AsyncOS 8.1.1 for Cisco Content Security Management ユーザ ガイド

2013 年 10 月 29 日

Text Part Number: N/A

【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。

AsyncOS 8.1.1 for Cisco Content Security Management ユーザ ガイド

CONTENTS

CHAPTER 1

スタートアップ ガイド

今回のリリースでの変更点

ここでは、AsyncOS for Cisco Content Security Management のこのリリースにおける新機能と拡張機能について説明します。リリースの詳細については、次の URL にある製品リリース ノートを参照してください。

http://www.cisco.com/en/US/products/ps10155/tsd_products_support_series_home.html

アップグレードする場合、以前のリリースとこのリリースの間の他のリリースのリリース ノートも確認する必要があります。これは、これらのリリースで追加された機能および拡張機能を確認するためです。

機能	説明
リリース 8.1.1 の新機能：	
新しいハードウェアのサポート	このリリースでは、新しい M380 および M680 ハードウェアをサポートします。
リモート電源管理	この機能は M380 および M680 ハードウェアでのみ使用可能です。 アプライアンス シャーシの電源をリモートからリセットできるようになりました。 必要なときにこの機能を使用できるようにするには、事前にこの機能を設定する必要があります。「リモート電源管理のイネーブル化」（P.14-6）および「リモートからのアプライアンス電源のリセット」（P.16-6）を参照してください。
リリース 8.1.0 の新機能：	

機能	説明
集約ポリシー、ウイルス、およびアウトブレイク隔離	次の隔離がシスコのコンテンツ セキュリティ管理アプライアンスにまとめて集約されます。 • ウイルス対策 • アウトブレイク • 以下によって捕らえられるメッセージに使用されるポリシー隔離 – メッセージ フィルタ – コンテンツ フィルタ – データ漏洩防止ポリシー これらの隔離の集約には次の利点があります。 • 管理者は 1 か所で複数の電子メール セキュリティ アプライアンスからの隔離済みメッセージを管理できます。 • 隔離されたメッセージは、DMZ 内ではなくファイアウォールの背後に保存され、セキュリティ リスクを減らします。 • 集約隔離は、シスコのコンテンツ セキュリティ管理アプライアンスの標準バックアップ機能の一部としてバックアップされることができます。 詳細については、第 8 章「集約ポリシー、ウイルス、およびアウトブレイク隔離」を参照してください。
[お気に入り（My Favorites）] リスト	頻繁に使用するページをお気に入りページのクイック アクセス メニューに追加します。 詳細については、「お気に入りページの使用」（P.14-57）を参照してください。
バックグラウンドでのアップグレードのダウンロード	バックグラウンドでアップグレードをダウンロードしておき、後でインストールすることができ、サービスの中断を最小限に抑えることができます。 詳細については、「AsyncOS のアップグレード」（P.14-18）を参照してください。
以前のコンフィギュレーションへのロールバック	現在のコンフィギュレーションを以前のコンフィギュレーションに設定して、そのコンフィギュレーション以降のすべてのコンフィギュレーション変更をロールバックできます。 詳細については、「以前コミットしたコンフィギュレーションへのロールバック」（P.14-52）を参照してください。
最近のアラートの表示	アラート電子メールが配信されていなかったりまたは削除されていてもアプリケーションの最近のアラートのリストを表示できます。 詳細については、「最新アラートの表示」（P.14-35）を参照してください。

機能	説明
レポート作成機能の拡張	レポート作成機能の拡張により、以下が可能になります。 • 頻繁に参照するグラフやテーブルを使用したカスタム ページを作成します。詳細については、「カスタム レポート」（P.3-7）を参照してください。 • データ漏洩防止またはコンテンツ フィルタリング ポリシーに違反するメッセージのメッセージ トラッキング データを表示するためにレポート内のリンクをクリックします。この機能拡張により、こうした違反の調査パターンと根本原因を簡素化します。 さらに、Common Access Card（CAC）を使用している組織用に、クライアント証明書のある SMTP セッション認証を使用して受信したメッセージのデータの概要を新しい受信 SMTP 認証レポートに示します。
メッセージ トラッキング機能拡張	• 現在、次に対するメッセージ トラッキングを検索できます。 – UTF-8 符号化された件名のメッセージ – なんらかの隔離状態にあるメッセージ – コンテンツ フィルタで検出されたメッセージ • メッセージ トラッキングの検索結果およびメッセージの詳細にはメッセージが保存されている隔離のメッセージ詳細ページへのリンクが含まれるようになりました。 • メッセージ トラッキング クエリーから 1000 件以上のメッセージが返された場合、他のツールを使用した分析のためにカンマ区切り値ファイルとしてクエリーに一致する最大 50,000 件のメッセージをエクスポートできます。 • メッセージ トラッキングには、Common Access Card（CAC）を使用している組織用に、クライアント証明書のある SMTP セッション認証を使用して受信したメッセージのデータを含みます。
より柔軟なパスワードの長さのサポート	文字数ゼロも含め任意の長さのアプライアンスのパスワードがサポートされるようになりました。 詳細については、「パスワードの設定およびログインの要件」（P.13-13）を参照してください。
SNMP トラップの向上	linkUp および linkDown の SNMP トラップは、標準 RFC 実装（RFC-3418）に置き換えられました。
スパム隔離の向上	スパム隔離の検索結果の表示が、より簡単になりました。

詳細情報の入手先

Cisco 通知サービス

セキュリティ アドバイザリ、フィールド ノーティス、販売終了とサポート終了の通知、およびソフトウェア アップデートと既知の問題に関する情報などのシスコのコンテンツ セキュリティ アプライアンスに関連する通知が配信されるように署名して参加します。

受信する情報通知の頻度やタイプなどのオプションを指定できます。使用する製品ごとの通知に個別に参加する必要があります。

参加するには、次に移動します。http://www.cisco.com/cisco/support/notifications.html

Cisco.com アカウントが必要です。ない場合は、「シスコ アカウントの登録」（P.1-6）を参照してください。

マニュアル

この製品および関連製品のマニュアルは、次の Web サイトで入手可能です。

シスコのコンテンツ セキュリティ製品のマニュアル	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
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
電子メール セキュリティ アプライアンス	http://www.cisco.com/en/US/products/ps10154/tsd_products_support_series_home.html
コンテンツ セキュリティ製品用コマンドライン リファレンス ガイド	http://www.cisco.com/en/US/products/ps10154/prod_command_reference_list.html
Cisco IronPort 暗号化	http://www.cisco.com/en/US/partner/products/ps10602/tsd_products_support_series_home.html

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。

シスコ コンテンツ セキュリティ 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）。

- すべての製品のリリース ノート
- 『The *Quick Start Guide* for the Cisco Content Security Management appliance』
- *AsyncOS 8.1 for Cisco Content Security Management ユーザ ガイド*（このマニュアル）
- *『Cisco IronPort AsyncOS for Web Security User Guide』*
- Cisco AsyncOS for Email Security のドキュメント：

  Email Security リリース 8.0 以降：

  - 『*Cisco AsyncOS for Email User Guide*』

  Email Security リリース 8.0 より前：

  - 『*Cisco IronPort AsyncOS for Email Security Configuration Guide*』
  - 『*Cisco IronPort AsyncOS for Email Security Advanced Configuration Guide*』
  - 『*Cisco IronPort AsyncOS for Email Security Daily Management Guide*』
- 『*Cisco AsyncOS CLI Reference Guide*』

サード パーティ コントリビュータ

AsyncOS 内に付属の一部のソフトウェアは、FreeBSD、Stichting Mathematisch Centrum、Corporation for National Research Initiatives などのサード パーティ コントリビュータのソフトウェア使用許諾契約の条項、通知、条件の下に配布されています。これらすべての契約条件は、シスコのライセンス契約に含まれています。

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

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

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

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

シスコ コンテンツ セキュリティ製品に関する情報についてのナレッジ ベースにアクセスするには、以下の場所を参照してください。

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 ユーザ ID がない場合は、「シスコ アカウントの登録」（P.1-6）を参照してください。

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。コンテンツ セキュリティに関する一般的な問題や、特定のシスコ製品に関する技術情報について話し合う場を提供します。このフォーラムにトピックを投稿して質問したり、他のユーザと情報を共有したりできます。

シスコ サポート コミュニティには次の URL からアクセスできます。

- 電子メール セキュリティと関連管理:

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

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

シスコのテクニカル サポート

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

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

以下を含むさまざまな作業にこの Web サイトが役立ちます。

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

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

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

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

シスコ アカウントの登録

Cisco.com の多数のリソースへアクセスするには、シスコのアカウントが必要です。

Cisco.com のユーザ ID をお持ちでない場合は、https://tools.cisco.com/RPF/register/register.do で登録できます。

関連項目

- 「Cisco 通知サービス」（P.1-4）
- 「ナレッジ ベース」（P.1-5）

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。

シスコのコンテンツ セキュリティ管理の概要

AsyncOS for Cisco Content Security Management には次の機能が統合されています。

- **外部スパム隔離**：エンドユーザ向けのスパム メッセージおよび陽性と疑わしいスパム メッセージを保持しており、エンドユーザおよび管理者は、スパムとフラグ付けされたメッセージをレビューしてから最終的な決定を下すことができます。
- **集約ポリシー、ウイルス、アウトブレイク隔離**：これらの隔離および複数の電子メール セキュリティ アプライアンスから隔離内に隔離されたメッセージを管理するための単一のインタフェースを提供します。隔離されたメッセージをファイアウォールの背後に保存できます。
- **中央集中型レポーティング**：複数の電子メールおよび Web セキュリティ アプライアンスから集約したデータに対してレポートを実行します。個別アプライアンスで使用できる同じレポーティング機能を、セキュリティ管理アプライアンスでも使用できます。また、セキュリティ管理アプライアンスでのみ使用できる、Web セキュリティの拡張レポートがいくつかあります。
- **中央集中型トラッキング**：単一のインターフェイスを使用して、電子メール メッセージを追跡すること、および複数の電子メールおよび Web セキュリティ アプライアンスにより処理された Web トランザクションを追跡することができます。
- **中央集中型コンフィギュレーション管理**：簡易性および一貫性のために、最大 150 の Web セキュリティ アプライアンスのポリシー定義およびポリシー展開を管理できます。ポリシーは、セキュリティ管理アプライアンスから、複数の AsyncOS バージョンを実行するアプライアンスにプッシュできます。
- **データのバックアップ**：レポーティング データ、トラッキング データ、隔離されたメッセージ、安全な送信者とブロックされた送信者のリストなど、セキュリティ管理アプライアンスのデータをバックアップできます。

1 台のセキュリティ管理アプライアンスからのセキュリティ操作を調整することも、複数のアプライアンス間に負荷を分散させることもできます。

（注）　セキュリティ管理アプライアンスは、集約電子メール管理または電子メール セキュリティ アプライアンスの「クラスタリング」には関係ありません。

CHAPTER 2

セットアップ、インストール、および基本設定

ソリューション導入の概要

シスコのコンテンツ セキュリティ ソリューションにサービスを提供するシスコのコンテンツ セキュリティ管理アプライアンスを設定するには、次の手順に従います。

	対象アプライアンス	操作内容	追加情報
ステップ 1	すべてのアプライアンス	お使いのアプライアンスが、使用する機能のシステム要件を満たしていることを確認してください。 必要に応じて、アプライアンスをアップグレードします。	「SMA 互換性マトリクス」（P.2-2）を参照してください。
ステップ 2	電子メール セキュリティ アプライアンス	中央集中型サービスを環境に取り入れる前に、必要なセキュリティ機能が提供されるようにすべての電子メール セキュリティ アプライアンスを設定し、各アプライアンスですべての機能が予期したとおりに動作することを確認します。	Cisco Email Security のご使用のリリースのマニュアルを参照してください。

	対象アプライアンス	操作内容	追加情報
ステップ 3	Web セキュリティ アプライアンス	中央集中型サービスを環境に取り入れる前に、必要なセキュリティ機能が提供されるように少なくとも 1 つの Web セキュリティ アプライアンスを設定し、すべての機能が予期したとおりに動作することを確認します。	『*Cisco IronPort AsyncOS for Web Security User Guide*』を参照してください。
ステップ 4	セキュリティ管理アプライアンス	アプライアンスを設定し、システム セットアップ ウィザードを実行します。	「設置計画」（P.2-2）、「セットアップの準備」（P.2-4）、および「システム セットアップ ウィザードの実行」（P.2-8）を参照してください。
ステップ 5	すべてのアプライアンス	導入する各中央集中型サービスを設定します。	「セキュリティ管理アプライアンスでのサービスの設定」（P.2-14）から開始します。

SMA 互換性マトリクス

セキュリティ管理アプライアンスと電子メール セキュリティ アプライアンスおよび Web セキュリティ アプライアンスの互換性について、および Web セキュリティ アプライアンス設定をインポートおよび公開するときの設定ファイルの互換性については、「Compatibility Matrix」（http://www.cisco.com/en/US/products/ps10155/prod_release_notes_list.html）を参照してください。

設置計画

- 「ネットワーク プランニング」（P.2-2）
- 「セキュリティ管理アプライアンスと電子メール セキュリティ アプライアンスの統合について」（P.2-3）
- 「集中管理型の電子メール セキュリティ アプライアンスの展開」（P.2-3）

ネットワーク プランニング

セキュリティ管理アプライアンスの利用により、エンド ユーザのアプリケーションと、非武装地帯（DMZ）に存在する、より安全なゲートウェイ システムを切り離すことができます。2 層ファイアウォールの使用によって、ネットワーク プランニングの柔軟性が高まり、エンド ユーザが外部 DMZ に直接接続することを防止できます（図 2-1 を参照）。

図 2-1　セキュリティ管理アプライアンスを含む一般的なネットワーク設定

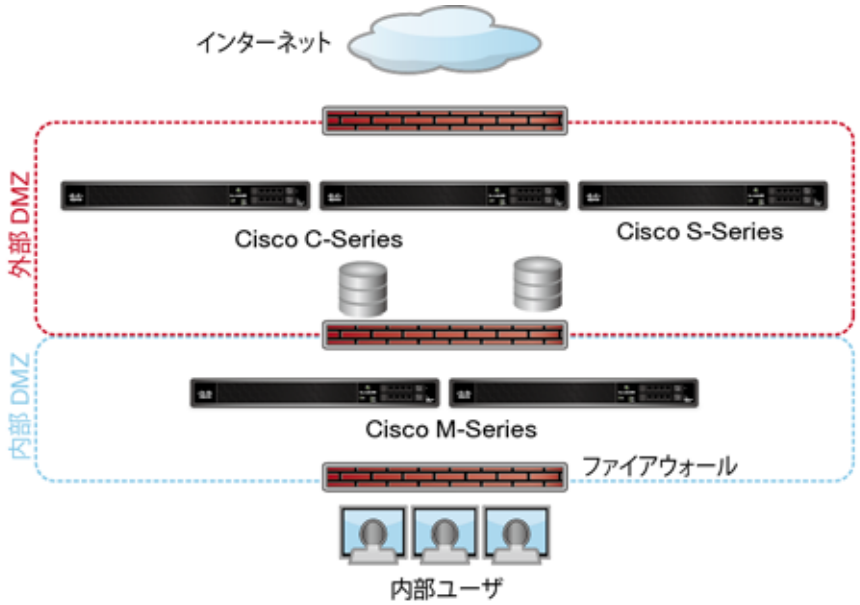


図 2-1 に、セキュリティ管理アプライアンスと複数の DMZ を含む一般的なネットワーク設定を示します。内部ネットワークで、DMZ の外側に セキュリティ管理アプライアンスを導入します。すべての接続は、セキュリティ管理アプライアンス（M シリーズ）から開始され、管理 電子メール セキュリティ アプライアンス（C シリーズ）および管理 Web セキュリティ アプライアンス（S シリーズ）で終わります。

企業データセンターは セキュリティ管理アプライアンスを共有し、複数の Web セキュリティ アプライアンスおよび 電子メール セキュリティ アプライアンスの中央集中型レポーティングおよびメッセージ トラッキング、および複数の Web セキュリティ アプライアンスの中央集中型ポリシー設定を実行できます。また、セキュリティ管理アプライアンスは外部スパム隔離として使用されます。

電子メール セキュリティ アプライアンスおよび Web セキュリティ アプライアンスを セキュリティ管理アプライアンスに接続してすべてのアプライアンスを適切に設定した後、AsyncOS は管理対象アプライアンスからデータを収集して集約します。集約されたデータからレポートを作成できます。また、電子メールの全体像と Web の使用状況を判断できます。

セキュリティ管理アプライアンスと電子メール セキュリティ アプライアンスの統合について

セキュリティ管理アプライアンスと電子メール セキュリティ アプライアンスの統合の詳細については、ユーザ ドキュメントの「Cisco Content Security Management Appliance」の章または使用している電子メール セキュリティ アプライアンスのオンライン ヘルプを参照してください。

集中管理型の電子メール セキュリティ アプライアンスの展開

セキュリティ管理アプライアンスをクラスタに配置することはできません。ただし、クラスタ化された電子メール セキュリティ アプライアンスは、中央集中型レポーティングとトラッキングのためにセキュリティ管理アプライアンスにメッセージを配信し、外部スパム隔離にメッセージを保存できます。

セットアップの準備

システム セットアップ ウィザードを実行する前に、次の手順を実行してください。

ステップ 1　製品の最新リリース ノートを確認します。「マニュアル」（P.1-4）を参照してください。

ステップ 2　セキュリティ ソリューションのコンポーネントに互換性があることを確認します。「SMA 互換性マトリクス」（P.2-2）を参照してください。

ステップ 3　この導入に対応できるネットワークと物理的空間の準備があることを確認します。「設置計画」（P.2-2）を参照してください。

ステップ 4　セキュリティ管理アプライアンスを物理的に設定し、接続します。「アプライアンスの物理的なセットアップと接続」（P.2-4）を参照してください。

ステップ 5　ネットワーク アドレスと IP アドレスの割り当てを決定します。「ネットワーク アドレスと IP アドレスの割り当ての決定」（P.2-4）を参照してください。

ステップ 6　システム セットアップに関する情報を収集します。「セットアップ情報の収集」（P.2-5）を参照してください。

アプライアンスの物理的なセットアップと接続

この章の手順を続行する前に、アプライアンスに付属するクイック スタート ガイドに記載された手順を実行してください。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。

GUI にログインするには、PC と セキュリティ管理アプライアンスの間にプライベート接続を設定する必要があります。たとえば、付属するクロス ケーブルを使用して、アプライアンスの管理ポートからラップトップに直接接続できます。任意で、PC とネットワーク間、およびネットワークとセキュリティ管理アプライアンスの管理ポート間をイーサネット接続（イーサネット ハブなど）で接続できます。

ネットワーク アドレスと IP アドレスの割り当ての決定

（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、コンテンツ セキュリティ 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。各アプライアンスの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。

設定後に、メイン セキュリティ管理アプライアンスの [管理アプライアンス（Management Appliance）] > [ネットワーク（Network）] > [IP インターフェイス（IP Interfaces）] ページに移動し、セキュリティ管理アプライアンスが使用するインターフェイスを変更します。

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

- IP アドレス
- ネットマスク

さらに、ネットワーク全体に関する次の情報も必要になります。

- ネットワークのデフォルト ルータ（ゲートウェイ）の IP アドレス

- DNS サーバの IP アドレスおよびホスト名（インターネット ルート サーバを使用する場合は不要）
- NTP サーバのホスト名または IP アドレス（システム時刻を手動で設定する場合は不要）

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

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

（注）　電子メール セキュリティ アプライアンスとの間で電子メール メッセージを送受信するには、常にセキュリティ管理アプライアンスで同じ IP アドレスを使用してください。説明については、使用している電子メール セキュリティ アプライアンスのマニュアルにあるメール フローに関する情報を参照してください。

セットアップ情報の収集

次の表を使用して、システム セットアップの情報を収集してください。システム セットアップ ウィザードを実行するときに、この情報を手元に用意する必要があります。

（注）　ネットワークおよび IP アドレスの詳細については、付録 B「ネットワークと IP アドレスの割り当て」を参照してください。

表 2-1　システム セットアップ ワークシート

1	通知		システム アラートが送信される電子メール アドレス：
2	システム時刻		NTP サーバ（IP アドレスまたはホスト名）：
3	admin パスワード		「admin」アカウントの新しいパスワードを選択：
4	AutoSupport		Cisco IronPort AutoSupport をイネーブルにするかどうか。 ___ はい ___ いいえ
5	ホスト名		セキュリティ管理アプライアンスの完全修飾ホスト名：
6	インターフェイス/IP アドレス		IP アドレス：
			ネットマスク：
7	ネットワーク	ゲートウェイ	デフォルト ゲートウェイ（ルータ）の IP アドレス：
		DNS	___ インターネットのルート DNS サーバを使用
			___ これらの DNS サーバを使用

セキュリティ管理アプライアンスへのアクセス

セキュリティ管理アプライアンスには、標準の Web ベース グラフィカル ユーザ インターフェイス、スパム隔離を管理するための別個の Web ベース インターフェイス、コマンドライン インターフェイス、および特定の機能へのアクセス権が付与された管理ユーザ用の特別な、または制限付きの Web ベース インターフェイスがあります。

ブラウザ要件

GUI 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、受け入れるよう設定されている必要があり、さらに、Cascading Style Sheet（CSS）を含む HTML ページを描画できる必要があります。

表 2-2　サポートされるブラウザおよびリリース

ブラウザ	Windows XP	Windows 7	MacOS 10.6
Safari	—	—	5.1
Google Chrome	最新の安定リリース	—	—

ブラウザ	Windows XP	Windows 7	MacOS 10.6
Microsoft Internet Explorer	7.0、8.0	8.0、9.0	—
Mozilla Firefox	最新の安定リリース	最新の安定リリース	最新の安定リリース

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

Web インターフェイスへのアクセス

手順

ステップ 1　Web ブラウザを開き、IP アドレス テキスト フィールドに **192.168.42.42** と入力します。

ステップ 2　次のデフォルト値を入力します。

- ユーザ名：**admin**
- パスワード：**ironport**

Web インターフェイスへのアクセスについて

セキュリティ管理アプライアンスには、デフォルトではポート 80 で使用可能な標準管理者インターフェイスと、デフォルトではポート 82 で使用可能な Cisco IronPort スパム隔離エンド ユーザ インターフェイスの、2 つの Web インターフェイスがあります。イネーブルにすると、Cisco IronPort スパム隔離 HTTPS インターフェイスは、デフォルトでポート 83 に設定されます。

各 Web インターフェイスを設定する際に HTTP または HTTPS を指定できるため（セキュリティ管理アプライアンス上で [管理アプライアンス（Management Appliance）] > [ネットワーク（Network）] > [IP インターフェイス（IP Interfaces）] に移動）、セッション中にそれらを切り替える場合は、再認証を要求される場合があります。たとえば、ポート 80 の HTTP を介して admin Web インターフェイスにアクセスし、同じブラウザでポート 83 の HTTPS を介して Cisco IronPort Spam Quarantine エンド ユーザ Web インターフェイスにアクセスした場合、admin Web インターフェイスに戻るときに再認証を要求されます。

（注）　GUI へのアクセス時には、複数のブラウザ ウィンドウまたはタブを同時に使用して、セキュリティ管理アプライアンスに変更を行わないように注意してください。GUI セッションと CLI セッションを同時に使用しないてください。同時に使用すると、予期しない動作が発生し、サポート対象外になります。

（注）　デフォルトでは、30 分以上アイドル状態になっている場合、またはログアウトせずにブラウザを閉じた場合は、セッションがタイムアウトします。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。タイムアウト制限を変更するには、「Web UI セッション タイムアウトの設定」（P.13-23）を参照してください。

セキュリティ管理アプライアンスのコマンドライン インターフェイスへのアクセス

このコマンドライン インターフェイス（CLI）には、すべてのシスコ コンテンツ セキュリティ アプライアンス上での CLI アクセスと同じ方法でセキュリティ管理アプライアンスにアクセスします。ただし、次のような違いがあります。

- システム セットアップは、GUI を使用して実行する*必要があります*。
- セキュリティ管理アプライアンスでは、一部の CLI コマンドを使用できません。サポートされていないコマンドの一覧については、*『Cisco IronPort AsyncOS CLI Reference Guide』*を参照してください。

実動環境では、CLI にアクセスするために、SSH を使用する必要があります。ポート 22 でアプライアンスにアクセスするために、標準 SSH クライアントを使用します。ラボ展開の場合、Telnet も使用できますが、このプロトコルは暗号化されません。

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（繁体字および簡体字）
- ロシア語

GUI とデフォルトのレポーティング言語を選択するには、次のいずれかを実行してください。

- 言語を設定します。「プリファレンスの 設定」（P.14-58）を参照してください。
- GUI ウィンドウの右上にある [オプション（Options）] メニューを使用して、セッションの言語を選択します。

（有効な方法は、ログイン資格情報の認証に使用する方法によって異なります）。

システム セットアップ ウィザードの実行

AsyncOS には、システム設定を実行するための、ブラウザベースのシステム セットアップ ウィザードが用意されています。後で、ウィザードでは使用できないカスタム設定オプションを利用する場合があります。ただし、初期セットアップではウィザードを使用して、設定に漏れがないようにする*必要があります*。

セキュリティ管理アプライアンスでは、GUI を使用する場合のみ、このウィザードがサポートされます。コマンドライン インターフェイス（CLI）によるシステム セットアップはサポートされません。

はじめる前に

「セットアップの準備」（P.2-4）のすべてのタスクを実行します。

警告　**システム セットアップ ウィザードを使用すると、アプライアンスが完全に再設定されます。アプライアンスを最初に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、このウィザードを使用してください。**

セキュリティ管理アプライアンスが、管理ポートからネットワークに接続されていることを確認します。

警告　**セキュリティ管理アプライアンスは、管理ポートにデフォルトの IP アドレス 192.168.42.42 が設定された状態で出荷されます。セキュリティ管理アプライアンスをネットワークに接続する前に、他の装置の IP アドレスが、このエ場出荷時のデフォルト設定と競合していないことを確認してください。**

（注）　デフォルトでは、30 分以上アイドル状態になっている場合、またはログアウトせずにブラウザを閉じた場合は、セッションがタイムアウトします。システム セットアップ ウィザードを実行中にセッションがタイムアウトした場合は、最初からやり直す必要があります。

セッション タイムアウト制限を変更するには、「Web UI セッション タイムアウトの設定」（P.13-23）を参照してください。

（注）　デフォルトでは、30 分以上アイドル状態になっている場合、またはログアウトせずにブラウザを閉じた場合は、セッションがタイムアウトします。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。システム セットアップ ウィザードを実行中にセッションがタイムアウトした場合は、最初からやり直す必要があります。タイムアウト制限を変更するには、「Web UI セッション タイムアウトの設定」（P.13-23）を参照してください。

システム セットアップ ウィザードの概要

手順

ステップ 1　エンド ユーザ ライセンス契約書の確認

ステップ 2　次に示すシステム設定の実行：

- 通知設定と AutoSupport
- システム時刻設定
- admin パスワード

ステップ 3　次に示すネットワーク設定の実行：

- アプライアンスのホスト名
- アプライアンスの IP アドレス、ネットワーク マスク、およびゲートウェイ

- デフォルト ルータと DNS 設定

ステップ 4　設定の確認

ウィザードの各ページを実行し、ステップ 4 で設定を慎重に確認します。[前へ（Previous）] をクリックすると、前の手順に戻ることができます。プロセスの最後に、変更を確定するようウィザードのプロンプトが表示されます。確定するまで、大部分の変更は有効になりません。

システム セットアップ ウィザードの起動

ウィザードを起動するには、「Web インターフェイスへのアクセス」（P.2-7）の説明に従って GUI にログインします。GUI に初めてログインすると、デフォルトでは、システム セットアップ ウィザードの最初のページが表示されます。また、[システム管理（System Administration）] メニューからシステム セットアップ ウィザードにアクセスすることもできます（[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [システム セットアップ ウィザード（System Setup Wizard）]）。

エンド ユーザ ライセンス契約書の確認

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

システムの設定

システム アラート用の電子メール アドレスの入力

ユーザの介入を必要とするシステム エラーが発生した場合、AsyncOS では、電子メールでアラート メッセージが送信されます。アラートの送信先となる電子メール アドレス（複数可）を入力します。

システム アラート用の電子メール アドレスを 1 つ以上追加する必要があります。複数のアドレスを指定する場合は、カンマで区切ります。入力した電子メール アドレスでは、当初、すべてのレベルのすべてのタイプのアラートが受信されます。アラート設定は、後からカスタマイズできます。詳細については、「アラートの管理」（P.14-33）を参照してください。

時間の設定

セキュリティ管理アプライアンス上の時間帯を設定して、メッセージ ヘッダーおよびログ ファイルのタイムスタンプが正確になるようにします。ドロップダウン メニューを使用して時間帯を見つけるか、GMT オフセットによって時間帯を定義します。

システム クロック時刻は、手動で設定するか、ネットワーク タイム プロトコル（NTP）サーバを使用してネットワーク上またはインターネット上の他のサーバと時刻を同期することもできます。デフォルトでは、Cisco NTP サーバ（time.sco.cisco.com）がコンテンツ セキュリティ アプライアンスで時刻を同期するためにエントリとして追加されました。NTP サーバのホスト名を入力し、[エントリを追加（Add Entry）] をクリックして追加の NTP サーバを設定します。詳細については、「システム時刻の設定」（P.14-46）を参照してください。

（注）　レポートのデータを収集すると、セキュリティ管理アプライアンスによってデータにタイム スタンプが適用されます。タイム スタンプは、「システム時刻の設定」（P.14-46）の手順で実装された設定を使用して適用されます。
セキュリティ管理アプライアンスがデータを収集する方法の詳細については、「セキュリティ アプライアンスによるレポート用データの収集方法」（P.3-2）を参照してください。

パスワードの設定

AsyncOS の admin アカウントのパスワードを変更する必要があります。新しいパスワードは 6 文字以上の長さである必要があります。パスワードは安全な場所に保管してください。パスワードの変更はすぐに有効になります。

（注）　パスワードの再設定後にシステム設定を取り消しても、パスワードの変更は元に戻りません。

AutoSupport のイネーブル化

Cisco IronPort AutoSupport 機能（デフォルトで有効）で、セキュリティ管理アプライアンスに関する問題をカスタマー サポートに通知することにより、最適なサポートを提供できます。詳細については、「Cisco IronPort オートサポート」（P.14-37）を参照してください。

ネットワークの設定

マシンのホスト名を定義し、ゲートウェイと DNS 設定値を設定します。

（注）　セキュリティ管理アプライアンスが、管理ポートを通してネットワークに接続されていることを確認します。

ネットワーク設定

セキュリティ管理アプライアンスの完全修飾ホスト名を入力します。この名前は、ネットワーク管理者が割り当てる必要があります。

セキュリティ管理アプライアンスの IP アドレスを入力します。

ネットワーク上のデフォルト ルータ（ゲートウェイ）のネットワーク マスクと IP アドレスを入力します。

次に、Domain Name Service（DNS）設定値を設定します。AsyncOS には、インターネットのルート サーバに直接問い合わせできる、高性能な内部 DNS リゾルバ/キャッシュが組み込まれていますが、指定した DNS サーバを使用することもできます。独自のサーバを使用する場合は、各 DNS サーバの IP アドレスを指定する必要があります。システム セットアップ ウィザードを使用して入力できる DNS サーバは、4 台までです。

（注）　指定した DNS サーバの初期プライオリティは 0 です。詳細については、「ドメイン ネーム システムの設定」（P.14-42）を参照してください。

（注）　アプライアンスでは、着信接続のための DNS ルックアップを実行するために、稼働中の DNS サーバへのアクセスが必要です。アプライアンスをセットアップするときに、アプライアンスからアクセス可能な稼働中の DNS サーバを指定できない場合は、[Use Internet Root DNS Servers] を選択するか、管理インターフェイスの IP アドレスを一時的に指定することによってシステム セットアップ ウィザードを完了できます。

設定の確認

これで、入力した設定情報の要約がシステム セットアップ ウィザードに表示されます。変更する必要がある場合は、ページの下部にある [前へ（Previous）] をクリックし、情報を編集します。

情報を確認した後、[この設定をインストール（Install This Configuration）] をクリックします。次に、表示される確認ダイアログ ボックスで [インストール（Install）] をクリックします。

次の手順

システム セットアップ ウィザードによって セキュリティ管理アプライアンスに設定が正しくインストールされると、[システム セットアップの次のステップ（System Setup Next Steps）] ページが表示されます。

[システム セットアップの次のステップ（System Setup Next Steps）] ページのいずれかのリンクをクリックして、シスコ コンテンツ セキュリティ アプライアンスの設定を続行します。

セキュリティ管理アプライアンスをインストールし、システム セットアップ ウィザードを実行した後、アプライアンス上の他の設定を修正して、モニタリング サービスを設定できます。

設定およびトラブルシューティングを容易にするために、「ソリューション導入の概要」（P.2-1）で説明するプロセスに従うことを推奨します。

管理対象アプライアンスの追加について

各アプライアンスに対して最初の中央集中型サービスを設定するときに、管理対象の電子メール Web セキュリティ アプライアンスをセキュリティ管理アプライアンスに追加します。

サポートされている電子メールおよび Web セキュリティ アプライアンスは、「SMA 互換性マトリクス」（P.2-2）に記載されています。

リモート アプライアンスを追加すると、セキュリティ管理アプライアンスによって、リモート アプライアンスの製品名と追加するアプライアンスのタイプが比較されます。たとえば、[Web セキュリティ アプライアンスの追加（Add Web セキュリティ アプライアンス）] ページを使用してアプライアンスを追加すると、そのアプライアンスは Web セキュリティ アプライアンスであって 電子メール セキュリティ アプライアンスではないことを確認するために、セキュリティ管理アプライアンスによってリモート アプライアンスの製品名がチェックされます。また、セキュリティ管理アプライアンスは、リモート アプライアンス上のモニタリング サービスをチェックして、それらが正しく設定され、互換性があることを確認します。

[セキュリティ アプライアンス（Security Appliances）] ページには、追加した管理対象アプライアンスが表示されます。接続が確立されていますか？（Connection Established?）カラムは、モニタリング サービスの接続が適切に設定されているかどうかを示します。

管理対象アプライアンスの追加方法は、次の手順に含まれています。

- 「管理対象の各電子メール セキュリティ アプライアンスへの中央集中型電子メール レポーティング サービスの追加」（P.4-3）

- 「管理対象の各電子メール セキュリティ アプライアンスへの中央集中型メッセージ トラッキング サービスの追加」（P.6-3）
- 「管理対象の各電子メール セキュリティ アプライアンスへの中央集中型スパム隔離サービスの追加」（P.7-7）
- 「管理対象の各電子メール セキュリティ アプライアンスへの集約ポリシー、ウイルス、アウトブレイク隔離サービスの追加」（P.8-5）
- 「管理対象の各 Web セキュリティ アプライアンスへの中央集中型 Web レポーティング サービスの追加」（P.5-4）
- 「Web セキュリティ アプライアンスの追加と Configuration Master のバージョンとの関連付け」（P.9-5）

管理対象アプライアンス設定の編集

手順

ステップ 1　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [セキュリティ アプライアンス（Security Appliances）] を選択します。

ステップ 2　[セキュリティ アプライアンス（Security Appliance）] セクションで、編集するアプライアンスの名前をクリックします。

ステップ 3　アプライアンスの設定に必要な変更を行います。

たとえば、モニタリング サービスのチェックボックスをオンまたはオフにする、ファイル転送アクセスを再設定する、または IP アドレスを変更する、などの変更を行います。

（注）　管理対象アプライアンスの IP アドレスを変更すると、さまざまな問題が発生する可能性があります。Web セキュリティ アプライアンスの IP アドレスを変更すると、アプライアンスの公開履歴が失われ、スケジュールされた公開ジョブに対して Web セキュリティ アプライアンスが現在選択されていると、公開エラーが発生します。（割り当てられたすべてのアプライアンスを使用するように設定されたスケジュール済み公開ジョブは、影響を受けません）。電子メール セキュリティ アプライアンスの IP アドレスを変更すると、アプライアンスのトラッキング アベイラビリティ データが失われます。

ステップ 4　[送信（Submit）] をクリックして、ページ上の変更を送信し、[変更を確定（Commit Changes）] をクリックして変更を保存します。

管理対象アプライアンスのリストからのアプライアンスの削除

はじめる前に

リモート アプライアンスをセキュリティ管理アプライアンスから削除する前にそのアプライアンスで有効なすべての集約管理サービスを無効にする必要があります。たとえば、集約ポリシー、ウイルス、アウトブレイク隔離サービスが有効な場合、電子メール セキュリティ アプライアンスでまずそのサービスを無効にする必要があります。電子メールまたはネットワークのセキュリティ アプライアンスのマニュアルを参照してください。

手順

ステップ 1　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [セキュリティ アプライアンス（Security Appliances）] を選択します。

ステップ 2　[セキュリティ アプライアンス（Security Appliances）] セクションで、削除する管理対象アプライアンスの行にあるゴミ箱アイコンをクリックします。

ステップ 3　確認のダイアログボックスで [削除（Delete）] をクリックします。

ステップ 4　変更を送信し、保存します。

セキュリティ管理アプライアンスでのサービスの設定

電子メール セキュリティ サービス：

- 第 4 章「中央集中型電子メール セキュリティ レポーティングの使用」
- 第 6 章「電子メール メッセージのトラッキング」
- 第 7 章「Cisco IronPort スパム隔離の管理」
- 第 8 章「集約ポリシー、ウイルス、およびアウトブレイク隔離」

Web セキュリティ サービス：

- 第 5 章「中央集中型 Web レポーティングおよびトラッキングの使用」
- 第 9 章「Web セキュリティ アプライアンスの管理」

設定変更のコミットおよび破棄

シスコ コンテンツ セキュリティ アプライアンス GUI で設定を変更した後、ほとんどの場合、変更を明示的にコミットする必要があります。

図 2-2　[変更を確定（Commit Changes）] ボタン

目的	操作内容
すべての保留中の変更をコミットする	ウィンドウの右上にあるオレンジ色の [変更を確定（Commit Changes）] ボタンをクリックします。変更内容の説明を追加し、[確定する（Commit）] をクリックします。 コミットが必要な変更を実行していない場合、[変更を確定（Commit Changes）] の代わりにグレーの [未確定の処理なし（No Changes Pending）] ボタンが表示されます。
すべての保留中の変更を破棄する	ウィンドウの右上にあるオレンジ色の [変更を確定（Commit Changes）] ボタンをクリックし、[変更を破棄（Abandon Changes）] をクリックします。

関連項目

- 「以前コミットしたコンフィギュレーションへのロールバック」（P.14-52）

CHAPTER 3

レポートでの作業

特に明記されていない限り、この章の情報は、シスコのコンテンツ セキュリティ管理アプライアンスの電子メールおよび Web レポートの両方に適用されます。

レポーティング データを表示する方法

表 3-1　レポーティング データを表示する方法

目的	参照先
Web ベースのインタラクティブ レポート ページを表示およびカスタマイズする	• 「レポート データのビューのカスタマイズ」（P.3-3） • 第 4 章「中央集中型電子メール セキュリティ レポーティングの使用」 • 第 5 章「中央集中型 Web レポーティングおよびトラッキングの使用」
PDF レポートまたは CSV レポートを自動的に繰り返し生成する	• 「電子メール レポートのスケジュール設定」（P.4-56） • 「Web レポートのスケジュール設定」（P.5-67）
PDF レポートまたは CSV レポートをオンデマンドで生成する	• 「オンデマンドでの電子メール レポートの生成」（P.4-58） • 「オンデマンドでの Web レポートの生成」（P.5-71）

表 3-1　レポーティング データを表示する方法 （続き）

目的	参照先
raw データを CSV（カンマ区切り）ファイルとしてエクスポートする	• 「レポーティング データおよびトラッキング データの印刷およびエクスポート」（P.3-10） • 「カンマ区切り（CSV）ファイルとしてのレポート データのエクスポート」（P.3-11）
レポート データの PDF を生成する	「レポーティング データおよびトラッキング データの印刷およびエクスポート」（P.3-10）
レポート情報を自分自身や他のユーザに電子メールで送信する	• 「オンデマンドでの電子メール レポートの生成」（P.4-58） • 「電子メール レポートのスケジュール設定」（P.4-56） • 「オンデマンドでの Web レポートの生成」（P.5-71） • 「Web レポートのスケジュール設定」（P.5-67）
スケジュールされたレポートまたはオンデマンド レポートのアーカイブ済みのコピーを、システムから削除されるまで表示する	「アーカイブされた Web レポートの表示と管理」（P.5-72）
特定のトランザクションに関する情報を検索する	• 「レポートに含まれるメッセージやトランザクションの詳細の表示」（P.3-8）

（注）　ロギングとレポーティングの違いについては、「ロギングとレポーティング」（P.15-1）を参照してください。

セキュリティ アプライアンスによるレポート用データの収集方法

セキュリティ管理アプライアンスは、約 15 分ごとにすべての管理対象アプライアンスからすべてのレポートのデータをプルし、それらのアプライアンスのデータを集約します。使用するアプライアンスによっては、セキュリティ管理アプライアンスでレポーティング データに特定のメッセージを組み込むのに時間が掛かる場合があります。データの情報については、[システム ステータス（System Status）] ページを確認してください。

（注）　セキュリティ管理アプライアンスは、レポートのデータを収集する際に、セキュリティ管理アプライアンス上で時間設定を行った際に設定した情報からタイム スタンプを適用します。セキュリティ管理アプライアンス上の時間設定の詳細については、「システム時刻の設定」（P.14-46）を参照してください。

レポーティング データの保存方法

すべてのアプライアンスで、レポーティング データが保存されます。表 3-2 に、各アプライアンスがデータを保存する期間を示します。

表 3-2　電子メール アプライアンスと Web セキュリティ アプライアンスでのレポーティング データの保存

	毎分	毎時	毎日	毎週	毎月	毎年
ローカル レポート 電子メール セキュリティ アプライアンスまたは Web セキュリティ アプライアンス	•	•	•	•	•	
電子メール セキュリティ アプライアンスまたは Web セキュリティ アプライアンスでの中央集中型レポーティング	•	•	•	•		
セキュリティ管理アプライアンス		•	•	•	•	•

レポーティングおよびアップグレードについて

新しいレポーティング機能は、アップグレード前に実行されたトランザクションには適用できない場合があります。これは、これらのトランザクションについては、必須データが保持されていない場合があるためです。レポーティング データおよびアップグレードに関連する制限については、ご使用のリリースのリリース ノートを参照してください。

レポート データのビューのカスタマイズ

Web インターフェイスでレポート データを表示する場合、ビューをカスタマイズできます。

目的	操作内容
アプライアンスまたはレポート グループごとにデータを表示する	「アプライアンスまたはレポーティング グループのレポーティング データの表示」（P.3-4）を参照してください。
時間範囲を指定する	「レポートの時間範囲の選択」（P.3-4）を参照してください。
（Web レポートの場合）チャート化するデータを選択する	「（Web レポートのみ）チャート化するデータの選択」（P.3-5）を参照してください。
テーブルをカスタマイズする	「レポート ページのテーブルのカスタマイズ」（P.3-6）を参照してください。
表示する特定の情報またはデータのサブセットを検索する	• 電子メール レポートについては、「検索およびインタラクティブ電子メール レポート ページ」（P.4-6）を参照してください。 • Web レポートについては、ほとんどのテーブルの下方にある [検索（Find）] オプションまたは [フィルタ（Filter）] オプションを探してください。 • 一部のテーブルには、集約したデータの詳細へのリンク（青色のテキスト）が含まれます。
レポート関連の設定を指定する	「プリファレンスの 設定」（P.14-58）を参照してください。
使用したいチャートと表だけを使ったカスタム レポートを作成する	「カスタム レポート」（P.3-7）を参照してください。

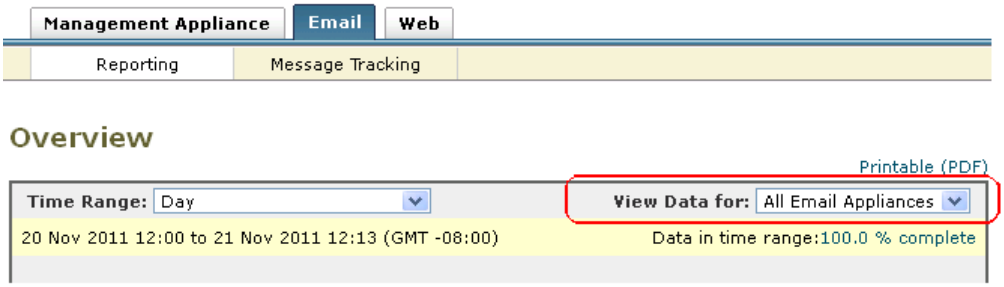
（注）　すべてのレポートにすべてのカスタマイズ機能を使用できるわけではありません。

アプライアンスまたはレポーティング グループのレポーティング データの表示

電子メールおよび Web の概要レポートについて、および電子メールのシステム キャパシティ レポートについては、すべてのアプライアンスから、または中央で管理されている 1 台のアプライアンスからデータを表示できます。

電子メール レポートでは、「電子メール レポート グループの作成」（P.4-4）の説明に従い電子メール セキュリティ アプライアンスのグループを作成した場合、各レポーティング グループのデータを表示できます。

ビューを指定するには、サポートされるページの [データ参照（View Data for）] リストからアプライアンスまたはグループを選択します。



最近、別のセキュリティ管理アプライアンスからのデータをバックアップしたセキュリティ管理アプライアンスでレポート データを表示する場合は、まず、[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [セキュリティ アプライアンス（Security Appliances）] で各アプライアンスを追加する必要があります（ただし、各アプライアンスとの接続は確立しないでください）。

レポートの時間範囲の選択

ほとんどの事前定義レポート ページでは、含まれるデータの時間範囲を選択できます。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 ページに対して使用されます。

使用可能な時間範囲オプションは、アプライアンスごとに異なり、またセキュリティ管理アプライアンス上の電子メール レポートおよび Web レポートによって異なります。

表 3-3　レポートの時間範囲オプション

オプション	説明	SMA 電子メール レポート	ESA	SMA Web レポート	WSA
時（Hour）	過去 60 分間と最大 5 分間の延長時間		•		•
日（Day）	過去 24 時間	•	•	•	•
週（Week）	当日の経過時間を含む、過去 7 日間	•	•	•	•
30 日（30 days）	当日の経過時間を含む、過去 30 日間	•	•	•	•
90 日（90 days）	当日の経過時間を含む、過去 90 日間	•	•	•	
年（Year）	過去 12 ヵ月と現在月の経過日数	•			
昨日（Yesterday）	アプライアンスで定義された時間帯を使用した、前日の 24 時間（00:00 ～ 23:59）	•	•	•	•
先月（Previous Calendar Month）	月の第 1 日目の 00:00 からその月の最終日の 23:59 まで	•	•	•	
カスタム範囲（Custom Range）	ユーザ指定の時間範囲。 開始日時と終了日時を選択する場合は、このオプションを選択します。	•	•	•	•

（注）　レポート ページの時間範囲は、グリニッジ標準時（GMT）オフセットで表示されます。たとえば、太平洋標準時は、GMT + 7 時間（GMT + 07:00）です。

（注）　すべてのレポートで、システム設定の時間帯に基づき、グリニッジ標準時（GMT）オフセットで日付および時刻情報が表示されます。ただし、データ エクスポートでは、世界の複数のタイム ゾーンの複数のシステムに対応するために、GMT で時刻が表示されます。

ヒント　ログインするたびに常に表示する、デフォルトの時間範囲を指定できます。詳細については、「プリファレンスの 設定」（P.14-58）を参照してください。

（Web レポートのみ）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と同じです。ただし、チャート化できないカラムもあります。カラムの見出しについては、「Web レポートのテーブル カラムの説明」（P.5-11）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。

手順

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 ページのテーブルのカスタマイズ

表 3-4　Web レポート ページのテーブルのカスタマイズ

目的	操作内容	追加情報
• 追加のカラムを表示する • 表示可能なカラムを非表示にする • テーブルに使用可能なカラムを判断する	テーブルの下の [列（Columns）] リンクをクリックし、表示するカラムを選択して、[完了（Done）] をクリックします。	ほとんどのテーブルでは、デフォルトで一部のカラムが非表示になります。 レポート ページごとに、異なるカラムが提供されます。 カラムの詳細については、次の項を参照してください。 • 「電子メール レポーティング ページのテーブル カラムの説明」（P.4-9） • 「Web レポートのテーブル カラムの説明」（P.5-11）
テーブル カラムの順序を変える	カラムの見出しを目的の位置までドラッグします。	—
選択した見出しでテーブルをソートする	カラムの見出しをクリックします。	—
表示するデータの行数を加減する	テーブルの右上にある [表示されたアイテム（Items Displayed）] ドロップダウン リストから、表示する行数を選択します。	Web レポートの場合、デフォルトの表示行数を設定することもできます。「プリファレンスの 設定」（P.14-58）を参照してください。
可能な場合は、テーブル エントリの詳細を表示する	テーブル内の青色のエントリをクリックします。	「レポートに含まれるメッセージやトランザクションの詳細の表示」（P.3-8）も参照してください。
データのプールを特定のサブセットに絞り込む	可能な場合は、テーブルの下のフィルタ設定で値を選択するか、入力します。	Web レポートの使用可能なフィルタについては、各レポート ページの説明に記載されています。「Web レポーティング ページについて」（P.5-7）を参照してください。

カスタム レポート

既存のレポートのページからチャート（グラフ）とテーブルを組み合わせてカスタム電子メール セキュリティ レポートのページおよびカスタム Web セキュリティ レポートのページを作成できます。

目的	操作内容
カスタム レポート ページへのモジュールの追加	**1.** [メール（Email）] または [Web] > [レポート（Reporting）] > [マイ レポート（My Reports）] に移動し、必要としないサンプル モジュールの右上隅の [X] をクリックしてそのモジュールを削除します。 **2.** 次のいずれかを実行します。 – カスタム レポートにモジュールを追加するには、[メール（Email）] タブまたは [Web] タブのレポート ページ内のモジュール上の [+ マイ レポート（+My Reports）] ボタンをクリックします。 – [メール（Email）] または [Web] > [レポート（Reporting）] > [マイ レポート（My Reports）] に移動し、[+ モジュール レポート（+ Report Module）] ボタンをクリックし、次に追加するレポート モジュールを選択します。 **3.** モジュールがデフォルト設定に追加されます。カスタマイズした（たとえば、列を追加、削除、または並べ替えしたり、チャートのデフォルト以外のデータを表示したりして）モジュールを追加する場合は、これらのモジュールを追加した後、再度カスタマイズします。元のモジュールの時間範囲は保持されません。 **4.** 別の凡例を含むチャートを追加する場合（たとえば、([概要（Overview）] ページからのグラフ）は、凡例を別に追加します。必要に応じて、凡例で説明しているデータの側の位置にドラッグ アンド ドロップします。 （注） • レポート ページやモジュールによっては上記の方法の 1 つのみが使用可能なものもあります。1 つの方法を使用してモジュールを追加できない場合は、他の方法を試してください。 • カスタム レポートに次のモジュールは追加できません。 – [管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [システム ステータス（System Status）] ページのすべてのモジュール – [Web] > [レポート（Reporting）] > [使用可能なデータ（Data Availability）] のページのすべてのモジュール – [メール（Email）] > [レポート（Reporting）] > [有効なレポート データ（Reporting Data Availability）] ページ のすべてのモジュール – [メール（Email）] > [メッセージ トラッキング（Message Tracking）] > [有効なメッセージ トラッキング データ（Message Tracking Data Availability）] ページのすべてのモジュール – 送信者プロファイル詳細レポートのページからの、[SenderBase からの最新情報（Current Information from SenderBase）]、[送信者グループ情報（Sender Group Information）]、および [ネットワーク情報（Network Information）] といったドメイン単位のモジュール – [アウトブレイク フィルタ（Outbreak Filters）] レポート ページの [過去 1 年間のウイルス アウトブレイク サマリー（Past Year Virus Outbreak Summary）] チャートおよび、[過去 1 年間のウイルス アウトブレイク（Past Year Virus Outbreaks）] テーブル – すべてのレポートの検索結果 • 各モジュールを追加できるのは 1 回だけで、レポートにすでに特定のモジュールを追加している場合は、そのモジュールを追加するオプションが使用可能ではありません。

目的	操作内容
カスタム レポート ページの表示	1. [メール（Email）] または [Web] > [レポート（Reporting）] > [マイ レポート（My Reports）] を選択します。 2. すべてのレポートのページに選択された時間範囲が、[マイ レポート（My Reports）] ページのすべてのモジュールに適用されます。表示する時間範囲を選択します。 新しく追加されたモジュールはカスタム レポートの上部に表示されます。
カスタム レポート ページのモジュールの再配置	目的の場所にモジュールをドラッグ アンド ドロップします。
カスタム レポート ページからのモジュールの削除	モジュールの右上隅にある [X] をクリックします。

レポートに含まれるメッセージやトランザクションの詳細の表示

手順

ステップ 1　レポート ページのテーブルにある青色の番号をクリックします

（これらのリンクがあるのは、一部のテーブルのみです）。）

この数に含まれるメッセージまたはトランザクションは [メッセージ トラッキング（Message Tracking）] または [Web トラッキング（Web Tracking）] にそれぞれ表示されます。

ステップ 2　メッセージまたはトランザクションのリストを表示するには、スクロール ダウンします。

関連トピック

- 第 6 章「電子メール メッセージのトラッキング」
- 「Web トラッキング（Web Tracking）」（P.5-55）

電子メール レポートのパフォーマンスの向上

月内に固有のエントリが多数発生したことで、集約レポーティングのパフォーマンスが低下する場合は、レポーティング フィルタを使用して前年を対象としたレポート（[昨年（Last Year）] レポート）でのデータの集約を制限します。これらのフィルタにより、レポート内の詳細、個々の IP、ドメイン、またはユーザ データを制限できます。概要レポートおよびサマリー情報は、引き続きすべてのレポートで利用できます。

CLI で **reportingconfig -> filters** メニューを使用すると、1 つ以上のレポート フィルタをイネーブルにできます。変更を有効にするには、変更をコミットする必要があります。

- [IP 接続レベルの詳細（IP Connection Level Detail）]。このフィルタをイネーブルにすると、セキュリティ管理アプライアンスは、個々の IP アドレスに関する情報を記録しません。このフィルタは、攻撃による大量の受信 IP アドレスを処理するシステムに適しています。

  このフィルタは、次の [昨年（Last Year）] レポートに影響を与えます。

  - Sender Profile for Incoming Mail
  - IP Addresses for Incoming Mail
  - IP Addresses for Outgoing Senders
- [ユーザの詳細（User Detail）]。このフィルタをイネーブルにすると、セキュリティ管理アプライアンスは、電子メールを送受信する個々のユーザ、およびユーザの電子メールに適用されるコンテンツ フィルタに関する情報を記録しません。このフィルタは、何百万もの内部ユーザの電子メールを処理するアプライアンス、またはシステムが受信者のアドレスを検証しない場合に適しています。

  このフィルタは、次の [昨年（Last Year）] レポートに影響を与えます。
  - Internal Users
  - Internal User Details
  - IP Addresses for Outgoing Senders
  - Content Filters
- [メール トラフィックの詳細（Mail Traffic Detail）]。このフィルタをイネーブルにすると、セキュリティ管理アプライアンスは、アプライアンスがモニタする個々のドメインおよびネットワークに関する情報を記録しません。このフィルタは、有効な着信または発信ドメインの数が数千万の単位で測定される場合に適しています。

  このフィルタは、次の [昨年（Last Year）] レポートに影響を与えます。
  - Domains for Incoming Mail
  - Sender Profile for Incoming Mail
  - Internal User Details
  - Domains for Outgoing Senders

（注） 過去 1 時間の最新のレポート データを表示するには、個々のアプライアンスにログインして、そこでデータを表示する必要があります。

レポーティング データおよびトラッキング データの印刷およびエクスポート

表 3-5　レポート データの印刷とエクスポート

取得対象	PDF	CSV	操作内容	コメント
インタラクティブ レポート ページの PDF	•		インタラクティブ レポート ページの右上にある [印刷可能（PDF）（Printable (PDF)）] リンクをクリックします。	PDF には、現在表示しているカスタマイゼーションが反映されます。 PDF は、プリンタ対応の形式に設定されます。
レポート データの PDF	•		スケジュール設定されたレポートまたはオンデマンドのレポートを作成します。次の各項を参照してください。 • 「オンデマンドでの電子メール レポートの生成」（P.4-58） • 「電子メール レポートのスケジュール設定」（P.4-56） • 「オンデマンドでの Web レポートの生成」（P.5-71） • 「Web レポートのスケジュール設定」（P.5-67）	—
raw データ 「カンマ区切り（CSV）ファイルとしてのレポート データのエクスポート」（P.3-11）も参照してください。		•	チャートまたはテーブルの下にある [エクスポート（Export）] リンクをクリックします。	CSV ファイルには、チャートや表で見ることのできるデータだけでなく、すべての適用可能なデータが含まれます。
		•	スケジュール設定されたレポートまたはオンデマンドのレポートを作成します。次の各項を参照してください。 • 「オンデマンドでの電子メール レポートの生成」（P.4-58） • 「電子メール レポートのスケジュール設定」（P.4-56） • 「オンデマンドでの Web レポートの生成」（P.5-71） • 「Web レポートのスケジュール設定」（P.5-67）	各 CSV ファイルには、最大 100 行を含めることができます。 レポートに複数のテーブルが含まれる場合、各テーブルに対して別個の CSV ファイルが作成されます。 一部の拡張レポートは、CSV 形式で使用できません。

表 3-5　レポート データの印刷とエクスポート（続き）

取得対象	PDF	CSV	操作内容	コメント
さまざまな言語によるレポート	•		レポートをスケジュール設定するか、オンデマンドで作成するときは、必要なレポート言語を選択します。	Windows コンピュータ上で中国語、日本語、または韓国語で PDF を生成するには、該当するフォント パックを Adobe.com からダウンロードして、ローカル コンピュータにインストールする必要があります。
（Web セキュリティ）レポート データのカスタム サブセット（特定のユーザ用のデータなど）。	•	•	[Web トラッキング（Web Tracking）] で検索を実行し、[Web トラッキング（Web Tracking）] ページの [印刷可能なダウンロード（Printable Download）] リンクをクリックします。PDF 形式または CSV 形式を選択します。	PDF には、Web ページのすべての情報が含まれていない場合があります。具体的には、PDF ファイルには以下が含まれます。 • 最大 1,000 のトランザクション。 • 詳細を表示する場合、関連する 100 のトランザクション • 関連トランザクションごとに最大 3000 文字。 CSV ファイルには、検索条件に一致するすべての raw データが含まれます。
（電子メール セキュリティ）データのカスタム サブセット（特定のユーザ用のデータなど）。		•	[メッセージ トラッキング（Message Tracking）] で検索を実行し、検索結果の上にある [エクスポート（Export）] リンクまたは [すべてをエクスポート（Export All）] リンクをクリックします。	[エクスポート（Export）] リンクでは、表示された検索結果を使用して検索基準で指定された制限まで CSV ファイルをダウンロードします。 [すべてをエクスポート（Export All）] リンクでは、検索条件に一致する最大 50,000 件のメッセージを含む CSV ファイルをダウンロードします。 ヒント：50,000 件以上のメッセージをエクスポートする必要がある場合は、短い時間範囲のエクスポートのセットを実行します。

カンマ区切り（CSV）ファイルとしてのレポート データのエクスポート

raw データをカンマ区切り（CSV）ファイルにエクスポートし、Microsoft Excel などのデータベース アプリケーションを使用してアクセスおよび処理できます。データをエクスポートするその他の方法については、「レポーティング データおよびトラッキング データの印刷およびエクスポート」（P.3-10）を参照してください。

CSV エクスポートには raw データのみ含まれるため、Web ベースのレポート ページからエクスポートされたデータには、パーセンテージなどの計算データが含まれていない場合があります（そのデータが Web ベースのレポートで表示された場合でも、含まれていない場合があります）。

