポートのデータだけを含めるには、テーブル下部のボックスにポート番号を入力し、[ポート別にフィルタ（Filter by Port）] をクリックします。この機能を使用して、サイトまたはポートをブロックするかどうかを判断できます。 詳細を表示するには、テーブル内のエントリをクリックします。たとえば、[ブロックされたマルウェア接続（Malware Connections Blocked）] の数値をクリックすると、特定のサイトに対してブロックされた各接続のリストが表示されます。このリストは、[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）] タブに検索結果として表示されます。リストの詳細については、「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」（P.23-36）を参照してください。

[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。

SOCKS ポリシーの設定を変更する手順については、第 6 章「SOCKS プロキシ サービス」を参照してください。

SOCKS Proxy

Printable (PDF)

Time Range: Day

31 Oct 2012 15:00 to 01 Nov 2012 15:56 (GMT -07:00)

Top Destinations for SOCKS: Total Transactions

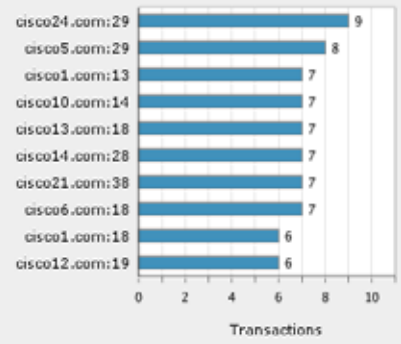


Chart Options... | Export...

Top Users for SOCKS: Total Transactions

Chart Options... | Export...

Destinations

Items Displayed 10

Domain/IP:Port	TCP / UDP	Bandwidth Used	Transactions Allowed	Transactions Blocked	Total Transactions
cisco1.com:3	TCP	120B	4	0	4
cisco1.com:9	TCP	360B	4	0	4
cisco1.com:13	TCP	910B	7	0	7
cisco1.com:14	UDP	420B	3	0	3
cisco1.com:18	UDP	1,080B	6	0	6
cisco1.com:19	TCP	570B	3	0	3
cisco1.com:23	TCP	230B	1	0	1
cisco1.com:24	UDP	960B	4	0	4
cisco10.com:13	UDP	130B	1	0	1
cisco10.com:14	TCP	980B	7	0	7
Totals (all available data):	--	162.0KB	627	0	627

Find Domain/IP

Columns... | Export...

Users

Items Displayed 10

User ID or Client IP	Bandwidth Used	Transactions Allowed	Transactions Blocked	Total Transactions
user10	4,150B	17	0	17
user11	5,040B	20	0	20
user12	5,690B	20	0	20
user13	6,990B	26	0	26
user14	10,050B	35	0	35
user15	3,800B	13	0	13
user16	7,990B	26	0	26
user17	10,110B	35	0	35
user18	7,440B	25	0	25
user19	8,240B	24	0	24
Totals (all available data):	162.0KB	627	0	627

Find User ID or Client IP

Columns... | Export...

関連トピック

- 「SOCKS プロキシの設定」（P.6-2）

[ユーザの場所別のレポート（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。リモートおよびローカル ユーザの詳細については、「リモート ユーザの操作」（P.14-2）を参照してください。

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。

図 23-12 は、[ユーザの場所別レポート（Reports by User Location）] ページを示します。

図 23-12　[ユーザの場所別レポート（Reports by User Location）] ページ

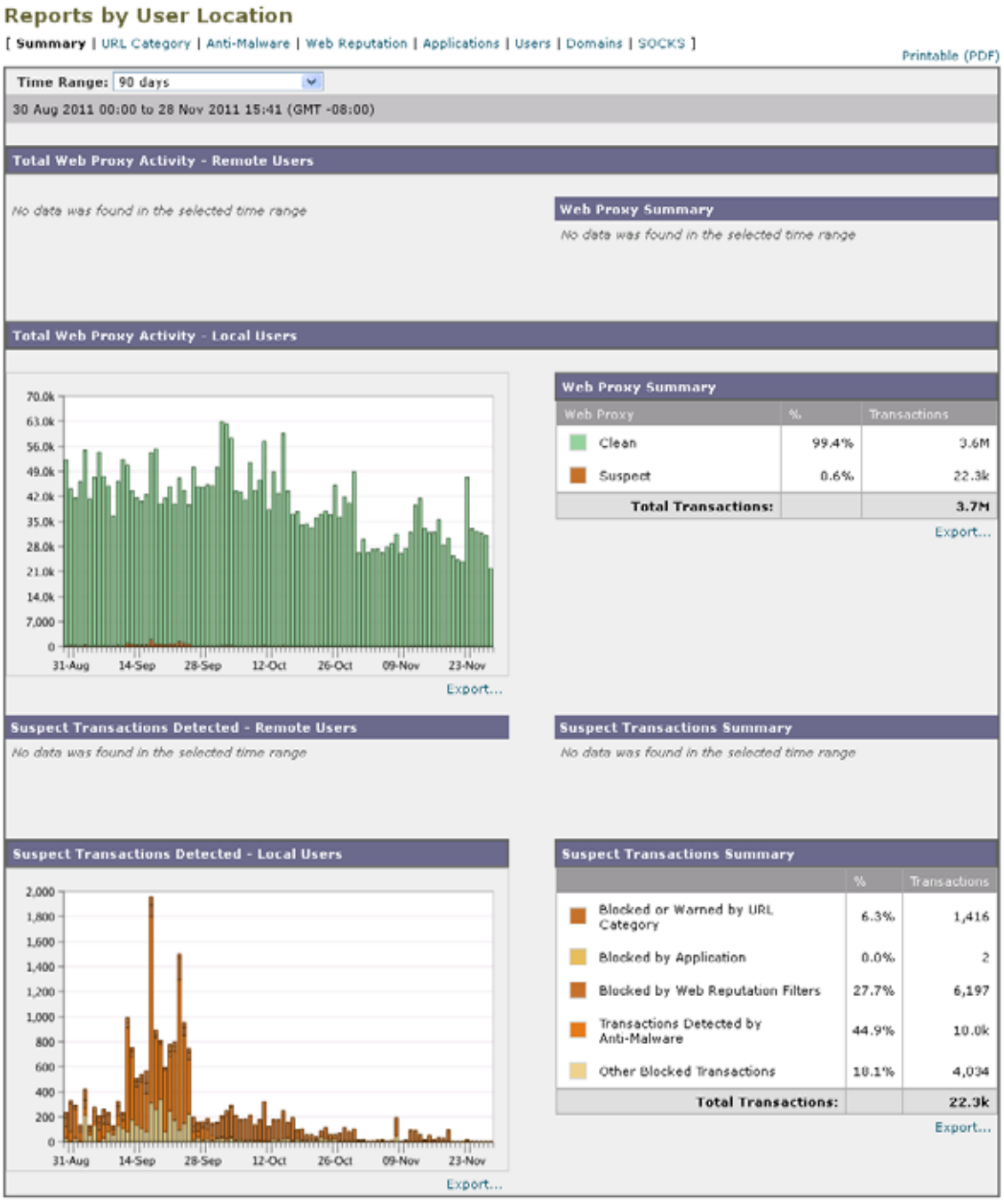


表 23-11 では、[ユーザの場所別レポート（Reports by User Location）] ページに表示される情報を説明します。

表 23-11　[ユーザの場所別レポート（Reports by User Location）] レポート ページのコンポーネント

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。詳細については、「時間範囲の変更」（P.22-3）を参照してください。
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）	このセクションには、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、グラフ形式で表示されます。
Web プロキシの概要（Web Proxy Summary）	このセクションには、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。
Web プロキシ アクティビティ総数：ローカル ユーザ（Total Web Proxy Activity: Local Users）	このセクションには、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、グラフ形式で表示されます。
検出された疑わしいトランザクション：リモート ユーザ（Suspect Transactions Detected: Remote Users）	このセクションには、リモート ユーザに対して定義したアクセス ポリシーによって指定した時間内（横方向）に検出された疑わしいトランザクション（縦方向）が、グラフ形式で表示されます。
疑わしいトランザクションの概要（Suspect Transactions Summary）	このセクションには、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。
検出された疑わしいトランザクション：ローカル ユーザ（Suspect Transactions Detected: Local Users）	このセクションには、リモート ユーザに対して定義したアクセス ポリシーによって指定した時間内（横方向）に検出された疑わしいトランザクション（縦方向）が、グラフ形式で表示されます。
疑わしいトランザクションの概要（Suspect Transactions Summary）	このセクションには、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。

[ユーザの場所別レポート（Reports by User Location）] ページでは、ローカル ユーザとリモート ユーザのアクティビティを示すレポートを生成できます。これにより、ユーザのローカル アクティビティとリモート アクティビティを簡単に比較できます。

[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または両方で検索を行います。

- 「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」（P.23-34）
- 「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」（P.23-36）
- 「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」（P.23-36）

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）] タブを使用して、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、レポートできます。このタブは、個々のセキュリティ コンポーネントおよびアクセプタブル ユース適用コンポーネントからの Web トラッキング情報を集約し、Web トラフィックのパターンおよびセキュリティ リスクのモニタに使用可能なデータを記録します。

[プロキシ サービス（Proxy Services）] には、個々のトランザクションの結果が表示され、その結果には、単にドメイン名（google.com など）ではなく、URL（mail.google.com など）内のホスト名とドメインが含まれます。

このデータを使用して、次の役割を補助することができます。

- **人事または法律マネージャ。**所定の期間内の従業員に関するレポートを調査します。
- **ネットワーク セキュリティ管理者。**会社のネットワークが従業員のスマートフォンを介してマルウェアの脅威にさらされていないかどうかを調査します。

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。

一連のトランザクションの検索後、表示するカラムを選択し、カラムによってデータをソートできます。詳細については、「レポート ページのカラムの使用」（P.22-4）を参照してください。

（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。

関心のある Web アクティビティのインスタンスを検索するには、次の手順を実行します。

ステップ 1　[レポート（Reporting）] > [Web トラッキング（Web Tracking）] ページに移動します。

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　表 23-12 で定義されるフィールドを設定します。

表 23-12　[Web トラッキング（Web Tracking）] ページの [プロキシ サービス（Proxy Services）] タブの基本設定

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。詳細については、「時間範囲の変更」（P.22-3）を参照してください。
ユーザ/クライアント IP（User/Client IP）	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 アドレスを任意で入力します。IP 範囲を 172.16.0.0/16 のような 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。
Web サイト（Website）	追跡対象の Web サイトを任意で入力します。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　任意で、[詳細（Advanced）] セクションを展開して、表 23-13 で定義されるフィールドを設定し、より詳細な基準を使用して Web トラッキングの結果をフィルタリングします。

表 23-13　[Web トラッキング（Web Tracking）] ページの [プロキシ サービス（Proxy Services）] タブの高度な設定

設定	説明
URL カテゴリ（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。 一連の URL カテゴリが更新されると、一部のカテゴリに「Deprecated」のラベルが付けられる場合があります。これらのカテゴリは、新しいトランザクションには使用されなくなりますが、一連のカテゴリを更新する前に発生したトランザクションの検索に使用できます。URL カテゴリ セットの更新の詳細については、「URL カテゴリ セットの更新とレポート」（P.23-12）を参照してください。
アプリケーション（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（Policy）	ポリシー グループでフィルタリングするには、[ポリシーでフィルタ（Filter by Policy）] を選択し、フィルタリングに使用するポリシー グループ名を入力します。
マルウェア脅威（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。
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（AnyConnect Secure Mobility）	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。
ユーザ要求（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、検索結果には「最良の推測」トランザクションが含まれる場合があります。

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ます。

ステップ 6　任意で、各トランザクションに関する詳細情報を表示するには、[トランザクション（Transactions）] カラムの [詳細の表示（Display Details）] をクリックします。

（注）　1000 件を超える結果を表示する必要がある場合は、[印刷可能なダウンロード（Printable Download）] リンクをクリックすると、関連するトランザクションの詳細を除く 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　結果内の URL が切り詰められている場合、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。

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
- 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。

疑わしいサイトにあるホスト名を表示するには、[送信先 IP アドレス（Destination IP Address）] カラム見出しの [詳細の表示（Display Detail）] リンクをクリックします。

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。カスタム URL カテゴリ、一致するポリシー、およびユーザの場所（ローカルまたはリモート）により、結果をフィルタリングすることもできます。

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。

関連トピック

- 「[SOCKS プロキシ（SOCKS Proxy）] ページ」（P.23-29）

[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）] レポートを使用して、次のタスクを実行する場合可能性があります。

- Web セキュリティ アプライアンスが推奨キャパシティを超える時点を把握し、追加アプライアンスをアップグレードしたり、取得したりする時期を決定するために利用します。
- 計画が必要になるキャパシティの問題が今後発生する可能性を示す履歴のトレンドを識別します。
- 最も多くのリソースを使用したシステムの部分（トラブルシューティングを支援するため）

図 23-13 は、[システム容量（System Capacity）] ページの最初の 4 つのグラフを示します。

図 23-13　[システム容量（System Capacity）] ページ：上のグラフ

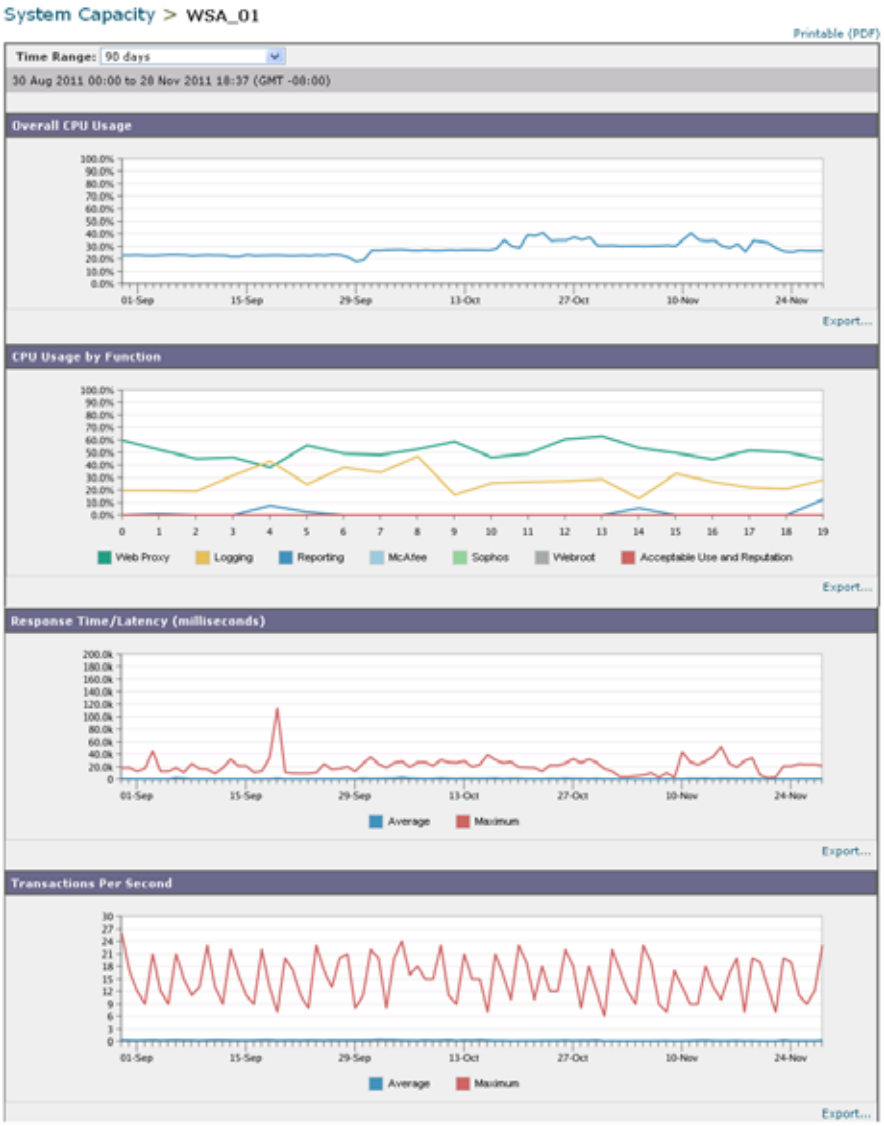


図 23-14 は、[システム容量（System Capacity）] ページの最後の 3 つのグラフを示します。

図 23-14　[システム容量（System Capacity）] ページ：下のグラフ

[システム容量（System Capacity）] レポートには、アプライアンスの全体的な CPU 使用率を示すグラフが表示されます。AsyncOS for Web は、アイドル状態の CPU リソースを使用してトランザクション スループットを向上させるように最適化されています。CPU 使用率が高くても、必ずしもシステム キャパシティの問題を示すわけではありません。CPU サイクルの使用率を表示する [機能別 CPU 使用率（CPU Usage by Function）] グラフは、Web プロキシやロギングなどのさまざまな機能で使用されます。[機能別 CPU 使用率（CPU Usage by Function）] グラフは、最も多くのリソースを使用するアプライアンス コンポーネントを示すことができます。アプライアンスの最適化が必要な場合、このグラフは、調整が必要な機能を判断するのに役立ちます。

応答時間 / 遅延のグラフと 1 秒あたりのトランザクションのグラフには、全体的な応答時間（ミリ秒単位）、および [時間範囲（Time Range）] ドロップダウン メニューで指定した日付範囲での 1 秒あたりのトランザクション数が示されます。

[システム容量（System Capacity）] レポートの下の 3 つのグラフは、発信接続、アプライアンスがアップストリーム サーバに接続するのに使用する帯域幅、および Web プロキシのメモリ バッファのサイズを示します。

[プロキシ バッファ メモリ（Proxy Buffer Memory）] では、ネットワーク トラフィックのスパイクが表れることがあります。しかし、グラフが最大値に向かって着実に上昇している場合は、アプライアンスが最大キャパシティに達する可能性があり、キャパシティの追加を検討する必要があります。

[システム容量に表示されるデータ（Data You See on System Capacity）] ページに表示されるデータの解釈

[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。この情報は時間テーブルから収集されます。
- **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。

[システム容量（System Capacity）] ページの [最大（Maximum）] 値インジケータは、指定された期間内の最大値を示します。[平均（Average）] 値は指定された期間内のすべての値の平均です。集計期間は、レポートに対して選択された間隔に応じて異なります。たとえば、月単位のチャートの場合は、日付ごとの [平均（Average）] 値と [最大（Maximum）] 値を表示することができます。

[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。表 23-14 は、各セクションについて説明します。

表 23-14　[システム ステータス（System Status）] レポート ページのコンポーネント

セクション	表示内容
Web セキュリティ アプライアンスのステータス（Web Security Appliance Status）	• システムの動作期間 • システム リソースの使用率：レポーティングおよびロギングに使用される CPU 使用率、RAM 使用率、およびディスク領域の使用率。 システムによって使用されない RAM は Web オブジェクト キャッシュによって使用されるので、効率的に動作する RAM 使用率は 90% を超える場合があります。システムで重大なパフォーマンス問題が発生していない場合で、この値が 100% に固定されない場合、システムは正常に動作しています。 **（注）** プロキシバッファ メモリは、この RAM を使用する 1 つのコンポーネントです。このステータスの詳細については、「[システム容量（System Capacity）] ページ」（P.23-37）を参照してください。

表 23-14　[システム ステータス（System Status）] レポート ページのコンポーネント （続き）

セクション	表示内容
プロキシ トラフィックの特性（Proxy Traffic Characteristics）	• 1 秒あたりのトランザクション • 帯域幅 • 応答時間 • キャッシュ ヒット率 • 接続
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

24
ロギング

ロギングの概要

ログ ファイルを使用して、Web トラフィックをモニタできます。ログ ファイルを作成するようにアプライアンスを設定するには、ログ サブスクリプションを作成します。ログ サブスクリプションは、ログ ファイル タイプを名前、ロギング レベル、その他のパラメータ（サイズや宛先情報など）と関連付けるアプライアンスの設定です。さまざまなログ ファイル タイプをサブスクライブできます。ログ サブスクリプションの詳細については、「ログ サブスクリプションの使用」（P.24-7）を参照してください。

一般的なアプライアンスのモニタリングでは、通常アプライアンスの管理者は次のログ ファイルを確認します。

- **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 アクティビティを記録します。アクセス ログの詳細については、「ログ ファイルへのアクセス」（P.24-17）を参照してください。
- **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 アクティビティを記録します。トラフィック モニタ ログの詳細については、「トラフィック モニタ ログ」（P.24-43）を参照してください。

アプライアンスは、システム ログ ファイルなど、その他のタイプのログ ファイルも作成します。アプライアンスのエラーのトラブルシューティングを行うために、場合によってはその他のタイプのログ ファイルを確認します。各タイプのリストについては、「ログ ファイル タイプ」（P.24-2）を参照してください。

アプライアンスには、アクセス ログに記録される情報のタイプをカスタマイズするために複数のオプションが用意されています。詳細については、「アクセス ログおよび W3C ログのカスタム フォーマット」（P.24-31）を参照してください。

ログ ファイル タイプ

ログ ファイル タイプは、Web トラフィックやシステム データなど、生成されたログに記録される情報を示します。デフォルトで、Web セキュリティ アプライアンスにはすでに作成されたほとんどのログ ファイル タイプのログ サブスクリプションが含まれています。ただし、Web プロキシのトラブルシューティング用のいくつかのログ ファイル タイプがあります。デフォルトでは、これらのログは作成されません。これらのログ ファイル タイプの詳細については、「Web プロキシ ロギング」（P.24-6）を参照してください。

表 24-1 は、デフォルトで作成される Web セキュリティ アプライアンスのログ ファイル タイプを示します。

表 24-1　デフォルトのログ ファイル タイプ

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。	No	No
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。	Yes	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。	No	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。	No	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。	Yes	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。	Yes	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。	No	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。	No	No
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 ログの詳細については、「ロギング」（P.13-17）を参照してください。	Yes	Yes
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。	No	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 IronPort Web 使用コントロール 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。	No	No
DCA エンジン ログ（動的コンテンツ分析）	Cisco IronPort Web 使用コントロール 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。	Yes	Yes

表 24-1　デフォルトのログ ファイル タイプ （続き）

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。 Web プロキシのロギングの詳細については、「Web プロキシ ロギング」（P.24-6）を参照してください。	Yes	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。	No	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。 外部認証の詳細については、「RADIUS ユーザ認証」（P.26-13）を参照してください。	No	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。	Yes	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。	No	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。	Yes	Yes
GUI ログ （グラフィカル ユーザ インターフェイス）	Web インターフェイスでのページの更新履歴を記録します。GUI ログには、アプライアンスから電子メールで送信される定期レポートに関する情報など、SMTP トランザクションに関する情報も含まれます。	Yes	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。	Yes	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）。	No	No
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連するメッセージを記録します。	No	No
ロギング フレームワーク ログ	Web プロキシのロギング システムに関連するメッセージを記録します。	No	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。	Yes	Yes

表 24-1　デフォルトのログ ファイル タイプ （続き）

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
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。	No	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。	Yes	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。	No	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。	No	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。	Yes	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。	Yes	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。	Yes	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。	No	Yes
レポーティング ログ	レポート生成履歴を記録します。	Yes	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。	Yes	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。	No	No
SaaS 認証ログ	SaaS アクセス コントロール機能に関連するメッセージを記録します。	Yes	Yes
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。	Yes	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。	Yes	Yes

表 24-1　デフォルトのログ ファイル タイプ （続き）

ログ ファイル タイプ	説明	syslog プッシュのサポート	デフォルトのイネーブル設定
SNMP 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。	No	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。	No	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。	Yes	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。	Yes	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。	Yes	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。	Yes	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。	No	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。 詳細については、「セキュア モビリティの実現の概要」（P.14-1）および「ユーザの透過的識別」（P.8-12）を参照してください。	Yes	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。	Yes	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」（P.24-29）を参照してください。	Yes	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。	No	Yes
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。	No	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。	No	No

表 24-1　デフォルトのログ ファイル タイプ （続き）

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
Webcat 統合フレームワーク ログ	Web プロキシと Cisco IronPort Web 使用コントロールに関連付けられた 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。	No	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。	No	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。	Yes	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。	Yes	Yes

Web プロキシ ロギング

デフォルトで、Web セキュリティ アプライアンスには、Web プロキシ ロギング メッセージである「デフォルト プロキシ ログ」用に作成された 1 つのログ サブスクリプションが含まれています。このログに保存された Web プロキシ情報は、Web プロキシのすべての側面、つまりモジュールをカバーしています。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。

Web プロキシの動作の問題が発生した場合、ユーザまたは管理者はまずデフォルト プロキシ ログを読み取る必要があります。問題の症状を示す可能性のある不審なログ エントリを見つけた場合、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できます。その後、問題のトラブルシューティングに役立つプロキシ ログを読み取ります。

Web インターフェイスまたは CLI で、これらのプロキシ モジュール ログのログ サブスクリプションを作成できます。ただし、CLI ではリクエスト デバッグ ログのみ作成できます。

次のリストは、すべての Web プロキシ モジュールのログ タイプを示します。

- 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
- 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

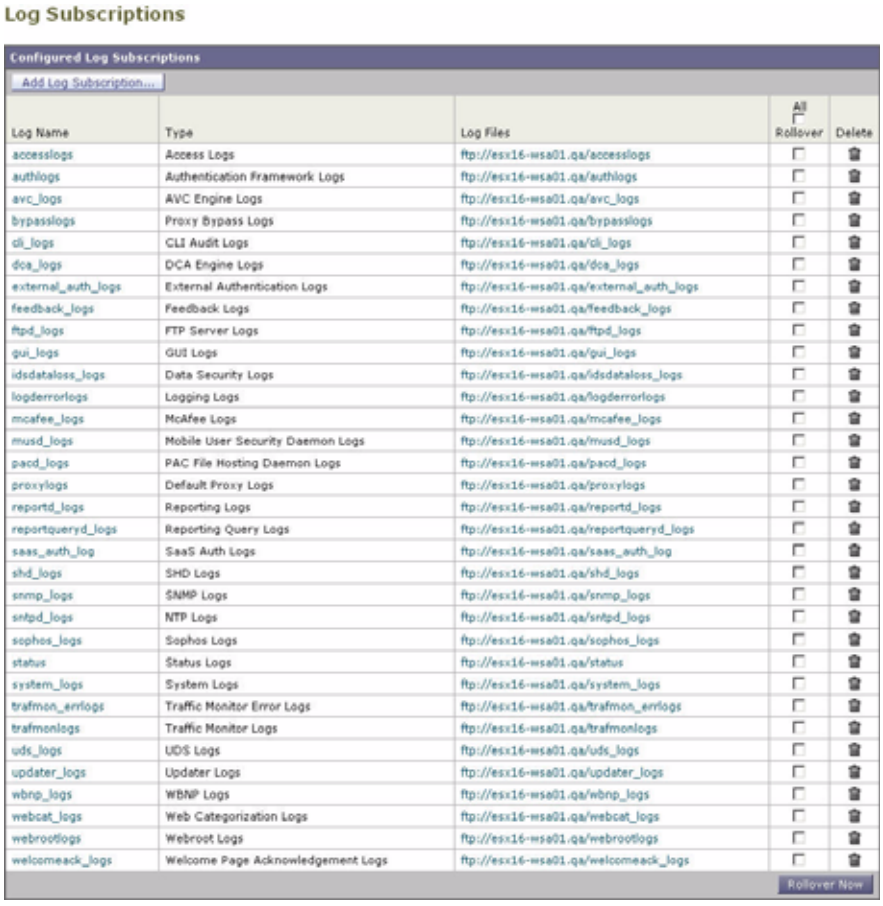
各ログ タイプの説明については、表 24-1「デフォルトのログ ファイル タイプ」（P.2）を参照してください。

ログ サブスクリプションの使用

ログ サブスクリプションは、ログ ファイル名やログ ファイルを取得する方法など、作成するログ ファイルのタイプやその他の要素を指定するアプライアンスの設定です。ログ ファイルのサブスクリプションを設定するには、[システム管理（System Administration）] > [ログ サブスクリプション（Log Subscriptions）] ページを使用します。

図 24-1 は、ログ サブスクリプションを操作する [ログ サブスクリプション（Log Subscriptions）] ページを示します。

図 24-1　　ログ ファイルのサブスクリプション



デフォルトで、アプライアンスは、大部分のログ タイプに対して 1 つのログ サブスクリプションが設定されます。ログ サブスクリプションを追加、編集、または削除できます。SCP、FTP、または Syslog を使用して、アプライアンスからログ ファイルを取得できます。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。

アプライアンスには、アクセス ログの設定時に使用する次のオプションが用意されています。

- **[各ログ エントリに追加情報を含める（Include additional information in each log entry）]。**アクセス ログのカスタマイズの詳細については、「アクセス ログおよび W3C ログのカスタム フォーマット」（P.24-31）を参照してください。
- **[情報のフォーマットを選択（Choose the format of the information）]。**次のフォーマット オプションから選択できます。
  - Apache
  - Squid
  - Squid の詳細（Squid Details）
- **HTTP ステータス コードに基づくエントリを除外（Exclude entries based on HTTP status codes）。**特定の HTTP ステータス コードに基づくトランザクションを含まないようにアクセス ログを設定し、特定のトランザクションを除外できます。たとえば、コード 407 または 401 を持つ認証に失敗した要求を除外したい場合があります。

ログ ファイル名とアプライアンス 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 サブスクリプションのロール オーバー

アプライアンス上のログ ファイルが大きくなりすぎないようにするために、ログ ファイルがユーザ指定の最大ファイル サイズまたは時間間隔に達すると、AsyncOS は「ロールオーバー」を実行してログ ファイルをアーカイブし、着信するログ データ用の新しいファイルを作成します。ログ サブスクリプション用に定義された取得方法に基づいて、AsyncOS は取得のためにアプライアンス上に古いログ ファイルを保存するか、または外部マシンに配信します。アプライアンスからログ ファイルを取得する方法の詳細については、表 24-4（P.24-15）を参照してください。

AsyncOS は、ログ ファイルをロールオーバーするときに次のアクションを実行します。

- ロールオーバーのタイムスタンプと、saved（保存済み）を示す文字 .s 拡張子を使用して、現在のログ ファイルの名前を変更します。
- ロールオーバーのタイムスタンプで新規ログ ファイルを作成し、文字 .c 拡張子を使用して、ファイルを current（現在のもの）と指定します。
- ログの取得方法がプッシュ ベースの場合、最近保存したログ ファイルをリモート ホストに転送します。ログの取得方法の一覧については、表 24-4（P.24-15）を参照してください。
- 先に転送しようとして失敗した同じサブスクリプションから既存のログ ファイルを転送します（プッシュ ベースの取得方法を使用している場合）。
- アプライアンスに保存するファイルの総数が超過した場合は、ログ サブスクリプション内の最も古いファイルを削除します（ポーリング ベースの取得方法を使用している場合）。