電子メール メッセージ トラッキングおよびレポーティング データについては、セキュリティ管理アプライアンスに設定されている内容に関係なく、エクスポートした CSV データはすべて GMT で表示されます。これにより、特に複数のタイム ゾーンのアプライアンスからデータを参照する場合に、アプライアンスとは関係なくデータを使用することが容易になります。

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 3-6　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。

ローカライズされた CSV データをエクスポートすると、ブラウザによっては見出しが正しく表示されない場合があります。これは、ブラウザによっては、ローカライズされたテキストに対して適切な文字セットが使用されない場合があることから発生します。この問題の回避策としては、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。

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。

電子メール レポートおよび Web レポート

電子メール レポートに固有の情報については、第 4 章「中央集中型電子メール セキュリティ レポーティングの使用」を参照してください。

Web レポートに固有の情報については、第 5 章「中央集中型 Web レポーティングおよびトラッキングの使用」を参照してください。

CHAPTER 4

中央集中型電子メール セキュリティ レポーティングの使用

中央集中型電子メール レポーティングの概要

シスコのコンテンツ セキュリティ管理アプライアンスは、電子メールのトラフィック パターンおよびセキュリティ リスクを監視できるように、個別または複数の電子メール セキュリティ アプライアンスからの集計情報を示します。リアルタイムでレポートを実行して、特定の期間のシステム アクティビティをインタラクティブに表示することも、レポートをスケジュール設定して、定期的に実行することもできます。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。

この機能により、電子メール セキュリティ アプライアンスの [モニタ（Monitor）] メニューの下にリストされるレポートが集中管理されます。

中央集中型電子メール レポーティング機能は、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。

中央集中型トラッキング機能は、複数の電子メール セキュリティ アプライアンスを通過する電子メール メッセージの追跡を可能にします。

（注） 電子メール セキュリティ アプライアンスでデータが保存されるのは、ローカル レポーティングが使用される場合だけです。中央集中型レポーティングを電子メール セキュリティ アプライアンスに対してイネーブルにした場合、電子メール セキュリティ アプライアンスでは、システム キャパシティおよび

システム ステータス以外のレポーティング データは保持されません。中央集中型電子メール レポーティングがイネーブルでない場合、生成されるレポートはシステム ステータスとシステム キャパシティだけです。

中央集中型レポーティングへの移行中および移行後のレポート データの可用性の詳細についてはお使いの電子メール セキュリティ アプライアンスの「Centralized Reporting Mode」の項を参照してください。

中央集中型電子メール レポーティングの設定

中央集中型電子メール レポーティングを設定するには、次の手順を順序どおりに実行します。

- 「セキュリティ管理アプライアンスでの中央集中型電子メール レポーティングのイネーブル化」（P.4-2）
- 「管理対象の各電子メール セキュリティ アプライアンスへの中央集中型電子メール レポーティング サービスの追加」（P.4-3）
- 「電子メール レポート グループの作成」（P.4-4）
- 「電子メール セキュリティ アプライアンスでの中央集中型電子メール レポーティングのイネーブル化」（P.4-5）

（注）　レポーティングとトラッキングを常に同時にイネーブルにせず、レポーティングとトラッキングが適切に機能しない場合、または、レポーティングとトラッキングが各電子メール セキュリティ アプライアンスで常に同時に集中管理またはローカル保存されない場合、レポートからドリルダウンしたときのメッセージ トラッキングの結果は、予想した結果には一致しません。これは、各機能（レポーティング、トラッキング）のデータが、その機能がイネーブルになっている間にのみキャプチャされるためです。

セキュリティ管理アプライアンスでの中央集中型電子メール レポーティングのイネーブル化

はじめる前に

- 中央集中型レポーティングをイネーブルにする前に、すべての電子メール セキュリティ アプライアンスが設定され、想定どおりに動作している必要があります。
- 中央集中型電子メール レポーティングをイネーブルにする前に、十分なディスク領域がサービスに割り当てられていることを確認します。「ディスク使用量の管理」（P.14-56）を参照してください。

手順

ステップ 1　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [メール（Email）] > [集約管理レポート（Centralized Reporting）] を選択します。

ステップ 2　[有効（Enable）] をクリックします。

ステップ 3　システム セットアップ ウィザードを実行してから初めて中央集中型電子メール レポーティングをイネーブルにする場合は、エンドユーザ ライセンス契約書を確認し、[承認（Accept）] をクリックします。

ステップ 4　変更を送信し、保存します。

（注）　アプライアンスで電子メール レポーティングがイネーブルになっていて、この処理にディスク領域が割り当てられていない場合、ディスク領域が割り当てられるまで、中央集中型電子メール レポーティングが機能しません。電子メール レポーティングおよびトラッキングに設定するクォータが、現在使用しているディスク領域よりも大きい場合、レポーティングおよびトラッキングのデータは失われません。詳細については、「ディスク使用量の管理」（P.14-56）を参照してください。

管理対象の各電子メール セキュリティ アプライアンスへの中央集中型電子メール レポーティング サービスの追加

ここで実行する手順は、他の中央集中型管理機能の設定時に、すでにこのアプライアンスを追加したかどうかによって異なります。

手順

ステップ 1　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [セキュリティ アプライアンス（Security Appliances）] を選択します。

ステップ 2　このページのリストに、すでに電子メール セキュリティ アプライアンスを追加している場合は、次の手順を実行します。

a.　電子メール セキュリティ アプライアンスの名前をクリックします。

b.　[集約管理レポート（Centralized Reporting）] サービスを選択します。

ステップ 3　電子メール セキュリティ アプライアンスをまだ追加していない場合は、次の手順を実行します。

a.　[メール アプライアンスの追加（Add Email Appliance）] をクリックします。

b.　[アプライアンス名（Appliance Name）] および [IP アドレス（IP Address）] テキスト フィールドに、セキュリティ管理アプライアンスの管理インターフェイスのアプライアンス名と IP アドレスを入力します。

（注）　[IP アドレス（IP Address）] テキスト フィールドに DNS 名を入力した場合でも、[送信（Submit）] をクリックすると、すぐに IP アドレスに解決されます。

c.　[集約管理レポート（Centralized Reporting）] サービスが事前に選択されています。

d.　[接続の確立（Establish Connection）] をクリックします。

e.　管理対象となるアプライアンスの管理者アカウントのユーザ名とパスワードを入力し、[接続の確立（Establish Connection）] をクリックします。

（注）　ログイン資格情報を入力すると、セキュリティ管理アプライアンスからリモート アプライアンスへのファイル転送のための公開 SSH キーが渡されます。ログイン資格情報は、セキュリティ管理アプライアンスには保存されません。

f. [成功（Success）] メッセージがページのテーブルの上に表示されるまで待機します。

g. [テスト接続（Test Connection）] をクリックします。

h. テーブルの上のテスト結果を確認します。

ステップ 4　[送信（Submit）] をクリックします。

ステップ 5　中央集中型レポーティングをイネーブルにする各電子メール セキュリティ アプライアンスに対して、この手順を繰り返します。

ステップ 6　変更を保存します。

電子メール レポート グループの作成

セキュリティ管理アプライアンスからレポーティング データを表示する電子メール セキュリティ アプライアンスのグループを作成できます。

グループには 1 つ以上のアプライアンスを含めることができ、アプライアンスは複数のグループに所属できます。

はじめる前に

各アプライアンスで中央集中型レポーティングがイネーブルになっていることを確認します。「管理対象の各電子メール セキュリティ アプライアンスへの中央集中型電子メール レポーティング サービスの追加」（P.4-3）を参照してください。

手順

ステップ 1　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [集約管理レポート（Centralized Reporting）] を選択します。

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　グループの一意の名前を入力します。

電子メール セキュリティ アプライアンスで、セキュリティ管理アプライアンスに追加した 電子メール セキュリティ アプライアンスが表示されます。グループに追加するアプライアンスを選択します。

追加できるグループの最大数は、接続可能な電子メール アプライアンスの最大数以下です。

（注）　電子メール セキュリティ アプライアンスを セキュリティ管理アプライアンスに追加したが、リストに表示されない場合は、セキュリティ管理アプライアンスが電子メール セキュリティ アプライアンスからレポーティング データを収集するように、その 電子メール セキュリティ アプライアンスの設定を編集します。

ステップ 4　[追加（Add）] をクリックして、[グループ メンバー（Group Members）] リストにアプライアンスを追加します。

ステップ 5　変更を送信し、保存します。

電子メール セキュリティ アプライアンスでの中央集中型電子メール レポーティングのイネーブル化

管理対象の各電子メール セキュリティ アプライアンスで、中央集中型電子メール レポーティングをイネーブルにする必要があります。

手順については、お使いの電子メール セキュリティ アプライアンスに対するマニュアルの「Configuring an Email Security Appliance to Use Centralized Reporting」の項またはオンライン ヘルプを参照してください。

電子メール レポート データの操作

- レポート データのアクセスおよび表示に関するオプションついては、「レポーティング データを表示する方法」（P.3-1）を参照してください。
- レポート データのビューをカスタマイズする方法については、「レポート データのビューのカスタマイズ」（P.3-3）を参照してください。
- データ内の特定の情報を検索するには、「検索およびインタラクティブ電子メール レポート ページ」（P.4-6）を参照してください。
- レポート情報を印刷またはエクスポートするには、「レポーティング データおよびトラッキング データの印刷およびエクスポート」（P.3-10）を参照してください。
- さまざまなインタラクティブ レポート ページを理解するには、「[メール レポート（Email Reporting）] ページの概要」（P.4-7）を参照してください。
- レポートをオンデマンドで生成するには、「オンデマンドでの電子メール レポートの生成」（P.4-58）を参照してください。
- 指定した間隔および時刻に自動的に実行されるようにレポートをスケジュール設定するには、「電子メール レポートのスケジュール設定」（P.4-56）を参照してください。
- アーカイブしたオンデマンドのレポートおよびスケジュール設定したレポートを表示するには、「アーカイブ電子メール レポートの表示と管理」（P.4-60）を参照してください。
- バックグラウンド情報については、「セキュリティ アプライアンスによるレポート用データの収集方法」（P.3-2）を参照してください。
- 大量のデータを処理するときにパフォーマンスを向上させるには、「電子メール レポートのパフォーマンスの向上」（P.3-8）を参照してください。
- チャートまたはテーブル内に青色のリンクとして表示されるエンティティまたは番号に関する詳細を取得するには、エンティティまたは番号をクリックします。

  たとえば、そうすることを許可されている場合は、この機能を使用してコンテンツ フィルタリング、データ漏洩防止ポリシーに違反したメッセージの詳細を表示することができます。これは、メッセージ トラッキングで関連する検索を実行します。結果を表示するには、スクロール ダウンします。

検索およびインタラクティブ電子メール レポート ページ

インタラクティブ電子メール レポート ページの多くでは、ページの下部に [検索対象：（Search For:）] ドロップダウン メニューがあります。

ドロップダウン メニューから、次のような数種類の条件で検索できます。

- IP アドレス
- ドメイン
- ネットワーク オーナー
- 内部ユーザ
- 宛先ドメイン
- 内部送信者のドメイン
- 内部送信者の IP アドレス
- 着信 TLS ドメイン
- 発信 TLS ドメイン

多くの検索では、検索テキストに完全に一致させるか、入力したテキストで始まる項目を検索するか（たとえば、「ex」で始まる項目を検索する場合、「example.com」が一致します）を選択します。

IPv4 検索では、入力したテキストが最大で 4 IP オクテット（ドット付き 10 進表記）の先頭部として常に解釈されます。たとえば、「17」は 17.0.0.0 ～ 17.255.255.255 の範囲で検索されるので、17.0.0.1 は一致しますが、172.0.0.1 は一致しません。完全一致検索の場合は、4 つすべてのオクテットを入力します。IP アドレス検索は、クラスレス ドメイン間ルーティング（CIDR）形式（17.16.0.0/12）もサポートします。

IPv6 検索の場合、次の例の形式を使用して、アドレスを入力できます。

- 2001:db8:2004:4202::0-2001:db8:2004:4202::ff
- 2001:db8:2004:4202::
- 2001:db8:2004:4202::23
- 2001:db8:2004:4202::/64

[メール レポート（Email Reporting）] ページの概要

表 4-1　[メール レポート（Email Reporting）] タブのオプション

[メール レポート（Email Reporting）] メニュー	アクション
電子メール レポーティングの [概要（Overview）] ページ	[概要（Overview）] ページには、お使いの電子メール 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。これには、着信および発信メッセージに関するグラフやサマリー テーブルが含まれます。 詳細については、「電子メール レポーティングの [概要（Overview）] ページ」（P.4-11）を参照してください。
[受信メール（Incoming Mail）] ページ	[受信メール（Incoming Mail）] ページには、管理対象の 電子メール セキュリティ アプライアンスに接続されているすべてのリモート ホストのリアルタイム情報の、インタラクティブなレポートが表示されます。システムに電子メールを送信している IP アドレス、ドメイン、およびネットワーク オーナー（組織）の情報を収集できます。 詳細については、「[受信メール（Incoming Mail）] ページ」（P.4-16）を参照してください。
[送信先（Outgoing Destinations）] ページ	[送信先（Outgoing Destinations）] ページに、組織が電子メールを送信する宛先のドメインについての情報が表示されます。ページの上部には、発信脅威メッセージごとの上位の宛先、および発信クリーン メッセージ別の上位の宛先を示すグラフが表示されます。ページの下部には、総受信者数別にソートされた（デフォルト設定）カラムを示す表が表示されます。 詳細については、「[送信先（Outgoing Destinations）] ページ」（P.4-24）を参照してください。
[送信メッセージ送信者（Outgoing Senders）] ページ	[送信メッセージ送信者（Outgoing Senders）] ページには、ネットワーク内の IP アドレスおよびドメインから送信された電子メールの数と種類についての情報が表示されます。 詳細については、「[送信メッセージ送信者（Outgoing Senders）] ページ」（P.4-26）を参照してください。
[内部ユーザ（Internal Users）] ページ	[内部ユーザ（Internal Users）] には、*電子メール アドレスごと* に内部ユーザによって送受信された電子メールについての情報が表示されます。1 人のユーザが複数の電子メール アドレスを持っている場合があります。レポートでは、電子メール アドレスがまとめられません。 詳細については、「[内部ユーザ（Internal Users）] ページ」（P.4-28）を参照してください。
[DLP インシデント サマリー（DLP Incident Summary）] ページ	[DLP インシデントサマリー（DLP Incident Summary）] ページには、送信メールで発生したデータ漏洩防止（DLP）ポリシー違反インシデントに関する情報が示されます。 詳細については、「[DLP インシデント サマリー（DLP Incident Summary）] ページ」（P.4-31）を参照してください。

表 4-1　[メール レポート（Email Reporting）] タブのオプション （続き）

[メール レポート（Email Reporting）] メニュー	アクション
[コンテンツ フィルタ（Content Filters）] ページ	[コンテンツ フィルタ（Content Filters）] ページには、送受信コンテンツ フィルタの上位一致（最も多くのメッセージに一致したコンテンツ フィルタ）に関する情報が表示されます。このページでは、データが棒グラフとリストの形式でも表示されます。[コンテンツ フィルタ（Content Filters）] ページを使用すると、コンテンツ フィルタごとまたはユーザごとに企業ポリシーを確認できます。 詳細については、「[コンテンツ フィルタ（Content Filters）] ページ」（P.4-34）を参照してください。
[ウイルス タイプ（Virus Types）] ページ	[ウイルス タイプ（Virus Types）] ページでは、ネットワークで送受信されたウイルスの概要が示されます。[ウイルス タイプ（Virus Types）] ページには、電子メール セキュリティ アプライアンスで稼働し、セキュリティ管理アプライアンスに表示されるウイルス スキャン エンジンによって検出されたウイルスが表示されます。このレポートを使用して、特定のウイルスに対して処置を行います。 詳細については、「[ウイルス タイプ（Virus Types）] ページ」（P.4-35）を参照してください。
[TLS 接続（TLS Connections）] ページ	[TLS 接続（TLS Connections）] ページには、メールの送受信に使用される TLS 接続の全体的な使用状況が表示されます。このレポートでは、TLS 接続を使用してメールを送信する各ドメインの詳細についても示されます。 詳細については、「[TLS 接続（TLS Connections）] ページ」（P.4-37）を参照してください。
[受信 SMTP 認証（Inbound SMTP Authentication）] ページ	[受信 SMTP 認証（Inbound SMTP Authentication）] ページには、クライアント証明書の使用情報、および電子メール セキュリティ アプライアンスとユーザのメール クライアント間で SMTP セッションを認証するための SMTP AUTH コマンドが表示されます。 詳細については、「[受信 SMTP 認証（Inbound SMTP Authentication）] ページ」（P.4-39）を参照してください。
[レート制限（Rate Limits）] ページ	[レート制限（Rate Limits）] ページには、送信者あたりのメッセージ受信者数に対して設定したしきい値を超える電子メール送信者（MAIL-FROM アドレスに基づく）が表示されます。 詳細については、「[レート制限（Rate Limits）] ページ」（P.4-40）を参照してください。
[アウトブレイク フィルタ（Outbreak Filters）] ページ	[アウトブレイク フィルタ（Outbreak Filters）] ページには、ウイルス感染フィルタによって隔離された最近のアウトブレイクやメッセージに関する情報が示されます。このページを使用して、ウイルス攻撃に対する防御をモニタします。 詳細については、「[アウトブレイク フィルタ（Outbreak Filters）] ページ」（P.4-41）を参照してください。

表 4-1　[メール レポート（Email Reporting）] タブのオプション （続き）

[メール レポート（Email Reporting）] メニュー	アクション
[システム容量（System Capacity）] ページ	レポーティング データを セキュリティ管理アプライアンスに送信する、全体的なワークロードを表示できます。 詳細については、「[システム容量（System Capacity）] ページ」（P.4-44）を参照してください。
[有効なレポート データ（Reporting Data Availability）] ページ	各アプライアンスの セキュリティ管理アプライアンス上のレポーティング データの影響を把握できます。詳細については、「[有効なレポート データ（Reporting Data Availability）] ページ」（P.4-50）を参照してください。
電子メール レポートのスケジュール設定	指定した時間範囲のレポートのスケジュールを設定できます。詳細については、「電子メール レポートのスケジュール設定」（P.4-56）を参照してください。
アーカイブ電子メール レポートの表示と管理	アーカイブ済みのレポートを表示および管理できます。詳細については、「アーカイブ電子メール レポートの表示と管理」（P.4-60）を参照してください。 また、オンデマンド レポートを生成することもできます。「オンデマンドでの電子メール レポートの生成」（P.4-58）を参照してください。

電子メール レポーティング ページのテーブル カラムの説明

表 4-2　電子メール レポーティング ページのテーブル カラムの説明

カラム名	説明
受信メールの詳細（Incoming Mail Details）	
接続拒否（Connections Rejected）	HAT ポリシーによってブロックされたすべての接続。アプライアンスに重い負荷がかけられている場合、拒否された接続の正確な数を送信者別に維持できません。代わりに、拒否された接続数は、インターバルごとの最大送信者だけに対して維持されます。
接続承認（Connections Accepted）	受け入れられたすべての接続。
試行されたメッセージの合計数（Total Attempted）	すべての受け入れられた接続試行と、拒否された接続試行。
受信者スロットルによる停止（Stopped by Recipient Throttling）	これは、レピュテーション フィルタリングによる阻止の 1 要素です。HAT 制限のいずれか（1 時間当たりの最大受信者数、メッセージ別の最大受信者数、接続別の最大メッセージ数）を超えたため阻止された受信者メッセージの数を表します。これは、[レピュテーション フィルタによる停止（Stopped by Reputation Filtering）] が発生した、拒否された、または TCP 拒否された接続に関連する受信者メッセージを推定して集計されます。

表 4-2　電子メール レポーティング ページのテーブル カラムの説明 （続き）

カラム名	説明
レピュテーション フィルタによる停止（Stopped by Reputation Filtering）	[レピュテーション フィルタによる停止（Stopped by Reputation Filtering）] の値は、次の複数の要素に基づいて算出されます。 • この送信者からの「調整された」メッセージの数 • 拒否された、または TCP 拒否の接続数（部分的に集計されます） • 接続ごとのメッセージ数に対する控えめな乗数 アプライアンスに重い負荷がかけられている場合、拒否された接続の正確な数を送信者別に維持できません。代わりに、拒否された接続数は、インターバルごとの最大送信者だけに対して維持されます。この場合、表示される値は「下限」、つまり少なくともこの数のメッセージが阻止されたと解釈できます。 **（注）** [概要（Overview）] ページの [レピュテーション フィルタによる停止（Stopped by Reputation Filtering）] の総数は、すべての拒否された接続の完全な集計値に常に基づいています。送信者別の接続数だけは、負荷が原因で限定的なものになります。
無効な受信者として停止（Stopped as Invalid Recipients）	従来の LDAP 拒否によって拒否されたすべての電子メール受信者数にすべての RAT 拒否数を加えた値。
スパム検出（Spam Detected）	検出されたすべてのスパム。
ウイルス検出（Virus Detected）	検出されたすべてのウイルス。
コンテンツ フィルタによる停止（Stopped by Content Filter）	コンテンツ フィルタによって阻止されたメッセージの総数。
合計脅威件数（Total Threat）	脅威メッセージ（評価により阻止されたもの、無効な受信者、スパム、およびウイルスとして阻止されたもの）の総数。
マーケティング（Marketing）	不要なマーケティング メッセージとして検出されたメッセージの数。
正常（Clean）	すべてのクリーン メッセージ。
User Mail Flow Details（[内部ユーザ（Internal Users）] ページ）	
受信スパム検出（Incoming Spam Detected）	検出されたすべての着信スパム。
受信ウイルス検出（Incoming Virus Detected）	検出された着信ウイルス。
受信コンテンツ フィルタの一致数（Incoming Content Filter Matches）	検出された着信コンテンツ フィルタの一致。
コンテンツ フィルタによる受信停止（Incoming Stopped by Content Filter）	設定されていたコンテンツ フィルタのために阻止された着信メッセージ。
正常な受信（Incoming Clean）	すべての着信クリーン メッセージ。
送信スパム検出（Outgoing Spam Detected）	検出された発信スパム。

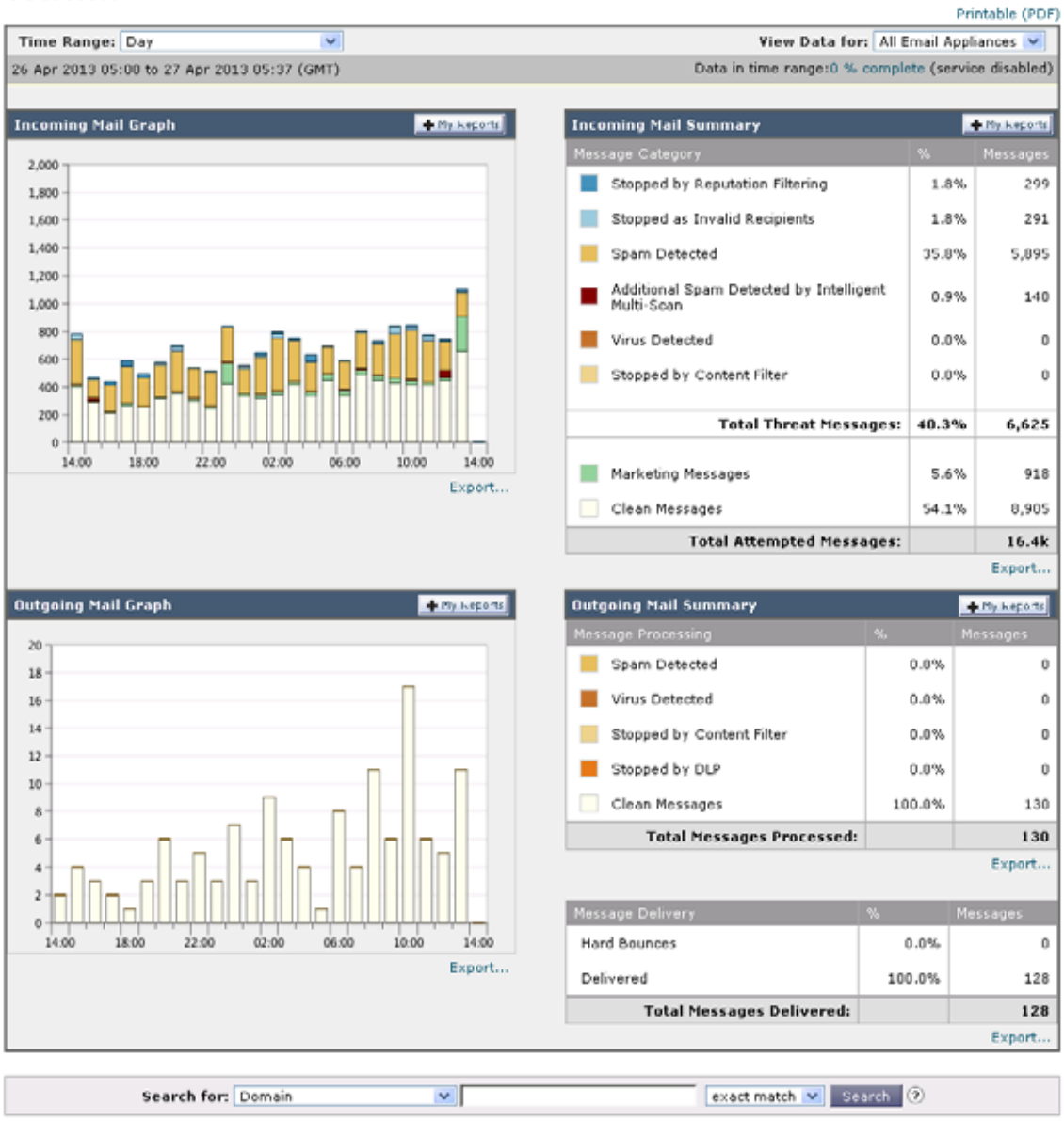
表 4-2　電子メール レポーティング ページのテーブル カラムの説明 （続き）

カラム名	説明
送信ウイルス検出（Outgoing Virus Detected）	検出された発信ウイルス。
送信コンテンツ フィルタの一致数（Outgoing Content Filter Matches）	検出された発信コンテンツ フィルタの一致。
コンテンツ フィルタによる送信停止（Outgoing Stopped by Content Filter）	設定されていたコンテンツ フィルタのため阻止された発信メッセージ。
正常な送信（Outgoing Clean）	すべての発信クリーン メッセージ。
Incoming and Outgoing TLS Connections（[TLS 接続（TLS Connections）] ページ）	
必要な TLS：失敗（Required TLS: Failed）	失敗した、必要なすべての TLS 接続。
必要な TLS：成功（Required TLS: Successful）	成功した、必要なすべての TLS 接続。
優先する TLS：失敗（Preferred TLS: Failed）	失敗した、優先するすべての TLS 接続。
優先する TLS：成功（Preferred TLS: Successful）	成功した、優先するすべての TLS 接続。
合計接続数（Total Connections）	TLS 接続の合計数。
合計メッセージ数（Total Messages）	TLS メッセージの総数。
アウトブレイク フィルタ（Outbreak Filters）	
アウトブレイク名（Outbreak Name）	アウトブレイクの名前。
アウトブレイク ID（Outbreak ID）	アウトブレイク ID。
最初にグローバルで確認した日時（First Seen Globally）	ウイルスが最初にグローバルに発見された時刻。
保護時間（Protection Time）	ウイルスから保護されていた時間。
隔離されたメッセージ（Quarantined Messages）	隔離に関するメッセージ。

電子メール レポーティングの [概要（Overview）] ページ

セキュリティ管理アプライアンスの [メール（Email）] > [レポート（Reporting）] > [概要（Overview）] ページには、電子メール セキュリティ アプライアンスからの電子メール メッセージ アクティビティの概要が表示されます。[概要（Overview）] ページには、グラフや、着信および発信メッセージの要約テーブルが表示されます。

図 4-1　[メール（Email）] > [レポート（Reporting）] > [概要（Overview）] ページ



概要レベルの [概要（Overview）] ページに、送受信メールのグラフと送受信メールのサマリーが表示されます。

メール トレンド グラフは、メール フローを視覚的に表したものです。このページのメール トレンド グラフを使用して、アプライアンスを行き来するすべてのメールの流れをモニタできます。

（注）　[ドメイン毎のエグゼクティブ サマリー（Domain-Based Executive Summary）] レポートおよび [エグゼクティブ サマリー（Executive Summary）] レポートは、電子メール レポーティングの [概要（Overview）] ページに基づきます。詳細については、「[ドメイン毎のエグゼクティブ サマリー（Domain-Based Executive Summary）] レポート」（P.4-53）および「[エグゼクティブ サマリー（Executive Summary）] レポート」（P.4-56）を参照してください。

表 4-3　[メール（Email）] > [レポート（Reporting）] > [概要（Overview）] ページの詳細

セクション	説明
時間範囲（Time Range）	表示する時間範囲を選択するためのオプションを伴うドロップダウン リスト。詳細については、「レポートの時間範囲の選択」（P.3-4）を参照してください。
データ参照（View Data for）	[概要（Overview）] のデータを表示する電子メール セキュリティ アプライアンスを選択するか、[全メール アプライアンス（All Email Appliances）] を選択します。 「アプライアンスまたはレポーティング グループのレポーティング データの表示」（P.3-4）も参照してください。
受信メールのグラフ（Incoming Mail Graph）	[受信メールのグラフ（Incoming Mail Graph）] には、着信メールの内訳をリアルタイムで視覚的に示したグラフが表示されます。
送信メールのグラフ（Outgoing Mail Graph）	[送信メールのグラフ（Outgoing Mail Graph）] には、アプライアンスでの発信メールの内訳を視覚的に示したグラフが表示されます。
受信メール サマリー（Incoming Mail Summary）	[受信メール サマリー（Incoming Mail Summary）] には、レピュテーション フィルタリングによって阻止された（SBRS）メッセージ、無効な受信者として阻止されたメッセージ、スパムが検出されたメッセージ、ウイルスが検出されたメッセージ、およびコンテンツ フィルタによって阻止されたメッセージ、ならびに「クリーン」と見なされたメッセージのパーセンテージと数が表示されます。
送信メール サマリー（Outgoing Mail Summary）	[送信メール サマリー（Outgoing Mail Summary）] セクションには、発信脅威メッセージおよび発信クリーン メッセージの情報が含まれます。また、配信されたメッセージとハードバウンスされたメッセージの内訳も含まれます。

着信メール メッセージのカウント方法

AsyncOS は、メッセージごとの受信者数に応じて着信メールをカウントします。たとえば、example.com から 3 人の受信者に送信された着信メッセージは、その送信者からの 3 通のメッセージとしてカウントされます。

レピュテーション フィルタリングによってブロックされたメッセージは、実際には作業キューに入らないので、アプライアンスは、着信メッセージの受信者のリストにはアクセスできません。この場合、乗数を使用して受信者の数が予測されます。この乗数は既存の顧客データの大規模なサンプリング調査に基づいています。

アプライアンスによる電子メール メッセージの分類方法

メッセージは電子メール パイプラインを通過するので、複数のカテゴリに該当する場合があります。たとえば、メッセージにスパム陽性またはウイルス陽性というマークを付けることができます。コンテンツ フィルタに一致させることもできます。

これらの優先ルールに続いて、次のようなさまざまな判定が行われます。

- アウトブレイク フィルタの隔離
  （この場合、メッセージが隔離から解放されるまで集計されず、作業キューによる処理が再び行われます）
- スパム陽性
- ウイルス陽性
- コンテンツ フィルタとの一致

これらの規則に従って、メッセージがスパム陽性とマークされると、アンチスパム設定がスパム陽性のメッセージをドロップするように設定されている場合には、このメッセージがドロップされ、スパム カウンタが増分します。

さらに、スパム陽性のメッセージを引き続き電子メール パイプラインで処理し、以降のコンテンツ フィルタがこのメッセージをドロップ、バウンス、または隔離するようにアンチスパム設定が設定されている場合にも、スパム カウンタは増分します。メッセージがスパム陽性またはウイルス陽性ではない場合、コンテンツ フィルタ カウントが増分するだけです。

[概要（Overview）] ページでの電子メール メッセージの分類

[概要（Overview）] ページでレポートされるメッセージは、次のように分類されます。

表 4-4　[概要（Overview）] ページの電子メールのカテゴリ

カテゴリ	説明
レピュテーション フィルタによる停止（Stopped by Reputation Filtering）	HAT ポリシーによってブロックされたすべての接続数に、固定乗数（「着信メール メッセージのカウント方法」（P.4-13）を参照）を掛けたものに、受信者のスロットリングによってブロックされたすべての受信者数を加えた値。 [概要（Overview）] ページの [レピュテーション フィルタによる停止（Stopped by Reputation Filtering）] の総数は、すべての拒否された接続の完全な集計値に常に基づいています。送信者別の接続数だけは、負荷が原因で限定的なものになります。
無効な受信者（Invalid Recipients）	従来の LDAP 拒否によって拒否されたすべての電子メール受信者数にすべての RAT 拒否数を加えた値。
スパム メッセージ検出（Spam Messages Detected）	アンチスパム スキャン エンジンで陽性、または疑いありとして検出されたメッセージの総数。さらに、スパムとウイルスの両方で陽性と検出されたメッセージの総数。

表 4-4　[概要（Overview）] ページの電子メールのカテゴリ （続き）

カテゴリ	説明
ウィルス メッセージ検出（Virus Messages Detected）	ウイルス陽性だがスパムではないと検出されたメッセージの総数および割合。 次のメッセージは、[ウイルス検出（Virus Detected）] カテゴリにカウントされます。 • ウイルス スキャン結果が [修復（Repaired）] または [感染（Infectious）] であるメッセージ • 暗号化されたメッセージをウイルスを含むメッセージとしてカウントするオプションが選択されている場合に、ウイルス スキャン結果が [暗号化（Encrypted）] であるメッセージ • スキャンできないメッセージに対するアクションが [「配信」なし（NOT "Deliver"）] の場合に、ウイルス スキャン結果が [スキャン不可（Unscannable）] であるメッセージ • 代替メール ホストまたは代替受信者へ送信するオプションが選択されている場合に、ウイルス スキャン結果が [スキャン不可（Unscannable）] または [暗号化（Encrypted）] であるメッセージ • アウトブレイク隔離から手動またはタイムアウトにより削除されたメッセージ
コンテンツ フィルタによる停止（Stopped by Content Filter）	コンテンツ フィルタによって阻止されたメッセージの総数。
マーケティング メッセージ（Marketing Messages）	不要なマーケティング メッセージと検出されたメッセージの総数および割合。このページのこのリスト項目は、システムにマーケティング データが存在している場合にだけ表示されます。
正常なメッセージ受信（Clean Messages Accepted）	このカテゴリは、受け入れられ、ウイルスでもスパムでもないと見なされたメールです。 受信者単位のスキャン アクション（個々のメール ポリシーで処理される分裂したメッセージなど）を考慮したときに受信されたクリーン メッセージを最も正確に表したものです。 ただし、スパム陽性またはウイルス陽性というマークを付けられたが、それでも配信されるメッセージはカウントされないため、配信される実際のメッセージ数はクリーン メッセージ数とは異なる可能性があります。 メッセージが*メッセージ フィルタ*と一致し、フィルタによってドロップされたり、バウンスされたりしていない場合は、クリーンなメッセージとして扱われます。メッセージ フィルタによってドロップされたか、バウンスされたメッセージは、総数に含まれません。

（注）　スキャンできないメッセージまたは暗号化されたメッセージを配信するようにアンチウイルス設定を行った場合、これらのメッセージは、ウイルス陽性としてではなく、クリーン メッセージとして集計されます。それ以外の場合は、メッセージはウイルス陽性として集計されます。

[受信メール（Incoming Mail）] ページ

セキュリティ管理アプライアンスの [受信メール（Incoming Mail）] > [レポート（Reporting）] > [受信メール（Incoming Mail）] ページには、管理対象の セキュリティ管理アプライアンスに接続されているすべてのリモート ホストのリアルタイム情報のインタラクティブなレポートが表示されます。システムに電子メールを送信している IP アドレス、ドメイン、およびネットワーク オーナー（組織）の情報を収集できます。また、メール送信者の IP アドレス、ドメイン、組織については、送信者プロファイル検索を実行することもできます。

[受信メール（Incoming Mail）] ページは、2 つの主要なセクションからなります。つまり、上位送信者（脅威メッセージの合計とクリーン メッセージの合計による）をまとめたメール トレンド グラフと、[受信メールの詳細（Incoming Mail Details）] インタラクティブ テーブルです。

[受信メールの詳細（Incoming Mail Details）] インタラクティブ テーブルには、特定の IP アドレス、ドメイン、またはネットワーク オーナー（組織）についての詳細情報が表示されます。[受信メール（Incoming Mail）] ページまたは他の [送信者プロファイル（Sender Profile）] ページの上部にある対応するリンクをクリックすると、IP アドレス、ドメイン、またはネットワーク オーナーの [送信者プロファイル（Sender Profile）] ページにアクセスできます。

[受信メール（Incoming Mail）] ページでは、次の操作を実行できます。

- セキュリティ管理アプライアンスに電子メールを送信したメール送信者の IP アドレス、ドメイン、またはネットワーク オーナー（組織）に関する検索を実行する。「検索およびインタラクティブ電子メール レポート ページ」（P.4-6）を参照してください。
- 送信者グループ レポートを表示して、特定の送信者グループおよびメール フロー ポリシー アクションに従って接続をモニタする。詳細については、「[送信者グループ（Sender Groups）] レポート ページ」（P.4-23）を参照してください。
- 電子メールをアプライアンスに送信した送信者の詳細な統計情報を表示する。統計情報には、セキュリティ サービス（評価フィルタリング、アンチスパム、アンチウイルスなど）によってブロックされたメッセージの数が含まれます。
- アンチスパムまたはアンチウイルス セキュリティサービスによって測定される、大量のスパムまたはウイルス電子メールを送信した送信者別にソートする。
- SenderBase レピュテーション サービスを使用して特定の IP アドレス、ドメイン、および組織の間の関係の分析を行い、送信者に関する情報を取得する。
- 送信者の SenderBase レピュテーション スコア、ドメインが直近に一致した送信者グループなど SenderBase レピュテーション サービスから送信者に関する詳細を取得する。送信者を送信者グループに追加する。
- アンチスパムまたはアンチウイルス セキュリティ サービスによって測定される、大量のスパムまたはウイルス電子メールを送信した特定の送信者についての詳細情報を取得する。

[受信メール（Incoming Mail）] ページ内のビュー

[受信メール（Incoming Mail）] ページには、次の 3 つのビューがあります。

- IP アドレス
- ドメイン
- ネットワーク オーナー

これらのビューでは、システムに接続されたリモート ホストのスナップショットが、選択したビューのコンテキストで提供されます。

さらに、[受信メール（Incoming Mail）] ページの [受信メールの詳細（Incoming Mail Details）] セクションでは、[送信者 IP アドレス（Sender’s IP Address）]、[ドメイン名（Domain name）]、または [ネットワーク所有者情報（Network Owner Information）] をクリックすると、特定の [送信者プロファイル情報（Sender Profile Information）] を取得できます。[送信者プロファイル（Sender Profile）] の情報の詳細については、「[送信者プロファイル（Sender Profile）] ページ」（P.4-20）を参照してください。

（注）　*ネットワーク オーナー*は、ドメインを含むエンティティです。*ドメイン*は、IP アドレスを含むエンティティです。

選択したビューに応じて、[受信メールの詳細（Incoming Mail Details）] インタラクティブ テーブルに、電子メール セキュリティ アプライアンスで設定されたすべてのパブリック リスナーに電子メールを送信した上位 IP アドレス、ドメイン、またはネットワーク オーナーが表示されます。アプライアンスに入ったすべてのメールのフローをモニタできます。

IP アドレス、ドメイン、またはネットワーク オーナーをクリックすると、[送信者プロファイル（Sender Profile）] ページの送信者の詳細にアクセスできます。[送信者プロファイル（Sender Profile）] ページは特定の IP アドレス、ドメインまたはネットワーク オーナーに固有の [受信メール（Incoming Mail）] ページです。

送信者グループ別のメール フロー情報にアクセスするには、[受信メール（Incoming Mail）] ページの下部にある [送信者グループのレポート（Sender Groups Report）] リンクをクリックします。「[送信者グループ（Sender Groups）] レポート ページ」（P.4-23）を参照してください。

[受信メール（Incoming Mail）] ページでの電子メール メッセージの分類

[受信メール（Incoming Mail）] ページでレポートされるメッセージは、次のように分類されます。

表 4-5　[受信メール（Incoming Mail）] ページの電子メールのカテゴリ

カテゴリ	説明
レピュテーション フィルタによる停止（Stopped by Reputation Filtering）	HAT ポリシーによってブロックされたすべての接続数に、固定乗数（「着信メール メッセージのカウント方法」（P.4-13）を参照）を掛けたものに、受信者のスロットリングによってブロックされたすべての受信者数を加えた値。 [レピュテーション フィルタによる停止（Stopped by Reputation Filtering）] の値は、次の複数の要素に基づいて算出されます。 • この送信者からの「調整された」メッセージの数 • 拒否された、または TCP 拒否の接続数（部分的に集計されます） • 接続ごとのメッセージ数に対する控えめな乗数 アプライアンスに重い負荷がかけられている場合、拒否された接続の正確な数を送信者別に維持できません。代わりに、拒否された接続数は、インターバルごとの最大送信者だけに対して維持されます。この場合、表示される値は「下限」、つまり少なくともこの数のメッセージが阻止されたと解釈できます。
無効な受信者（Invalid Recipients）	従来の LDAP 拒否によって拒否されたすべての電子メール受信者数にすべての RAT 拒否数を加えた値。

表 4-5　[受信メール（Incoming Mail）] ページの電子メールのカテゴリ （続き）

カテゴリ	説明
スパム メッセージ検出（Spam Messages Detected）	アンチスパム スキャン エンジンで陽性、または疑いありとして検出されたメッセージの総数。さらに、スパムとウイルスの両方で陽性と検出されたメッセージの総数。
ウィルス メッセージ検出（Virus Messages Detected）	ウイルス陽性だがスパムではないと検出されたメッセージの総数および割合。
コンテンツ フィルタによる停止（Stopped by Content Filter）	コンテンツ フィルタによって阻止されたメッセージの総数。 アクセス権限でメッセージ トラッキング データを表示できる場合、このレポートのコンテンツ フィルタ違反に対するメッセージ トラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。
マーケティング メッセージ（Marketing Messages）	不要なマーケティング メッセージと検出されたメッセージの総数および割合。このページのこのリスト項目は、システムにマーケティング データが存在している場合にだけ表示されます。
正常なメッセージ受信（Clean Messages Accepted）	受け入れられ、ウイルスでもスパムでもないと見なされたメール。受信者単位のスキャン アクション（個々のメール ポリシーで処理される分裂したメッセージなど）を考慮したときに受信されたクリーン メッセージを最も正確に表したものです。ただし、スパム陽性またはウイルス陽性というマークを付けられたが、それでも配信されるメッセージはカウントされないため、配信される実際のメッセージ数はクリーン メッセージ数とは異なる可能性があります。

（注）スキャンできないメッセージまたは暗号化されたメッセージを配信するようにアンチウイルス設定を行った場合、これらのメッセージは、ウイルス陽性としてではなく、クリーン メッセージとして集計されます。それ以外の場合は、メッセージはウイルス陽性として集計されます。

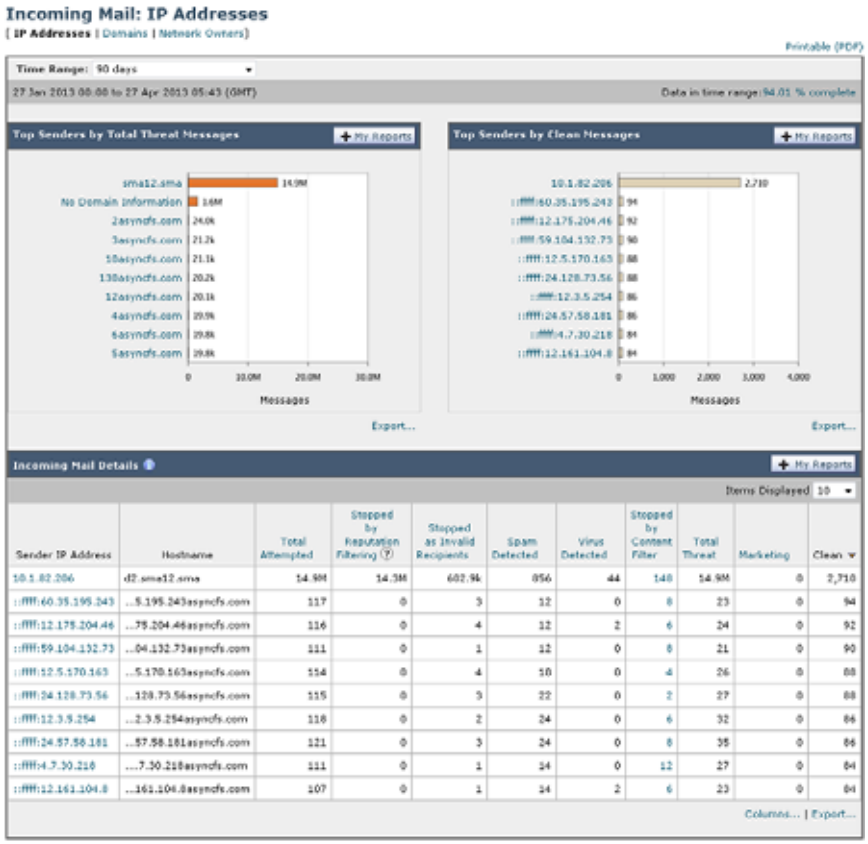
さらに、メッセージが*メッセージ フィルタ*と一致し、フィルタによってドロップされたり、バウンスされたりしていない場合、クリーンなメッセージとして扱われます。メッセージ フィルタによってドロップされたか、バウンスされたメッセージは、総数に含まれません。

場合によっては、いくつかのレポート ページに、トップレベルのページからアクセスできる独自のサブレポートが複数含まれることがあります。たとえば、セキュリティ管理アプライアンスの [受信メール（Incoming Mail）] レポート ページでは、個々の IP アドレス、ドメイン、およびネットワーク オーナーの情報を表示できます。これらは [受信メール（Incoming Mail）] レポート ページからアクセスできるサブページです。

トップレベル ページ（この場合には [受信メール（Incoming Mail）] レポート ページ）の右上にある [印刷可能 PDF（Printable PDF）] リンクをクリックすると、これらの各サブレポート ページの結果を、1 つの統合レポートに生成できます。「[メール レポート（Email Reporting）] ページの概要」（P.4-7）の重要な情報を参照してください。

[メール（Email）] > [レポート（Reporting）] > [受信メール（Incoming Mail）] ページには次のビューがあります : [IP アドレス（IP Addresses）]、[ドメイン（Domains）]、または [ネットワーク所有者（Network Owners）]

図 4-2　[受信メール（Incoming Mail）] ページ : [IP アドレス（IP Address）] ビュー



[受信メールの詳細（Incoming Mail Details）] インタラクティブ テーブルに含まれるデータの説明については、「[受信メールの詳細（Incoming Mail Details）] テーブル」（P.4-20）を参照してください。

この例では、[ドメイン（Domain）] ビューが選択されています。

[受信メール（Incoming Mail）] ページから、PDF を生成したり、raw データを CSV ファイルにエクスポートしたりすることもできます。ファイルを印刷またはエクスポートする方法の詳細については、「[メール レポート（Email Reporting）] ページの概要」（P.4-7）を参照してください。

（注）　[受信メール（Incoming Mail）] レポート ページのスケジュール設定されたレポートを生成できます。「電子メール レポートのスケジュール設定」（P.4-56）を参照してください。

[ドメイン情報がありません（No Domain Information）] リンク

セキュリティ管理アプライアンスに接続したものの、ダブル DNS ルックアップで検証できなかったドメインは、専用ドメイン [ドメイン情報がありません（No Domain Information）] に自動的に分類されます。これらの種類の検証されないホストを、送信者の検証によってどのように管理するかを制御できます。送信者の検証の詳細については、ご使用の電子メール セキュリティ アプライアンスのマニュアルまたはオンライン ヘルプを参照してください。

[表示されたアイテム（Items Displayed）] メニューを使用して、リストに表示する送信者の数を選択できます。

メール トレンド グラフにおける時間範囲

メールのグラフは、さまざまなきめ細かさを選択して表示できます。同じデータの日、週、月、および年のビューを選択できます。データはリアルタイムでモニタリングされているので、情報は定期的に更新され、データベースで集計されます。

時間範囲の詳細については、「レポートの時間範囲の選択」（P.3-4）を参照してください。

[受信メールの詳細（Incoming Mail Details）] テーブル

[受信メール（Incoming Mail）] ページの下部にあるインタラクティブな [受信メールの詳細（Incoming Mail Details）] テーブルには、電子メール セキュリティ アプライアンス上のパブリック リスナーに接続された上位送信者が表示されます。このテーブルには、選択したビューに基づいて、ドメイン、IP アドレス、またはネットワーク オーナーが表示されます。データをソートするには、カラム見出しをクリックします。

*ダブル DNS ルックアップ*を実行することで、システムはリモート ホストの IP アドレスの正当性を確保および検証します。ダブル DNS ルックアップおよび送信者検証の詳細については、電子メール セキュリティ アプライアンスのマニュアルまたはオンライン ヘルプを参照してください。

[受信メールの詳細（Incoming Mail Details）] テーブルの最初のカラム、または [脅威メッセージの送信者上位（Top Senders by Total Threat Messages）] に表示される送信者、つまりネットワーク オーナー、IP アドレスまたはドメインについては、[送信者（Sender）] または [ドメイン情報がありません（No Domain Information）] リンクをクリックすると、送信者の詳細情報が表示されます。結果は、[送信者のプロファイル（Sender Profile）] ページに表示され、SenderBase レピュテーション サービスからのリアルタイム情報が含まれます。送信者プロファイル ページからは、特定の IP アドレスまたはネットワーク オーナーに関する詳細を表示できます。詳細については、「[送信者プロファイル（Sender Profile）] ページ」（P.4-20）を参照してください。

[受信メール（Incoming Mail）] ページの下部にある [送信者グループのレポート（Sender Groups Report）] をクリックして、[送信者グループ（Sender Groups）] レポートを表示することもできます。[送信者グループ（Sender Groups）] レポート ページの詳細については、「[送信者グループ（Sender Groups）] レポート ページ」（P.4-23）を参照してください。

アクセス権限でメッセージ トラッキング データを表示できる場合、このレポートのコンテンツ フィルタ違反に対するメッセージ トラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。

[送信者プロファイル（Sender Profile）] ページ

[受信メール（Incoming Mail）] ページで [受信メールの詳細（Incoming Mail Details）] インタラクティブ テーブルの送信者をクリックすると、[送信者プロファイル（Sender Profile）] ページが表示されます。ここには、特定の IP アドレス、ドメイン、またはネットワーク オーナー（組織）の詳細情報が表示されます。[受信メール（Incoming Mail）] ページまたは他の [送信者プロファイル（Sender Profile）] ページにある対応するリンクをクリックすると、IP アドレス、ドメイン、またはネットワーク オーナーの [送信者プロファイル（Sender Profile）] ページにアクセスできます。

*ネットワーク オーナー*は、ドメインを含むエンティティです。*ドメイン*は、IP アドレスを含むエンティティです。

IP アドレス、ドメインおよびネットワーク オーナーに関して表示される送信者プロファイル ページは、多少異なります。それぞれのページには、特定の送信者からの着信メールに関するグラフおよびサマリー テーブルが含まれます。グラフの下の表に、送信者に関連付けられたドメインまたは IP アドレスが表示されます。（個々の IP アドレスの [送信者プロファイル（Sender Profile）] ページに、詳細なリストは含まれません）。[送信者プロファイル（Sender Profile）] ページには、この送信者の現在の SenderBase 情報、送信者グループ情報、およびネットワーク情報を含む情報セクションもあります。

- ネットワーク オーナー プロファイル ページには、ネットワーク オーナー、およびこのネットワーク オーナーに関連するドメインや IP アドレスに関する情報が含まれます。
- ドメイン プロファイル ページには、このドメインおよびこのドメインに関連する IP アドレスに関する情報が含まれます。
- IP アドレス プロファイル ページには、IP アドレスのみに関する情報が含まれます。

各 [送信者プロファイル（Sender Profile）] ページには、ページの下部の現在の情報テーブルに次のデータが含まれます。

- SenderBase 評価サービスからのグローバル情報。たとえば、次の情報です。
  - IP アドレス、ドメイン名、またはネットワーク オーナー
  - ネットワーク オーナーのカテゴリ（ネットワーク オーナーのみ）
  - CIDR 範囲（IP アドレスのみ）
  - IP アドレス、ドメイン、またはネットワーク オーナーの日単位マグニチュードおよび月単位マグニチュード
  - この送信者から最初のメッセージを受信してからの日数
  - 最後の送信者グループと DNS が検証されたかどうか（IP アドレス送信者プロファイル ページのみ）

  日単位マグニチュードは、直近 24 時間にドメインが送信したメッセージの数の基準です。地震を測定するために使用されるリヒター スケールと同様に、SenderBase マグニチュードは、10 を底とした対数目盛を使用して計算されるメッセージ量の測定単位です。目盛の最大理論値は 10 に設定されます。これは、世界の電子メール メッセージの量に相当します。この対数目盛を使用した場合、マグニチュードの 1 ポイントの上昇は、実際の量の 10 倍増加に相当します。

  月単位マグニチュードは、直近 30 日間に送信された電子メールの量に基づいて割合が算出される点を除いて、日単位マグニチュードと同じ方法を使用して算出されます。

  - 平均マグニチュード（IP アドレスのみ）
  - 総累積量 /30 日の量（IP アドレス プロファイル ページのみ）
  - Bonded Sender ステータス（IP アドレス プロファイル ページのみ）
  - SenderBase 評価スコア（IP アドレス プロファイル ページのみ）
  - 最初のメッセージからの日数（ネットワーク オーナーとドメイン プロファイル ページのみ）
  - このネットワーク オーナーに関連するドメインの数（ネットワーク オーナー プロファイル ページおよびドメイン プロファイル ページのみ）
  - このネットワーク オーナーの IP アドレスの数（ネットワーク オーナー プロファイル ページおよびドメイン プロファイル ページのみ）
  - 電子メールの送信に使用された IP アドレスの数（ネットワーク オーナー ページのみ）

  SenderBase 評価サービスによって提供されるすべての情報を示すページを表示するには、[SenderBase からの詳細情報（More from SenderBase）] をクリックします。
- このネットワーク オーナーによって管理されるドメインおよび IP アドレスに関する詳細は、ネットワーク オーナー プロファイル ページに表示されます。ドメイン内の IP アドレスに関する詳細は、ドメイン ページに表示されます。

ドメイン プロファイルのページから、特定の IP アドレスをクリックして特定の情報を表示することも、組織プロファイルのページを表示することもできます。

図 4-3　ネットワーク オーナーの現在の情報

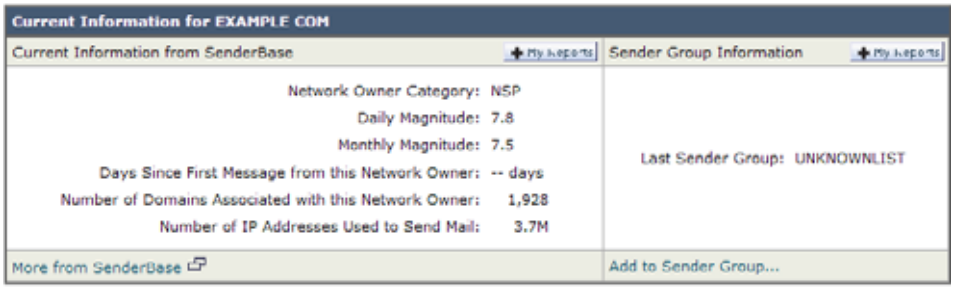
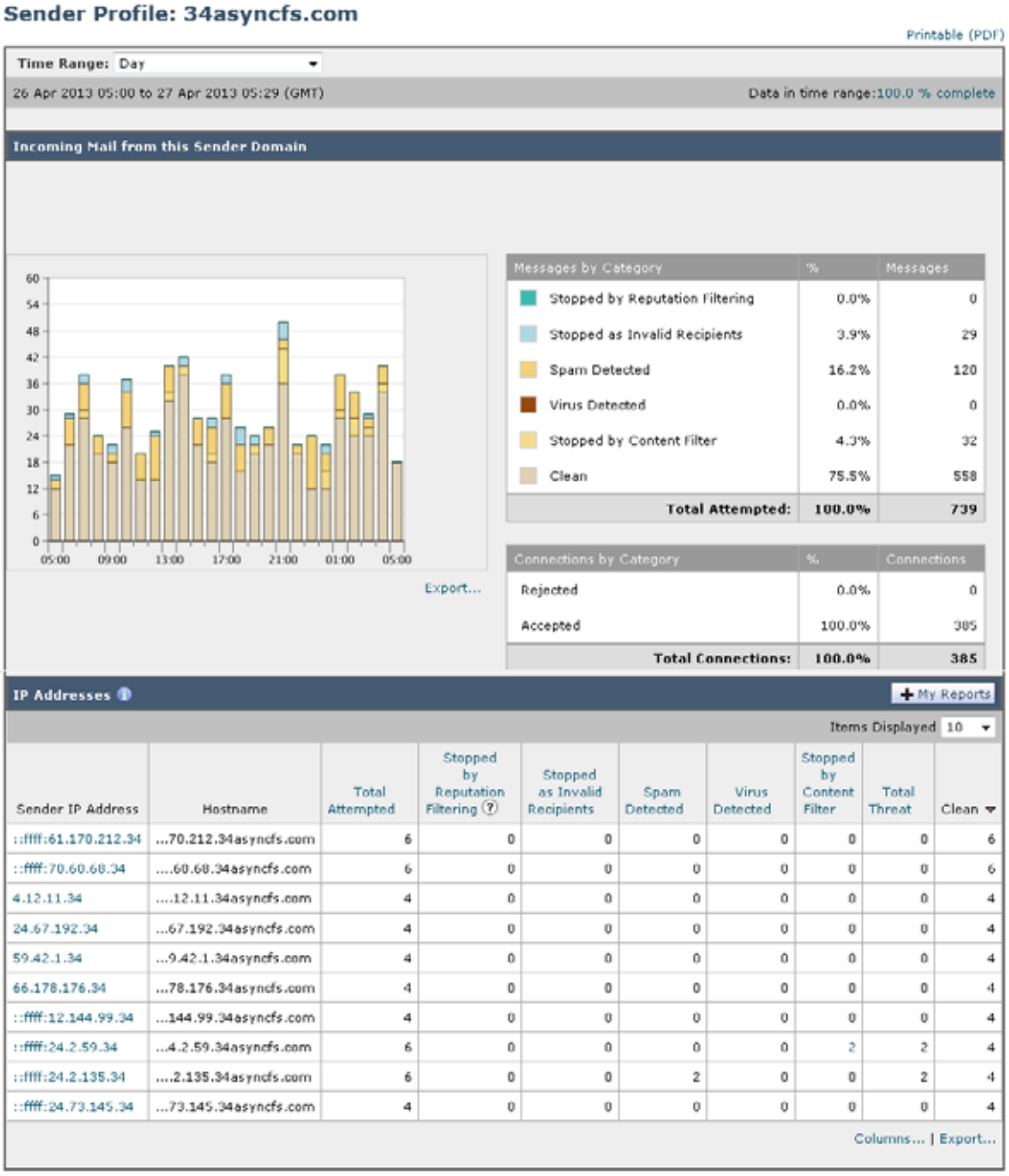


図 4-4　[送信者プロファイル（Sender Profile）] ページ



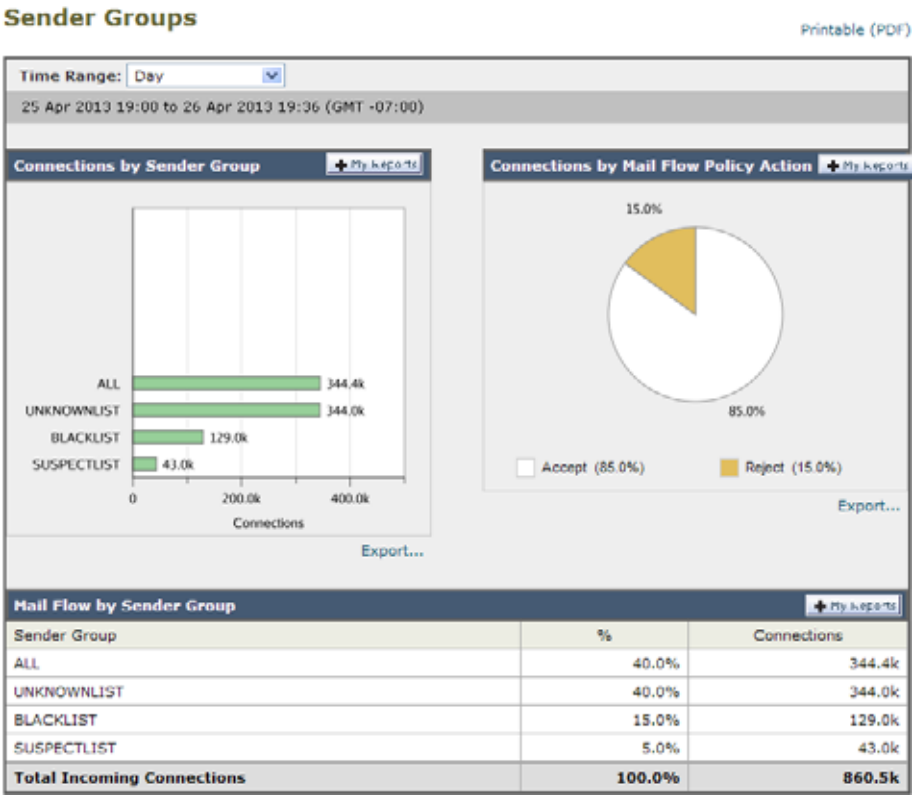
[送信者グループ（Sender Groups）] レポート ページ

[送信者グループ（Sender Groups）] レポート ページは、送信者グループ別およびメール フロー ポリシー アクション別の接続のサマリーを提供し、SMTP 接続およびメール フロー ポリシーのトレンドを確認できるようにします。[送信者グループによるメール フロー（Mail Flow by Sender Group）] リストには、各送信者グループの割合および接続数が示されます。[メール フロー ポリシー アクションによる接続（Connections by Mail Flow Policy Action）] グラフは、各メール フロー ポリシー アクショ

ンの接続の割合を示します。このページには、Host Access Table（HAT; ホスト アクセス テーブル）ポリシーの有効性の概要が示されます。HAT に関する詳細については、電子メール セキュリティ アプライアンスのマニュアルまたはオンライン ヘルプを参照してください。

[送信者グループ（Sender Groups）] レポート ページを表示するには、[受信メール（Incoming Mail）] レポート ページの下部にある [送信者グループのレポート（Sender Groups Report）] リンクをクリックします。

図 4-5　[送信者グループ（Sender Groups）] レポート ページ



[送信者グループ（Sender Groups）] レポート ページから、PDF を生成したり、raw データを CSV ファイルにエクスポートしたりすることもできます。ファイルを印刷またはエクスポートする方法の詳細については、「[メール レポート（Email Reporting）] ページの概要」（P.4-7）を参照してください。

（注）　[送信者グループ（Sender Groups）] レポート ページのスケジュール設定されたレポートを生成できます。「電子メール レポートのスケジュール設定」（P.4-56）を参照してください。

[送信先（Outgoing Destinations）] ページ

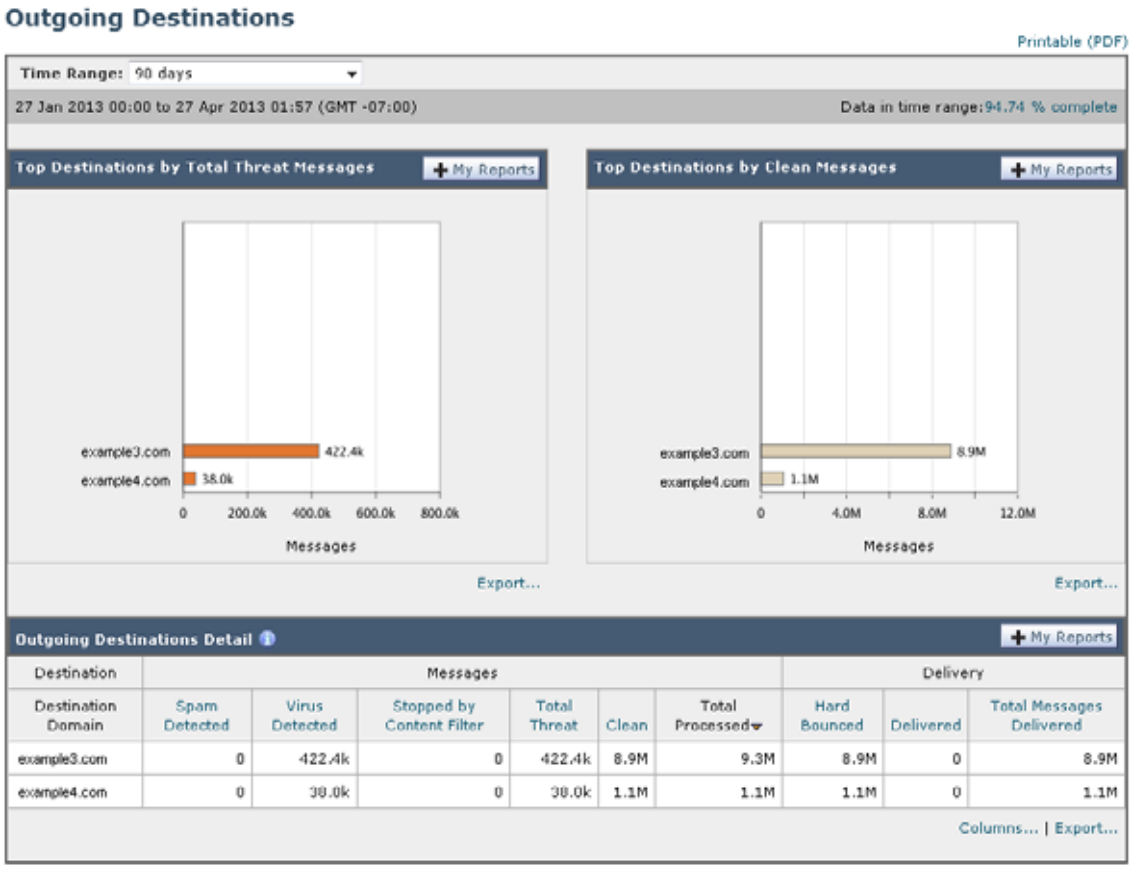
[メール（Email）] > [レポート（Reporting）] > [送信先（Outgoing Destinations）] ページには、組織が電子メールを送信する宛先のドメインについての情報が表示されます。

[送信先（Outgoing Destinations）] ページを使用して、次の情報を入手できます。

- 電子メール セキュリティ アプライアンスが電子メールを送信する宛先ドメイン
- 各ドメインに送信される電子メールの量

- クリーン、スパム陽性、またはコンテンツ フィルタによる阻止のメールの割合
- 配信されたメッセージおよび宛先サーバによってハードバウンスされたメッセージの数

図 4-6　[メール（Email）] > [レポート（Reporting）] > [送信先（Outgoing Destinations）] ページ



次のリストでは、[送信先（Outgoing Destinations）] ページのさまざまなセクションについて説明します。

表 4-6　[メール（Email）] > [レポート（Reporting）] > [送信先（Outgoing Destinations）] ページの詳細

セクション	説明
時間範囲（Time Range）（ドロップダウン リスト）	1 ～ 90 日間またはカスタム日数範囲を指定できるドロップダウン リスト。時間範囲の詳細と実際のニーズに合わせたカスタマイズについては、「レポートの時間範囲の選択」（P.3-4）を参照してください。
脅威メッセージの送信先上位（Top Destination by Total Threat）	組織によって送信された発信脅威メッセージ（スパム、アンチウイルスなど）の上位の宛先ドメイン。コンテンツ フィルタをトリガーしたスパム陽性またはウイルス陽性の脅威メッセージを含む、脅威メッセージの総数。

表 4-6　[メール（Email）] > [レポート（Reporting）] > [送信先（Outgoing Destinations）] ページの詳細 （続き）

セクション	説明
正常なメッセージの送信先上位（Top Destination by Clean Messages）	組織によって送信されたクリーンな発信脅威メッセージの上位の宛先ドメイン。
送信先の詳細（Outgoing Destination Details）	組織によって送信されたすべての発信メッセージの宛先ドメインに関する、総受信者数別にソートされたすべての詳細情報。詳細情報には検出されたスパム、ウイルス、クリーンメッセージなどが含まれます。 アクセス権限でメッセージ トラッキング データを表示できる場合、このレポートのコンテンツ フィルタ違反に対するメッセージ トラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。

[送信先（Outgoing Destinations）] ページから、PDF を生成したり、raw データを CSV ファイルにエクスポートしたりすることもできます。ファイルを印刷またはエクスポートする方法の詳細については、「[メール レポート（Email Reporting）] ページの概要」（P.4-7）を参照してください。

（注）　[送信先（Outgoing Destinations）] ページのスケジュール設定されたレポートを生成できます。「電子メール レポートのスケジュール設定」（P.4-56）を参照してください。

[送信メッセージ送信者（Outgoing Senders）] ページ

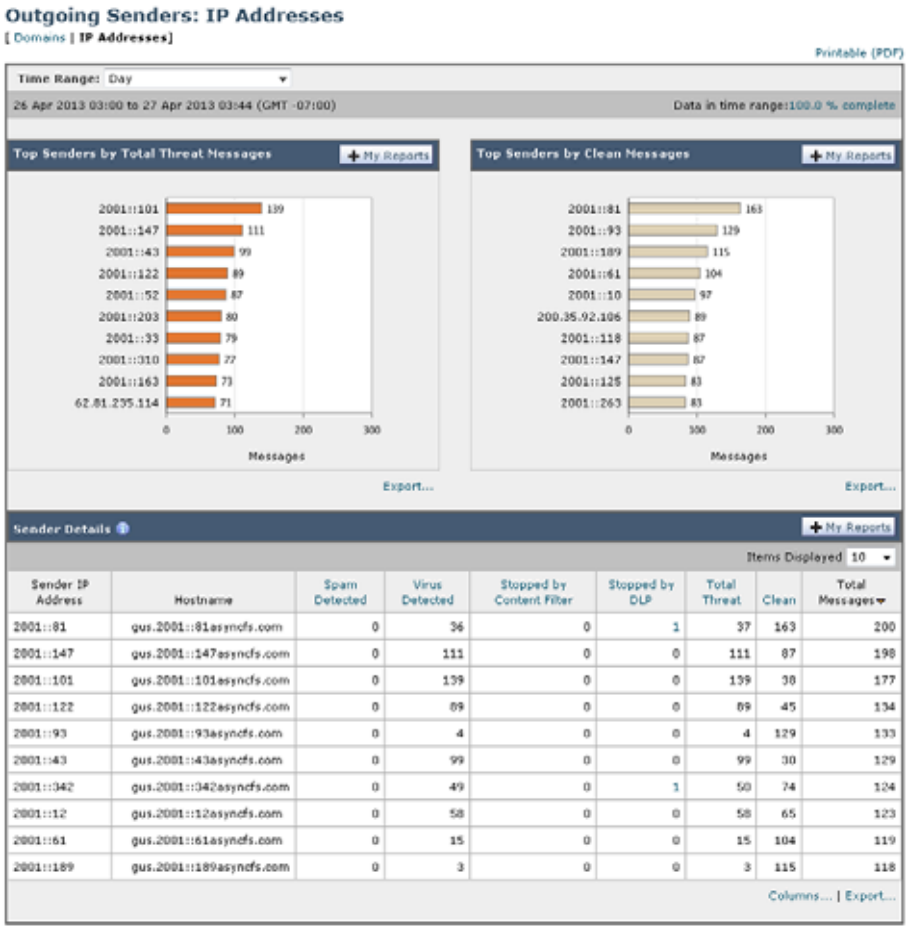
[メール（Email）] > [レポート（Reporting）] > [送信メッセージ送信者（Outgoing Senders）] ページには、ネットワーク内の IP アドレスおよびドメインから送信された電子メールの数と種類についての情報が表示されます。

[送信メッセージ送信者（Outgoing Senders）] ページを使用して、次の情報を入手できます。

- 最も多くのウイルスまたはスパム陽性の電子メールを送信した IP アドレス
- 最も頻繁にコンテンツ フィルタをトリガーした IP アドレス
- 最も多くのメールを送信するドメイン
- 配信が試行された場所で処理された受信者の総数

[送信メッセージ送信者（Outgoing Sender）] ページを表示するには、次の手順を実行します。

図 4-7　[メール（Email）] > [レポート（Reporting）] > [送信メッセージ送信者（Outgoing Senders）] ページ（IP アドレスを表示中）



[送信メッセージ送信者（Outgoing Senders）] の結果は次の 2 種類のビューで表示できます。

- [ドメイン（Domain）] : このビューでは、各ドメインから送信された電子メールの量を表示できます。
- [IP アドレス（IP address）] : このビューでは、最も多くのウイルス メッセージを送信したか、または最も多くのコンテンツ フィルタをトリガーした IP アドレスを表示できます。

次のリストでは、[送信先（Outgoing Destinations）] ページの両方のビューのさまざまなセクションについて説明します。

表 4-7　[メール（Email）] > [レポート（Reporting）] > [送信メッセージ送信者（Outgoing Sender）] ページの詳細

セクション	説明
時間範囲（Time Range）（ドロップダウン リスト）	1 ～ 90 日間またはカスタム日数範囲を指定できるドロップダウン リスト。時間範囲の詳細と実際のニーズに合わせたカスタマイズについては、「レポートの時間範囲の選択」（P.3-4）を参照してください。
脅威メッセージの送信者上位（Top Senders by Total Threat Messages）	組織内の発信脅威メッセージ（スパム、アンチウイルスなど）の上位送信者（IP アドレス別またはドメイン別）。

表 4-7　[メール（Email）] > [レポート（Reporting）] > [送信メッセージ送信者（Outgoing Sender）] ページの詳細 （続き）

セクション	説明
正常なメッセージの送信者上位（Top Sender by Clean Messages）	組織内で送信されたクリーンな発信メッセージの上位送信者（IP アドレス別またはドメイン別）。
送信者の詳細（Sender Details）	組織内によって送信されたすべての発信メッセージの送信者のすべての詳細情報（IP アドレス別またはドメイン別）。詳細情報には検出されたスパム、ウイルス、クリーンメッセージなどが含まれます。 アクセス権限でメッセージ トラッキング データを表示できる場合、このレポートの DLP およびコンテンツ フィルタ違反に対するメッセージ トラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。

（注）　このページには、メッセージ配信に関する情報は表示されません。特定のドメインからのバウンスされたメッセージの数などの配信情報を追跡するには、適切な電子メール セキュリティ アプライアンスにログインし、[モニタ（Monitor）] > [送信処理ステータス（Delivery Status）] を選択します。

[送信メッセージ送信者（Outgoing Senders）] ページから、PDF を生成したり、raw データを CSV ファイルにエクスポートしたりすることもできます。ファイルを印刷またはエクスポートする方法の詳細については、「[メール レポート（Email Reporting）] ページの概要」（P.4-7）を参照してください。

（注）　[送信メッセージ送信者（Outgoing Senders）] レポート ページのスケジュール設定されたレポートを生成できます。「電子メール レポートのスケジュール設定」（P.4-56）を参照してください。

[内部ユーザ（Internal Users）] ページ

[メール（Email）] > [レポート（Reporting）] > [内部ユーザ（Internal Users）] ページには、*電子メール アドレスごとに* 内部ユーザによって送受信された電子メールについての情報が表示されます。1 人のユーザが複数の電子メール アドレスを持っている場合があります。レポートでは、電子メール アドレスがまとめられません。

[内部ユーザ（Internal Users）] インタラクティブ レポート ページを使用すると、次のような情報を取得できます。

- 最も多くの外部メールを送信したユーザ
- 最も多くのクリーン電子メールを受信したユーザ
- 最も多くのスパムを受信したユーザ
- 特定のコンテンツ フィルタをトリガーしたユーザ
- 特定のユーザからの電子メールを阻止したコンテンツ フィルタ

図 4-8　[メール（Email）] > [レポート（Reporting）] > [内部ユーザ（Internal Users）] ページ

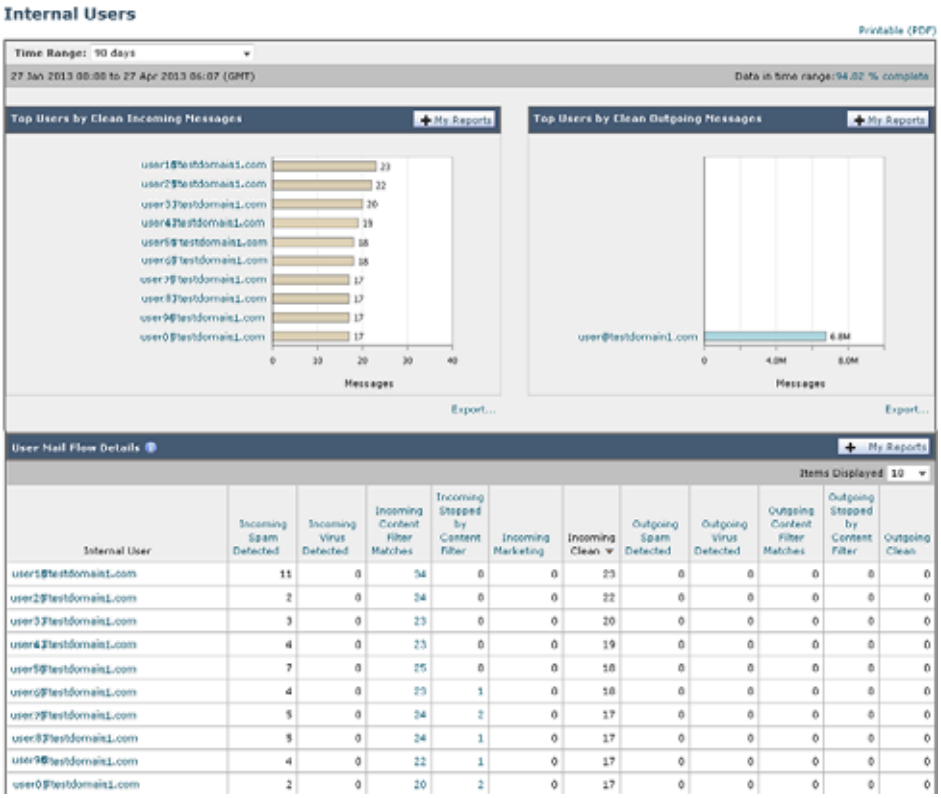


表 4-8　[メール（Email）] > [レポート（Reporting）] > [内部ユーザ（Internal Users）] ページの詳細

セクション	説明
時間範囲（Time Range）（ドロップダウン リスト）	1 ～ 90 日間またはカスタム日数範囲を指定できるドロップダウン リスト。時間範囲の詳細と実際のニーズに合わせたカスタマイズについては、「レポートの時間範囲の選択」（P.3-4）を参照してください。
上位ユーザ（正常な受信メッセージ）（Top Users by Clean Incoming Messages）	組織内で送信されたクリーンな着信メッセージの上位ユーザ（IP アドレス別またはドメイン別）。

表 4-8　[メール（Email）] > [レポート（Reporting）] > [内部ユーザ（Internal Users）] ページの詳細 （続き）

セクション	説明
上位ユーザ（正常な送信メッセージ）（Top Users by Clean Outgoing Messages）	組織内で送信されたクリーンな発信メッセージの上位ユーザ（IP アドレス別またはドメイン別）。
ユーザ メール フローの詳細（User Mail Flow Details）	[ユーザ メール フローの詳細（User Mail Flow Details）] インタラクティブ セクションでは、各電子メール アドレスで送受信した電子メールが [正常（Clean）]、[スパム検出（Spam Detected）]（受信のみ）、[ウイルス検出（Virus Detected）]、[コンテンツフィルタの一致（Content Filter Matches）] に分類されます。カラム ヘッダーをクリックすることにより、表示をソートできます。 ユーザの詳細を参照するには、[内部ユーザ（Internal Users）] カラムでユーザ名をクリックします。詳細については、「[内部ユーザの詳細（Internal User Details）] ページ」（P.4-30）を参照してください。 アクセス権限でメッセージ トラッキング データを表示できる場合、このレポートのコンテンツ フィルタ違反に対するメッセージ トラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。

[内部ユーザ（Internal Users）] ページから、PDF を生成したり、raw データを CSV ファイルにエクスポートしたりすることもできます。ファイルを印刷またはエクスポートする方法の詳細については、「[メール レポート（Email Reporting）] ページの概要」（P.4-7）を参照してください。

（注）　[内部ユーザ（Internal Users）] ページのスケジュール設定されたレポートを生成できます。「電子メール レポートのスケジュール設定」（P.4-56）を参照してください。

[内部ユーザの詳細（Internal User Details）] ページ

[内部ユーザの詳細（Internal User Details）] ページでは、各カテゴリ（[スパム検出（Spam Detected）]、[ウイルス検出（Virus Detected）]、[コンテンツフィルタによる停止（Stopped By Content Filter）]、および [正常（Clean）]）のメッセージ数を示す着信および発信メッセージの内訳など、ユーザに関する詳細情報が示されます。送受信コンテンツ フィルタの一致も示されます。

着信内部ユーザとは、Rcpt To: アドレスに基づいてシステムで電子メールを受信する対象ユーザのことです。発信内部ユーザは Mail From: アドレスに基づいており、内部ネットワーク内の送信者が送信している電子メールの種類を追跡する場合に役立ちます。

コンテンツ フィルタの詳細情報を対応するコンテンツ フィルタ情報ページに表示するには、そのコンテンツ フィルタ名をクリックします（「[コンテンツ フィルタ（Content Filters）] ページ」（P.4-34）を参照）。この方法を使用すると、特定のコンテンツ フィルタに一致したメールを送受信したすべてのユーザのリストも表示できます。

（注）　送信メールの中には（バウンスなど）、送信者が null になっているものがあります。これらの送信者は、送信「不明」として集計されます。

特定の内部ユーザの検索

[内部ユーザ（Internal Users）] ページおよび [内部ユーザの詳細（Internal User Details）] ページの下部にある検索フォームで、特定の内部ユーザ（電子メール アドレス）を検索できます。検索テキストに完全に一致させるか、入力したテキストで始まる項目を検索するか（たとえば、「ex」で始まる項目を検索する場合、「example@example.com」が一致します）を選択します。

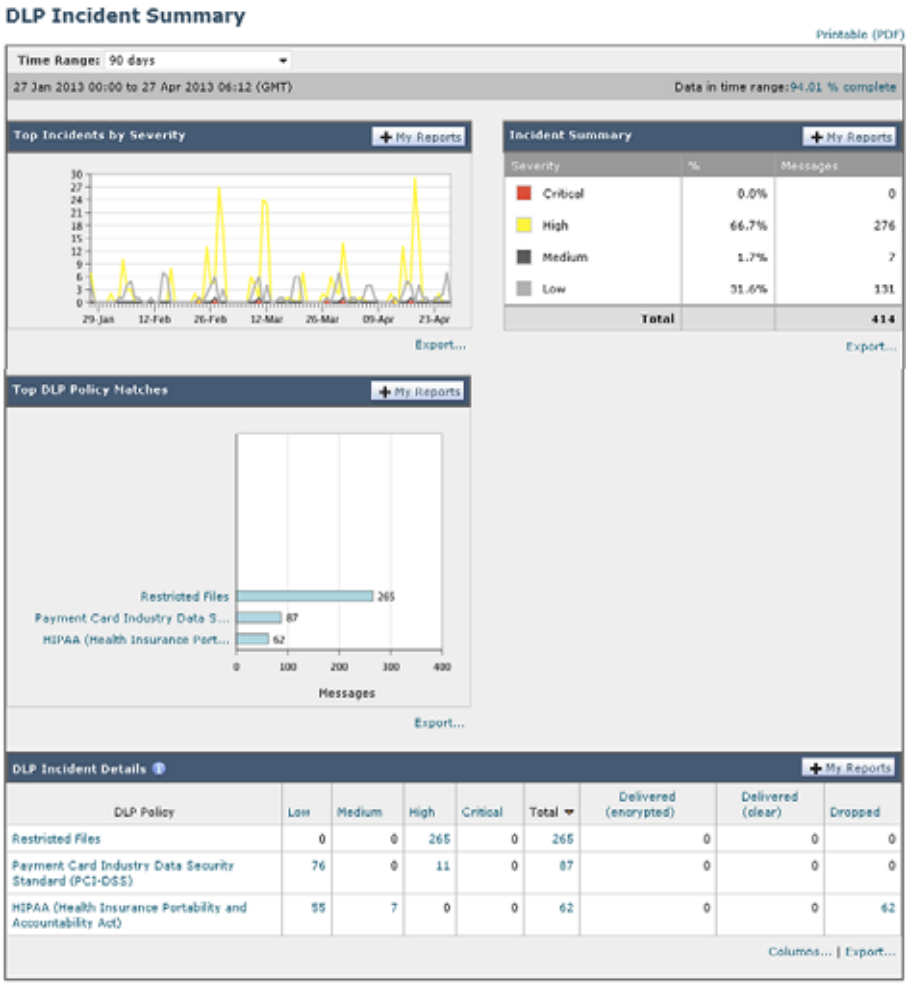
[DLP インシデント サマリー（DLP Incident Summary）] ページ

[メール（Email）] > [レポート（Reporting）] > [DLP インシデント サマリー（DLP Incident Summary）] ページには、送信メールで発生した、データ漏洩防止（DLP）ポリシーに違反するインシデントの情報が示されます。電子メール セキュリティ アプライアンスでは、[送信メール ポリシー（Outgoing Mail Policies）] テーブルでイネーブルにした DLP 電子メール ポリシーを使用して、ユーザが送信した機密データを検出します。DLP ポリシーに違反する送信メッセージが発生するたびに、インシデントとして報告されます。

[DLP インシデント サマリー（DLP Incident Summary）] レポートを使用すると、次のような情報を取得できます。

- ユーザが送信した機密データの種類
- これらの DLP インシデントの重大度
- これらのメッセージのうち、配信されたメッセージの数
- これらのメッセージのうち、ドロップされたメッセージの数
- これらのメッセージの送信者

図 4-9　[メール（Email）] > [レポート（Reporting）] > [DLP サマリー（DLP Summary）] ページ



[DLP インシデント サマリー（DLP Incident Summary）] ページには次の 2 つのメイン セクションがあります。

- 重大度（[低（Low）]、[中（Medium）]、[高（High）]、[クリティカル（Critical）]）別の上位 DLP インシデントおよびポリシーの一致数を集約する DLP インシデントのトレンド グラフ
- [DLP インシデントの詳細（DLP Incident Details）] リスト

表 4-9　[メール（Email）] > [レポート（Reporting）] > [DLP インシデント サマリー（DLP Incident Summary）] ページの詳細

セクション	説明
時間範囲（Time Range）（ドロップダウン リスト）	1 ～ 90 日間またはカスタム日数範囲を指定できるドロップダウン リスト。時間範囲の詳細と実際のニーズに合わせたカスタマイズについては、「レポートの時間範囲の選択」（P.3-4）を参照してください。
重大度別上位インシデント（Top Incidents by Severity）	重大度別の上位 DLP インシデント。

表 4-9　[メール（Email）] > [レポート（Reporting）] > [DLP インシデント サマリー（DLP Incident Summary）] ページの詳細 （続き）

セクション	説明
インシデント サマリー（Incident Summary）	各電子メール アプライアンスの送信メール ポリシーで現在イネーブルになっている DLP ポリシーは、[DLP インシデント サマリー（DLP Incident Summary）] ページの下部にある [DLP インシデントの詳細（DLP Incident Details）] インタラクティブ テーブルに表示されます。詳細情報を表示するには、DLP ポリシーの名前をクリックします。
DLP ポリシー一致の上位（Top DLP Policy Matches）	一致している上位 DLP ポリシー。
DLP インシデントの詳細（DLP Incident Details）	[DLP インシデントの詳細（DLP Incident Details）] テーブルには、ポリシーごとの DLP インシデントの数に加えて、重大度レベル別の内訳、メッセージのいずれかがクリアに配信されたか、暗号化されて配信されたか、ドロップされたかが示されます。 [DLP インシデントの詳細（DLP Incident Details）] テーブルの詳細については、「[DLP インシデントの詳細（DLP Incident Details）] テーブル」（P.4-33）を参照してください。

ポリシーによって検出された DLP インシデントに関する詳細情報を表示するには、DLP ポリシーの名前をクリックします。この方法を使用すると、ポリシーによって検出された、機密データを含むメールを送信したユーザのリストを取得できます。

[DLP インシデントの詳細（DLP Incident Details）] テーブル

[DLP インシデントの詳細（DLP Incident Details）] テーブルは、ポリシーごとの DLP インシデントの数に加えて、重大度レベル別の内訳、メッセージのいずれかがクリアに配信されたか、暗号化されて配信されたか、ドロップされたかが表示されるインタラクティブ テーブルです。データをソートするには、カラム見出しをクリックします。

このテーブルに表示される DLP ポリシーの詳細情報を検索するには、DLP ポリシー名をクリックして、その DLP ポリシーのページを表示します。詳細については、「[DLP ポリシー詳細（DLP Policy Detail）] ページ」（P.4-33）を参照してください。

アクセス権限でメッセージ トラッキング データを表示できる場合、このレポートに記載されるメッセージに対するメッセージ トラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。

[DLP ポリシー詳細（DLP Policy Detail）] ページ

[DLP インシデントの詳細（DLP Incident Details）] テーブルで DLP ポリシーの名前をクリックした場合、その結果として表示される [DLP インシデントの詳細（DLP Incident Details）] ページにそのポリシーに関する DLP インシデント データが表示されます。このページには、重大度に基づいた DLP インシデントのグラフが表示されます。

このページには、DLP ポリシーに違反したメッセージを送信した各内部ユーザを表示する、ページ下部にある [送信者別インシデント（Incidents by Sender）] テーブルも含まれます。このテーブルには、このポリシーに関するユーザごとの DLP インシデントの総数に加えて、重大度レベル別の内訳、メッ

セージのいずれかがクリアに配信されたか、暗号化されて配信されたか、ドロップされたかが示されます。[送信者別インシデント（Incidents by Sender）] テーブルを使用すると、組織の機密データをネットワーク外のユーザに送信した可能性のあるユーザを検索できます。

インシデント詳細ページの送信者名をクリックすると [内部ユーザ（Internal Users）] ページが開きます。詳細については、「[内部ユーザ（Internal Users）] ページ」（P.4-28）を参照してください。

[コンテンツ フィルタ（Content Filters）] ページ

[メール（Email）] > [レポート（Reporting）] > [コンテンツ フィルタ（Content Filters）] ページには、送受信コンテンツ フィルタの上位一致（最も多くのメッセージに一致したコンテンツ フィルタ）に関する情報が表示されます。このページでは、データが棒グラフとリストの形式でも表示されます。[コンテンツ フィルタ（Content Filters）] ページを使用すると、コンテンツ フィルタごとまたはユーザごとに企業ポリシーを確認し、次の情報を取得できます。

- 受信メールまたは送信メールによってトリガーされた回数の最も多いコンテンツ フィルタ
- 特定のコンテンツ フィルタをトリガーしたメールを送受信した上位ユーザ

特定のフィルタの詳細情報を表示するには、フィルタ名をクリックします。[コンテンツ フィルタの詳細（Content Filter Details）] ページが表示されます。[コンテンツ フィルタの詳細（Content Filter Details）] ページの詳細については、「[コンテンツ フィルタの詳細（Content Filter Details）] ページ」（P.4-34）を参照してください。

アクセス権限でメッセージ トラッキング データを表示できる場合、このレポートに記載されるメッセージに対するメッセージ トラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。

[コンテンツ フィルタ（Content Filters）] ページから、PDF を生成したり、raw データを CSV ファイルにエクスポートしたりすることもできます。ファイルを印刷またはエクスポートする方法の詳細については、「[メール レポート（Email Reporting）] ページの概要」（P.4-7）を参照してください。

（注）　[コンテンツ フィルタ（Content Filter）] ページのスケジュール設定されたレポートを生成できます。「電子メール レポートのスケジュール設定」（P.4-56）を参照してください。

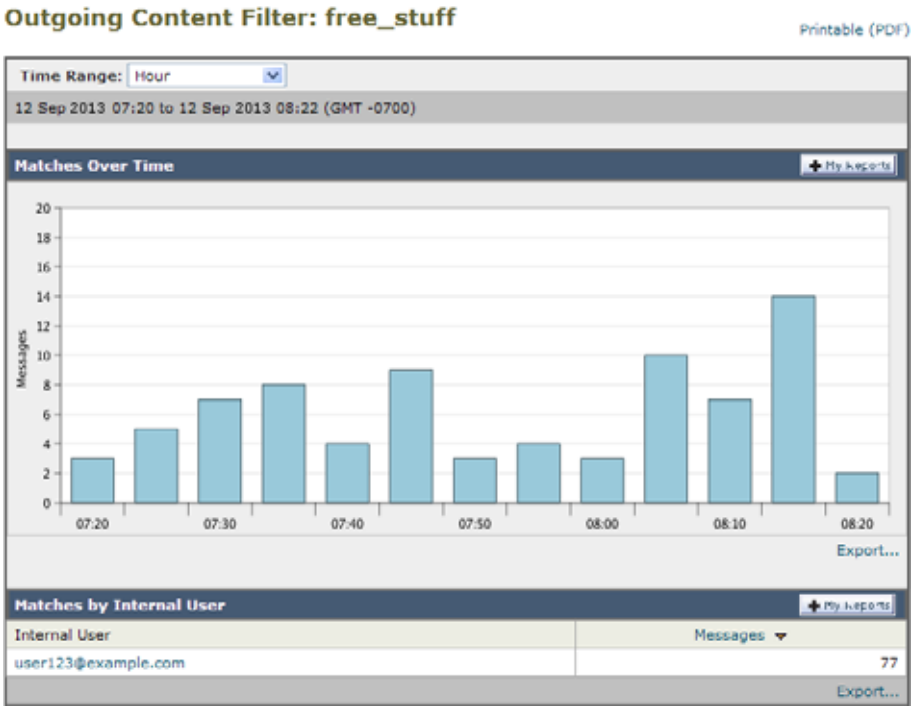
[コンテンツ フィルタの詳細（Content Filter Details）] ページ

[コンテンツ フィルタの詳細（Content Filter Details）] ページには、このフィルタの経時的な一致および内部ユーザ別の一致が表示されます。

[内部ユーザ別の一致（Matches by Internal User）] セクションで、内部ユーザ（電子メール アドレス）の詳細ページを表示するユーザ名をクリックします。詳細については、「[内部ユーザの詳細（Internal User Details）] ページ」（P.4-30）を参照してください。

アクセス権限でメッセージ トラッキング データを表示できる場合、このレポートに記載されるメッセージに対するメッセージ トラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。

図 4-10　[コンテンツ フィルタの詳細（Content Filters Details）] ページ

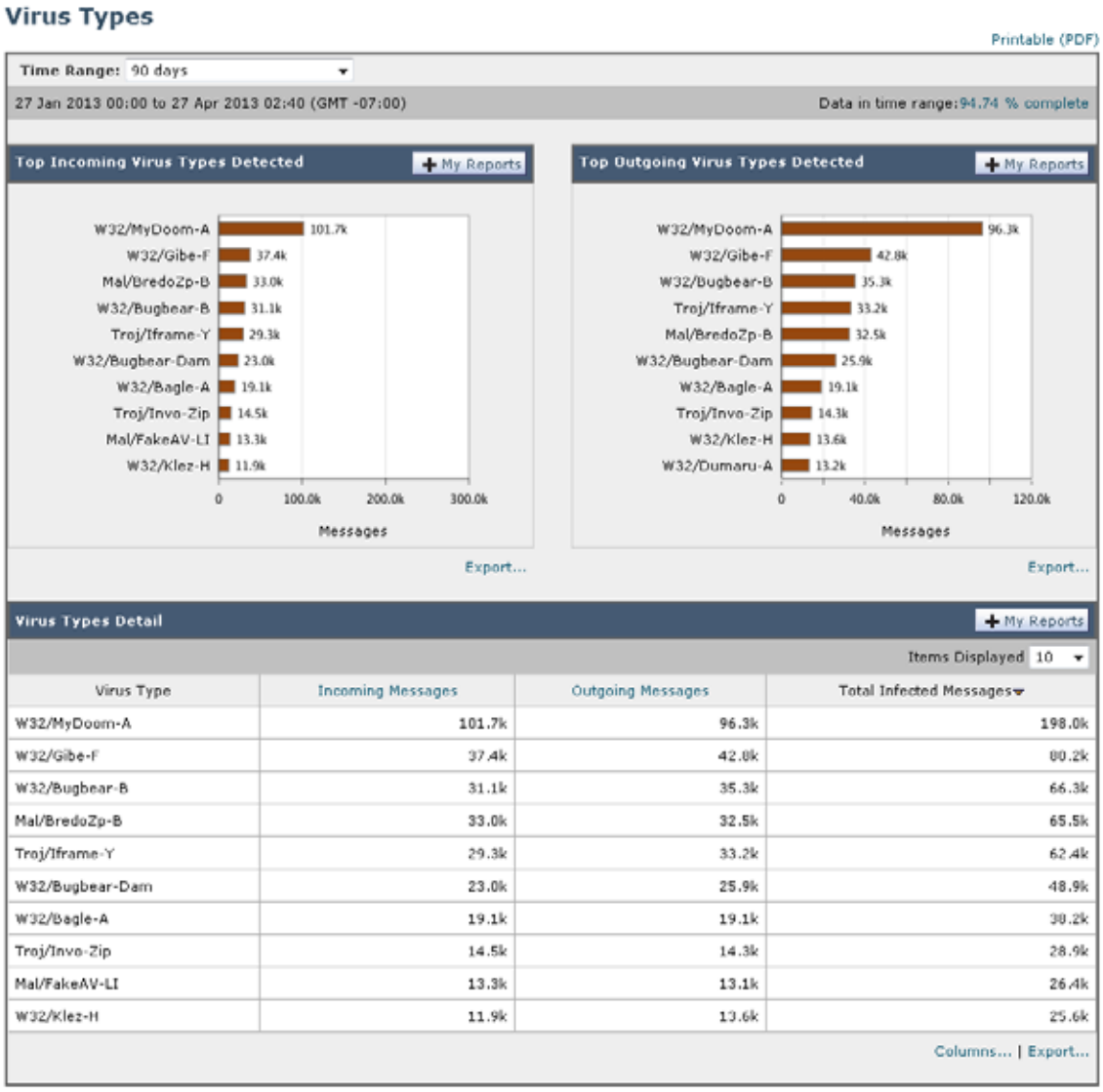


[ウイルス タイプ（Virus Types）] ページ

[メール（Email）] > [レポート（Reporting）] > [ウイルス タイプ（Virus Types）] ページでは、ネットワークで送受信されたウイルスの概要が示されます。[ウイルス タイプ（Virus Types）] ページには、電子メール セキュリティ アプライアンスで稼働し、セキュリティ管理アプライアンスに表示されるウイルス スキャン エンジンによって検出されたウイルスが表示されます。このレポートを使用して、特定のウイルスに対して処置を行います。たとえば、PDF ファイルに組み込まれることが判明しているウイルスを大量に受信している場合、PDF が添付されているメッセージを隔離するフィルタ アクションを作成することが推奨されます。

（注）　ウイルス感染フィルタでは、ユーザが介入することなく、これらの種類のウイルスに感染したメッセージを隔離することができます。

図 4-11　[メール（Email）] > [レポート（Reporting）] > [ウイルス タイプ（Virus Types）] ページ



複数のウイルス スキャン エンジンを実行している場合、[ウイルス タイプ（Virus Types）] ページには、イネーブルになっているすべてのウイルス スキャン エンジンの結果が含まれます。ページに表示されるウイルスの名前は、ウイルス スキャン エンジンによって判定された名前です。複数のスキャン エンジンが 1 つのウイルスを検出した場合、同じウイルスに対して複数のエントリが存在する可能性があります。

表 4-10　[メール（Email）] > [レポート（Reporting）] > [ウイルス タイプ（Virus Types）] ページの詳細

セクション	説明
時間範囲（Time Range）（ドロップダウン リスト）	1 ～ 90 日間またはカスタム日数範囲を指定できるドロップダウン リスト。時間範囲の詳細と実際のニーズに合わせたカスタマイズについては、「レポートの時間範囲の選択」（P.3-4）を参照してください。
検出した受信ウイルス タイプの上位（Top Incoming Virus Types Detected）	このセクションでは、ネットワークに送信されたウイルスのチャート ビューが表示されます。
検出した送信ウイルス タイプの上位（Top Outgoing Virus Types Detected）	このセクションでは、ネットワークから送信されたウイルスのチャート ビューが表示されます。
ウイルス タイプ詳細（Virus Types Detail）	各ウイルス タイプの詳細が表示されるインタラクティブ テーブル。

（注）　ウイルスに感染したメッセージをネットワークに送信したホストを表示するには、[受信メール（Incoming Mail）] ページに移動し、同じ報告期間を指定して、ウイルス陽性別にソートします。同様に、ネットワーク内でウイルス陽性の電子メールを送信した IP アドレスを表示するには、[送信メッセージ送信者（Outgoing Senders）] ページを表示し、ウイルス陽性メッセージ別にソートします。

[ウイルス タイプ（Virus Types）] ページから、PDF を生成したり、raw データを CSV ファイルにエクスポートしたりすることもできます。ファイルを印刷またはエクスポートする方法の詳細については、「[メール レポート（Email Reporting）] ページの概要」（P.4-7）を参照してください。

（注）　[ウイルス タイプ（Virus Types）] ページのスケジュール設定されたレポートを生成できます。「電子メール レポートのスケジュール設定」（P.4-56）を参照してください。

[TLS 接続（TLS Connections）] ページ

[メール（Email）] > [レポート（Reporting）] > [TLS 接続（TLS Connections）] ページには、メールの送受信に使用される TLS 接続の全体的な使用状況が表示されます。このレポートでは、TLS 接続を使用してメールを送信する各ドメインの詳細についても示されます。

[TLS 接続（TLS Connections）] ページを使用すると、次の情報を測定できます。

- 送受信接続による、全体的な TLS の使用割合
- TLS 接続に成功したパートナー
- TLS 接続に成功しなかったパートナー
- TLS 認証に問題のあるパートナー
- パートナーが TLS を使用したメールの全体的な割合

図 4-12　[TLS 接続レポート（TLS Connections Report）] ページ : [受信接続数（Incoming Connections）]

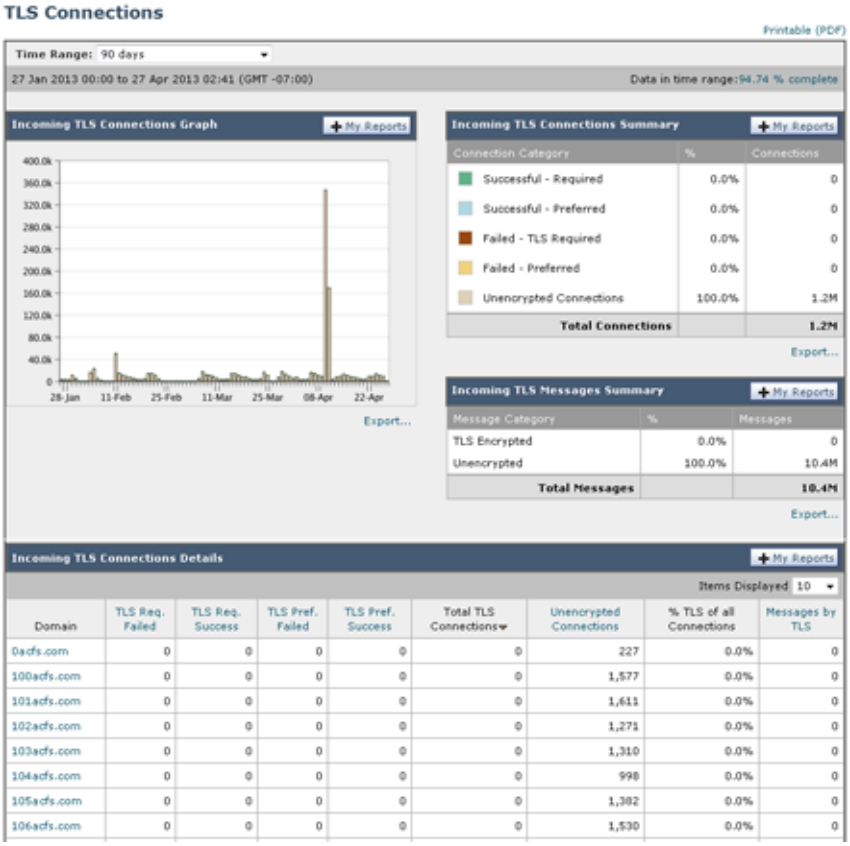


表 4-11　[メール（Email）] > [レポート（Reporting）] > [TLS 接続（TLS Connections）] ページの詳細

セクション	説明
時間範囲（Time Range）（ドロップダウン リスト）	1 ～ 90 日間またはカスタム日数範囲を指定できるドロップダウン リスト。時間範囲の詳細と実際のニーズに合わせたカスタマイズについては、「レポートの時間範囲の選択」（P.3-4）を参照してください。
受信 TLS 接続数グラフ（Incoming TLS Connections Graph）	グラフには、選択したタイム フレームに応じて、直近の 1 時間、1 日、または 1 週間における、受信 TLS の暗号化された接続および暗号化されない接続のビューが表示されます。
受信 TLS 接続数サマリー（Incoming TLS Connections Summary）	この表には、着信メッセージの総量、暗号化された / 暗号化されないメッセージの量、成功 / 失敗した受信 TLS 暗号化メッセージの量が表示されます。
受信 TLS メッセージ サマリー（Incoming TLS Message Summary）	この表には、着信メッセージの総量の概要が表示されます。
受信 TLS 接続数詳細（Incoming TLS Connections Details）	表には、暗号化されたメッセージを送受信するドメインの詳細が表示されます。各ドメインについて、接続の総数、送信されたメッセージ、および成功 / 失敗した TLS 接続の数を表示できます。各ドメインについて、成功 / 失敗した接続の割合を表示することもできます。

表 4-11　[メール（Email）] > [レポート（Reporting）] > [TLS 接続（TLS Connections）] ページの詳細 （続き）

セクション	説明
送信 TLS 接続数グラフ（Outgoing TLS Connections Graph）	グラフには、選択したタイム フレームに応じて、直近の 1 時間、1 日、または 1 週間における、送信 TLS の暗号化された接続および暗号化されない接続のビューが表示されます。
送信 TLS 接続数サマリー（Outgoing TLS Connections Summary）	この表には、発信メッセージの総量、暗号化された/暗号化されないメッセージの量、成功/失敗した送信 TLS 暗号化メッセージの量が表示されます。
Outgoing TLS Message Summary	この表には、発信メッセージの総量が表示されます。
送信 TLS 接続数詳細（Outgoing TLS Connections Details）	表には、暗号化されたメッセージを送受信するドメインの詳細が表示されます。各ドメインについて、接続の総数、送信されたメッセージ、成功/失敗した TLS 接続の数、および最後の TLS ステータスを表示できます。各ドメインについて、成功/失敗した接続の割合を表示することもできます。

[受信 SMTP 認証（Inbound SMTP Authentication）] ページ

[受信 SMTP 認証（Inbound SMTP Authentication）] ページには、クライアント証明書の使用情報、および電子メール セキュリティ アプライアンスとユーザのメール クライアント間で SMTP セッションを認証するための SMTP AUTH コマンドが表示されます。アプライアンスは、証明書または SMTP AUTH コマンドを受け入れると、メール クライアントへの TLS 接続を確立します。クライアントはこの接続を使用してメッセージを送信します。アプライアンスは、これらの試行をユーザ単位で追跡できないため、レポートには、ドメイン名とドメイン IP アドレスに基づいて SMTP 認証の詳細が表示されます。

次の情報を確認するには、このレポートを使用します。

- SMTP 認証を使用している着信接続の総数
- クライアント証明書を使用している接続の数
- SMTP AUTH を使用している接続の数
- SMTP 認証を使用しようとして、接続が失敗したドメイン
- SMTP 認証が失敗した一方で、フォールバックを正常に使用している接続の数

[受信 SMTP 認証（Inbound SMTP Authentication）] ページには、受信した接続のグラフ、SMTP 認証接続を試行したメール受信者のグラフ、および接続の認証試行の詳細を含むテーブルが表示されます。

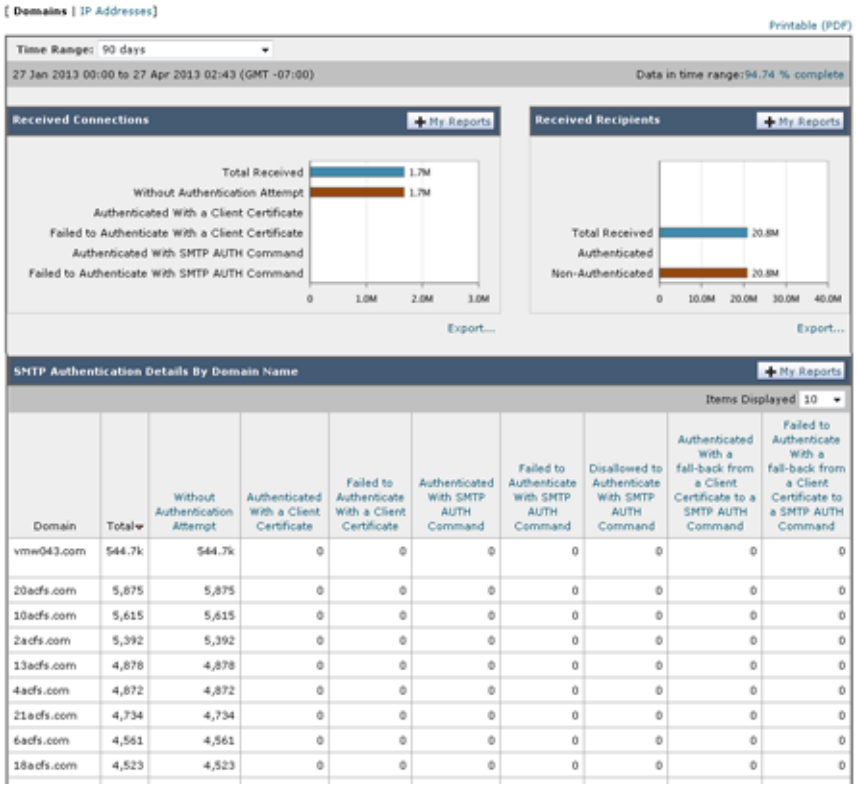
[受信した接続（Received Connections）] グラフでは、指定した時間範囲において SMTP 認証を使用して接続を認証しようとしたメール クライアントの着信接続が示されます。このグラフには、アプライアンスが受信した接続の総数、SMTP 認証を使用して認証を試行しなかった接続の数、クライアント証明書を使用して認証が失敗および成功した接続の数、SMTP AUTH コマンドを使用して認証が失敗および成功した接続の数が表示されます。

[受信した受信者（Received Recipients）] グラフには、SMTP 認証を使用して、メッセージを送信するために電子メール セキュリティ アプライアンスへの接続を認証しようとしたメール クライアントを所有する受信者の数が表示されます。このグラフでは、接続が認証された受信者の数、および接続が認証されなかった受信者の数も示されます。

[SMTP 認証の詳細（SMTP Authentication details）] テーブルには、メッセージを送信するために電子メール セキュリティ アプライアンスへの接続を認証しようとしたユーザを含むドメインの詳細が表示されます。ドメインごとに、クライアント証明書を使用した接続試行（成功または失敗）の数、SMTP

AUTH コマンドを使用した接続試行（成功または失敗）の数、およびクライアント証明書接続試行が失敗した後、SMTP AUTH にフェールバックした接続の数を表示できます。ページ上部のリンクを使用して、ドメイン名またはドメイン IP アドレス別にこの情報を表示できます。

図 4-13　[受信 SMTP 認証（Inbound SMTP Authentication）] ページ



[レート制限（Rate Limits）] ページ

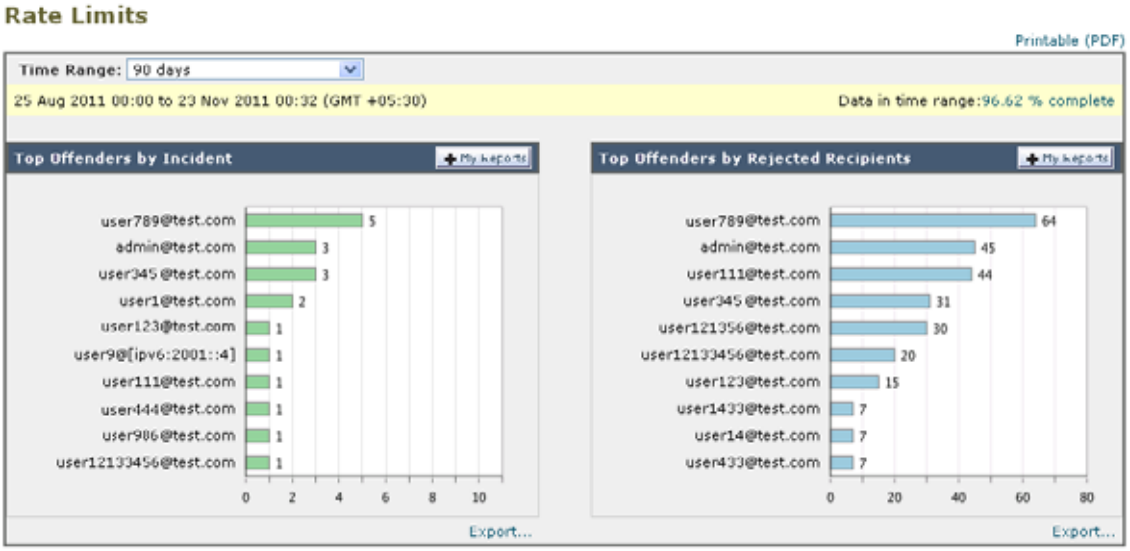
エンベロープ送信者ごとのレート制限を使用すると、メール送信者アドレスに基づいて、個々の送信者からの時間間隔ごとの電子メール メッセージ受信者数を制限できます。[レート制限（Rate Limits）] レポートには、この制限を最も上回った送信者が表示されます。

このレポートは、以下を特定する場合に役立ちます。

- 大量のスパムを送信するために使用される可能性のある信用できないユーザ アカウント
- 通知、アラート、自動報告などに電子メールを使用する組織内の制御不能アプリケーション
- 内部請求やリソース管理のために、組織内で電子メールを過剰に送信している送信元
- スパムとは見なされないが、大量の着信電子メール トラフィックを送信している送信元

内部送信者に関する統計情報を含む他のレポート（[内部ユーザ（Internal Users）]、[送信メッセージ送信者（Outgoing Senders）] など）では、送信されたメッセージの数のみ計測されます。これらのレポートでは、少数のメッセージを多数の受信者に送信した送信者は識別されません。

図 4-14　[レート制限（Rate Limits）] ページ



[上位攻撃者 (インシデント別) （Top Offenders by Incident）] チャートには、設定済み制限よりも多くの受信者にメッセージを最も頻繁に送信しようとしたエンベロープ送信者が表示されます。各試行が 1 インシデントに相当します。このチャートでは、すべてのリスナーからのインシデント数が集計されます。

[上位攻撃者（拒否した受信者別）（Top Offenders by Rejected Recipients）] チャートには、設定済みの制限を上回る、最も多くの受信者にメッセージを送信したエンベロープ送信者が表示されます。このチャートでは、すべてのリスナーからの受信者数が集計されます。

[エンベロープ送信者のレート制限（Rate Limit for Envelope Senders）] 設定を含む [レート制限（Rate Limiting）] 設定は、電子メール セキュリティ アプライアンス の [メール ポリシー（Mail Policies）] > [メール フロー ポリシーの設定（Mail Flow Policies settings）] で行います。レート制限の詳細については、ご使用の電子メール セキュリティ アプライアンスのマニュアルまたはオンラインヘルプを参照してください。

[アウトブレイク フィルタ（Outbreak Filters）] ページ

[メール（Email）] > [レポート（Reporting）] > [アウトブレイク フィルタ（Outbreak Filters）] ページには、最近の発生状況やウイルス感染フィルタによって隔離されたメッセージに関する情報が表示されます。このページを使用すると、攻撃対象となったウイルス、詐欺、およびフィッシング攻撃に対する防御をモニタできます。

[アウトブレイク フィルタ（Outbreak Filters）] ページを使用して、次の情報を入手できます。

- ウイルス感染フィルタ ルールによって隔離されたメッセージの数と使用されたルール
- ウイルスの発生に対する、ウイルス感染機能のリード タイム
- グローバル ウイルス感染発生と比較したローカル ウイルスの発生状況

[タイプ別脅威（Threats By Type）] セクションには、アプライアンスで受信したさまざまな種類の脅威メッセージが表示されます。[脅威サマリー（Threat Summary）] セクションには、ウイルス、フィッシング攻撃、および詐欺によるメッセージの内訳が表示されます。

[過去 1 年間のアウトブレイク サマリー（Past Year Outbreak Summary）] には、前年のグローバルな発生およびローカルでの発生が表示されるので、ローカル ネットワーク トレンドとグローバル トレンドを比較できます。グローバル発生リストは、すべての発生（ウイルスとウイルス以外の両方）の上位集合です。これに対して、ローカル発生は、お使いのアプライアンスに影響を与えたウイルス発生に限定されています。ローカル発生データには非ウイルス性の脅威は含まれません。グローバル感染発生データは、アウトブレイク隔離で現在設定されているしきい値を超えた、Cisco IronPort Threat Operations Center によって検出されたすべての感染を表します。ローカル感染発生データは、アウトブレイク隔離で現在設定されているしきい値を超えた、このアプライアンスで検出されたすべてのウイルス感染を表します。[ローカル保護の合計時間（Total Local Protection Time）] は、Cisco IronPort Threat Operations Center による各ウイルス感染の検出と、主要ベンダーによるアンチウイルス シグニチャの解放との時間差に常に基づいています。必ずしもすべてのグローバル発生が、お使いのアプライアンスに影響を与えるわけではありません。「--」値は、保護時間が存在しないか、アンチウイルス ベンダーからシグニチャ時間を入手できないことを示します（一部のベンダーは、シグニチャ時間を報告しません）。これは、保護時間がゼロであることを示すのではなく、保護時間の算出に必要な情報を入手できないことを示します。