AsyncOS は、次の方法でログ サブスクリプションをロール オーバーします。

- **手動。**アプライアンスの管理者は、Web インターフェイスまたは CLI のいずれかの要求に応じて、手動でログ サブスクリプションをロール オーバーできます。[システム管理（System Administration）] > [ログ サブスクリプション（Log Subscriptions）] ページの [今すぐロールオーバー（Rollover Now）] ボタン、または `ollovernow` CLI コマンドを使用します。`rollovernow` コマンドを使用すると、一度にすべてのログ ファイルをロール オーバーするか、リストから特定のログ ファイルを選択することができます。
- **自動。**AsyncOS は、最初に到達したユーザ指定の制限（最大ファイル サイズまたは最大時間）に基づいて、ログ サブスクリプションをロール オーバーします。FTP ポーリング取得方法方式に基づくログ サブスクリプションは、リモート FTP クライアントから取得されるまで、またはシステムでログ ファイル用の空き領域を作成する必要が生じるまで、アプライアンスの FTP ディレクトリにファイルを作成し、保存します。

GUI を使用した、手動によるログ サブスクリプションのロール オーバー

ステップ 1　[システム管理（System Administration）] > [ログ サブスクリプション（Log Subscriptions）] ページで、ロール オーバーするログ サブスクリプションの右側のチェックボックスをオンにします。

ステップ 2　任意で、[すべて（All）] チェックボックスをオンにして、すべてのログ サブスクリプションをロール オーバー対象として選択できます。

ステップ 3　選択したログをロール オーバーするには、[今すぐロールオーバー（Rollover Now）] をクリックします。

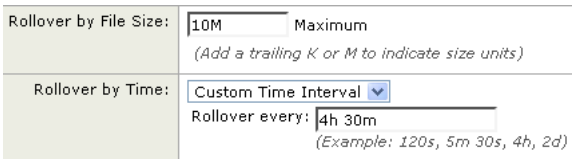
ログ サブスクリプションの自動によるロール オーバー

ログ サブスクリプションのロールオーバーの設定は、GUI の [システム管理（System Administration）] > [ログ サブスクリプション（Log Subscriptions）] ページ、または CLI の `logconfig` コマンドを使用して、サブスクリプションを作成または編集するときに定義します。ログ ファイルのロールオーバーをトリガーするために使用できる 2 つの設定は次のとおりです。

- **最大ファイル サイズ。**詳細については、「ファイル サイズによるロールオーバー」（P.24-10）を参照してください。
- **時間間隔。**詳細については、「時間によるロールオーバー」（P.24-10）を参照してください。

図 24-2 は、ログ サブスクリプションで使用可能なロールオーバー設定を示します。

図 24-2　ログ サブスクリプションのためのログ ファイルのロールオーバーの設定



ファイル サイズによるロールオーバー

AsyncOS は、ログ ファイルで使用されるディスク領域が多くなりすぎないようにするために、最大ファイル サイズに達したログ ファイルをロールオーバーします。ロールオーバーのための最大ファイル サイズを定義する場合は、メガバイトを示す `m` とキロバイトを示す `k` のサフィックスを使用します。たとえば、ログ ファイルが 10 MB に達したら AsyncOS によってロールオーバーされるようにする場合は、「`10m`」と入力します。

時間によるロールオーバー

ロールオーバーを定期的に実行されるようにスケジュールする場合は、次のいずれかの時間間隔を選択できます。

- **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。スケジュール設定されたロールオーバーのためのカスタムの時間間隔を作成するには、`d`、`h`、および `m` をサフィックスとして使用して、ロールオーバー間の日数、時間数、および分数を入力します。

- **[日次ロールオーバー（Daily Rollover）]。**AsyncOS は、毎日指定された時刻にロールオーバーを実行します。日単位のロールオーバーを選択した場合は、24 時間形式（HH:MM）を使用して、AsyncOS がロールオーバーを実行する時刻を入力します。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。AsyncOS が 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。たとえば、毎週水曜日と金曜日の午前 0：00 にログ ファイルをロールオーバーするように AsyncOS を設定できます。週単位のロールオーバーを設定するには、ロールオーバーを実行する曜日と 24 時間形式（HH:MM）の時刻を選択します。

  CLI を使用している場合は、ダッシュ（-）を使用して日の範囲を指定するか、アスタリスク（*）を使用してすべての曜日を指定するか、またはカンマ（,）を使用して複数の日と時刻を区切ることができます。

  図 24-3 は、[週次ロールオーバー（Weekly Rollover）] オプションで利用可能な設定を示します。

図 24-3　[週次ロールオーバー（Weekly Rollover）] 設定

圧縮ログ ファイルの使用

Web セキュリティ アプライアンスのディスク スペースを節約するために、ログ サブスクリプションは、ロール オーバーするログ ファイルを圧縮してからディスクに保存できます。ロール オーバーするログだけが圧縮されます。現在アクティブなログ ファイルは圧縮されません。

各ログ サブスクリプションに独自のログ圧縮設定が用意されているので、圧縮するログ サブスクリプションを選択できます。AsyncOS は gzip 圧縮形式を使用してログ ファイルを圧縮します。

最新のログ ファイルの表示

次の場所から、ログ ファイルの最新バージョンを表示できます。

- **Web インターフェイス。**[システム管理（System Administration）] > [ログ サブスクリプション（Log Subscriptions）] ページで、ログ サブスクリプションのリストの [ログ ファイル（Log Files）] カラムにあるログ サブスクリプション名をクリックします。ログ サブスクリプションのリンクをクリックすると、AsyncOS はパスワードの入力を求めるプロンプトを表示します。次に、このサブスクリプションで使用可能なログ ファイルの一覧が表示されます。ログ ファイルのいずれかをクリックして、ブラウザに表示するか、またはディスクに保存します。
- **コマンドライン インターフェイス。**`tail` CLI コマンドを使用します。AsyncOS は、設定されたログ サブスクリプションを表示し、表示するログ サブスクリプションの選択を求めるプロンプトを表示します。Ctrl+C を使用して、いつでも `tail` コマンドを終了します。

（注）　ログ サブスクリプションが圧縮されている場合は、それをダウンロードしてから解凍して開く必要があります。

ホスト キーの設定

Web セキュリティ アプライアンスから他のサーバにログ ファイルをプッシュするときに、`logconfig -> hostkeyconfig` サブコマンドを使用して SSH で使用するホスト キーを管理します。SSH サーバには、秘密キーと公開キーの 2 つのホスト キーが必要です。秘密ホスト キーは SSH サーバにあり、リモート マシンから読み取ることはできません。公開ホスト キーは、SSH サーバと対話する必要のある任意のクライアント マシンに配信されます。

`hostkeyconfig` サブコマンドによって、次の機能が実行されます。

表 24-2　ホスト キーの管理 : サブコマンドの一覧

コマンド	説明
New	新しいキーを追加します。
Scan	ホスト キーを自動的にダウンロードします。
Host	システム ホスト キーを表示します。これは、リモート システムの「known_hosts」ファイルに配置される値です。
Fingerprint	システム ホスト キーのフィンガープリントを表示します。
User	リモート マシンにログをプッシュするシステム アカウントの公開キーを表示します。これは、SCP プッシュ サブスクリプションを設定するときに表示されるキーと同じです。これは、リモート システムの「authorized_keys」ファイルに配置される値です。

ログ サブスクリプションの追加および編集

ステップ 1　[システム管理（System Administration）] > [ログ サブスクリプション（Log Subscriptions）] ページに移動します。

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　[ログ タイプ（Log Type）] フィールドから、このサブスクリプションに関連付けるログのタイプを選択します。

ステップ 4　[ログ名（Log Name）] フィールドに、ログ サブスクリプションの名前を入力します。

アプライアンスは、ログ ファイルを含むアプライアンスのディレクトリにこの名前を使用します。

ステップ 5　アクセス ログを作成する場合は、次のオプションを設定します。

アクセス ログ オプション	説明
ログ スタイル（Log Style）	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）	任意で、各アクセス ログ エントリに含めるその他のタイプの情報を入力します。詳細については、「アクセス ログおよび W3C ログのカスタム フォーマット」（P.24-31）を参照してください。

ステップ 6　W3C アクセス ログを作成する場合は、次のオプションを設定します。

アクセス ログ オプション	説明
ログ フィールド（Log Fields）	W3C アクセス ログに含めるフィールドを選択します。 [使用可能フィールド（Available Fields）] リストでフィールドを選択し、または [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。 詳細については、「W3C 準拠のアクセス ログ」（P.24-29）を参照してください。

（注）　W3C ログ サブスクリプションに含まれるログ フィールドを変更すると、ログ サブスクリプションは自動的にロール オーバーします。これにより、ログ ファイルの最新バージョンに適切な新しいフィールド ヘッダーを含めることができます。

ステップ 7　[ファイル名（File Name）] フィールドに、ログ ファイルの名前を入力します。

ステップ 8　[最大ファイル サイズ（Maximum File Size）] フィールドにログ ファイルを含めることができる最大ファイル サイズ（バイト単位）を入力します。数値の後に、「G」（ギガバイト）、「M」（メガバイト）、または「K」（キロバイト）を入力し、サイズの単位を指定します。

ステップ 9　[ログ圧縮（Log Compression）] フィールドを使用して、ロール オーバーされた後にログ ファイルを圧縮するかどうかを選択します。

詳細については、「圧縮ログ ファイルの使用」（P.24-11）を参照してください。

ステップ 10　（任意）アクセス ログまたは W3C アクセス ログから関連付けられたトランザクションを除外するには、[ログ除外（Log Exclusions）] フィールドに HTTP ステータス コード（4xx または 5xx のみ）を指定します。

たとえば、コード 407 または 401 を持つ認証に失敗した要求を除外したい場合があります。

ステップ 11　[ログ レベル（Log Level）] フィールドでログ ファイルに含める情報の詳細レベルを選択します。

[ログ レベル（Log Level）] フィールドには、アクセスおよび W3C ログ アクセス サブスクリプションは表示されません。

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。詳細レベルの高い設定には、詳細レベルの低い設定に保持されるすべてのメッセージと、その他のメッセージも含まれます。詳細レベルを上げるほど、システムのパフォーマンスは低下します。

表 24-3 は、[ログ レベル（Log Level）] フィールドで選択できる詳細レベルを示します。

表 24-3　ログ レベル

ログ レベル	説明
クリティカル（Critical）	これは、詳細レベルの最も低い設定です。このレベルにはエラーだけが含まれます。この設定にすると、パフォーマンスやその他の重要なアクティビティをモニタできません。ただし、ログ ファイルがすぐには最大サイズに到達しなくなります。このログ レベルは、syslog レベルの「Alert」と同等です。
警告（Warning）	このレベルには、システムによって作成されたすべてのエラーと警告が含まれます。この設定にすると、パフォーマンスやその他の重要なアクティビティをモニタできません。このログ レベルは、syslog レベル「Warning」と同等です。
情報（Information）	このレベルには、詳細なシステム操作が含まれます。これはデフォルトです。このログ レベルは、syslog レベル「Info」と同等です。
デバッグ（Debug）	このレベルには、システム問題のデバッグに役立つデータが含まれます。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「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「Debug」と同等です。

ステップ 12　[検索方法（Retrieval Method）] フィールドで、アプライアンスからログ ファイルを取得する方法を選択します。

表 24-4 は、ログ ファイルを取得できるさまざまな方法を説明します。

表 24-4　ログ転送プロトコル

取得方法	説明
アプライアンス上の FTP （FTP ポーリング）	この方法では、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アプライアンスにアクセスするリモート FTP クライアントが必要です。 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。 これはデフォルトです。
リモート サーバ上の FTP （FTP プッシュ）	この方法では、リモート コンピュータ上の FTP サーバに定期的にログ ファイルをプッシュします。 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。 • ファイル転送の最大時間 • 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。

表 24-4　ログ転送プロトコル （続き）

取得方法	説明
リモート サーバ上の SCP （SCP プッシュ）	この方法では、Secure Copy Protocol（SCP）を使用して、リモート コンピュータ上の SCP サーバに定期的にログ ファイルをプッシュします。この方法には、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。 • ファイル転送の最大時間 • 転送に使用するプロトコル • 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 ホスト キーの確認をイネーブルにするかどうかを選択します。
Syslog プッシュ	この方法では、リモート syslog サーバにログ メッセージを送信します。この方法は、RFC 3164 に準拠しています。アプライアンスはポート 514 を使用します。 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。 • 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） • ログで使用するファシリティ テキスト ベースのログの syslog のみを選択できます。 **（注）** 1024 バイトを超える syslog メッセージは切り捨てられます。可変長など、多くのカスタム変数数を持つアクセス ログや W3C アクセス ログは、1024 バイトの制限を超える場合があります。

ステップ 13　変更を送信し、保存します。

ステップ 14　取得方法として SCP を選択した場合、アプライアンスは SCP サーバ ホスト上に配置する必要がある SSH キーを表示します。

ログ サブスクリプションの削除

ステップ 1　[システム管理（System Administration）] > [ログ サブスクリプション（Log Subscriptions）] ページに移動します。

ステップ 2　削除対象のログ サブスクリプションの [削除（Delete）] カラムの下にあるアイコンをクリックします。

ステップ 3　変更を送信し、保存します。

ログ ファイルへのアクセス

アクセス ログ ファイルは、すべての Web プロキシ フィルタリングとスキャン アクティビティの説明的な記録を提供します。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。[システム管理（System Administration）] > [ログ サブスクリプション（Log Subscriptions）] ページからアクセス ログ ファイルを表示できます。

（注）　W3C ログ アクセスも、すべての Web プロキシ フィルタリングとスキャン アクティビティを記録しますが、W3C 準拠の形式に限定されます。詳細については、「W3C 準拠のアクセス ログ」（P.24-29）を参照してください。

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-AccessOrDecryptionPolicy-Identity-OutboundMalwareScanningPolicy-DataSecu
rityPolicy-ExternalDLPPolicy-RoutingPolicy
<IW_comp,6.9,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-","-",-,-,IW_comp,-,"-","-","Unknown","Un
known","-","-",198.34,0,-,[Local],"-","-"> -
```

表 24-5 は、アクセス ログ ファイル エントリのさまざまなフィールドについて説明します。

表 24-5　アクセス ログ ファイルの入力フィールド

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、「トランザクション結果コード」（P.24-19）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 ログでは「%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。

表 24-5　アクセス ログ ファイルの入力フィールド （続き）

フォーマット指定子	フィールド値	フィールドの説明
%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」（P.24-20）を参照してください。
N/A（ACL デシジョン タグの一部）	AccessOrDecryptionPolicy	アクセス ポリシーまたは復号化ポリシー グループの名前。トランザクションがグローバル アクセス ポリシーまたはグローバル復号化ポリシーに一致する場合、この値は「DefaultGroup」。 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）	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）	OutboundMalwareScanningPolicy	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」。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だけ表示されます。データ セキュリティ ポリシーが適用されなかった場合、「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。

表 24-5　アクセス ログ ファイルの入力フィールド （続き）

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）	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な外部 DLP ポリシーに一致する場合、この値は「DefaultGroup」。外部 DLP ポリシーが適用されなかった場合、「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なルーティング ポリシーに一致する場合、この値は「DefaultRouting」。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」。 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。
%Xr	<IW_comp,6.9,-,"-",-, -,-,-,"-",-,-,-,"-",-,-, "-","-",-,-,IW_comp,-,"-", "-","Unknown","Unknown","-", "-",198.34,0,-,[Local], "-","-">	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。 山カッコ内に含まれる値の詳細については、「スキャン判定情報について」（P.24-24）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。

表 24-6　トランザクション結果コード

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。

表 24-6　トランザクション結果コード （続き）

結果コード	説明
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」応答を送信しました。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。
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。

表 24-7 は、ACL デシジョン タグの値を示します。

表 24-7　ACL デシジョン タグの値

ACL デシジョン タグ	説明
ALLOW_ADMIN_ERROR_PAGE	Web プロキシが、IronPort 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。

表 24-7　ACL デシジョン タグの値 （続き）

ACL デシジョン タグ	説明
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_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）] に設定されたアクセス 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。

表 24-7　ACL デシジョン タグの値 （続き）

ACL デシジョン タグ	説明
BLOCK_CONTINUE_WEBCAT	Web プロキシが、[警告（Warn）] に設定されたアクセス 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。
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。

表 24-7　ACL デシジョン タグの値 （続き）

ACL デシジョン タグ	説明
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_AMW_RESP	Web プロキシが、アクセス ポリシー グループの Anti-Malware 設定に基づいてサーバ応答をモニタしました。
MONITOR_AMW_RESP_URL	Web プロキシが HTTP 要求の URL が安全ではないと疑っていますが、アクセス ポリシー グループの Anti-Malware 設定に基づいてトランザクションをモニタしました。
MONITOR_AVC	Web プロキシが、アクセス ポリシー グループのアプリケーション設定に基づいてトランザクションをモニタしました。
MONITOR_CONTINUE_CONTENT_UNSAFE	任意で、Web プロキシが、アクセス ポリシー グループのサイト コンテンツ レーティング設定に基づいてトランザクションをブロックし、[警告して継続（Warn and Continue）] ページを表示しました。クライアント要求はアダルト コンテンツに対するものであり、ポリシーはアダルト コンテンツにアクセスするユーザに警告を表示するように設定されています。ユーザが警告を受け入れ、続けて最初に要求したサイトにアクセスし、その後他のスキャン エンジンは要求をブロックしませんでした。
MONITOR_CONTINUE_CUSTOMCAT	当初、Web プロキシが、[警告（Warn）] に設定されたアクセス 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 プロキシが、[警告（Warn）] に設定されたアクセス 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。

表 24-7　ACL デシジョン タグの値 （続き）

ACL デシジョン タグ	説明
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	ユーザが認証レルムに対してすでに認証されていたが、SaaS 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認証されていなかったため、Web プロキシは SaaS 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。
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）] に設定されたアクセス 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 SaaS 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 SaaS アプリケーションへのユーザ アクセスを許可しました。
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。

スキャン判定情報について

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],"-","-">
```

（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、「ログ ファイルへのアクセス」（P.24-17）を参照してください。

表 24-8 は、各アクセス ログ ファイル エントリのスキャン判定情報セクションのさまざまなフィールドについて説明します。

表 24-8　アクセス ログ ファイル エントリ：スキャン判定情報

ポジションとフォーマット指定子	フィールド値	説明
ポジション 1 %XC	IW_infr	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」（P.17-26）を参照してください。
ポジション 2 %XW	ns	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、スコアがない場合「ns」、DNS ルックアップ エラーがある場合、「dns」が表示されます。
ポジション 3 %Xv	24	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」（P.24-42）を参照してください。
ポジション 4 "%Xn"	"Trojan-Phisher-Gamec"	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。
ポジション 5 %Xt	0	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。
ポジション 6 %Xs	354385	Webroot が脅威識別子として使用する値。Cisco IronPort カスタマー サポートは、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。
ポジション 7 %Xi	12559	Webroot がトレース識別子として使用する値。Cisco IronPort カスタマー サポートは、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。
ポジション 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」（P.24-42）を参照してください。
ポジション 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。
ポジション 10 %Xf	-	McAfee がスキャン エラーとして使用する値。Cisco IronPort カスタマー サポートは、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。

表 24-8　アクセス ログ ファイル エントリ：スキャン判定情報 （続き）

ポジションとフォーマット指定子	フィールド値	説明
ポジション 11 %Xg	-	McAfee が検出タイプとして使用する値。Cisco IronPort カスタマー サポートは、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。
ポジション 12 %Xh	-	McAfee がウイルス タイプとして使用する値。Cisco IronPort カスタマー サポートは、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。
ポジション 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。
ポジション 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」（P.24-42）を参照してください。
ポジション 15 %Xx	-	Sophos がスキャン戻りコードとして使用する値。Cisco IronPort カスタマー サポートは、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。
ポジション 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、`archive.zip/virus.exe` などのアーカイブ内のオブジェクトです。 Sophos でのみ検出された応答に適用します。
ポジション 17 "%Xz"	"-"	Sophos が脅威名として使用する値。Cisco IronPort カスタマー サポートは、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。
ポジション 18 %Xl	-	Cisco IronPort データ セキュリティ ポリシーの [コンテンツ（Content）] カラムの処理に基づく Cisco IronPort データセキュリティ ポリシーのスキャン評価。 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 • **1.** ブロック • **-（ハイフン）** Cisco IronPort 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 IronPort 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 アクションが許可に設定されている場合に表示されます。

表 24-8　アクセス ログ ファイル エントリ：スキャン判定情報 （続き）

ポジションとフォーマット指定子	フィールド値	説明
ポジション 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 • **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）] ページの免除 URL カテゴリにより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。
ポジション 20 %XQ	IW_infr	要求側のスキャン中に判定された URL カテゴリの評価（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」（P.17-26）を参照してください。
ポジション 21 %XA	-	応答側のスキャン中に動的コンテンツ分析エンジンによって判定された URL カテゴリの評価（省略形）。Cisco IronPort Web 使用コントロール 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の場合で、要求時にカテゴリが割り当てられていない場合にのみ適用されます（値「nc」は、要求側のスキャンの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」（P.17-26）を参照してください。
ポジション 22 "%XZ"	"Trojan Phisher"	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。
ポジション 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。
ポジション 24 "%XO"	"Unknown"	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。
ポジション 25 "%Xu"	"Unknown"	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。
ポジション 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。
ポジション 27 "%XS"	"-"	安全なブラウジング スキャンの判定。この値は、安全検索またはサイト 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。 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」（P.17-20）を参照してください。

表 24-8　アクセス ログ ファイル エントリ：スキャン判定情報 （続き）

ポジションとフォーマット指定子	フィールド値	説明
ポジション 28 %XB	489.73	要求に対応するために使用された平均帯域幅（KB/秒）。
ポジション 29 %XT	0	要求が帯域幅制限制御設定によって調整されたかどうかを示す値。要求が調整された場合は「1」、調整されなかった場合は「0」。
ポジション 30 %l	[Local]	要求を行うユーザのタイプ（[ローカル（Local）] または [リモート（Remote）] のいずれか）。AnyConnect セキュア モビリティをイネーブルにした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。
ポジション 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。
ポジション 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。

Web レピュテーション フィルタの例

次の例では、URL の Web レピュテーション スコアがマルウェアをスキャンせずに許可を与えられるほど高かったために URL 要求は許可されました。

```
1278100150.818 1303 172.xx.xx.xx TCP_MISS/200 46578 GET http://www.cisco.com/ -
DIRECT/www.cisco.com - ALLOW_WBRS_11-AccessPolicy-Identity-NONE-NONE-NONE-DefaultGroup
<IW_comp,6.5,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-","-",-,-,IW_comp,-,"-","-","Unknown","Un
known","-","-",285.97,0,-,[Local],"-","-"> -
```

この例では、「6.5」は Web レピュテーション スコアです。ハイフン（-）で示された値は、要求がアンチマルウェア スキャンのために DVS エンジンに転送されなかったことを示します。この ACL デシジョン タグ「ALLOW_WBRS」は、要求が許可されたため、この Web レピュテーション スコアに基づいてアンチマルウェア スキャンに転送されなかったことを示します。

アンチマルウェア要求の例

次の例では、Webroot スキャン エンジンは URL 要求をスキャンし、URL 要求に基づいてマルウェア スキャンの判定を割り当てました。Webroot は URL 要求をスキャンする唯一のスキャン エンジンです。Webroot スキャンの詳細については、「Webroot スキャン」（P.19-7）を参照してください。

```
1278106367.381 170 172.xx.xx.xx TCP_DENIED/403 1828 GET http://www.gator.com/ - NONE/- -
BLOCK_AMW_REQ_URL_11-AccessPolicy-Identity-OMSPolicy-NONE-NONE-NONE
<IW_busi,3.4,13,"GAIN - Common
Components",95,37607,10,-,"-",-,-,-,"-",-,-,"-","-",-,-,IW_busi,-,"Adware","-","Unknown"
,"Unknown","-","-",86.02,0,-,[Local],"-","-">
```

この例では、「3.4」は Web レピュテーション スコアです。Web サイトのマルウェアをスキャンすることを示します。つまり、Web プロキシはアンチマルウェア スキャンのために DVS エンジンに要求を渡しました。

値 13 は、Webroot が DVS エンジンに渡した、「アドウェア」に相当するマルウェア スキャンの判定です。ACL デシジョン タグ「BLOCK_AMW_REQ_URL」は、Webroot の要求側の URL のチェックによりこの判定が生成されたことを示します。残りのフィールドは、Webroot がその評価から抽出した、マルウェアの名前（「GAIN：共通コンポーネント」）、脅威のリスク レーティング（「95」）、脅威 ID（「37607」）、およびトレース ID（「10」）の値を示します。McAfee および Sophos 関連の値は、McAfee または Sophos スキャン エンジンのいずれも URL 要求をスキャンしなかったため、すべて空（-）です。

アンチマルウェア応答の例

次の例では、McAfee スキャン エンジンがサーバの応答をスキャンし、サーバの応答に基づいてマルウェア スキャンの判定を割り当て、それをユーザからブロックします。

```
1278097193.276 51 172.xx.xx.xx TCP_DENIED/403 3122 GET http://badsite.com/malware.exe -
DIRECT/badsite.com application/x-dosexec
BLOCK_AMW_RESP_11-AccessPol-Identity-NONE-NONE-NONE-DefaultGroup
<IW_infr,3.0,24,"Trojan-Phisher-Gamec",0,354385,12559,
-,"-",-,-,-,"-",-,-,"-","-",-,-,IW_infr,-,"Trojan
Phisher","-","Unknown","Unknown","-","-",489.73,0,[Local],"-","-"> -
```

次のリストでは、このトランザクションが Webroot スキャン エンジンの結果に基づいてブロックされたことを示す、このアクセス ログ エントリ内の値を説明しています。

- **TCP_DENIED。**Web サイトがアクセス ポリシーによって拒否されました。
- **BLOCK_AMW_RESP _11 - AccessPol。**このトランザクションは、「AccessPol」アクセス ポリシー グループに一致し、そのポリシー グループで定義され設定によって、検出されたマルウェアによってサーバ応答がブロックされました。
- **山カッコ（<>）内の「3.0」。**URL は、Web レピュテーション スコア 3.0 を受け取りました。このスコアは、追加スキャンが必要な範囲に分類されます。
- **山カッコ（<>）内の「24」。**Webroot が DVS エンジンに渡した、トロイのフィッシャに相当するマルウェア スキャンの判定。
- **「Trojan-Phisher-Gamec」。**Webroot がスキャンしたマルウェアの名前。

W3C 準拠のアクセス ログ

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 準拠であり、W3C 拡張ログ ファイル（ELF）形式でトランザクション履歴を記録します。

複数の W3C アクセス ログ サブスクリプションを作成し、それぞれに含めるデータを定義できます。組織で一般的に必要になるすべての情報を含む W3C アクセス ログを作成する一方で、トラブルシューティングまたは特殊な分析に使用できる特殊な W3C アクセス ログを作成する場合があります。たとえば、特定の情報へのアクセスのみが必要になる人事マネージャ用に W3C アクセス ログを作成する場合があります。

W3C アクセス ログを使用するときは、以下のルールとガイドラインを考慮してください。

- 各アクセス W3C ログ サブスクリプションに記録されるデータを定義します。

- 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 アクセス ログ サブスクリプションを定義する場合、定義済みログ フィールドのリストから選択するか、またはカスタム ログ フィールドを入力できます。詳細については、「W3C アクセス ログのログ フィールドの使用」（P.24-31）を参照してください。
- 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 ログを読み取り、解析するときに、[タイムスタンプ（timestamp）] フィールドを含める必要がある場合があります。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。
- W3C アクセス ログに含まれるログ フィールドを順序どおりコピーする場合は、`logconfig > edit` CLI コマンドを使用します。CLI は、コマンドをコピーし、別の Web セキュリティ アプライアンス Web インターフェイスに貼り付ける順序でログ フィールドを表示します。

W3C ログ ファイルのヘッダー

各 W3C ログ ファイルには、ファイルの先頭にヘッダー テキストが含まれています。各行は、# 文字で始まり、ログ ファイルを作成した Web 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。

表 24-9 は、各 W3C ログ ファイルの先頭に記載されているヘッダー フィールドについて説明します。

表 24-9　W3C ログ ファイルのヘッダー フィールド

ヘッダー フィールド	説明
バージョン（Version）	使用される W3C の ELF 形式バージョン
日付（Date）	エントリが追加された日付と時刻
システム（System）	「Management_IP - Management_hostname」形式でログ ファイルを生成した Web セキュリティ アプライアンス
ソフトウェア（Software）	これらのログを生成したソフトウェア
フィールド（Fields）	ログに記録されたフィールド