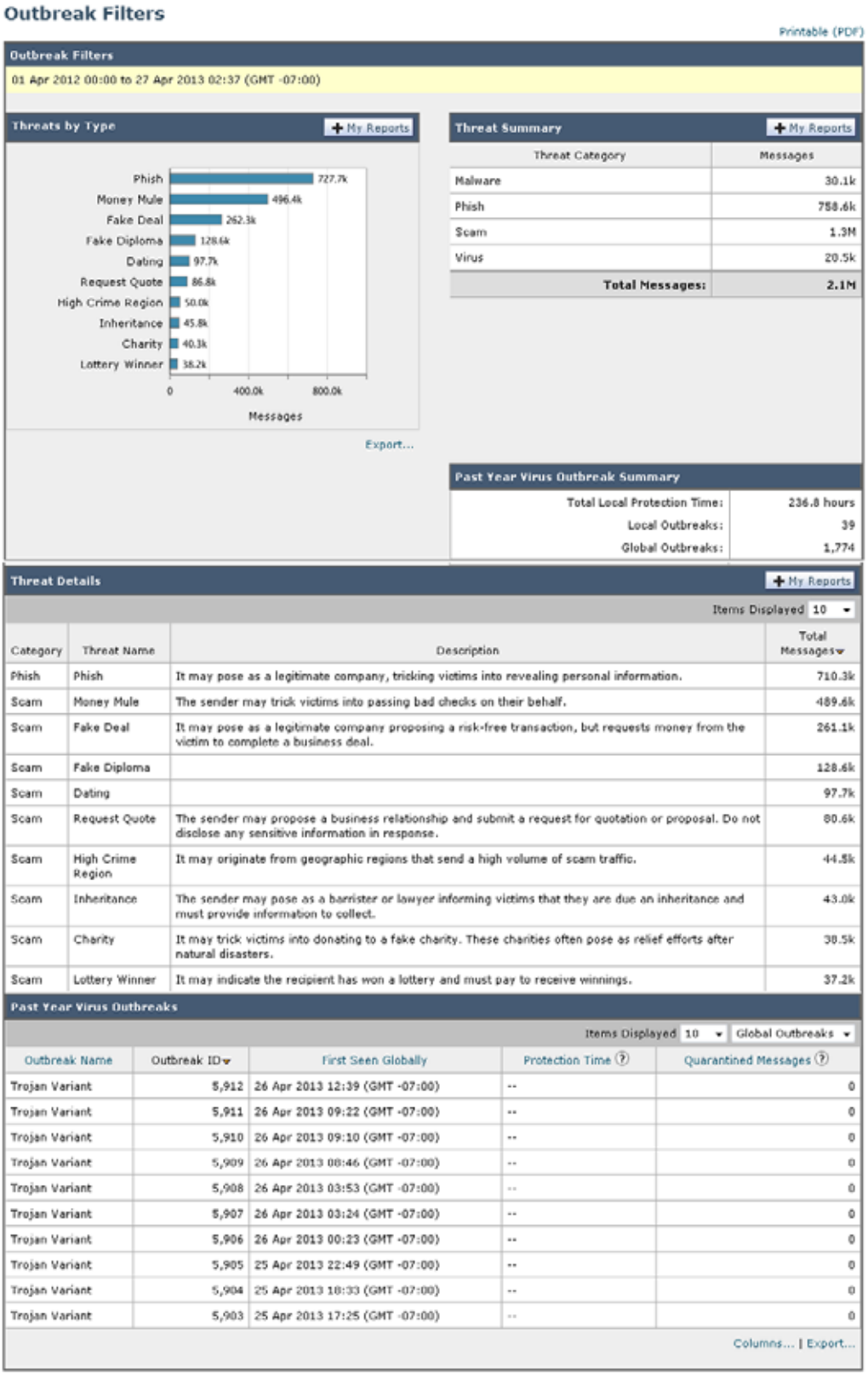
[隔離されたメッセージ（Quarantined Messages）] セクションでは、感染フィルタの隔離状況の概要が示されます。これは、感染フィルタが捕捉した潜在的な脅威メッセージの数を把握するのに役立つ尺度です。隔離されたメッセージは、解放時に集計されます。通常、アンチウイルス ルールおよびアンチスパム ルールが使用可能になる前に、メッセージが隔離されます。メッセージが解放されると、アンチウイルス ソフトウェアおよびアンチスパム ソフトウェアによってスキャンされ、ウイルス陽性か、クリーンかを判定されます。感染トラッキングの動的性質により、メッセージが隔離領域内にあるときでも、メッセージの隔離ルール（および関連付けられる発生）が変更される場合があります。（隔離領域に入った時点ではなく）解放時にメッセージを集計することにより、件数の変動による混乱を防ぎます。

[脅威の詳細（Threat Details）] リストには、脅威のカテゴリ（ウイルス、詐欺、またはフィッシング）、脅威名、脅威の説明、識別されたメッセージ数など、特定の発生についての情報が表示されます。ウイルス感染発生の場合、[過去 1 年間のウイルス アウトブレイク（Past Year Virus Outbreaks）] に感染名、および ID、ウイルス感染が最初にグローバルに発見された時刻と日付、感染フィルタによって保護された時刻、および隔離されたメッセージ数が含まれます。左側のメニューを使用して、グローバル発生またはローカル発生のいずれか、および表示するメッセージの数を選択できます。カラム ヘッダーをクリックすることにより、表示をソートできます。

[最初にグローバルで確認した日時（First Seen Globally）] の時刻は、世界最大規模の電子メールおよび Web トラフィック モニタリング ネットワークである SenderBase からのデータに基づき、Cisco IronPort Threat Operations Center によって決定されます。[保護時間（Protection Time）] は、Cisco IronPort Threat Operations Center による各脅威の検出と、主要ベンダーによるアンチウイルス シグニチャの解放との時間差に常に基づいています。

「--」値は、保護時間が存在しないか、アンチウイルス ベンダーからシグニチャ時間を入手できないことを示します（一部のベンダーは、シグニチャ時間を報告しません）。保護時間がゼロであることを示しているわけではありません。むしろ、保護時間の算出に必要な情報を入手できないことを意味します。

図 4-15　[アウトブレイク フィルタ（Outbreak Filters）] ページ



（注）　[アウトブレイク フィルタ（Outbreak Filters）] ページにテーブルが正しく表示されるためには、セキュリティ管理アプライアンスが downloads.cisco.com と通信できる必要があります。

[システム容量（System Capacity）] ページ

[メール（Email）] > [レポート（Reporting）] > [システム容量（System Capacity）] ページでは、作業キュー内のメッセージ数、着信および発信メッセージ（量、サイズ、件数）、全体的な CPU 使用率、機能別の CPU 使用率、メモリ ページ スワップ情報などシステム負荷の詳細が示されます。

[システム容量（System Capacity）] ページを使用すると、次の情報を確認できます。

- 電子メール セキュリティ アプライアンスが推奨キャパシティをいつ超えたか。これによって、設定の最適化または追加アプライアンスが、いつ必要になったかがわかります。
- キャパシティの問題が今後発生する可能性を示すシステム挙動の過去のトレンド。
- トラブルシューティングのために、システムが最もリソースを使用している部分を識別します。

Monitor your 電子メール セキュリティ アプライアンスをモニタして、キャパシティがメッセージ量に適したものになっているかを確認します。量は、時間の経過に伴って必ず増加しますが、適切にモニタリングしていれば、追加キャパシティまたは設定変更を予防的に適用できます。システム キャパシティをモニタする最も効果的な方法は、全体的な量、作業キュー内のメッセージ、およびリソース節約モードのインシデントを追跡することです。

- **量**：「正常」なメッセージ量と環境内での「通常」のスパイクを把握することが重要です。経時的にこのデータを追跡して、量の増加を測定します。[受信メール（Incoming Mail）] ページおよび [送信メール（Outgoing Mail）] ページを使用すると、経時的に量を追跡できます。詳細については、「[システム容量（System Capacity）] : [受信メール（Incoming Mail）]」（P.4-46）および「[システム容量（System Capacity）] : [送信メール（Outgoing Mail）]」（P.4-47）を参照してください。
- **作業キュー**：作業キューは、スパム攻撃の吸収とフィルタリングを行い、非スパム メッセージの異常な増加を処理する、「緩衝装置」として設計されています。ただし、作業キューは負荷のかかっているシステムを示す指標でもあります。長く、頻繁な作業キューのバックアップは、キャパシティの問題を示している可能性があります。[システム容量（System Capacity）] : [ワークキュー（Workqueue）] ページを使用すると、作業キュー内のアクティビティを追跡できます。詳細については、「[システム容量（System Capacity）] : [ワークキュー（Workqueue）]」（P.4-45）を参照してください。
- **リソース節約モード**：アプライアンスがオーバーロードになると、リソース節約モード（RCM）になり、CRITICAL システム アラートが送信されます。このモードは、デバイスを保護し、未処理分のメッセージを処理できるように設計されています。お使いのアプライアンスは、頻繁に RCM になるのではなく、メール量が非常に多い場合または異常に増加した場合にのみ RCM になる必要があります。頻繁な RCM アラートは、システムがオーバーロードになりつつあることを示している可能性があります。RCM は、[システム容量（System Capacity）] ページでは追跡できません。

[システム容量（System Capacity）] ページに表示されるデータの解釈方法

[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。

- Day レポート：Day レポートでは、時間テーブルを照会し、24 時間の間に 1 時間ごとにアプライアンスが受信したクエリー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。これは正確な数値です。

- Month レポート : Month レポートでは、30 日間または 31 日間（その月の日数に応じる）の日テーブルを照会し、30 日間または 31 日間の正確なクエリー数を表示します。これも正確な数値です。

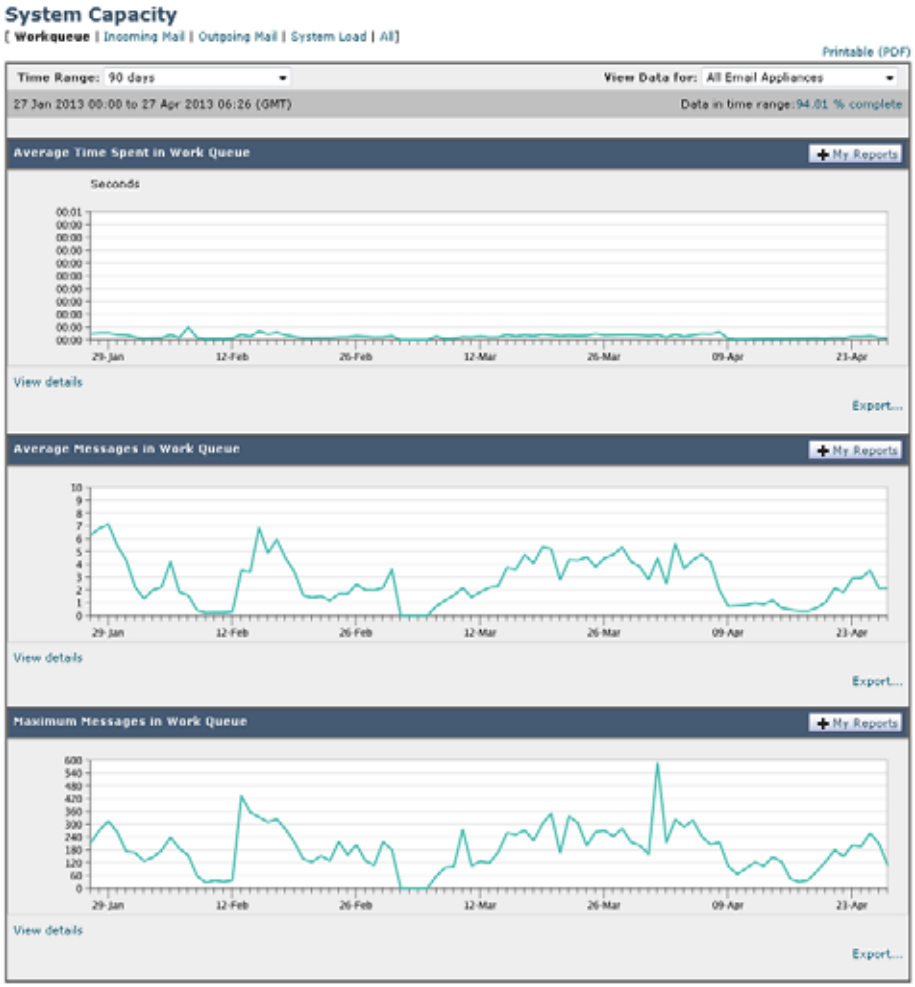
[システム容量（System Capacity）] ページの [最大（Maximum）] 値インジケータは、指定された期間の最大値を示します。[平均（Average）] 値は指定された期間のすべての値の平均です。集計期間は、レポートに対して選択された間隔に応じて異なります。たとえば、月単位のチャートの場合は、日付ごとの [平均（Average）] 値と [最大（Maximum）] 値を表示することができます。

特定のグラフの [詳細表示（View Details）] リンクをクリックすると、個々の電子メール セキュリティ アプライアンスのデータおよびセキュリティ管理アプライアンスに接続されたアプライアンスのデータ全体が表示されます。

[システム容量（System Capacity）] : [ワークキュー（Workqueue）]

[システム容量（System Capacity）] : [ワークキュー（Workqueue）] ページには、指定された期間の作業キュー内のメッセージ量が表示されます。また、同じ期間の作業キュー内の最大メッセージも表示されます。日、週、月、または年のデータを表示することもできます。[ワークキュー（Workqueue）] グラフにおける不定期のスパイクは、正常であり、発生する可能性があります。スパイクの発生頻度が高くなり、長期間にわたって同様の状態が続く場合、キャパシティの問題を示している可能性があります。[ワークキュー（Workqueue）] ページを確認するときは、作業キュー バックアップの頻度を測定し、10,000 メッセージを超える作業キュー バックアップに注意することが推奨されます。

図 4-16　[システム容量（System Capacity）] : [ワークキュー（Workqueue）]



[システム容量（System Capacity）] : [受信メール（Incoming Mail）]

[システム容量（System Capacity）] : [受信メール（Incoming Mail）] ページには、着信接続、着信メッセージの総数、平均メッセージ サイズ、着信メッセージの総サイズが示されます。日、週、月、または年の結果を表示することもできます。ご自身の環境における通常のメッセージ量とスパイクのトレンドを理解しておくことが重要です。[システム容量（System Capacity）] : [受信メール（Incoming Mail）] ページを使用すると、経時的にメール量の増加を追跡し、システム キャパシティの計画を立てることができます。着信メール データと送信者プロファイル データを比較して、特定のドメインからネットワークに送信される電子メール メッセージの量のトレンドを表示することも推奨されます。

（注）　着信接続数の増加は、必ずしもシステム負荷に影響を与えるわけではありません。

図 4-17　[システム容量（System Capacity）] : [受信メール（Incoming Mail）]

[システム容量（System Capacity）] : [送信メール（Outgoing Mail）]

[システム容量（System Capacity）] : [送信メール（Outgoing Mail）] ページには、発信接続、発信メッセージの総数、平均メッセージ サイズ、発信メッセージの総サイズが示されます。日、週、月、または年の結果を表示することもできます。ご自身の環境における通常のメッセージ量とスパイクのトレンドを理解しておくことが重要です。[システム容量（System Capacity）] : [送信メール（Outgoing Mail）] ページを使用すると、経時的にメール量の増加を追跡し、システム キャパシティの計画を立てることができます。発信メール データと発信宛先データを比較して、特定のドメインまたは IP アドレスから送信される電子メール メッセージの量のトレンドを表示することも推奨されます。

図 4-18　[システム容量（System Capacity）] : [送信メール（Outgoing Mail）]

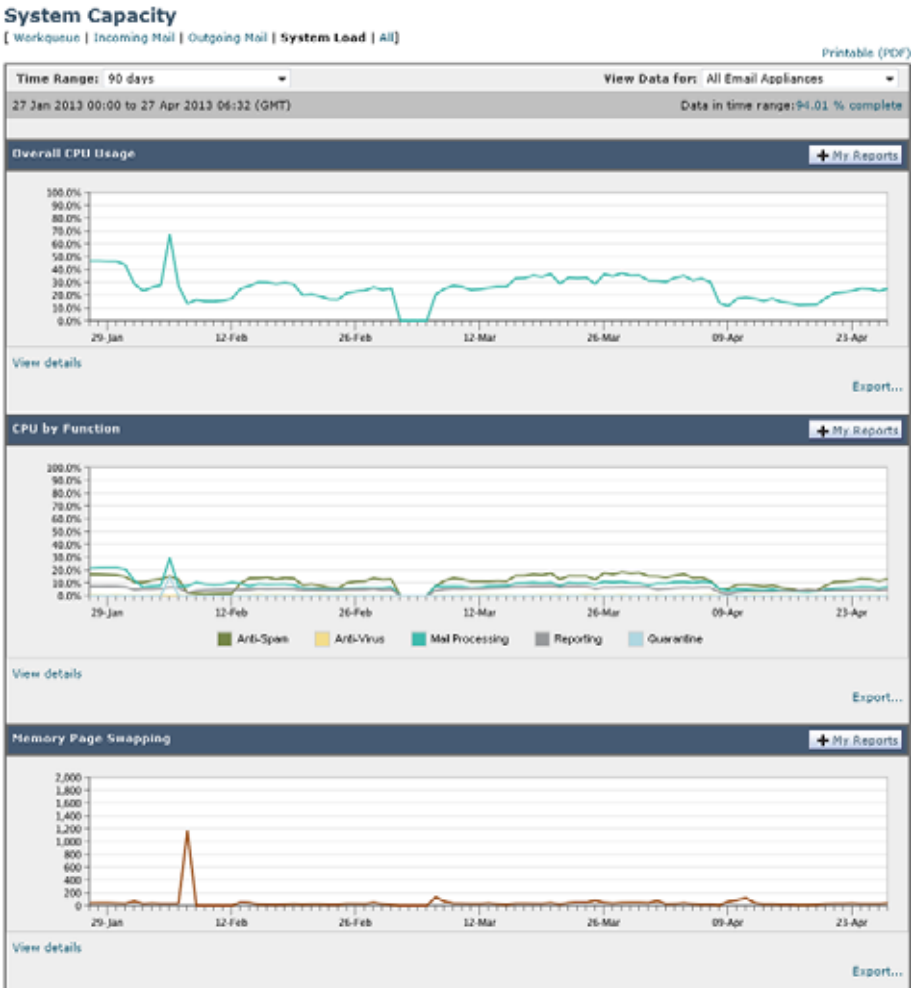
[システム容量（System Capacity）] : [システムの負荷（System Load）]

システム負荷レポートには、電子メール セキュリティ アプライアンスでの総 CPU 使用率が示されます。AsyncOS は、アイドル状態の CPU リソースを使用してメッセージ スループットを向上させるように最適化されています。CPU 使用率が高くても、必ずしもシステム キャパシティの問題を示すわけではありません。CPU 使用率が高く、かつ高ボリュームのメモリ ページ スワッピングが発生する場合、キャパシティの問題の可能性があります。このページでは、メール処理、スパムおよびウイルス エンジン、レポート、および隔離などさまざまな機能によって使用される CPU の量を表示するグラフ

も示されます。機能別 CPU のグラフは、システム上で最も多くのリソース使用する製品の領域を示す指標です。アプライアンスの最適化が必要な場合、このグラフは、調整やディセーブル化の必要な機能を判断するのに役立ちます。

メモリ ページ スワッピングのグラフは、システムによるディスクへのページングが必要な頻度を示します（KB/秒単位）。

図 4-19　[システム容量（System Capacity）] : [システムの負荷（System Load）]



メモリ ページ スワッピングに関する注意事項

システムは、定期的にメモリをスワップするように設計されているので、一部のメモリ スワッピングは起こり得るものであり、アプライアンスの問題を示すものではありません。システムが *常に* 高ボリュームのメモリ スワッピングを行う場合以外は、メモリ スワッピングは正常であり、起こり得る挙動です（特に C150 アプライアンスの場合）。たとえば、図 4-20 に、高ボリュームのメモリ スワッピングを常に行うシステムを示します。パフォーマンスを向上させるには、ネットワークにシスコ コンテンツ セキュリティ アプライアンスを追加するか、設定を調整して、最大のスループットを確保することが必要な場合もあります。

図 4-20　[システム容量（System Capacity）] : [システムの負荷（System Load）]（高負荷時のシステム）

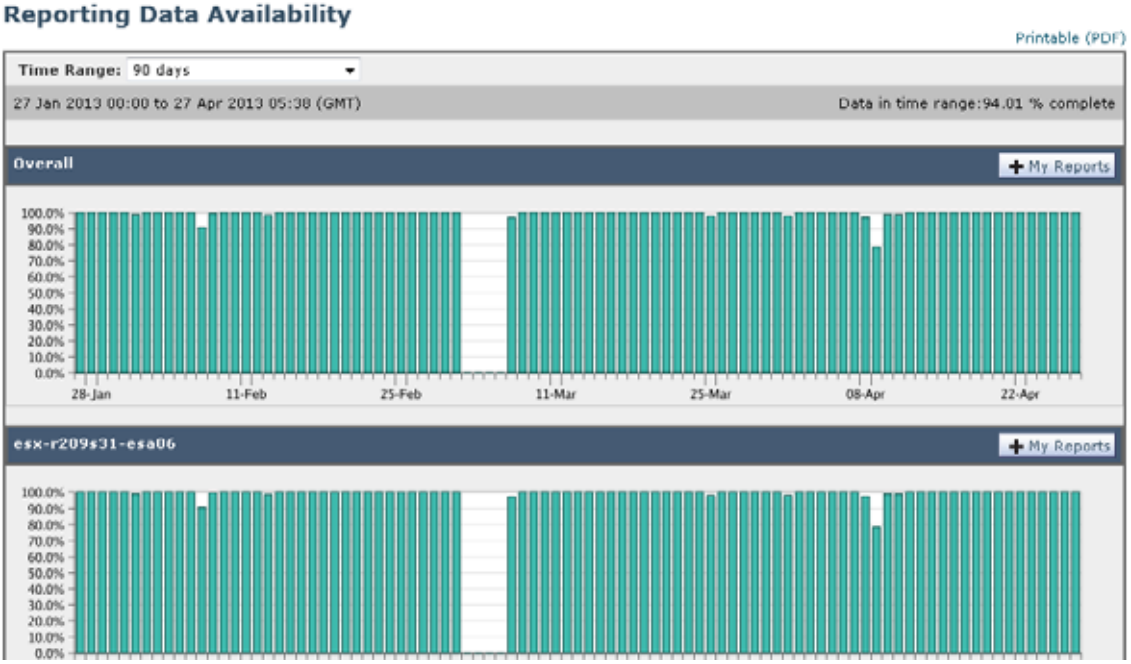
[システム容量（System Capacity）] : [すべて（All）]

[すべて（All）] ページでは、これまでのすべてのシステム キャパシティ レポートを単一のページに統合し、さまざまなレポート同士の関係を表示することができます。たとえば、過剰なメモリ スワッピングの発生と同時期にメッセージ キューが高いことを確認できます。これは、キャパシティの問題の兆候である可能性があります。このページを PDF ファイルとして保存し、後で参照するために（またはサポート スタッフと共有するために）システム パフォーマンスのスナップショットを保存することが推奨されます。

[有効なレポート データ（Reporting Data Availability）] ページ

[メール（Email）] > [レポート（Reporting）] > [有効なレポート データ（Reporting Data Availability）] ページでは、リソース使用率および電子メール トラフィックの障害のある場所がリアルタイムに表示されるようにデータを表示、更新およびソートできます。

図 4-21　[有効なメール レポート データ（Email Reporting Data Availability）] ページ



このページから、セキュリティ管理アプライアンスによって管理されるアプライアンス全体のデータ アベイラビリティを含めて、すべてのデータ リソース使用率および電子メール トラフィックに障害のある場所が表示されます。

このレポート ページから、特定のアプライアンスおよび時間範囲のデータ アベイラビリティを表示することもできます。

スケジュール設定された電子メール レポートとオンデマンドの電子メール レポートについて

使用可能なレポートの種類

特記のない限り、次のタイプの電子メール セキュリティ レポートは、スケジュール設定されたレポートおよびオンデマンド レポートとして使用できます。

- [コンテンツ フィルタ（Content Filters）]：このレポートには最大 40 のコンテンツ フィルタが表示されます。このページに表示されるその他の情報については、「[コンテンツ フィルタ（Content Filters）] ページ」（P.4-34）を参照してください。
- [DLP インシデント サマリー（DLP Incident Summary）]：このページに表示される情報については、「[DLP インシデント サマリー（DLP Incident Summary）] ページ」（P.4-31）を参照してください。
- [送信処理ステータス（Delivery Status）]：このレポート ページには、特定の受信者ドメインまた仮想ゲートウェイ アドレスへの配信の問題についての情報が表示されます。また、このページには、直近 3 時間以内にシステムによって配信されたメッセージの上位 20、50、または 100 の受信者ドメインのリストが表示されます。各統計情報のカラム見出しのリンクをクリックすることによって、最新のホスト ステータス、アクティブな受信者（デフォルト）、切断した接続、配信された受信者、ソフト バウンス イベント、およびハード バウンス受信者別にソートできます。電子

メール セキュリティ アプライアンスでの [送信処理ステータス（Delivery Status）] ページの役割の詳細については、お使いの電子メール セキュリティ アプライアンスのマニュアルまたはオンライン ヘルプを参照してください。

- [ドメイン毎のエグゼクティブ サマリー（Domain-Based Executive Summary）]：このレポートは電子メール レポーティングの [概要（Overview）] ページに基づき、指定されたドメインのグループに制限されます。表示される情報については、「[ドメイン毎のエグゼクティブ サマリー（Domain-Based Executive Summary）] レポート」（P.4-53）を参照してください。
- [エグゼクティブ サマリー（Executive Summary）]：このレポートは 電子メール レポーティングの [概要（Overview）] ページの情報に基づきます。表示される情報については、「[ドメイン毎のエグゼクティブ サマリー（Domain-Based Executive Summary）] レポート」（P.4-53）を参照してください。
- [受信メール サマリー（Incoming Mail Summary）]：このページに表示される情報については、「[受信メール（Incoming Mail）] ページ」（P.4-16）を参照してください。
- [内部ユーザのサマリー（Internal Users Summary）]：このページに表示される情報については、「[内部ユーザ（Internal Users）] ページ」（P.4-28）を参照してください。
- [アウトブレイク フィルタ（Outbreak Filters）]：このページに表示される情報については、「[アウトブレイク フィルタ（Outbreak Filters）] ページ」（P.4-41）を参照してください。
- [送信先（Outgoing Destinations）]：このページに表示される情報については、「[送信先（Outgoing Destinations）] ページ」（P.4-24）を参照してください。
- [送信メール サマリー（Outgoing Mail Summary）]：このページに表示される情報については、「[送信メッセージ送信者（Outgoing Senders）] ページ」（P.4-26）を参照してください。
- [送信メッセージ送信者（Outgoing Senders）]：このページに表示される情報については、「[送信メッセージ送信者（Outgoing Senders）] ページ」（P.4-26）を参照してください。
- [送信者グループ（Sender Groups）]：このページに表示される情報については、「[送信者グループ（Sender Groups）] レポート ページ」（P.4-23）を参照してください。
- [システム容量（System Capacity）]：このページに表示される情報については、「[システム容量（System Capacity）] ページ」（P.4-44）を参照してください。
- [TLS 接続（TLS Connections）]：このページに表示される情報については、「[TLS 接続（TLS Connections）] ページ」（P.4-37）を参照してください。
- [ウイルス タイプ（Virus Types）]：このページに表示される情報については、「[ウイルス タイプ（Virus Types）] ページ」（P.4-35）を参照してください。

時間範囲

各レポートは、前日、過去 7 日間、前月、過去の日（最大 250 日）、または過去の月（最大 12 ヵ月）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。

言語とロケール

（注）　個々のレポートに特定のロケールを使用して、PDF レポートをスケジュール設定したり、raw データを CSV ファイルとしてエクスポートしたりすることができます。[定期レポート（Scheduled Reports）] ページの言語ドロップダウン メニューでは、ユーザが現在選択しているロケールおよび言語で PDF レポートを表示またはスケジュールすることができます。「レポーティング データおよびトラッキング データの印刷およびエクスポート」（P.3-10）の重要な情報を参照してください。

アーカイブ済みレポートの保存

レポートの保存期間や、アーカイブ済みレポートがいつシステムから削除されるかについては、「アーカイブ電子メール レポートの表示と管理」（P.4-60）を参照してください。

その他のレポート タイプ

セキュリティ管理アプライアンスの [メール（Email）] > [レポート（Reporting）] セクションでは、次の 2 種類の特別なレポートを生成できます。

- [ドメイン毎のエグゼクティブ サマリー（Domain-Based Executive Summary）] レポート
- [エグゼクティブ サマリー（Executive Summary）] レポート

[ドメイン毎のエグゼクティブ サマリー（Domain-Based Executive Summary）] レポート

[ドメイン毎のエグゼクティブ サマリー（Domain-Based Executive Summary）] レポートには、ネットワーク内の 1 つまたは複数のドメインの着信および発信メッセージの概要が表示されます。これは [エグゼクティブ サマリー（Executive Summary）] レポートと似ていますが、レポート データが、指定したドメインで送受信されるメッセージに制限されます。[送信メール サマリー（Outgoing Mail Summary）] には、送信サーバの PTR（ポインタ レコード）のドメインが、指定したドメインに一致する場合にのみデータが表示されます。複数のドメインが指定されている場合、このアプライアンスはすべてのドメインのデータを 1 つのレポートに集約します。

サブドメインのレポートを生成するには、電子メール セキュリティ アプライアンスおよび セキュリティ管理アプライアンスのレポーティング システムで、親ドメインをセカンドレベル ドメインとして追加する必要があります。たとえば、example.com をセカンドレベル ドメインとして追加した場合、subdomain.example.com のようなサブドメインをレポーティングに使用できるようになります。セカンドレベル ドメインを追加するには、電子メール セキュリティ アプライアンスの CLI で **reportingconfig -> mailsetup -> tld** を実行し、セキュリティ管理アプライアンスの CLI で **reportingconfig -> domain -> tld** を実行します。

その他のスケジュール設定されたレポートとは異なり、[ドメイン毎のエグゼクティブ サマリー（Domain-Based Executive Summary）] レポートはアーカイブされません。

[ドメイン毎のエグゼクティブ サマリー（Domain-Based Executive Summary）] レポートとレピュテーション フィルタリングによってブロックされたメッセージ

レピュテーション フィルタリングによってブロックされたメッセージは作業キューに入らないため、AsyncOS はこれらのメッセージに対して、宛先ドメインを判定するための処理は行いません。アルゴリズムによって、ドメインごとに拒否されたメッセージ数が推定されます。ドメインごとのブロックされたメッセージの正確な数を知るには、メッセージ受信者レベル（RCPT TO）に達するまでセキュリティ管理アプライアンス HAT 拒否を遅延します。そうすることで、AsyncOS が着信メッセージから受信者データを収集できるようになります。電子メール セキュリティ アプライアンスで **listenerconfig**

-> setup コマンドを使用して拒否を遅らせることができます。ただし、このオプションはシステムのパフォーマンスに影響を及ぼす可能性があります。遅延した HAT 拒否の詳細については、ご使用の電子メール セキュリティ アプライアンスのマニュアルを参照してください。

（注）　セキュリティ管理アプライアンスで [ドメイン毎のエグゼクティブ サマリー（Domain-Based Executive Summary）] レポートの [レピュテーション フィルタによる停止（Stopped by Reputation Filtering）] の結果を表示するには、電子メール セキュリティ アプライアンスと セキュリティ管理アプライアンスの両方で **hat_reject_info** をイネーブルにする必要があります。

セキュリティ管理アプライアンスで **hat_reject_info** をイネーブルにするには、**reportingconfig > domain > hat_reject_info** コマンドを実行します。

[ドメイン毎のエグゼクティブ サマリー（Domain-Based Executive Summary）] レポートのドメインおよび受信者のリストの管理

コンフィギュレーション ファイルを使用して、[ドメイン毎のエグゼクティブ サマリー（Domain-Based Executive Summary）] レポートのドメインおよび受信者を管理できます。コンフィギュレーション ファイルは、アプライアンスのコンフィギュレーション ディレクトリに保存されるテキスト ファイルです。このファイルの行ごとに、個別のレポートが生成されます。これによって、大量のドメインおよび受信者を 1 つのレポートに含めることができ、複数のドメイン レポートを 1 つのコンフィギュレーション ファイルで定義できます。

コンフィギュレーション ファイルの各行には、ドメイン名のスペース区切りリストと、レポート受信者の電子メール アドレスのスペース区切りリストが含まれます。ドメイン名のリストと電子メール アドレスのリストはカンマで区切られます。subdomain.example.com のように、親ドメイン名の前にサブドメイン名とピリオドを追加すると、サブドメインを含めることができます。

次に示すファイルは、3 つのレポートを生成する 1 つのレポート コンフィギュレーション ファイルです。

```
yourdomain.com sampledomain.com, admin@yourdomain.com
sampledomain.com, admin@yourdomain.com user@sampledomain.com
subdomain.example.com mail.example.com, user@example.com
```

（注）　コンフィギュレーション ファイルと 1 つの名前付きレポートに定義された設定を使用して、複数のレポートを同時に生成することができます。たとえば、Bigfish という名前の会社が Redfish と Bluefish という名前の会社を買収し、Redfish と Bluefish のドメインを引き続き維持するとします。Bigfish 社は、個々のドメイン レポートに対応する 3 行が含まれるコンフィギュレーション ファイルを使用して 1 つの [ドメイン毎のエグゼクティブ サマリー（Domain-Based Executive Summary）] レポートを作成します。アプライアンスで [ドメイン毎のエグゼクティブ サマリー（Domain-Based Executive Summary）] レポートが生成されると、Bigfish 社の管理者は Bigfish.com、Redfish.com、および Bluefish.com のレポートを受信し、Redfish 社の管理者は Redfish.com ドメインのレポートを受信し、Bluefish 社の管理者は Bluefish.com ドメインのレポートを受信します。

名前付きレポートごとに異なるコンフィギュレーション ファイルをアプライアンスにアップロードできます。また、複数のレポートに対して同じコンフィギュレーション ファイルを使用することもできます。たとえば、異なる期間の同じドメインに関するデータが表示される、複数の名前付きレポートを作成できます。アプライアンスにコンフィギュレーション ファイルをアップロードする場合は、ファイル名を変更しない限り、GUI でレポート設定を更新する必要がありません。

[ドメイン毎のエグゼクティブ サマリー（Domain-Based Executive Summary）] レポートの作成

手順

ステップ 1　セキュリティ管理アプライアンスでレポートのスケジュールを設定することも、すぐにレポートを生成することもできます。

レポートのスケジュールを設定するには、次の手順を実行します。

a. [メール（Email）] > [レポート（Reporting）] > [定期レポート（Scheduled Reports）] を選択します。

b. [定期レポートを追加（Add Scheduled Report）] をクリックします。

オンデマンド レポートを作成するには、次の手順を実行します。

a. [メール（Email）] > [レポート（Reporting）] > [アーカイブ レポート（Archived Reports）] を選択します。

b. [今すぐレポートを生成（Generate Report Now）] をクリックします。

ステップ 2　[レポート タイプ（Report Type）] ドロップダウン リストから、[ドメイン毎のエグゼクティブ サマリー（Domain-Based Executive Summary）] レポート タイプを選択します。

ステップ 3　レポートを含めるドメインおよびレポート受信者の電子メール アドレスを指定します。レポートを生成するための、次のいずれかのオプションを選択できます。

- [個別のドメインを指定してレポートを生成（Generate report by specifying individual domains）]。レポートのドメインおよびレポート受信者の電子メール アドレスを入力します。複数のエントリを区切るには、カンマを使用します。また、subdomain.yourdomain.com のようなサブドメインを使用することもできます。あまり頻繁には変更されないと予測される少数のドメインのレポートを作成する場合は、ドメインを個別に指定することを推奨します。
- [ファイルをアップロードしてレポートを生成（Generate reports by uploading file）]。レポートのドメイン、および受信者の電子メール アドレスのリストが含まれるコンフィギュレーション ファイルをインポートします。アプライアンスのコンフィギュレーション ディレクトリからコンフィギュレーション ファイルを選択することも、ローカル コンピュータからアップロードすることもできます。頻繁に変更される多数のドメインのレポートを作成する場合は、コンフィギュレーション ファイルの使用を推奨します。ドメインベースのレポートのコンフィギュレーション ファイルの詳細については、「[ドメイン毎のエグゼクティブ サマリー（Domain-Based Executive Summary）] レポートのドメインおよび受信者のリストの管理」（P.4-54）を参照してください。

（注）　外部アカウント（Yahoo! メールまたは Gmail など）にレポートを送信する場合は、レポート メッセージが誤ってスパムに分類されないように外部アカウントのホワイト リストにレポーティング返信アドレスを追加する必要がある場合があります。

ステップ 4　[タイトル（Title）] テキスト フィールドに、レポートのタイトル名を入力します。

AsyncOS では、レポート名が一意かどうかは確認されません。混乱を避けるために、同じ名前で複数のレポートを作成しないでください。

ステップ 5　[送信ドメイン（Outgoing Domain）] セクションで、発信メール サマリーのドメイン タイプを選択します。選択肢は [サーバ別（By Server）] または [メール アドレス別（By Email Address）] です。

ステップ 6　[時間範囲（Time Range to Include）] ドロップダウン リストから、レポート データの時間範囲を選択します。

ステップ 7　[形式（Format）] セクションで、レポートの形式を選択します。

次のオプションがあります。

- [PDF]。配信用、アーカイブ用、またはその両方の用途で PDF 形式のドキュメントを作成します。[PDF レポートをプレビュー（Preview PDF Report）] をクリックすると、ただちに PDF ファイルでレポートを表示できます。
- [CSV]。カンマ区切りの値として raw データが含まれる ASCII テキスト ファイルを作成します。各 CSV ファイルには、最大 100 行を含めることができます。レポートに複数の種類の表が含まれる場合、各表に対して別個の CSV ファイルが作成されます。

ステップ 8　[スケジュール（Schedule）] セクションから、レポートを生成するスケジュールを選択します。

選択肢は [毎日（Daily）]、[毎週（Weekly）]（曜日のドロップダウン リストがあります）または [毎月（monthly）] です。

ステップ 9　（任意）レポートのカスタム ロゴをアップロードします。ロゴは、レポートの上部に表示されます。

- このロゴは、最大で 550 x 50 ピクセルの .jpg、.gif、または .png ファイルにする必要があります。
- ロゴ ファイルをアップロードしなかった場合、デフォルトの Cisco ロゴが使用されます。

ステップ 10　このレポートの言語を選択します。アジア言語での PDF ファイルの生成については、「レポーティング データおよびトラッキング データの印刷およびエクスポート」（P.3-10）の重要な情報を参照してください。

ステップ 11　[送信（Submit）] をクリックして、ページ上の変更を送信し、[変更を確定（Commit Changes）] をクリックして変更を保存します。

[エグゼクティブ サマリー（Executive Summary）] レポート

[エグゼクティブ サマリー（Executive Summary）] レポートは、電子メール セキュリティ アプライアンスからの着信および発信メッセージ アクティビティの概要です。セキュリティ管理アプライアンス上で表示できます。

このレポート ページには、電子メール レポーティングの [概要（Overview）] ページで表示できる情報の概要が表示されます。[電子メール レポーティングの概要（Email Reporting Overview）] ページの詳細については、「電子メール レポーティングの [概要（Overview）] ページ」（P.4-11）を参照してください。

電子メール レポートのスケジュール設定

「スケジュール設定された電子メール レポートとオンデマンドの電子メール レポートについて」（P.4-51）に示されているすべてのレポートをスケジュール設定できます。

レポートのスケジュール設定の管理方法については、次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」（P.4-56）
- 「スケジュール設定されたレポートの編集」（P.4-58）
- 「スケジュール設定されたレポートの中止」（P.4-58）

スケジュール設定されたレポートの追加

スケジュール設定された電子メール レポートを追加するには、次の手順を実行します。

手順

ステップ 1　セキュリティ管理アプライアンスで、[メール（Email）] > [レポート（Reporting）] > [定期レポート（Scheduled Reports）] を選択します。

ステップ 2　[定期レポートを追加（Add Scheduled Report）] をクリックします。

ステップ 3　レポート タイプを選択します。

レポート タイプの説明については、「スケジュール設定された電子メール レポートとオンデマンドの電子メール レポートについて」（P.4-51）を参照してください。

（注）　[ドメイン毎のエグゼクティブ サマリー（Domain-Based Executive Summary）] レポートの設定の詳細については、「[ドメイン毎のエグゼクティブ サマリー（Domain-Based Executive Summary）] レポート」（P.4-53）を参照してください。

（注）　スケジュール設定されたレポートに使用できるオプションは、レポート タイプによって異なります。この手順の残りの部分で説明するオプションを、すべてのレポートに適用する必要はありません。

ステップ 4　[タイトル（Title）] フィールドに、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推奨します。

ステップ 5　[時間範囲（Time Range to Include）] ドロップダウン メニューからレポートの時間範囲を選択します。

ステップ 6　生成されるレポートの**形式**を選択します。

デフォルト形式は PDF です。ほとんどのレポートでは、raw データを CSV ファイルとして保存することも可能です。

ステップ 7　レポートに応じて、[行数（Number of Rows）] で、レポートに含めるデータの量を選択します。

ステップ 8　レポートに応じて、レポートをソートする基準となるカラムを選択します。

ステップ 9　[スケジュール（Schedule）] 領域で、レポートのスケジュールを設定する日、週、または月の横にあるオプション ボタンを選択します。また、レポートのスケジュール設定に時刻を含めることもできます。時刻は、深夜 0 時を基準とした増分になります（00:00 ～ 23:59 が 1 日）。

ステップ 10　[メール（Email）] テキスト フィールドに、生成されたレポートが送信される電子メール アドレスを入力します。

電子メール受信者を指定しない場合でも、レポートはアーカイブされます。

必要に応じた数（ゼロも含む）のレポート受信者を追加できます。レポートを多数のアドレスに送信する必要がある場合、個別に受信者を設定するよりも、メーリング リストを作成するほうが容易です。

ステップ 11　レポートの言語を選択します。

アジア言語については、「レポーティング データおよびトラッキング データの印刷およびエクスポート」（P.3-10）の重要な情報を参照してください。

ステップ 12　[送信（Submit）] をクリックします。

スケジュール設定されたレポートの編集

手順

ステップ 1　セキュリティ管理アプライアンスで、[メール（Email）] > [レポート（Reporting）] > [定期レポート（Scheduled Reports）] を選択します。

ステップ 2　[レポートのタイトル（Report Title）] カラムの、変更するレポート名リンクをクリックします。

ステップ 3　レポート設定値を変更します。

ステップ 4　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中止

スケジュール設定されたレポートで、今後のインスタンスが生成されないようにするには、次のステップを実行します。

手順

ステップ 1　セキュリティ管理アプライアンスで、[メール（Email）] > [レポート（Reporting）] > [定期レポート（Scheduled Reports）] を選択します。

ステップ 2　生成を中止するレポートに対応するチェックボックスを選択します。スケジュール設定されたすべてのレポートを削除するには、[すべて（All）] チェックボックスを選択します。

ステップ 3　[削除（Delete）] をクリックします。

（注）　削除されたレポートのアーカイブ版は、自動的に削除されるわけでは*ありません*。以前に生成されたレポートを削除するには、「アーカイブ済みのレポートの削除」（P.4-61）を参照してください。

オンデマンドでの電子メール レポートの生成

「[メール レポート（Email Reporting）] ページの概要」（P.4-7）で説明したインタラクティブ レポート ページを使用して表示（および PDF を生成）できるレポートに加えて、「スケジュール設定された電子メール レポートとオンデマンドの電子メール レポートについて」（P.4-51）に示したレポートの、指定したタイム フレームの PDF ファイルまたは raw データ CSV ファイルをいつでも保存できます。

オンデマンド レポートを生成するには、次の手順を実行します。

手順

ステップ 1　セキュリティ管理アプライアンスで、[メール（Email）] > [レポート（Reporting）] > [アーカイブ レポート（Archived Reports）] を選択します。

ステップ 2　[今すぐレポートを生成（Generate Report Now）] をクリックします。

ステップ 3　レポート タイプを選択します。

レポート タイプの説明については、「スケジュール設定された電子メール レポートとオンデマンドの電子メール レポートについて」（P.4-51）を参照してください。

ステップ 4　[タイトル（Title）] テキスト フィールドに、レポートのタイトル名を入力します。

AsyncOS では、レポート名が一意かどうかは確認されません。混乱を避けるために、同じ名前で複数のレポートを作成しないでください。

（注）　[ドメイン毎のエグゼクティブ サマリー（Domain-Based Executive Summary）] レポートの設定の詳細については、「[ドメイン毎のエグゼクティブ サマリー（Domain-Based Executive Summary）] レポート」（P.4-53）を参照してください。

（注）　スケジュール設定されたレポートに使用できるオプションは、レポート タイプによって異なります。この手順の残りの部分で説明するオプションを、すべてのレポートに適用する必要はありません。

ステップ 5　[時間範囲（Time Range to Include）] ドロップダウン リストから、レポート データの時間範囲を選択します。

これはカスタム時間範囲オプションです。

ステップ 6　[形式（Format）] セクションで、レポートの形式を選択します。

次のオプションがあります。

- [PDF]。配信用、アーカイブ用、またはその両方の用途で PDF 形式のドキュメントを作成します。[PDF レポートをプレビュー（Preview PDF Report）] をクリックすると、ただちに PDF ファイルでレポートを表示できます。
- [CSV]。カンマ区切りの値の raw データが含まれる ASCII テキスト ファイルを作成します。各 CSV ファイルには、最大 100 行を含めることができます。レポートに複数の種類の表が含まれる場合、各表に対して別個の CSV ファイルが作成されます。

ステップ 7　レポートを実行するアプライアンスまたはアプライアンス グループを選択します。アプライアンス グループを作成していない場合、このオプションは表示されません。

ステップ 8　[送信オプション（Delivery Option）] セクションから、次のオプションを選択します。

- [アーカイブ レポート（Archive Report）] チェックボックスをオンにして、レポートをアーカイブします。

  このオプションを選択すると、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。

（注）　[ドメイン毎のエグゼクティブ サマリー（Domain-Based Executive Summary）] レポートはアーカイブできません。

- [今すぐ受信者にメールを送る（Email now to recipients）] チェックボックスをオンにして、レポートを電子メールで送信します。

  テキスト フィールドに、レポートの受信者の電子メールアドレスを入力します。

ステップ 9　このレポートの言語を選択します。アジア言語での PDF ファイルの生成については、「レポーティング データおよびトラッキング データの印刷およびエクスポート」（P.3-10）の重要な情報を参照してください。

ステップ 10　[このレポートを送信（Deliver This Report）] をクリックして、レポートを生成します。

アーカイブ電子メール レポートの表示と管理

スケジュール設定されたレポートおよびオンデマンド レポートは、一定期間アーカイブされます。

セキュリティ管理アプライアンスでは、スケジュール設定された各レポートの最大 12 のインスタンスで、生成された最新のレポートをすべてのレポートに対して、合計 1000 バージョンまで保持します。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。

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。

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。（詳細については、付録 A「IP インターフェイスおよびアプライアンスへのアクセス」を参照してください）。

アーカイブ済みのレポートへのアクセス

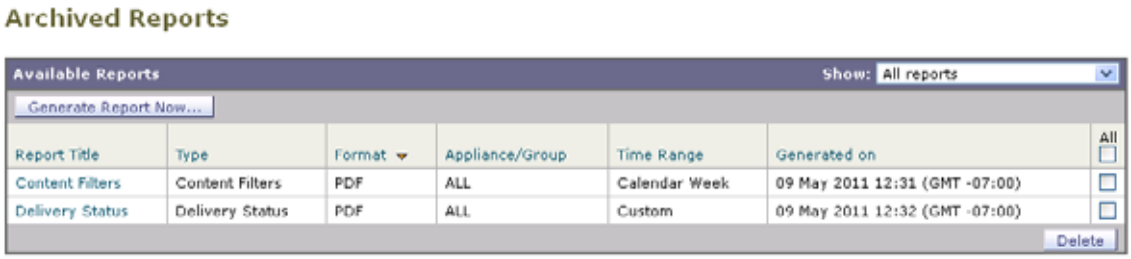
[メール（Email）] > [レポート（Reporting）] > [アーカイブ レポート（Archived Reports）] ページには、生成されたがまだ消去されておらず、アーカイブすることを指定した、スケジュール設定されたレポートとオンデマンド レポートが表示されます。

手順

ステップ 1　[メール（Email）] > [レポート（Reporting）] > [アーカイブ レポート（Archived Reports）] を選択します。

[アーカイブ レポート（Archived Reports）] のリストが表示されます。

図 4-22　　アーカイブ レポート（Archived Reports）



ステップ 2　リストが長い場合に特定のレポートを見つけるには、[表示（Show）] メニューからレポート タイプを選択してリストをフィルタリングするか、またはカラムのヘッダーをクリックし、そのカラムでソートします。

ステップ 3　[レポートのタイトル（Report Title）] をクリックすると、そのレポートが表示されます。

アーカイブ済みのレポートの削除

「アーカイブ電子メール レポートの表示と管理」（P.4-60）で説明したルールに従って、レポートは自動的にシステムから削除されます。ただし、不要なレポートを手動で削除することもできます。

アーカイブ済みのレポートを手動で削除するには、次の手順を実行します。

手順

ステップ 1　セキュリティ管理アプライアンスで、[メール（Email）] > [レポート（Reporting）] > [アーカイブ レポート（Archived Reports）] を選択します。

選択可能なアーカイブ済みのレポートが表示されます。

ステップ 2　削除する 1 つまたは複数のレポートのチェックボックスを選択します。

ステップ 3　[削除（Delete）] をクリックします。

ステップ 4　スケジュール設定されたレポートで、今後のインスタンスが生成されないようにするには、「スケジュール設定されたレポートの中止」（P.4-58）を参照してください。

CHAPTER 5

中央集中型 Web レポーティングおよびトラッキングの使用

中央集中型 Web レポーティングの概要

シスコのコンテンツ セキュリティ管理アプライアンスは、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。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。

中央集中型 Web レポーティング機能を使用すると、管理者は概要レポートを作成してネットワークの現状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。

ドメイン情報

ドメインについては、Web レポーティング機能で以下のデータ要素を生成し、ドメイン レポートに含めることができます。たとえば Facebook.com ドメインに関するレポートを作成している場合、レポートに次の情報を出力できます。

- Facebook.com にアクセスした上位ユーザのリスト
- Facebook.com 内でアクセスされた上位 URL のリスト

ユーザ

ユーザについては、Web レポーティング機能で以下のデータ要素を生成し、ユーザ レポートに含めることができます。たとえば、「Jamie」というタイトルのレポートに次の情報を含めることができます。

- ユーザ「Jamie」がアクセスした上位ドメインのリスト
- マルウェアまたはウイルスが陽性であった上位 URL のリスト
- ユーザ「Jamie」がアクセスした上位カテゴリのリスト

カテゴリ

カテゴリに対しては、カテゴリ レポートに含めるデータを、Web レポーティング機能で生成できます。たとえば、「Sports」というカテゴリに次の情報を含めることができます。

- 「Sports」カテゴリに含まれていた上位ドメインのリスト
- 「Sports」カテゴリにアクセスした上位ユーザのリスト

上記のどの例のレポートも、ネットワーク上の特定の項目に関する包括的なビューを提供して、管理者が対処できるようにすることを目的としています。

一般

ロギング ページとレポーティング ページの詳細については、「ロギングとレポーティング」（P.15-1）を参照してください。

（注） アクセスされた特定の URL だけでなく、ユーザが利用するすべてのドメイン情報を取得することができます。ユーザがアクセスしている特定の URL、その URL にアクセスした時刻、その URL が許可されているかどうかなどの情報を入手するには、[Web トラッキング（Web Tracking）] ページの Web プロキシ サービスによって処理されたトランザクションの検索を使用します。

（注） Web セキュリティ アプライアンスでデータが保存されるのは、ローカル レポーティングが使用される場合だけです。Web セキュリティ アプライアンスで中央集中型レポーティングがイネーブルな場合、その Web セキュリティ アプライアンスではシステム キャパシティとシステム ステータスのデータのみが維持されます。中央集中型 Web レポーティングがイネーブルになっていない場合、生成されるレポートはシステム キャパシティとシステム ステータスだけです。

セキュリティ管理アプライアンスでレポーティング データを表示するには、いくつかの方法があります。

- インタラクティブ レポート ページを表示する場合は、「Web レポーティング ページについて」（P.5-7）を参照してください。
- レポートをオンデマンドで生成するには、「オンデマンドでの Web レポートの生成」（P.5-71）を参照してください。
- レポートが定期的に繰り返し作成されるようにスケジュールを設定する場合は、「スケジュール設定されたレポートとオンデマンド Web レポートについて」（P.5-66）を参照してください。
- 以前に実行されたレポート（スケジュール設定されたレポートとオンデマンドで生成されたレポートの両方）のアーカイブ版を表示する方法については、「アーカイブされた Web レポートの表示と管理」（P.5-72）を参照してください。

中央集中型 Web レポーティングの設定

中央集中型 Web レポーティングを設定するには、次の手順を順序どおり実行します。

- 「セキュリティ管理アプライアンスでの中央集中型 Web レポーティングのイネーブル化」（P.5-3）

セキュリティ管理アプライアンスでの中央集中型 Web レポーティングのイネーブル化

手順

ステップ 1　中央集中型 Web レポーティングをイネーブルにする前に、十分なディスク領域がサービスに割り当てられていることを確認します。「ディスク使用量の管理」（P.14-56）を参照してください。

ステップ 2　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [Web] > [集約管理レポート（Centralized Reporting）] を選択します。

ステップ 3　システム セットアップ ウィザードの実行後初めて中央集中型レポーティングをイネーブルにする場合は、次の手順を実行します

a.　[有効（Enable）] をクリックします。

b.　エンド ユーザ ライセンス契約書を確認して、[承認（Accept）] をクリックします。

ステップ 4　以前に中央集中型レポーティングをディセーブルにし、その後イネーブルにする場合は、次の手順を実行します。

a.　[設定を編集（Edit Settings）] をクリックします。

b.　[集約 Web レポートサービスを有効にする（Enable Centralized Web Report Services）] チェックボックスを選択します。

c.　「Web レポートでのユーザ名の匿名化」（P.5-5）はここで実行することも、後で実行することもできます。

ステップ 5　変更を送信し、保存します。

（注）　アプライアンスで Web レポーティングがイネーブルになっていて、この処理にディスク領域が割り当てられていない場合、ディスク領域が割り当てられるまで、中央集中型 Web レポーティングが機能しません。Web レポーティングおよびトラッキングに設定するクォータが、現在使用しているディスク領域よりも大きい場合、Web レポーティングおよびトラッキングのデータは失われません。詳細については、「ディスク使用量の管理」（P.14-56）を参照してください。

Web セキュリティ アプライアンスでの中央集中型レポーティングのイネーブル化

中央集中型レポーティングをイネーブルにする前に、すべての Web セキュリティ アプライアンスが設定され、想定どおりに動作している必要があります。

中央集中型レポーティングは、それを使用する各 Web セキュリティ アプライアンスごとにイネーブルにする必要があります。

『*Cisco IronPort AsyncOS for Web Security User Guide*』の「Enabling Centralized Reporting」を参照してください。

管理対象の各 Web セキュリティ アプライアンスへの中央集中型 Web レポーティング サービスの追加

ここで実行する手順は、他の中央集中型管理機能の設定時に、すでにこのアプライアンスを追加したかどうかによって異なります。

手順

ステップ 1　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [セキュリティ アプライアンス（Security Appliances）] を選択します。

ステップ 2　リストに Web セキュリティ アプライアンスを追加済みの場合は、次の手順を実行します。

a.　Web セキュリティ アプライアンスの名前をクリックします。

b.　[集約管理レポート（Centralized Reporting）] サービスを選択します。

ステップ 3　Web セキュリティ アプライアンスをまだ追加していない場合は、次の手順を実行します。

a.　[Web アプライアンスの追加（Add Web Appliance）] をクリックします。

b.　[アプライアンス名（Appliance Name）] および [IP アドレス（IP Address）] テキスト フィールドに、Web セキュリティ アプライアンスの管理インターフェイスのアプライアンス名と IP アドレスを入力します。

（注）　[IP アドレス（IP Address）] テキスト フィールドに DNS 名を入力した場合でも、[送信（Submit）] をクリックすると、すぐに IP アドレスに解決されます。

c.　[集約管理レポート（Centralized Reporting）] サービスが事前に選択されています。

d.　[接続の確立（Establish Connection）] をクリックします。

e.　管理対象となるアプライアンスの管理者アカウントのユーザ名とパスワードを入力し、[接続の確立（Establish Connection）] をクリックします。

（注）　ログイン資格情報を入力すると、セキュリティ管理アプライアンスからリモート アプライアンスへのファイル転送のための公開 SSH キーが渡されます。ログイン資格情報は、セキュリティ管理アプライアンスには保存されません。

f.　[成功（Success）] メッセージがページのテーブルの上に表示されるまで待機します。

g.　[テスト接続（Test Connection）] をクリックします。

h.　テーブルの上のテスト結果を確認します。

ステップ 4　[送信（Submit）] をクリックします。

ステップ 5　中央集中型レポーティングをイネーブルにする各 Web セキュリティ アプライアンスに対してこの手順を繰り返します。

ステップ 6　変更を保存します。

Web レポートでのユーザ名の匿名化

デフォルトでは、レポーティング ページと PDF にユーザ名が表示されます。ただし、ユーザのプライバシーを保護するために、Web レポートでユーザ名を識別できないようにすることができます。

（注）　このアプライアンスの管理者権限を持つユーザは、インタラクティブ レポートを表示する際、常にユーザ名を表示できます。

図 5-1　ユーザ名が表示されたレポーティング ページ

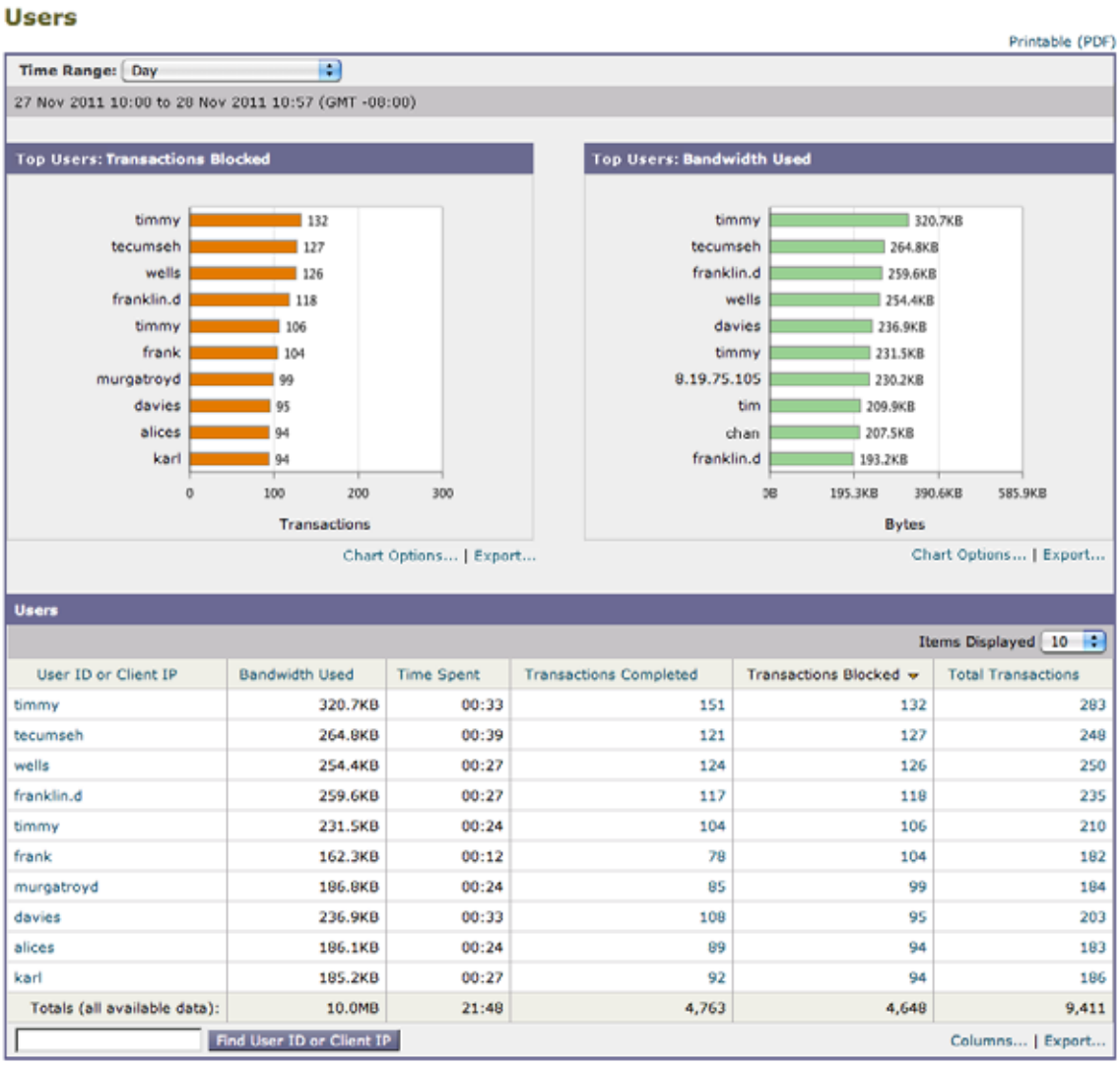
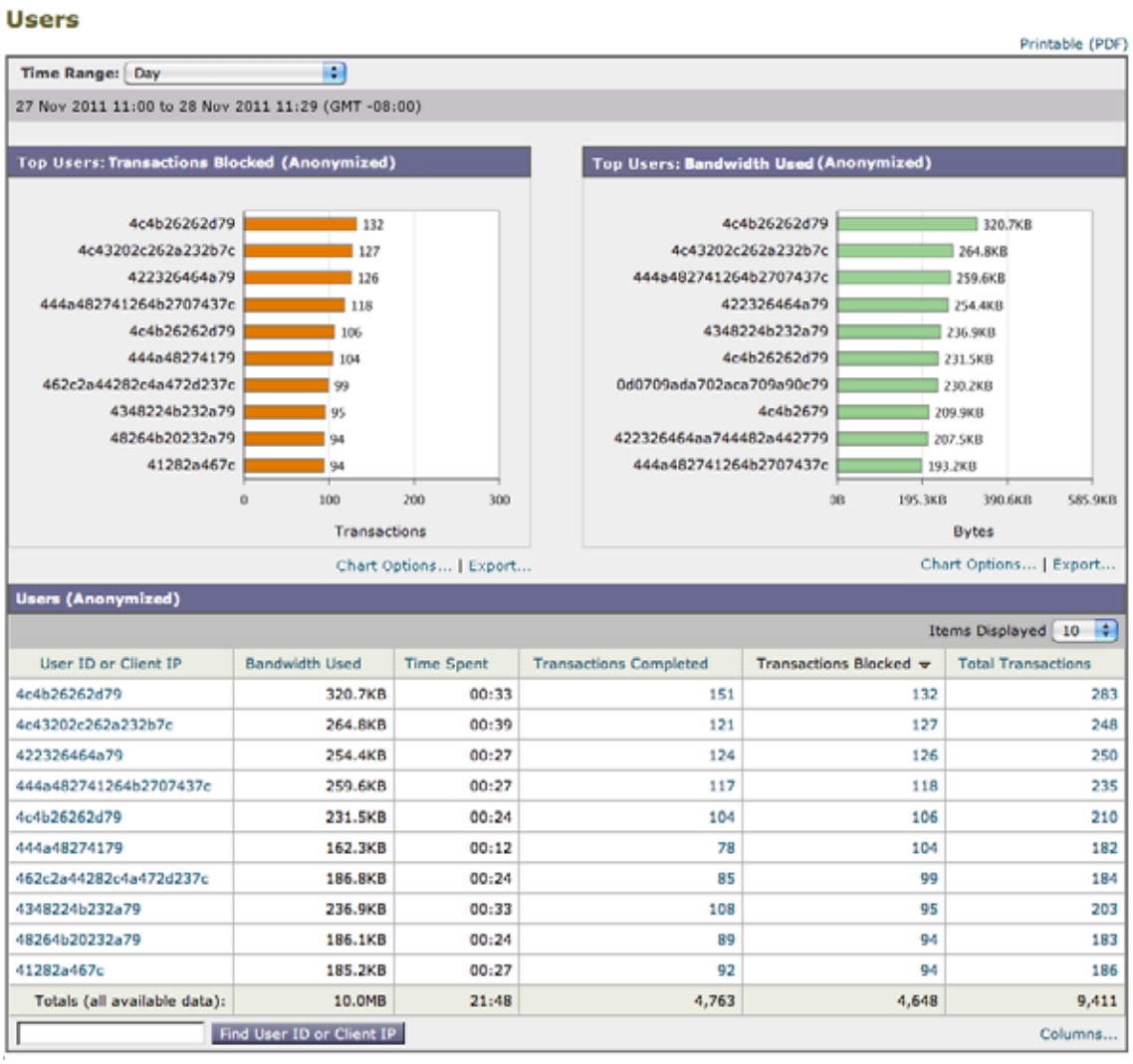


図 5-2　ユーザを匿名にしたレポーティング ページ



レポートでユーザ名を識別できないようにするには、次の手順を実行します。

手順

ステップ 1　[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [Web] > [集約管理レポート（Centralized Reporting）] を選択します。

ステップ 2　[設定を編集（Edit Settings）] をクリックします。

ステップ 3　[レポートでユーザ名を匿名にする（Anonymize usernames in reports）] チェックボックスをオンにします。

ステップ 4　変更を送信し、保存します。

インタラクティブ Web レポーティング ページの操作

インタラクティブ Web レポーティング ページでは、システム内で管理対象とする 1 つまたはすべての Web セキュリティ アプライアンスアプライアンスに関する情報をモニタできます。

これらのページの操作については、次の項目を参照してください。

表 5-1　インタラクティブ Web レポーティング ページの操作

目的	参照先
レポート データのアクセスおよび表示オプションを確認する	「レポーティング データを表示する方法」（P.3-1）
テーブル内のデータの意味を理解する	「Web レポートのテーブル カラムの説明」（P.5-11）
インタラクティブ レポート ページのビューをカスタマイズする	「レポート データのビューのカスタマイズ」（P.3-3）
データ内の情報を検索する	「Web トラッキング（Web Tracking）」（P.5-55）
レポート情報を印刷またはエクスポートする	「レポーティング データおよびトラッキング データの印刷およびエクスポート」（P.3-10）
さまざまなインタラクティブ レポート ページについて理解する	「Web レポーティング ページについて」（P.5-7）
レポートをオンデマンドで生成する	「スケジュール設定されたレポートとオンデマンド Web レポートについて」（P.5-66）
レポートが指定した間隔で所定の時刻に自動的に実行されるようスケジュールを設定する	「スケジュール設定されたレポートとオンデマンド Web レポートについて」（P.5-66）
アーカイブ済みのオンデマンド レポートとスケジュールされたレポートを表示する	「アーカイブされた Web レポートの表示と管理」（P.5-72）
データの収集方法を理解する	「セキュリティ アプライアンスによるレポート用データの収集方法」（P.3-2）

Web レポーティング ページについて

[Web] > [レポート（Reporting）] タブには、レポート 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。ここでは、このタブに表示される各レポーティング ページ、および各レポーティング ページに表示される情報について説明します。

（注）　[Web レポート（Web Reporting）] タブのどのオプションをオンデマンドまたはスケジュール済みレポートとして使用できるかについては、「スケジュール設定されたレポートとオンデマンド Web レポートについて」（P.5-66）を参照してください。

表 5-2　[Web レポート（Web Reporting）] タブの詳細

[Web レポート（Web Reporting）] メニュー	アクション
Web レポートの概要	[概要（Overview）] ページには、お使いの 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。これには、着信および発信トランザクションに関するグラフやサマリー テーブルも含まれます。詳細については、「Web レポートの概要」（P.5-13）を参照してください。
[ユーザ（Users）] レポート（Web）	[ユーザ（Users）] ページには複数の Web トラッキング リンクが表示され、各ユーザの Web トラッキング情報を確認できます。 [ユーザ（Users）] ページでは、システム上のユーザ（1 人または複数）がインターネット、特定のサイト、または特定の URL で費やした時間と、そのユーザが使用している帯域幅の量を表示できます。 [ユーザ（Users）] ページのインタラクティブな [ユーザ（Users）] テーブルで個々のユーザをクリックすると、その特定のユーザの詳細情報が [ユーザの詳細（User Details）] ページに表示されます。 [ユーザの詳細（User Details）] ページでは、[Web] > [レポート（Reporting）] > [ユーザ（Users）] ページのインタラクティブな [ユーザ（Users）] テーブルで指定したユーザについて具体的な情報を確認できます。このページから、お使いのシステムでの各ユーザのアクティビティを調査できます。特に、ユーザ レベルの調査を実行している場合に、ユーザがアクセスしているサイト、ユーザが直面しているマルウェアの脅威、ユーザがアクセスしている URL カテゴリ、これらのサイトで特定のユーザが費やしている時間などを確認する必要があるときは、このページが役立ちます。 詳細については、「[ユーザ（Users）] レポート（Web）」（P.5-17）を参照してください。システムにおける各ユーザの情報については、「[ユーザの詳細（User Details）]（Web レポーティング）」（P.5-20）を参照してください。
[Web サイト（Web Sites）] レポート	[Web サイト（Web Sites）] ページでは、管理対象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て表示できます。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。詳細については、「[Web サイト（Web Sites）] レポート」（P.5-24）を参照してください。

表 5-2　[Web レポート（Web Reporting）] タブの詳細 （続き）

[Web レポート（Web Reporting）] メニュー	アクション
URL カテゴリ レポート	[URL カテゴリ（URL Categories）] ページでは、アクセスされている次の上位 URL カテゴリを表示できます。 • 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。 • 完了したトランザクションと、警告とブロックが行われたトランザクションの両方を対象とした、指定した時間範囲内のすべての URL カテゴリ。これはインタラクティブなカラム見出しのあるインタラクティブ テーブルとなっていて、必要に応じてデータをソートできます。 詳細については、「URL カテゴリ レポート」（P.5-26）を参照してください。
[アプリケーションの表示（Application Visibility）] レポート	[アプリケーションの表示（Application Visibility）] ページでは、セキュリティ管理アプライアンスおよび Web セキュリティ アプライアンス内で特定のアプリケーション タイプに適用されている制御を適用し、表示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表示（Application Visibility）] レポート」（P.5-30）を参照してください。
[マルウェア対策（Anti-Malware）] レポート	[マルウェア対策（Anti-Malware）] ページでは、指定した時間範囲内にアンチマルウェア スキャン エンジンで検出された、マルウェア ポートとマルウェア サイトに関する情報を表示できます。レポートの上部には、上位の各マルウェア ポートおよび各マルウェア Web サイトの接続数が表示されます。レポートの下部には、検出されたマルウェア ポートとマルウェア サイトが表示されます。詳細については、「[マルウェア対策（Anti-Malware）] レポート」（P.5-33）を参照してください。
[クライアント マルウェア リスク（Client Malware Risk）] レポート	[クライアント マルウェア リスク（Client Malware Risk）] ページは、セキュリティ関連のレポーティング ページです。このページを使用して、著しく頻繁にマルウェア サイトへ接続している可能性がある個々のクライアント コンピュータを特定できます。 詳細については、「[クライアント マルウェア リスク（Client Malware Risk）] レポート」（P.5-40）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）] レポート	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 フィルタリングに関するレポートを表示できます。詳細については、「[Web レピュテーション フィルタ（Web Reputation Filters）] レポート」（P.5-43）を参照してください。
[L4 トラフィック モニタ（L4 Traffic Monitor）] レポート	指定した時間範囲内に L4 トラフィック モニタで検出された、マルウェア ポートとマルウェア サイトに関する情報を表示できます。詳細については、「[L4 トラフィック モニタ（L4 Traffic Monitor）] レポート」（P.5-46）を参照してください。

表 5-2　[Web レポート（Web Reporting）] タブの詳細 （続き）

[Web レポート（Web Reporting）] メニュー	アクション
[SOCKS プロキシ（SOCKS Proxy）] レポート	宛先、ユーザなど、SOCKS プロキシ トランザクションのデータを表示できます。 詳細については、「[SOCKS プロキシ（SOCKS Proxy）] レポート」（P.5-51）を参照してください。
ユーザ ロケーション別のレポート（Reports by User Location）	[ユーザ ロケーション別のレポート（Reports by User Location）] ページでは、モバイル ユーザがローカル システムまたはリモート システムから実行しているアクティビティを確認できます。 詳細については、「ユーザ ロケーション別のレポート（Reports by User Location）」（P.5-53）を参照してください。
Web トラッキング（Web Tracking）	[Web トラッキング（Web Tracking）] ページでは、次のタイプの情報を検索できます。 • Web プロキシ サービスによって処理されたトランザクションの検索では、基本的な Web 関連情報（アプライアンスで処理されている Web トラフィックのタイプなど）を追跡して表示することができます。 これには、時間範囲、ユーザ ID、クライアント IP アドレスなどの情報が含まれるほか、特定のタイプの URL、各接続が占有している帯域幅の量、特定のユーザの Web 使用状況のトラッキングなどの情報も含まれます。 • L4 トラフィック モニタによって処理されたトランザクションの検索では、マルウェアの転送アクティビティに関与しているサイト、ポート、およびクライアント IP アドレスの L4TM データを検索できます。 • SOCKS プロキシによって処理されたトランザクションの検索では、SOCKS プロキシによって処理されたトランザクションを検索できます。 詳細については、「Web トラッキング（Web Tracking）」（P.5-55）を参照してください。
[システム容量（System Capacity）] ページ	レポーティング データを セキュリティ管理アプライアンスに送信する、全体的なワークロードを表示できます。 詳細については、「[システム容量（System Capacity）] ページ」（P.5-61）を参照してください。
[使用可能なデータ（Data Availability）] ページ	各アプライアンスの セキュリティ管理アプライアンス上のレポーティング データの影響を把握できます。詳細については、「[使用可能なデータ（Data Availability）] ページ」（P.5-65）を参照してください。

表 5-2　[Web レポート（Web Reporting）] タブの詳細 （続き）

[Web レポート（Web Reporting）] メニュー	アクション
定期レポート（Scheduled Reports）	指定した時間範囲のレポートのスケジュールを設定できます。詳細については、「スケジュール設定されたレポートとオンデマンド Web レポートについて」（P.5-66）を参照してください。
アーカイブ レポート（Archived Reports）	指定した時間範囲のレポートをアーカイブできます。詳細については、「アーカイブされた Web レポートの表示と管理」（P.5-72）を参照してください。

（注）　ほとんどの Web レポーティング カテゴリでレポートをスケジュール設定できます。これには、拡張された上位 URL カテゴリおよび上位アプリケーション タイプに関する追加のレポートが含まれます。レポートのスケジュール設定の詳細については、「スケジュール設定されたレポートとオンデマンド Web レポートについて」（P.5-66）を参照してください。

Web レポートのテーブル カラムの説明

ここでは、さまざまな Web レポート ページのテーブルで使用されるカラム見出しについて説明します。

（注）　すべてのカラムを各レポート ページで使用できるわけではありません。また、使用可能なすべてのカラムがデフォルトで表示されるわけではありません。テーブルで使用可能なカラムを表示するには、テーブルの下の [列（Column）] リンクをクリックします。

レポートでのテーブルの操作の詳細については、「レポート ページのテーブルのカスタマイズ」（P.3-6）を参照してください。

表 5-3　Web レポーティング ページのテーブル 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のユーザ ID またはクライアント IP。
使用済み帯域幅（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。
ブロッキングによって節減できた帯域幅（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。

表 5-3　Web レポーティング ページのテーブル カラムの説明 （続き）

カラム名	説明
滞留時間（Time Spent）	Web ページに費やされた時間。ユーザの調査が目的の場合、各 URL カテゴリでユーザが費やした時間。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。 トランザクション イベントに「viewed」のタグが付けられる（ユーザが特定の URL に進む）と、[滞留時間（Time Spent）] の値の計算が開始され、Web レポーティング テーブルのフィールドとして追加されます。 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。
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。

表 5-3　Web レポーティング ページのテーブル カラムの説明 （続き）

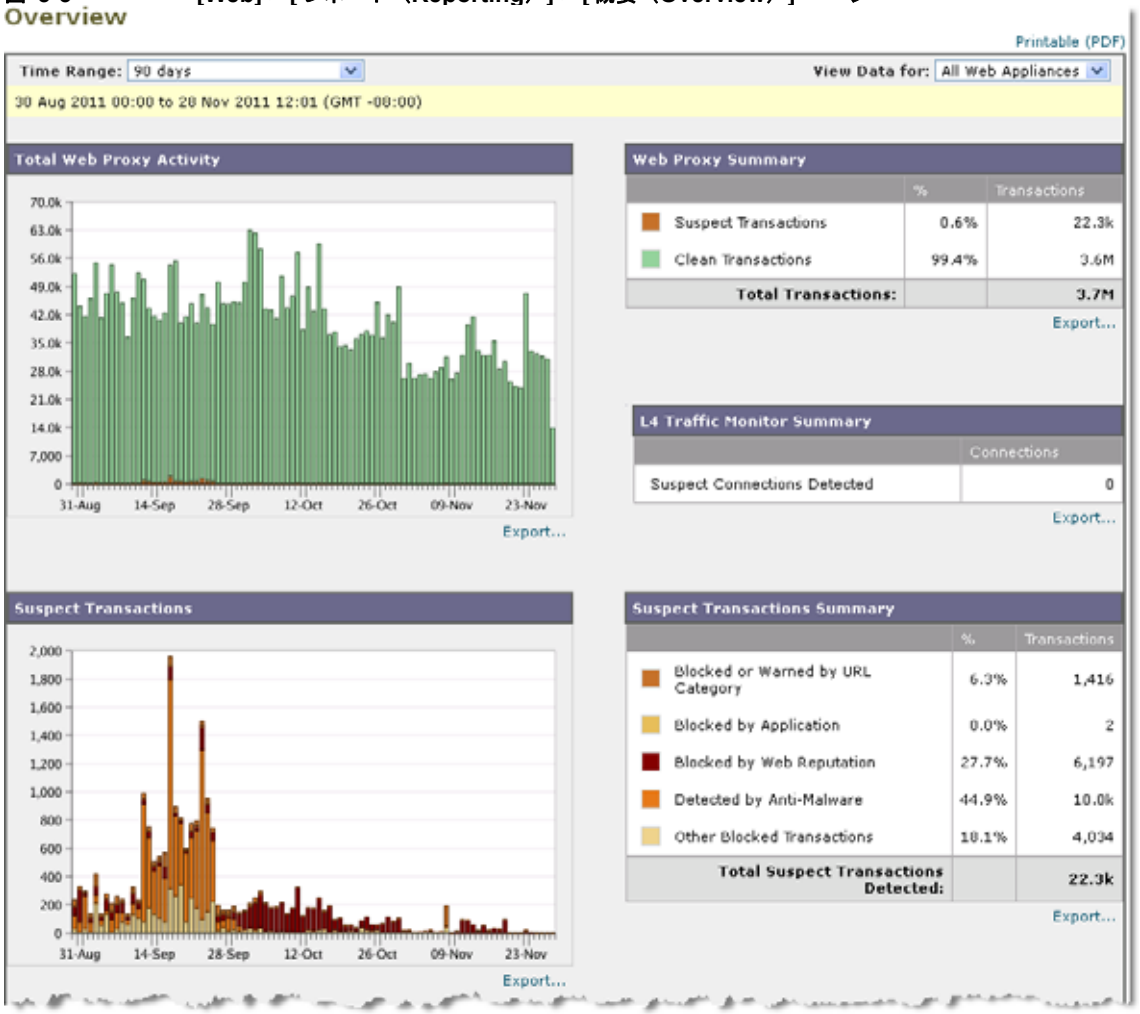
カラム名	説明
その他のブロックされたトランザクション（Other Blocked Transactions）	ブロックされた他のすべてのトランザクション。単位はトランザクション タイプで表示されます。
帯域幅制限のあるトランザクション（Transactions with Bandwidth Limit）	帯域幅の制限があるトランザクションの数。
帯域幅制限のないトランザクション（Transactions without Bandwidth Limit）	帯域幅の制限がないトランザクションの数。
ブロックされたトランザクション（アプリケーション別）（Transactions Blocked by 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。
トランザクション完了（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。

Web レポートの概要

[Web] > [レポート（Reporting）] > [概要（Overview）] ページでは、お使いの 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。これには、着信および発信トランザクションに関するグラフやサマリー テーブルも含まれます。

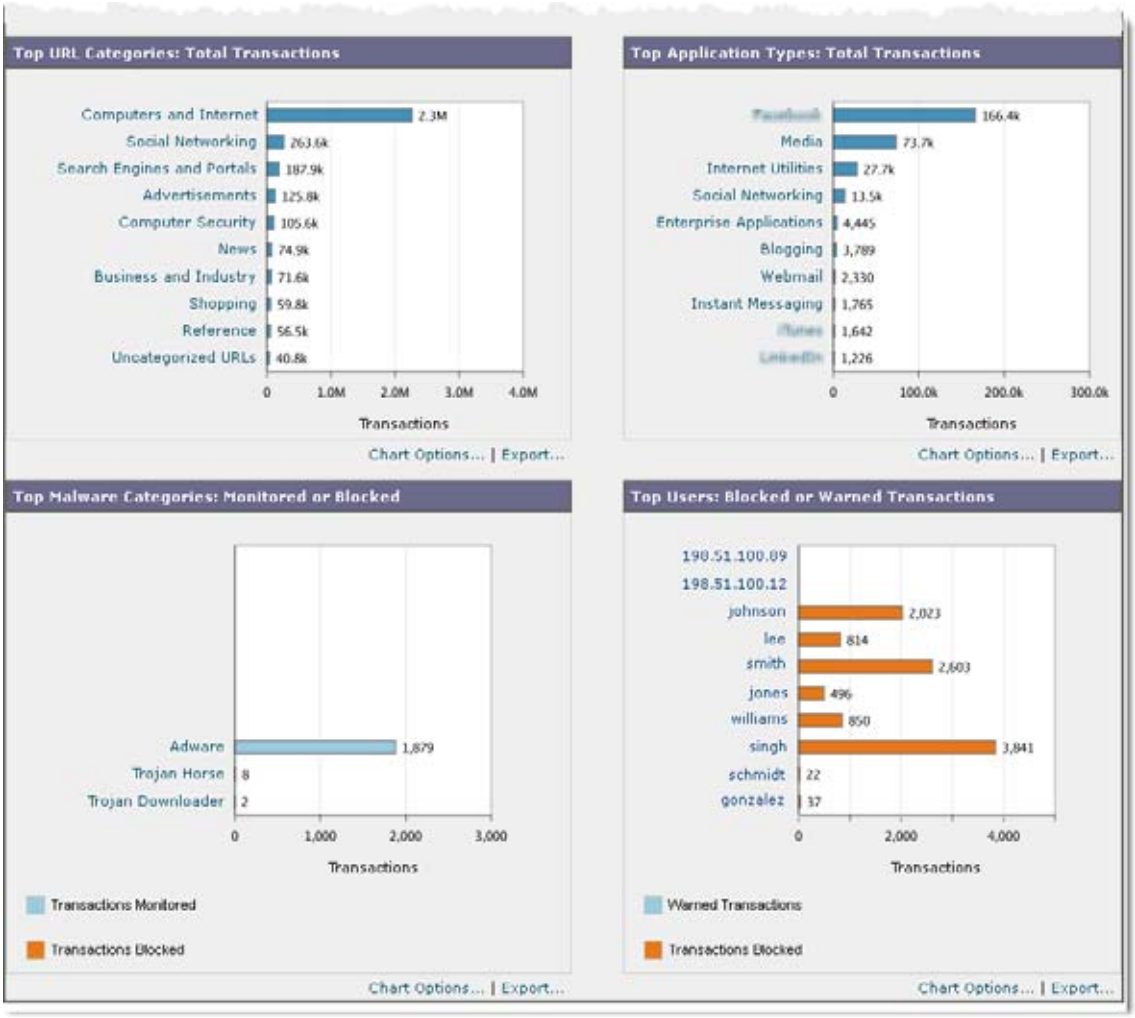
図 5-3 に、[概要（Overview）] ページを示します。

図 5-3　[Web] > [レポート（Reporting）] > [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。

次のリストでは、[概要（Overview）] ページの各セクションについて説明します。

表 5-4　[Web] > [レポート（Reporting）] > [概要（Overview）] ページの詳細

セクション	説明
時間範囲（Time Range）（ドロップダウン リスト）	1 ～ 90 日間またはカスタム日数範囲を指定できるドロップダウン リスト。時間範囲の詳細と実際のニーズに合わせたカスタマイズについては、「レポートの時間範囲の選択」（P.3-4）を参照してください。
データ参照（View Data for）	概要データを表示する Web セキュリティ アプライアンスを選択するか、[すべての Web アプライアンス（All Web Appliances）] を選択します。 「アプライアンスまたはレポーティング グループのレポーティング データの表示」（P.3-4）も参照してください。
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、現在セキュリティ管理アプライアンスで管理されている Web セキュリティ アプライアンスによって報告される Web プロキシ アクティビティを表示できます。 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。
Web プロキシのサマリー（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 モニタのサマリー（L4 Traffic Monitor Summary）	この項には、現在セキュリティ管理アプライアンスで管理されている Web セキュリティ アプライアンスによって報告される L4 トラフィックが表示されます。
疑わしいトランザクション（Suspect Transactions）	このセクションでは、管理者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サマリー（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、ブロックされている上位 10 の URL カテゴリが表示されます。URL カテゴリのタイプ（縦の目盛り）、特定タイプのカテゴリが実際にブロックされた回数（横の目盛り）などがあります。 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.5-28）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、ブロックされている上位アプリケーション タイプが表示されます。これには、実際のアプリケーション タイプ名（縦の目盛り）、特定のアプリケーションがブロックされた回数（横の目盛り）が含まれます。

表 5-4　[Web] > [レポート（Reporting）] > [概要（Overview）] ページの詳細 （続き）

セクション	説明
検出した上位マルウェア 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の上位ユーザ（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実際のユーザが表示されます。ユーザは IP アドレスまたはユーザ名で表示できます。ユーザ名を識別できないようにするには、「Web レポートでのユーザ名の匿名化」（P.5-5）を参照してください。

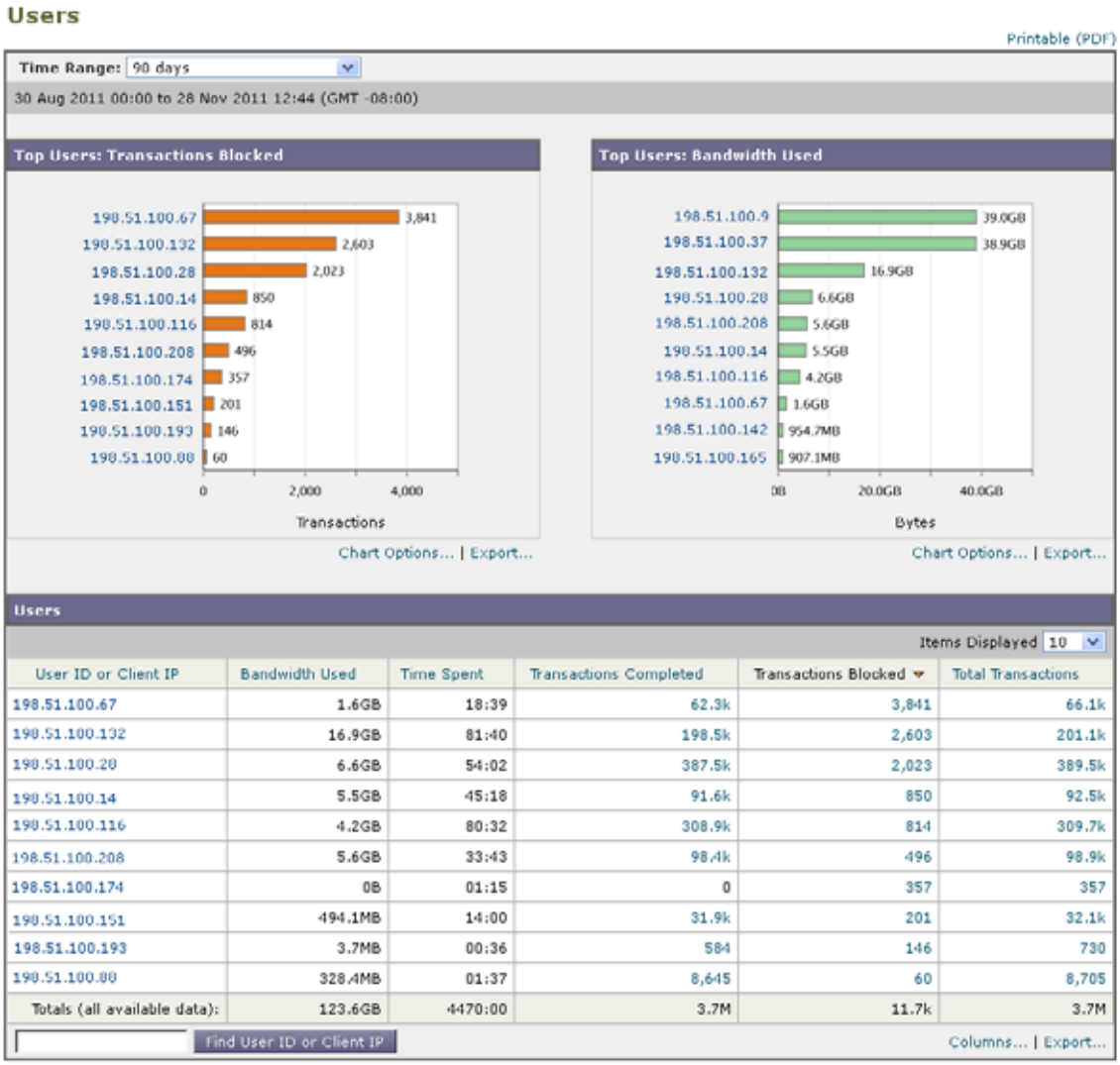
[ユーザ（Users）] レポート（Web）

[Web] > [レポート（Reporting）] > [ユーザ（Users）] ページには、各ユーザの Web レポーティング情報を表示できる複数のリンクが表示されます。

[ユーザ（Users）] ページでは、システム上のユーザ（1 人または複数）がインターネット、特定のサイト、または特定の URL で費やした時間と、そのユーザが使用している帯域幅の量を表示できます。

（注）　セキュリティ管理アプライアンスがサポートできる Web セキュリティ アプライアンス上の最大ユーザ数は 500 です。

図 5-4　[Web] > [レポート（Reporting）] > [ユーザ（Users）] ページ



[ユーザ（Users）] ページには、システム上のユーザに関する次の情報が表示されます。

表 5-5　[Web] > [レポート（Reporting）] > [ユーザ（Users）] ページの詳細

セクション	説明
時間範囲（Time Range）（ドロップダウン リスト）	1 ～ 90 日間またはカスタム日数範囲を指定できるドロップダウン リスト。時間範囲の詳細と実際のニーズに合わせたカスタマイズについては、「レポートの時間範囲の選択」（P.3-4）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、IP アドレスまたはユーザ名で示された上位ユーザ（縦の目盛り）、そのユーザがブロックされたトランザクションの数（横の目盛り）が表示されます。レポーティングを目的として、ユーザ名または IP アドレスを認識できないようにすることができます。このページまたはスケジュール設定されたレポートでユーザ名を認識不可能にする方法の詳細については、「セキュリティ管理アプライアンスでの中央集中型 Web レポーティングのイネーブル化」（P.5-3）を参照してください。デフォルト設定では、すべてのユーザ名が表示されます。ユーザ名を非表示にするには、「Web レポートでのユーザ名の匿名化」（P.5-5）を参照してください。
使用済み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）を使用している上位ユーザが、IP アドレスまたはユーザ名（縦の目盛り）で表示されます。
[ユーザ（Users）] テーブル	このテーブルのデータの詳細については、「Web レポートのテーブル カラムの説明」（P.5-11）を参照してください。 さらに、特定のユーザ ID またはクライアント IP アドレスを検索できます。[ユーザ（User）] セクション下部のテキスト フィールドに特定のユーザ ID またはクライアント IP アドレスを入力し、[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）] をクリックします。IP アドレスが正確に一致していなくても結果は返されます。 [ユーザ（Users）] テーブルでは、特定のユーザをクリックして、さらに具体的な情報を得ることができます。この情報は、[ユーザの詳細（User Details）] ページに表示されます。[ユーザの詳細（User Details）] ページの詳細については、「[ユーザの詳細（User Details）]（Web レポーティング）」（P.5-20）を参照してください。

（注） クライアント IP アドレスの代わりにユーザ ID を表示するには、セキュリティ管理アプライアンスを設定し、LDAP サーバからユーザ情報を取得する必要があります。詳細については、第 9 章の「Creating the LDAP Server Profile」を参照してください。

ヒント このレポートのビューをカスタマイズするには、「インタラクティブ Web レポーティング ページの操作」（P.5-7）を参照してください。

[ユーザ（Users）] ページの使用例については、「例 1：ユーザの調査」（P.D-1）を参照してください。

（注）　[ユーザ（Users）] ページについて、レポートを生成またはスケジュールすることができます。詳細については、「スケジュール設定されたレポートとオンデマンド Web レポートについて」（P.5-66）を参照してください。

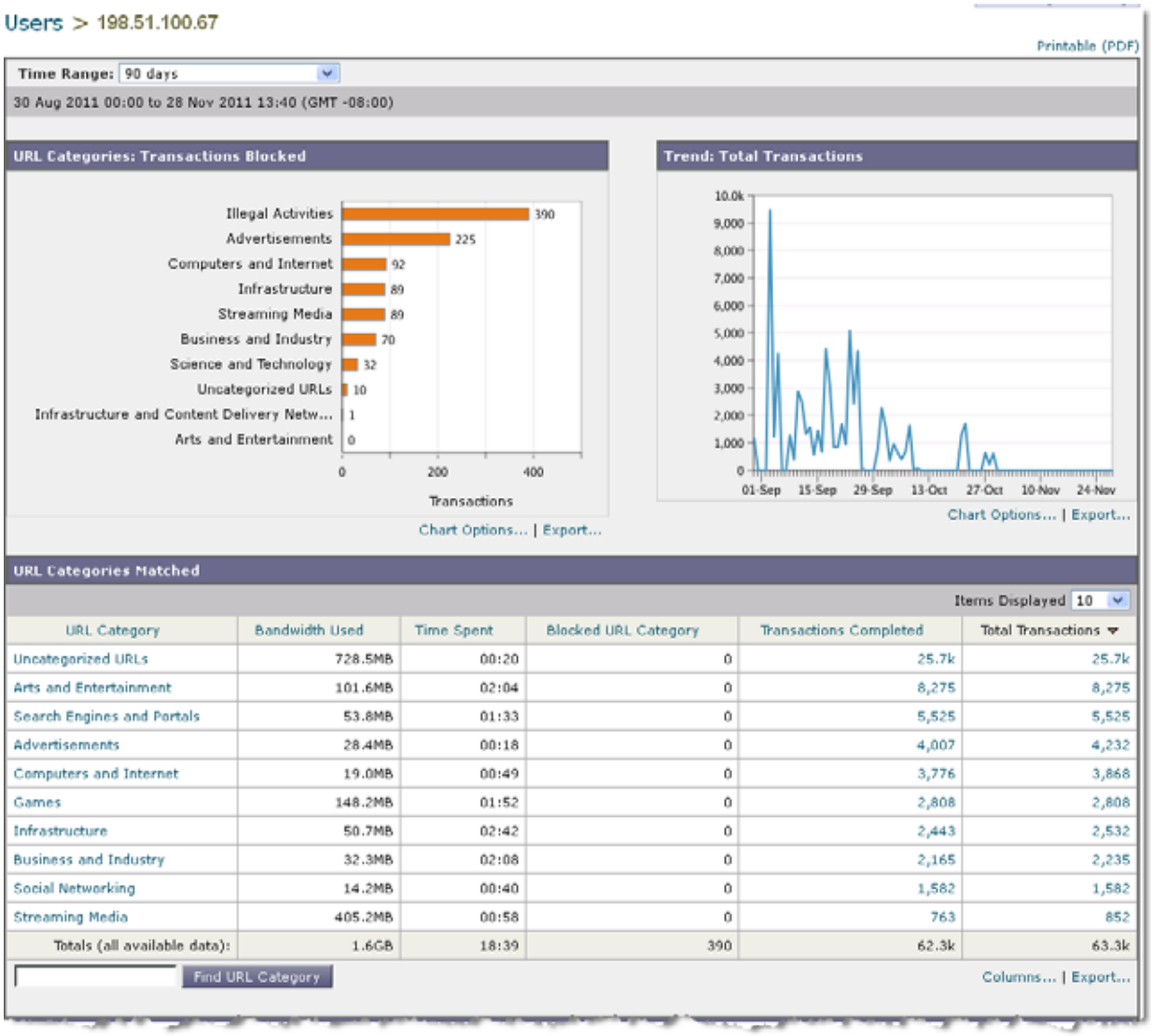
[ユーザの詳細（User Details）]（Web レポーティング）

[ユーザの詳細（User Details）] ページでは、[Web] > [レポート（Reporting）] > [ユーザ（Users）] ページのインタラクティブな [ユーザ（Users）] テーブルで指定したユーザに関する具体的な情報を確認できます。

[ユーザの詳細（User Details）] ページでは、システムでの個々のユーザのアクティビティを調査できます。特に、ユーザ レベルの調査を実行している場合に、ユーザがアクセスしているサイト、ユーザが直面しているマルウェアの脅威、ユーザがアクセスしている URL カテゴリ、これらのサイトで特定のユーザが費やしている時間などを確認する必要があるときは、このページが役立ちます。

特定のユーザの [ユーザの詳細（User Details）] ページを表示するには、[Web] > [ユーザ（Users）] ページの [ユーザ（User）] テーブルで対象のユーザをクリックします。

図 5-5　[ユーザの詳細（User Details）] ページ



（次のページに続く）

（前ページからの続き）

Domains Matched

Items Displayed 10

Domain or IP	Bandwidth Used	Time Spent	Transactions Completed	Transactions Blocked	Total Transactions
[redacted].com	713.4MB	00:29	24.5k	0	24.5k
[redacted].com	92.4MB	02:02	8,037	0	8,037
[redacted].com	31.2MB	00:38	3,095	0	3,095
[redacted].com	1.7MB	00:56	179	1,769	1,948
[redacted].com	3.7MB	00:00	1,041	0	1,041
[redacted].com	2.4MB	02:12	1,539	80	1,619
[redacted].tv	12.6MB	00:03	1,033	0	1,033
[redacted].net	10.5MB	00:00	1,001	0	1,001
[redacted].com	46.5KB	00:57	4	898	902
[redacted].com	8.8MB	00:09	778	0	778

Find Domain or IP　　Columns... | Export...

Applications Matched

Items Displayed 10

Application	Application Type	Bandwidth Used	Transactions Completed	Other Blocked Transactions	Total Transactions
[redacted]	Internet Utilities	3.7MB	1,832	0	1,832
[redacted] Video	Media	380.6MB	1,517	0	1,517
[redacted] General	[redacted]	10.2MB	1,283	0	1,283
[redacted]	Media	274.2MB	517	0	517
[redacted]	Instant Messaging	337.3KB	95	0	95
[redacted]	Webmail	1.4MB	68	0	68
[redacted] Mail	Webmail	425.8KB	61	0	61
[redacted]	Social Networking	364.5KB	58	0	58
[redacted] Photos	[redacted]	2.2MB	54	0	54
[redacted]	Media	157.6MB	40	0	40
Totals (all available data):	--	832.1MB	5,621	0	5,621

Find Application　　Columns... | Export...

Malware Threats Detected

Malware Threat	Malware Category	Bandwidth Saved by Blocking	Transactions Monitored	Transactions Blocked	Total Malware Transactions Detected
[redacted]	Adware	0B	82	0	82
[redacted]	Adware	0B	8	0	8
[redacted]	Trojan Horse	36.0KB	0	3	3
Totals (all available data):	--	36.0KB	90	3	93

Find Malware Threat　　Columns... | Export...

Policies Matched

Policy Name	Policy Type	Bandwidth Used	Completed Transactions	Blocked Transactions	Total Transactions
Policy 1	Access	1.6GB	62.2k	1,174	63.4k
Policy 2	Access	0B	0	2,667	2,667
Policy 3	Decryption	768.3KB	91	0	91
Totals (all available data):	--	1.6GB	62.3k	3,841	66.1k

Find Policy Name　　Columns... | Export...

[ユーザの詳細（User Details）] ページには、システム上の個々のユーザに関係する次の情報が表示されます。

表 5-6　[Web] > [レポート（Reporting）] > [ユーザ（User）] > [ユーザの詳細（User Details）] ページの詳細

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。時間範囲の詳細と実際のニーズに合わせたカスタマイズについては、「レポートの時間範囲の選択」（P.3-4）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.5-28）を参照してください。
総トランザクション数別傾向（Trend by Total Transactions）	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）	[一致した URL カテゴリ（URL Categories Matched）] 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ついて、一致したカテゴリが表示されます。 このセクションでは、特定の URL カテゴリを検索することもできます。セクション下部のテキスト フィールドに URL カテゴリを入力し、[URL カテゴリの検索（Find URL Category）] をクリックします。カテゴリは正確に一致している必要はありません。 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.5-28）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 5-6　[Web] > [レポート（Reporting）] > [ユーザ（User）] > [ユーザの詳細（User Details）] ページの詳細 （続き）

セクション	説明
一致したアプリケーション（Applications Matched）	このセクションでは、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。 特定のマルウェア脅威の名前に関するデータを [マルウェア脅威の検索（Find Malware Threat）] フィールドで検索できます。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）] をクリックしてください。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、Web にアクセスする際にこのユーザに適用されるポリシー グループを検索できます。 セクション下部のテキスト フィールドにポリシー名を入力し、[ポリシーの検索（Find Policy）] をクリックします。ポリシーの名前は正確に一致している必要はありません。

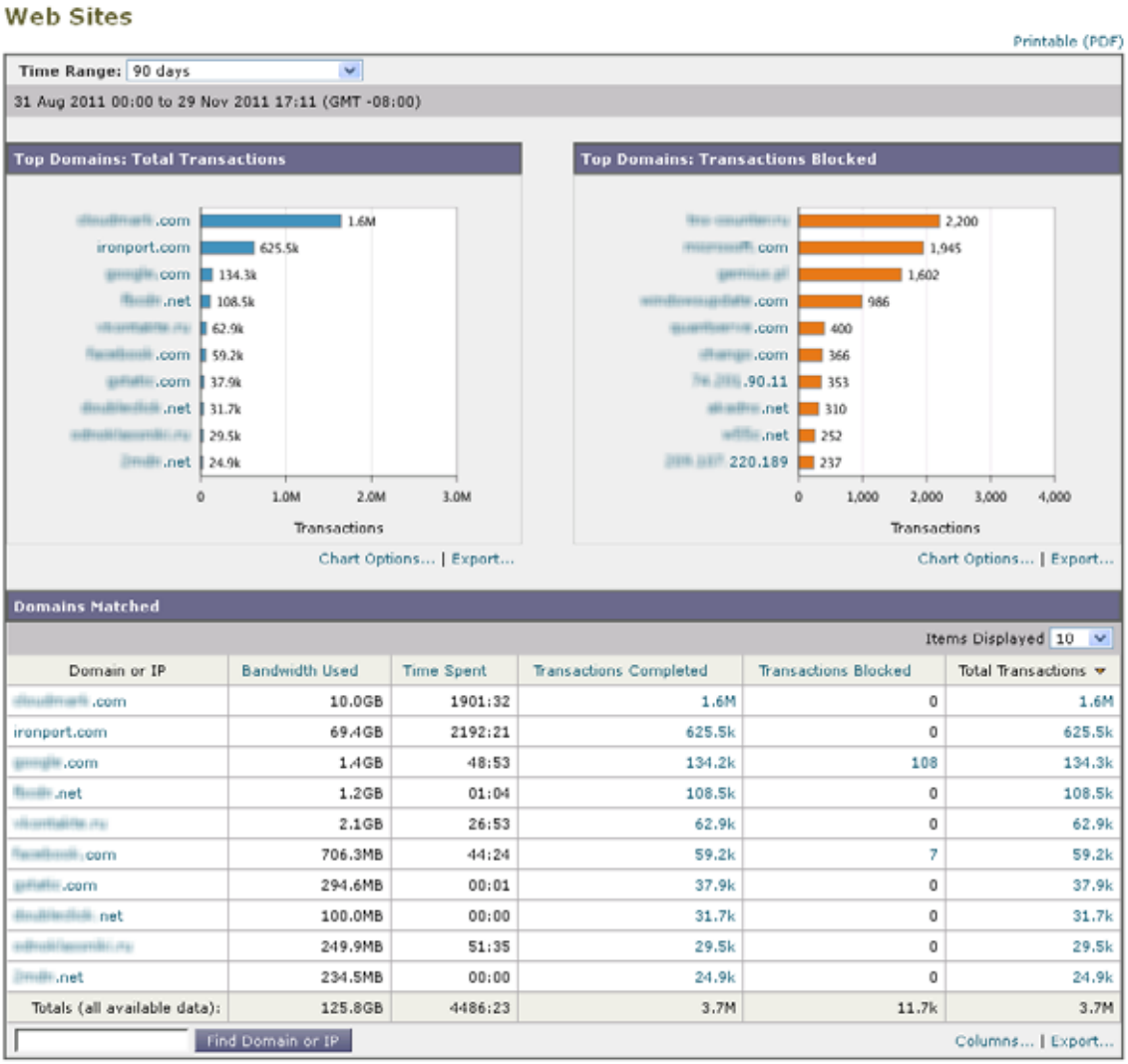
（注）　[クライアント マルウェア リスクの詳細（Client Malware Risk Details）] テーブルのクライアント レポートでは、ユーザ名の末尾にアスタリスク（*）が付いていることがあります。たとえば、クライアント レポートに「jsmith」と「jsmith*」の両方のエントリが表示される場合があります。アスタリスク（*）が付いているユーザ名は、ユーザの指定したユーザ名が認証サーバで確認されていないことを示しています。この状況は、認証サーバがその時点で使用できず、かつ認証サービスを使用できないときもトラフィックを許可するようにアプライアンスが設定されている場合に発生します。

[ユーザの詳細（Users Details）] ページの使用例については、「例 1：ユーザの調査」（P.D-1）を参照してください。

[Web サイト（Web Sites）] レポート

[Web] > [レポート（Reporting）] > [Web サイト（Web Sites）] ページでは、管理対象の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 5-6　[Web サイト（Web Sites）] ページ



[Web サイト（Web Sites）] ページには次の情報が表示されます。

表 5-7　[Web] > [レポート（Reporting）] > [Web サイト（Web Sites）] ページの詳細

セクション	説明
時間範囲（Time Range）（ドロップダウン リスト）	1 ～ 90 日間またはカスタム日数範囲を指定できるドロップダウン リスト。時間範囲の詳細と実際のニーズに合わせたカスタマイズについては、「レポートの時間範囲の選択」（P.3-4）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 5-7　[Web] > [レポート（Reporting）] > [Web サイト（Web Sites）] ページの詳細 （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。 このテーブルのデータの詳細については、「Web レポートのテーブル カラムの説明」（P.5-11）を参照してください。 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。 Web トラッキングの使用例については、「例 2：URL のトラッキング」（P.D-5）を参照してください。

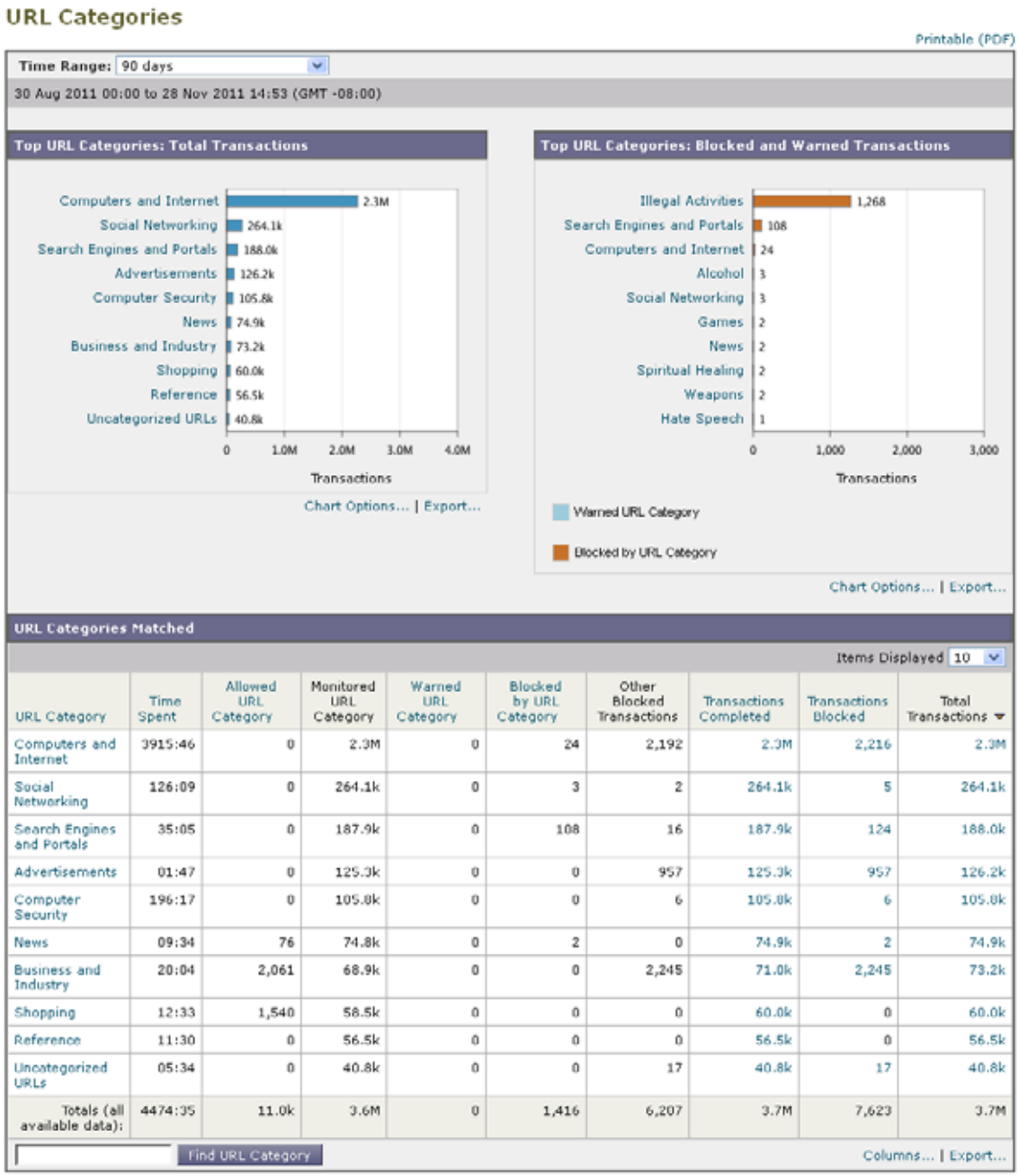
ヒント　このレポートのビューをカスタマイズするには、「インタラクティブ Web レポーティング ページの操作」（P.5-7）を参照してください。

（注）　[Web サイト（Web Sites）] ページの情報について、レポートを生成またはスケジュールすることができます。詳細については、「スケジュール設定されたレポートとオンデマンド Web レポートについて」（P.5-66）を参照してください。

URL カテゴリ レポート

[Web] > [レポート（Reporting）] > [URL カテゴリ（URL Categories）] ページを使用して、システム上のユーザがアクセスしているサイトの URL カテゴリを表示できます。

図 5-7　[URL カテゴリ（URL Categories）] ページ



[URL カテゴリ（URL Categories）] ページには次の情報が表示されます。

表 5-8　[Web] > [レポート（Reporting）] > [URL カテゴリ（URL Categories）] ページの詳細

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、「レポートの時間範囲の選択」（P.3-4）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 5-8　[Web] > [レポート（Reporting）] > [URL カテゴリ（URL Categories）] ページの詳細

セクション	説明
ブロックまたは警告され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、『*Cisco IronPort AsyncOS for Web Security User Guide*』の「Custom URL Categories」を参照してください。 • 既存またはその他のカテゴリに含めるべきサイトについては、「誤って分類された URL と未分類の URL のレポート」（P.5-29）を参照してください。

ヒント　このレポートのビューをカスタマイズするには、「インタラクティブ Web レポーティング ページの操作」（P.5-7）を参照してください。

（注）

- このページよりもさらに詳細なレポートを生成するには、「上位 URL カテゴリ - 拡張（Top URL Categories — Extended）」（P.5-68）を参照してください。
- URL カテゴリに関するスケジュール設定されたレポート内でデータ アベイラビリティが使用されている場合に、いずれかのアプライアンスでデータに欠落があると、ページの下部に「この時間範囲の一部のデータは使用不可でした。（`Some data in this time range was unavailable.`）」というメッセージが表示されます。欠落がない場合は何も表示されません。

URL カテゴリ セットの更新とレポート

「URL カテゴリ セットの更新と中央集中型コンフィギュレーション管理」（P.9-24）で説明されているように、セキュリティ管理アプライアンスでは一連の定義済み URL カテゴリが定期的に更新される場合があります。

これらの更新が行われた場合、古いカテゴリのデータは、古すぎて価値がなくなるまで、引き続きレポートと Web トラッキング結果に表示されます。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）] ページと [アプリケーションの表示（Application Visibility）] レポートおよび [ユーザ（Users）] レポート（Web）を併用すると、特定のユーザと、特定のユーザがアクセスしようとしているアプリケーション タイプまたは Web サイトを調査できます。

たとえば、URL カテゴリ レポートで、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）] インタラクティブ 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）]（Web レポーティング）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 [トランザクション完了（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 サービスによって処理された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。

[URL カテゴリ（URL Categories）] ページの他の使用例については、「例 3：アクセス数の多い URL カテゴリの調査」（P.D-6）を参照してください。

誤って分類された URL と未分類の URL のレポート

誤って分類された URL と未分類の URL について、次の URL で報告できます。

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

送信内容は評価され、今後のルール更新に活用されます。

送信された URL のステータスを確認するには、このページの [送信した URL のステータス（Status on Submitted URLs）] タブをクリックします。

[アプリケーションの表示（Application Visibility）] レポート

（注）[アプリケーションの表示（Application Visibility）] の詳細については、『*Cisco IronPort AsyncOS for Web Security User Guide*』の「Understanding Application Visibility and Control」を参照してください。

[Web] > [レポート（Reporting）] > [アプリケーションの表示（Application Visibility）] ページでは、セキュリティ管理アプライアンスおよび Web セキュリティ アプライアンス内の特定のアプリケーション タイプに制御を適用できます。

アプリケーション制御を使用すると、URL フィルタリングのみを使用する場合よりも Web トラフィックをきめ細かく制御できるだけでなく、次のタイプのアプリケーションおよびアプリケーション タイプの制御を強化できます。

- 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、Facebook、インスタント メッセージングなど）。
- 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）。

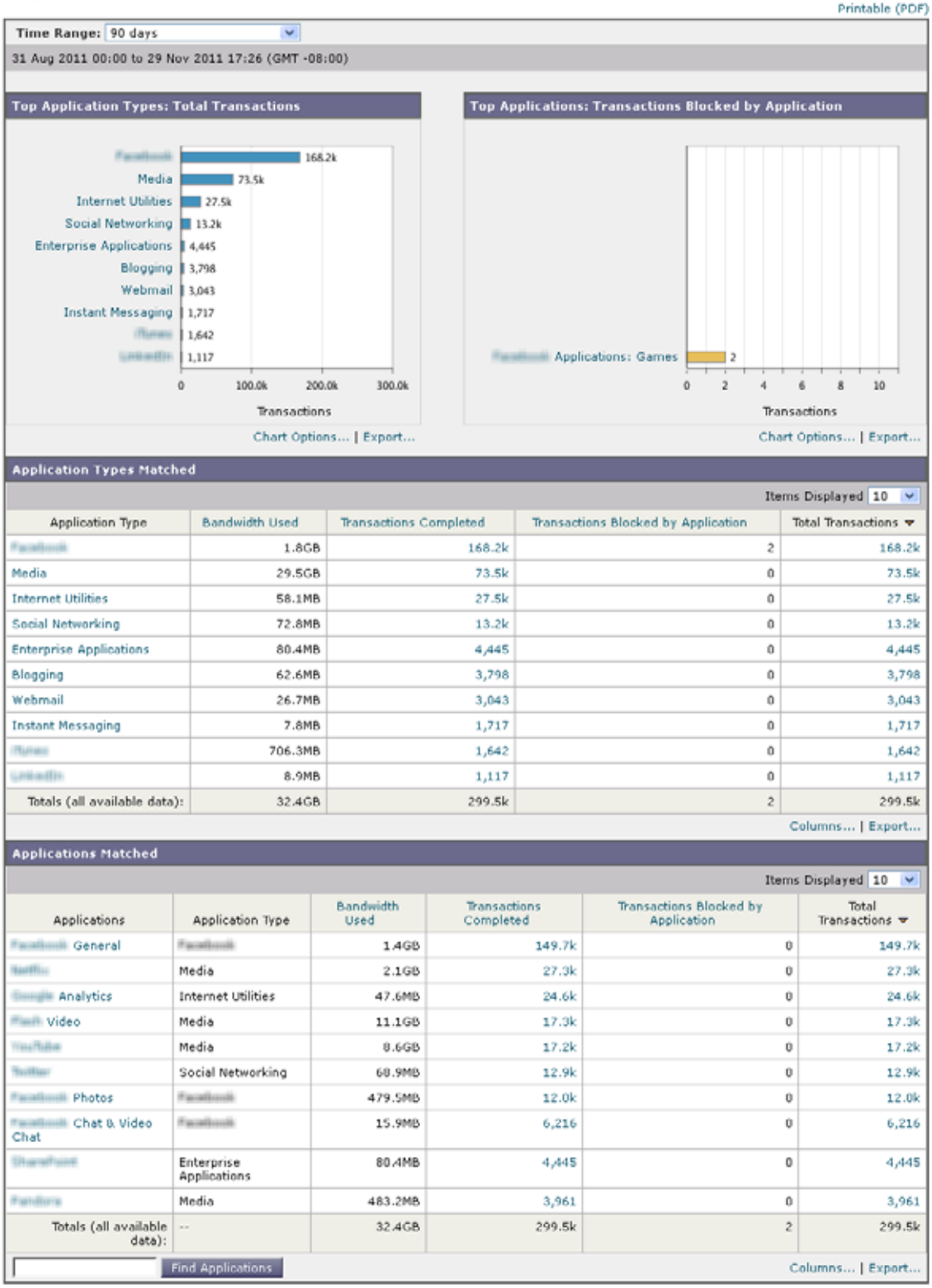
アプリケーションとアプリケーション タイプの違いについて

レポートに関連するアプリケーションを制御するには、アプリケーションとアプリケーション タイプの違いを理解することが非常に重要です。

- **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**検索エンジン**は、Google Search や Craigslist などの検索エンジンを含むアプリケーション タイプです。インスタント メッセージングは、Yahoo Instant Messenger や Cisco WebEx などを含む別のアプリケーション タイプです。Facebook もアプリケーション 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。**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です。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。

（注）Application Visibility and Control（AVC）エンジンを使用して Facebook アクティビティを制御する方法の詳細については、『*Cisco IronPort AsyncOS for Web Security User Guide*』の「Understanding Application Visibility and Control」を参照してください。

図 5-8　[アプリケーションの表示（Application Visibility）] ページ



[アプリケーションの表示（Application Visibility）] ページには次の情報が表示されます。

表 5-9　[Web] > [レポート（Reporting）] > [アプリケーションの表示（Application Visibility）] ページの詳細

セクション	説明
時間範囲（Time Range）（ドロップダウン リスト）	1 ～ 90 日間またはカスタム日数範囲を指定できるドロップダウン リスト。時間範囲の詳細と実際のニーズに合わせたカスタマイズについては、「レポートの時間範囲の選択」（P.3-4）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、Facebook、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 や Yahoo Instant Messenger などの特定のアプリケーション タイプを起動しようとしたが、特定のポリシーが適用されているために、ブロック アクションがトリガーされたとします。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）] インタラクティブ 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）] テーブル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。これはインタラクティブなカラム見出しのあるインタラクティブ テーブルとなっていて、必要に応じてデータをソートできます。 [一致したアプリケーション（Applications Matched）] セクションに表示するカラムを設定することができます。このセクションのカラムの設定については、「インタラクティブ Web レポーティング ページの操作」（P.5-7）を参照してください。 [アプリケーション（Applications）] テーブルに表示する項目を選択後、表示する項目の数を [表示されたアイテム（Items Displayed）] ドロップダウン メニューから選択できます。選択肢は [10]、[20]、[50]、[100] です。 さらに、[一致したアプリケーション（Applications Matched）] セクション内で特定のアプリケーションを検索できます。このセクション下部のテキスト フィールドに特定の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。