たとえば、W3C ログ ファイルには次のようなヘッダー情報が含まれています。

```
#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 アクセス ログのログ フィールドの使用

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。詳細については、「アクセス ログおよび W3C ログのカスタム フォーマット」（P.24-31）を参照してください。
- **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。詳細については、「ログ ファイルへの HTTP/HTTPS ヘッダーの組み込み」（P.24-41）を参照してください。

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。表 24-10（P.24-31）は、W3C ログ フィールドのプレフィックスについて説明します。

表 24-10　W3C ログ フィールドのプレフィックス

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 log フィールドの「cs-method」は、クライアントからサーバに送信された要求の方法を参照し、「c-ip」はクライアントの IP アドレスを参照します。

アクセス ログおよび W3C ログのカスタム フォーマット

アクセス ログおよび W3C アクセス ログをカスタマイズして多くの異なるフィールドを組み込み、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することができます。アクセス ログはフォーマット指定子を使用し、W3C アクセス ログは W3C ログ フィールドを使用します。

表 24-11 は、W3C アクセス ログに含めることができる W3C ログ フィールドと対応するカスタム フォーマット指定子（アクセス ログ用）について説明します。

表 24-11　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	説明
—	%XP	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。これは、YouTube for Schools など、クライアント要求を認証し、リダイレクトする方法として、これらの要求にヘッダーを追加する特殊なシステムのトラブルシューティングをサポートします。
bytes	%B	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-ip	%a	クライアント IP アドレス
c-port	%F	クライアントの送信元ポート
CMF	%M	キャッシュ ミス フラグ（CMF フラグ）
cs(Cookie)	%C	クッキー 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。
cs(Referer)	%<Referer:	履歴
cs(User-Agent)	%u	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。
cs(X-Forwarded-For)	%f	X-Forwarded-For ヘッダー
cs-auth-group	%g	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。

表 24-11　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 （続き）

W3C ログ フィールド	アクセス ログのフォーマット指定子	説明
cs-auth-mechanism	%m	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。 • **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_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。**ユーザが SaaS アプリケーションへのアクセス時に Web ブラウザのフォームで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。
cs-bytes	%q	要求サイズ（ヘッダー + 本文）。
cs-method	%y	メソッド
cs-mime-type	%c	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。
x-req-first-line	%r	要求の先頭行：要求方法（URI）。
cs-uri	%U	リクエスト URI
cs-url	%Y	URL 全体
cs-username	%A	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。
cs-version	%P	プロトコル
date	%v	YYYY-MM-DD 形式の日付
DCF	%j	応答コードをキャッシュしません（DCF フラグ）
s-computerName	%N	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。
s-hierarchy	%H	階層の取得
s-hostname	%d	データ ソースまたはサーバの IP アドレス。
s-ip	%k	データ ソースの IP アドレス（サーバの IP アドレス）

表 24-11　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 （続き）

W3C ログ フィールド	アクセス ログのフォーマット指定子	説明
s-port	%p	宛先ポート番号
sc(Server)	%>Server:	応答のサーバ ヘッダー
sc-body-size	%b	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。
sc-bytes	%s	応答サイズ（ヘッダー + 本文）。
sc-http-status	%h	HTTP 応答コード
sc-result-code	%w	結果コード 例：TCP_MISS、TCP_HIT
sc-result-code-denial	%W	結果コードの拒否
time	%V	HH:MM:SS 形式の時刻
timestamp	%t	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 ログを読み取り、解析するときに、[タイムスタンプ（timestamp）] フィールドを含める必要がある場合があります。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。
user-type	%l	ユーザのタイプ（ローカルまたはリモート）。詳細については、「リモート ユーザの操作」（P.14-2）を参照してください。
x-acltag	%D	ACL デシジョン タグ
x-as-malware-threat-name	%X6	Adaptive Scanning が、アンチマルウェア スキャン エンジンを起動することなくトランザクションをブロックしたかどうかを示します。次の値が可能です。 • **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。
x-avc-app	%XO	AVC エンジンによって識別される Web アプリケーション。
x-avc-behavior	%Xb	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。
x-avc-reqbody-scanverdict	%XH	AVC 要求本文の評価
x-avc-reqbody-scanverdict	%XN	AVC 応答本文の評価
x-avc-reqhead-scanverdict	%XG	AVC 要求ヘッダーの評価
x-avc-resphead-scanverdict	%XM	AVC 応答ヘッダーの評価

表 24-11　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 （続き）

W3C ログ フィールド	アクセス ログのフォーマット指定子	説明
x-avc-type	%Xu	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。
x-avg-bw	%XB	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。
x-bw-throttled	%XT	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。
x-elapsed-time	%e	経過時間
x-error-code	%E	カスタマー サポートが失敗したトランザクションの原因をトラブルシューティングするのに役立つエラー コード番号。
x-hierarchy-origin	該当なし	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。 （例：DIRECT/www.example.com）
x-icap-server	%i	要求の処理中に接続された最後の ICAP サーバの IP アドレス
x-icap-verdict	%Xp	外部 DLP サーバのスキャンの判定
x-ids-verdict	%Xl	Cisco IronPort データ セキュリティ ポリシーのスキャンの判定 このフィールドが含まれる場合、IDS 判定が表示され、IDS がアクティブになっているが、ドキュメントがクリーンにスキャンされた場合、「0」が表示され、要求に対する IDS ポリシーがアクティブになっていなかった場合、「-」が表示されます。
x-latency	%x	遅延
x-local_time	%L	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。
x-mcafee-av-detecttype	%Xg	McAfee 固有の ID：（検出タイプ）
x-mcafee-av-scanerror	%Xf	McAfee 固有の ID：（スキャン エラー）
x-mcafee-av-virustype	%Xh	McAfee 固有の ID：（ウイルス タイプ）
x-mcafee-filename	%Xe	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。
x-mcafee-scanverdict	%Xd	McAfee 固有の ID：（スキャンの判定）
x-mcafee-virus-name	%Xj	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。
x-req-dvs-scanverdict	%X2	要求側 DVS スキャンの判定
x-req-dvs-threat-name	%X4	要求側 DVS 脅威の名前
x-req-dvs-verdictname	%X3	要求側 DVS 判定の名前

表 24-11　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 （続き）

W3C ログ フィールド	アクセス ログのフォーマット指定子	説明
x-request-source-ip	%XV	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。
x-request-rewrite	%XS	安全なブラウジング スキャンの判定。 安全検索またはサイト 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。詳細については、「アダルト コンテンツ アクセスのロギング」（P.17-20）を参照してください。
x-resp-dvs-scanverdict	%X0	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。
x-resp-dvs-threat-name	%X1	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。
x-resp-dvs-verdictname	%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。 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-result-code	%Xr	スキャン判定情報
x-resultcode-httpstatus	該当なし	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）。
x-sophos-file-name	%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、`archive.zip/virus.exe` などのアーカイブ内のオブジェクトです。

表 24-11　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 （続き）

W3C ログ フィールド	アクセス ログのフォーマット指定子	説明
x-sophos-scanerror	%Xx	Sophos 固有の ID：（スキャンの戻りコード）
x-sophos-scanverdict	%XY	Sophos 固有の ID：（スキャンの判定）
x-sophos-virus-name	%Xz	Sophos 固有の ID：（脅威の名前）
x-suspect-user-agent	%?BLOCK_SUSPECT_USER_AGENT,MONITOR_SUSPECT_USER_AGENT?%<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 Web プロキシが判定した場合、このフィールドにそのユーザ エージェントを記録します。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。
x-transaction-id	%I	トランザクション ID
x-wbrs-score	%XW	復号化された WBRS スコア <-10.0-10.0>
x-wbrs-threat-reason	%XK	Web レピュテーションの脅威の理由
x-wbrs-threat-type	%Xk	Web レピュテーションの脅威タイプ
x-webcat-code-abbr	%XC	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。
x-webcat-code-full	%XF	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。
x-webcat-req-code-abbr	%XQ	要求側のスキャン中に判定された URL カテゴリの評価（省略形）。
x-webcat-req-code-full	%XR	要求側のスキャン中に判定された URL カテゴリの評価（完全名）。
x-webcat-resp-code-abbr	%XA	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 IronPort Web 使用コントロール URL フィルタリング エンジンにのみ適用されます。
x-webcat-resp-code-full	%XL	応答側のスキャン中に判定された URL カテゴリの評価（完全名）。 Cisco IronPort Web 使用コントロール URL フィルタリング エンジンにのみ適用されます。
x-webroot-scanverdict	%Xv	Webroot からのマルウェア スキャンの判定
x-webroot-spyid	%Xs	Webroot 固有の ID：（スパイ ID）
x-webroot-threat-name	%Xn	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。
x-webroot-trace-id	%Xi	Webroot 固有のスキャン識別子：（トレース ID）
x-webroot-trr	%Xt	Webroot 固有の ID：（脅威リスク比率（TRR））

表 24-11　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 （続き）

W3C ログ フィールド	アクセス ログのフォーマット指定子	説明
x-p2s-first-byte-time	%:<l	Web プロキシがサーバへの接続を開始した時点から最初にサーバに書き込みが行えるようになるまでの時間。Web プロキシが複数のサーバに接続してトランザクションを完了する必要がある場合、これらの時間の合計になります。
x-s2p-first-byte-time	%:>l	サーバからの最初の応答バイトの待機時間
x-c2p-first-byte-time	%:l<	新しいクライアント接続からの最初の要求バイトの待機時間
x-p2c-first-byte-time	%:l>	クライアントに書き込まれる最初のバイトの待機時間
x-p2p-auth-wait-time	%:<a	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。
x-p2p-auth-svc-time	%:>a	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）。
x-p2p-avc-svc-time	%:A<	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）。
x-p2p-avc-wait-time	%:A>	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。
x-p2s-body-time	%:<b	ヘッダーの後に要求の本文をサーバに書き込む待機時間
x-s2p-body-time	%:>b	受信したヘッダーの後の完全な応答本文の待機時間
x-c2p-body-time	%:b<	完全なクライアント本文の待機時間
x-p2c-body-time	%:b>	クライアントに書き込まれる完全な本文の待機時間
x-p2p-fetch-time	%:>c	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。
x-p2p-dca-resp-wait-time	%:C>	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。
x-p2p-dca-resp-svc-time	%:C<	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）。
x-p2p-dns-wait-time	%:<d	Web プロキシが要求を送信後、Web プロキシの DNS プロセスからの応答を受信する待機時間。
x-p2p-dns-svc-time	%:>d	Web プロキシの DNS 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）。

表 24-11　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 （続き）

W3C ログ フィールド	アクセス ログのフォーマット指定子	説明
x-p2s-header-time	%:<h	最初のバイトの後に要求ヘッダーをサーバに書き込む待機時間
x-s2p-header-time	%:>h	最初の応答バイト後のサーバ ヘッダーの待機時間
x-c2p-header-time	%:h<	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
x-s2p-header-time	%:h>	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
x-p2p-mcafee-resp-svc-time	%:m<	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）。
x-p2p-mcafee-resp-wait-time	%:m>	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。
x-p2p-sophos-resp-svc-time	%:p<	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）。
x-p2p-sophos-resp-wait-time	%:p>	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。
x-p2p-reputation-wait-time	%:<r	Web プロキシが要求を送信後、Web レピュテーション フィルタからの応答を受信する待機時間。
x-p2p-reputation-svc-time	%:>r	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）。
x-p2p-asw-req-wait-time	%:<s	Web プロキシが要求を送信後、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待機時間。
x-p2p-asw-req-svc-time	%:>s	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）。
x-p2p-webroot-resp-svc-time	%:w<	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）。
x-p2p-webroot-resp-wait-time	%:w>	Web プロキシが要求を送信後、Webroot スキャン エンジンからの応答を受信する待機時間。

アクセス ログのカスタム フォーマットの設定

[システム管理（System Administration）] > [ログ サブスクリプション（Log Subscriptions）] ページを使用して、アクセス ログ ファイル エントリのカスタム フォーマットを設定します。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。

図 24-4　　アクセス ログのカスタム ログ フィールドの設定

[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_specifier1> <format_specifier2>
```

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
```

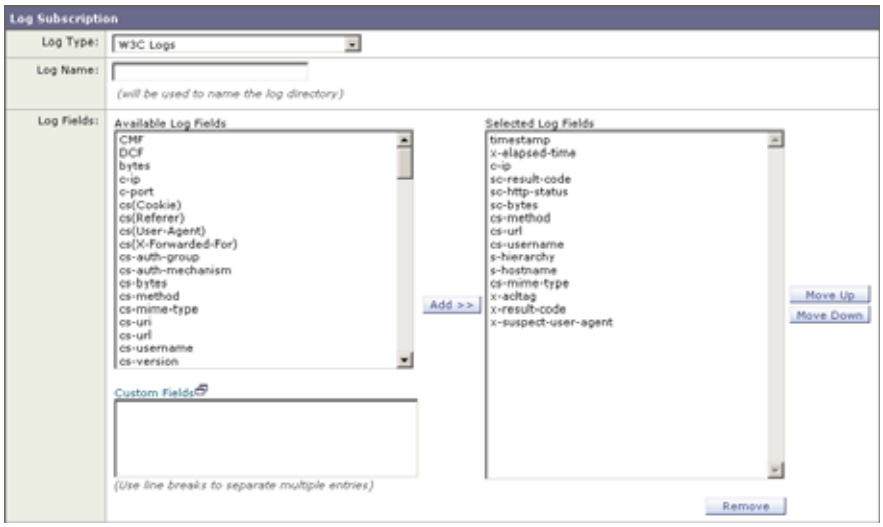
ここで、`client_IP` はログ フォーマット指定子 `%a` の説明トークン、`body_bytes` は `%b` の説明トークン、`error_type` は `%E` の説明トークンです。

（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。詳細については、「ログ ファイルへの HTTP/HTTPS ヘッダーの組み込み」（P.24-41）を参照してください。

W3C ログのカスタム フォーマットの設定

[システム管理（System Administration）] > [ログ サブスクリプション（Log Subscriptions）] ページを使用して、W3C ログ ファイル エントリのカスタム フォーマットを設定します。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。

図 24-5　W3C ログのカスタム ログ フィールドの設定



[ログ フィールド（Log Fields）] セクションの [カスタム フィールド（Custom Field）] テキスト ボックスに追加するカスタム フィールドを入力します。[カスタム フィールド（Custom Field）] テキスト ボックスに複数のカスタム 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。

（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。詳細については、「ログ ファイルへの HTTP/HTTPS ヘッダーの組み込み」（P.24-41）を参照してください。

ログ ファイルへの HTTP/HTTPS ヘッダーの組み込み

定義済みのアクセス ログおよび W3C ログ フィールドのリストに、HTTP/HTTPS トランザクションからのログを記録するすべてのヘッダー情報が含まれていない場合、アクセスおよび W3C ログ 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 フィールドを入力できます。

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。

表 24-12 は、アクセスおよび W3C ログに使用する構文を定義しています。

表 24-12　ログ ファイルの HTTP/HTTPS ヘッダーの設定

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)
```

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。スキャン エンジンがマルウェア スキャンの判定を DVS エンジンに返すので、DVS エンジンはスキャンされたオブジェクトをモニタするか、ブロックするかを判定できます。

これらは、URL 要求または応答コンテンツのいずれかにマルウェアが含まれる確率を示す数値を関連付ける独自の計算結果です。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。

Webroot、McAfee、および Sophos スキャン エンジンは、マルウェア スキャンの判定を DVS エンジンに返すことができます。DVS エンジンによるマルウェア スキャンの判定の処理方法の詳細については、「Cisco IronPort DVS™（Dynamic Vectoring and Streaming）エンジン」（P.19-5）を参照してください。

表 24-13 は、さまざまなマルウェア スキャンの判定値と対応する各マルウェア カテゴリを示します。

表 24-13　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	タイムアウト
3	エラー
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	Adware
14	システム モニタ
18	商用システム モニタ
19	ダイヤラ
20	ハイジャッカー
21	フィッシング URL
22	トロイのダウンローダ
23	トロイの木馬
24	トロイのフィッシャ
25	ワーム
26	暗号化ファイル
27	ウィルス
33	その他のマルウェア
34	PUA

表 24-13　マルウェア スキャンの判定値 （続き）

マルウェア スキャンの判定値	マルウェア カテゴリ
35	Aborted
36	アウトブレイク ヒューリスティック

トラフィック モニタ ログ

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。L4 トラフィック モニタ ログ ファイル エントリを確認し、ファイアウォールのブロック リストおよびファイアウォールの許可リストの更新を追跡できます。次に示すログ エントリの例を考慮してください。

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。L4 トラフィック モニタが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 アドレスを照合しました。その後、IP アドレスはファイアウォールのブロック リストに入力されます。

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。L4 トラフィック モニタがドメイン名エントリを照合し、それをアプライアンスの許可リストに追加しました。その後、IP アドレスはファイアウォールの許可リストに入力されます。

例 3

```
Firewall noted data from 172.xx.xx.xx to 209.xx.xx.xx (allowsite.net):80.
```

この例では、L4 トラフィック モニタがブロック リストにある内部 IP アドレスと外部 IP アドレス間で渡されたデータのログを記録します。また、L4 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ます。

トラブルシューティング

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。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するには、Cisco IronPort カスタマー サポートにお問い合わせください。

25
ネットワーク設定の構成

システム ホスト名の変更

hostname パラメータは、CLI プロンプトでシステムを識別する際に使用されます。システムの完全修飾ホスト名を入力する必要があります。hostname パラメータは、エンド ユーザ通知ページ、エンド ユーザ確認ページ、および 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際にマシンの NetBIOS 名を形成するためにも使用します。インターフェイスに設定されているホスト名とは直接関係はありません。

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
```

ネットワーク インターフェイスの設定

管理インターフェイス インターフェイス、データ インターフェイス、および L4 トラフィック モニタ インターフェイスの IP アドレス、サブネット、およびホスト名の情報を変更し、アプライアンスのネットワーク インターフェイスを設定できます。表 25-1 は、ユーザが設定できるネットワーク インターフェイスの設定を示します。

表 25-1　Web セキュリティ アプライアンスのネットワーク インターフェイスの設定

インターフェイス	ポート番号	説明
管理（Management）	M1	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。
データ（Data）	P1 および P2（プロキシ）	データ インターフェイスは Web プロキシのモニタリングと L4 トラフィック モニタのブロッキング（任意）に使用されます。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。 データ インターフェイスの設定に関する詳細については、「データ インターフェイスの設定」（P.25-2）を参照してください。
L4 トラフィック モニタ（L4 Traffic Monitor）	T1 および T2	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を設定するために使用されます。 • **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。

（注）　管理およびデータ インターフェイスをすべて設定する場合、それぞれに異なるサブネット上の IP アドレスを割り当てる必要があります。

次の方法を使用してネットワーク インターフェイスを管理できます。

- **Web インターフェイス。**[ネットワーク（Network）] > [インターフェイス（Interfaces）] ページを使用します。詳細については、「Web インターフェイスからのネットワーク インターフェイスの設定」（P.25-3）を参照してください。
- **コマンドライン インターフェイス。**ネットワーク インターフェイスを作成、編集、および削除するには、`ifconfig` CLI コマンドを使用します。

データ インターフェイスの設定

次のネットワーク インターフェイスの任意の組み合わせをデータ トラフィックに使用するように、Web セキュリティ アプライアンスを設定できます。

- M1 のみ
- M1 および P1
- M1、P1、および P2

- P1 のみ
- P1 および P2

システム セットアップ中またはシステム セットアップ後に、M1 および P1 ポートをイネーブルにできます。ただし、Web インターフェイスから、あるいは `ifconfig` CLI コマンドを使用する場合、システム セットアップ後に P2 ポートのみイネーブルにできます。

Web プロキシは、Web セキュリティ アプライアンスの設定に応じて、さまざまなネットワーク インターフェイス上のクライアントの Web 要求をリッスンします。

- **M1。**Web プロキシがアプライアンス管理サービス専用に制限するように設定されていない場合、このインターフェイス上の要求をリッスンします。
- **P1。**Web プロキシがイネーブルになっている場合、このインターフェイス上の要求をリッスンします。
- **P2。**デフォルトでは、Web プロキシがイネーブルになっている場合でも、このインターフェイスの要求をリッスンすることはありません。ただし、`advancedproxyconfig > miscellaneous` CLI コマンドを使用して、P2 上の要求をリッスンするように設定できます。

P2 を 2 番めのインターフェイスとして使用するようにアプライアンスを設定するには、次の手順を実行します。

ステップ 1　データ トラフィックのインターフェイスとして P1 を使用するようにアプライアンスを設定します。この操作は、システム セットアップ中、または [ネットワーク（Network）] > [インターフェイス（Interfaces）] ページで初期設定後に実行できます。

ステップ 2　Web インターフェイスで（「Web インターフェイスからのネットワーク インターフェイスの設定」（P.25-3）を参照）、または `ifconfig` CLI コマンドを使用して、P2 をイネーブルにします。

（注）　管理およびデータ インターフェイスをすべて設定する場合、それぞれに異なるサブネット上の IP アドレスを割り当てる必要があります。

ステップ 3　Web インターフェイスで、[ネットワーク（Network）] > [ルート（Routes）] ページに移動します。データ トラフィックのデフォルト ルートを変更して、P2 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。

（注）　`advancedproxyconfig > miscellaneous` CLI コマンドを使用して、クライアント要求をリスンするために 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。

Web インターフェイスからのネットワーク インターフェイスの設定

ステップ 1　[ネットワーク（Network）] > [インターフェイス（Interfaces）] ページに移動します。[設定の編集（Edit Settings）] をクリックします。

ステップ 2　必要に応じて、インターフェイスを設定します。

表 25-2 は、ユーザが各インターフェイスに定義できるインターフェイスの設定について説明します。

表 25-2　インターフェイスの設定

インターフェイスの設定	説明
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 IP アドレスを入力します。 管理ネットワーク上にある IP アドレスを入力します。
ネットマスク（Netmask）	このネットワーク インターフェイス上の Web セキュリティ アプライアンスを管理する際に使用するネットワーク マスクを入力します。
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を入力します。

ステップ 3　[ポート M1 をアプライアンス管理サービス用のみに制限（Restrict M1 port to appliance management services only）] フィールドを使用して、管理サービス用に別個のルーティングを設定するかどうかを指定します。

このチェックボックスがオンになっている場合、M1 ポートはアプライアンス管理サービスにのみ使用され、データ トラフィック（Web プロキシ）には使用されません。データ トラフィックにはもう 1 つのポートを設定し、管理トラフィックとデータ トラフィックには別個のルートを設定する必要があります。ルートの設定の詳細については、「TCP/IP トラフィック ルートの設定」（P.25-4）を参照してください。

ステップ 4　アプライアンス管理サービスを設定します。

Web インターフェイスを介して AsyncOS を管理するために HTTP または HTTPS を使用するかどうかを選択します。ユーザが設定した各プロトコルを使用して AsyncOS にアクセスするポートを指定する必要があります。

HTTP 要求を HTTPS にリダイレクトするように選択することもできます。この操作を行う場合、AsyncOS は HTTP と HTTPS の両方を自動的にイネーブルにします。

ステップ 5　「T」ネットワーク インターフェイスに接続されている有線接続のタイプを選択します。

- **デュプレックス タップ。**T1 ポートが着信トラフィックおよび発信トラフィックの両方を受信する場合、[デュプレックス タップ（Duplex TAP）] を選択します。半二重または全二重イーサネット接続を使用できます。
- **シンプレックス タップ。**T1 ポートを内部ネットワーク（クライアントからインターネットへのトラフィック フロー）に接続し、T2 ポートを外部ネットワーク（インターネットからクライアントへのトラフィック フロー）に接続する場合は、シンプレックス タップを選択します。

（注）　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。

ステップ 6　変更を送信し、保存します。

TCP/IP トラフィック ルートの設定

[ネットワーク（Network）] > [ルート（Routes）] ページまたは `routeconfig` コマンドを使用して、アプライアンス トラフィックのルートを定義し、スタティック ルートを追加し、IP ルーティング テーブルをロードし、デフォルト ゲートウェイを変更できます。

ルートは、トラフィック（ルーティング トラフィック）の送信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に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、ただし設定している場合）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。

分割ルーティングをイネーブルにするには、[ネットワーク（Network）] > [インターフェイス（Interfaces）] ページの [ポート M1 をアプライアンス管理サービス用のみに制限（Restrict M1 port to appliance management services only）] フィールドを使用します。詳細については、「Web インターフェイスからのネットワーク インターフェイスの設定」（P.25-3）を参照してください。

[ネットワーク（Network）] > [ルート（Routes）] ページ上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 トラフィックに別個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）。**管理トラフィックにのみ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（1 つは管理トラフィック、1 つはデータ トラフィック）が含まれます。図 25-1（P.25-6）は、オプションがイネーブルの場合の [ルート（Routes）] ページを示します。
- **すべてのトラフィックに 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）。**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）] ポート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 つのセクションが含まれます。

（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。

デフォルト ルートの変更

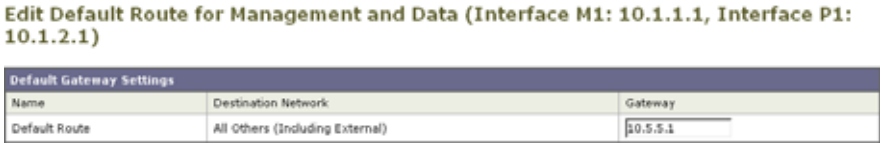
Web インターフェイスで、または CLI で `setgateway` CLI コマンドを使用して、デフォルト ゲートウェイを変更できます。

（注） 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にあるデータ インターフェイス上でトランザクションを送信します。

Web インターフェイスのデフォルト ゲートウェイを変更するには、次の手順を実行します。

ステップ 1　[ネットワーク（Network）] > [ルート（Routes）] ページに移動し、対応するテーブルの [デフォルト ルート（Default Route）] をクリックします。

図 25-1　デフォルト ルートの編集



ステップ 2　[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 3　変更を送信し、保存します。

ルーティング テーブルの操作

現在のルーティング テーブルをファイルに保存できます。以前に保存したルート テーブルをロードできます。新しいルートを追加したり、既存のルートを削除したりできます。

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。

以前に保存したルート 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、変更を送信し、保存します。

（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。

ルートの追加

ステップ 1　[ネットワーク（Network）] > [ルート（Routes）] ページに移動します。

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。

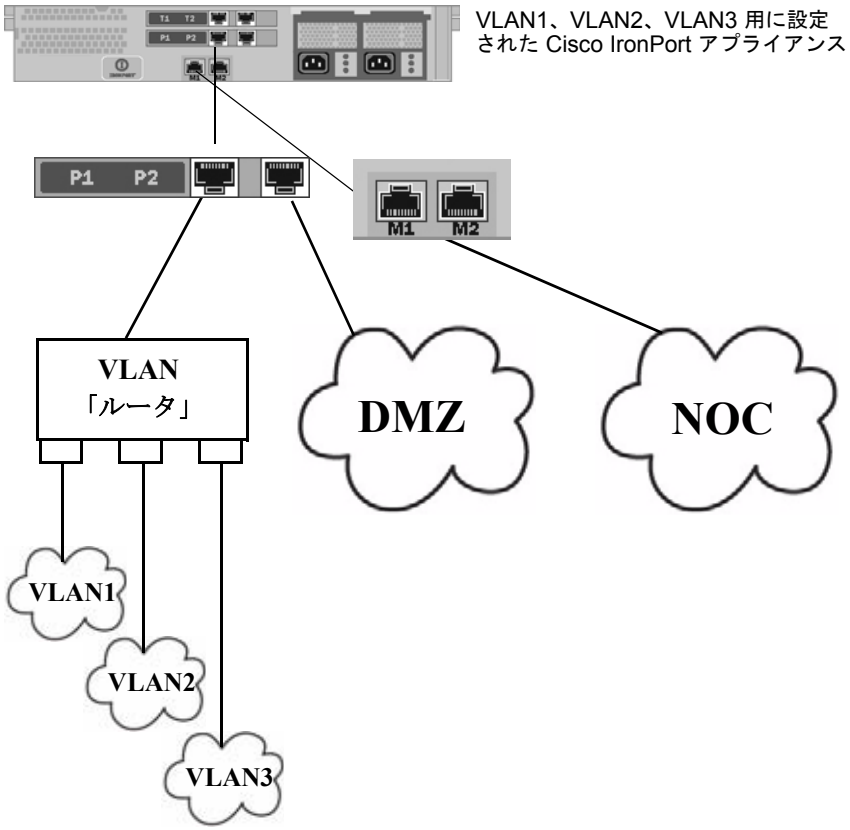
ステップ 3　名前、宛先ネットワーク、およびゲートウェイを入力します。

ステップ 4　変更を送信し、保存します。

仮想ローカル エリア ネットワーク（VLAN）

VLAN は物理データ ポートにバインドされた仮想ローカル エリア ネットワークです。1 つまたは複数の VLAN を設定し、組み込まれている物理インターフェイスの数を超えて、IronPort アプライアンスが接続できるネットワークの数を増加できます。たとえば、Web セキュリティ アプライアンスが VLAN に使用できる P1 と管理という 2 つのデータ インターフェイスがあるとします。VLAN は、既存のインターフェイスの別個の「ポート」上に追加のネットワークを定義できます。図 25-2 は、P1 インターフェイス上に複数の VLAN を設定する例を示します。

図 25-2　VLAN によるアプライアンスで使用可能なネットワーク数の増加



VLAN を使ってネットワークを分割することにより、セキュリティを向上させたり、管理作業を軽減したり、帯域幅を拡大したりできます。たとえば、P1 インターフェイス上に複数の VLAN を作成し、それぞれに異なるポリシーを適用します。VLAN は、「VLAN DDDD」という形式の名前を持つ動的な「データ ポート」として表示されます。「DDDD」は最大 4 桁の ID です（たとえば、VLAN 2、VLAN 4094 など）。AsyncOS は、最大 30 の VLAN をサポートします。同じ IronPort アプライアンス上で重複する VLAN ID は設定できません。

VLAN と物理ポート

物理ポートは、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。

VLAN の管理

VLAN の作成、編集、および削除を行うには、`etherconfig` コマンドを使用します。作成した VLAN は、CLI の `interfaceconfig` コマンドを使用して設定できます。すべての変更を保存することを忘れないでください。

etherconfig コマンドによる新しい VLAN の作成

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

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

```
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.