ヒント　このレポートのビューをカスタマイズするには、「インタラクティブ Web レポーティング ページの操作」（P.5-7）を参照してください。

（注）　[アプリケーションの表示（Application Visibility）] ページの情報に関して、スケジュール設定されたレポートを生成することができます。レポートのスケジュール設定については、「スケジュール設定されたレポートとオンデマンド Web レポートについて」（P.5-66）を参照してください。

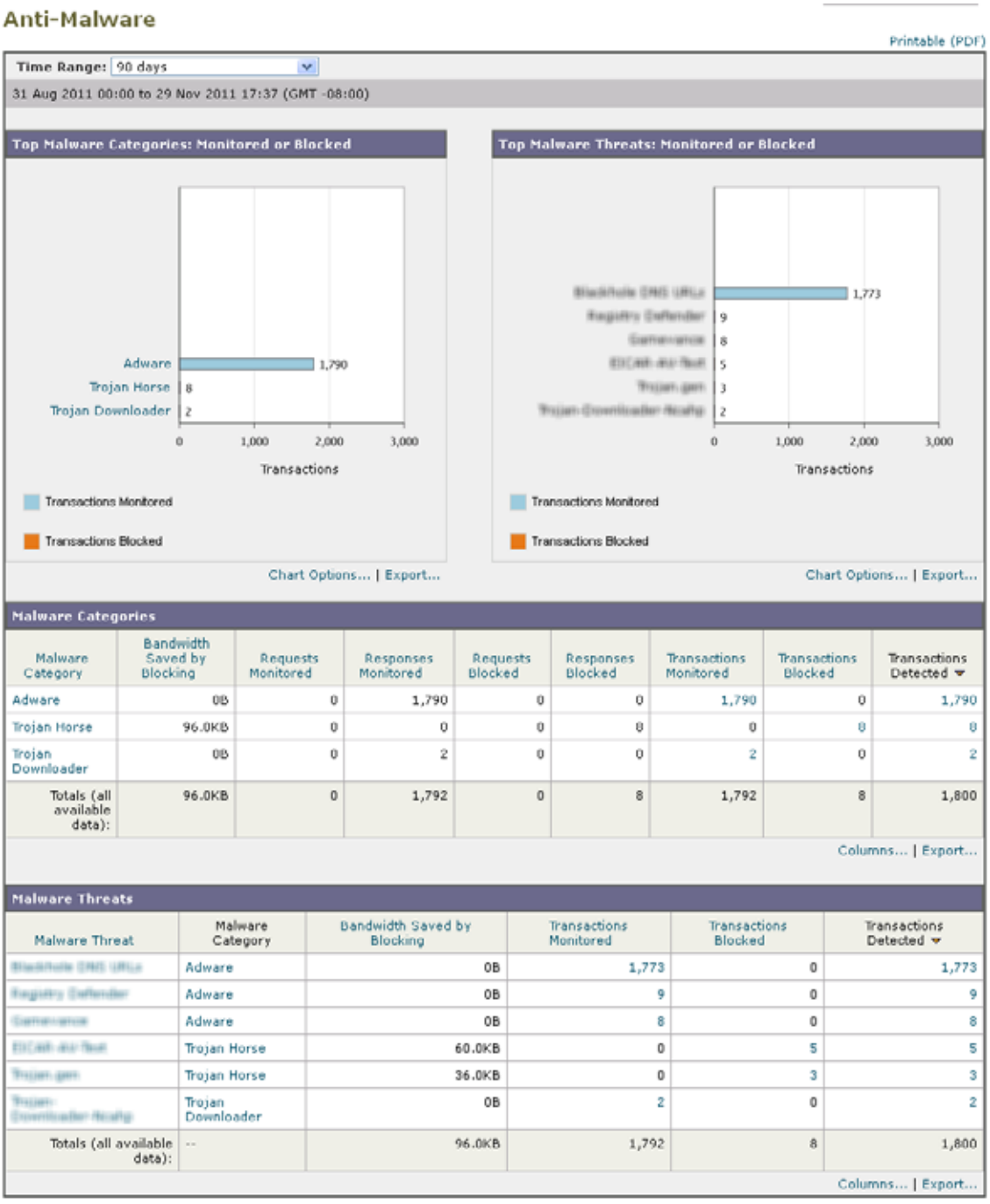
[マルウェア対策（Anti-Malware）] レポート

[Web] > [レポート（Reporting）] > [マルウェア対策（Anti-Malware）] ページはセキュリティ関連のレポーティング ページであり、イネーブルなスキャン エンジン（Webroot、Sophos、McAfee、または Adaptive Scanning）によるスキャン結果が反映されます。

このページを使用して、Web ベースのマルウェアの脅威を特定およびモニタすることができます。

（注）　L4 トラフィック モニタリングで検出されたマルウェアのデータを表示するには、「[L4 トラフィック モニタ（L4 Traffic Monitor）] レポート」（P.5-46）を参照してください。

図 5-9　[マルウェア対策（Anti-Malware）] ページ



[マルウェア対策（Anti-Malware）] ページには次の情報が表示されます。

表 5-10　[Web] > [レポート（Reporting）] > [マルウェア対策（Anti-Malware）] ページの詳細

セクション	説明
時間範囲（Time Range）（ドロップダウン リスト）	1 ～ 90 日間またはカスタム日数範囲を指定できるドロップダウン リスト。時間範囲の詳細と実際のニーズに合わせたカスタマイズについては、「レポートの時間範囲の選択」（P.3-4）を参照してください。
上位マルウェア カテゴリ：モニタまたはブロック（Top Malware Categories: Monitored or Blocked）	このセクションには、所定のカテゴリ タイプ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。有効なマルウェア 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.5-39）を参照してください。
上位マルウェア脅威：モニタまたはブロック（Top Malware Threats: Monitored or Blocked）	このセクションには、上位のマルウェアの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）] インタラクティブ テーブルには、[上位マルウェア カテゴリ（Top Malware Categories）] チャート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。 [マルウェア カテゴリ（Malware Categories）] インタラクティブ 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。 例外：このテーブルの [アウトブレイク ヒューリスティック（Outbreak Heuristics）] リンクを使用すると、そのカテゴリでいつトランザクションが発生したかを示すチャートが表示されます。 有効なマルウェア 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.5-39）を参照してください。
マルウェア脅威（Malware Threats）	[マルウェア脅威（Malware Threats）] インタラクティブ 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 [不明マルウェア（Unnamed Malware）] が表示されます。

ヒント　このレポートのビューをカスタマイズするには、「インタラクティブ Web レポーティング ページの操作」（P.5-7）を参照してください。

マルウェア カテゴリ レポート

[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。

[マルウェア カテゴリ（Malware Category）] レポート ページにアクセスするには、次の手順を実行します。

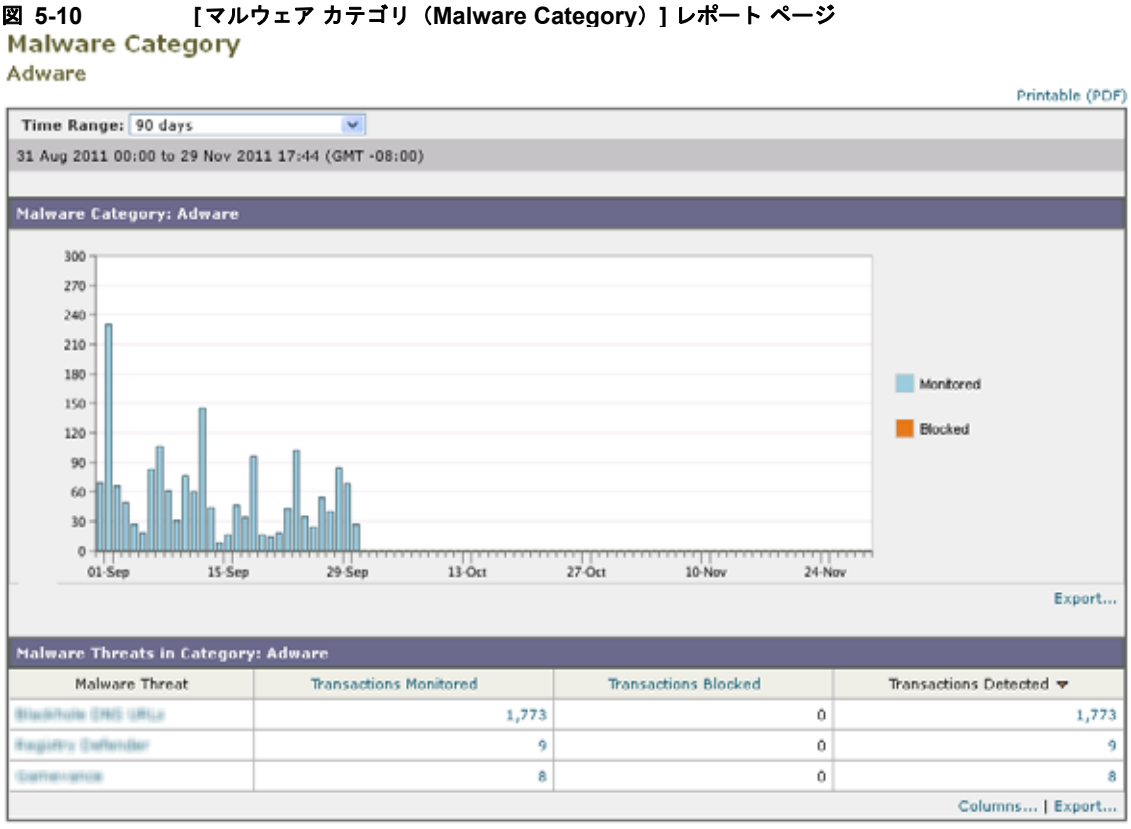
手順

ステップ 1　セキュリティ管理アプライアンスで、[Web] > [レポート（Reporting）] > [マルウェア対策（Anti-Malware）] を選択します。

ステップ 2　[マルウェア カテゴリ（Malware Categories）] インタラクティブ テーブルで、[マルウェア カテゴリ（Malware Category）] カラム内のカテゴリをクリックします。

[マルウェア カテゴリ（Malware Category）] レポート ページが表示されます。

図 5-10　[マルウェア カテゴリ（Malware Category）] レポート ページ



ステップ 3　このレポートのビューをカスタマイズするには、「インタラクティブ Web レポーティング ページの操作」（P.5-7）を参照してください。

[マルウェア脅威（Malware Threat）] レポート

[マルウェア脅威（Malware Threat）] 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。

[マルウェア脅威（Malware Threat）] レポート ページにアクセスするには、次の手順を実行します。

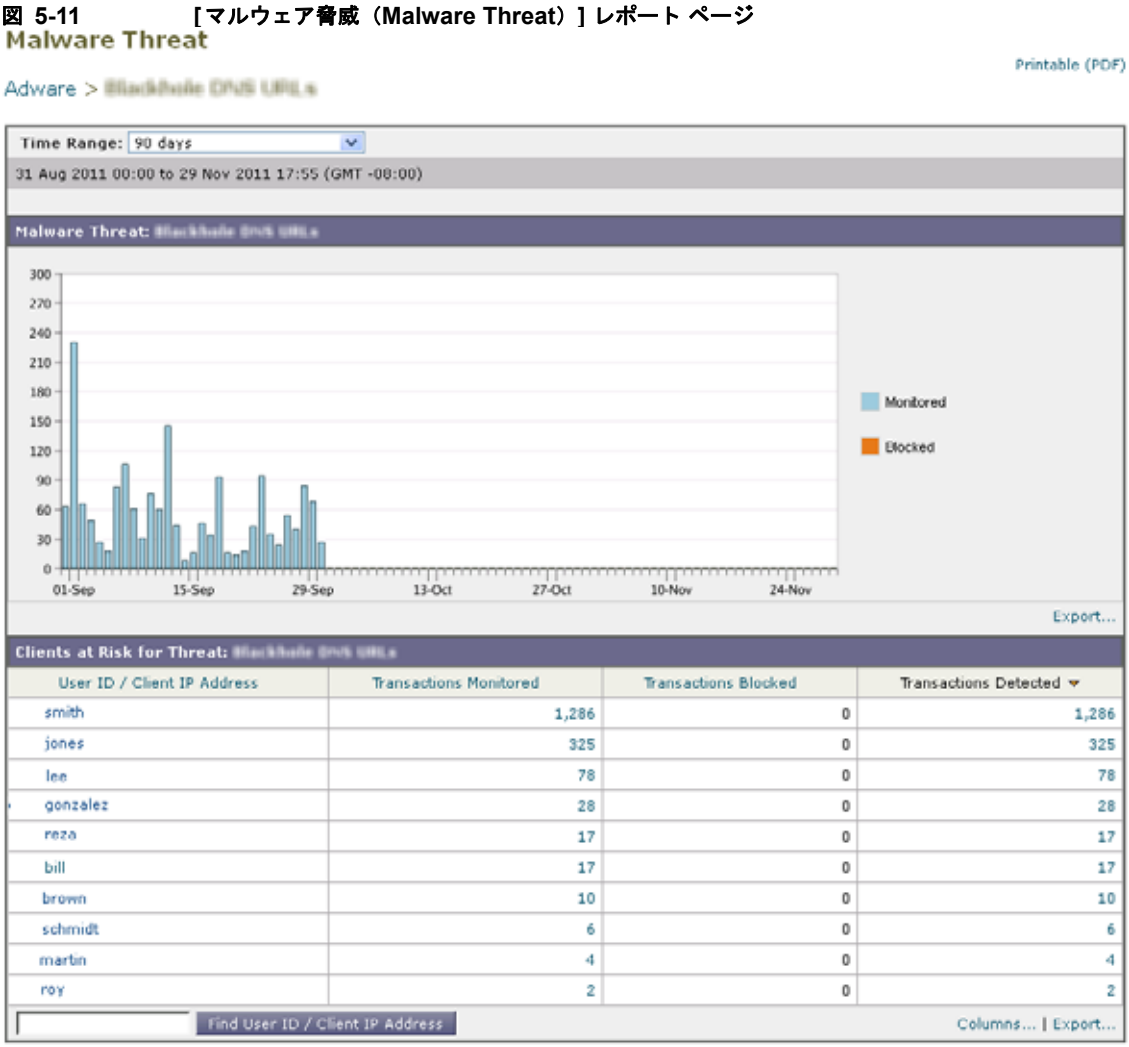
手順

ステップ 1　セキュリティ管理アプライアンスで、[Web] > [レポート（Reporting）] > [マルウェア対策（Anti-Malware）] を選択します。

ステップ 2　[マルウェア脅威（Malware Threat）] インタラクティブ テーブルで、[マルウェア カテゴリ（Malware Category）] カラム内のカテゴリをクリックします。

[マルウェア脅威（Malware Threat）] レポート ページが表示されます。

図 5-11　[マルウェア脅威（Malware Threat）] レポート ページ



ステップ 3　このレポートのビューをカスタマイズするには、「インタラクティブ Web レポーティング ページの操作」（P.5-7）を参照してください。

ステップ 4　詳細については、テーブルの下の [サポート ポータル マルウェア詳細（Support Portal Malware Details）] リンクをクリックしてください。

（注）　[マルウェア対策（Anti-Malware）] ページの [検出した上位マルウェア カテゴリ（Top Malware Categories Detected）] および [検出した上位マルウェア脅威（Top Malware Threats Detected）] に関して、スケジュール設定されたレポートを生成することができます。ただし、[マルウェア カテゴリ（Malware Categories）] および [マルウェア脅威（Malware Threats）] レポート ページから生成されるレポートを、スケジュール設定することはできません。レポートのスケジュール設定については、「スケジュール設定されたレポートとオンデマンド Web レポートについて」（P.5-66）を参照してください。

マルウェアのカテゴリについて

Web セキュリティ アプライアンスは、次のタイプのマルウェアをブロックできます。

マルウェアのタイプ	説明
アドウェア	アドウェアには、販売目的でユーザを製品に誘導する、すべてのソフトウェア実行可能ファイルおよびプラグインが含まれます。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。
アウトブレイク ヒューリスティック	このカテゴリは、他のアンチマルウェア エンジンとは別に、Adaptive Scanning によって検出されたマルウェアを示しています。
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。
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。ウイルスとは異なり、トロイの木馬は自己複製しません。

マルウェアのタイプ	説明
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。
ウイルス	ウイルスは、ユーザが気付かない間にコンピュータにロードされ、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。

[クライアント マルウェア リスク（Client Malware Risk）] レポート

[Web] > [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 5-12 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 5-12　[クライアント マルウェア リスク（Client Malware Risk）] ページ

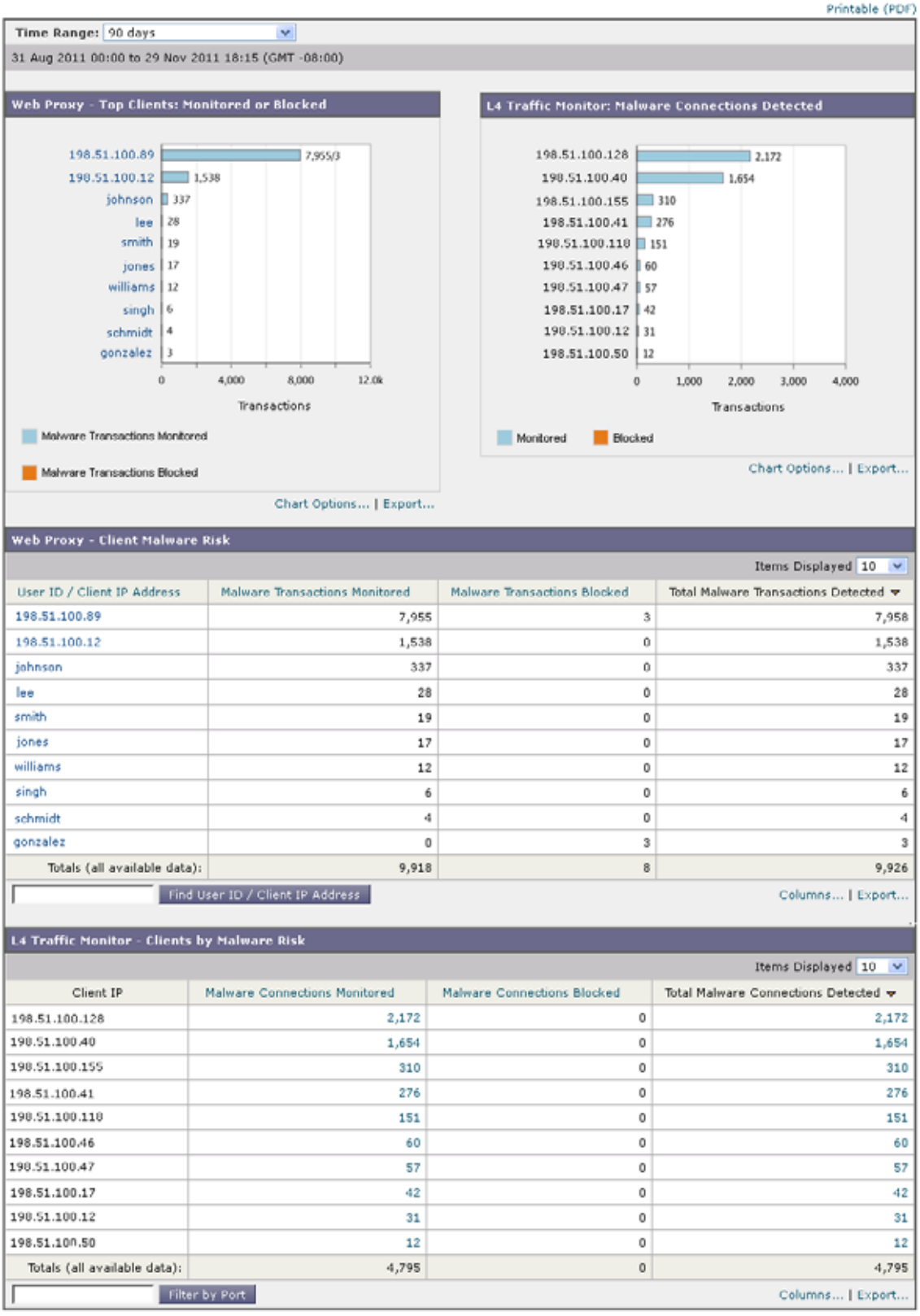


表 5-11 で [クライアント マルウェア リスク（Client Malware Risk）] ページの情報について説明します。

表 5-11　[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、「レポートの時間範囲の選択」（P.3-4）を参照してください。
Web プロキシ：モニタまたはブロックされた上位クライアント（Web Proxy: Top Clients Monitored or Blocked）	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数（L4 Traffic Monitor: Malware Connections Detected）	このチャートには、組織内で最も頻繁にマルウェア サイトに接続している 10 台のコンピュータの 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）] レポート」（P.5-46）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：クライアント マルウェア リスク（Web Proxy: Client Malware Risk）	[Web プロキシ：クライアント マルウェア リスク（Web Proxy: Client 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。 このテーブルで各ユーザをクリックすると、そのクライアントに関連する [ユーザの詳細（User Details）] ページが表示されます。このページの詳細については、「[ユーザの詳細（User Details）]（Web レポーティング）」（P.5-20）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）] レポート」（P.5-46）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。

ヒント　このレポートのビューをカスタマイズするには、「インタラクティブ Web レポーティング ページの操作」（P.5-7）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）] レポート

[Web] > [レポート（Reporting）] > [Web レピュテーション フィルタ（Web Reputation Filters）] 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。

Web レピュテーション フィルタとは

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、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 に割り当てます。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、URL 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するとともに、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、アクセス ポリシーと復号化ポリシーの両方と組み合わせて使用できます。

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。

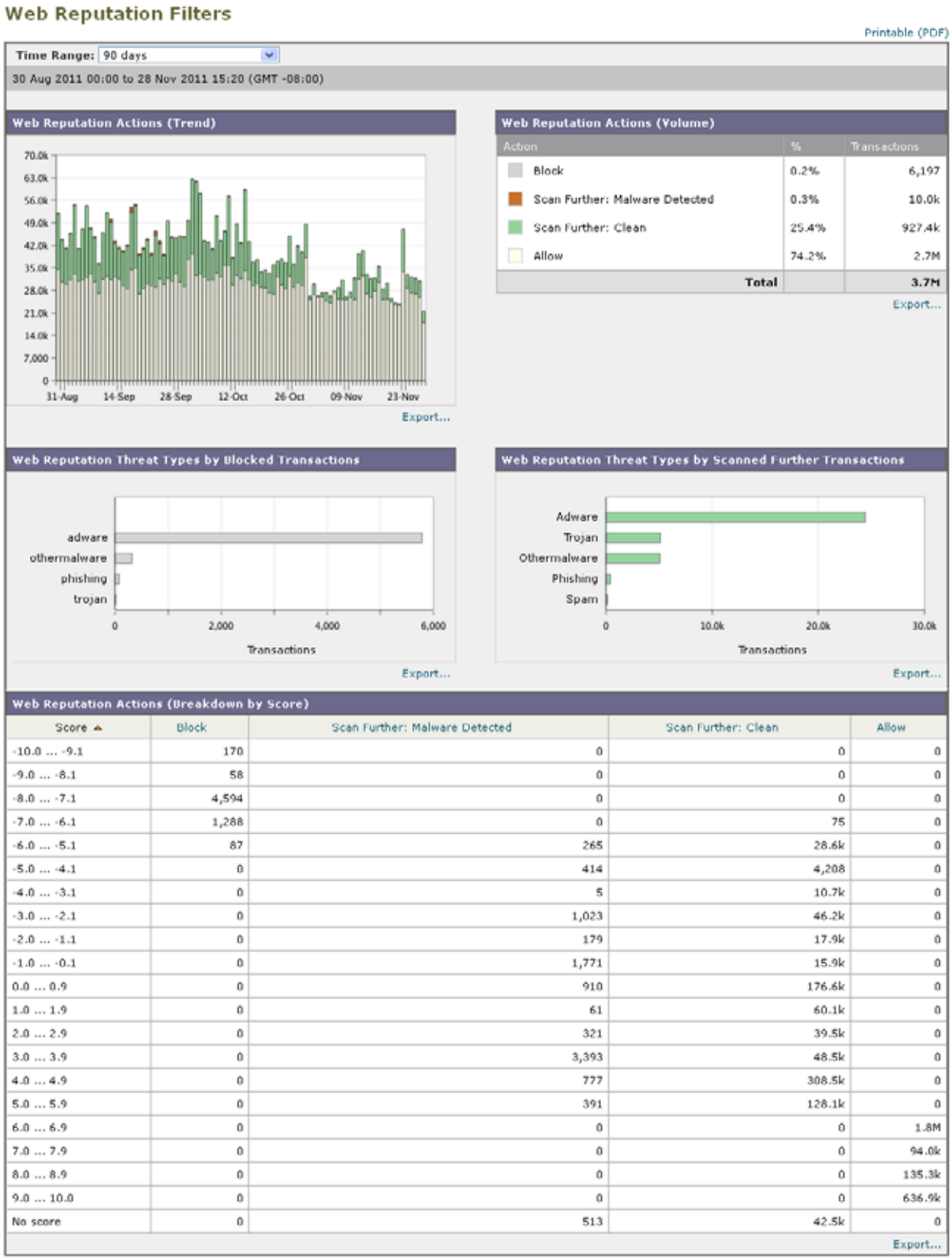
Web レピュテーションの計算では、URL をネットワーク パラメータに関連付けて、マルウェアが存在する可能性が判定されます。マルウェアが存在する可能性の累計が、-10 ～ +10 の Web レピュテーション スコアにマッピングされます（+10 がマルウェアを含む可能性が最も低い）。

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

Web レピュテーション フィルタリングの詳細については、『*Cisco IronPort AsyncOS for Web Security User Guide*』の「Web Reputation Filters」を参照してください。

図 5-13　[Web レピュテーション フィルタ（Web Reputation Filters）] ページ



[Web レピュテーション フィルタ（Web Reputation Filters）] ページには次の情報が表示されます。

表 5-12　[Web] > [レポート（Reporting）] > [Web レピュテーション フィルタ（Web Reputation Filters）] ページの詳細

セクション	説明
時間範囲（Time Range）（ドロップダウン リスト）	1 ～ 90 日間またはカスタム日数範囲を指定できるドロップダウン リスト。時間範囲の詳細と実際のニーズに合わせたカスタマイズについては、「レポートの時間範囲の選択」（P.3-4）を参照してください。
Web レピュテーション アクション（傾向）（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。
Web レピュテーション脅威タイプ（ブロックされたトランザクション別）（Web Reputation Threat Types by Blocked Transactions）	このセクションには、ブロックされた Web レピュテーション タイプが表示されます。
Web レピュテーション脅威タイプ（詳細にスキャンされたトランザクション別）（Web Reputation Threat Types by Scanned Further Transactions）	Adaptive Scanning がイネーブルの場合、このセクションには脅威の可能性が検出されたトランザクションの数が表示されます。 Adaptive Scanning がイネーブルでない場合、このセクションにはブロックされたためにさらにスキャンを必要とする Web レピュテーション タイプが表示されます。Web レピュテーション フィルタリングの結果が「Scan Further」の場合、トランザクションはアンチマルウェア ツールに渡されて追加のスキャンが行われます。
Web レピュテーション アクション（スコアによる内訳）（Web Reputation Actions (Breakdown by Score)）	Adaptive Scanning がイネーブルでない場合、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。

ヒント　このレポートのビューをカスタマイズするには、「インタラクティブ Web レポーティング ページの操作」（P.5-7）を参照してください。

Web レピュテーション設定の調整

指定済みの Web レピュテーションの設定は、レポート結果に基づいて調整することができます。たとえば、しきい値スコアを調整したり、Adaptive Scanning をイネーブルまたはディセーブルにしたりできます。Web レピュテーションの設定に関する詳細については、お使いの Cisco IronPort AsyncOS for Web Security のバージョンに対応するユーザ ガイドを参照してください。

[L4 トラフィック モニタ（L4 Traffic Monitor）] レポート

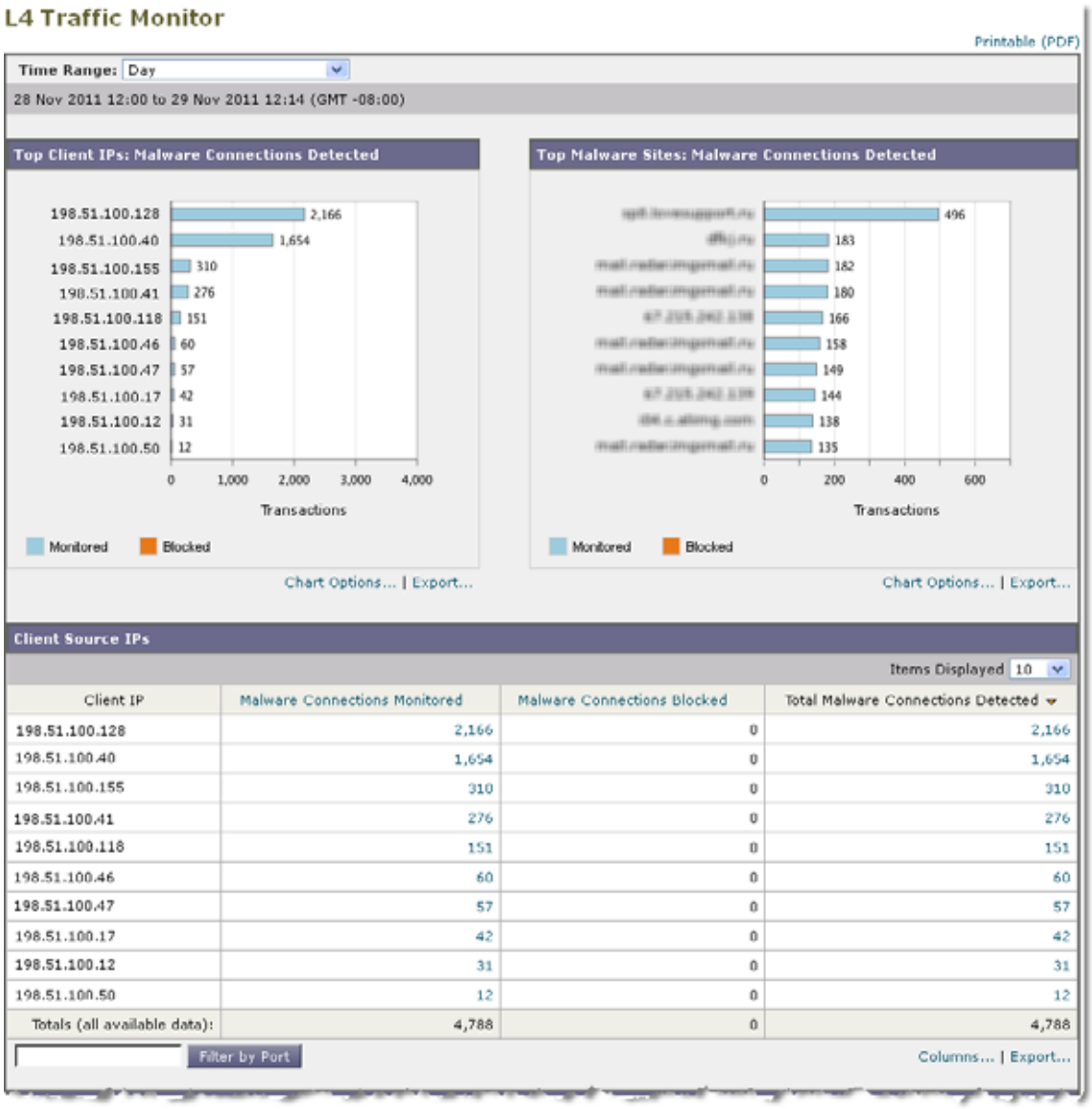
[Web] > [レポート（Reporting）] > [L4 トラフィック モニタ（L4 Traffic Monitor）] ページは指定した時間範囲内に L4 トラフィック モニタによってお使いの Web セキュリティ アプライアンス上で検出されたマルウェア ポートとマルウェア サイトに関する情報が表示されます。マルウェア サイトに頻繁にアクセスしているクライアントの IP アドレスも表示されます。

L4 トラフィック モニタは、各 Web セキュリティ 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。

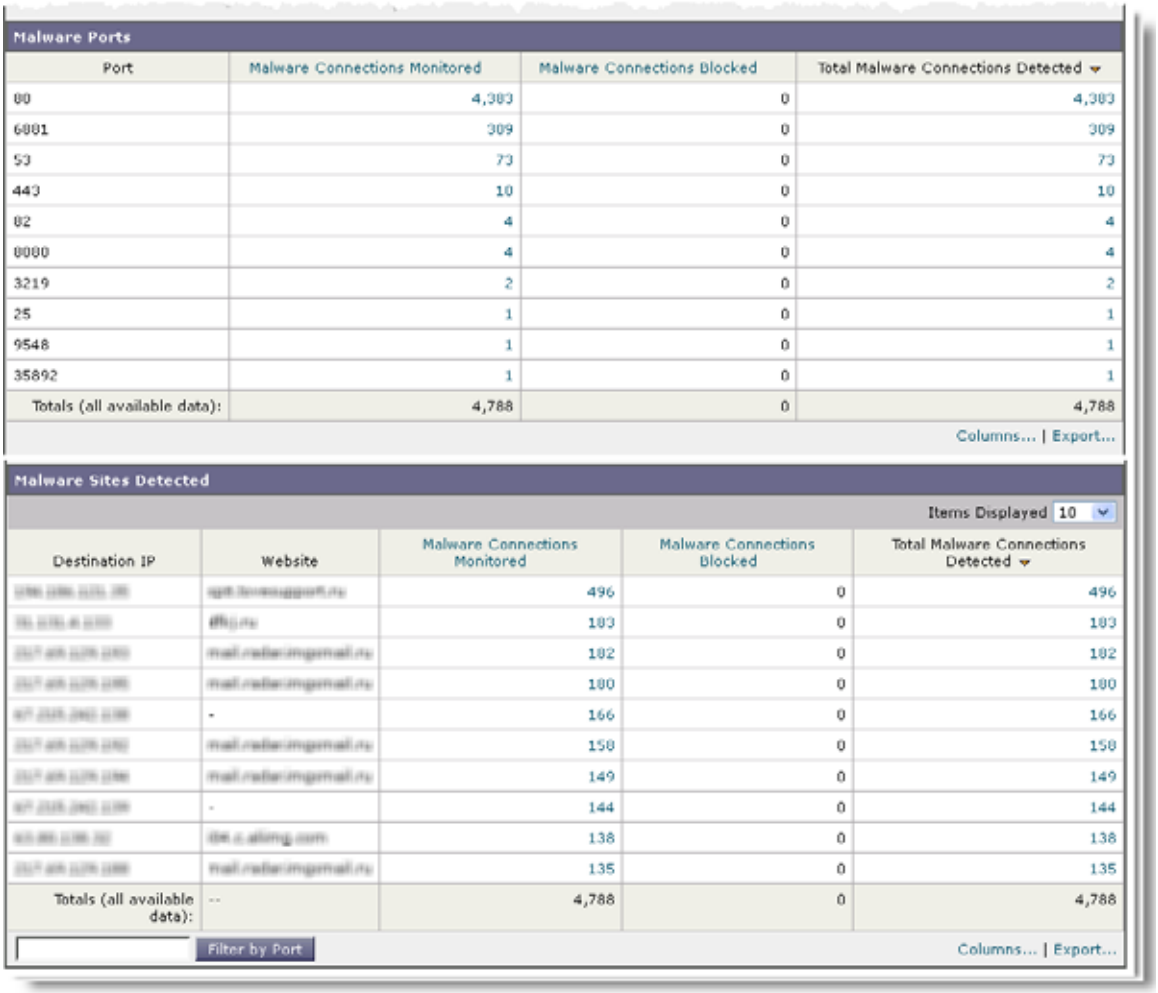
ヒント　このレポートのビューをカスタマイズするには、「インタラクティブ Web レポーティング ページの操作」（P.5-7）を参照してください。

図 5-14　[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 5-13 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 5-13　[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、「レポートの時間範囲の選択」（P.3-4）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 [グラフ 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総数（Malware Connections Detected）] から [マルウェア接続がモニタされました（Malware Connections Monitored）] または [マルウェア接続がブロックされました（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）] レポート」（P.5-40）の [L4 トラフィック モニタ : 検出されたマルウェア接続数（L4 Traffic Monitor: Malware Connections Detected）] 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 [グラフ 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総数（Malware Connections Detected）] から [マルウェア接続がモニタされました（Malware Connections Monitored）] または [マルウェア接続がブロックされました（Malware Connections Blocked）] に変更できます。

表 5-13　[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
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 [マルウェア接続がブロックされました（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、[Web] > [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たトランザクションの検索」（P.5-60）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）] レポート」（P.5-40）の [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）] テーブルと同じです。
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、[検出されたマルウェア接続総数（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、[Web] > [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たトランザクションの検索」（P.5-60）を参照してください。

表 5-13　[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 サイトが検出されました（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、[マルウェア接続がブロックされました（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、[Web] > [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たトランザクションの検索」（P.5-60）を参照してください。

ヒント　このレポートのビューをカスタマイズするには、「インタラクティブ Web レポーティング ページの操作」（P.5-7）を参照してください。

関連トピック

- 「L4 トラフィック モニタによって処理されたトランザクションの検索」（P.5-60）

[SOCKS プロキシ（SOCKS Proxy）] レポート

[Web] > [レポート（Reporting）] > [SOCKS プロキシ（SOCKS Proxy）] ページでは、宛先、ユーザなど、SOCKS プロキシを通じて処理されたトランザクションのデータおよびトレンドを表示できます。

（注）　レポートに表示される宛先は、SOCKS クライアント（通常はブラウザ）が SOCKS プロキシに送信するアドレスです。

SOCKS ポリシーの設定を変更する方法については、『*Cisco IronPort AsyncOS for Web Security User Guide*』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

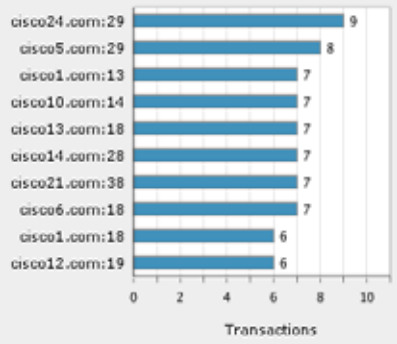


Chart Options... | Export...

Top Users for SOCKS: Total Transactions

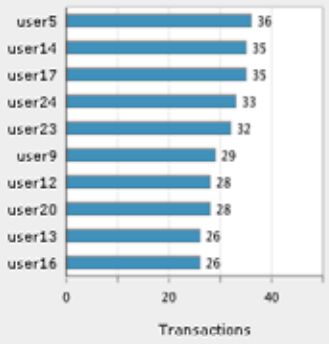


Chart Options... | Export...

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 プロキシによって処理されたトランザクションの検索」（P.5-60）

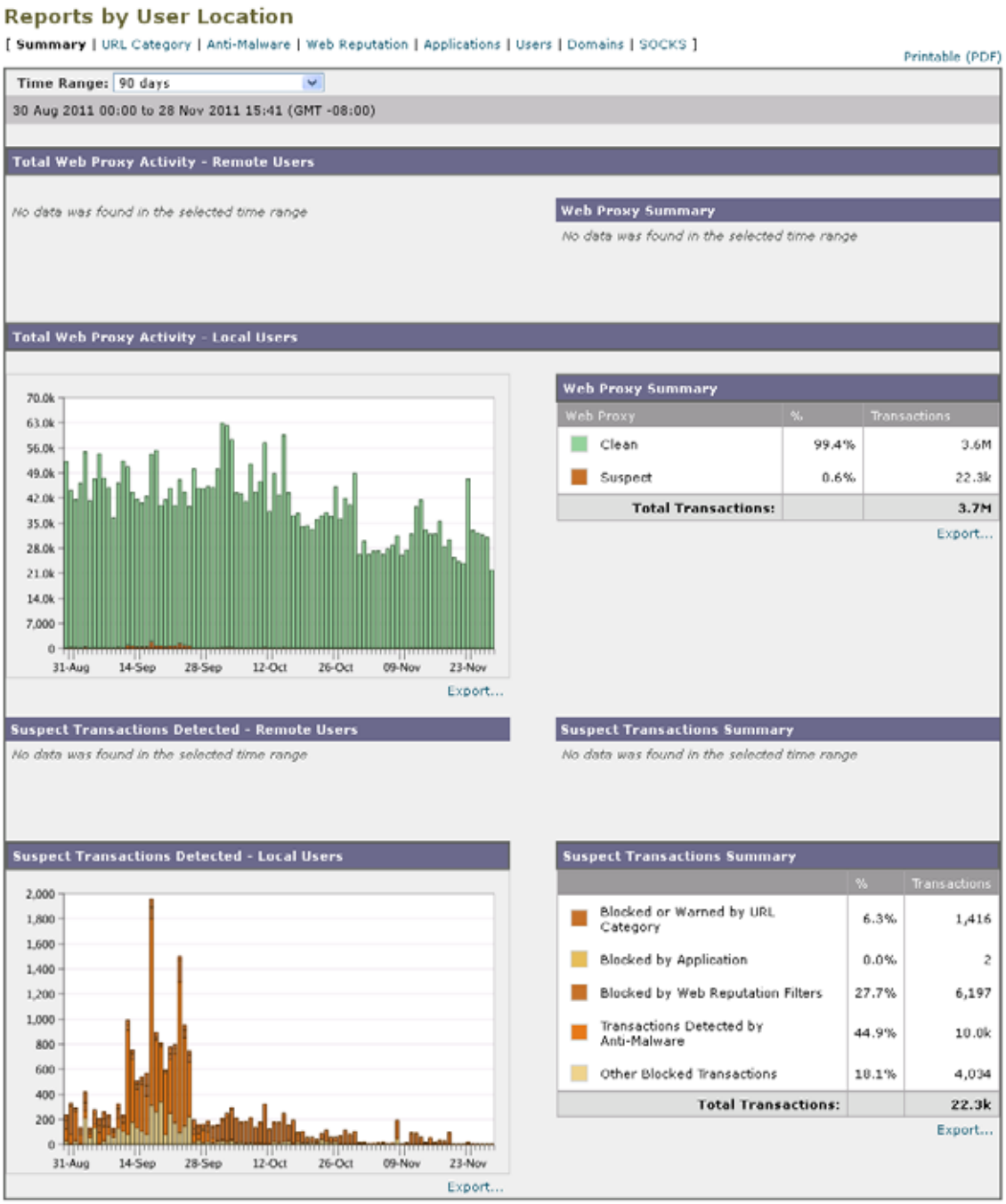
ユーザ ロケーション別のレポート（Reports by User Location）

[Web] > [レポート（Reporting）] > [ユーザ ロケーション別のレポート（Reports by User Location）] ページでは、モバイル ユーザがローカル システムまたはリモート システムから実行しているアクティビティを確認できます。

対象となるアクティビティは次のとおりです。

- ローカル ユーザおよびリモート ユーザがアクセスしている URL カテゴリ。
- ローカル ユーザおよびリモート ユーザがアクセスしているサイトによってトリガーされているアンチマルウェア アクティビティ。
- ローカル ユーザおよびリモート ユーザがアクセスしているサイトの Web レピュテーション。
- ローカル ユーザおよびリモート ユーザがアクセスしているアプリケーション。
- ユーザ（ローカルおよびリモート）。
- ローカル ユーザおよびリモート ユーザがアクセスしているドメイン。

図 5-15　[ユーザ ロケーション別のレポート（Reports by User Location）] ページ



[ユーザ ロケーション別のレポート（Reports by User Location）] ページには次の情報が表示されます。

表 5-14　[Web] > [レポート（Reporting）] > [ユーザ ロケーション別のレポート（Reports by User Location）] ページの詳細

セクション	説明
時間範囲（Time Range）（ドロップダウン リスト）	1 ～ 90 日間またはカスタム日数範囲を指定できるドロップダウン リスト。時間範囲の詳細と実際のニーズに合わせたカスタマイズについては、「レポートの時間範囲の選択」（P.3-4）を参照してください。
全体の Web プロキシ アクティビティ：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 プロキシのサマリー（Web Proxy Summary）	このセクションには、システム上のローカル 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。
全体の Web プロキシ アクティビティ：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。
検出された疑が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サマリー（Suspect Transactions Summary）	このセクションには、システム上のリモート 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。
検出された疑が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サマリー（Suspect Transactions Summary）	このセクションには、システム上のローカル 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 ロケーション別のレポート（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。

ヒント　このレポートのビューをカスタマイズするには、「インタラクティブ Web レポーティング ページの操作」（P.5-7）を参照してください。

（注）　[ユーザ ロケーション別のレポート（Reports by User Location）] ページの情報について、スケジュール設定されたレポートを生成することができます。レポートのスケジュール設定については、「スケジュール設定されたレポートとオンデマンド Web レポートについて」（P.5-66）を参照してください。

Web トラッキング（Web Tracking）

[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、その詳細を表示します。展開で使用するサービスに基づき、関連するタブで検索を行います。

- 「Web プロキシ サービスによって処理されたトランザクションの検索」（P.5-56）
- 「L4 トラフィック モニタによって処理されたトランザクションの検索」（P.5-60）
- 「SOCKS プロキシによって処理されたトランザクションの検索」（P.5-60）

Web プロキシと L4 トラフィック モニタの違いについては、『*Cisco IronPort AsyncOS for Web Security User Guide*』の「Understanding How the Web Security Appliance Works」を参照してください。

関連トピック

- 「Web トラッキングおよびアップグレードについて」（P.5-61）

Web プロキシ サービスによって処理されたトランザクションの検索

[Web] > [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、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収集された Web トラッキング データを検索します。このデータに L4 トラフィック モニタリング データは含まれません。

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。

  たとえば、[プロキシ サービス（Proxy Services）] タブを使用して、ユーザがアクセスしている特定の URL について、ユーザがアクセスした時刻や、それが許可された URL であるかどうか、といった情報を取得できます。

- **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（ブロック、モニタリング、および警告されたトランザクション、完了したトランザクションなど）の検索結果を表示できます。URL カテゴリ、マルウェアの脅威、アプリケーションなど、複数の条件を使用してデータ結果をフィルタリングすることもできます。

（注）　Web プロキシは、OTHER-NONE 以外の ACL デシジョン タグを含むトランザクションのみレポートします。

Web トラッキングの使用例については、「例 1：ユーザの調査」（P.D-1）を参照してください。

[プロキシ サービス（Proxy Services）] タブと他の Web レポーティング ページの併用例については、「[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」（P.5-29）を参照してください。

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。

手順

ステップ 1　セキュリティ管理アプライアンスで、[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　[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　検索オプションとフィルタリング オプションをすべて表示するには、[拡張（Advanced）] をクリックします。

ステップ 4　検索条件を入力します。

表 5-15　[プロキシ サービス（Proxy Services）] タブの Web トラッキング検索条件

オプション	説明
デフォルトの検索条件	
時間範囲（Time Range）	レポート対象の時間範囲を選択します。セキュリティ管理アプライアンスで使用できる時間範囲については、「レポートの時間範囲の選択」（P.3-4）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（Completed）]、[ブロック済み（Blocked）]、[モニタ済み（Monitored）]、または [警告済み（Warned）] から選択します。
高度な検索条件	
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 カテゴリによるフィルタ（Filter by URL Category）] を選択し、フィルタリング対象とするカスタムまたは定義済み 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、少なくとも 1 つの管理対象 Web セキュリティ アプライアンスでの新しいトランザクションでは使用できなくなります。ただし、そのカテゴリが有効な間に発生した最近のトランザクションについては、引き続き検索を実行できます。URL カテゴリ セットの更新については、「URL カテゴリ セットの更新とレポート」（P.5-28）を参照してください。 ドロップダウン リストに表示されるエンジン名に関係なく、カテゴリ名に一致する最近のトランザクションがすべて含まれます。
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、[アプリケーションによるフィルタ（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 タイプによるフィルタ（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、[ポリシーによるフィルタ（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。 このポリシーが Web セキュリティ アプライアンスで宣言済みであることを確認してください。

表 5-15　[プロキシ サービス（Proxy Services）] タブの Web トラッキング検索条件

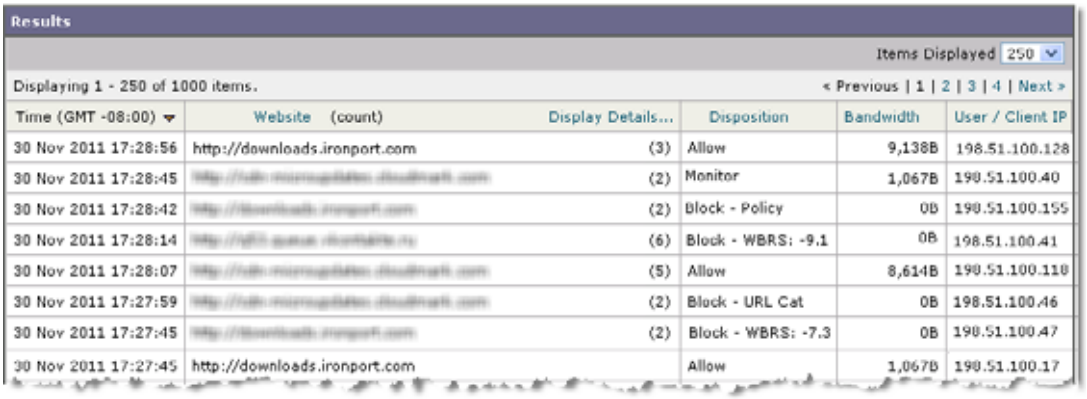
オプション	説明
マルウェアの脅威（Malware Threat）	特定のマルウェアの脅威でフィルタリングするには、[マルウェア脅威によるフィルタ（Filter by Malware Threat）] を選択し、フィルタリングに使用するマルウェアの脅威名を入力します。 マルウェア カテゴリでフィルタリングするには、[マルウェア カテゴリによるフィルタ（Filter by Malware Category）] を選択し、フィルタリングに使用するマルウェア カテゴリを選択します。
WBRS	[WBRS] セクションでは、Web ベースのレピュテーション スコアによるフィルタリングと、特定の Web 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によるフィルタ（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。 WBRS スコアの詳細については、『*Cisco IronPort AsyncOS for Web Security User Guide*』を参照してください。
AnyConnect セキュア モビリティ（AnyConnect Secure Mobility）	リモートまたはローカル アクセスでフィルタリングするには、[ユーザロケーションによるフィルタ（Filter by User Location）] を選択し、アクセス タイプを選択します。すべてのアクセス タイプを含めるには、[フィルタを無効にする（Disable Filter）] を選択します （旧リリースでは、このオプションは Mobile User Security と呼ばれていました）。
ユーザ要求（User Request）	ユーザによって実際に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、[ユーザがリクエスト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ます。
Web アプライアンス（Web Appliance）	特定の Web アプライアンスでフィルタリングするには、[Web アプライアンスによるフィルタ（Filter by Web Appliance）] の横のオプション ボタンをクリックし、テキスト フィールドに Web アプライアンス名を入力します。 [フィルタを無効にする（Disable Filter）] を選択すると、検索にはセキュリティ管理アプライアンスに関連付けられたすべての Web セキュリティ アプライアンスが含まれます。

ステップ 5　[検索（Search）] をクリックします。

Web トラッキング検索結果について

デフォルトでは、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。

図 5-16　Web トラッキング検索結果（[プロキシ サービス（Proxy Services）] タブ）



[結果（Results）] ウィンドウには次の情報が表示されます。

- URL がアクセスされた時刻
- トランザクションに関係した Web サイト
- 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。この数値は、カラム見出しの [詳細を表示（Display Details）] リンクの下にカッコで囲まれて表示されます。
- 処理（トランザクションの結果。該当する場合、トランザクションがブロックまたはモニタされた理由、あるいは警告が発行された理由が表示されます）。
- トランザクションの帯域幅
- ユーザ ID/ クライアント IP アドレス

ステップ 6　トランザクションについてさらに詳細な情報を表示するには、[Web サイト（Website）] カラム見出しの [詳細を表示 ...（Display Details...）] リンクをクリックします。

（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　結果の URL が切り詰められている場合は、どのホスト Web セキュリティ アプライアンスでトランザクションが処理されたかに注目し、そのアプライアンスのアクセスログを確認すると、完全な URL を特定できます。

500 件までの関連トランザクションのリストを表示するには、[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たトランザクションの検索

[Web] > [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
- 接続を処理した Web セキュリティ アプライアンス

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、またはトランザクションを処理した Web セキュリティ アプライアンスを表示するには、[送信先 IP アドレス（Destination IP Address）] カラム見出しの [詳細を表示（Display Details）] リンクをクリックします。

この情報の詳細な使用方法については、「[L4 トラフィック モニタ（L4 Traffic Monitor）] レポート」（P.5-46）を参照してください。

関連トピック

- 「[L4 トラフィック モニタ（L4 Traffic Monitor）] レポート」（P.5-46）

SOCKS プロキシによって処理されたトランザクションの検索

ブロックされたトランザクション、完了したトランザクション、ユーザ、宛先ドメイン、宛先 IP アドレス、宛先ポートなど、各種条件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、一致ポリシー、およびユーザ ロケーション（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。

手順

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、[拡張（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）] レポート」（P.5-51）

Web トラッキングおよびアップグレードについて

新しい Web トラッキング機能は、アップグレード前に実行されたトランザクションには適用できない場合があります。これは、これらのトランザクションについては、必須データが保持されていない場合があるためです。Web トラッキング データおよびアップグレードに関連する制限については、ご使用のリリースのリリース ノートを参照してください。

[システム容量（System Capacity）] ページ

[Web] > [レポート（Reporting）] > [システム容量（System Capacity）] ページでは、Web セキュリティ アプライアンスによってセキュリティ管理アプライアンスで発生する作業負荷全体を表示できます。重要な点は、[システム容量（System Capacity）] ページを使用して、経時的に増大をトラッキングしてシステム キャパシティの計画を立てられることです。Web セキュリティ アプライアンスをモニタすると、キャパシティが実際の量に適しているかを確認できます。量は、時間の経過に伴って必ず増加しますが、適切にモニタリングしていれば、追加キャパシティまたは設定変更を予防的に適用できます。

[システム容量（System Capacity）] ページを使用すると、次の情報を確認できます。

- Web セキュリティ アプライアンスが推奨される CPU キャパシティをいつ超えたかを特定します。これによって、設定の最適化や追加アプライアンスがいつ必要になったかがわかります。
- トラブルシューティングのために、システムが最もリソースを使用している部分を識別します。
- 応答時間とプロキシ バッファ メモリを確認します。
- 1 秒あたりのトランザクション、および顕著な接続を確認します。

[システム容量（System Capacity）] ページに表示されるデータの解釈方法

[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。

- Day レポート : Day レポートでは、時間テーブルを照会し、24 時間の間に 1 時間ごとにアプライアンスが受信したクエリー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。
- Month レポート : Month レポートでは、30 日間または 31 日間（その月の日数に応じる）の日テーブルを照会し、30 日間または 31 日間の正確なクエリー数を表示します。これも正確な数値です。

[システム容量（System Capacity）] ページの [最大（Maximum）] 値インジケータは、指定された期間の最大値を示します。[平均（Average）] 値は指定された期間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。

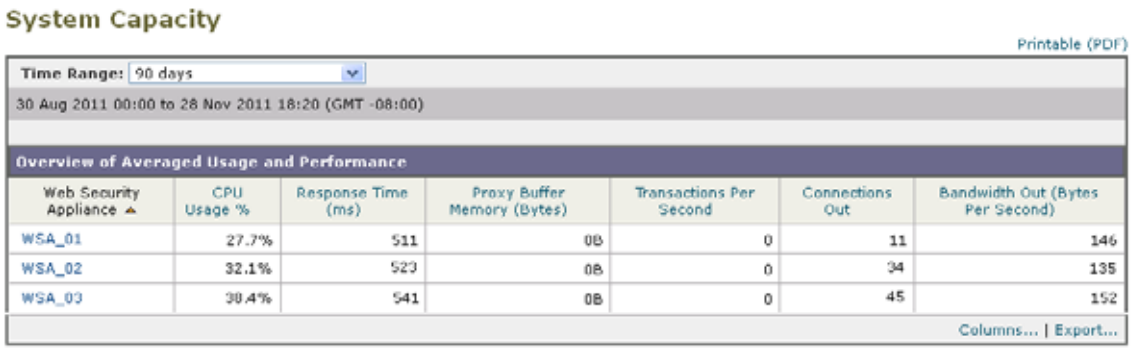
（注）　他のレポートで時間範囲に [年（Year）] を選択した場合は、最大の時間範囲である 90 日を選択することを推奨します。

[システム容量（System Capacity）] ページにアクセスするには、次の手順を実行します。

手順

ステップ 1　セキュリティ管理アプライアンスで、[Web] > [レポート（Reporting）] > [システム容量（System Capacity）] を選択します。

図 5-17　[システム容量（System Capacity）] ページ



ステップ 2　他のタイプのデータを表示するには、[列（Columns）] をクリックし、表示するデータを選択します。

ステップ 3　単一のアプライアンスのシステム キャパシティを表示するには、[平均使用率およびパフォーマンスの概要（Overview of Averaged Usage and Performance）] テーブルの [Web セキュリティ アプライアンス] カラムで目的のアプライアンスをクリックします。

このアプライアンスに関する [システム容量（System Capacity）] グラフが表示されます。このページのグラフは次の 2 種類に分かれています。

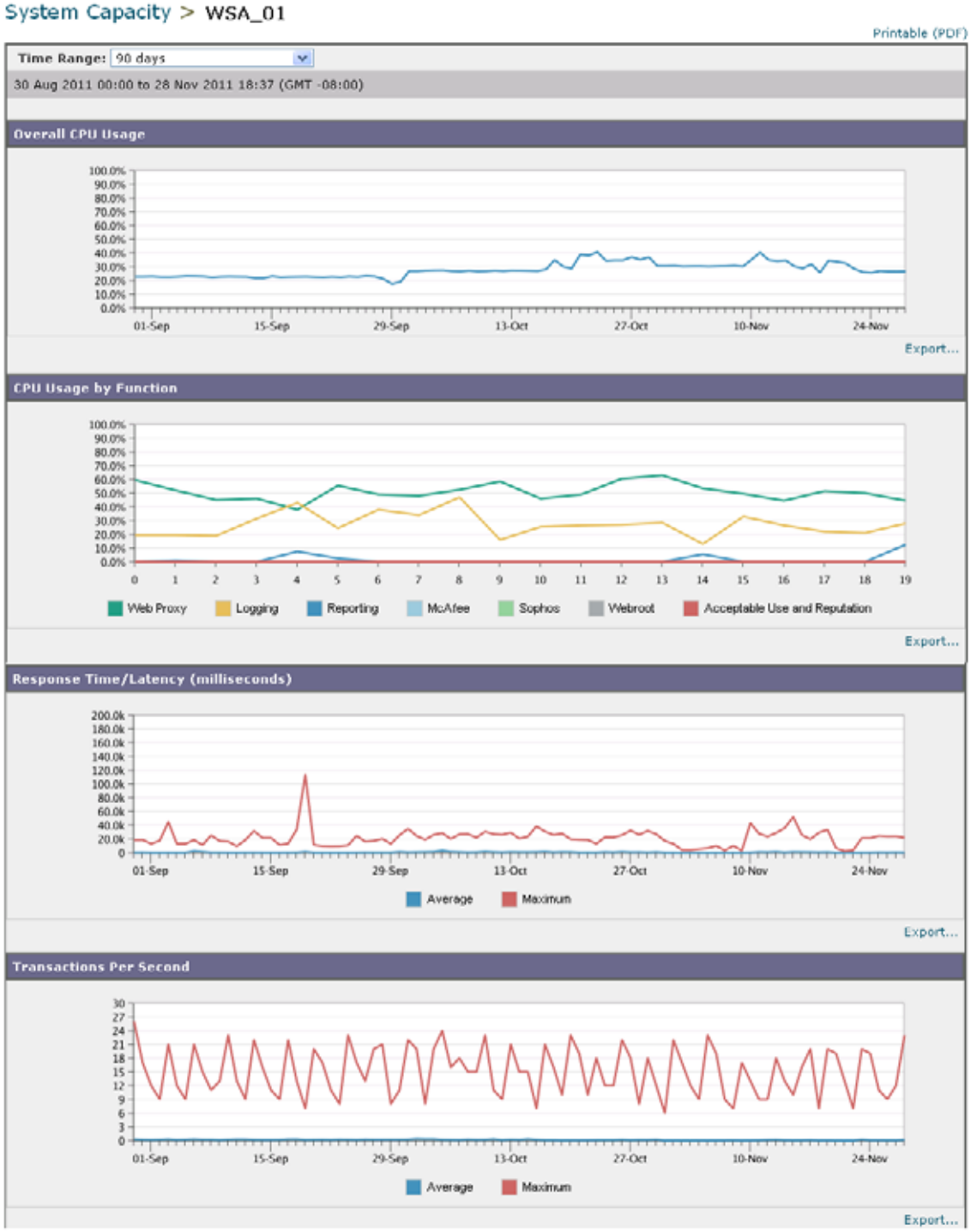
- [システム容量（System Capacity）] : [システムの負荷（System Load）]
- 「[システム容量（System Capacity）] : [ネットワーク負荷（Network Load）]」