[]>
```

interfaceconfig コマンドによる VLAN 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。

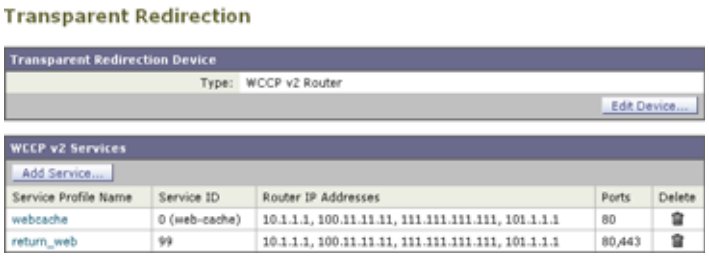
```
example.com> interfaceconfig

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.
- GROUPS - Define interface groups.
- 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
```

透過的リダイレクションの設定

Web セキュリティ アプライアンス Web プロキシ サービスをトランスペアレント モードで設定する場合は、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、接続されているデバイスを認識できるようにアプライアンスを設定する必要があります。[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）] ページでデバイスを設定します。

図 25-3　[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）] ページ



このページで、トラフィックをアプライアンスに透過的にリダイレクトするデバイス（レイヤ 4 スイッチまたは WCCP ルータ）を選択できます。デバイスとしてレイヤ 4 スイッチを選択した場合、このページで設定するものはありません。

ただし、デバイスとして WCCP ルータを選択した場合は、少なくとも 1 つの WCCP サービスを作成する必要があります。

WCCP サービスの使用

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。

次のサービス タイプを使用する WCCP サービスを作成できます。

- **標準サービス。**標準サービスは、その特性が WCCP ルータとアプライアンスの両方に認識されているため、ウェルノウン サービスとも呼ばれています。ポート 80 のトラフィックをリダイレクトします。これは、「web-cache」サービスとして識別されます。
- **ダイナミック サービス。**ダイナミック サービスは Web プロキシが作成するその他のサービスです。ただし、Web プロキシはサービス グループのコンポーネントをルータに記述する必要があります。AsyncOS は、定義を希望するダイナミック サービスの作成をサポートします。ダイナミック サービスを作成するには、サービス ID 番号、ポート番号を入力し、パケットを宛先ポートに基づいてリダイレクトするか、送信元ポートに基づいてリダイレクトするか、およびパケットをクライアント アドレスに基づいて配信するか、サーバ アドレスに基づいて配信するかを指定する必要があります。

Web キャッシュ通信プロトコルは 257 という別のサービス ID を使用できます。AsyncOS では、可能なサービス ID ごとにダイナミック WCCP サービスを作成できます。ただし、一般的な使用方法では、大部分のユーザが 1 つまたは 2 つ（この場合、1 つが標準サービス、その他がダイナミック サービス）の WCCP サービスを作成します。

任意のタイプの WCCP サービスを作成する場合は、次の情報を指定する必要もあります。

- **割り当て方式。**詳細については、「割り当て方式の使用」（P.25-12）を参照してください。
- **転送方式とリターン方式。**詳細については、「転送方式とリターン方式の使用」（P.25-13）を参照してください。

アプライアンスで IP スプーフィングをイネーブルにする場合は、2 つの WCCP サービスを作成する必要があります。詳細については、「WCCP 使用時の IP スプーフィング」（P.25-14）を参照してください。

割り当て方式の使用

WCCP は、リダイレクトされたパケットを Web プロキシ間で配布する方式として割り当て方式を定義します。この場合、1 つまたは複数の Web セキュリティ アプライアンス間で配布されます。割り当て方式は、ルータが複数 Web セキュリティ アプライアンスの間でパケットのロード バランシングを実行する方法を示します。

WCCP サービスを作成または編集するときは、[詳細（Advanced）] セクションの [ロードバランス方法（Load-Balancing Method）] フィールドで WCCP サービスの割り当て方式を設定します。

次の割り当て方式のいずれかを使用するように WCCP サービスを設定できます。

- **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。WCCP ルータがマスキングをサポートしない場合、ハッシュを使用する場合があります。

- **Allow Mask Only。**この方式は、マスキングに依存して、リダイレクションに関する決定を下します。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、ハードウェアがパケットをリダイレクトするため、非常に効率的です。ルータの CPU サイクルを削減し、ルータのパフォーマンスを向上するためにマスクを選択する場合があります。マスクの割り当てをサポートする WCCP ルータでのみマスクを使用できます。
- **Allow Hash or Mask。**マスクまたはハッシュ ロード バランシングのいずれかを行えるように WCCP サービスを設定することもできます。WCCP サービスがマスクとハッシュの両方を許可する場合、AsyncOS はルータと通信してルータがマスクをサポートするかどうかを決定します。ルータがマスクをサポートする場合、AsyncOS はサービス グループにマスキングを使用し、ルータがマスクをサポートしない場合、AsyncOS はサービス グループにハッシュを使用します。

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。
- **システムによって生成されるマスク。**システムがマスクを生成するように設定できます。任意で、システムにより生成されたマスクにビット数（最大 5 ビット）を指定できます。

転送方式とリターン方式の使用

WCCP は、ルータから Web プロキシにリダイレクトされたパケットを転送する方式として転送方式を定義します。逆に、リターン方式は Web プロキシからルータにパケットをリダイレクトします。

WCCP サービスを作成または編集する場合、[詳細（Advanced）] セクションの [フォワーディング方法（Forwarding Method）] および [リターン方法（Return Method）] フィールドで WCCP サービスの転送方式とリターン方式を設定します。

次の方式のいずれかを使用するように WCCP サービスを設定できます。

- **Layer 2 (L2)。**この方式は、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、トラフィックをリダイレクトします。この方式では、ターゲット Web プロキシがレイヤ 2 で直接ルータに接続されている必要があります。WCCP ルータは、アプライアンスがレイヤ 2 で直接ルータに接続されている場合にのみ、L2 ネゴシエーションを許可します。L2 方式は、ルータのハードウェア レベルでトラフィックをリダイレクトし、Generic Routing Encapsulation（GRE）よりもパフォーマンスがよくなります。ルータが直接アプライアンスに接続され、L2 方式を使用してパフォーマンスを向上させたい場合は、L2 を選択する場合があります。L2 転送をサポートする WCCP ルータでのみ L2 方式を使用できます。
- **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。この方式は、パフォーマンスに影響する可能性があるルータのソフトウェア レベルでトラフィックをリダイレクトします。アプライアンスが直接ルータに接続されていない場合、GRE を選択する場合があります。

L2 または GRE 方式のいずれかを許可するように WCCP サービスを設定することもできます。WCCP サービスが L2 と GRE の両方を許可する場合、アプライアンスはルータがサポートを表明す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。

（注） 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。

WCCP 使用時の IP スプーフィング

IP スプーフィングを行うように Web プロキシを設定できます。イネーブルになっている場合、クライアントから発信された要求はクライアントの送信元アドレスを保持し、Web プロキシではなくクライアントから発信されたように表示されます。

IP スプーフィングをイネーブルにするときは、2 つの WCCP サービスを作成する必要があります。1 つの WCCP サービス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必要があり、もう 1 つの WCCP サービスはリターン パスの送信元ポートに基づいてトラフィックをリダイレクトする必要があります。宛先ポートに基づくサービスは、標準 Web キャッシュ サービスにすることができます。ただし、ダイナミック サービスを少なくとも 1 つ作成する必要があります。

IP スプーフィングのために定義する 2 つの WCCP サービスは次の設定と同じ値を持つ必要があります。

- ポート番号
- ルータの IP アドレス
- ルータのセキュリティとパスワード

（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。

WCCP サービス作成の詳細については、「WCCP サービスの追加と編集」（P.25-14）を参照してください。

WCCP サービスの追加と編集

透過的リダイレクション デバイスを WCCP ルータとして設定する場合、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。アプライアンスで IP スプーフィングをイネーブルにする場合は、2 つの WCCP サービスを作成する必要があります。IP スプーフィングの詳細については、「WCCP 使用時の IP スプーフィング」（P.25-14）を参照してください。

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）] ページに移動します。

ステップ 2　透過的リダイレクション デバイスが WCCP v2 ルータになっていることを確認します。そうでない場合、[デバイスの編集（Edit Device）] をクリックして変更します。

ステップ 3　WCCP サービスを追加するには、[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）] カラムで WCCP サービスの名前をクリックします。

ステップ 4　WCCP オプションを設定します。

表 25-3 は、WCCP オプションについて説明します。

表 25-3　WCCP サービス オプション

WCCP サービス オプション	説明
サービス プロファイル名（Service Profile Name）	WCCP サービスの名前を入力します。
サービス（Service）	このセクションを使用して、ルータのサービス グループについて記述します。 標準（「ウェルノウン」）サービス グループまたはダイナミック サービス グループのいずれかを作成するように選択します。 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。**[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。**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。 • **ロード バランシングの基礎。**ネットワークが複数 Web セキュリティ アプライアンスを使用している場合、アプライアンス間でパケットを配布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。 ウェルノウンおよびダイナミック サービス グループの詳細については、「WCCP サービスの使用」（P.25-12）を参照してください。
ルータの IP アドレス（Router IP Addresses）	1 つまたは複数の WCCP 対応ルータの IP アドレスを入力します。サービス グループに最大 32 個のルータを入力できます。各ルータの IP アドレスを入力する必要があります。マルチキャスト アドレスは入力できません。

表 25-3　WCCP サービス オプション （続き）

WCCP サービス オプション	説明
ルータのセキュリティ（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。必要に応じて、[パスワード（Password）] フィールドにパスワードを入力します。パスワードは 7 文字以下の文字列です。 サービス グループのセキュリティをイネーブルにする場合、サービス グループを使用するすべてのアプライアンスと WCCP ルータが同じパスワードを使用する必要があります。 パスワードの要求により、どのルータおよび WCCP 対応システム（Web セキュリティ アプライアンスなど）をサービス グループの一部にするかを制御できます。 WCCP は、MD5 ハッシュ プロトコルを使用してパスワードを暗号化します。 **（注）** サービス グループの各アプライアンスまたは WCCP ルータは、WCCP メッセージ ヘッダーの確認後すぐに受信した WCCP パケットのセキュリティ コンポーネントを認証します。認証に失敗したパケットは廃棄されます。
詳細（Advanced）	次のフィールドを設定します。 • **ロード バランシング方式。** これは割り当て方式とも呼ばれています。マスク、ハッシュ、または両方を選択します。デフォルトは両方です。 ロード バランシングの詳細については、「割り当て方式の使用」（P.25-12）を参照してください。 • **転送方式。** L2、GRE、または両方を選択します。デフォルトは両方です。 転送方式に関する詳細については、「転送方式とリターン方式の使用」（P.25-13）を参照してください。 • **リターン方式。** L2、GRE、または両方を選択します。デフォルトは両方です。 リターン方式に関する詳細については、「転送方式とリターン方式の使用」（P.25-13）を参照してください。

ステップ 5　変更を送信し、保存します。

WCCP サービスの削除

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）] ページに移動します。

ステップ 2　ユーザが削除する WCCP サービスの [削除（Delete）] カラムのアイコンをクリックします。

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、および 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。

次のシナリオで SMTP リレー ホストを設定する場合があります。

- システムにより生成された電子メールを非ローカル電子メール アドレスに送信し、外部ネットワークへのポート 25 をブロックする場合。
- メール サーバが内部ホストから直接ポート 25 へのトラフィックを許可しない場合。

SMTP リレー ホストが定義されていない場合、AsyncOS は各電子メール アドレスのメール サーバに直接配信します。

（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。1 つのシステムが使用できなくなった場合の冗長性を確保するために、複数の SMTP リレー ホストを設定する場合があります。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。

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（CLI）のいずれかから SMTP リレー ホストを設定できます。

- **Web インターフェイス。**[ネットワーク（Network）] > [内部 SMTP リレー（Internal SMTP Relay）] ページを使用します。
- **コマンドライン インターフェイス。**`smtprelay` CLI コマンドを使用します。

Web インターフェイスからの SMTP の設定

ステップ 1　[ネットワーク（Network）] > [内部 SMTP リレー（Internal SMTP Relay）] ページに移動します。

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　表 25-4 に記載されている情報を入力します。

表 25-4　SMTP リレー ホスト設定

プロパティ	説明
リレーのホスト名または IP アドレス（Relay Hostname or IP Address）	SMTP リレーに使用するホスト名または IP アドレスを入力します。

表 25-4　SMTP リレー ホスト設定 （続き）

プロパティ	説明
ポート（Port）	SMTP リレーに接続するためのポートを入力します。このプロパティが空の場合、アプライアンスはポート 25 を使用します。このプロパティは省略可能です。
SMTP に使用するルーティング テーブル（Routing Table to Use for SMTP）	SMTP リレーへの接続に使用するアプライアンスのネットワーク インターフェイス（管理またはデータのいずれか）に関連付けられているルーティング テーブルを選択します。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　任意で、[行を追加（Add Row）] をクリックし、さらに SMTP リレー ホスト情報を追加できます。

ステップ 5　変更を送信し、保存します。

CLI からの SMTP の設定

smtprelay コマンドを使用して、SMTP リレー ホストを設定します。

次に例を示します。

```
example.com> smtprelay

No internal SMTP relay host configured.

Choose the operation you want to perform:

- NEW - Add a new host.

[]> new

Please enter the hostname of your relay host. You may put a colon after the hostname to
indicate a port to use other than 25, such as "smtp.example.com:547".
```

DNS サーバの設定

[ネットワーク（Network）] > [DNS] ページまたは dnsconfig コマンドを使用して、アプライアンスの DNS 設定を構成できます。DNS を設定する前に、次の点を考慮してください。

- インターネットの DNS サーバまたはユーザ独自の DNS サーバを利用するか、および使用する具体的なサーバ。
- DNS トラフィックに使用するルーティング テーブル。

  DNS サーバに接続するインターフェイス（データまたは管理）に関連付けられたルーティング テーブルを使用する必要があります。
- 逆引き DNS ルックアップがタイムアウトするまで待機する秒数。
- DNS キャッシュのクリア。

DNS サーバの指定

AsyncOS for Web 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

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。

インターネット ルート サーバの使用

AsyncOS DNS リゾルバは大量の同時 DNS 接続に対応するように設計されています。

複数エントリとプライオリティ

入力する各 DNS サーバに、数値でプライオリティを指定できます。AsyncOS では、プライオリティが 0 に最も近い DNS サーバの使用を試みます。DNS サーバが応答しない場合、AsyncOS は次のプライオリティを持つサーバの使用を試みます。同じプライオリティを持つ DNS サーバに複数のエントリを指定する場合、システムはクエリーを実行するたびに同じプライオリティを持つ DNS サーバをリストからランダムに選びます。次にシステムは最初のクエリーが期限切れになるか、「タイムアウト」になるまで短時間待機した後、さらに増加するそれよりわずかに長い時間後続のサーバを待機するという動作を続けます。待機時間の長さは、DNS サーバの実際の数と、設定されたプライオリティによって異なります。タイムアウトの長さはプライオリティに関係なく、すべての IP アドレスで同じです。最初のプライオリティには最も短いタイムアウトが設定されており、次のプライオリティにはより長いタイムアウトが設定されています。最終的なタイムアウト時間は約 60 秒です。1 つのプライオリティを設定している場合、該当のプライオリティに対する各サーバのタイムアウトは 60 秒になります。2 つのプライオリティを設定している場合、最初のプライオリティに対する各サーバのタイムアウトは 15 秒になり、次のプライオリティに対する各サーバのタイムアウトは 45 秒になります。3 つのプライオリティを設定している場合、タイムアウトは 5、10、45 秒と順に増加します。

たとえば、4 つの DNS サーバを設定し、2 つにプライオリティ 0 を、1 つにプライオリティ 1 を、もう 1 つにプライオリティ 2 を設定したとします。

表 25-5　DNS サーバ、プライオリティ、およびタイムアウト間隔の例

プライオリティ	サーバ	タイムアウト（秒）
0	1.2.3.4、1.2.3.5	5、5
1	1.2.3.6	10
2	1.2.3.7	45

AsyncOS は、プライオリティ 0 に設定された 2 つのサーバをランダムに選択します。プライオリティ 0 のサーバの 1 つがダウンしている場合は、もう 1 つのサーバが使用されます。プライオリティ 0 のサーバが両方ダウンしている場合、プライオリティ 1 のサーバ（1.2.3.6）が使用され、最終的にプライオリティ 2（1.2.3.7）のサーバが使用されます。

タイムアウト時間はプライオリティ 0 のサーバは両方とも同じであり、プライオリティ 1 のサーバにはより長い時間が設定され、プライオリティ 2 のサーバにはさらに長い時間が設定されます。

DNS アラート

アプライアンスのリブート時に、メッセージ「Failed to bootstrap the DNS cache」を含むアラートが生成される場合、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意味します。この事象は、ネットワーク接続が確立される前に DNS サブシステムがオンラインになった場合、ブートのタイミングで発生します。このメッセージが別のタイミングで表示された場合、ネットワーク問題が発生しているか、または DNS 設定で有効なサーバが指定されていないことを示しています。

DNS キャッシュのクリア

[ネットワーク（Network）] > [DNS] ページの [DNS キャッシュを消去（Clear DNS Cache）] ボタン、または `dnsflush` コマンドを使用して、ローカル DNS システムに変更が加えられたときに DNS キャッシュのすべての情報をクリアできます。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可能性があります。

DNS 設定の編集

ステップ 1　[ネットワーク（Network）] > [DNS] ページに移動します。

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　インターネットのルート DNS サーバまたはユーザ独自の DNS サーバを使用するか、またはインターネットのルート DNS サーバを使用して権威 DNS サーバを指定するかを選択します。

ステップ 4　ユーザ独自の DNS サーバを使用するか、権威 DNS サーバを指定する場合は、サーバ ID を入力し、プライオリティを指定し、必要に応じて Add Row キーを使用してサーバごとに繰り返します。

ステップ 5　DNS トラフィック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。

ステップ 6　逆引き DNS ルックアップを中止するまでに待機する秒数を入力します。

ステップ 7　ドメイン検索リストで、AsyncOS が DNS 一致を行う前にホスト名に追加する 0 個以上のドメイン サフィックスを入力します。

DNS ドメイン検索リストは、要求が DNS サーバで解決されない場合に使用されます。個々の指定されたドメインに対して、ホスト名とドメインの DNS 一致が見つかるかどうか順に試行されます。リストは、一致が見つかるまで順番に（左から右へ）検索されます。

ステップ 8　変更を送信し、保存します。

26
システム管理

S シリーズ アプライアンスの管理

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
- セキュリティ コンポーネントへのアップデート
- システム時刻

アプライアンスの設定の保存とロード

Web セキュリティ アプライアンス 内のすべての設定は、1 つのコンフィギュレーション ファイルを使用して管理できます。このファイルは Extensible Markup Language（XML）形式で保持されます。

現在の設定をアーカイブするには、[システム管理（System Administration）] > [設定のサマリー（Configuration Summary）] ページを使用して、アプライアンス設定の概要を印刷し、[システム管理（System Administration）] > [設定のサマリー（Configuration Summary）] ページを使用してシステムのコンフィギュレーション ファイルのローカル コピーを作成します。システムのコンフィギュレーション ファイルは、完全なコンフィギュレーションをインポートまたは一意のサブセクションをロードし、特定の設定を更新するために使用できます。

コンフィギュレーション ファイルを保存する場合、システムにより生成された名前を選択するか、独自のファイル名を定義できます。チェックボックスをクリックすることにより、ユーザのパスワードをマスクできます。パスワードをマスクすると、元の暗号化されたパスワードが、エクスポートまたは保存されたファイルで「*****」に置き換えられます。ただし、パスワードがマスクされたコンフィギュレーション ファイルを Web 用 AsyncOS に再びロードすることはできないことに注意してください。

[システム管理（System Administration）] > [設定ファイル（Configuration File）] ページの [設定をロード（Load Configuration）] セクションを使用して新しい設定情報を Web セキュリティ アプライアンスにロードします。次の方法のいずれかを使用して、情報をロードできます。

- `configuration` ディレクトリに情報を格納し、アップロードする。
- コンフィギュレーション ファイルをローカル マシンから直接アップロードする。
- Web インターフェイスに設定情報を直接貼り付ける。

コンフィギュレーション ファイルのコピーをロードするには、Web インターフェイスのページに直接コンフィギュレーションを貼ってください。コンフィギュレーション ファイルの上部に次のタグを含める必要があります。

```
<?xml version=”1.0” encoding=”ISO-8859-1”?> <!DOCTYPE config SYSTEM “config.dtd”>
<config> ... your configuration information in valid XML </config>
```

XML サブセクションをロードした後、アップデートを送信し、コミットします。

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。詳細については、「URL カテゴリのセットに対する更新の管理」（P.17-5）を参照してください。

アプライアンスの設定に変更内容をコミットする

設定を変更し、S シリーズ Web インターフェイスを使用してアプライアンスの動作を変更するたびに、まず変更内容を送信し、アクティブな設定にコミットする必要があります。

変更内容のコミットの詳細については、「変更内容のコミットおよびクリア」（P.2-9）を参照してください。

サポート コマンド

この項の機能は、アプライアンスをアップグレードする場合やサポート プロバイダーに問い合わせる場合に役に立ちます。[サポートとヘルプ（Support and Help）] メニューの [テクニカル サポート（Technical Support）] セクションで、次のコマンドを検索できます。

- **[サポートへの問い合わせを開く（Open a Support Case）]。**詳細については、「サポート事例を開く」（P.26-3）を参照してください。
- **[リモート アクセス（Remote Access）]。**詳細については、「リモート アクセス」（P.26-3）を参照してください。

- **[パケット キャプチャ（Packet Capture）]。**詳細については、「パケット キャプチャ」（P.26-4）を参照してください。

サポート事例を開く

アプライアンスを使用して、電子メールを Cisco IronPort カスタマー サポートに送信し、サポートを要請することができます。アプライアンスは電子メールを送信すると、アプライアンスの設定も送信します。次の方法で実行できます。

- **CLI。**`supportrequest` コマンドを使用します。
- **Web インターフェイス。**[サポートとヘルプ（Support and Help）] メニュー > [サポート ケースを開く（Open A Support Case）] ページを使用します。

サポート要求を送信すると、サポートが必要な問題を説明するコメントを入力できます。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。

ステップ 1　[サポートとヘルプ（Support and Help）] メニューから、[サポートへの問い合わせを開く（Open A Support Case）] を選択します。

ステップ 2　このサポート要求を他の人に送信する場合は、[その他の受信者（Other Recipients）] フィールドに、カンマで区切った他の電子メール アドレスを入力します。

デフォルトでは、サポート要求（コンフィギュレーション ファイルを含む）が Cisco IronPort カスタマー サポートに送信されます（フォーム上部のチェックボックスを使用）。

ステップ 3　名前および電子メールなどの連絡先情報を入力します。

ステップ 4　[問題の優先度（Issue Priority）] フィールドから、このサポート要求の優先度を選択します。

ステップ 5　[問題の優先度（Issue Priority）] フィールドに、送信される電子メールの件名行で使用されるテキストを入力します。

ステップ 6　[問題の説明（Issue Description）] フィールドに、問題の説明を入力します。

ステップ 7　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。

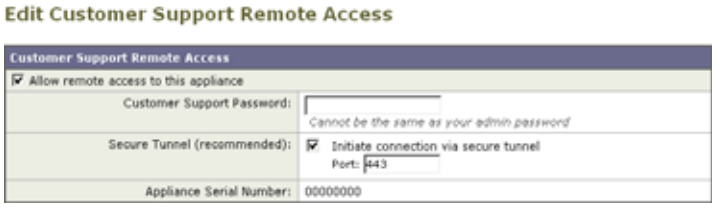
ステップ 8　[送信（Send）] をクリックします。トラブル チケットがシスコで作成されます。

詳細については、「シスコのテクニカル サポート」（P.1-10）を参照してください。

リモート アクセス

Web セキュリティ アプライアンスへの Cisco IronPort カスタマー サポート リモート アクセスを許可するには、[サポートとヘルプ（Support and Help）] メニュー > [リモート アクセス（Remote Access）] ページを使用します。[リモート アクセス設定の編集（Edit Remote Access Settings）] をクリックして、アプライアンスにアクセスするための Cisco IronPort カスタマー サポートを許可します。

図 26-1　[リモート アクセス（Remote Access）] ページ



リモート アクセスをイネーブルにすると、デバッグとシステムへの一般的なアクセスに対して、Cisco IronPort カスタマー サポートによって使用される特別なアカウントを有効にすることになります。これは、Cisco IronPort カスタマー サポートがシステムの設定、設定の理解、および問題レポートの調査でお客様を補助するなどの作業に使用します。また、CLI で `techsupport` コマンドを使用することもできます。

「セキュアなトンネル」をイネーブルにすると、アプライアンスは指定済みポートを介してサーバ upgrades.ironport.com への SSH トンネルを作成します。デフォルトでこの接続はほとんどの環境で機能するポート 443 を介して行われます。upgrades.ironport.com への接続が確立されたら、Cisco IronPort 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へのアクセスを取得できます。ポート 443 を介した接続が許可される限り、ほとんどのファイアウォールの制限は適用されません。また、CLI で `techsupport tunnel` コマンドを使用することもできます。

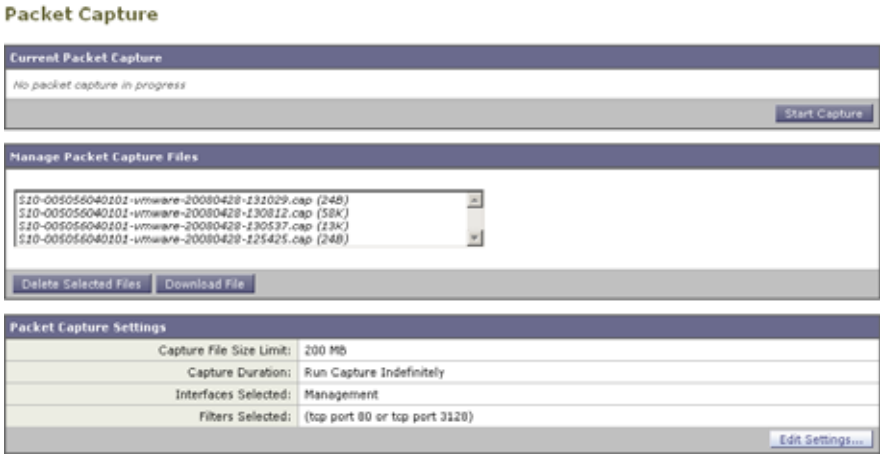
「リモート アクセス」と「トンネル」の両方のモードでは、パスワードが必要です。これは、システムへのアクセスに使用されるパスワードでは*ない*ことを理解しておくことが重要です。そのパスワードとシステムのシリアル番号（物理アプライアンス）または VLN（仮想アプライアンス）がカスタマー サポート担当者に提供された後で、アプライアンスへのアクセスに使用されるパスワードが生成されます。

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 日経ったら、techsupport トンネルを使用して新しく接続することはできません。7 日後にトンネルを使用している既存の接続がある場合、これらの接続は継続して作用します。ただし、これらの接続が切断されると、techsupport トンネルは 7 日後に切断されるため、再接続することはできません。SSH トンネル接続に設定されたタイムアウトはリモート アクセス アカウントに適用されません。リモート アクセス アカウントは特に非アクティブ化するまではアクティブです。

パケット キャプチャ

場合によっては、問題発生時に Cisco IronPort カスタマー サポートに問い合わせたときに、Web セキュリティ アプライアンスとのネットワーク状況について尋ねられることがあります。アプライアンスでは、アプライアンスが接続されたネットワークで送受信されている TCP/IP と他のパケットを傍受および表示できます。

パケット キャプチャを実行してネットワーク設定をデバッグしたり、どのようなネットワーク トラフィックがアプライアンスに到達または送出されているかを検出したりする場合があります。



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。パケット キャプチャ ファイルの最大サイズ、パケット キャプチャの実行時間、およびキャプチャを実行するネットワーク インターフェイスを設定できます。また、フィルタを使用して、パケット キャプチャで表示されるパケット数を制限できます。これは、大量のトラフィックによるネットワークの出力をより使用しやすくします。FTP または Cisco IronPort カスタマー サポートを使用して、保存された任意のパケット キャプチャ ファイルを、デバッグやトラブルシューティングのために送信できます。

[サポートとヘルプ（Support and Help）] > [パケット キャプチャ（Packet Capture）] ページには、ハード ドライブに格納された完全なパケット キャプチャ ファイルの一覧が表示されます。パケット キャプチャが実行されている場合、Web インターフェイスには、実行中のキャプチャのステータス（ファイル サイズや経過時間など）の現在の統計情報が表示されます。

Web インターフェイスの [ダウンロード（Download）] ボタンを使用するか、FTP を使用してアプライアンスに接続して、captures ディレクトリから取得することで、パケット キャプチャ ファイルをダウンロードできます。

CLI では、`packetcapture` コマンドを使用します。

Web インターフェイスで、[サポートとヘルプ（Support and Help）] メニューの下の [パケット キャプチャ（Packet Capture）] オプションを選択します。

（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

CLI でパケット キャプチャを開始するには、`packetcapture` > start コマンドを実行します。実行中のパケット キャプチャを停止する必要がある場合は、`packetcapture > stop` コマンドを実行します。

Web インターフェイスでパケット キャプチャを開始するには、[サポートとヘルプ（Support and Help）] メニューの [パケット キャプチャ（Packet Capture）] オプションを選択し、[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停止するには、[キャプチャを停止（Stop Capture）] をクリックします。

（注）　Web インターフェイスに表示されるのは Web インターフェイスで開始されたパケット キャプチャだけで、CLI で開始されたパケット キャプチャは表示されません。同様に、CLI には CLI で開始された現在のパケット キャプチャのステータスだけが表示されます。

パケット キャプチャ設定の編集

CLI でパケット キャプチャ設定を編集するには、`packetcapture` > setup コマンドを実行します。

Web インターフェイスでパケット キャプチャ設定を編集するには、[サポートとヘルプ（Support and Help）] メニューの [パケット キャプチャ（Packet Capture）] オプションを選択し、[設定を編集（Edit Settings）] をクリックします。

表 26-1 に、設定可能なパケット キャプチャの項目を示します。

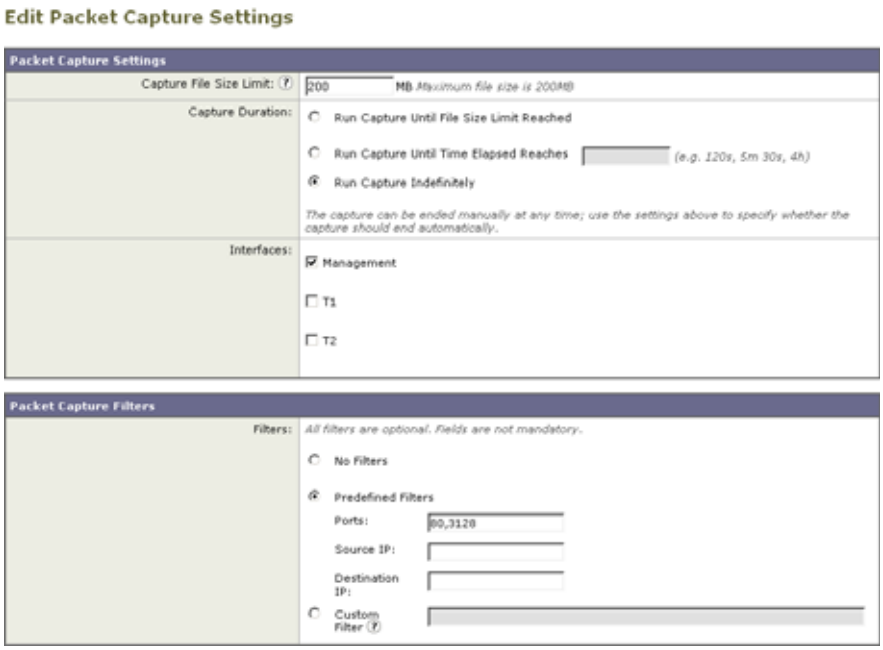
表 26-1　パケット キャプチャ設定オプション

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）	すべてのパケット キャプチャ ファイルの最大ファイル サイズ。
キャプチャ期間（Capture duration）	パケット キャプチャの実行時間を選択します。 • **[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）]。**パケット キャプチャは、ファイル サイズ制限に到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）]。**パケット キャプチャは、設定された時間が経過するまで実行されます。時間は秒単位（s）、分単位（m）、または時間単位（h）で入力できます。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。 **注：**全体の時間が経過する前にファイルが最大サイズ制限に到達した場合は、既存のファイルが削除され（データが破棄されます）、現在のパケット キャプチャ データで新しいファイルが開始されます。 • **[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：**パケット キャプチャを手動で停止する前にファイルが最大サイズ制限に到達した場合は、既存のファイルが削除され（データが破棄されます）、現在のパケット キャプチャ データで新しいファイルが開始されます。 パケット キャプチャはいつでも手動で停止できます。
キャプチャ対象ネットワーク インターフェイス（Network interface to capture）	パケット キャプチャを実行するネットワーク インターフェイスを選択します。
フィルタ（Filters）	パケット キャプチャで保存されるデータの量を削減するために、パケット キャプチャにフィルタを適用するかどうかを選択します。 事前定義されたフィルタの 1 つを使用してポート、ソース IP アドレス、または宛先 IP アドレスでフィルタリングしたり、UNIX の tcpdump コマンドでサポートされた構文を使用してカスタム フィルタを作成したりできます。

（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。

図 26-2（P.26-7）に、Web インターフェイスでパケット キャプチャ設定を編集する例を示します。

図 26-2　Web インターフェイスでのパケット キャプチャ設定の編集



機能キーでの作業

場合によっては、サポート チームが、システムで特定の機能をイネーブルにするキーを提供することがあります。Web インターフェイスで [システム管理（System Administration）] > [ライセンス キー（Feature Keys）] ページ（または CLI で `featurekey` コマンド）を使用し、キーを入力して、関連付けられた機能をイネーブルにします。

キーはアプライアンスのシリアル番号とイネーブルにされる機能に固有です（あるシステムのキーを別のシステムで再使用することはできません）。キーを間違って入力した場合は、エラー メッセージが生成されます。

機能キーの機能は [ライセンス キー（Feature Keys）] と [ライセンス キーの設定（Feature Key Settings）] の 2 つのページに分割されます。

（注）　Web セキュリティ仮想アプライアンスの機能キーは仮想アプライアンスのライセンス ファイルに含まれ、別途インストールできません。詳細については、「Cisco Web セキュリティ仮想アプライアンス ライセンス」（P.26-9）を参照してください。

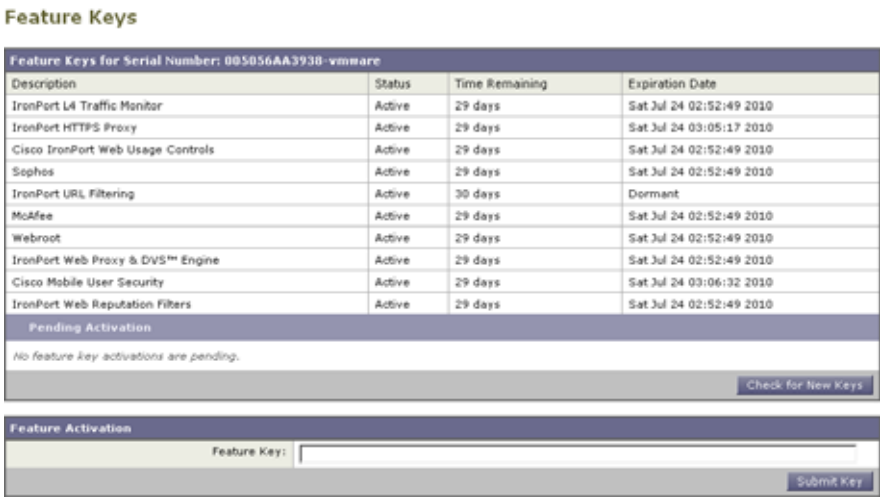
[ライセンス キー（Feature Keys）] ページ

[ライセンス キー（Feature Keys）] ページの内容は次のとおりです。

- アプライアンスのすべてのアクティブな機能キーが表示されます。
- アクティベーション待ちのすべての機能キーが表示されます。
- 発行された新しいキーを検索します（これは任意で、キーをインストールすることもできます）。

現在イネーブルな機能の一覧が表示されます。[保留中のライセンス（Pending Activation）] セクションは、アプライアンスに対して発行され、まだアクティベートされていない機能キーの一覧です。設定に応じてアプライアンスが新しいキーを定期的に確認することがあります。[新しいキーをチェック（Check for New Keys）] をクリックすると、待機状態のキーの一覧が更新されます。

図 26-3　　[ライセンス キー（Feature Keys）] ページ

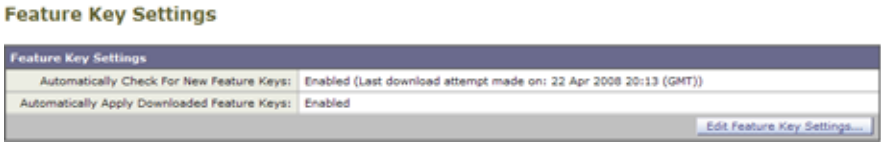


また、`featurekey` CLI コマンドを使用して、[ライセンス キー（Feature Keys）] ページで同じタスクを行うことができます。

[ライセンス キーの設定（Feature Key Settings）] ページ

[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。

図 26-4　　[ライセンス キーの設定（Feature Key Settings）] ページ



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。機能が追加されない場合は、エラー メッセージが表示されます（キーが正しくない場合など）。それ以外の場合は、機能キーが画面に追加されます。

[保留中のライセンス（Pending Activation）]一覧の新しい機能キーをアクティベートするには、そのキーを選択し（[選択（Select）] チェックボックスをオンにします）、[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。

また、`featurekeyconfig` CLI コマンドを使用して、[ライセンス キーの設定（Feature Key Settings）] ページと同じタスクを行うことができます。

期限切れ機能キー

（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。

Cisco Web セキュリティ仮想アプライアンス 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。このライセンスは複数のクローン作成された仮想アプライアンスに使用できます。

このライセンスをインストールするには、`loadlicense` CLI コマンドを実行します。CLI にライセンスをコピー アンド ペーストするか、コマンドを実行する前に、FTP を使用してアプライアンスの `configuration` ディレクトリにアップロードできます。また、システム セットアップ ウィザードを実行する前にアプライアンスにインストールする必要があります。

機能キーは仮想アプライアンスのライセンスに含まれています。機能キーは、まだキーがアクティブ化されてない場合でも、ライセンスと同時に失効します。新しい機能キーの購入の際は、新しい仮想アプライアンスのライセンスをダウンロードしてインストールする必要があります。

仮想アプライアンスのライセンスに機能キーが含まれるため、AsyncOS for Web 機能の 30 日間評価はありません。

（注） 仮想アプライアンスのライセンスをインストールする前に、テクニカル サポートのトンネルを開くことはできません。

Web セキュリティ仮想アプライアンスの設定および実行の詳細については、『*Cisco Security Virtual Appliance Installation Guide*』を参照してください。

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。

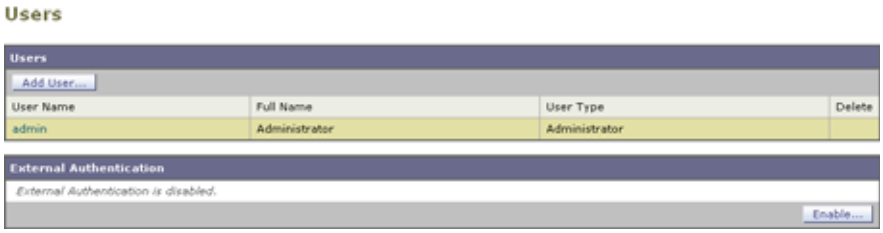
- **ローカル ユーザ。**アプライアンス自体にローカルにユーザを定義できます。詳細については、「ローカル ユーザの管理」（P.26-10）を参照してください。

- **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。詳細については、「RADIUS ユーザ認証」（P.26-13）を参照してください。

Web インターフェイスで [システム管理（System Administration）] > [ユーザ（Users）] ページ（または、CLI で `userconfig` コマンド）を使用して、ローカル ユーザおよび外部認証サーバへの接続を管理できます。

図 26-5 に、ローカル ユーザおよび外部認証を管理する例を示します。

図 26-5　[システム管理（System Administration）] > [ユーザ（Users）] ページ



（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。

ローカル ユーザの管理

Web セキュリティ アプライアンスにローカルに任意の数のユーザを定義できます。ローカル ユーザを追加、編集、および削除できます。ローカル ユーザを定義する場合は、次のルールを考慮してください。

- ユーザ名には小文字、数字、およびダッシュ（-）文字を含めることができます。
- ユーザ名は先頭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。
- パスワードは最低 6 文字にする必要があります。
- ユーザ名はシステムで予約されている特殊名（「operator」や「root」など）にすることはできません。
- 外部認証も使用する場合は、ユーザ名を外部認証されたユーザ名と重複させることはできません。

（注）　ローカル ユーザの異なるプリファレンス（言語サポートなど）を定義できます。詳細については、「ユーザ プリファレンスの定義」（P.26-16）を参照してください。

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。

新しいユーザ アカウントを作成するには、ユーザ名と氏名を指定してから、ユーザ ロール タイプにユーザを割り当てます。各ユーザ タイプは、異なるレベルのデフォルト権限を提供します。表 26-2 は、割り当てることができるユーザ タイプを一覧表示します。

表 26-2　ユーザ タイプ

グループ	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` 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）	ユーザがユーザ アカウントを作成、編集、または削除できないように制限します。また、オペレータ グループは次のコマンドの使用を制限します。: • `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 ユーザは、システムのステータス情報だけを参照できます。

グループにユーザを割り当てたら、新しいアカウントのパスワードを指定する必要があります。

（注）　admin ユーザ パスワードを紛失した場合、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 ユーザの追加

ステップ 1　[システム管理（System Administration）] > [ユーザ（Users）] ページで、[ユーザを追加（Add User）] をクリックします。

ステップ 2　ユーザの名前を入力します。一部の単語（「operator」や「root」など）は予約されています。

ステップ 3　ユーザの氏名を入力します。

ステップ 4　ユーザ タイプを選択します ユーザ タイプの詳細については、表 26-2「ユーザ タイプ」（P.11）を参照してください。

ステップ 5　パスワードを入力し、パスワードを再入力します。

ステップ 6　変更を送信し、保存します。

ユーザの削除

ステップ 1　[システム管理（System Administration）] > [ユーザ（Users）] ページで、一覧表示されたユーザ名に対応するゴミ箱アイコンをクリックします。

ステップ 2　表示される警告ダイアログで [削除（Delete）] をクリックして削除を確認します。

ステップ 3　変更を送信し、保存します。

ユーザの編集

ステップ 1　[システム管理（System Administration）] > [ユーザ（Users）] ページで、ユーザ名をクリックします。

ステップ 2　[ユーザの編集（Edit User）] ページでユーザに変更を加えます。

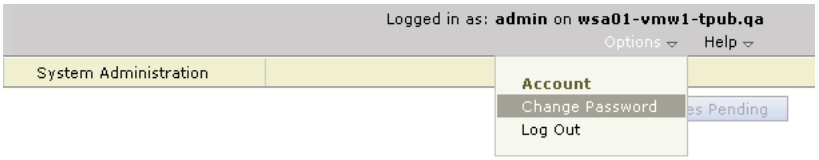
ステップ 3　変更を送信し、保存します。

パスワードの変更

Web インターフェイスの右側上部の [オプション（Options）] メニューの下にある [パスワード変更（Change Password）] オプションを使用して、自分のパスワードを変更できます。

図 26-6 に、現在のユーザ パスワードを変更する例を示します。

図 26-6　[パスワード変更（Change Password）] オプション



（注）　admin アカウントのパスワードを変更するには、[システム管理（System Administration）] > [ユーザ（Users）] ページを使用するか、CLI で `password` または `passwd` コマンドを使用します。パスワードの変更はすぐに有効になり、コミットする必要はありません。

CLI でのユーザのモニタリング

`who`、`whoami`、および `last` コマンドは、アプライアンスへのユーザ アクセスをモニタするのに使用できます。

- `who` コマンドは、ユーザ、ログイン時間、アイドル時間、およびユーザがログインしたリモート ホストを一覧表示します。

```
example.com> who

Username  Login Time  Idle Time  Remote Host  What
```

```
========  ==========  =========  ===========  ====

admin     03:27PM     0s         10.xx.xx.xx  cli
```

- whoami コマンドは、ユーザ名とグループの情報を表示します。

```
example.com> whoami

Username: admin

Full Name: Administrator

Groups: admin, operators, config, log, guest
```

- last コマンドは、アプライアンスに最近ログインしていたユーザに関する情報を表示します。

```
example.com> last

Username  Remote Host  Login Time        Logout Time       Total Time

========  ===========  ================  ================  ==========

admin     10.xx.xx.xx  Sat May 15 23:42  still logged in   15m

admin     10.xx.xx.xx  Sat May 15 22:52  Sat May 15 23:42  50m

admin     10.xx.xx.xx  Sat May 15 11:02  Sat May 15 14:14  3h 12m

admin     10.xx.xx.xx  Fri May 14 16:29  Fri May 14 17:43  1h 13m

shutdown                                 Fri May 14 16:22
```

RADIUS ユーザ認証

アプライアンスにログインするユーザの認証に RADIUS ディレクトリ サービスを使用して行うように、Web セキュリティ アプライアンスを設定できます。HTTP、HTTPS、SSH、および FTP を使用してアプライアンスにログインする場合、外部認証を使用できます。認証のために外部ディレクトリを使用するようアプライアンスを設定するには、Web インターフェイスで [システム管理（System Administration）] > [ユーザ（Users）] ページを使用するか、userconfig > external CLI コマンドを使用します。

アプライアンスは、認証用に複数の外部サーバと連携させるように設定できます。1 つのサーバが一時的に使用できない場合、フェールオーバーを実行できるように、複数の外部サーバを定義する必要がある場合があります。複数の外部サーバを定義する場合、アプライアンスは、アプライアンスに定義されている順序でサーバに接続します。

外部認証がイネーブルであり、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、アプライアンスは最初に、ユーザがシステム定義の「admin」アカウントであるかどうかを確認します。ユーザがシステム定義の「admin」アカウントでない場合、アプライアンスは最初に設定された外部サーバをチェックしてユーザがそこで定義されたかどうかを確認します。アプライアンスが最初の外部サーバに接続できなければ、アプライアンスは一覧の次の外部サーバをチェックします。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。そのユーザが外部サーバまたはアプライアンスに存在しない場合、またはユーザが間違ったパスワードを入力した場合は、アプライアンスへのアクセスが拒否されます。

外部認証を使用する場合、次のルールとガイドラインを考慮してください。

- 最大 10 個の RADIUS サーバを設定できます。
- アプライアンスでは、Password Authentication Protocol（PAP）または Challenge Handshake Authentication Protocol（CHAP）を使用して RADIUS ディレクトリと通信できます。
- 管理者ユーザのロール タイプにすべての RADIUS ユーザをマッピングしたり、異なる Web セキュリティ アプライアンスのユーザ ロール タイプにすべての RADIUS ユーザをマッピングできます。
- ローカル ユーザも追加する場合は、ローカル ユーザ名が外部認証されたユーザ名と重複していないようにしてください。

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、[有効（Enable）] をクリックします。

ステップ 2　すでに有効になっていない場合は、[外部認証を有効にする（Enable External Authentication）] オプションをオンにします。

ステップ 3　RADIUS サーバのホスト名を入力します。

ステップ 4　RADIUS サーバのポート番号を入力します。デフォルトのポート番号は 1812 です。

ステップ 5　RADIUS サーバの共有秘密パスワードを入力します。

ステップ 6　タイムアウトするまでアプライアンスがサーバからの応答を待つ時間を秒単位で入力します。

ステップ 7　（任意）[行を追加（Add Row）] をクリックして別の RADIUS サーバを追加します。各 RADIUS ログについて、3 ～ 6 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 8　RADIUS サーバに問い合わせ、「External Authentication Cache Timeout」フィールドで再認証するまで、AsyncOS が外部認証クレデンシャルを保存する秒数を入力します。デフォルトはゼロ（0）です。

（注）　RADIUS サーバがワンタイム パスワード（たとえば、トークンから作成されるパスワード）を使用する場合、ゼロ（0）を入力します。値をゼロに設定すると、AsyncOS は、現在のセッション中に認証のために RADIUS サーバに再アクセスしません。

ステップ 9　グループ マッピングの設定

設定	説明
外部認証されたユーザを複数のローカルロールに割り当てます。（Map externally authenticated users to multiple local roles.）	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： • 3 文字以上 • 253 文字以下 • コロン、カンマ、または改行文字なし • 各 RADIUS ユーザに対し 1 つ以上のマップ済み CLASS 属性（この設定を使用する場合、AsyncOS は、マップ済み CLASS 属性のない RADIUS ユーザへのアクセスを拒否します）。 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。 次のアプライアンス ロールは、制限の少ないものから順番に並べられています。 • 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）
外部認証されたすべてのユーザを管理者ロールに割り当てます。（Map all externally authenticated users to the Administrator role.）	AsyncOS は RADIUS ユーザを Administrator ロールに割り当てます。

ステップ 10　管理者ロールまたは異なるアプライアンス ユーザ ロール タイプにすべての外部認証されたユーザをマッピングするかを選択します。

ステップ 11　異なるロール タイプにユーザをマッピングする場合、[グループ名（Group Name）] または [ディレクトリ（Directory）] フィールドの RADIUS CLASS 属性に定義されているようにグループ名を入力し、[ロール（Role）] フィールドからアプライアンス ロール タイプを選択します。[行を追加（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。

ユーザ ロール タイプの詳細については、「ローカル ユーザの管理」（P.26-10）を参照してください。

ステップ 12　変更を送信し、保存します。

ユーザ プリファレンスの定義

ローカル ユーザは、各アカウントに固有な言語などのプリファレンス設定を定義できます。これらの設定は、ユーザがアプライアンスに最初にログインするときにデフォルトで適用されます。各ユーザにプリファレンス設定が保存され、ユーザがアプライアンスにログインするクライアント マシンに関係なく同じです。

ユーザがこれらの設定を変更し、変更をコミットしないと、再びログインするときに設定がデフォルト値に戻ります。

表 26-3 に、定義できるユーザ プリファレンス設定を示します。

表 26-3　ユーザ プリファレンス設定

プリファレンス設定	説明
言語の表示（Language Display）	Web インターフェイスおよび CLI で使用する言語の Web 用 AsyncOS。
ランディング ページ（Landing Page）	ユーザがアプライアンスにログインするときに表示されるページ。
表示されるレポート時間範囲（デフォルト）（Reporting Time Range Displayed (default)）	[レポート（Reporting）] タブでレポートに対して表示するデフォルトの時間範囲。
表示されるレポート行数（Number of Reporting Rows Displayed）	デフォルトで各レポートに表示されるデータの行数。

ステップ 1　プリファレンス設定を定義するユーザ アカウントによるアプライアンスにログインします。

ステップ 2　[オプション（Options）] メニューから [環境設定（Preferences）] を選択します。

ステップ 3　[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 4　表 26-3 で説明されている設定を設定します。

ステップ 5　変更を送信し、保存します。

管理者の設定

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。特定の組織の要件を満たすには、これを実行する必要がある場合があります。

`adminaccessconfig` CLI コマンドを使用してこれらの設定を設定します。次のようにアプライアンスを設定できます。

- 管理者のログインでユーザ定義のテキストを表示する。
- 特定のマシンへの管理者のアクセスを制限する。
- 管理者アクセスにより強力な SSL 暗号を必要とする。

ログイン時のカスタム テキストの設定

`adminaccessconfig > banner` CLI コマンドを使用して、管理者がログインを試みるときに、指定するテキストを表示するようにアプライアンスを設定できます。組織のポリシーと条件をユーザに知らせるバナーを表示するように、この設定が必要となる場合があります。Web インターフェイスまたは FTP 経由などですべてのインターフェイスを通じて管理者がアプライアンスにアクセスしようとするときに、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。

IP ベースの管理者アクセスの設定

`adminaccessconfig > ipaccess` CLI コマンドを使用して、どの IP アドレスで管理者が Web セキュリティ アプライアンスにアクセスするかを制御できます。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。

管理者アクセスに対する SSL 暗号の設定

`adminaccessconfig > strictssl` CLI コマンドを使用して、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できます。

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。

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。返信アドレスの表示、ユーザ、およびドメイン名を指定できます。ドメイン名に仮想ゲートウェイ ドメインの使用を選択することもできます。

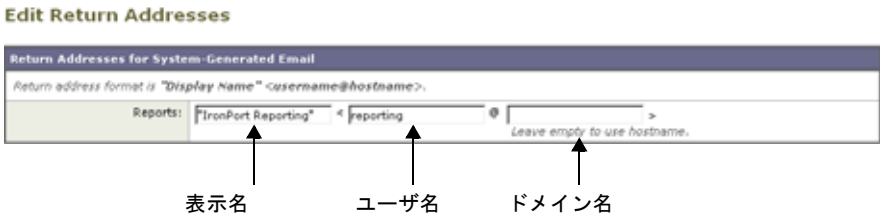
[システム管理（System Administration）] > [返信先アドレス（Return Addresses）] ページで返信アドレスを設定します。

図 26-7　　[返信先アドレス（Return Addresses）] の設定

ステップ 1　[システム管理（System Administration）] > [返信先アドレス（Return Addresses）] ページの順に進みます。

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

図 26-8　返信アドレス設定の編集



ステップ 3　レポートでは、図 26-8 に表示されているフィールドに、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、IronPort アプライアンスで発生しているイベントに関する情報が記載されている、電子メールによる通知のことです。これらのイベントにはマイナー（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。アラートは、IronPort アプライアンスで生成されます。送信するアラート メッセージの種類、重大度、および送信するユーザを指定できます。アラートは、Web インターフェイスの [システム管理（System Administration）] > [アラート（Alerts）] ページ（または CLI の `alertconfig` コマンド）で管理します。

（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。SMTP リレー ホストの設定については、「SMTP リレー ホストの設定」（P.25-17）を参照してください。

アラートの概要

アラート機能は 2 つの主要な部分から構成されます。

- [アラート（Alerts）] : アラート受信者（アラートを受信する電子メール アドレス）、および受信者に送信されるアラート通知（重大度およびアラート タイプ）で構成されます。
- [アラート設定（Alert Settings）] : アラート送信者（[FROM:]）アドレス、重複したアラートを送信するまでに待機する秒数、および AutoSupport をイネーブルにするかどうか（およびオプションで毎週 AutoSupport レポートを送信するかどうか）などのアラート機能に関する全般的な動作を指定します。

アラート：アラート受信者、アラート分類、および重要度

アラートとは、アラート受信者に送信される、ハードウェアやアンチウイルスの問題など特定の機能（またはアラート分類）に関する情報が記載された電子メール メッセージまたは通知のことです。アラート受信者とは、アラート通知が送信される電子メール アドレスのことです。通知に含まれる情報は、アラート分類と重大度によって決まります。アラート受信者に送信するアラート分類と重大度を指定できます。アラート エンジンでは、送信するアラートの種類とアラート受信者を詳細に制御できます。たとえば、アラート受信者が System（アラートの種類）に関する Critical（重大度）の情報が送信されたときのみ通知を受信するように設定することで、アラート受信者に特定のアラートのみを送信するように設定できます。また、一般的な設定値も設定できます（「アラート設定値の設定」（P.26-23）を参照してください）。

アラートの分類

AsyncOS では、次のアラート分類を送信します。

表 26-4　アラートの分類とコンポーネント

アラートの分類	アラートのコンポーネント
システム	System
ハードウェア	Hardware
アップデータ	Updater
Web プロキシ	Proxy
DVS™ および Anti-Malware	DVS
L4 トラフィック モニタ	TrafMon

重大度

アラートは、次の重大度に従って送信されます。

- Critical：すぐに対処が必要です。
- Warning：今後モニタリングが必要な問題またはエラー。すぐに対処が必要な可能性もあります。
- Information：デバイスのルーティン機能で生成される情報。

アラート設定

アラート設定では、アラートの全般的な動作と設定を制御します。設定には次のような項目があります。

- RFC 2822 Header From：アラートを送信するタイミング（アドレスを入力するか、デフォルトの「alert@<hostname>」を使用します）。また、`alertconfig > from` コマンドを使用して、この値を CLI で設定することもできます。
- 重複したアラートを送信するまでに待機する秒数の初期値。
- 重複したアラートを送信するまでに待機する秒数の最大値。
- AutoSupport のステータス（イネーブルまたはディセーブル）。
- Information レベルの System アラートを受信するように設定されたアラート受信者への、AutoSupport の毎週のステータス レポートの送信。

重複したアラートの送信

AsyncOS が重複したアラートを送信するまでに待機する秒数の初期値を指定できます。この値を 0 に設定した場合、重複したアラートのサマリーは送信されず、代わりにすべての重複したアラートがリアルタイムに送信されます（短時間に大量の電子メールを受信する可能性があります）。重複したアラートを送信するまでに待機する秒数は、アラートを送信するたびに増加します。この増加は、待機する秒数に、直前の間隔の 2 倍を加えたものになります。つまり、この値を 5 秒に設定すると、アラートは 5 秒後、15 秒後、35 秒後、75 秒後、155 秒後、315 秒後といった間隔で送信されます。

最終的に、送信間隔は非常に大きな秒数になります。[重複するアラート メッセージを送信する前に待機する最大の秒数（Maximum Number of Seconds to Wait Before Sending a Duplicate Alert）] フィールドを使用して、待機間隔の秒数に制限を設けることができます。たとえば、初期値を 5 秒に設定し、最大値を 60 秒に設定すると、アラートは 5 秒後、15 秒後、35 秒後、60 秒後、120 秒後といった間隔で送信されます。

Cisco IronPort AutoSupport

十分なサポートと今後のシステム変更の設計を可能にするため、システムで生成されたすべてのアラート メッセージをシスコに送信するようにアプライアンスを設定できます。この機能は AutoSupport と呼ばれ、シスコによるお客様のニーズへのプロアクティブな対応に役立ちます。また、AutoSupport はシステムの稼働時間、`status` コマンドの出力、および使用されている AsyncOS バージョンを通知するレポートを毎週送信します。

デフォルトでは、アラート タイプが System で重大度レベルが Information のアラートを受信するように設定されているアラート受信者は、シスコに送信される各メッセージのコピーを受信します。内部にアラート メッセージを毎週送信しない場合は、この設定をディセーブルにできます。この機能をイネーブルまたはディセーブルにするには、「アラート設定値の設定」（P.26-23）を参照してください。

アラート メッセージ

アラート メッセージは標準的な電子メール メッセージです。Header From: アドレスは設定できますが、メッセージのその他の部分は自動的に生成されます。

アラートの From アドレス

[設定の編集（Edit Settings）] ボタンまたは CLI を使用して、Header From: アドレスを設定できます。

アラートの件名

アラートの電子メール メッセージの件名は、次の形式に従っています。

```
Subject: [severity]-[hostname]: ([class]) short message
```

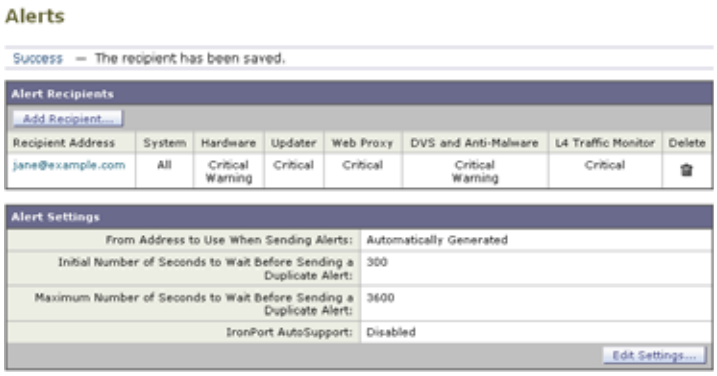
アラート メッセージの例

```
Date: 23 May 2007 21:10:19 +0000

To: joe@example.com

From: IronPort S650 Alert [alert@example.com]

Subject: Critical <System> example.com: Internal SMTP giving up on message to
jane@company.com with...



The Critical message is:



Internal SMTP giving up on message to jane@company.com with subject 'IronPort Report:
Client Web Activity (example.com)': Unrecoverable error.