[システム容量（System Capacity）] : [システムの負荷（System Load）]

[システム容量（System Capacity）] ウィンドウの最初の 4 つのグラフは、システム負荷に関するレポートです。これらのレポートには、アプライアンスでの全体的な CPU 使用状況が示されます。AsyncOS は、アイドル状態の CPU リソースを使用してトランザクション 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 使用率が高く、かつ高ボリュームのメモリ ページ スワッピングが発生する場合、キャパシティの問題の可能性があります。このページには、Web セキュリティ アプライアンスのレポーティングの処理などのさまざまな機能で使用される CPU 量を示すグラフも示されます。機能別 CPU のグラフは、システム上で最も多くのリソース使用する製品の領域を示す指標です。アプライアンスの最適化が必要な場合、このグラフは、調整やディセーブル化の必要な機能を判断するのに役立ちます。

また、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。

図 5-18　[システム容量（System Capacity）] : [システムの負荷（System Load）]



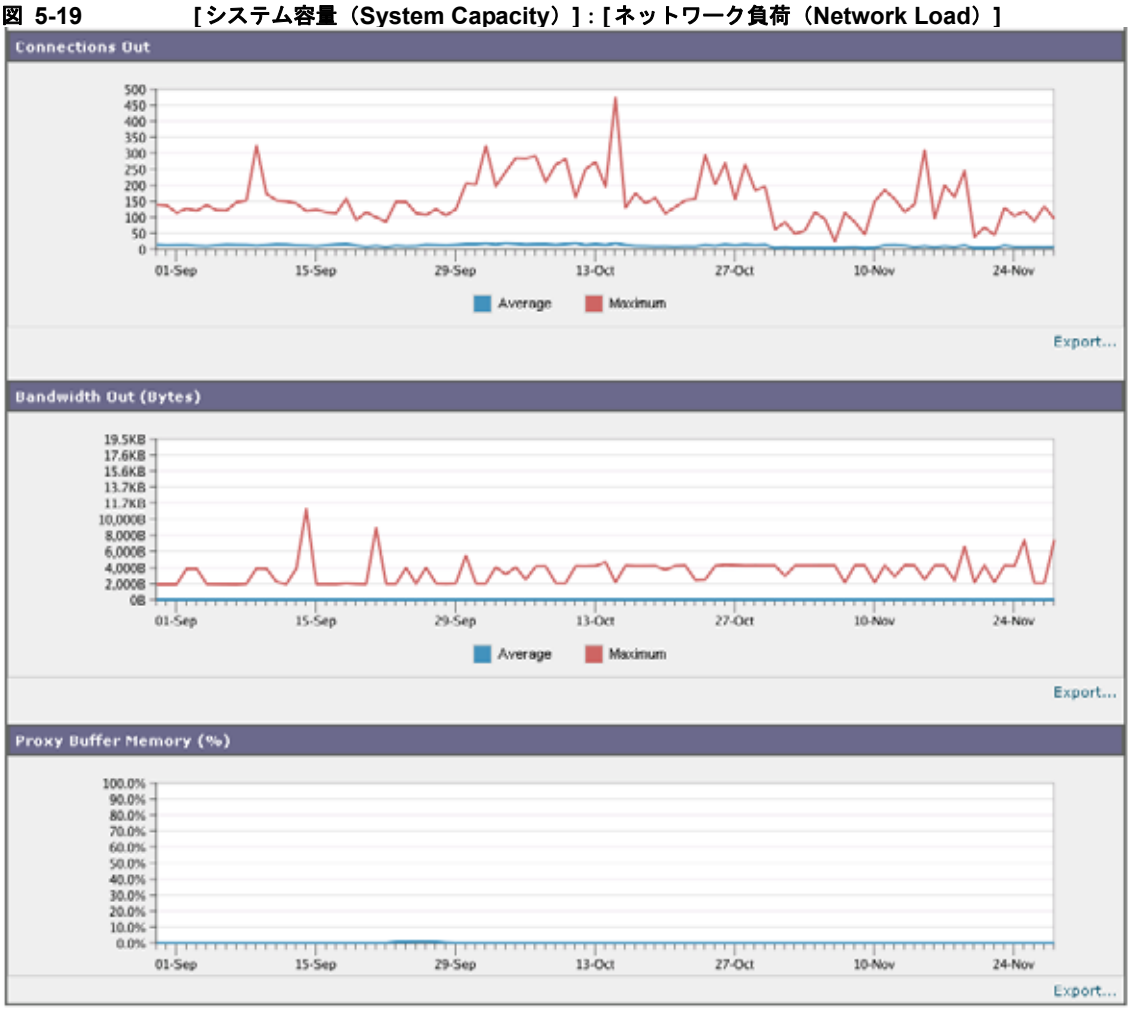
[システム容量（System Capacity）]：[ネットワーク負荷（Network Load）]

[システム容量（System Capacity）] ウィンドウの次のグラフには、発信接続、出力用帯域幅、プロキシ バッファ メモリの統計情報が示されます。日、週、月、または年の結果を表示することもできます。ご自身の環境における通常量とスパイクのトレンドを理解しておくことが重要です。

[プロキシ バッファ メモリ（Proxy Buffer Memory）] は、通常動作時におけるネットワーク トラフィックの急増を示している場合もありますが、グラフが最大値まで徐々に上昇している場合は、アプライアンスがのキャパシティが最大値に達しており、キャパシティの追加を検討すべきである可能性もあります。

次のチャートは、「[システム容量（System Capacity）]：[システムの負荷（System Load）]」、図 5-18 と同じページでこれらのチャートの下に表示されます。

図 5-19　[システム容量（System Capacity）]：[ネットワーク負荷（Network Load）]



プロキシ バッファ メモリ スワッピングに関する注意事項

システムは、定期的にプロキシ バッファ メモリをスワップするように設計されているので、一部のプロキシ バッファ メモリ スワッピングは起こり得るものであり、アプライアンスの問題を示すものではありません。システムが*継続的に*高ボリュームのプロキシ バッファ メモリをスワップする場合を除き、プロキシ バッファ メモリのスワッピングは正常かつ通常の動作です。システムが極端に大量の処理を

行い、大量であるためにプロキシ バッファ メモリを絶えずスワップする場合は、ネットワークに Web セキュリティ アプライアンスを追加するか、またはスループットが最大になるように設定を調整して、パフォーマンスの向上を図る必要があります。

[使用可能なデータ（Data Availability）] ページ

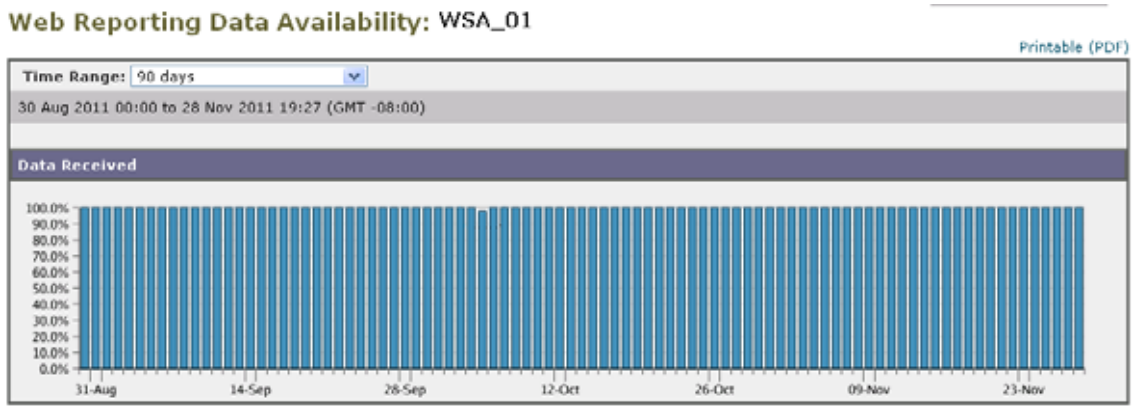
[Web] > [レポート（Reporting）] > [使用可能なデータ（Data Availability）] ページには、管理対象の各 Web セキュリティ アプライアンスに対応するセキュリティ管理アプライアンスでレポーティングおよび Web トラッキング データを使用できる日付範囲の概要が表示されます。

図 5-20　[有効な Web レポート データ（Web Reporting Data Availability）] ページ

（注）　Web レポーティングがディセーブルになると、セキュリティ管理アプライアンスは Web セキュリティ アプライアンスから新しいデータを取得しなくなりますが、以前に取得したデータは セキュリティ管理アプライアンスに残っています。ディスク使用率の管理方法については、「ディスク使用量の管理」（P.14-56）を参照してください。

[Web レポート（Web Reporting）] の [差出人（From）] カラムと [宛先（To）] カラム、および [Web レポートとトラッキング（Web Reporting and Tracking）] の [差出人（From）] カラムと [宛先（To）] カラムでステータスが異なる場合は、[ステータス（Status）] カラムに最も深刻な結果が示されます。

特定のアプライアンスのデータ アベイラビリティをグラフ形式で表示するには、[Web セキュリティ アプライアンス] カラムでアプライアンスをクリックします。



（注）　URL カテゴリに関するスケジュール済みレポートでデータ アベイラビリティが使用されている場合、いずれかのアプライアンスのデータにギャップがあると、ページの下部に「この時間範囲の一部のデータは使用不可でした。(Some data in this time range was unavailable.)」というメッセージが表示されます。
ギャップが存在しない場合は何も表示されません。

スケジュール設定されたレポートとオンデマンド Web レポートについて

特記のない限り、次のタイプの Web セキュリティ レポートを、スケジュール設定されたレポートまたはオンデマンド レポートとして作成できます。

- [Web レポートの概要（Web Reporting Overview）]：このページに表示される情報については、「Web レポートの概要」（P.5-13）を参照してください。
- [ユーザ（Users）]：このページに表示される情報については、「[ユーザ（Users）] レポート（Web）」（P.5-17）を参照してください。
- [Web サイト（Web Sites）]：このページに表示される情報については、「[Web サイト（Web Sites）] レポート」（P.5-24）を参照してください。
- [URL カテゴリ（URL Categories）]：このページに表示される情報については、「URL カテゴリ レポート」（P.5-26）を参照してください。
- [上位 URL カテゴリ - 拡張（Top URL Categories — Extended）]：[上位 URL カテゴリ - 拡張（Top URL Categories — Extended）] のレポートを生成する方法については、「上位 URL カテゴリ - 拡張（Top URL Categories — Extended）」（P.5-68）を参照してください。

  このレポートをオンデマンド レポートとして使用することはできません。
- [アプリケーションの表示（Application Visibility）]：このページに表示される情報については、「[アプリケーションの表示（Application Visibility）] レポート」（P.5-30）を参照してください。
- [上位のアプリケーション タイプ - 拡張（Top Application Types — Extended）]：[上位 URL カテゴリ - 拡張（Top URL Categories — Extended）] のレポートを生成する方法については、「上位のアプリケーション タイプ - 拡張（Top Application Types — Extended）」（P.5-70）を参照してください。

  このレポートをオンデマンド レポートとして使用することはできません。
- [マルウェア対策（Anti-Malware）]：このページに表示される情報については、「[マルウェア対策（Anti-Malware）] レポート」（P.5-33）を参照してください。
- [クライアント マルウェア リスク（Client Malware Risk）]：このページに表示される情報については、「[クライアント マルウェア リスク（Client Malware Risk）] レポート」（P.5-40）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）]：このページに表示される情報については、「[Web レピュテーション フィルタ（Web Reputation Filters）] レポート」（P.5-43）を参照してください。
- [L4 トラフィックモニタ（L4 Traffic Monitor）]：このページに表示される情報については、「[L4 トラフィック モニタ（L4 Traffic Monitor）] レポート」（P.5-46）を参照してください。
- [モバイル セキュア ソリューション（Mobile Secure Solution）]：このページに表示される情報については、「ユーザ ロケーション別のレポート（Reports by User Location）」（P.5-53）を参照してください。

- [システム容量（System Capacity）] : このページに表示される情報については、「[システム容量（System Capacity）] ページ」（P.5-61）を参照してください。

Web レポートのスケジュール設定

ここでは、次の内容について説明します。

（注）　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。詳細については、「Web レポートでのユーザ名の匿名化」（P.5-5）を参照してください。

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。スケジュール設定されたレポートは、前日、過去 7 日間、前月、過去の日（最大 250 日）、過去の月（最大 12 ヵ月）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。

セキュリティ管理アプライアンスは、生成した最新のレポートを保持します（すべてのレポートに対して、最大で 1000 バージョン）。必要に応じた数（ゼロも含む）のレポート受信者を定義できます。電子メール受信者を指定しない場合でも、レポートはアーカイブされます。レポートを多数のアドレスに送信する必要がある場合、個別に受信者を設定するよりも、メーリング リストを作成するほうが容易です。

デフォルトでは、スケジュール設定された各レポートのうち、直近の 12 のレポートがアーカイブされます。レポートは、アプライアンスの **/periodic_reports** ディレクトリに保管されます。（詳細については、付録 A「IP インターフェイスおよびアプライアンスへのアクセス」を参照してください）。

スケジュール設定されたレポートの追加

手順

ステップ 1　セキュリティ管理アプライアンスで、[Web] > [レポート（Reporting）] > [定期レポート（Scheduled Reports）] を選択します。

ステップ 2　[定期レポートを追加（Add Scheduled Report）] をクリックします。

ステップ 3　[タイプ（Type）] の横のドロップダウン メニューから、レポート タイプを選択します。

ステップ 4　[タイトル（Title）] フィールドに、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推奨します。

ステップ 5　[時間範囲（Time Range）] ドロップダウン メニューから、レポートの時間範囲を選択します。

ステップ 6　生成されるレポートの形式を選択します。

デフォルト形式は PDF です。ほとんどのレポートでは、raw データを CSV ファイルとして保存することも可能です。

ステップ 7　[項目数（Number of Items）] の横のドロップダウン リストから、生成されるレポートに出力する項目の数を選択します。

有効な値は 2 ～ 20 です。デフォルト値は 5 です。

ステップ 8　[グラフ（Charts）] では、[表示するデータ（Data to display）] の下のデフォルト チャートをクリックし、レポートの各チャートに表示するデータを選択します。

ステップ 9　[ソート列（Sort Column）] の横のドロップダウン リストから、このレポートでデータをソートするためのカラムを選択します。これにより、スケジュール設定されたレポート内の任意のカラムを基準とする上位「N」個の項目のレポートを作成できます。

ステップ 10　[スケジュール（Schedule）] 領域で、レポートのスケジュールを設定する日、週、または月の横にあるオプション ボタンを選択します。

ステップ 11　[メール（Email）] テキスト フィールドに、生成されたレポートが送信される電子メール 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 12　[送信（Submit）] をクリックします。

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、[Web] > [レポート（Reporting）] > [定期レポート（Scheduled Reports）] ページに移動し、編集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。設定を変更し、[送信（Submit）] をクリックしてページでの変更を送信し、[変更を確定（Commit Changes）] ボタンをクリックしてアプライアンスへの変更を確定します。

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、[Web] > [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選択し、[削除（Delete）] を実行して変更を [確定（Commit）] 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。

追加の拡張レポート

さらに 2 種類のレポートを、スケジュール設定されたレポートとしてのみセキュリティ管理アプライアンスで使用することができます。

- 上位 URL カテゴリ - 拡張（Top URL Categories — Extended）
- 上位のアプリケーション タイプ - 拡張（Top Application Types — Extended）

上位 URL カテゴリ - 拡張（Top URL Categories — Extended）

[上位 URL カテゴリ - 拡張（Top URL Categories — Extended）] レポートは、管理者が [URL カテゴリ（URL Categories）] レポートよりも詳細な情報を必要とする場合に役立ちます。

たとえば、通常の [URL カテゴリ（URL Categories）] レポートでは、大きい URL カテゴリ レベルで特定の従業員の帯域幅使用状況を評価する情報を収集できます。各 URL カテゴリの上位 10 個の URL、または各 URL カテゴリの上位 5 人のユーザについて、帯域幅の使用状況をモニタする詳細なレポートを生成するには、[上位 URL カテゴリ - 拡張（Top URL Categories — Extended）] レポートを使用します。

（注）
- このタイプのレポートで生成できる最大レポート数は 20 です。
- 定義済みの URL カテゴリ リスト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.5-28）を参照してください。

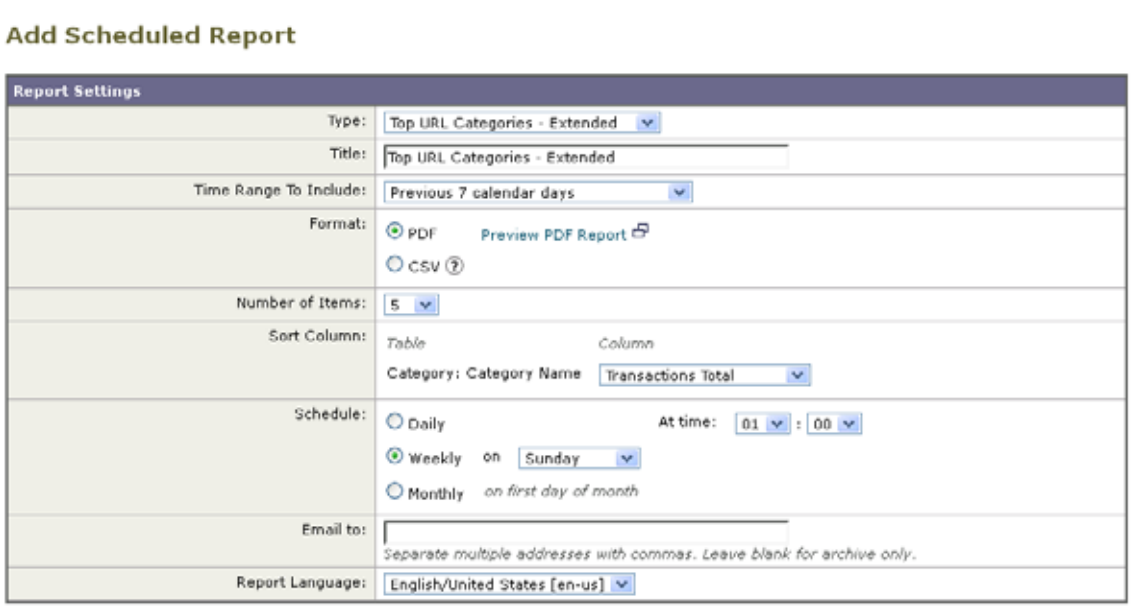
[上位 URL カテゴリ - 拡張（Top URL Categories — Extended）] レポートを生成するには、次の手順を実行します。

手順

ステップ 1　セキュリティ管理アプライアンスで、[Web] > [レポート（Reporting）] > [定期レポート（Scheduled Reports）] を選択します。

ステップ 2　[定期レポートを追加（Add Scheduled Report）] をクリックします。

ステップ 3　[タイプ（Type）] の横のドロップダウン メニューから、[上位 URL カテゴリ - 拡張（Top URL Categories — Extended）] を選択します。



ステップ 4　[タイトル（Title）] テキスト フィールドに、URL 拡張レポートのタイトルを入力します。

ステップ 5　[時間範囲（Time Range）] ドロップダウン メニューから、レポートの時間範囲を選択します。

ステップ 6　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。

ステップ 7　[項目数（Number of Items）] の横のドロップダウン リストから、生成されるレポートに出力する URL カテゴリの数を選択します。

有効な値は 2 ～ 20 です。デフォルト値は 5 です。

ステップ 8　[ソート列（Sort Column）] の横のドロップダウン リストから、このレポートでデータをソートするためのカラムを選択します。これにより、スケジュール設定されたレポート内の任意のカラムを基準とする上位「N」個の項目のレポートを作成できます。

ステップ 9　[グラフ（Charts）] では、[表示するデータ（Data to display）] の下のデフォルト チャートをクリックし、レポートの各チャートに表示するデータを選択します。

ステップ 10　[スケジュール（Schedule）] 領域で、レポートのスケジュールを設定する日、週、または月の横にあるオプション ボタンを選択します。

ステップ 11　[メール（Email）] テキスト フィールドに、生成されたレポートが送信される電子メール アドレスを入力します。

ステップ 12　[送信（Submit）] をクリックします。

上位のアプリケーション タイプ - 拡張（Top Application Types — Extended）

[上位のアプリケーション タイプ - 拡張（Top Application Types — Extended）] レポートを生成するには、次の手順を実行します。

手順

ステップ 1　セキュリティ管理アプライアンスで、[Web] > [レポート（Reporting）] > [定期レポート（Scheduled Reports）] を選択します。

ステップ 2　[定期レポートを追加（Add Scheduled Report）] をクリックします。

ステップ 3　[タイプ（Type）] の横のドロップダウン メニューから、[上位のアプリケーション タイプ - 拡張（Top Application Types — Extended）] を選択します。

このページのオプションは変更される場合があります。

ステップ 4　[タイトル（Title）] テキスト フィールドにレポートのタイトルを入力します。

ステップ 5　[時間範囲（Time Range）] ドロップダウン メニューから、レポートの時間範囲を選択します。

ステップ 6　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。

ステップ 7　[項目数（Number of Items）] の横のドロップダウン リストから、生成されたレポートに出力するアプリケーション タイプの数を選択します。

有効な値は 2 ～ 20 です。デフォルト値は **5** です。

ステップ 8　[ソート列（Sort Column）] の横のドロップダウン リストから、テーブルに表示するカラムのタイプを選択します。選択肢は、[トランザクション完了（Transactions Completed）]、[ブロックされたトランザクション（Transactions Blocked）]、[トランザクション数計（Transaction Totals）] です。

ステップ 9　[グラフ（Charts）] では、[表示するデータ（Data to display）] の下のデフォルト チャートをクリックし、レポートの各チャートに表示するデータを選択します。

ステップ 10　[スケジュール（Schedule）] 領域で、レポートのスケジュールを設定する日、週、または月の横にあるオプション ボタンを選択します。

ステップ 11　[メール（Email）] テキスト フィールドに、生成されたレポートが送信される電子メール アドレスを入力します。

ステップ 12　[送信（Submit）] をクリックします。

オンデマンドでの Web レポートの生成

スケジュールを設定できるレポートのほとんどは、オンデマンドでの作成も可能です。

（注）　一部のレポートは、オンデマンドではなくスケジュール設定されたレポートとしてのみ使用できます。「追加の拡張レポート」（P.5-68）を参照してください。

レポートをオンデマンドで作成するには、次の手順を実行します。

手順

ステップ 1　セキュリティ管理アプライアンスで、[メール（Email）] > [レポート（Reporting）] > [アーカイブ レポート（Archived Reports）] を選択します。

ステップ 2　[今すぐレポートを生成（Generate Report Now）] をクリックします。

ステップ 3　[レポート タイプ（Report type）] セクションで、ドロップダウン リストからレポート タイプを選択します。

このページのオプションは変更される場合があります。

ステップ 4　[タイトル（Title）] テキスト フィールドに、レポートのタイトル名を入力します。

AsyncOS では、レポート名が一意かどうかは確認されません。混乱を避けるために、同じ名前で複数のレポートを作成しないでください。

ステップ 5　[時間範囲（Time Range to Include）] ドロップダウン リストから、レポート データの時間範囲を選択します。

ステップ 6　[形式（Format）] セクションで、レポートの形式を選択します。

次のオプションがあります。

- [PDF]。配信用、アーカイブ用、またはその両方の用途で PDF 形式のドキュメントを作成します。[PDF レポートをプレビュー（Preview PDF Report）] をクリックすると、ただちに PDF ファイルでレポートを表示できます。
- [CSV]。カンマ区切りの値として raw データが含まれる ASCII テキスト ファイルを作成します。各 CSV ファイルには、最大 100 行を含めることができます。レポートに複数の種類の表が含まれる場合、各表に対して別個の CSV ファイルが作成されます。

ステップ 7　レポートで使用可能なオプションに応じて次の項目を選択します。

- [行数（Number of rows）] : テーブルに表示するデータの行数。
- [グラフ（Charts）] : レポートのチャートに表示するデータ。
- [表示するデータ（Data to display）] の下のデフォルト オプションを選択します。
- [ソート列（Sort Column）] : 各テーブルのソート基準となるカラム。

ステップ 8　[送信オプション（Delivery Option）] セクションから、次のオプションを選択します。

- このレポートを [アーカイブ レポート（Archived Reports）] ページに表示するには、[アーカイブ レポート（Archive Report）] チェックボックスを選択します。

（注）　[ドメイン毎のエグゼクティブ サマリー（Domain-Based Executive Summary）] レポートはアーカイブできません。

- レポートを電子メールで送信する場合は、[今すぐ受信者にメールを送る（Email now to recipients）] チェックボックスをオンにします。
- テキスト フィールドに、レポートの受信者の電子メールアドレスを入力します。

ステップ 9　[このレポートを送信（Deliver This Report）] をクリックして、レポートを生成します。

アーカイブされた Web レポートの表示と管理

[Web] > [レポート（Reporting）] > [アーカイブ レポート（Archived Reports）] ページには次の内容が表示されます。

- 「スケジュール設定されたレポートの追加」（P.5-67）の手順を使用してスケジュールを設定したレポート
- 「オンデマンドでの Web レポートの生成」（P.5-71）の手順を使用して作成したレポート

レポートを表示するには、[レポートのタイトル（Report Title）] カラムでレポート名をクリックします。[表示（Show）] ドロップダウン メニューでは、[アーカイブ レポート（Archived Reports）] ページに表示されるレポートのタイプをフィルタリングできます。

リストが長い場合に特定のレポートを見つけるには、[表示（Show）] メニューからレポート タイプを選択してリストをフィルタリングするか、またはカラムのヘッダーをクリックし、そのカラムでソートします。

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。

CHAPTER 6

電子メール メッセージのトラッキング

トラッキング サービスの概要

シスコのコンテンツ セキュリティ管理アプライアンスのトラッキング サービスは、電子メール セキュリティ アプライアンスを補完します。セキュリティ管理アプライアンスによって、電子メール管理者はすべての電子メール セキュリティ アプライアンスを通過するメッセージのステータスを 1 箇所から追跡できます。

セキュリティ管理アプライアンスを使用すると、電子メール セキュリティ アプライアンスで処理されるメッセージのステータスを容易に検出できます。電子メール管理者は、メッセージの正確な場所を判断することで、ヘルプ デスク コールを迅速に解決できます。管理者はセキュリティ管理アプライアンスを使用して、特定のメッセージについて、配信されたか、ウイルス感染が検出されたか、スパム隔離に入れられたか、あるいはメール ストリーム以外の場所にあるのかを判断できます。

`grep` や同様のツールを使用してログ ファイルを検索する代わりに、セキュリティ管理アプライアンスの柔軟なトラッキング インターフェイスを使用してメッセージの場所を特定できます。さまざまな検索パラメータを組み合わせて使用できます。

トラッキング クエリーには次の項目を含めることができます。

- **エンベロープ情報：**照合するテキスト文字列を入力し、特定のエンベロープ送信者または受信者からのメッセージを検索します。
- **件名ヘッダー：**件名行のテキスト文字列を照合します。警告：規制によりそのようなトラッキングが禁止されている環境では、このタイプの検索を使用しないでください。
- **タイム フレーム：**指定された日数と時間内に送信されたメッセージを検索します。
- **送信元 IP アドレスまたは拒否された接続：**特定の IP アドレスからのメッセージを検索します。または、検索結果内の拒否された接続を表示します。
- **添付ファイル名**：メッセージを添付ファイル名で検索できます。照会した名前の添付ファイルが少なくとも 1 つ含まれているメッセージが検索結果に表示されます。

  パフォーマンス上の理由から、OLE オブジェクトなどの添付ファイルや .ZIP ファイルなどのアーカイブに含まれるファイル名は追跡されません。

添付ファイルの中には追跡されないものもあります。パフォーマンス上の理由から、添付ファイル名のスキャンは他のスキャン動作の一環としてのみ実行されます。たとえば、メッセージまたはコンテンツ フィルタリング、DLP、免責事項スタンプなどです。添付ファイル名は、ファイルがまだ添付されている間に本文スキャンを通過するメッセージでのみ使用できます。添付ファイル名が表示されない例を次に示します（ただしこれらに限られるわけではありません）。

  - システムがコンテンツ フィルタのみを使用しており、アンチスパムまたはアンチウイルス フィルタによってメッセージがドロップされたか、その添付ファイルが除去された場合
  - 本文スキャンの実行前に、メッセージ分裂ポリシーによって一部のメッセージから添付ファイルが除去された場合

- **イベント：**ウイルス陽性、スパム陽性、またはスパムの疑いのフラグが設定されたメッセージや、配信された、ハード バウンスされた、ソフト バウンスされた、またはウイルス アウトブレイク隔離に送信されたメッセージなど、指定されたイベントに一致するメッセージを検索します。
- **メッセージ ID：**SMTP「Message-ID:」ヘッダー、または Cisco IronPort メッセージ ID（MID）を識別してメッセージを検索します。
- **電子メール セキュリティ アプライアンス（ホスト）：**検索条件を特定の電子メール セキュリティ アプライアンスに絞り込むか、すべての管理対象アプライアンスを検索します。

中央集中型メッセージ トラッキングの設定

中央集中型メッセージ トラッキングを設定するには、次の手順を順序どおりに実行します。

- 「セキュリティ管理アプライアンスでの中央集中型電子メール トラッキングのイネーブル化」（P.6-2）
- 「電子メール セキュリティ アプライアンスでの中央集中型メッセージ トラッキングの設定」（P.6-3）
- 「管理対象の各電子メール セキュリティ アプライアンスへの中央集中型メッセージ トラッキング サービスの追加」（P.6-3）

セキュリティ管理アプライアンスでの中央集中型電子メール トラッキングのイネーブル化

手順

ステップ 1　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [メール（Email）] > [集約メッセージ トラッキング（Centralized Message Tracking）] を選択します。

ステップ 2　[メッセージ トラッキング サービス（Message Tracking Service）] セクションで [有効（Enable）] をクリックします。

ステップ 3　システム セットアップ ウィザードを実行してから初めて中央集中型電子メッセージ トラッキングをイネーブルにする場合は、エンドユーザ ライセンス契約書を確認し、[承認（Accept）] をクリックします。

ステップ 4　変更を送信し、保存します。

電子メール セキュリティ アプライアンスでの中央集中型メッセージ トラッキングの設定

手順

ステップ 1　電子メール セキュリティ アプライアンスでメッセージ トラッキングが設定され、正常に動作していることを確認します。

ステップ 2　[セキュリティ サービス（Security Services）] > [メッセージ トラッキング（Message Tracking）] に移動します。

ステップ 3　[設定を編集（Edit Settings）] をクリックします。

ステップ 4　[集約管理トラッキング（Centralized Tracking）] を選択します。

ステップ 5　[送信（Submit）] をクリックします。

ステップ 6　電子メールの添付ファイル名を検索および記録できるようにする場合は、次の点に注意してください。

少なくとも 1 つの受信コンテンツ フィルタまたは本文スキャン機能が 電子メール セキュリティ アプライアンスで設定され、イネーブルになっていることを確認します。コンテンツ フィルタおよび本文スキャンの詳細については、ご使用の電子メール セキュリティ アプライアンスのマニュアルまたはオンライン ヘルプを参照してください。

ステップ 7　変更を保存します。

ステップ 8　管理対象の各電子メール セキュリティ アプライアンスに対してこの手順を繰り返します。

管理対象の各電子メール セキュリティ アプライアンスへの中央集中型メッセージ トラッキング サービスの追加

ここで実行する手順は、他の中央集中型管理機能の設定時に、すでにこのアプライアンスを追加したかどうかによって異なります。

手順

ステップ 1　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [セキュリティ アプライアンス（Security Appliances）] を選択します。

ステップ 2　このページのリストに、すでに電子メール セキュリティ アプライアンスを追加している場合は、次の手順を実行します。

a.　電子メール セキュリティ アプライアンスの名前をクリックします。

b.　[集約メッセージ トラッキング（Centralized Message Tracking）] サービスを選択します。

ステップ 3　電子メール セキュリティ アプライアンスを追加していない場合は、次の手順を実行します。

a.　[メール アプライアンスの追加（Add Email Appliance）] をクリックします。

b.　[アプライアンス名（Appliance Name）] および [IP アドレス（IP Address）] テキスト フィールドに、電子メール セキュリティ アプライアンスの管理インターフェイスのアプライアンス名と IP アドレスを入力します。

（注）　[IP アドレス（IP Address）] テキスト フィールドに DNS 名を入力した場合でも、[送信（Submit）] をクリックすると、すぐに IP アドレスに解決されます。

c. [集約メッセージ トラッキング（Centralized Message Tracking）] サービスがすでに選択されています。

d. [接続の確立（Establish Connection）] をクリックします。

e. 管理対象となるアプライアンスの管理者アカウントのユーザ名とパスワードを入力し、[接続の確立（Establish Connection）] をクリックします。

（注）　ログイン資格情報を入力すると、セキュリティ管理アプライアンスからリモート アプライアンスへのファイル転送のための公開 SSH キーが渡されます。ログイン資格情報は、セキュリティ管理アプライアンスには保存されません。

f. [成功（Success）] メッセージがページのテーブルの上に表示されるまで待機します。

g. [テスト接続（Test Connection）] をクリックします。

h. テーブルの上のテスト結果を確認します。

ステップ 4　[送信（Submit）] をクリックします。

ステップ 5　中央集中型メッセージ トラッキングをイネーブルにする各電子メール セキュリティ アプライアンスに対し、この手順を繰り返します。

ステップ 6　変更を保存します。

機密情報へのアクセスの管理

管理タスクを数人で分配する場合、データ漏洩防止（DLP）ポリシーに違反するメッセージに表示される機密情報へのアクセスを制限するには、「メッセージ トラッキングでの DLP 機密情報へのアクセスの制御」（P.13-24）を参照してください。

メッセージ トラッキング データ アベイラビリティの確認

メッセージ トラッキング データに含まれる日付範囲を確認すること、およびそのデータの欠落インターバルを識別することができます。

ステップ 1　[メール（Email）] > [メッセージ トラッキング（Message Tracking）] > [有効なメッセージ トラッキング データ（Message Tracking Data Availability）] を選択します。

電子メール メッセージの検索

セキュリティ管理アプライアンスのトラッキング サービスを使用して、メッセージ件名行、日時の範囲、エンベロープ送信者または受信者、処理イベント（たとえば、メッセージがウイルス陽性またはスパム陽性かどうかや、ハード バウンスまたは配信されたかどうか）など、指定した条件に一致する特定の電子メール メッセージまたはメッセージのグループを検索できます。メッセージ トラッキングでは、メッセージ フローの詳細なビューが表示されます。また、特定の電子メール メッセージをドリルダウンし、処理イベント、添付ファイル名、エンベロープおよびヘッダー情報など、メッセージの詳細情報を確認することもできます。

（注） このトラッキング コンポーネントにより個々の電子メール メッセージの詳細な情報が提供されますが、このコンポーネントを使用してメッセージの内容を読むことはできません。

手順

ステップ 1 セキュリティ管理アプライアンスで、[メール（Email）] > [メッセージ トラッキング（Message Tracking）] > [メッセージ トラッキング（Message Tracking）] を選択します。

ステップ 2 （任意）[拡張（Advanced）] リンクをクリックし、その他の検索オプションを表示します。

ステップ 3 検索条件を入力します。

（注） トラッキング検索では、ワイルドカード文字や正規表現はサポートされません。トラッキング検索では大文字と小文字は区別されません。

- [エンベロープ送信者（Envelope Sender）] : [次で始まる（Begins With）]、[次に合致する（Is）]、または [次を含む（Contains）] を選択し、テキスト文字列を入力してエンベロープ送信者を検索します。電子メール アドレス、ユーザ名、またはドメインを入力できます。次の形式を使用します。
  - 電子メール ドメインの場合
    example.com, *[203.0.113.15]*, *[ipv6:2001:db8:80:1::5]*
  - 完全な電子メール アドレスの場合
    user@example.com, *user@[203.0.113.15]* または *user@[ipv6:2001:db8:80:1::5]*
  - 文字を入力できます。入力の検証は実行されません。
- [エンベロープ受信者（Envelope Recipient）] : [次で始まる（Begins With）]、[次に合致する（Is）]、または [次を含む（Contains）] を選択し、テキストを入力してエンベロープ受信者を検索します。電子メール アドレス、ユーザ名、またはドメインを入力できます。

  電子メール セキュリティ アプライアンスでエイリアス拡張にエイリアス テーブルを使用している場合は、本来のエンベロープ アドレスではなく、拡張された受信者アドレスが検索されます。それ以外のあらゆる場合においては、メッセージ トラッキング クエリーによって本来のエンベロープ受信者アドレスが検索されます。

  この点を除けば、エンベロープ受信者の有効な検索条件はエンベロープ送信者の場合と同じです。

  文字を入力できます。入力の検証は実行されません。
- [件名（Subject）] : [次で始まる（Begins With）]、[次に合致する（Is）]、[次を含む（Contains）]、または [は空である（Is Empty）] を選択し、テキスト文字列を入力してメッセージ件名行を検索します。

- [受信したメッセージ数（Message Received）] : [前日（Last Day）]、[最近 1 週間（Last 7 Days）]、または [カスタム範囲（Custom Range）] を使用してクエリーの日時の範囲を指定します。過去 24 時間以内のメッセージを検索するには [前日（Last Day）] オプションを使用し、過去 7 日間のメッセージを検索するには [最近 1 週間（Last 7 Days）] オプションと当日の経過時間を使用します。

  日付を指定しなければ、クエリーは、すべての日付に対するデータを返します。時間範囲だけを指定すると、クエリーは、すべての利用可能な日付にわたってその時間範囲内のデータを返します。終了日と終了時刻に現在の日付と 23:59 を指定すると、クエリーは現在の日付に関するすべてのデータを返します。

  日付と時間は、データベースに保管される際に GMT 形式に変換されます。アプライアンス上で日付と時刻を表示する場合は、そのアプライアンスの現地時間で表示されます。

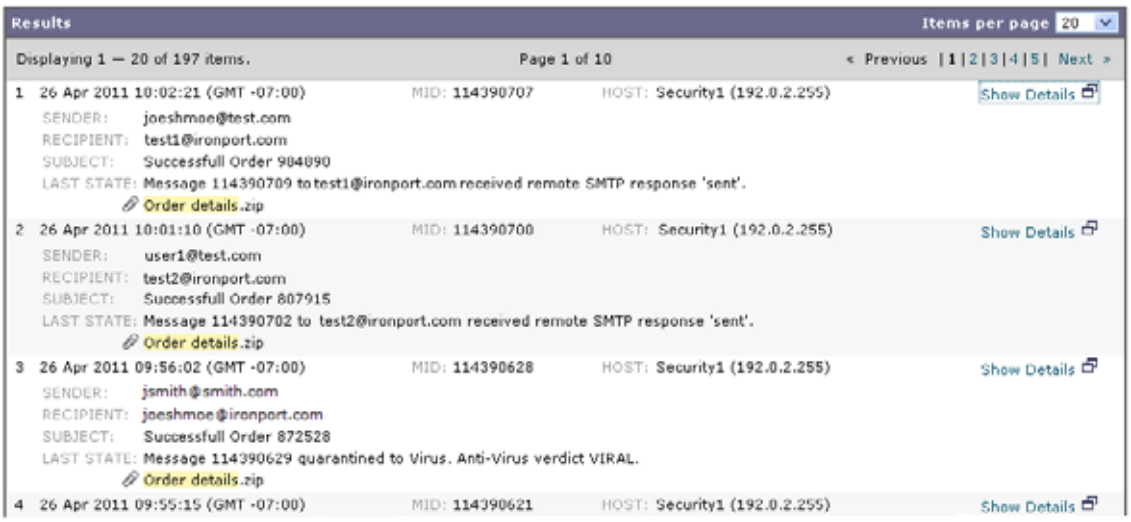
  メッセージの検索結果は、それらメッセージが電子メール セキュリティ アプライアンスのログに記録され、セキュリティ管理アプライアンスが取得した後でのみ表示されます。ログのサイズとポーリングの頻度によっては、電子メール メッセージが送信された時間と、それがトラッキングとレポーティングの結果に実際に表示される時間との間にわずかな差が生じることがあります。
- [送信者 IP アドレス（Sender IP Address）] : 送信者の IP アドレスを入力し、メッセージを検索するか、あるいは拒否された接続だけを検索するかを選択します。
  - IPv4 アドレスは、ピリオドで区切られた 4 つの数値であり、それぞれの数値は 0 ～ 255 でなければなりません （例 : *203.0.113.15*）。
  - IPv6 アドレスでは、8 つの 16 ビットの 16 進数値がコロンで区切られて構成されます。いずれか 1 箇所で、*2001:db8:80:1::5* のようにゼロ圧縮を使用できます。
- [メッセージ イベント（Message Event）] : 追跡対象のイベントを選択します。オプションは、コンテンツ フィルタによって検出され、ポリシー、ウイルス、またはアウトブレイク隔離に現在ある [ウイルス検出（Virus Positive）]、[明確なスパム（Spam Positive）]、[サスペクト スパム（Suspect Spam）]、[送信完了（Delivered）]、[DLP 違反（DLP Violations）]（DLP ポリシー名を入力し違反の重大度または対処を選択可能）、[ハード バウンス（Hard Bounced）]、[ソフト バウンス（Soft Bounced）]、および [スパムとして隔離（Quarantined as Spam）] です。トラッキング クエリーに追加する多くの条件と違い、イベントは「OR」演算子を使用して追加します。複数のイベントを選択すると、検索結果は拡大します。
- [メッセージ ID ヘッダーと Cisco IronPort MID（Message ID Header and Cisco IronPort MID）] : メッセージ ID ヘッダーのテキスト文字列、Cisco IronPort メッセージ ID（MID）、またはその両方を入力します。
- [クエリ設定（Query Settings）] : ドロップダウン メニューから、タイムアウトまでのクエリーの実行時間を選択します。オプションは、[1 分（1 minute）]、[2 分（2 minutes）]、[5 分（5 minutes）]、[10 分（10 minutes）]、[時間制限なし（No time limit）] です。クエリーから返される結果の最大数（最大 1000）も選択します。
- [添付ファイル名（Attachment name）] : [次で始まる（Begins With）]、[次に合致する（Is）]、または [次を含む（Contains）] を選択し、検索する添付ファイル名の ASCII または Unicode テキスト文字列を入力します。入力したテキストの先頭および末尾のスペースは除去されません。

すべてのフィールドに入力する必要はありません。[メッセージ イベント（Message Event）] オプションを除き、クエリーは「AND」検索になります。このクエリーは、検索フィールドで指定された「AND」条件に一致するメッセージを返します。たとえば、エンベロープ受信者と件名行のパラメータにテキスト ストリングを指定すると、クエリーは、指定されたエンベロープ受信者*と*件名行の*両方*に一致するメッセージだけを返します。

ステップ 4　[検索（Search）] をクリックします。

ページの下部にクエリー結果が表示されます。各行が 1 つの電子メール メッセージに対応します。

図 6-1　　メッセージ トラッキング クエリーの結果



各行で検索条件が強調表示されます。

返された行数が [ページ当たりのアイテム数（Items per page）] フィールドで指定した値よりも大きい場合、結果は複数のページに表示されます。ページ間を移動するには、リストの上部または下部にあるページ番号をクリックします。

必要に応じて、新しい検索条件を入力して検索精度を高め、再びクエリーを実行します。あるいは、次の項で説明するように、結果セットを絞り込んで検索精度を高めることもできます。

結果セットの絞り込み

クエリーを実行すると、結果セットに必要以上の情報が含まれていることがあります。新しいクエリーを作成するのではなく、結果リストの行内の値をクリックし、結果セットを絞り込みます。値をクリックすると、そのパラメータ値が検索の条件として追加されます。たとえば、クエリー結果に複数の日付のメッセージが含まれている場合、行内の特定の日付をクリックすると、その日付に受信されたメッセージだけが表示されます。

手順

ステップ 1　条件として追加する値の上にカーソルを移動します。値が黄色で強調表示されます。

次のパラメータ値を使用して、検索を精密化します。

- 日時（Date and time）
- メッセージ ID（Message ID）（MID）
- ホスト（Host）（電子メール セキュリティ アプライアンス）
- 送信者（Sender）
- 受信者（Recipient）
- メッセージの件名行、または件名の先頭語

ステップ 2　値をクリックして、検索を精密化します。

[結果（Results）] セクションに、元のクエリー パラメータおよび追加した新しい条件に一致するメッセージが表示されます。

ステップ 3　必要に応じて、結果内の他の値をクリックして、検索をさらに精密化します。

（注）　クエリー条件を削除するには、[消去（Clear）] をクリックし、新しいトラッキング クエリーを実行します。

トラッキング クエリー結果について

トラッキング クエリー結果には、トラッキング クエリーで指定した条件に一致するすべてのメッセージがリストされます。[メッセージ イベント（Message Event）] オプションを除き、クエリー条件は「AND」演算子を使用して追加します。結果セット内のメッセージは、すべての「AND」条件を満たしている必要があります。たとえば、エンベロープ送信者は j で始まり、件名は t で始まることを指定すると、クエリーは、両方の条件を満たすメッセージだけを返します。

メッセージの詳細情報を表示するには、各メッセージの [詳細の表示（Show Details）] リンクをクリックします。詳細については、「メッセージの詳細」（P.6-8）を参照してください。

（注）

- 50 名以上の受信者がいるメッセージは、トラッキング クエリー結果に表示されません。この問題は、今後のリリースで解決される予定です。
- クエリーを指定するとき、最大 1000 件の検索結果を表示することを選択できます。条件に一致したメッセージを最大 50,000 件表示するには、検索結果セクションの上の [すべてをエクスポート（Export All）] リンクをクリックし、別のアプリケーションで結果の .csv ファイルを開きます。
- レポート ページのリンクをクリックして、メッセージ トラッキングのメッセージ詳細を表示し、その結果が予期しないものであった場合、これは、確認期間中にレポーティングとトラッキングを同時におよび継続してイネーブルにしていない場合に発生する可能性があります。
- メッセージ トラッキングの検索結果の印刷およびエクスポートについて詳しくは、「レポーティング データおよびトラッキング データの印刷およびエクスポート」（P.3-10）を参照してください。

メッセージの詳細

メッセージ ヘッダー情報や処理の詳細など、特定の電子メール メッセージの詳細情報を表示するには、検索結果リストの任意のアイテムで [詳細の表示（Show Details）] をクリックします。メッセージの詳細が表示された新しいウィンドウが開きます。

メッセージの詳細には次のセクションが含まれます。

- 「エンベロープとヘッダーのサマリー」（P.6-9）
- 「ホスト サマリーの送信」（P.6-9）
- 「処理詳細」（P.6-9）

エンベロープとヘッダーのサマリー

このセクションには、エンベロープ送信者や受信者など、メッセージのエンベロープとヘッダーの情報が表示されます。収集する情報は次のとおりです。

[受信時間（Received Time）]：電子メール セキュリティ アプライアンスがメッセージを受信した時刻。

[MID]：メッセージ ID。

[件名（Subject）]：メッセージの件名行。

メッセージに件名がない場合、または電子メール セキュリティ アプライアンスがログ ファイルに件名行を記録するように設定されていない場合、トラッキング結果の件名行は「(件名なし（No Subject))」という値になることがあります。

[エンベロープ送信者（Envelope Sender）]：SMTP エンベロープ内の送信者のアドレス。

[エンベロープ受信者（Envelope Recipients）]：SMTP エンベロープ内の受信者のアドレス。

[メッセージ ID ヘッダー（Message ID Header）]：各電子メール メッセージを一意に識別する「Message-ID:」ヘッダー。これは最初にメッセージが作成されるときに挿入されます。「Message-ID:」ヘッダーは、特定のメッセージを検索する際に役立つ場合があります。

[Cisco IronPort ホスト（Cisco IronPort Host）]：メッセージを処理した電子メール セキュリティ アプライアンス。

[SMTP Auth ユーザ ID（SMTP Auth User ID）]：送信者が SMTP 認証を使用して電子メールを送信した場合は、送信者の SMTP 認証ユーザ名。それ以外の場合、この値は「N/A」となります。

[添付ファイル（Attachments）]：メッセージに添付されたファイルの名前。

ホスト サマリーの送信

[逆引き DNS ホスト名（Reverse DNS Hostname）]：送信側ホストのホスト名。逆引き DNS（PTR）ルックアップで検証されます。

[IP アドレス（IP Address）]：送信側ホストの IP アドレス。

[SBRS スコア（SBRS Score）]:（SenderBase レピュテーション スコア）。範囲は、10（最も信頼できる送信者）～ -10（明らかなスパム送信者）です。スコアが「None」の場合、そのメッセージが処理された時点において、このホストに関する情報が存在しなかったことを意味します。

処理詳細

このセクションには、メッセージの処理中にログに記録されたさまざまなステータス イベントが表示されます。

エントリには、アンチスパムおよびアンチウイルス スキャンなどの電子メール ポリシーの処理や、メッセージ分割などその他のイベントに関する情報が含まれます。

メッセージが配信されると、配信の詳細情報がここに表示されます。たとえば、メッセージが配信され、コピーが隔離に保存されている場合があります。

記録された最新のイベントは、処理の詳細内で強調表示されます。

[DLP に一致した内容（DLP Matched Content）] タブ

このセクションには、データ漏洩防止（DLP）ポリシーに違反するコンテンツが表示されます。

通常、このコンテンツには機密情報、たとえば企業秘密や、クレジット カード番号、健康診断の結果などの個人情報が含まれるため、セキュリティ管理アプライアンスへのアクセス権はあるが管理者レベルの権限を所持していないユーザに対し、このコンテンツへのアクセスをディセーブルにする必要が生じることがあります。「メッセージ トラッキングでの DLP 機密情報へのアクセスの制御」（P.13-24）を参照してください。

CHAPTER 7

Cisco IronPort スパム隔離の管理

Cisco IronPort スパム隔離について

Cisco IronPort スパム隔離では、組織内の電子メール ユーザに対するスパム メッセージやスパムであると疑われるメッセージを捕捉します。スパム隔離は、「誤検出」（正規の電子メールがスパムとして検出または削除されること）が問題とされる組織でのセーフガード メカニズムとなります。この機能により、エンド ユーザおよび管理者は、スパムとフラグ付けされたメッセージを確認してから最終的な決定を下すことができるようになります。さらに、セーフリスト/ブロックリスト機能をイネーブルにすると、どのようなメッセージをスパムとしてマークするかをエンド ユーザ（電子メール ユーザ）が制御できるようになります。

（注） ポリシー、ウイルス、アウトブレイク隔離は、スパム隔離とは異なります。詳細については、使用する電子メール セキュリティ アプライアンスのマニュアルおよび第 8 章「集約ポリシー、ウイルス、およびアウトブレイク隔離」を参照してください。

ローカルの Cisco IronPort スパム隔離は、電子メール セキュリティ ゲートウェイ アプライアンスに常駐します。通常はシスコのコンテンツセキュリティ管理アプライアンスですが、別のコンテンツ アプライアンスにある*外部の* Cisco IronPort スパム隔離エリアに送信されるメッセージを使用できます。

（注） Cisco IronPort スパム隔離へのエンド ユーザのアクセスは、指定したユーザまたはユーザ グループに対してのみ実装できます。また、最初にエンド ユーザ アクセスを実装した後で、エンド ユーザが隔離内のメッセージを表示および解放することがほとんどない場合は、アクセスをディセーブルにできます。

また、スパムおよびその疑いのあるメッセージが隔離されたことをエンド ユーザに電子メールで通知するように、AsyncOS を設定することもできます。通知には、そのユーザ向けに現在 Cisco IronPort スパム隔離で捕捉されているメッセージの要約が記述されています。ユーザはこのメッセージを確認して、電子メールの受信ボックスに配信するか、削除するかを判断できます。また、ユーザは隔離された

メッセージ全体を検索することができます。スパム隔離には通知メッセージからアクセスすることも、Web ブラウザを使用して直接アクセスすることもできます。（スパム隔離にエンド ユーザが直接アクセスするには、認証が必要です）。詳細については、「エンド ユーザ隔離へのアクセスの設定」（P.7-9）を参照してください）。

デフォルトでは、Cisco IronPort スパム隔離は自己メンテナンス型になっています。古いメッセージによって隔離領域がすべて消費されることを避けるために、AsyncOS は Cisco IronPort スパム隔離から定期的にメールを削除します。

管理者レベルのすべてのユーザ（デフォルトの admin ユーザなど）は、Cisco IronPort スパム隔離にアクセスし、変更を行うことができます。AsyncOS オペレータ ユーザ、およびカスタム ロールによってスパム隔離へのアクセス権が割り当てられているユーザは、隔離コンテンツの表示および管理ができますが、隔離設定の変更はできません。Cisco IronPort スパム隔離へのエンド ユーザ アクセスがイネーブルになっている場合、メールのエンド ユーザは、隔離領域にある自分のメッセージにアクセスできます。

中央集中型スパム隔離の設定

スパム隔離を中央集中型にする前に、使用している電子メール セキュリティ アプライアンスでローカルのスパム隔離を設定し、動作をテストする必要があります。

アクティブなスパム隔離を電子メール セキュリティ アプライアンスからセキュリティ管理アプライアンスへ移行するには、次の作業を順番に行ってください。

- 「必要な IP アドレスの特定」（P.7-2）
- 「セキュリティ管理アプライアンスでの Cisco IronPort スパム隔離の設定」（P.7-2）
- 「セキュリティ管理アプライアンスでのインターフェイスの設定」（P.7-4）
- 「中央集中型スパム隔離のための電子メール セキュリティ アプライアンスの設定」（P.7-5）
- 「管理対象の各電子メール セキュリティ アプライアンスへの中央集中型スパム隔離サービスの追加」（P.7-7）

必要な IP アドレスの特定

「セキュリティ管理アプライアンスでの発信 IP インターフェイスの設定」（P.7-4）の手順で使用する IP アドレスを入手または特定します。通常、これはセキュリティ管理アプライアンスの Data 2 インターフェイスのものになります。ネットワーク要件の詳細については、付録 B「ネットワークと IP アドレスの割り当て」を参照してください。

セキュリティ管理アプライアンスでの Cisco IronPort スパム隔離の設定

手順

ステップ 1　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [スパム隔離（Spam Quarantine）] を選択します。

ステップ 2　システム セットアップ ウィザードの実行後、Cisco IronPort スパム隔離を初めてイネーブルにする場合は、次の手順を実行します。

a.　[有効（Enable）] をクリックします。

b.　エンド ユーザ ライセンス契約書を確認して、[承認（Accept）] をクリックします。

ステップ 3　既存の設定を編集する場合は、[Cisco IronPort スパム隔離の設定（Cisco IronPort Spam Quarantine Settings）] セクションで [設定を編集（Edit Settings）] をクリックします。

ステップ 4　[隔離 IP インターフェイス（Quarantine IP Interface）] セクションで、ドロップダウン リストからスパム隔離用の適切な IP インターフェイスとポートを指定します。

デフォルトでは、スパム隔離では管理インターフェイスとポート 6025 を使用します。IP インターフェイスは、着信メールをリッスンするように設定されている セキュリティ管理アプライアンスのインターフェイスです。隔離ポートは、送信アプライアンスが外部隔離設定で使用しているポート番号です。

電子メール 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と同じネットワークに存在しない場合、管理インターフェイスを使用する必要があります。

ステップ 5　[送信メッセージ（Deliver Messages Via）] セクションで、対応するテキスト フィールドに、メールを配送するためのプライマリ ルートと代替用ルートを入力します。

セキュリティ管理アプライアンスからメッセージを直接送信することはしないため、発信する隔離関係の電子メール（スパム隔離から送信されるスパム通知やメッセージなど）は、メッセージ送信が設定されている他のアプライアンスまたはサーバを経由して配送する必要があります。

これらのメッセージは、SMTP またはグループウェア サーバを使用して送信できます。また、電子メール セキュリティ アプライアンスの発信リスナー インターフェイス（通常は Data2 インターフェイス）を指定することもできます。

代替用アドレスは、ロードバランシングとフェールオーバーに使用します。

電子メール セキュリティ アプライアンスが複数台ある場合は、管理対象の任意の電子メール セキュリティ アプライアンスの発信リスナー インターフェイスをプライマリ アドレスまたは代替用アドレスとして使用できます。これらはいずれも同じインターフェイス（Data 1 または Data 2）を発信リスナーとして使用する必要があります。

これらのアドレスについての他の注意事項を画面で確認してください。

ステップ 6　[次の日数の経過後に削除（Schedule Delete After）] セクションで、メッセージを削除する前に保持する日数を指定します。

または、[削除日を決めない（Do not schedule a delete）] オプション ボタンを選択して、スケジュールされた削除をディセーブルにします。削除をスケジュールするよう、隔離を設定することを推奨します。隔離によってキャパシティがいっぱいになると、最も古いメッセージから削除されます。

ステップ 7　[デフォルト言語（Default Language）] セクションで、デフォルト言語を指定します。

これは、エンド ユーザが Cisco IronPort スパム隔離にアクセスしたときに表示される言語です。

ステップ 8　（任意）[メッセージのリリース時に Cisco IronPort に通知（Notify Cisco IronPort upon Message Release）] で、解放されたメッセージのコピーを分析のために Cisco IronPort に送信する機能のチェックボックスをオンにします。

解放されたメッセージを分析のために送信するよう、隔離を設定することを推奨します。

ステップ 9　（任意）[スパム隔離のアピアランス（Spam Quarantine Appearance）] セクションで、エンド ユーザが隔離結果を表示するときに表示されるページをカスタマイズします。

次のオプションがあります。

- 現在のロゴを使用（Use Current logo）
- Cisco IronPort スパム隔離のロゴを使用（Use Cisco IronPort Spam Quarantine logo）
- カスタムロゴをアップロードする（Upload Custom logo）

[カスタムロゴをアップロードする（Upload Custom logo）] を選択すると、隔離されたメッセージを表示するためにユーザがログインしたときに、[Cisco IronPort スパム隔離（Cisco IronPort Spam Quarantine）] ページの上部にロゴが表示されます。このロゴは、最大で 550 x 50 ピクセルの .jpg、.gif、または .png ファイルにする必要があります。ロゴ ファイルがない場合、デフォルトの Cisco IronPort スパム隔離のロゴが使用されます。

ステップ 10　（任意）[ログイン メッセージ（Login Page Message）] テキスト フィールドに、ログイン ページのメッセージを入力します。このメッセージは、エンド ユーザに対して隔離へのログイン プロンプトを表示するときに表示されます。

ステップ 11　オプションで、Cisco IronPort スパム隔離を表示する権限を持つユーザのリストを変更します。詳細については、「Cisco IronPort スパム隔離への管理者ユーザ アクセスの設定」（P.7-8）を参照してください。