Product: IronPort S650 Web Security Appliance

Model: S650

Version: 5.1.0-225

Serial Number: XXXXXXXXXXXX-XXXXXXX

Timestamp: Tue May 10 09:39:24 2007



For more information about this error, please see

    http://support.ironport.com

If you desire further information, please contact your support provider.
```

アラート受信者の管理

S シリーズ アプライアンス Web インターフェイス（GUI）にログインして、[システム管理（System Administration）] タブをクリックします。左側のメニューで [アラート（Alerts）] リンクをクリックします。S シリーズ アプライアンスの Web インターフェイスのアクセス方法の詳細については、「Web セキュリティ アプライアンスへのアクセス」（P.2-2）を参照してください。

図 26-9　[アラート（Alerts）] ページ



（注）　システムのセットアップ時に AutoSupport をイネーブルにした場合、指定した電子メール アドレスにすべての重大度およびクラスのアラートを受信します（デフォルト）。この設定はいつでも変更できます。

[アラート（Alerts）] ページは、既存のアラート受信者およびアラート設定のリストを表示します。

[アラート（Alerts）] ページからは、次の操作ができます。

- アラート受信者の追加、設定、または削除
- アラート設定値の変更

新規アラート受信者の追加

ステップ 1　[アラート（Alerts）] ページで [受信者を追加...（Add Recipient...）] をクリックします。

ステップ 2　受信者の電子メール アドレスを入力します。複数のアドレスをカンマで区切って入力することもできます。

ステップ 3　受信するアラートの重大度を選択します。

ステップ 4　変更を送信し、保存します。

既存のアラート受信者の設定

ステップ 1　[アラート受信者（Alert Recipients）] のリストからアラート受信者をクリックします。

ステップ 2　アラート受信者の設定を変更します。

ステップ 3　変更を送信し、保存します。

アラート受信者の削除

ステップ 1　[アラート受信者（Alert Recipient）] のリストから、アラート受信者に対応するゴミ箱アイコンをクリックします。

ステップ 2　表示される警告ダイアログで [削除（Delete）] をクリックして削除を確認します。

ステップ 3　変更を保存します。

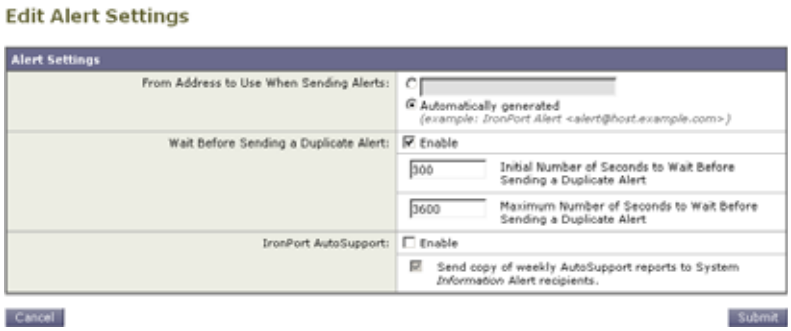
アラート設定値の設定

アラート設定はグローバルな設定であるため、すべてのアラートの動作に影響します。

アラート設定値の編集

ステップ 1　[アラート（Alerts）] ページで [設定を編集 ...（Edit Settings...）] をクリックします。

図 26-10　　アラート設定値の編集



ステップ 2　アラートの送信に使用する Header From: アドレスを入力するか、[自動生成（Automatically Generated）]（「alert@<hostname>」を自動生成）を選択します。

ステップ 3　重複したアラートを送信するまでに待機する秒数を指定する場合は、チェックボックスをオンにします。詳細については、「重複したアラートの送信」（P.26-20）を参照してください。

- 重複したアラートを送信するまでに待機する秒数の初期値を指定します。
- 重複したアラートを送信するまでに待機する秒数の最大値を指定します。

ステップ 4　[Cisco IronPort AutoSupport] オプションをオンにすることで、AutoSupport をイネーブルにできます。AutoSupport の詳細については、「Cisco IronPort AutoSupport」（P.26-20）を参照してください。

- AutoSupport がイネーブルの場合、Information レベルの System アラートを受信するように設定されたアラート受信者に、毎週 AutoSupport レポートが送信されます。チェックボックスを外すことでディセーブルにできます。

ステップ 5　変更を送信し、保存します。

アラート リスト

次の項では、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。アラートの実際

のテキストでは、パラメータ値は置き換えられます。たとえば、次のアラート メッセージではメッセージのテキストに「$ip」が記述されています。アラート生成時に「$ip」は実際の IP アドレスに置き換えられます。

Feature Key Alerts

表 26-5 に、AsyncOS で生成される可能性があるさまざまな機能キー アラートのリストを示します。この表には、アラートの説明とアラートの重大度が記載されています。

表 26-5　発生する可能性がある機能キー アラートのリスト

メッセージ	アラートの重大度	パラメータ
A “$feature” key was downloaded from the IronPort key server and placed into the pending area.EULA acceptance required.	Information	**$feature**：機能の名前。
Your “$feature” evaluation key has expired.Please contact your authorized IronPort sales representative.	Warning	**$feature**：機能の名前。
Your “$feature” evaluation key will expire in under $days day(s).Please contact your authorized IronPort sales representative.	Warning	**$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

表 26-6 に、AsyncOS で生成される可能性があるさまざまなハードウェア アラートのリストを示します。この表には、アラートの説明とアラートの重大度が含まれています。

表 26-6　発生する可能性があるハードウェア アラートのリスト

メッセージ	アラートの重大度	パラメータ
A RAID-event has occurred: $error	Warning	**$error**：RAID エラーのテキスト。

ロギング アラート

表 26-7 に、AsyncOS で生成される可能性があるさまざまなロギング アラートのリストを示します。この表には、アラートの説明とアラートの重大度が含まれています。

表 26-7　発生する可能性があるロギング アラートのリスト

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。

表 26-7　発生する可能性があるロギング アラートのリスト （続き）

メッセージ	アラートの重大度	パラメータ
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。
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

表 26-8 に、AsyncOS で生成される可能性があるさまざまなレポート アラートのリストを示します。この表には、アラートの説明とアラートの重大度が含まれています。

表 26-8　発生する可能性があるレポート リスト

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	なし。
The reporting system is now able to handle new data.	Information	なし。

表 26-8　発生する可能性があるレポート リスト （続き）

メッセージ	アラートの重大度	パラメータ
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。
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。

表 26-8　発生する可能性があるレポート リスト （続き）

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。
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

表 26-9 に、AsyncOS で生成される可能性があるさまざまなシステム アラートのリストを示します。この表には、アラートの説明とアラートの重大度が含まれています。

表 26-9　発生する可能性があるシステム アラートのリスト

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。

表 26-9　発生する可能性があるシステム アラートのリスト （続き）

メッセージ	アラートの重大度	パラメータ
An error occurred while attempting to share statistical data through the Network Participation feature.Please forward this tracking information to your IronPort 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。
Tech support: Service tunnel has been disabled.	Information	なし。

アップデータ アラート

表 26-10 に、AsyncOS で生成される可能性があるさまざまなアップデータ アラートのリストを示します。この表には、アラートの説明とアラートの重大度が含まれています。

表 26-10　発生する可能性があるアップデータ アラートのリスト

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。

FIPS 準拠

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、これらの要件を満たす証明書が必要です。

証明書	アルゴリズム	ビット キー サイズ	Signature Algorithm	コメント
X509	RSA	1024	sha1WithRSAEncryption	最良の復号化パフォーマンスと適切なセキュリティに対して、1024 のビット キー サイズが推奨されます。
	RSA	2048、3072、または 4096	sha1WithRSAEncryption	1024 を超えるビット サイズはセキュリティを強化しますが、復号化のパフォーマンスに影響します。
	DSA	1024	dsaWithSHA1	最良の復号化パフォーマンスと適切なセキュリティに対して、1024 のビット キー サイズが推奨されます。

FIPS モードの開始と終了

はじめる前に

- FIPS モードの開始と終了はどちらも、アプライアンスのリブートを開始することに注意してください。
- FIPS モードで使用される証明書が FIPS 140-2 認定公開キー アルゴリズムで使用することを確認します。
- 管理者アカウントにログインします。

Web インターフェイス

ステップ 1　[システム管理（System Administration）] > [FIPS モード（FIPS Mode）] ページで、[設定を編集（Edit Settings）] をクリックします。

ステップ 2　[Select | Deselect] FIPS レベル 1 準拠をイネーブルにします。

ステップ 3　[実行（Submit）] をクリックします。

ステップ 4　[継続（Continue）] をクリックして、アプライアンスのリブートを許可します。

コマンドライン インターフェイス

コマンド	サブコマンド	説明
`fipsconfig`	セットアップ	FIPS モードを開始および終了します。

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。

GUI および CLI の両方では、タイム ゾーンを調整して、システムの日付/時刻を手動で調整したり、照会する NTP サーバを指定することができます。

CLI を使用したシステムの日時の管理

コマンド	サブコマンド	説明
`ntpconfig`		NTP サーバを使用してシステムの日時を同期します。サブコマンドなしで、現在設定されている NTP サーバを一覧表示します。
	new	設定に新しい NTP サーバを追加します。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。
	delete	設定から NTP サーバを削除します。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。
`settime`		手動でシステムの日時を設定します。時刻を MM/DD/YYYY HH:MM:SS 形式で入力します。
`settz`	**setup**	地域、国、および各国ごとのタイム ゾーンを指定するタイム ゾーンを設定します。

GUI を使用したシステムの日時の管理

GMT オフセット

GUI では、選択する場合に GMT オフセットを使用してタイム ゾーンを指定できます。GMT オフセットは、ローカル時間と Greenwich Mean Time (GMT) の間の時差を時間単位で表示します。GMT は本初子午線にある英国のグリニッジの現在のローカル時刻です。時間の前にマイナス記号（「-」）が付いている場合、グリニッジ子午線の*東側*にあたります。プラス記号（「+」）の場合、グリニッジ子午線の*西側*にあたります。

たとえば、ニュー ヨーク市の GMT オフセットは +5 です。ニュー ヨーク市のローカル時刻と GMT には 5 時間の違いがあります。ニュー ヨーク市は、本初子午線の*西側*にあります。ニュー ヨーク市のローカル時刻に 5 時間を追加すると GMT になります。

タイム ゾーンの設定

ステップ 1　[システム管理（System Administration）] > [タイム ゾーン（Time Zone）] の順に移動します。

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　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。（「CLI を使用したシステムの日時の管理」（P.26-30）を参照してください）。

ステップ 4　変更を送信し、保存します。

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）] > [時刻設定（Time Settings）] の順に移動します。

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　[時刻の設定方法（Time Keeping Method）] として [ネットワーク タイム プロトコルを使用（Use Network Time Protocol）] を選択します。

ステップ 4　サーバの追加に必要な [行を追加（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　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）] > [時刻設定（Time Settings）] の順に移動します。

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　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）] > [時刻設定（Time Settings）] の順に移動します。

ステップ 2　[時刻を手動で設定（Set Time Manually）] を選択します。

ステップ 3　日時を設定します。

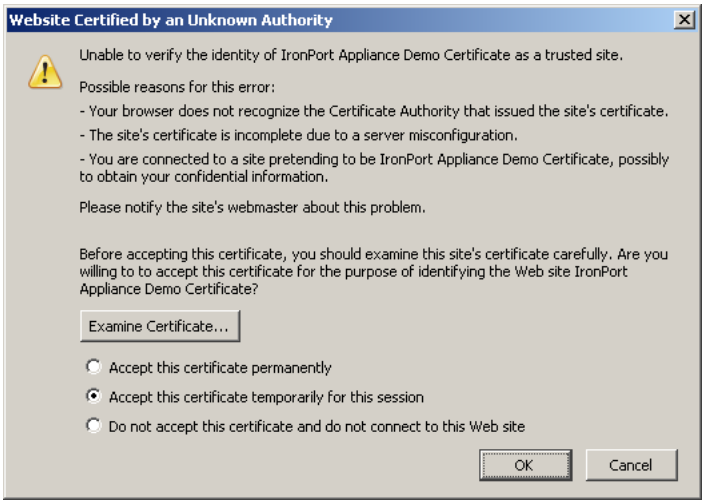
ステップ 4　[実行（Submit）] をクリックします。

サーバのデジタル証明書のインストール

管理者が HTTPS を使用して Web セキュリティ アプライアンスにログインすると、アプライアンスはデジタル証明書を使用して、クライアント アプリケーションとの接続を安全に確立します。Web セキュリティ アプライアンスは、デフォルトで事前インストールされている「Cisco IronPort Web Security Appliance Demo Certificate」を使用します。ただし、クライアント アプリケーションは、この証明書を認識するようにはプログラミングされていないため、アプリケーションが自動的に認識するデジタル証明書をアプライアンスにアップロードできます。

図 26-11 は、Cisco IronPort Web Security Appliance Demo Certificate を使用して Web セキュリティ アプライアンスにアクセスする場合、Firefox で表示される警告メッセージを示します。

図 26-11　不明な認証局としての Cisco IronPort Web Security Appliance Demo Certificate



異なるデジタル サーバ証明書を使用するように Web セキュリティ アプライアンスを設定するには、次の手順に従います。

ステップ 1　アップロードする証明書と秘密キー ペアを取得します。詳細については、「証明書の取得」（P.26-32）を参照してください。

ステップ 2　アプライアンスに証明書と秘密キー ペアをアップロードします。詳細については、「Web セキュリティ アプライアンスへの証明書のアップロード」（P.26-33）を参照してください。

証明書の取得

ステップ 1　秘密 / 公開キー ペアを生成します。

ステップ 2　証明書署名要求（CSR）を生成します。

ステップ 3　証明書に署名する認証局（CA）にお問い合わせください。

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。

- 秘密キーが暗号化されていないこと。

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。

最初に証明書を取得する場合、インターネットで「certificate authority services SSL server certificates（SSL サーバ証明書を提供している認証局）」を検索して、お客様の環境のニーズに最適なサービスを選択してください。サービスの手順に従って、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では、信頼できるルート認証局の秘密キーと同様に example.com の秘密キーが検証される必要があります。

Web セキュリティ アプライアンスへの証明書のアップロード

デジタル証明書を Web セキュリティ アプライアンスにアップロードするには、`certconfig` コマンドを使用します。

次に、アップロードされている証明書の例を示します。このコマンドから中間証明書を追加することもできます。

```
example.com> certconfig


Currently using the demo certificate/key for HTTPS management access.


Choose the operation you want to perform:

- SETUP - Configure security certificate and key.

[]> setup
```

```
Management (HTTPS):
paste cert in PEM format (end with '.'):
-----BEGIN CERTIFICATE-----
MIICLDCCAdYCAQAwDQYJKoZIhvcNAQEEBQAwgaAxCzAJBgNVBAYTAlBUMRMwEQYD
VQQIEwpRdWVlbnNsYW5kMQ8wDQYDVQQHEwZMaXNib2ExFzAVBgNVBAoTDk5ldXJv
bmlvLCBMZGEuMRgwFgYDVQQLEw9EZXNlbnZvbHZpbWVudG8xGzAZBgNVBAMTEmJy
dXR1cy5uZXVyb25pby5wdDEbMBkGCSqGSIb3DQEJARYMc2FtcG9AaWtpLmZpMB4X
DTk2MDkwNTAzNDI0M1oXDTk2MTAwNTAzNDI0M1owgaAxCzAJBgNVBAYTAlBUMRMw
EQYDVQQIEwpRdWVlbnNsYW5kMQ8wDQYDVQQHEwZMaXNib2ExFzAVBgNVBAoTDk51
dXJvbmlvLCBMZGEuMRgwFgYDVQQLEw9EZXNlbnZvbHZpbWVudG8xGzAZBgNVBAMT
EmJydXR1cy5uZXVyb25pby5wdDEbMBkGCSqGSIb3DQEJARYMc2FtcG9AaWtpLmZp
MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAL7+aty3S1iBA/+yxjxv4q1MUTd1kjNw
L4lYKbpzzlmC5beaQXeQ2RmGMTXU+mDvuqItjVHOK3DvPK7lTcSGftUCAwEAATAN
BgkqhkiG9w0BAQQFAANBAFqPEKFjk6T6CKTHvaQeEAsX0/8YHPHqH/9AnhSjrwuX
9EBc0n6bVGhN7XaXd6sJ7dym9sbsWxb+pJdurnkxjx4=
-----END CERTIFICATE-----
.

paste key in PEM format (end with '.'):
-----BEGIN RSA PRIVATE KEY-----
MIIBPAIBAAJBAL7+aty3S1iBA/+yxjxv4q1MUTd1kjNwL4lYKbpzzlmC5beaQXeQ
2RmGMTXU+mDvuqItjVHOK3DvPK7lTcSGftUCAwEAAQJBALjkK+jc2+iihI98riEF
oudmkNziSRTYjnwjx8mCoAjPWviB3c742eO3FG4/soi1jD9A5alihEOXfUzloenr
8IECIQD3B5+0l+68BA/6d76iUNqAAV8djGTzvxnCxycnxPQydQIhAMXt4trUI3nc
a+U8YL2HPFA3gmhBsSICbq2OptOCnM7hAiEA6Xi3JIQECob8YwkRj29DU3/4WYD7
WLPgsQpwo1GuSpECICGsnWH5oaeD9t9jbFoSfhJvv0IZmxdcLpRcpslpeWBBAiEA
6/5B8J0GHdJq89FHwEG/H2eVVUYu5y/aD6sgcm+0Avg=
-----END RSA PRIVATE KEY-----
.
```

```
Do you want add an intermediate certificate? [N]> N


Currently using custom certificate/key for HTTPS management access.


Choose the operation you want to perform:

- SETUP - Configure security certificate and key.

[]>


example.com> commit


Please enter some comments describing your changes:

[]> Installed certificate and key for HTTPS management.


Changes committed: Fri Sep 26 17:59:53 2008 GMT
```

Web 用 AsyncOS のアップロード

ステップ 1　**アップデートおよびアップグレード設定を設定します。**Web セキュリティ アプライアンスのアップグレード情報のダウンロード方法に影響する設定を設定できます。たとえば、アップグレード イメージなどをダウンロードする場所を選択できます。詳細については、「アップグレードおよびサービス アップデートの設定」（P.26-37）を参照してください。

ステップ 2　**システム ソフトウェアをアップグレードします。**アップデートおよびアップグレード設定を設定したら、アプライアンスのソフトウェアをアップグレードします。アプライアンスで [アップグレードの通知（Upgrade Notifications）] がオンの場合、Web インターフェイスの上部に、入手可能なアップグレードを通知するメッセージが管理者に対して表示されます。詳細については、「Web インターフェイスからの Web 用 AsyncOS のアップグレード」（P.26-37）および「CLI からの Web 用 AsyncOS のアップグレード」（P.26-37）を参照してください。

Web 用 AsyncOS のアップグレード時には、次のガイドラインを考慮してください。

- 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。詳細については、「アプライアンスの設定の保存とロード」（P.26-1）を参照してください。

- 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。
- PAC ファイルまたはカスタマイズされたエンド ユーザ通知ページなど、アプライアンスに保存されている他のファイルを保存することを考慮してください。
- 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することを考慮してください。

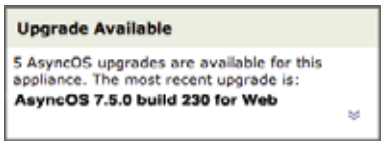
入手使可能なアップグレードの通知

Web セキュリティ アプライアンスを設定して、AsyncOS へのアップグレードがアプライアンスで入手可能であることを通知するメッセージが Web インターフェイスの上部に表示できます。AsyncOS は、アプライアンスにログインした管理者にこの通知を表示します。

図 26-12　入手可能なアップグレードの通知

マウス カーソルを通知に合わせて、アプライアンスで入手可能なアップグレード数および入手可能な最新のアップグレードのバージョンとビルド番号を表示します。

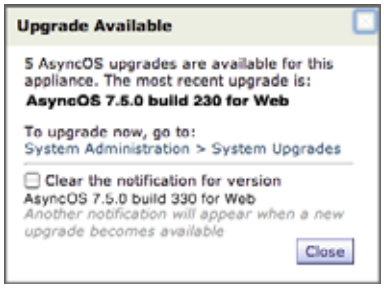
図 26-13　AsyncOS アップグレードのビルド情報



右下隅にある下矢印をクリックして、通知ウィンドウを展開します。ウィンドウは、アップグレードを開始するための [システム管理（System Administration）] > [システム アップグレード（System Upgrade）] ページへのリンクを表示します。

メッセージを消去するには、[通知をクリア（Clear the notification）] チェックボックスをオンにし、[閉じる（Close）] をクリックします。新しいアップグレードが入手可能になるまで、アプライアンスは別の通知を表示しません。

図 26-14　展開された [アップグレードを使用可能（Upgrade Available）] ウィンドウ



[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）] ページを使用して、アプライアンスでこれらの通知をイネーブルにできます。詳細については、「アップグレードおよびサービス アップデートの設定」（P.26-37）を参照してください。

Web インターフェイスからの Web 用 AsyncOS のアップグレード

ステップ 1　[システム管理（System Administration）] > [設定ファイル（Configuration File）] ページで、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。

ステップ 2　[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。

CLI からの Web 用 AsyncOS のアップグレード

CLI から `upgrade` コマンドを発行して、入手可能なアップグレードのリストを表示します。リストから目的のアップグレードを選択して、インストールします。メッセージを確認するか、ライセンス契約等を読んで、同意するように求められる場合があります。

従来のアップグレード方式との違い

従来の方式と比較して、AsyncOS をローカル サーバからアップグレードする場合には、次の違いがあることに注意してください。

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

Web Reputation Filters や Web アップグレード用の AsyncOS など、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、ファイルのダウンロード時に使用するネットワーク インターフェイスを選択し、アップデート間隔を設定できます。または、自動アップデートをディセーブルにできます。

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、「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」（P.26-43）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 IronPort アップデート サーバ。**詳細については、「Cisco IronPort アップデート サーバからのアップデートおよびアップグレード」（P.26-39）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」（P.26-39）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」として知られています。
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。

デフォルトでは、AsyncOS はアップデート イメージ、アップグレード イメージおよびマニフェスト XML ファイルに対して Cisco IronPort アップデート サーバに問い合わせます。ただし、アップグレード イメージ、アップデート イメージおよびマニフェスト ファイルをダウンロードする場所を選択できます。次の理由からイメージまたはマニフェスト ファイルのローカルのアップデート サーバを指定する必要がある場合があります。

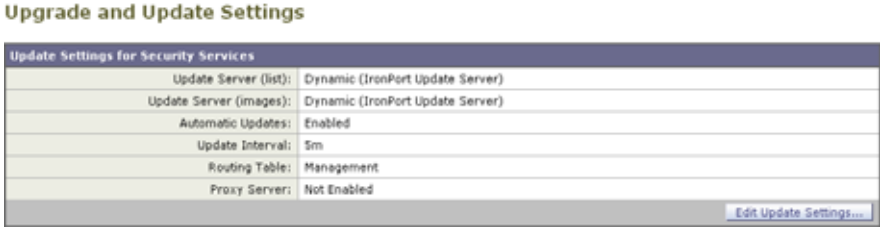
- **同時にアップグレードするアプライアンスが複数あります。**組織にアップグレードが必要な複数の Web セキュリティ アプライアンスがある場合は、ネットワーク内の Web サーバにアップグレード イメージをダウンロードし、ネットワーク内のすべてのアプライアンスに使用できます。
- **ご使用のファイアウォールの設定には、Cisco IronPort アップデート サーバ**のスタティック IP アドレスが必要です。Cisco IronPort アップデート サーバは、ダイナミック IP アドレスを使用します。ファイアウォール ポリシーを厳しく設定している場合、アップデートおよび AsyncOS 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 IronPort アップデート サーバへのスタティック アドレスの設定」（P.26-39）を参照してください。

（注）　ローカル アップデート サーバはアップグレード イメージ専用に使用し、セキュリティ アップデート イメージには使用しないでください。ローカル アップデート サーバを指定した場合、ローカル サーバはシスコからアップデートされたセキュリティ サービス アップデートを自動的には受信しないため、ネットワーク上のアプライアンスはいずれ古くなります。AsyncOS のアップグレード用にローカル アップデート サーバを使用して、アップデートおよびアップグレード用の設定値を再び Cisco IronPort アップデート サーバを使用するように変更してください。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。

Web インターフェイスまたは CLI でアップグレードおよびアップデートの設定値を設定できます。詳細については、「Web インターフェイスからのアップデートおよびアップグレード設定値の設定」（P.26-41）および「CLI からのアップデートおよびアップグレード設定値の設定」（P.26-42）を参照してください。

図 26-15 は、Web インターフェイスでアップグレードおよびアップデートの設定値を設定できます。

図 26-15　[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



Cisco IronPort アップデート サーバからのアップデートおよびアップグレード

Web セキュリティ アプライアンスは、Cisco IronPort アップデート サーバに直接接続し、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。

シスコでは分散アップデート サーバ アーキテクチャを使用して、顧客がどこからでもアップデートおよび AsyncOS アップグレードをすばやくダウンロードできます。この分散サーバ アーキテクチャのため、Cisco IronPort アップデート サーバではダイナミック IP アドレスが使用されます。ファイアウォール ポリシーを厳しく設定している場合、AsyncOS アップグレードに対して静的な参照先を設定する必要がある場合があります。詳細については、「Cisco IronPort アップデート サーバへのスタティック アドレスの設定」（P.26-39）を参照してください。

Cisco IronPort アップデート サーバへのスタティック アドレスの設定

Cisco IronPort アップデート サーバは、ダイナミック IP アドレスを使用します。ファイアウォール ポリシーを厳しく設定している場合、アップデートおよび AsyncOS アップグレードに対して静的な参照先を設定する必要がある場合があります。

ステップ 1　Cisco IronPort カスタマー サポートに問い合わせて、スタティック URL アドレスを取得します。

ステップ 2　[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　[更新設定を編集（Edit Update Settings）] ページの [更新サーバ（イメージ）（Update Servers (images)）] セクションで、[ローカル更新サーバ（Local Update Servers）] を選択し、ステップ 1 で受け取ったスタティック URL アドレスを入力します。

ステップ 4　Cisco IronPort アップデート サーバが [更新サーバ（リスト）（Update Servers (list)）] セクションで選択されていることを確認します。

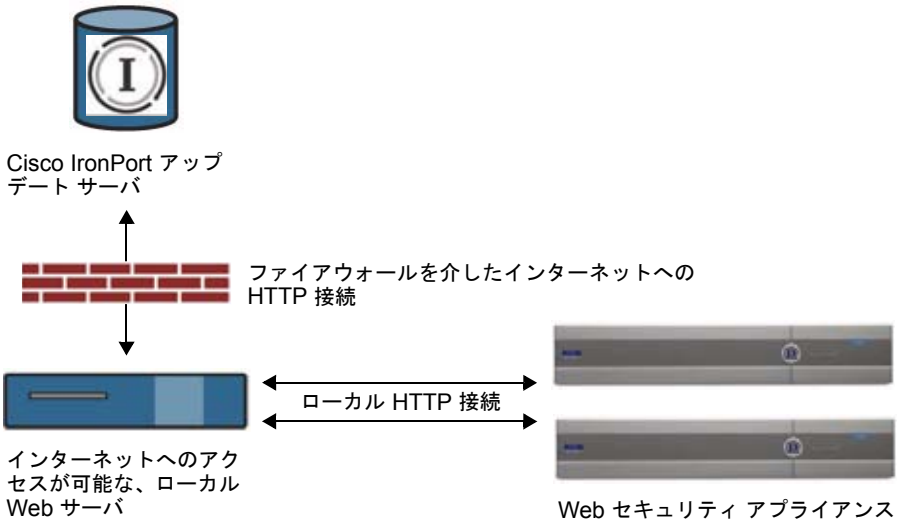
ステップ 5　変更を送信し、保存します。

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 IronPort 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場合は、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、ネットワーク内のすべての Web セキュリティ アプライアンスに使用することができます。

図 26-16 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 26-16　ローカル サーバからのアップグレード



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 コンポーネントが自動的に更新されるように、シスコではアップデートとアップグレードの設定を変更して、Cisco IronPort 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 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 ファイルの*ダウンロード*では、Web ブラウザ（「ブラウザ要件」（P.2-6）を参照）を備えた内部ネットワークにシステムを構築する必要があり、Cisco IronPort アップデート サーバへのインターネット アクセスが必要になります。

（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

Web インターフェイスからのアップデートおよびアップグレード設定値の設定

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）] 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 2　表 26-11 の情報を参照して、設定値を設定します。

表 26-11　設定値のアップデートおよびアップグレード

設定	説明
自動更新（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。
アップグレードの通知（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、「入手使可能なアップグレードの通知」（P.26-36）を参照してください。
アップデートサーバ（リスト）（Update Servers (list)）	利用可能なアップグレードおよびアップデートのリスト（マニフェスト XML ファイル）を、Cisco IronPort アップデート サーバまたはローカル Web サーバのどちらからダウンロードするかを選択します。 デフォルトは、Cisco IronPort アップデート サーバです。一時的に、ローカル Web サーバに保存されたアップグレード イメージをダウンロードする場合は、ローカル Web サーバを選択します。イメージをダウンロードした後、この設定を変えて Cisco IronPort アップデート サーバに戻し、セキュリティ コンポーネントが自動的にアップデートされるようにすることを推奨します。 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。 詳細については、「ローカル サーバからのアップグレード」（P.26-39）を参照してください。

表 26-11　設定値のアップデートおよびアップグレード （続き）

設定	説明
アップデートサーバ（イメージ）（Update Servers (images)）	Cisco IronPort アップデート サーバまたはローカル Web サーバからアップグレードおよびアップデート イメージをダウンロードするかどうかを選択します。デフォルトは、Cisco IronPort アップデート サーバです。次の条件のいずれかが該当する場合は、ローカル Web サーバを選択します。 • シスコからアップグレードおよびアップデート イメージをダウンロードできますが、Cisco IronPort カスタマー サポートから提供されたスタティック アドレスを入力する必要があります。 • 一時的に、ローカル Web サーバに保存されたアップグレード イメージをダウンロードする場合。イメージをダウンロードした後、この設定を変えて Cisco IronPort アップデート サーバ（または使用している場合にはスタティック アドレス）に戻し、セキュリティ コンポーネントが自動的にアップデートされるようにすることを推奨します。 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。 詳細については、「Cisco IronPort アップデート サーバからのアップデートおよびアップグレード」（P.26-39）および「ローカル サーバからのアップグレード」（P.26-39）を参照してください。
ルーティング テーブル（Routing Table）	アップデート サーバに問い合わせるときに、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。利用可能なプロキシ データ インターフェイスが表示されます。デフォルトは Management です。
プロキシサーバ（オプション）（Proxy Server (optional)）	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 3　変更を送信し、保存します。

CLI からのアップデートおよびアップグレード設定値の設定

`updateconfig` コマンドは、アプライアンスがサービス アップデートと AsyncOS アップグレードを検索するアップデートおよびアップグレードの設定に使用されます。`updateconfig` コマンドを使用して設定する設定値は、Web インターフェイスで定義できるものと同じです。これらの設定の詳細については、表 26-11（P.26-41）を参照してください。

（注）　`ping` コマンドを使用して、アプライアンスがローカル サーバに接続できることを確認できます。また、`telnet` CLI コマンドを使用してローカル サーバのポート 80 に Telnet 接続することで、ローカル サーバが該当のポートをリッスンしていることが確認できます。

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 IronPort アップデート サーバからデータベース テーブルで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。

通常、データベース テーブルに手動で更新する必要はありません。手動アップデートが必要なイベントでは、デフォルト設定を変更し、[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）] ページのオプションを使用してアップデートを設定できます。

（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。たとえば、手動で URL カテゴリのセットだけを更新するには、「URL カテゴリ セットの手動の更新」（P.17-9）を参照してください。

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）] ページの順に進みます。

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。

以前のバージョンの Web 用 AsyncOS 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。

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、シスコでは手動でローカル マシンにコンフィギュレーション ファイルをバックアップとして

保存することを推奨します)。これにより以前のバージョンに戻した後で、Web 用 AsyncOS は以前のリリースに関連付けられた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。

AsyncOS を復元する場合、現在実行されているビルドに復元することができます。これにより、アプライアンス上のすべてのデータをクリアし、新しいクリーンな設定から開始することができます。

（注）　URL カテゴリのセットへのアップデートが入手可能な場合、AsyncOS の復帰後に適用されます。

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。
- 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おり、1 つのバージョンの Web 用 AsyncOS を以前のバージョンに戻す場合（たとえば、バージョン 7.6 をバージョン 7.5）、Web セキュリティ アプライアンスを適切な Configuration Master に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。

利用可能なバージョン

アップグレードによって主要なサブシステムの一方向の変換が行われるため、復元プロセスは複雑であり、Cisco 品質保証チームの認定が必要です。以前のすべてのバージョンの Web 用 AsyncOS オペレーティング システムが復元に利用できるわけではありません。最初にこの機能がサポートされた AsyncOS バージョンは AsyncOS 7.5.0 です。これより以前のバージョンの Web 用 AsyncOS はサポートされていません。

復元の影響に関する重要な注意事項

Web セキュリティ アプライアンスにおけるオペレーティング システムの復元は、非常に破壊的な操作になります。この操作はすべての設定ログおよびデータベースを破壊します。さらに、復元はアプライアンスが再設定されるまで Web トラフィック処理を中断します。

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。

Web 用 AsyncOS に復元する前に、次の情報を Web セキュリティ アプライアンスから別のマシンにバック 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。
- 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。

以前のバージョンへの Web 用の AsyncOS の復元

ステップ 1　アプライアンスの現在の設定のバックアップ コピーを、（パスワードをマスクしない状態で）別のマシンに保存します。

（注）　このコピーは、バージョンを戻した後にロードするコンフィギュレーション ファイルではありません。

ステップ 2　保持する次のファイルのいずれかを別のマシンにバックアップします。

- ログ ファイル
- 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 3　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 4　CLI から `revert` コマンドを入力します。

ステップ 5　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 6　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。

27
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 のコマンドライン インターフェイス（CLI）は、Web セキュリティ アプライアンスを設定およびモニタするために設計されたインタラクティブなインターフェイスです。引数を指定しても指定しなくても、コマンド名を入力すると、コマンドが起動されます。引数を指定せずにコマンドを入力した場合は、必要な情報を要求するプロンプトが表示されます。

コマンドライン インターフェイスには、これらのサービスがイネーブルの状態で設定されている IP インターフェイスの SSH を使用して、またはシリアル ポートで端末エミュレーション ソフトウェアを使用してアクセスできます。デフォルトでは、SSH が管理ポートで設定されています。

コマンドライン インターフェイスの使用

ここでは、AsyncOS コマンドライン インターフェイスのルールおよび表記法について説明します。

コマンドライン インターフェイスへのアクセス

CLI へのアクセスは、アプライアンスのセットアップ時に選択した管理接続方式によって異なります。工場出荷時のデフォルト ユーザ名およびパスワードを次に示します。当初は、admin ユーザ アカウントだけが CLI にアクセスできます。admin アカウントを使用して CLI に初回アクセスしたうえで、さまざまな許可レベルの他のユーザを追加できます。システム セットアップ ウィザードによって、admin アカウントのパスワードを変更するよう要求されます。

また、管理者アカウント 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。

次の方法のいずれかを使用して接続できます。

- **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**

次に例を示します。

```
login: admin

password: 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場合は、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に大なり（>）記号が表示されます。デフォルト値がない場合は、ブラケットが空です。

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る場合に Return を入力すると、デフォルト値を受け入れたことになります。

コマンド構文

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

```
example.com> logconfig
```

選択リスト

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

次に例を示します。

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

Yes/No クエリー

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

次に例を示します。

```
Do you want to enable the proxy? [Y]> Y
```

サブコマンド

一部のコマンドでは、NEW、EDIT、DELETE などのサブコマンド命令を使用できます。EDIT および DELETE 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、すぐに最上位の 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し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↑および↓の矢印キーを使用するか、Ctrl+P キーと Ctrl+N キーを組み合わせて使用します。

コマンドのオートコンプリート

AsyncOS CLI は、コマンドの補完機能をサポートしています。あるコマンドの先頭の数文字を入力して Tab キーを入力すると、CLI によって、残りの文字列が入力されます。入力した文字がコマンドの中で一意ではない場合、CLI はそのセットを「絞り込み」ます。次に例を示します。

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

設定変更の確定

確定するまで、設定の変更は有効になりません。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は有効になりません。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、コミット、変更のクリアなど、一般的な CLI セッションで使用する可能性のある基本コマンドについて説明します。完全なコマンド リストについては、「Web セキュリティ アプライアンスの CLI コマンド」（P.27-6）を参照してください。

設定変更の確定

commit コマンドを使用すると、他の作業が通常どおりに進行する間にコンフィギュレーションの設定を変更できます。変更は、確認およびタイムスタンプを受信するまでは、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 を入力します。

設定変更のクリア

clear コマンドは、commit コマンドまたは clear コマンドが最後に発行されてから、アプライアンスの設定に対して行われた変更内容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します。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
```

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、システムのアップグレードおよび管理を実行するプロキシおよび UNIX コマンドをサポートしています。

表 27-1 は、Web セキュリティ アプライアンスのコマンドライン インターフェイス コマンドのリストです。

表 27-1　Web セキュリティ アプライアンスの管理コマンド

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。 advancedproxyconfig コマンドの詳細については、「高度なプロキシ設定」（P.5-21）を参照してください。
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。 adminaccessconfig コマンドの詳細については、「管理者の設定」（P.26-16）を参照してください。
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、認証キャッシュに現在含まれているすべてのユーザのリストを表示できます。 ユーザ セッション制限の値がタイム アウトする前にユーザが別のマシンから再度ログインできるように、認証キャッシュからユーザをクリアすることができます。
bwcontrol	デフォルトのプロキシ ログ ファイルの帯域幅管理デバッグ 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、保留中の設定変更をクリアします。
commit	保留中のシステム設定への変更を確定します。
createcomputerobject	指定した場所にコンピュータ オブジェクトを作成します。
datasecurityconfig	最小要求本文サイズを定義します。これより本文サイズが小さい場合は、アップロード要求が Cisco IronPort データ セキュリティ フィルタでスキャンされません。 詳細については、「「最小サイズ以下のアップロード要求のバイパス」（P.13-2）」を参照してください。

表 27-1　Web セキュリティ アプライアンスの管理コマンド（続き）

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 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	最小要求本文サイズを定義します。これより本文サイズが小さい場合は、アップロード要求が外部 DLP サーバでスキャンされません。 詳細については、「最小サイズ以下のアップロード要求のバイパス」（P.13-2）」を参照してください。
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。 詳細については、「[ライセンス キー（Feature Keys）] ページ」（P.26-8）」を参照してください。
featurekeyconfig	自動的に機能キーをチェックして更新します。 詳細については、「[ライセンス キーの設定（Feature Key Settings）] ページ」（P.26-8）」を参照してください。
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）により管理される時期を示す、Web インターフェイスおよび CLI のメッセージをクリアします。
ifconfig or 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、または削除する操作メニューを提供します。
last	tty およびホストを含むユーザ固有のユーザ情報を、新しい順に並べたリスト、または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 をイネーブルにし、IP アドレスによるか、または 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、リモート ユーザの識別方法を設定します。 **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。 Secure Mobility のイネーブル化および設定の詳細については、「セキュア モビリティのイネーブル化」（P.14-2）を参照してください。

表 27-1　Web セキュリティ アプライアンスの管理コマンド （続き）

musstatus	このコマンドを使用して、Web セキュリティ アプライアンスが適応型セキュリティ アプライアンスと統合されたときに、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 アプライアンスの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。Web セキュリティ アプライアンスを介してトラフィックが渡されたリモート クライアントの数として定義されます。 • 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 サーバを設定します。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信または受信されている TCP/IP などのパケットを代行受信して表示します。 詳細については、「パケット キャプチャ」（P.26-4）」を参照してください。
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	指定し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。

表 27-1　Web セキュリティ アプライアンスの管理コマンド （続き）

saveconfig	現在のコンフィギュレーション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。 設定が「domain」の場合は、アプライアンスによって Active Directory ドメインがドメイン セキュリティ信頼アカウントに結合されます。設定が「ads」の場合は、ドメインがネイティブ Active Directory メンバーとして結合されます。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 ゾーンおよびタイム ゾーンのバージョンを表示します。ローカル タイム ゾーンを設定する操作メニューを提供します。
showconfig	すべての設定値を表示します。 **注：**ユーザのパス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。SMTP リレー ホストの設定については、「SMTP リレー ホストの設定」（P.25-17）を参照してください。
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。
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、システム情報と、マスター設定のコピーが含まれます。

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	システムにアクセスするための一時的な接続を Cisco IronPort カスタマー サポートに提供し、トラブルシューティングを支援します。
telnet	Telnet プロトコルを使用して、他のホストと通信します。

表 27-1　Web セキュリティ アプライアンスの管理コマンド （続き）

testauthconfig	特定の認証レルムの認証設定を、そのレルムで定義された認証サーバに対してテストします。 `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、ここから選択できます。 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、0 レベルが使用されます。レベル 0 の場合は、コマンドが成功または失敗を返します。テスト設定が失敗すると、失敗の原因のリストが表示されます。 **（注）** シスコでは、レベル 0 の使用を推奨します。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	ゲートウェイを経由し、パスをたどって、宛先ホストまで 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。詳細については、「「アップグレードおよびサービス アップデートの設定」（P.26-37）」を参照してください。
updatenow	すべてのコンポーネントを更新します。
upgrade	AsyncOS 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するか、アプライアンスにキャッシュされないドメインおよび URL を設定します。管理者が、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 キャッシュに保存されないドメインまたは URL を指定したりできるようにします。 詳細については、「「Web プロキシ キャッシュ」（P.5-3）」を参照してください。
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。

28
一般的なタスク

業務時間内のストリーミング メディア Web サイトへのユーザ アクセスの防止

このタスクでは、業務時間内（月曜日から金曜日の午前 8 時から午後 5 時として定義）にユーザがストリーミング メディアの Web サイトにアクセスすることを防止します。ただし、正午から午後 1 時の昼休みにはアクセスできるようにします。これは、勤務時間中の帯域幅の使用量を全体的に減らして、タスクに関連する作業を完了する十分な容量を確保するために実行する必要がある場合があります。

たとえば、SalesForce.com にアクセスするときに多くの従業員がネットワークが非常に遅いという不満を漏らしています。そして、業務時間内にストリーミング ミュージックに従業員の 30% がアクセスすることを IT 管理者が指摘しています。業務時間内のストリーミング ミュージックを防止することだけで、帯域幅を拡大して、重要でない業務時間中に従業員がすべてのサイトにアクセスできるようにしながら、SalesForce.com などの作業に関連するサイトにより迅速に従業員がアクセスするようにできます。

このタスクは、ストリーミング メディアの Web サイトへのアクセスを防止するユーザに ID ポリシーをすでに定義していることを前提とします。

ステップ 1　[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 Ranges）] ページに移動します。

ステップ 2　[時間範囲の追加（Add Time Range）] をクリックします。

ステップ 3　[時間範囲名（Time Range Name）] フィールドに、[業務時間（Business Hours）] など、設定するこの時間範囲の名前を入力します。

ステップ 4　[タイム ゾーン（Time Zone）] セクションで、「Use Time Zone Setting from Appliance」を選択します。

ステップ 5　[時間値（Time Values）] 領域の [曜日（Day of Week）] セクションで、次のチェックボックスをオンにします。

[月曜日（Monday）]、[火曜日（Tuesday）]、[水曜日（Wednesday）]、[木曜日（Thursday）]、[金曜日（Friday）]

ステップ 6　[時間値（Time Values）] 領域の [時間（Time of Day）] セクションで、[開始時刻（From）] フィールドに [8:00] を入力し、[終了時刻（To）] フィールドに [12:00] を入力します。

ステップ 7　[行を追加（Add Row）] をクリックして、追加の時間値の行を作成します。

ステップ 8　新しい行の [曜日（Day of Week）] セクションで、次のチェックボックスをオンにします。

[月曜日（Monday）]、[火曜日（Tuesday）]、[水曜日（Wednesday）]、[木曜日（Thursday）]、[金曜日（Friday）]

ステップ 9　新しい行の [時間（Time of Day）] セクションで、[開始時刻（From）] フィールドに [13:00] を入力し、[終了時刻（To）] フィールドに [17:00] を入力します。

ステップ 10　[実行（Submit）] をクリックします。

ステップ 11　[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）] ページの順に進みます。

ステップ 12　[ポリシーを追加（Add Policy）] をクリックします。

ステップ 13　[ポリシー名（Policy Name）] フィールドに、[BlockStreamingMedia] など、ポリシー名を入力します。

ステップ 14　[上記ポリシーを挿入（Insert Above Policy）] フィールドで、現在最上位のポリシー グループの上にアクセス ポリシー グループを配置します。

ステップ 15　[アイデンティティとユーザ（Identities and Users）] セクションで、ドロップダウン フィールドの「Select one or More Identities」を選択します。

ステップ 16　[アイデンティティ（Identity）] フィールドで、ストリーミング メディアの Web サイトへのアクセスをブロックするユーザに相当する ID グループを選択します。

ステップ 17　識別に認証が必要な場合、すべての認証済みユーザなど、このポリシー グループで許可されているユーザを指定します。

ステップ 18　[実行（Submit）] をクリックします。

ステップ 19　アクセス ポリシーに対して作成したばかりの [URL フィルタ（URL Filtering）] カラムの下のリンクをクリックします。

ステップ 20　[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、[時間ベースのストリーミング メディア URL カテゴリ（Time-Based for the Streaming Media URL category）] をクリックします。

[時間ベースの URL カテゴリ（Time-Based for the URL category）] を選択すると、アクションを選択できるカテゴリ名の下に追加のフィールドが表示されます。

ステップ 21　[時間範囲（Time Range）] フィールドで、[業務時間（BusinessHours）] を選択します。

ステップ 22　[アクション（Action）] フィールドで、[ブロック（Block）] を選択します。

ステップ 23　[でなければ（Otherwise）] フィールドで、[モニタ（Monitor）] を選択します。

ステップ 24　変更を送信し、保存します。

ユーザが業務時間内に youtube.com などのストリーミング メディア アプリケーションを含む Web サイトにアクセスしようとすると、ブロックされ、ブロックされる理由が記載されるエンド ユーザ通知ページが表示されるようになります。

詳細情報の入手先

このタスクに含まれる手順の詳細情報については、次の項を参照してください。

- 「URL カテゴリを使用したトランザクションのフィルタリング」（P.17-10）
- 「時間ベースの URL フィルタの作成」（P.17-23）
- 「時間ベースのポリシーの使用」（P.7-9）

特定のユーザ エージェントの認証のバイパス

このタスクでは、ネットワークの特定のユーザ エージェントからの要求を Web プロキシが認証しないように確認します。これは、認証クレデンシャルにエンド ユーザを促すことができないユーザ エージェントに対して実行する必要がある場合があります。特に、このタスクは iPhone、iPad、および iPod で Web にアクセスするすべてのアプリケーションについて認証をバイパスします。

このタスクでは、1 つ以上の認証レルムが Web セキュリティ アプライアンスにすでに定義されていることを前提とします。

ステップ 1　[Web セキュリティ マネージャ（Web Security Manager）] > [アイデンティティ（Identities）] ページに移動します。

ステップ 2　[アイデンティティを追加（Add Identity）] をクリックします。

ステップ 3　[名前（Name）] フィールドに、[UserAgentsToBypass] など、このポリシーの名前を入力します。

ステップ 4　[上に挿入（Insert Above）] フィールドで、この ID が認証を必要とする他のすべての ID の上部にあることを確認します。

ステップ 5　[メンバーシップの定義（Membership Definition）] の下で、[詳細（Advanced）] をクリックして、詳細なポリシー オプションを展開します。

ステップ 6　[ユーザ エージェント（User Agents）] の横にあるリンクをクリックします。

ステップ 7　[アイデンティティ：ポリシー「UserAgentsToBypas」：ユーザエージェントによるメンバーシップ（Identities: Policy “UserAgentsToBypass”：Membership by User Agent）] ページの [共通ユーザエージェント（Common User Agents）] セクションで、[その他（Others）] をクリックして、他のユーザ エージェントを展開します。

ステップ 8　[Microsoft Windows アップデート（Microsoft Windows Update）] チェックボックスをオンにします。

ステップ 9　[カスタマ ユーザ エージェント（Customer User Agents）] フィールドに次のエントリを入力します。

- `iPhone`
- `iPad`
- `iPod`

ステップ 10　[完了（Done）] をクリックします。

ステップ 11　[実行（Submit）] をクリックします。

ステップ 12　[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）] ページの順に進みます。

ステップ 13　[ポリシーを追加（Add Policy）] をクリックします。

ステップ 14　[ポリシー名（Policy Name）] フィールドに、[APBypassAuthUserAgents] など、このポリシーの名前を入力します。

ステップ 15　[アイデンティティとユーザ（Identities and Users）] フィールドで、「Select One or More Identities」を選択します。

ステップ 16　[アイデンティティ（Identity）] フィールドで、ステップ 3 で作成した ID を選択します。

ステップ 17　変更を送信し、保存します。

iPhone、iPad、または iPod 上のアプリケーションが Web にアクセスしようとすると、正常に行われ、ユーザにユーザ名とパスワードの入力を求めません。

（注）　アクセス ログに %u カスタム フィールドを追加して、Web にアクセスしようとしているユーザ エージェントを確認できます。

詳細情報の入手先

このタスクに含まれる手順の詳細情報については、次の項を参照してください。

- 「ユーザ エージェント ベースのポリシーの使用」（P.7-11）
- 「ID の作成」（P.8-18）

特定の Web サイトの認証のバイパス

このタスクでは、特定の Web サイトにアクセスしようとしているユーザからの要求を Web プロキシが認証しないように確認します。これは、ユーザを認証するプロキシ サーバに正常に作用しないのに、Web レピュテーション フィルタリングおよびアンチマルウェア スキャンなどの Web サイトに Web プロキシがセキュリティ サービスを適用するようにするときに必要となる場合があります。また、複数のユーザ エージェントがアクセスする必要があり、ユーザ エージェントがユーザに Microsoft Windows アップデータのユーザ エージェントなどの認証クレデンシャルを入力するように促すことができないときに必要となる場合があります。

たとえば、ユーザはパートナー Web サイトでホストされて作業する必要があるファイルにアクセスできないという不満を漏らしています。ローカル ネットワークに接続されていない場合にパートナーの Web サイトのファイルにアクセスできますが、ローカル ネットワークに接続されている場合はパートナーの Web サイトにアクセスできません。IT は、Web セキュリティ アプライアンスのアクセス ログを読み取り、パートナーの Web サーバが HTTP による RFC に完全に準拠しておらず、エンド ユーザを認証するときに Web プロキシと正常に通信できないことを学習しました。パートナーの Web サイトにアクセスするユーザを認証しないことで、サーバからダウンロードしたコンテンツをスキャンしてユーザを保護しながらアクセスを許可することができます。

さらに、Windows マシンでは、Microsoft Windows のアップデータはエンド ユーザへのエラー メッセージの停止または表示で失敗します。

このタスクでは、1 つ以上の認証レルムが Web セキュリティ アプライアンスにすでに定義されていることを前提とします。

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）] ページに移動します。

ステップ 2　[カスタム URL カテゴリ（Custom URL Categories）] ページで、[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　[カテゴリ名（Category Name）] フィールドに、[BypassAuth] など、このカテゴリの名前を入力します。

ステップ 4　[サイト（Sites）] フィールドに、認証をバイパスする Web サイトのアドレスを入力します。このタスクでは、次のアドレスを入力してください。

- mypartnersite.com
- .mypartnersite.com
- download.windowsupdate.com
- .windowsupdate.microsoft.com
- .update.microsoft.com
- .download.windowsupdate.com
- update.microsoft.com
- .windowsupdate.com
- download.microsoft.com
- windowsupdate.microsoft.com
- ntservicepack.microsoft.com
- wustat.windows.com
- c.microsoft.com

ステップ 5　[実行（Submit）] をクリックします。

ステップ 6　[Web セキュリティ マネージャ（Web Security Manager）] > [アイデンティティ（Identities）] ページに移動します。

ステップ 7　[アイデンティティを追加（Add Identity）] をクリックします。

ステップ 8　[名前（Name）] フィールドに、[WebsitesToBypassAuth] など、このポリシーの名前を入力します。

ステップ 9　[上に挿入（Insert Above）] フィールドで、この ID が認証を必要とする他のすべての ID の上部にあり、認証を必要としないすべての ID の下部にあることを確認します。

ステップ 10　[メンバーシップの定義（Membership Definition）] の下で、[詳細（Advanced）] をクリックして、詳細なポリシー オプションを展開します。

ステップ 11　[URL カテゴリ（URL Categories）] の横にあるリンクをクリックします。

ステップ 12　[アイデンティティ：ポリシー「WebsitesToBypassAuth」: URL カテゴリによるメンバーシップ（Identities: Policy “UserAgentsToBypass”: Membership by URL Categories）] ページの [カスタム URL カテゴリ（Custom URL Categories）] セクションで、ステップ 3 で作成したカスタム URL カテゴリの [追加（Add）] カラムをクリックします。

ステップ 13　[完了（Done）] をクリックします。

ステップ 14　[実行（Submit）] をクリックします。

ステップ 15　[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）] ページの順に進みます。

ステップ 16　[ポリシーを追加（Add Policy）] をクリックします。

ステップ 17　[ポリシー名（Policy Name）] フィールドに、[APBypassAuthWebsites] など、このポリシーの名前を入力します。

ステップ 18　[アイデンティティとユーザ（Identities and Users）] フィールドで、「Select One or More Identities」を選択します。

ステップ 19　[アイデンティティ（Identity）] フィールドで、ステップ 8 で作成した ID を選択します。

ステップ 20　変更を送信し、保存します。

各クライアント マシンで実行される Microsoft Windows のアップデータは、ステップ 4 に一覧表示されている複数の Microsoft サーバにアクセスして、Windows アップデートを受信できます。さらに、ステップ 4（mypartnersite.com）に一覧表示されているパートナー Web サイトにユーザがアクセスしようとすると、問題なく、そしてユーザ名とパスワードの入力を促されることなくサイトを表示できます。

詳細情報の入手先

このタスクに含まれる手順の詳細情報については、次の項を参照してください。

- 「カスタム URL カテゴリの作成および編集」（P.17-16）
- 「ID の作成」（P.8-18）
- 「認証のバイパス」（P.20-30）

特定の HTTPS Web サイトの復号化のバイパス

このタスクでは、特定の HTTPS Web サイトにトラフィックをパススルーさせます。これは、他の Web サイトへのトラフィックを検査しながら、HTTPS Web サイトへのアクセスをユーザに許可するために必要となる場合があります。

Web セキュリティ アプライアンスがクライアントとサーバ間のトラフィックを復号化するときに、HTTPS を使用する Web サイトおよび Web ベースのアプリケーションが作用しない場合があります。これらの HTTPS Web サイトを信頼している場合、トラフィックを復号化してマルウェアの検査をし、利用規定を実施せずに、クライアントから HTTPS サーバにトラフィックをパススルーするようにアプライアンスを設定できます。

たとえば、ローカル ネットワークに接続されながら HTTPS を使用するパートナー Web サイトにアクセスできないことにユーザは不満を持っています。IT は、Web セキュリティ アプライアンスのアクセス ログを読み取り、パートナーの HTTPS サーバが HTTPS による RFC に完全に準拠しておらず、クライアントと HTTPS サーバ間のトラフィックを復号化するときに HTTPS プロキシと正常に通信できないことを学習しました。パートナーの Web サイトへのすべての HTTPS トラフィックをバイパスすることによって、他の HTTPS サーバへのトラフィックを復号化しながらアクセスを許可できます。

このタスクでは、HTTPS プロキシがイネーブルで、デフォルトでトラフィックを復号化することを前提としています。

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）] ページに移動します。

ステップ 2　[カスタム URL カテゴリ（Custom URL Categories）] ページで、[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　[カテゴリ名（Category Name）] フィールドに、[HTTPSPassThru] など、このカテゴリの名前を入力します。

ステップ 4　[サイト名（Sites）] フィールドに、[mypartnersite.com] などの復号化をバイパスする Web サイトのアドレスを入力します。

ステップ 5　[実行（Submit）] をクリックします。

ステップ 6　[Web セキュリティ マネージャ（Web Security Manager）] > [アイデンティティ（Identities）] ページに移動します。

ステップ 7　[アイデンティティを追加（Add Identity）] をクリックします。

ステップ 8　[名前（Name）] フィールドに、[WebsitesToBypassDecryption] など、このポリシーの名前を入力します。

ステップ 9　[メンバーシップの定義（Membership Definition）] の下で、[詳細（Advanced）] をクリックして、詳細なポリシー オプションを展開します。

ステップ 10　[URL Categories] の横にあるリンクをクリックします。

ステップ 11　[アイデンティティ：ポリシー「WebsitesToBypassDecryption」：URL カテゴリによるメンバーシップ（Identities: Policy “WebsitesToBypassDecryption”：Membership by URL Categories）] ページの [カスタム URL カテゴリ（Custom URL Categories）] セクションで、ステップ 3 で作成したカスタム URL カテゴリの [Add] カラムをクリックします。

ステップ 12　[完了（Done）] をクリックします。

ステップ 13　[実行（Submit）] をクリックします。

ステップ 14　[Web セキュリティ マネージャ（Web Security Manager）] > [復号化ポリシー（Decryption Policies）] ページに移動します。

ステップ 15　[ポリシーを追加（Add Policy）] をクリックします。

ステップ 16　[名前（Name）] フィールドに、[DPPassThrough] など、このポリシーの名前を入力します。

ステップ 17　[アイデンティティとユーザ（Identities and Users）] フィールドで、「Select One or More Identities」を選択します。

ステップ 18　[アイデンティティ（Identity）] フィールドで、ステップ 8 で作成した ID を選択します。

ステップ 19　変更を送信し、保存します。

ユーザがステップ 4 に一覧表示されている Web サイトにアクセスしようとすると、他のサイトのトラフィックを復号化しながら、問題なくサイトを表示できます。

詳細情報の入手先

このタスクに含まれる手順の詳細情報については、次の項を参照してください。

- 「カスタム URL カテゴリの作成および編集」（P.17-16）
- 「ID の作成」（P.8-18）
- 「HTTPS プロキシのイネーブル化」（P.11-13）
- 「復号ポリシーの作成」（P.11-17）

アンチマルウェア スキャンのバイパスなしの Web レピュテーション フィルタリングのバイパス

このタスクでは、一部の Web サイトからダウンロードされたコンテンツのマルウェアがスキャンされていることを確認しながら、それらのサイトの Web レピュテーション フィルタリングをバイパスします。これは、Web レピュテーション スコアが非常に低い特定の Web サイトとの作業が組織で必要で、このサイトへのアクセスを許可するために実行する必要がある場合があります（-6.0 などの設定されたデフォルトのスコアのしきい値より低いスコア）。ただし、マルウェアからユーザを保護したいので、サイトが確実にアンチマルウェア スキャン エンジンによってスキャンされるようにします。

たとえば、お客様の Web サイトが確実なドメインも実行する IP アドレスを持つサーバで実行されるので、お客様の全体的なレピュテーション スコアを下げます。IT 部門は、ユーザのアクセスを許可する程度に組織がお客様の Web サイトを信頼していることを確認しました。お客様のドメインの Web レピュテーション フィルタリングをバイパスすることで、ダウンロードしたコンテンツのマルウェアをスキャンしながら、ユーザのアクセスを許可できます。

このタスクでは、次の内容を前提とします。

- Adaptive Scanning 機能がイネーブルになっていないこと。Adaptive Scanning がイネーブルの場合、Web レピュテーション スコアのしきい値を設定できません。
- Web レピュテーション フィルタリングにバイパスするアドレスのリストがあること。このタスクでは、架空のサイト mylowreputationsite.com の Web レピュテーション フィルタリングをバイパスします。
- -7.0 以下の Web レピュテーション スコアですべての Web サイトをブロックしようとしていること。つまり、Web レピュテーション フィルタリングをバイバスする Web サイトは -7.0 以上のスコアを持ちます。

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）] ページに移動します。

ステップ 2　[カスタム URL カテゴリ（Custom URL Categories）] ページで、[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　[カテゴリ名（Category Name）] フィールドに、[BypassWebRep] など、このカテゴリの名前を入力します。

ステップ 4　[サイト（Sites）] フィールドに、Web レピュテーション フィルタリングをバイパスする Web サイトのアドレスを入力します。このタスクでは、次のアドレスを入力してください。

- mylowreputationsite.com
- アクセスする -7.0 より大きい Web レピュテーション スコアを持つ他の Web サイト。

ステップ 5　[実行（Submit）] をクリックします。

ステップ 6　[Web セキュリティ マネージャ（Web Security Manager）] > [アイデンティティ（Identities）] ページに移動します。

ステップ 7　[アイデンティティを追加（Add Identity）] をクリックします。

ステップ 8　[名前（Name）] フィールドに、[WebsitesToBypassWebRep] など、このポリシーの名前を入力します。

ステップ 9　[メンバーシップの定義（Membership Definition）] の下で、[詳細（Advanced）] をクリックして、詳細なポリシー オプションを展開します。

ステップ 10　[URL カテゴリ（URL Categories）] の横にあるリンクをクリックします。

ステップ 11　[アイデンティティ：ポリシー「WebsitesToBypassWebRep」URL カテゴリによるメンバーシップ（Identities: Policy “WebsitesToBypassWebRep”: Membership by URL Categories）] ページの [カスタム URL カテゴリ（Custom URL Categories）] セクションで、ステップ 3 で作成したカスタム URL カテゴリの [追加（Add）] カラムをクリックします。

ステップ 12　[完了（Done）] をクリックします。

ステップ 13　[実行（Submit）] をクリックします。

ステップ 14　[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）] ページの順に進みます。

ステップ 15　[ポリシーを追加（Add Policy）] をクリックします。

ステップ 16　[ポリシー名（Policy Name）] フィールドに、[APBypassWebRep] など、このポリシーの名前を入力します。

ステップ 17　[アイデンティティとユーザ（Identities and Users）] フィールドで、「Select One or More Identities」を選択します。

ステップ 18　[アイデンティティ（Identity）] フィールドで、ステップ 8 で作成した ID を選択します。

ステップ 19　[実行（Submit）] をクリックします。

ステップ 20　[アクセス ポリシー（Access Policies）] ページで、ステップ 16 で作成したアクセス ポリシーの [Web レピュテーションおよびマルウェア対策フィルタ（Web Reputation and Anti-Malware Filtering）] リンクをクリックします。

ステップ 21　「Web Reputation and Anti-Malware Settings」セクションの下で、選択されていない場合に、[Web レピュテーションおよびマルウェア対策カスタム設定を定義（Define Web Reputation and Anti-Malware Custom Settings）] を選択します。

ステップ 22　左側のマーカーを -7.0 に移動して、URL をブロックするスコアのしきい値を変更します。

ステップ 23　変更を送信し、保存します。

ユーザがステップ 4 で Web サイトへのアクセスを試みるとき、現在のスコアが -7.0 以上で、スキャン中にマルウェアが存在しない限り、アクセスできるようになっているはずです（Web レピュテーションによってブロックされたことを知らせるエンドユーザ通知ページは表示されません）。

詳細情報の入手先

このタスクに含まれる手順の詳細情報については、次の項を参照してください。

- 「カスタム URL カテゴリの作成および編集」（P.17-16）
- 「ID の作成」（P.8-18）
- 「アクセス ポリシーの Web レピュテーションとアンチマルウェア設定」（P.19-11）
- 「Web レピュテーション スコアの設定」（P.19-14）

Active Directory ユーザ グループに対するアクセス ポリシーの作成

ユーザごとに異なるアクセス コントロールの異なるレベルを付与する必要がある場合があります。たとえば、マーケティング ユーザによるパートナー Web サイトへのアクセスを許可し、エンジニアリング ユーザによるパートナー サイトへのアクセスをブロックする必要がある場合があります。ユーザが Microsoft Active Directory などの認証サーバに認証され、認証サーバに異なるユーザ グループが定義されている場合、異なるユーザ グループに対して異なるポリシーを作成できます。

このタスクでは、異なる Active Directory ユーザ グループでユーザに適用する 2 つのアクセス ポリシーを作成します。一方のポリシーはマーケティング ユーザ向けで、もう一方のポリシーはエンジニアリング ユーザ向けになります。

このタスクでは、設定されたユーザ エージェントで Active Directory サーバを参照する Web セキュリティ アプライアンスに NTLM 認証レルムが定義されていることを前提とします。

ステップ 1　[Web セキュリティ マネージャ（Web Security Manager）] > [アイデンティティ（Identities）] ページに移動します。

ステップ 2　[アイデンティティを追加（Add Identity）] をクリックします。

ステップ 3　[名前（Name）] フィールドに、[NTLMUsers] など、このポリシーの名前を入力します。

ステップ 4　[上に挿入（Insert Above）] フィールドで、この ID が認証を必要としない他の ID の下にあることを確認します。

ステップ 5　[認証別メンバの定義（Define Members by Authentication）] セクションで、ドロップダウン メニューから「Require Authentication」を選択します。

ステップ 6　[レルムまたはシーケンスを選択（Select a Realm or Sequence）] フィールドで、アプライアンスにすでに定義されている NTLM 認証レルムを選択します。

ステップ 7　[プロトコル別メンバの定義（Define Members by Protocol）] セクションで、「HTTP/HTTPS Only」を選択します。これは、ネイティブ FTP トランザクションで認証がサポートされていないためです。

ステップ 8　他のすべての設定でデフォルト値を使用します。または任意で、組織での必要に応じて変更します。

ステップ 9　[実行（Submit）] をクリックします。

ステップ 10　[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）] ページの順に進みます。

ステップ 11　[ポリシーを追加（Add Policy）] をクリックします。

ステップ 12　[ポリシー名を追加（Policy Name）] フィールドに、[MarketingPolicy] など、このポリシーの名前を入力します。

ステップ 13　[アイデンティティとユーザ（Identities and Users）] フィールドで、「Select one or More Identities」を選択します。

ステップ 14　[アイデンティティ（Identities）] フィールドで、ステップ 3 で作成した ID を選択します。

ステップ 15　[NTLM 承認レルムの承認済みユーザとグループ（Authorized Users and Groups for the NTLM authentication realm）] の下で、「Selected Groups and Users」を選択して、「Groups」の横のリンクをクリックします。

ステップ 16　[アクセス ポリシー：ポリシー「PoliceName」：グループを編集（Access Policies: Policy "PolicyName": Edit Groups）] ページで、[承認済みグループ（Authorized Groups）] セクションにユーザ グループを追加します。これには、次のいずれかの方法を使用できます。

- ディレクトリ検索リスト ウィンドウでユーザ グループを選択して、[追加（Add）] をダブルクリックするか、クリックします。
- ディレクトリ検索ウィンドウにグループ名全体を入力し、検索が完了したら、[追加（Add）] をクリックします。これにより、信頼されたドメインに属するグループまたはディレクトリでまだ使用できないグループなどのディレクトリ検索リストに表示されないグループを入力することができます。

ステップ 17　[完了（Done）] をクリックします。

ステップ 18　[実行（Submit）] をクリックします。

ステップ 19　[EngineeringPolicy] などの異なるアクセス ポリシー名を使用し、異なる Active Directory ユーザ グループを指定して、ステップ 11 ～ステップ 18 を繰り返します。

ステップ 20　[アクセス ポリシー（Access Policies）] ページで、必要に応じてアクセス ポリシーごとにアクセス コントロール設定を設定します。

ステップ 21　変更を送信します。

ステップ 16 で定義されているユーザ セットのユーザに、ステップ 19 で定義されているユーザとは別のアクセス ポリシーが適用されます。アクセス ポリシーごとに異なるアクセス コントロール設定を設定することを想定して、Web へのアクセス時に各ユーザ セットが異なる動作を観察します。

詳細情報の入手先

このタスクに含まれる手順の詳細情報については、次の項を参照してください。

- 「ID の作成」（P.8-18）
- 「他のポリシー グループの ID の設定」（P.8-22）

ログ ファイル転送の自動化

このタスクでは、SCP を使用してアクセス ログをリモート サーバに毎日正午と深夜に自動的に転送されるようにアプライアンスを設定します。これは、各ログ ファイルに同じ時間（12 時間）の Web Access 情報が含まれるようにする場合に必要な場合があります。

たとえば、毎日アクセス ログの Web データを分析するためにサードパーティ製ツールを使用し、各アクセス ログ ファイルに厳密に同じ量の時間（12 時間）を含めます。

このタスクでは、ホスト名、ディレクトリ、およびユーザ名を含む SCP サーバへのアクセスがあることを前提としています。

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）] ページに移動します。

ステップ 2　[ログ名（Log Name）] カラムの下の「accesslogs」リンクをクリックします。

ステップ 3　[ログ設定を編集（Edit Log Subscription）] ページの [時刻によりロールオーバー（Rollover by Time）] フィールドで、「Daily Rollover」を選択します。

ステップ 4　[時刻（Time of Day）] フィールドに次のテキストを入力します。

```
00:00, 12:00
```

（注）　カンマで分けて複数回入力することで、1 日に複数回ログ ファイルを自動的に転送できます。

ステップ 5　[検索方法:（Retrieval Method）] セクションで、「SCP on Remote Server」を選択します。

ステップ 6　SCP ホスト名およびユーザ名などの必須 SCP サーバ情報を入力します。

ステップ 7　他の設定はそのままにするか、必要に応じて変更します。

ステップ 8　変更を送信し、保存します。

Web 用 AsyncOS が新しく保存されたログ フィルを毎日正午と深夜に SCP サーバに転送されるようになります。ログ ファイルをロールオーバーするときに Web 用 AsyncOS が実行するタスクの詳細については、「ログ サブスクリプションのロール オーバー」（P.24-9）を参照してください。

詳細情報の入手先

このタスクに含まれる手順の詳細情報については、次の項を参照してください。

- 「ログ サブスクリプションの使用」（P.24-7）
- 「ログ サブスクリプションのロール オーバー」（P.24-9）

Web トラフィックのリダイレクト

Cisco IronPort Web セキュリティ アプライアンスを使用して、異なる Web サイトにユーザをリダイレクトできます。最初の宛先がカスタム URL カテゴリの URL であるトラフィックを指定する場所にリダイレクトするように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、アプライアンス上のトラフィックをリダイレクトできます。

たとえば福利厚生部門は、健康保険会社などの福利厚生情報を参照して編集するユーザのリンクが含まれる内部 Web ページを所有しています。福利厚生部門は、福利厚生の登録の期限を通知する電子メールをユーザに事前に送信しました。ただし、福利厚生の登録の期限の数日前に Web ページの場所を変更する必要がありました。すべてのユーザに新しい電子メールを送信する代わりに、元の URL からの新規の正しい URL にユーザをリダイレクトするために Web セキュリティ アプライアンスを使用できます。

このタスクでは、異なる内部サーバに内部サーバのトラフィックをリダイレクトします。

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）] ページに移動します。

ステップ 2　[カスタム URL カテゴリ（Custom URL Categories）] ページで、[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　[カテゴリ名（Category Name）] フィールドに、[IntranetToRedirect] など、このカテゴリの名前を入力します。

ステップ 4　[サイト（Sites）] フィールドに、別の URL にリダイレクトする Web サイトのアドレスを入力します。このタスクでは、次のアドレスを入力してください。

- intranet.example.com

ステップ 5　[実行（Submit）] をクリックします。

ステップ 6　[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）] ページの順に進みます。

ステップ 7　[ポリシーを追加（Add Policy）] をクリックします。

ステップ 8　[ポリシー名（Policy Name）] フィールドに、[APRedirectIntranet] など、このポリシーの名前を入力します。

ステップ 9　[アイデンティティとユーザ（Identities and Users）] フィールドで、「All Identities」のデフォルト値を保持します。

ステップ 10　[実行（Submit）] をクリックします。

ステップ 11　[アクセス ポリシー（Access Policies）] ページで、ステップ 8 で作成したアクセス ポリシーの [URL フィルタ（URL Filtering）] リンクをクリックします。

ステップ 12　[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 13　[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、ステップ 3 で作成したカスタム URL カテゴリの「Include in policy」を選択します。

ステップ 14　[適用（Apply）] をクリックします。

ステップ 15　[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、追加したばかりのカスタム URL カテゴリの [リダイレクト（Redirect）] カラムをクリックします。

ステップ 16　[リダイレクト先（Redirect to）] フィールドでは、[internal.example.com] などのステップ 4 の URL に最初に送信されたトラフィックをリダイレクトする URL を入力します。

ステップ 17　変更を送信し、保存します。

ユーザがブラウザを開き、intranet.example.com にアクセスしようとすると、ブラウザが internal.example.com にリダイレクトされます。

詳細情報の入手先

このタスクに含まれる手順の詳細情報については、次の項を参照してください。

- 「カスタム URL カテゴリの作成および編集」（P.17-16）
- 「トラフィックのリダイレクト」（P.17-20）

A
HTTPS リファレンス

この付録の内容は、次のとおりです。

HTTPS の概要

HTTPS は、HTTP の保護された形式として機能する Web プロトコルです。HTTPS は HTTP 要求と応答を暗号化してから、ネットワーク経由で送信されます。一般的に、HTTPS を使用しているサイトへの接続は「安全」であると考えられています。HTTPS 接続は保護されていますが、安全というわけではなく、悪意のあるサーバや信頼できないサーバは識別されません。HTTPS は、正当なトランザクションを完了するセキュリティで保護された方法ではありますが、ネットワークに感染するおそれのあるマルウェアも確実にダウンロードしてしまう危険な方法でもあります。

HTTPS トラフィックを検査できないと、ネットワークは次のようなリスクに対して無防備になってしまします。

- **セキュリティで保護されたサイトのマルウェアのホスティング。**スパマーやフィッシャは HTTPS 接続経由でのみ到達できる正当な閲覧用 Web サイトを作成できます。ユーザは、HTTPS 接続が必要であることから、その Web サーバを誤って信頼してしまい、その結果意図的あるいは意図せずにマルウェアをダウンロードしてしまうことがあります。
- **HTTPS Web アプリケーションからのマルウェア。**マルウェアの中には、セキュア メール クライアントなどの正当な Web アプリケーションから、添付ファイルをダウンロードすることでネットワークに感染できるものもあります。
- **セキュリティで保護された匿名プロキシ。**一部の Web サーバは HTTPS 接続を介してプロキシ サービスを提供し、それによりユーザはアクセプタブル ユース ポリシーを回避できます。ネットワーク上のユーザがネットワーク外のセキュア プロキシ サーバを使用する場合、ユーザは Web レピュテーションやマルウェア コンテンツに関係なく、どのような Web サイトにもアクセスできます。

アプライアンスは、URL フィルタリング エンジンと Web レピュテーション フィルタの両方を使用して、HTTPS 接続を復号化する時点について知的意志決定を行います。この組み合わせを使用することで、管理者とエンド ユーザは、プライバシーとセキュリティの間で無理に妥協をしなくても済むようになります。

あたかもプレーン テキスト HTTP トランザクションであるかのように、各方向へのデータの受け渡しを復号化し、アクセス ポリシーを適用して、HTTPS 接続を検査せずに続行できるようにするかどうか、アプライアンスを中継装置として機能させるかどうかを指定する HTTPS ポリシーを定義できます。

HTTPS 要求を処理するようにアプライアンスを設定するには、次のタスクを実行する必要があります。

1. **HTTPS プロキシをイネーブルにします。**HTTPS トラフィックをモニタし、復号化するには、まず HTTPS プロキシをイネーブルにする必要があります。詳細については、「HTTPS 証明書の検証およびコンテンツの復号化のイネーブル化」（P.11-8）を参照してください。
2. **復号化ポリシー グループを作成および設定します。**HTTPS プロキシがイネーブルになると、復号化ポリシー グループを作成および設定して、各ユーザからの個々の要求を処理する方法を決定できます。詳細については、「復号ポリシーの作成」（P.11-17）を参照してください。
3. **（任意）カスタム ルート証明書をインポートします。**1 つ以上のカスタム ルート証明書を任意でインポートできます。これにより、Web プロキシは、HTTPS プロキシ サーバで使用される追加の信頼できるルート認証局を認識できるようになります。詳細については、「信頼できるルート証明書」（P.11-23）を参照してください。

（注）　HTTPS プロキシがディセーブルになると、Web プロキシは、明示的な HTTPS 接続をパス スルーし、透過的にリダイレクトされた HTTPS 要求をドロップします。アクセス ログには、明示的な HTTPS 接続に対する CONNECT 要求が含まれますが、透過的にリダイレクトされた HTTPS 要求のドロップに関するエントリは存在しません。

このマニュアルでは、デジタル暗号化に関する多くの用語が使用されています。このマニュアルには、HTTPS およびデジタル暗号化に関する背景説明を使用したセクションも含まれています。これらの情報は参照用に提供されるものです。このマニュアルで使用される用語および定義の一覧については、「デジタル暗号化に関する用語」（P.A-2）を参照してください。HTTPS プロトコルの概要については、「HTTPS の基礎」（P.A-3）を参照してください。

デジタル暗号化に関する用語

暗号化および復号化がどのように行われるかを理解するには、暗号符号化技術についてある程度理解する必要があります。図 A-1 では、この章で説明する暗号化で使用されるいくつかの用語について説明します。

表 A-1　暗号化の用語と定義

用語	定義
認証局	他の関係者によって使用されるデジタル証明書を発行する事業体。 認証局は、信頼できる第三者と呼ばれる場合があります。通常、認証局は提供したサービスに対して料金を請求する営利企業です。ただし、一部の団体や政府は独自の認証局を所有し、中には無償でサービスを提供するものがあります。
暗号	適切なキーなしでシステムが判読できないようにテキストを符号化し、それを復号化するために使用されるアルゴリズム。 サイファは、キーを使用してテキストを符号化または復号化します。
暗号文	サイファを適用した後の符号化されたテキスト。

表 A-1　暗号化の用語と定義 （続き）

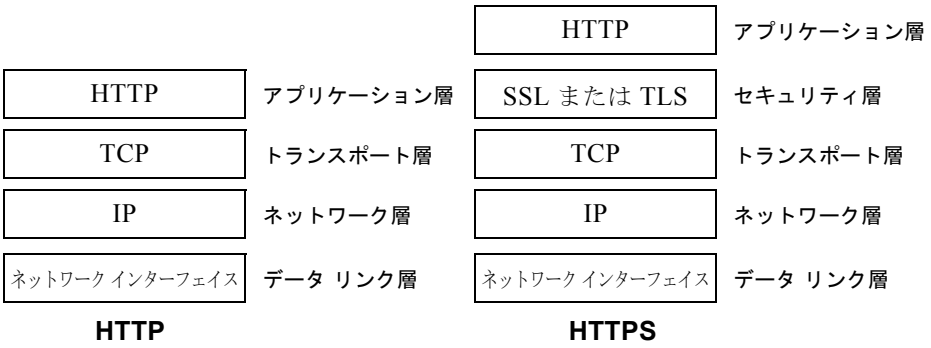
用語	定義
デジタル証明書。	認証局と呼ばれる信頼できる組織が確認および署名した組織を特定し、説明する電子文書。 デジタル証明書は、「ID カード」と概念が似ています。SSL は、証明書を使用してサーバを認証します。 デジタル証明書の詳細については、「デジタル証明書」（P.A-5）を参照してください。
デジタル署名	メッセージが表明された作成者によって作成され、作成後変更されていないかどうかを確認するチェックサム。
キー	テキストを符号化または暗号化するために、サイファによって使用される数値パラメータ。
プレーン テキストまたはクリア テキスト	サイファによって符号化される前の元の形式のメッセージ テキスト。
公開キー暗号化	1 つのキーだけが公開され、他のキーが非公開となっているときに、テキストを符号化および復号化するために異なる 2 つのキーを使用するシステム。 公開キー暗号化を使用すると、任意のユーザが公開キーを公開したサーバに符号化されたメッセージを送信できます。ただし、メッセージを復号化できるのは、秘密キーを所有する受信サーバだけです。 これは、非対称キー暗号方式とも呼ばれています。
公開キー インフラストラクチャ（PKI）	認証局による個々のユーザの ID を公開キーにバインドする仕組み。 X.509 は PKI 規格の例です。X.509 は公開キー証明書用の規格および認証パスを検証するアルゴリズムを指定します。
秘密キー暗号化	テキストの符号化および復号化に同じキーを使用するシステム。 トランザクションの両側で同じキーが必要になるため、特定の通信セッションで使用するキーに応じてセキュアな通信を行う方法が必要です。通常、公開キー暗号化を使用してセキュアな通信を確立してから、残りのセッションに使用する一時対称キーを生成します。 これは、対称キー暗号方式とも呼ばれています。
ルート証明書	証明書ツリー構造の最上位の証明書となる証明書。 ルート証明書の下位にある証明書は、すべてルート証明書の信頼性を継承します。 ルート証明書は、未署名公開キー証明書、または自己署名証明書を使用できます。
自己署名証明書	認証局と証明書作成者が同一であるデジタル証明書。

HTTPS の基礎

HTTPS は、HTTP の保護された形式として機能する Web プロトコルです。HTTPS は HTTP 要求と応答データを暗号化してから、ネットワーク経由で送信されるため安全です。HTTPS は、HTTP レイヤが Secure Sockets Layer（SSL）または Transport Layer Security（TLS）のいずれかを使用してセキュリティ層の上で送信されるのを除き HTTP と同様に動作します。SSL と TLS はよく似ているため、このガイドでは、特に指定しない限り、「SSL」を使用して SSL と TLS の両方を表すこととします。

図 A-1 は、HTTPS と HTTP の OSI ネットワーク層の違いを示します。この図は、HTTPS がセキュリティ層の SSL または TLS の上にあるアプリケーション層の HTTP プロトコルであることを示します。

図 A-1　　HTTPS と HTTP の OSI 層



通常、URL はクライアント アプリケーションがサーバと通信するために HTTP を使用するか、HTTPS を使用するかを指定します。

- **http://*servername*。**デフォルトで、クライアント アプリケーションはポート 80 でサーバへの接続を開き、プレーン テキストで HTTP コマンドを送信します。
- **https://*servername*。**デフォルトで、クライアント アプリケーションはポート 443 でサーバへの接続を開き、SSL「ハンドシェイク」の実行を開始して、クライアントとサーバ間のセキュアな接続を確立します。セキュアな接続が確立されると、クライアント アプリケーションは暗号化された HTTP コマンドを送信します。SSL ハンドシェイクの詳細については、「SSL ハンドシェイク」（P.A-4）を参照してください。

SSL ハンドシェイク

SSL「ハンドシェイク」は、クライアントとサーバが SSL プロトコルを使用してセキュアな接続を確立するために実行する一連の手順です。クライアントとサーバが暗号化された HTTP メッセージを送受信できるようにするには、次の手順を実行する必要があります。

1. **プロトコルのバージョン番号を交換します。**クライアントとサーバが互換性のある SSL または TLS のバージョンを使用して通信できることを両側で確認する必要があります。
2. **両側が認識するサイファを選択します。**まずクライアントが、サポートするサイファをアドバタイズし、サーバにその証明書を送信するように要求します。次に、サーバが最も強力なサイファを一覧から選択し、選択したサイファとそのデジタル証明書をクライアントに送信します。
3. **両側の ID を認証します。**通常、サーバだけが認証され、クライアントは未認証のままになります。クライアントがサーバの証明書を検証します。証明書および証明書を使用してサーバを認証する方法の詳細については、「デジタル証明書」（P.A-5）を参照してください。
4. **一時対称キーを生成して、このセッションのチャネルを暗号化します。**クライアントがセッション キー（通常は乱数）を生成し、それをサーバの公開キーを使用して暗号化してサーバに送信をます。サーバは、秘密キーを使用してセッション キーを復号化します。今後接続が閉じられるまで、すべての暗号化および復号化に使用する共通のマスター秘密キーを両側で計算します。

デジタル証明書

デジタル証明書とは、信頼できる組織によって確認および署名された、組織を特定し、説明する電子文書です。デジタル証明書は、運転免許証やパス ポートなどの ID カードと概念が似ています。証明書に署名する信頼できる組織は、認証局とも呼ばれています。

証明書によって、クライアントは通信する予定の組織と通信していることを確認できます。サーバ証明書が既知または信頼できる認証局によって署名されると、クライアントはどの程度サーバを信頼できるかをより正確に評価できます。

X.509 は、公開キー インフラストラクチャ（PKI）規格の例です。X.509 は、証明書用の規格および認証パスを検証するアルゴリズムを指定します。Web セキュリティ アプライアンスは X.509 規格を使用します。

X.509 証明書には、次の情報が含まれています。

- ユーザ、サーバ、または組織の名前など、サブジェクトの ID
- 証明書の有効期間
- 証明書を保証する認証局
- 認証局がその秘密キーを使用して作成した証明書のデジタル署名
- サブジェクトの公開キー

ユーザが Web ブラウザで確認できるデジタル証明書の例については、「ルート証明書の使用」（P.A-8）を参照してください。

誰でもデジタル証明書を作成できますが、誰もが評判の良い認証局に証明書の情報を保証してもらい、その秘密キーを使用して証明書に署名してもらうことはできません。デジタル証明書の認証局の検証に関する詳細については、「認証局の検証」（P.A-5）を参照してください。

認証局の検証

X.509 規格では、他の認証局によって署名されたデジタル証明書の発行を認証局に許可しています。このシステムがあるため、認証局はツリー構造の階層となっています。

ツリー構造の最上位の認証局は、ルート証明書と呼ばれています。ルート証明書は、ツリー構造の最上位にあるため、別の認証局により署名されることはありません。つまり、定義上、すべてのルート証明書は自己署名証明書となります。ルート証明書に記載されている認証局は証明書の作成者です。

ルート証明書の下位にある証明書は、すべてルート証明書の信頼性を継承します。たとえば、CertificateAuthorityABC が信頼できる認証局で、認証局 CertificateAuthorityXYZ の証明書に署名すると、CertificateAuthorityXYZ は自動的に信頼できる認証局になります。

図 A-2 は、Web ブラウザに表示される証明書の認証パスを示します。

図 A-2　認証パスの例

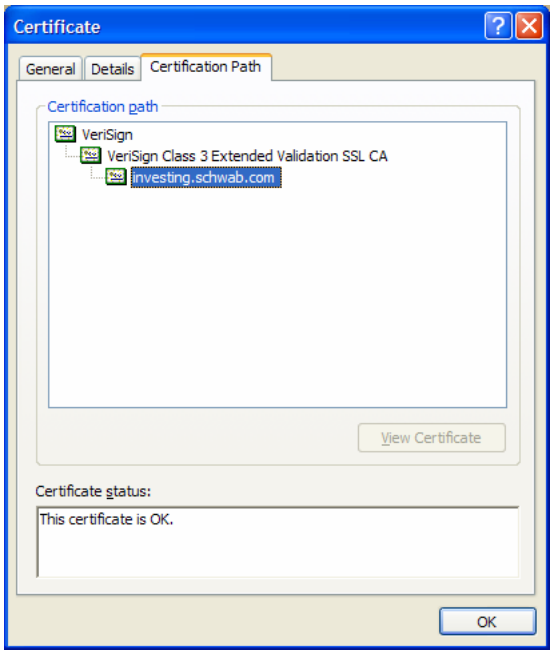


図 A-2 では、URL「investing.schwab.com」の証明書は、認証局「VeriSign Class 3 Extended Validation SSL CA」によって署名され、この認証局は認証局「VeriSign」によって署名されています。

定義上、ルート証明書は、X.509 規格に準拠するアプリケーションによって常に信頼されます。Web セキュリティ アプライアンスは X.509 規格を使用します。

標準 Web ブラウザには、一連の信頼できるルート証明書が付属しています。ルート証明書のリストは定期的に更新されます。Web ブラウザにインストールされたルート証明書を表示できます。

たとえば、Mozilla Firefox 2.0 でインストールされたルート証明書を表示するには、[ツール（Tools）] > [オプション（Options）] > [詳細（Advanced）] > [暗号化（Encryption）] > [証明書の表示（View Certificates）] を選択します。Internet Explorer 7 でインストールされているルート証明書を表示するには、[ツール（Tools）] > [インターネット オプション（Internet Options）] > [コンテンツ（Content）] > [証明書（Certificates）] > [信頼されたルート証明書機関（Trusted Root Certification Authorities）] を選択します。

図 A-2 では、VeriSign 証明書は Web ブラウザに付属するルート証明書です。

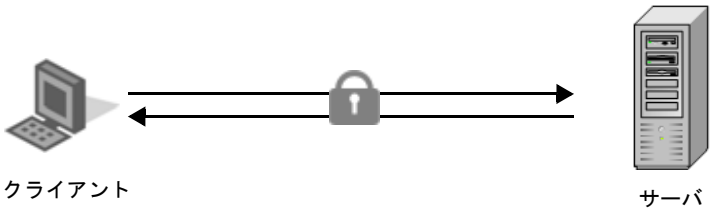
Web セキュリティ アプライアンスをインストールすると、一連の信頼できるルート証明書もインストールされます。ただし、Web プロキシが信頼できると見なす追加ルート証明書をアップロードできます。詳細については、「信頼できるルート証明書」（P.11-23）を参照してください。

HTTPS トラフィックの復号化

要求および応答データは、ネットワークを介して送信される前に HTTPS 接続用に暗号化されます。データが暗号化されるため、第三者はデータを表示できますが、HTTPS サーバの秘密キーがなければ、それを復号化してコンテンツを読み取ることはできません。

図 A-3 は、クライアントと HTTPS サーバ間の HTTPS 接続を示します。

図 A-3　　HTTPS 接続



Web セキュリティ アプライアンスは、サーバの秘密キーへのアクセス権がないため、クライアントとサーバの間のトラフィックを検査するために、接続をインターセプトし、この接続を 2 つの別個の接続に分割する必要があります。アプライアンスは、クライアントとサーバ間の中継装置として機能し、サーバがクライアントのように動作し、クライアントがサーバのように動作するようにします。これは、「中間者」と呼ばれることもあります。

図 A-4 は、Web セキュリティ アプライアンスを通過するクライアントと HTTPS サーバ間の HTTPS 接続を示します。

図 A-4　　Web セキュリティ アプライアンスによって復号化される HTTPS 接続

図 A-4 には、1 つはクライアントとアプライアンス間、1 つはアプライアンスとサーバ間の 2 つの HTTPS 接続があることに注意してください。アプライアンスは、1 回はクライアント、1 回はサーバの 2 回の SSL ハンドシェイクを実行します。

- **サーバとの SSL ハンドシェイク。**アプライアンスがサーバとの SSL ハンドシェイクを実行する際に、アプライアンスはあたかもサーバに要求を送信するクライアントであるかのように機能します。サーバとのセキュアな接続を確立後、暗号化データの受信を開始できます。クライアントとして動作し、SSL ハンドシェイクに参加することにより、サーバとの一時対称キーに合意しているので、サーバから送信されるデータを復号化し、読み取ることができます。また、アプライアンスはサーバのデジタル証明書も受信します。
- **クライアントとの SSL ハンドシェイク。**アプライアンスがクライアントとの SSL ハンドシェイクを実行する際に、アプライアンスはクライアントが要求するデータを提供する要求先サーバであるかのように機能します。クライアントとの SSL ハンドシェイクを実行するには、独自のデジタル証明書をクライアントに送信する必要があります。ただし、クライアントは要求されたサーバ証明書を予期するため、アプライアンスは、アプライアンス管理者がアップロードまたは設定したルート認証局を指定することで要求されたサーバの証明書を模倣します。

  サーバがサーバの証明書を模倣する仕組みに関する詳細については、「サーバのデジタル証明書の模倣」（P.A-8）を参照してください。

（注） アプライアンスは別のルート認証局を使用してサーバ証明書に署名し、その証明書をクライアントに送信するので、ネットワーク上のクライアント アプリケーションがルート認証局を認識することを確認する必要があります。詳細については、「ルート証明書の使用」（P.A-8）を参照してください。

2 つの別個の HTTPS 接続が確立されると、次のアクションが行われます。

1. サーバから暗号化されたデータを受信します。
2. サーバとネゴシエートした一時、対称キーを使用して、データが復号化されます。
3. あたかもプレーン 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 ポリシーが適用されます。アクセス ポリシーの詳細については、「トランザクション要求のブロック、許可、またはリダイレクト」（P.9-1）を参照してください。
4. アクセス ポリシー グループを使用してクライアントがデータを受信できることを前提として、データはクライアントとネゴシエートする一時、対称キーを使用して暗号化されます。
5. 暗号化されたデータがクライアントに送信されます。

（注）　復号化されたデータはキャッシュされません。ただし、復号化された HTTP トランザクションのアクセス ログがディスクに保存されます。

サーバのデジタル証明書の模倣

アプライアンスがクライアントと SSL ハンドシェイクを実行する際に、アプライアンスはサーバのデジタル証明書を模倣して、新しい証明書をクライアントに送信します。サーバのデジタル証明書を模倣するために、大部分のフィールド値を再利用し、一部のフィールド値を変更します。

模倣された証明書は、次のフィールドを除きサーバ証明書と同一です。

- **発行元。**発行元は、アプライアンスに設定されている生成済みまたはアップロード済みルート証明書から取得されます。
- **署名アルゴリズム。**このフィールドは、アプライアンスが使用するルート証明書に RSA キーまたは DSA キーが含まれるかどうかに応じて、常に「sha1WithRSAEncryption」または「dsaWithSHA1」になります。
- **公開キー。**アプライアンスは、元の証明書の公開キーを、元の証明書とビット強度が一致するように生成し、しかも公開キーと一致する秘密キーを持つように生成した公開キーに置き換えます。たとえば、サーバ証明書が 2048 ビット RSA キーを使用している場合、アプライアンスは新しい 2048 ビット RSA キーを生成します。
- **X509v3 拡張。**X509v3 拡張は、以下の項目を*除き*すべて削除されます。
  - 基本的制約
  - 主体者の代替名
  - キーの用途
  - サブジェクトキー識別子
  - キーの拡張用途

  たとえば、アプライアンスは、認証局キー識別子および認証局情報アクセスの X509v3 拡張を削除します。

ルート証明書の使用

Web セキュリティ アプライアンスは、クライアントが最初に接続要求を送信した HTTPS サーバを模倣します。要求先サーバのように振舞うクライアントとの間にセキュアな接続を確立するには、アプライアンスはアプライアンスに設定されたルート認証局によって署名されたクライアントにサーバ証明書を送信する必要があります。

アプライアンス上の HTTPS プロキシをイネーブルにすると、アプライアンスがサーバ証明書に署名するために使用するルート証明書情報の設定が可能になります。

証明書およびキー形式の変換

アプライアンスにアップロードするルート証明書と秘密キー 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。ただし、DER 形式の証明書とキーを PEM 形式に変換してから、アップロードすることはできます。たとえば、OpenSSL を使用して形式を変換できます。

次の OpenSSL コマンドを使用して、DER 形式の証明書ファイルを PEM 形式の証明書ファイルに変換します。

```
openssl x509 -inform DER -in cert_in_DER -outform PEM -out out_file_name
```

また、同様の OpenSSL コマンドを実行して、DER 形式のキー ファイルを PEM 形式に変換することもできます。

RSA キーの場合は、次のコマンドを使用します。

```
openssl rsa -inform DER -in key_in_DER -outform PEM -out out_file_name
```

DSA キーの場合は、次のコマンドを使用します。

```
openssl dsa -inform DER -in key_in_DER -outform PEM -out out_file_name
```

OpenSSL の使用の詳細については、OpenSSL のマニュアルを参照するか、http://openssl.org にアクセスしてください。

B
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.

INDEX

A

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W

X

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

よ

り

る

れ

ろ

わ

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先:シスコ コンタクトセンター
0120-092-255(フリーコール、携帯・PHS含む)
電話受付時間 : 平日 10:00〜12:00、13:00〜17:00
http://www.cisco.com/jp/go/contactcenter/