ステップ 12　オプションで、エンド ユーザのアクセス、およびスパム通知を設定します。詳細については、「エンド ユーザのためのスパム管理機能の設定」（P.7-9）を参照してください。

ステップ 13　変更を送信し、保存します。

セキュリティ管理アプライアンスでのインターフェイスの設定

セキュリティ管理アプライアンスでの発信 IP インターフェイスの設定

セキュリティ管理アプライアンスで、隔離に関係するメッセージ（通知や解放された電子メールなど）を 電子メール セキュリティ アプライアンスに送信するインターフェイスを設定します。

手順

ステップ 1　この手順は、「IP インターフェイスの設定」（P.A-2）の説明と併せて実行してください。

ステップ 2　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [ネットワーク（Network）] > [IP インターフェイス（IP Interfaces）] を選択します。

ステップ 3　[IP インターフェイスの追加（Add IP Interface）] をクリックします。

ステップ 4　次の設定値を入力します。

- 名前
- イーサネット ポート

  通常は Data 2 になります。具体的には、この設定は [管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [スパム隔離（Spam Quarantine）] の [スパム隔離設定（Spam Quarantine Settings）] ページにおいて、[送信メッセージ（Deliver Messages Via）] セクションでプライマリ サーバに指定した電子メール セキュリティ アプライアンスのデータ インターフェイスと同じである必要があります。
- IP アドレス

  上で指定したインターフェイスの IP アドレス。
- ネットマスク
- ホスト名

たとえば、Data 2 インターフェイスの場合は、data2.sma.example.com を使用します。

このインターフェイスの [スパム隔離（Spam Quarantine）] セクションには入力しないでください。

ステップ 5　変更を送信し、保存します。

スパム隔離にアクセスするための IP アドレスの設定

管理者またはエンド ユーザがスパム隔離にアクセスするときには、専用のブラウザ ウィンドウが開きます。

手順

ステップ 1　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [ネットワーク（Network）] > [IP インターフェイス（IP Interfaces）] を選択します。

ステップ 2　**管理**インターフェイスの名前をクリックします。

ステップ 3　[スパム隔離（Spam Quarantine）] セクションで、スパム隔離にアクセスするための設定を行います。

- [HTTP] または [HTTPS]、あるいはその両方を選択し、ポートを指定します。
- 通知とスパム隔離のブラウザ ウィンドウに記載される URL を指定します。

  たとえば、使用しているセキュリティ管理アプライアンスのホスト名を表示したくない場合には、代わりのホスト名を指定できます。

  ここに入力した URL や IP アドレスが、使用している DNS サーバで解決できることを確認してください。

ステップ 4　変更を送信し、保存します。

中央集中型スパム隔離のための電子メール セキュリティ アプライアンスの設定

セキュリティ管理アプライアンスで中央集中型の Cisco IronPort スパム隔離サービスを使用するには、電子メール セキュリティ アプライアンスでスパム隔離の設定を一部変更する必要があります。

操作内容	参照先
電子メール セキュリティ アプライアンスでスパム隔離が正しく動作していることを確認します。 何らかの問題がある場合は、スパム隔離を中央集中型にする前に解決します。	—
セキュリティ管理アプライアンスを外部スパム隔離として使用するよう、電子メール セキュリティ アプライアンスをイネーブル化および設定します。	「中央集中型スパム隔離のための電子メール セキュリティ アプライアンスの設定」（P.7-6）

操作内容	参照先
電子メール セキュリティ アプライアンス でローカルのスパム隔離をディセーブルにします。	ご使用の電子メール セキュリティ アプライアンスのマニュアルまたはオンライン ヘルプの「Disabling the Local Spam Quarantine」。 この変更によって生じたメール ポリシーを調整するための警告は無視します。メール ポリシーで外部スパム隔離を使用するようになります。
電子メール セキュリティ アプライアンスで既存のローカルのスパム隔離メッセージを管理する方法を確認します。	ご使用の電子メール セキュリティ アプライアンスのマニュアルまたはオンライン ヘルプの「Migrating from a Local Spam Quarantine to an External Quarantine」。

中央集中型スパム隔離のための電子メール セキュリティ アプライアンスの設定

電子メール セキュリティ アプライアンスでセキュリティ管理アプライアンスの Cisco IronPort スパム隔離を使用するには、電子メール セキュリティ アプライアンスの外部隔離を設定する必要があります。

（注） これまで、電子メール セキュリティ アプライアンスに別の外部スパム隔離を設定していた場合は、まず、その外部スパム隔離設定をディセーブルにする必要があります。

外部隔離を設定するには、次の手順を**すべての** 電子メール セキュリティ アプライアンスで実行する必要があります。

手順

ステップ 1　電子メール セキュリティ アプライアンスで、[セキュリティ サービス（Security Services）] > [外部スパム隔離（External Spam Quarantine）] を選択します。

ステップ 2　[設定（Configure）] をクリックします。

ステップ 3　チェックボックスを選択して、外部スパム隔離をイネーブルにします。

ステップ 4　Cisco IronPort スパム隔離の名前を入力します。隔離領域があるセキュリティ管理アプライアンスの名前を入力することもできます。

ステップ 5　セキュリティ管理アプライアンスの正しいインターフェイスの IP アドレスを入力します。

通常は管理インターフェイスのアドレスになります。具体的には、[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [スパム隔離（Spam Quarantine）] の [スパム隔離設定（Spam Quarantine Settings）] ページにある [隔離 IP インターフェイス（Quarantine IP Interface）] 設定で、セキュリティ管理アプライアンスに指定したインターフェイスに割り当てた IP アドレスです。

指定したインターフェイスの IP アドレスを表示するには、セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [ネットワーク（Network）] > [IP インターフェイス（IP Interfaces）] を選択して、インターフェイス名をクリックしてください。

ステップ 6　スパムおよびその疑いのあるメッセージの配信に使用するポート番号を入力します。デフォルトは 6025 です。このポート番号は、[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [スパム隔離（Spam Quarantine）] の [スパム隔離設定（Spam Quarantine Settings）] ページで入力した隔離ポート番号と同じである必要があります。

ステップ 7　簡単にするために、セーフリスト/ブロックリスト機能は後で設定します。全体の説明と詳細については、「エンド ユーザのセーフリスト/ブロックリスト機能の設定と管理」（P.7-12）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。

ステップ 9　ローカルのスパム隔離をディセーブルにします。ご使用の電子メール セキュリティ アプライアンスのマニュアルまたはオンライン ヘルプの「Disabling the Local Spam Quarantine」を参照してください。

この変更によって生じたメール ポリシーを調整するための警告は無視します。メール ポリシーで外部スパム隔離を使用するようになります。

ステップ 10　管理対象の電子メール セキュリティ アプライアンスに対して、この手順を繰り返します。

管理対象の各電子メール セキュリティ アプライアンスへの中央集中型スパム隔離サービスの追加

ここで実行する手順は、他の中央集中型管理機能の設定時に、すでにこのアプライアンスを追加したかどうかによって異なります。

手順

ステップ 1　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [セキュリティ アプライアンス（Security Appliances）] を選択します。

ステップ 2　このページのリストに、すでに電子メール セキュリティ アプライアンスを追加している場合は、次の手順を実行します。

a.　電子メール セキュリティ アプライアンスの名前をクリックします。

b.　[スパム隔離（Spam Quarantine）] サービスを選択します。

ステップ 3　電子メール セキュリティ アプライアンスをまだ追加していない場合は、次の手順を実行します。

a.　[メール アプライアンスの追加（Add Email Appliance）] をクリックします。

b.　[アプライアンス名および IP アドレス（Appliance Name and IP Address）] テキスト フィールドに、Cisco IronPort アプライアンスの管理インターフェイスのアプライアンス名と IP アドレスを入力します。

（注）　[IP アドレス（IP Address）] テキスト フィールドに DNS 名を入力した場合でも、[送信（Submit）] をクリックすると、すぐに IP アドレスに解決されます。

c.　Spam Quarantine サービスが事前に選択されています。

d.　[接続の確立（Establish Connection）] をクリックします。

e.　管理対象となるアプライアンスの管理者アカウントのユーザ名とパスワードを入力し、[接続の確立（Establish Connection）] をクリックします。

（注）　ログイン資格情報を入力すると、セキュリティ管理アプライアンスからリモート アプライアンスへのファイル転送のための公開 SSH キーが渡されます。ログイン資格情報は、セキュリティ管理アプライアンスには保存されません。

f. [成功（Success）] メッセージがページのテーブルの上に表示されるまで待機します。

g. [テスト接続（Test Connection）] をクリックします。

h. テーブルの上のテスト結果を確認します。

ステップ 4　[送信（Submit）] をクリックします。

ステップ 5　スパム隔離をイネーブルにする電子メール セキュリティ アプライアンスごとに、この手順を繰り返します。

ステップ 6　変更を保存します。

Cisco IronPort スパム隔離への管理者ユーザ アクセスの設定

この項の手順を実行すると、Operator、Read-Only Operator、Help Desk のロール、または Guest ロール、およびスパム隔離にアクセスできるカスタム ユーザ ロールを持つ管理者ユーザが、Cisco IronPort スパム隔離でメッセージを管理できるようになります。

デフォルトの admin ユーザ、Email Administrator ユーザを含む Administrator レベルのユーザは、常にスパム隔離にアクセスできるので、この手順を使用してスパム隔離機能に関連付ける必要はありません。

（注）　管理者レベル以外のユーザはスパム隔離のメッセージにアクセスできますが、隔離の設定を編集することはできません。管理者レベルのユーザは、メッセージにアクセスし、設定を編集することができます。

完全な管理者権限を持っていない管理者ユーザがスパム隔離のメッセージを管理できるようにするには、次の手順を実行してください。

手順

ステップ 1　ユーザを作成し、そのユーザにスパム隔離へのアクセス権があるユーザ ロールを割り当てる必要があります。詳細については、「管理タスクの分散について」（P.13-1）を参照してください。

ステップ 2　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [スパム隔離（Spam Quarantine）] を選択します。

ステップ 3　[スパム隔離設定（Spam Quarantine Settings）] セクションで、[有効（Enable）] または [設定を編集（Edit Settings）] をクリックします。

ステップ 4　[スパム隔離設定（Spam Quarantine Settings）] セクションの [管理ユーザ（Administrative Users）] 領域で、[ローカル ユーザ（Local Users）]、[外部認証ユーザ（Externally Authenticated Users）]、または [カスタム ユーザ ロール（Custom User Roles）] の選択リンクをクリックします。

ステップ 5　スパム隔離のメッセージを表示および管理できるアクセス権を付与するユーザを選択します。

ステップ 6　[OK] をクリックします。

ステップ 7　必要な場合、このセクションの [管理ユーザ（Administrative Users）] にリストされているその他のタイプ（[ローカル ユーザ（Local Users）]、[外部認証ユーザ（Externally Authenticated Users）]、または [カスタム ユーザ ロール（Custom User Roles）]）について繰り返します。

ステップ 8　変更を送信し、保存します。

エンドユーザのためのスパム管理機能の設定

（注）　追加設定はいずれか 1 つだけ設定でき、それ以外は設定できません。たとえば、常に要求に基づいて、または指定されたユーザにのみアクセスを許可する場合、エンド ユーザ アクセスを設定できますが、スパム通知は設定できません。

エンド ユーザ隔離へのアクセスの設定

電子メール ユーザが、Cisco IronPort スパム隔離で自身のメッセージを管理できるようにします。

手順

ステップ 1　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [スパム隔離（Spam Quarantine）] を選択します。

ステップ 2　[Cisco IronPort スパム隔離の設定（Cisco IronPort Spam Quarantine Settings）] セクションで [設定を編集（Edit Settings）] をクリックします。

ステップ 3　[エンドユーザの隔離へのアクセス（End-User Quarantine Access）] セクションまでスクロールします。

ステップ 4　[エンドユーザの隔離へのアクセスを有効にする（Enable End-User Quarantine Access）] チェックボックスをオンにします。

ステップ 5　エンド ユーザが隔離されたメッセージを表示しようとしたときに、エンド ユーザを認証する方式を指定します。メールボックス認証、LDAP 認証、または「なし」を指定できます。

- **メールボックス認証**：認証用の LDAP ディレクトリがないサイトの場合、スパム隔離では、ユーザのメールボックスを保有している標準の IMAP サーバまたは POP サーバにユーザの電子メール アドレスとパスワードを照合することができます。Web UI にログインするとき、ユーザは自身の完全な電子メール アドレスとメールボックスのパスワードを入力します。隔離はこの情報を使用し、そのユーザとしてメールボックス サーバにログインします。ログインに成功すると、そのユーザは認証され、スパム隔離はユーザの受信箱を変更せずにメールボックス サーバからログアウトします。LDAP ディレクトリを使用しないサイトには、メールボックス認証が推奨されます。ただし、メールボックス認証では、複数の電子メール エイリアスに送信された隔離済みメッセージを表示できません。

  メールボックス サーバのタイプ（IMAP または POP）を選択します。サーバ名と、安全な接続に SSL を使用するかどうかを指定します。サーバのポート番号を入力します。未修飾のユーザ名の後ろに追加するドメイン（company.com など）を入力します。

POP サーバがバナーに APOP サポートをアドバタイズする場合は、セキュリティの理由から（すなわち、パスワードがクリアな状態で送信されないように）、アプライアンスでは APOP だけを使用します。一部のユーザで APOP がサポートされていない場合は、APOP をアドバタイズしないように POP サーバを再設定する必要があります。

- [LDAP]：LDAP サーバまたはアクティブなエンド ユーザ認証クエリーが設定されていない場合は、[Management Appliance] > [システム管理（System Administration）] > [LDAP] リンクを選択して、LDAP サーバ設定とエンド ユーザ認証クエリー ストリングを設定します。LDAP 認証の設定の詳細については、「LDAP サーバ プロファイルの作成」（P.11-2）を参照してください。
- [なし（None）]：認証をイネーブルにしなくても、Cisco IronPort スパム隔離へのエンド ユーザのアクセスを許可できます。この場合、ユーザは通知メッセージのリンクをクリックして隔離にアクセスでき、システムはメールボックス認証または LDAP 認証を行いません。

ステップ 6　隔離からメッセージが解放される前に、メッセージ本文を表示するかどうかを指定します。

このチェックボックスが選択されていると、[Cisco IronPort スパム隔離（Cisco IronPort Spam Quarantine）] ページでメッセージ本文を表示できなくなります。代わりとして、隔離されたメッセージを表示するには、そのメッセージを解放してから、ユーザのメール アプリケーション（Microsoft Outlook など）で表示する必要があります。この機能は、ポリシーおよび規制（表示したすべての電子メールをアーカイブすることが要求されている場合など）へのコンプライアンスの目的で使用できます。

ステップ 7　変更を送信し、保存します。

エンドユーザのためのスパム通知の設定

スパム通知とは、Cisco IronPort スパム隔離内にメッセージが捕捉されているときに、電子メール ユーザに送信される電子メール メッセージのことです。通知には、そのユーザ宛の隔離されたスパムまたはその疑いのあるメッセージのリストが含まれます。さらに、各ユーザがそれぞれの隔離されたメッセージを表示できるリンクも含まれます。イネーブルにすると、指定したスケジュールに従って通知が送信されます。

スパム通知を使用すると、エンド ユーザが LDAP 認証またはメールボックス認証を使用しないでスパム隔離にログインできるようになります。ユーザは、受信した電子メール通知を介して隔離にアクセスします（その隔離に対して通知がイネーブルになっている場合）。メッセージの件名をクリックすると、ユーザは隔離の Web UI にログインします。

（注）　このログイン方式では、そのエンド ユーザが持っている可能性のある他のエイリアス宛の隔離済みメッセージは表示されません。また、アプライアンスで処理した後に展開される配布リストに通知が送信された場合、複数の受信者がそのリストの同じ隔離にアクセスできます。

アプライアンスがスパム通知を生成する方法でそのようになっているため、ユーザは、自分の電子メール エイリアス宛の複数のスパム通知を受信することがあります。また、複数の電子メール アドレスを使用しているユーザも、複数のスパム通知を受信することがあります。複数の通知は、エイリアス統合機能を使用して一部の発生を防ぐことができます。**LDAP サーバまたはアクティブなエイリアス統合クエリーが設定されていない場合は、[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [LDAP] を選択して、LDAP サーバ設定とエイリアス統合クエリー ストリングを設定します。**詳細については、「エンドユーザのためのスパム管理機能の設定」（P.7-9）を参照してください。

手順

ステップ 1　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [スパム隔離（Spam Quarantine）] を選択します。

ステップ 2　[Cisco IronPort スパム隔離の設定（Cisco IronPort Spam Quarantine Settings）] セクションで [設定を編集（Edit Settings）] をクリックします。

ステップ 3　[スパム通知を有効にする（Enable Spam Notification）] チェックボックスをオンにして、スパム通知をイネーブルにします。

ステップ 4　通知の [送信元アドレス（From Address）] を入力します。このアドレスを、ユーザの電子メール クライアントでサポートされている「ホワイトリスト」に追加することもできます。

ステップ 5　通知の [件名（Subject）] を入力します。

ステップ 6　カスタマイズする通知の [タイトル（Title）] を入力します。

ステップ 7　[デフォルト言語（Default Language）] を選択します。

ステップ 8　メッセージ本文をカスタマイズします。AsyncOS では、メッセージ本文に挿入されると、個々のエンド ユーザに対応した実際の値に展開されるいくつかのメッセージ変数がサポートされています。たとえば、**%username%** は、そのユーザへの通知が生成されるときに、実際のユーザ名に展開されます。サポートされるメッセージ変数には、次のものがあります。

- [新規メッセージ数（New Message Count）]（**%new_message_count%**）：ユーザの最後のログイン以後の新しいメッセージの数。
- [総メッセージ数（Total Message Count）]（**%total_message_count%**）：エンド ユーザ隔離内にあるこのユーザ宛のメッセージの数
- [メッセージ保存期間（Days Until Message Expires）]（**%days_until_expire%**）
- [隔離 URL（Quarantine URL）]（**%quarantine_url%**）：スパム隔離にログインし、メッセージを表示するための URL。
- [Username]（**%username%**）
- [新規メッセージ一覧（New Message Table）]（**%new_quarantine_messages%**）：隔離領域内にあるこのユーザ宛の新しいメッセージのリスト

これらのメッセージ変数は、[メッセージ本文（Message Body）] フィールドのテキスト内に直接入力して、メッセージ本文に挿入できます。あるいは、変数を挿入する場所にカーソルを配置してから、右側の [メッセージ変数（Message Variables）] リスト内にある変数の名前をクリックすることもできます。

ステップ 9　メッセージ形式（HTML、テキスト、または HTML/テキスト）を選択します。

ステップ 10　バウンス アドレスを指定します。バウンスされた通知は、このアドレスに送信されます。

ステップ 11　必要に応じて、異なるアドレスで同じ LDAP ユーザに送信されたメッセージを統合できます。

ステップ 12　通知スケジュールを設定します。通知を月に一度、週に一度、または毎日（平日のみ、または週末も含めて）の指定した時間に送信するように設定できます。

ステップ 13　変更を送信し、保存します。

エンド ユーザのセーフリスト/ブロックリスト機能の設定と管理

エンド ユーザによるセーフリストとブロックリストの作成を許可して、スパムとして処理する電子メール メッセージをより適切に制御できます。セーフリストによって、指定されたユーザおよびドメインからのメールがスパムとして処理されないようにできます。ブロックリストでは、他のユーザおよびドメインからのメールが常にスパムとして処理されるようにします。セーフリスト/ブロックリスト機能がイネーブルにされると、各エンド ユーザは、自分の電子メール アカウントに対してセーフリストとブロックリストを維持できるようになります。

（注）　セーフリストやブロックリストを設定しても、メッセージに対するウイルスのスキャンや、内容に関連したメール ポリシーの基準をメッセージが満たすかどうかの判定は、電子メール セキュリティ アプライアンスで実行されます。セーフリストのメンバーから送信されたメッセージの場合、他のスキャン設定に従って配信されない場合があります。

ユーザがセーフリストまたはブロックリストにエントリを追加すると、そのエントリは セキュリティ管理アプライアンス上のデータベースに保管され、関連するすべての 電子メール セキュリティ アプライアンスで、定期的に更新および同期されます。同期の詳細については、「セーフリストとブロックリストの設定とデータベースの同期」（P.7-13）を参照してください。データベースのバックアップの詳細については、「セーフリスト/ブロックリスト データベースのバックアップと復元」（P.7-15）を参照してください。

セーフリストとブロックリストは、エンド ユーザによって作成およびメンテナンスされます。ただし、この機能をイネーブルにし、ブロックリスト内のエントリに一致する電子メール メッセージの配信設定を設定するのは管理者です。セーフリストとブロックリストは Cisco IronPort スパム隔離に関連するため、配信の動作は、他のアンチスパム設定にも左右されます。電子メール パイプラインでメッセージが電子メール セキュリティ マネージャに到達する前に発生する処理に基づいて、メッセージがアンチスパム スキャンをスキップすることがあります。メッセージ処理に関する詳細情報については、お使いの電子メール セキュリティ アプライアンス のマニュアルまたはオンライン ヘルプの「Understanding the Email Pipeline」を参照してください。

たとえば、アンチスパム スキャンをスキップするように HAT で「Accept」メール フロー ポリシーを設定すると、そのリスナー上でメールを受信するユーザでは、自分のセーフリストとブロックリストの設定をそのリスナー上で受信されたメールに適用しないようになります。同様に、一部のメッセージ受信者についてアンチスパム スキャンをスキップするメールフロー ポリシーを作成すると、それらの受信者は、自分のセーフリストとブロックリストの設定が適用されなくなります。

セーフリスト/ブロックリスト メッセージの配信の詳細については、「セーフリストとブロックリストのメッセージ配信」（P.7-14）を参照してください。

セキュリティ管理アプライアンスでのセーフリスト/ブロックリストのイネーブル化と設定

セーフリスト/ブロックリスト機能をイネーブル化する前に、アプライアンスで Cisco IronPort スパム隔離をイネーブル化する必要があります。Cisco IronPort スパム隔離のイネーブル化の詳細については、「中央集中型スパム隔離の設定」（P.7-2）を参照してください。

手順

ステップ 1　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [スパム隔離（Spam Quarantine）] を選択します。

ステップ 2　[End-User Safelist/Blocklist] セクションで [有効（Enable）] をクリックします。

ステップ 3　[エンド ユーザ セーフリスト/ブロックリス（End-User Safelist/Blocklist）] セクションで [設定を編集（Edit Settings）] をクリックします。

ステップ 4　[エンド ユーザ セーフリスト/ブロックリスト機能を有効にする（Enable End User Safelist/Blocklist Feature）] 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　ユーザごとの最大リスト項目数を指定します。この値は、ユーザがそれぞれのセーフリスト/ブロックリストに含めることのできるアドレスとドメインの最大数です。デフォルトは 100 です。

（注）　ユーザごとのリスト エントリ数を大きくすると、システムのパフォーマンスに悪影響を与えることがあります。

ステップ 6　更新頻度を選択します。この値によって、AsyncOS がシステムにある 電子メール セキュリティ アプライアンスのセーフリスト/ブロックリスト データベースを更新する頻度が決まります。M10、M600、および M650 アプライアンスのデフォルトは、2 時間ごとです。M1000 および M1050 アプライアンスのデフォルトは、4 時間ごとです。

ステップ 7　変更を送信し、保存します。

ステップ 8　この機能の中央集中化をサポートするよう、電子メール セキュリティ アプライアンスを設定します。「電子メール セキュリティ アプライアンスでのセーフリスト/ブロックリストの設定」（P.7-13）を参照してください。

電子メール セキュリティ アプライアンスでのセーフリスト/ブロックリストの設定

管理対象の電子メール セキュリティ アプライアンスでセーフリスト/ブロックリストの設定を行うには、**それぞれの**電子メール セキュリティ アプライアンスで次の手順を実行してください。

手順

ステップ 1　電子メール セキュリティ アプライアンスで、[セキュリティ サービス（Security Services）] > [外部スパム隔離（External Spam Quarantine）] を選択します。

ステップ 2　[設定を編集（Edit Settings）] ボタンをクリックします。

ステップ 3　セーフリスト/ブロックリスト機能をイネーブルにするチェックボックスを選択します。

ステップ 4　ブロックリストに含まれる送信者からのメッセージを隔離するか、削除するかを選択します。

ステップ 5　変更を送信し、保存します。

ステップ 6　管理対象の電子メール セキュリティ アプライアンスに対して、この手順を繰り返します。

セーフリストとブロックリストの設定とデータベースの同期

セキュリティ管理アプライアンスを使用すると、簡単に、すべての管理対象アプライアンスでセーフリスト/ブロックリスト データベースを同期することができます。

（注）　セーフリスト/ブロックリスト データベースを同期する前に、セーフリスト/ブロックリスト機能をイネーブル化して、少なくとも 1 台の管理対象アプライアンスを セキュリティ管理アプライアンスに追加する必要があります。管理対象アプライアンスを追加する方法の詳細については、「管理対象アプライアンスの追加について」（P.2-12）を参照してください。

セーフリスト/ブロックリスト データベースを同期するには、[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [スパム隔離（Spam Quarantine）] ページで [すべてのアプライアンスを同期（Synchronize All Appliances）] ボタンをクリックします。

集中管理機能を使用して複数のアプライアンスを設定する場合は、集中管理を使用して管理者設定を設定できます。集中管理を使用しない場合は、マシン間で設定が整合していることを手動で確認できます。

FTP を使用してアプライアンスにアクセスする方法の詳細については、付録 A「IP インターフェイスおよびアプライアンスへのアクセス」（P.1）を参照してください。

セーフリストとブロックリストのメッセージ配信

セーフリストとブロックリストをイネーブルにすると、電子メール セキュリティ アプライアンスは、アンチスパム スキャンの直前にセーフリスト/ブロックリスト データベースと照合してメッセージをスキャンします。アプライアンスがエンド ユーザのセーフリスト/ブロックリスト設定に一致する送信者またはドメインを検出したとき、セーフリスト/ブロックリスト設定が異なる受信者が複数存在すると、そのメッセージは分割されます。たとえば、送信者 X が受信者 A と受信者 B の両方にメッセージを送信したとします。受信者 A のセーフリストには送信者 X のエントリがありますが、受信者 B のセーフリストにもブロックリストにも、この送信者のエントリがありません。この場合、メッセージは 2 つのメッセージ ID で 2 つのメッセージに分割されます。受信者 A に送信されたメッセージには、*X-SLBL-Result-Safelist* ヘッダーによって、セーフリストに登録されているというマークが付けられます。これにより、アンチスパム スキャンがスキップされます。受信者 B に宛てられたメッセージは、アンチスパム スキャン エンジンでスキャンされます。その後、どちらのメッセージもパイプライン（アンチウイルス スキャン、コンテンツ ポリシーなど）を続行し、設定されているすべての設定に従います。

メッセージの送信者またはドメインがブロックリストに含まれる場合、配信の動作は、ブロックリスト アクション設定によって決まります。セーフリストの配信の場合と同様に、セーフリスト/ブロックリスト設定の異なる複数の受信者が存在すると、そのメッセージは分裂します。分裂したメッセージのうちブロックリストに含まれるものは、ブロックリスト アクション設定に応じて隔離されるかドロップされます。

（注）　ブロックリスト アクションは、電子メール セキュリティ アプライアンスの外部スパム隔離設定で指定します。詳細については、「中央集中型スパム隔離のための電子メール セキュリティ アプライアンスの設定」（P.7-6）を参照してください。

メッセージを隔離するようにブロックリスト アクションを設定した場合、メッセージはスキャンされ、最終的に隔離されます。メッセージを削除するようにブロックリスト アクションを設定した場合、セーフリスト/ブロックリスト スキャンの直後にメッセージは削除されます。

セーフリスト/ブロックリスト データベースのバックアップと復元

セーフリスト/ブロックリスト データベースのバックアップを維持できるように、セキュリティ管理アプライアンスでデータベースを .csv ファイルとして保存できます。.csv ファイルは、アプライアンスの設定が格納される XML コンフィギュレーション ファイルとは別に保管されます。アプライアンスをアップグレードする場合、またはシステム セットアップ ウィザードを実行する場合、まず、セーフリスト/ブロックリスト データベースを .csv ファイルにバックアップする必要があります。

（注）　.csv ファイルを編集してからアップロードすると、個別のエンド ユーザのセーフリストおよびブロックリストを変更できます。

データベースをバックアップすると、アプライアンスによって、.csv ファイルが次の命名規則に従って `/configuration` ディレクトリに保存されます。

slbl-<serial number>-<timestamp>.csv

セキュリティ管理アプライアンスをバックアップするときには、セーフリストおよびブロックリストのデータベースを対象に含めるかどうかを選択できます 「セキュリティ管理アプライアンスのデータのバックアップ」（P.14-7）を参照してください。

手順

ステップ 1　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [設定ファイル（Configuration File）] を選択します。

ステップ 2　[エンド ユーザ セーフリスト/ブロックリスト データベース（スパム隔離）（End-User Safelist/Blocklist Database (Spam Quarantine)）] セクションまでスクロールします。

ステップ 3　データベースを .csv ファイルにバックアップするには、[今すぐバックアップ（Backup Now）] をクリックします。

ステップ 4　[リストアするファイルを選択（Select File to Restore）] をクリックして、データベースを復元します。

アプライアンスにより、`/configuration` ディレクトリに保管されているバックアップ ファイルのリストが表示されます。

ステップ 5　復元するセーフリスト/ブロックリスト バックアップ ファイルを選択し、[リストア（Restore）] をクリックします。

セーフリストとブロックリストのトラブルシューティング

エンド ユーザは、自分のセーフリストとブロックリストを管理します。管理者が、エンド ユーザ アカウントにそのユーザのログイン名とパスワードでログインすると、エンド ユーザのセーフリストまたはブロックリストにアクセスできます。または、管理者はセーフリスト/ブロックリスト データベースのバックアップ バージョンをダウンロードして、個別のユーザのリストを編集できます。

セーフリストとブロックリストに関する問題をトラブルシューティングするために、ログ ファイルまたはシステム アラートを表示できます。

電子メール メッセージがセーフリスト/ブロックリスト設定によってブロックされると、そのアクションが ISQ_logs またはアンチスパム ログ ファイルにロギングされます。

アラートは、データベースが作成または更新されたり、データベースの変更またはセーフリスト/ブロックリスト プロセスの実行においてエラーが発生したりすると送信されます。

アラートの詳細については、「アラートの管理」（P.14-33）を参照してください。

ログ ファイルの詳細については、第 15 章「ロギング」を参照してください。

エンド ユーザのセーフリストおよびブロックリストの使用

エンド ユーザは、指定した送信者からのメッセージをスパムの判定から除外するために、セーフリストを作成できます。また、指定した送信者からのメッセージを常にスパムとして扱うために、ブロックリストを使用できます。たとえば、エンド ユーザは、受信したくない電子メールをメーリング リストから受信する場合があります。この送信者をブロックリストに追加すると、この送信者からの電子メール メッセージが配信されないようになります。一方、エンド ユーザは、正当な送信者からの電子メール メッセージが Cisco IronPort スパム隔離に送信されていることに気づき、この電子メール メッセージがスパムとして処理されないようにしたいと考えることがあります。その送信者からのメールが隔離されないようにするには、ユーザのセーフリストに送信者を追加します。

（注）　セーフリスト/ブロックリスト設定は、システム管理者が設定する他の設定の影響を受けます。たとえば、セーフリストに登録されているメッセージが、ウイルス陽性と判断された場合、または管理者によって内容が企業の電子メール ポリシーに準拠していないと判断された場合、このメッセージは配信されません。

セーフリストとブロックリストへのアクセス

LDAP 認証またはメールボックス（IMAP または POP）認証を使用してアカウントが認証されるエンド ユーザは、セーフリストとブロックリストにアクセスするために、Cisco IronPort スパム隔離の自分のアカウントにログインする必要があります。これらのエンド ユーザは、通常はスパム通知経由でメッセージにアクセスしているとしても（この場合は一般に LDAP 認証またはメールボックス認証を必要としません）、自分のアカウントにログインしなければなりません。エンド ユーザ認証が [なし（None）] に設定されている場合、エンド ユーザは、セーフリスト/ブロックリスト設定にアクセスする際に自分のアカウントにログインする必要はありません。

セーフリストおよびブロックリストへのエントリの追加

エントリ（IPv6 アドレスを使用するものを含む）をセーフリスト/ブロックリストに追加するときには、次の形式を使用できます。

- user@domain.com

  user@[203.0.113.15]

  user@[ipv6:2001:db8:80:1::5]
- server.domain.com
- domain.com

  [203.0.113.15]

  [ipv6:2001:db8:80:1::5]

エンド ユーザは、同じ送信者またはドメインをセーフリストとブロックリストの両方に同時には追加できません。ただし、あるドメインをセーフリストに追加し、そのドメインに所属するユーザをブロックリストに追加した場合、両方のルールが適用されます（逆の場合も同様です）。たとえば、エンド

ユーザが *example.com* をセーフリストに追加し、*george@example.com* をブロックリストに追加すると、アプライアンスは、example.com からのすべてのメールをスパムかどうかスキャンせずに配信しますが、*george@example.com* からのメールはスパムとして処理します。

エンド ユーザは、.domain.com のような構文を使用して、サブドメインの範囲を許可したり、ブロックしたりはできません。ただし、エンド ユーザは、server.domain.com のような構文を使用して、特定のドメインを明示的にブロックすることはできます。

セーフリストの操作

エンド ユーザは、次の 2 つの方法で送信者をセーフリストに追加できます。Cisco IronPort スパム隔離から、グラフィカル ユーザ インターフェイスの右上にある [オプション（Options）] メニューをクリックし、[セーフリスト（Safelist）] を選択して、手動で送信者をセーフリストに追加できます。

電子メール アドレスまたはドメインをリストに追加し、[リストに追加（Add to List）] をクリックします。

エンド ユーザは、メッセージが Cisco IronPort スパム隔離に送信されていても、その送信者をセーフリストに追加できます。特定の送信者からのメッセージが Cisco IronPort スパム隔離に捕捉されている場合、エンド ユーザはそのメッセージの横にあるチェックボックスをオンにして、ドロップダウン メニューから [リリースしてセーフリストに追加（Release and Add to Safelist）] を選択できます。

指定したメールのエンベロープ送信者と差出人ヘッダーが両方ともセーフリストに追加されます。解放されたメッセージは、それ以降の電子メール パイプライン内の作業キューの処理をスキップして、宛先キューへ直接進みます。

（注）　エンド ユーザは、スパム通知メッセージを使用してメッセージを解放することもできます。[スパムではない（Not Spam）] リンクをクリックして、特定のメッセージを解放します。送信者をエンド ユーザのセーフリストに追加するオプションもあります。

ブロックリストの操作

エンド ユーザは、ブロックリストを使用して、指定した送信者からのメールが配信されないようにできます。送信者をブロックリストに追加するには、エンド ユーザ隔離から [オプション（Options）] > [ブロックリスト（Blocklist）] を選択します。

エンド ユーザ隔離から、フィールドに電子メール アドレスまたはドメインを入力し、[リストに追加（Add to List）] をクリックします。

電子メール セキュリティ アプライアンスは、ブロックリスト内のエントリと一致する電子メール アドレスまたはドメインからのメールを受信すると、そのメールをスパムとして処理します。ブロックリスト アクション設定に応じて、そのメールは削除または隔離されます。

Cisco IronPort スパム隔離内のメッセージの管理

ここでは、管理者が Cisco IronPort スパム隔離内のメッセージを管理する方法について説明します。管理者が隔離を表示する場合、その隔離領域に含まれるすべてのメッセージを利用できます。

（注）　メッセージを表示および管理するグラフィカル ユーザ インターフェイスは、Cisco IronPort スパム隔離にアクセスするエンド ユーザ用のものとは少し異なります。エンド ユーザ用のグラフィカル ユーザ インターフェイスについては、エンド ユーザとして Cisco IronPort スパム隔離にアクセスし、オンライン ヘルプを参照してください。

管理者として、Cisco IronPort スパム隔離内のメッセージに対して次のアクションを実行できます。

- メッセージの表示
- メッセージの配信
- メッセージの削除
- メッセージの検索

Cisco IronPort スパム隔離内でのメッセージの検索

手順

ステップ 1　セキュリティ管理アプライアンスで、[メール（Email）] > [メッセージの隔離（Message Quarantine）] > [スパム隔離（Spam Quarantine）] を選択します。

ステップ 2　[スパム隔離（Spam Quarantine）] リンクを選択します。

ステップ 3　検索フォームで、検索する日付を入力します。現在の日、または過去の週からメッセージを検索できます。または、カレンダー アイコンをクリックして、日付範囲を選択できます。

ステップ 4　オプションで、差出人アドレス、受取人アドレス、メッセージ件名のテキスト文字列を指定します。入力した値が検索結果に含まれる、含まれない、全体と一致、先頭と一致、末尾と一致のいずれかを選択します。

ステップ 5　オプションで、エンベロープ受信者を指定します。入力した値が検索結果に含まれる、含まれない、全体と一致、先頭と一致、末尾と一致のいずれかを選択します。

エンベロープ受信者とは、「RCPT TO」SMTP コマンドで定義されている電子メール メッセージ受信者のアドレスです。エンベロープ受信者は、「Recipient To」アドレスまたは「Envelope To」アドレスと呼ばれることもあります。

ステップ 6　[検索（Search）] をクリックします。

検索条件に一致するメッセージがページの [検索（Search）] セクションの下に表示されます。

大量メッセージの検索

Cisco IronPort スパム隔離内に大量のメッセージが保存されており、検索条件が狭く定義されていない場合、検索結果の表示に時間がかかることや、クエリーがタイムアウトすることがあります。

その場合、検索を再実行するかどうか確認されます。

（注）　大量の検索を同時に複数実行すると、アプライアンスのパフォーマンスに悪影響を与えることがあります。

Cisco IronPort スパム隔離内のメッセージの表示

メッセージのリストにより、Cisco IronPort スパム隔離内のメッセージが表示されます。1 ページに表示されるメッセージの数を選択できます。カラム見出しをクリックすることにより、表示をソートできます。再度カラム見出しをクリックすると、ソートの順を反転できます。

メッセージの件名をクリックしてメッセージを表示します。これには、本文とヘッダーが含まれます。[メッセージの詳細（Message Details）] ページには、メッセージの先頭 20K が表示されます。メッセージがそれよりも長い場合は、20K に切り詰められます。ページの下部にあるリンクをクリックすると、メッセージの残りの部分が表示されます。

[メッセージの詳細（Message Details）] ページから、[削除（Delete）] を選択してメッセージを削除したり、[リリース（Release）] を選択してメッセージを隔離から解放したりできます。メッセージを解放すると、そのメッセージは配信されます。

HTML メッセージの表示

Cisco IronPort スパム隔離では、HTML ベースのメッセージは近似で表示されます。イメージは表示されません。

符号化されたメッセージの表示

Base64 で符号化されたメッセージは、復号化されてから表示されます。

Cisco IronPort スパム隔離内のメッセージの配信

メッセージを配信のために解放するには、メッセージの隣にあるチェックボックスを選択して、[リリース（Release）] をクリックします。

ページに表示されているすべてのメッセージを選択するには、見出し行にあるチェックボックスをオンにします。

解放されたメッセージは、それ以降の電子メール パイプライン内の作業キューの処理をスキップして、宛先キューへ直接進みます。

Cisco IronPort スパム隔離からのメッセージの削除

Cisco IronPort スパム隔離では、指定された時間後にメッセージが自動で削除されるように設定できます。Cisco IronPort スパム隔離からメッセージを手動で削除することも可能です。

個別のメッセージを削除するには、削除するメッセージの横にあるチェックボックスをオンにして、[削除（Delete）] をクリックします。ページに表示されているすべてのメッセージを選択するには、見出し行にあるチェックボックスをオンにします。

Cisco IronPort スパム隔離内のすべてのメッセージを削除するには、[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [スパム隔離（Spam Quarantine）] ページから隔離をディセーブルにして、表示される [すべて削除（Delete All）] をクリックします。

CHAPTER 8

集約ポリシー、ウイルス、およびアウトブレイク隔離

集約隔離の概要

電子メール セキュリティ アプライアンス上の特定のフィルタ、ポリシー、およびスキャン操作により処理されたメッセージは、次の作業に備えて一時的に保管するために隔離内に置くことができます。シスコのコンテンツ セキュリティ管理アプライアンスの複数の電子メール セキュリティ アプライアンスからの隔離を集約できます。

集約隔離には次のような利点があります。

- 複数の電子メール セキュリティ アプライアンスから隔離されたメッセージを 1 箇所で管理できます。
- 隔離されたメッセージは、DMZ 内ではなくファイアウォールの背後に保存され、セキュリティ リスクを減らします。
- セキュリティ管理アプライアンスの標準のバック アップ機能の一部として、集約隔離はバックアップできます。

次の 2 種類の隔離を集約できます。

- ポリシー、ウイルス、アウトブレイク隔離

  ウイルス対策スキャンおよびアウトブレイク フィルタのどちらにも専用の隔離があります。メッセージ フィルタリング、コンテンツ フィルタリング、およびデータ漏洩防止ポリシーで検出されたメッセージを保持するためのポリシー隔離を作成します。

- スパム隔離

  第 7 章「Cisco IronPort スパム隔離の管理」を参照してください。

追加情報については、電子メール セキュリティ アプライアンスのマニュアルの「Quarantines」の章を参照してください。

隔離の種類

隔離領域タイプ	隔離名	デフォルトではシステムで作成されるか	説明	詳細情報
ウイルス	ウイルス	Yes	ウイルス対策エンジンによって判定されたため、マルウェアを送信する可能性のあるメッセージを保留します。	• 「ポリシー、ウイルス、およびアウトブレイク隔離の管理」（P.8-9） • 「ポリシー、ウイルス、アウトブレイク隔離内のメッセージの操作方法」（P.8-17）
アウトブレイク	アウトブレイク	Yes	スパムまたはマルウェアの可能性があるためアウトブレイク フィルタによって検出されたメッセージを保留します。	
ポリシー	ポリシー	Yes	メッセージ フィルタ、コンテンツ フィルタ、および DLP メッセージ アクションによって検出されたメッセージを保留します。 デフォルトのポリシー隔離が作成されています。	
	未分類	Yes	メッセージ フィルタ、コンテンツ フィルタ、または DLP メッセージ アクションで指定された隔離が削除されている場合のみメッセージを保留します。 この隔離はどのフィルタまたはメッセージ アクションにも割り当てることはできません。	
	（自分で作成したポリシー隔離）	No	メッセージ フィルタ、コンテンツ フィルタ、および DLP メッセージ アクションで使用するために作成するポリシー隔離。	
スパム	スパム	Yes	メッセージの受信者または管理者がレビューするためにスパム メッセージまたはサスペクト スパム メッセージを保留します。	第 7 章「Cisco IronPort スパム隔離の管理」

ポリシー、ウイルス、およびアウトブレイク隔離の集約

	手順	詳細情報
ステップ 1	ご使用の電子メール セキュリティ アプライアンスが DMZ 内にあり、セキュリティ管理アプライアンスがファイアウォールの背後にある場合は、アプライアンスが集約ポリシー、ウイルス、およびアウトブレイク隔離データを交換できるようにファイアウォール内のポートを開きます。	付録 C「ファイアウォール情報」
ステップ 2	セキュリティ管理アプライアンスで、この機能を有効にします。	「セキュリティ管理アプライアンスでの集約ポリシー、ウイルス、およびアウトブレイク隔離のイネーブル化」（P.8-4）
ステップ 3	セキュリティ管理アプライアンスで、非スパム隔離用ディスク領域を割り当てます。	「ディスク使用量の管理」（P.14-56）
ステップ 4	（オプション） • 必要な設定でセキュリティ管理アプライアンスに集約ポリシー隔離を作成します。 • 集約ウイルスおよびアウトブレイク隔離を設定します。 移行の前にこれらの設定を設定する場合、ご使用の電子メール セキュリティ アプライアンスの既存設定を参照できます。 カスタム移行の設定中に必要な隔離を作成することも、または自動移行の際に隔離が作成されるようにすることもできます。移行中に作成されたすべての隔離はデフォルト設定です。 ローカルの隔離の設定は隔離名が同じでも集約隔離では保持されません。	「ポリシー隔離の作成」（P.8-12）
ステップ 5	セキュリティ管理アプライアンスで、管理する電子メール セキュリティ アプライアンスを追加するか、追加済みアプライアンスの集約管理サービスから [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus and Outbreak Quarantines）] オプションを選択します。 ご使用の電子メール セキュリティ アプライアンスがクラスタ化されている場合、特定のレベル（マシン、グループ、またはクラスタ）に属するすべてのアプライアンスは、そのクラスタ内の任意の電子メール セキュリティ アプライアンスで集約された [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus and Outbreak Quarantines）] を有効にする前にセキュリティ管理アプライアンスに追加する必要があります。	「管理対象の各電子メールセキュリティ アプライアンスへの集約ポリシー、ウイルス、アウトブレイク隔離サービスの追加」（P.8-5）
ステップ 6	変更を保存します。	—
ステップ 7	セキュリティ管理アプライアンスで、電子メール セキュリティ アプライアンスから既存のポリシー隔離の移行を設定します。	「ポリシー、ウイルス、アウトブレイク隔離の移行の設定」（P.8-6）

	手順	詳細情報
ステップ 8	電子メール セキュリティ アプライアンスで、集約ポリシー、ウイルス、およびアウトブレイク隔離機能を有効にします。 **重要**： 電子メール セキュリティ アプライアンスでポリシー、ウイルス、およびアウトブレイク隔離を設定済みの場合、隔離およびすべてのメッセージの移行はこの変更を確定するとすぐに開始します。	お使いの電子メール セキュリティ アプライアンスのマニュアルの「Centralizing Services on a Cisco Content セキュリティ管理アプライアンス」の章の、特に次の項を参照してください。 • 「About Migration of Policy, Virus, and Outbreak Quarantines」 • 「Centralizing Policy, Virus, and Outbreak Quarantines」
ステップ 9	追加の電子メール セキュリティ アプライアンスを移行します。 一度に 1 つの移行プロセスだけしか処理できない可能性があります。前の移行が完了する前に、別の電子メール セキュリティ アプライアンスの集約ポリシー、ウイルス、およびアウトブレイク隔離を有効にしないでください。	—
ステップ 10	必要に応じて集約隔離設定を編集します。 移行中に作成された隔離は、集約および内部隔離名が同じでも元の内部隔離での設定ではなくデフォルト設定で作成されます。	「ポリシー隔離の作成」（P.8-12）
ステップ 11	メッセージ フィルタ、コンテンツ フィルタ、および DLP メッセージ アクションが集約隔離の名前で自動的に更新できない場合、お使いの電子メール セキュリティ アプライアンスのこれらの設定を手動で更新します。 クラスタ設定では、フィルタおよびメッセージ アクションがそのレベルで定義されている場合に限り、フィルタおよびメッセージ アクションは特定のレベルで自動的に更新できます。	お使いの電子メール セキュリティ アプライアンスのオンライン ヘルプまたはユーザ ガイドのメッセージ フィルタ、コンテンツ フィルタ、および DLP メッセージ アクションのついてのマニュアルを参照してください。
ステップ 12	（推奨）元のアプライアンスが使用できない場合、リリースされたメッセージを処理するために電子メール セキュリティ アプライアンスを指定します。	「リリースされたメッセージを処理する代替アプライアンスの指定」（P.8-8）
ステップ 13	カスタム ユーザ ロールに管理を委任する場合、特定の方法でアクセスを設定する必要があります。	「カスタム ユーザ ロールの集約隔離アクセスの設定」（P.8-8）

セキュリティ管理アプライアンスでの集約ポリシー、ウイルス、およびアウトブレイク隔離のイネーブル化

はじめる前に

「ポリシー、ウイルス、およびアウトブレイク隔離の集約」（P.8-3）の表に記載されたこの手順の前までの手順をすべて完了してください。

手順

ステップ 1　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] を選択します。

ステップ 2　[有効（Enable）] をクリックします。

ステップ 3　電子メール セキュリティ アプライアンスと通信するためインターフェイスとポートを次のように指定します。

- これらを変更する理由がない限り、デフォルトの選択を受け入れます。
- 電子メール 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と同じネットワークに存在しない場合、管理インターフェイスを使用する必要があります。
- ファイアウォールで開いたポートと同じポートを使用します。

ステップ 4　[送信（Submit）] をクリックします。

次の作業

「ポリシー、ウイルス、およびアウトブレイク隔離の集約」（P.8-3）内の表の次のステップに戻ります。

管理対象の各電子メール セキュリティ アプライアンスへの集約ポリシー、ウイルス、アウトブレイク隔離サービスの追加

すべての電子メール セキュリティ アプライアンスのすべての隔離の統合ビューを表示するには、すべての隔離を集約する前にすべての電子メール セキュリティ アプライアンスを追加することを検討してください。

はじめる前に

「ポリシー、ウイルス、およびアウトブレイク隔離の集約」（P.8-3）の表に記載されたここまでのすべての手順を完了したことを確認します。

手順

ステップ 1　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [セキュリティ アプライアンス（Security Appliances）] を選択します。

ステップ 2　このページのリストに、すでに電子メール セキュリティ アプライアンスを追加している場合は、次の手順を実行します。

a.　電子メール セキュリティ アプライアンスの名前をクリックします。

b.　[ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] サービスを選択します。

ステップ 3　電子メール セキュリティ アプライアンスを追加していない場合は、次の手順を実行します。

a.　[メール アプライアンスの追加（Add Email Appliance）] をクリックします。

b.　[アプライアンス名（Appliance Name）] および [IP アドレス（IP Address）] テキスト フィールドに、追加しているアプライアンスの管理インターフェイスのアプライアンス名と IP アドレスを入力します。

（注）　[IP Address] テキスト フィールドに DNS 名を入力した場合でも、[送信（Submit）] をクリックすると、すぐに IP アドレスに解決されます。

c.　[ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] サービスはあらかじめ選択されています。

d. [接続の確立（Establish Connection）] をクリックします。

e. 管理対象となるアプライアンスの管理者アカウントのユーザ名とパスワードを入力し、[接続の確立（Establish Connection）] をクリックします。

（注）　ログイン資格情報を入力すると、セキュリティ管理アプライアンスからリモート アプライアンスへのファイル転送のための公開 SSH キーが渡されます。ログイン資格情報は、セキュリティ管理アプライアンスには保存されません。

f. [成功（Success）] メッセージがページのテーブルの上に表示されるまで待機します。

ステップ 4　[送信（Submit）] をクリックします。

ステップ 5　[ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] を有効にする各電子メール セキュリティ アプライアンスに対してこの手順を繰り返して行ってください。

たとえば、クラスタ内の他のアプライアンスを追加します。

ステップ 6　変更を保存します。

次の作業

「ポリシー、ウイルス、およびアウトブレイク隔離の集約」（P.8-3）内の表の次のステップに戻ります。

ポリシー、ウイルス、アウトブレイク隔離の移行の設定

はじめる前に

- 「ポリシー、ウイルス、およびアウトブレイク隔離の集約」（P.8-3）の表に記載されたここまでのすべての手順を完了したことを確認します。
- 移行プロセスに関する警告や情報については、お使いの電子メール セキュリティ アプライアンスのマニュアルの「Centralizing Services on a Cisco Content セキュリティ管理アプライアンス」の章の「About Migration of Policy, Virus, and Outbreak Quarantines」の項を参照してください。

手順

ステップ 1　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] を選択します。

ステップ 2　[移行ウィザードの起動（Launch Migration Wizard）] をクリックします。

ステップ 3　移行方法を選択します。

条件	選択	その他の情報
• すべての関連する電子メール セキュリティ アプライアンスからのすべての既存ポリシー隔離を移行する場合、 および • 同じ名前のポリシー隔離をすべての電子メール セキュリティ アプライアンス上で同一の設定にする場合、 および • すべての電子メール セキュリティ アプライアンス上で同じ名前を持つすべてのポリシー隔離をこの名前を持つ単一の集約ポリシー隔離にマージする場合	自動（Automatic）	このプロセスを使用して作成されたすべての集約ポリシー隔離は、電子メール セキュリティ アプライアンスの同じ名前の隔離の設定に関係なく、デフォルト設定で自動的に設定されます。 移行後にこれらの設定を更新する必要があります。
• 同じ名前のポリシー隔離が別の電子メール セキュリティ アプライアンス上で異なる設定になっていてこの違いを維持する場合、 または • 内部隔離の一部を移行し、他のすべてを削除する場合、 または • 内部隔離を異なった名前の集約隔離に移行する場合 または • 単一の集約隔離に異なる名前の内部隔離をマージする場合	カスタム（Custom）	移行前ではなく移行中に作成するすべての集約ポリシー隔離は新しい隔離に対するデフォルト設定で設定されます。 移行後にこれらの設定を更新する必要があります。

ステップ 4　[次へ（Next）] をクリックします。

ステップ 5　[自動（Automatic）] を選択した場合、次の手順に従います。

移行するポリシー隔離および必要なこのページの他の情報を確認します。

ウイルスおよびアウトブレイク隔離も移行されます。

ステップ 6　[カスタム（Custom）] を選択した場合、次の手順に従います。

- すべての電子メール セキュリティ アプライアンスからの隔離を表示するか、または 1 つだけからの隔離を表示するかを選択するには、[隔離の表示元（Show Quarantines from）] リストから選択肢を選択します。
- 各集約ポリシー隔離に移動する内部ポリシー隔離を選択します。
- 必要に応じて追加の集約ポリシー隔離を作成します。これらはデフォルト設定になります。
- 隔離名は大文字と小文字が区別されます。
- 左のテーブルに残っている隔離は移行されず、移行時に電子メール セキュリティ アプライアンスから削除されます。
- 右のテーブルから隔離を選択し [集約隔離から削除（Remove from Centralized Quarantine）] をクリックして隔離のマッピングを変更できます。

ステップ 7　必要に応じて [次へ（Next）] をクリックします。

ステップ 8　変更を送信し、保存します。

次の作業

「ポリシー、ウイルス、およびアウトブレイク隔離の集約」（P.8-3）内の表の次のステップに戻ります。

リリースされたメッセージを処理する代替アプライアンスの指定

通常、メッセージが集約隔離からリリースされるとき、セキュリティ管理アプライアンスは最初にそのメッセージを集約隔離に送信した電子メール セキュリティ アプライアンスで処理するためにこれを返します。

メッセージの発信元の電子メール セキュリティ アプライアンスが利用可能でない場合、リリースされたメッセージを別の電子メール セキュリティ アプライアンスで処理し配信できます。この目的のアプライアンスを指定します。

はじめる前に

- リリースされたメッセージを代替アプライアンスで処理して配信できそうか確認します。たとえば、暗号化とアンチウイルス再スキャンの設定は、プライマリ アプライアンスの同じ設定と一致する必要があります。
- 代替アプライアンスは、集約ポリシー、ウイルス、およびアウトブレイク隔離に完全に設定する必要があります。そのアプライアンスに関して「ポリシー、ウイルス、およびアウトブレイク隔離の集約」（P.8-3）の表の手順を実行します。

手順

ステップ 1　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [セキュリティ アプライアンス（Security Appliances）] を選択します。

ステップ 2　[代替リリース アプライアンスの指定（Specify Alternate Release Appliance）] ボタンをクリックします。

ステップ 3　電子メール セキュリティ アプライアンスを選択します。

ステップ 4　変更を送信し、保存します。

関連項目

- 「電子メール セキュリティ アプライアンスが使用できないときのメッセージのリリース」（P.8-9）

カスタム ユーザ ロールの集約隔離アクセスの設定

カスタム ユーザ ロールを持つ管理者が電子メール セキュリティ アプライアンス上のメッセージおよびコンテンツ フィルタ内および DLP メッセージ アクション内で集約ポリシー隔離を指定できるようにするためには、セキュリティ管理アプライアンスの関連ポリシー隔離へのこれらのユーザ アクセスを許可し、セキュリティ管理アプライアンスに作成するカスタム ユーザ ロール名が電子メール セキュリティ アプライアンス上のものと一致する必要があります。

関連項目

- 「Custom Email User ロールの作成」（P.13-7）

集約ポリシー、ウイルス、およびアウトブレイク隔離のディセーブル化

通常、これらの集約隔離を無効にする必要がある場合は電子メール セキュリティ アプライアンスでそれを行う必要があります。

それを行った場合の影響のリストなど、集約ポリシー、ウイルス、アウトブレイク隔離の無効化の詳細については、お使いの電子メール セキュリティ アプライアンスのオンライン ヘルプまたはマニュアルを参照してください。

電子メール セキュリティ アプライアンスが使用できないときのメッセージのリリース

通常、メッセージが集約隔離からリリースされるとき、セキュリティ管理アプライアンスは最初にそのメッセージを集約隔離に送信した電子メール セキュリティ アプライアンスで処理するためにこれを返します。

メッセージの発信元の電子メール セキュリティ アプライアンスが利用可能でない場合、リリースされたメッセージを別の電子メール セキュリティ アプライアンスで処理し配信できます。この目的で、代替リリース アプライアンスを指定する必要があります。

代替アプライアンスが使用できない場合、代替リリース アプライアンスとして別の電子メール セキュリティ アプライアンスを指定できそのアプライアンスがキューに入っているメッセージを処理して配信します。

電子メール セキュリティ アプライアンスへの到達に繰り返し失敗した後に、アラートを受け取ります。

関連項目

- 「リリースされたメッセージを処理する代替アプライアンスの指定」（P.8-8）

ポリシー、ウイルス、およびアウトブレイク隔離の管理

- 「ポリシー、ウイルス、およびアウトブレイク隔離に対するディスク領域の割り当て」（P.8-10）
- 「隔離内のメッセージの保留時間」（P.8-10）
- 「自動的に処理される隔離メッセージのデフォルト アクション」（P.8-11）
- 「システム作成隔離の設定の確認」（P.8-12）
- 「ポリシー隔離の作成」（P.8-12）
- 「ポリシー、ウイルス、アウトブレイク隔離の設定の編集」（P.8-13）
- 「隔離を割り当てるフィルタおよびメッセージ アクションの決定」（P.8-14）
- 「ポリシー隔離の削除について」（P.8-14）
- 「隔離状態、容量、およびアクティビティのモニタリング」（P.8-15）
- 「隔離用のディスク容量の使用率に関するアラート」（P.8-16）
- 「ポリシー隔離とロギング」（P.8-16）

- 「メッセージ処理タスクの他のユーザへの配信について」（P.8-16）

ポリシー、ウイルス、およびアウトブレイク隔離に対するディスク領域の割り当て

ディスク領域の割り当てについては、「ディスク使用量の管理」（P.14-56）を参照してください。

複数の隔離内のメッセージは、単一の隔離内のメッセージと同じ容量のディスク領域を消費します。

アウトブレイク フィルタと集約隔離の両方が有効な場合、以下のようになります。

- 内部ポリシー、ウイルス、アウトブレイク隔離に割り当てられた電子メール セキュリティ アプライアンスのすべてのディスク領域が、アウトブレイク ルールが更新されるたびにこれらのメッセージをスキャンするために、アウトブレイク隔離内のメッセージのコピーを保留するために代わって使用されます。
- セキュリティ管理アプライアンス上のディスク領域は、電子メール セキュリティ アプライアンスの使用可能なディスク領域の容量によって制限される可能性があります。
- この状況の詳細については、「隔離内のメッセージの保留時間」（P.8-10）を参照してください。

関連項目

- 「隔離状態、容量、およびアクティビティのモニタリング」（P.8-15）
- 「隔離用のディスク容量の使用率に関するアラート」（P.8-16）
- 「隔離内のメッセージの保留時間」（P.8-10）

隔離内のメッセージの保留時間

メッセージは次の状況で隔離から自動的に削除されます。

- 通常の有効期限切れ：保留時間は、隔離内のメッセージに一致します。隔離ごとにメッセージの保留時間を指定します。各メッセージには、それぞれ独自の有効期限があり、リストに表示されます。このトピックで説明する別の状況が発生しなければ、メッセージは指定された時間だけ保留されます。

  （注）　アウトブレイク フィルタ内のメッセージの通常の保留時間は、アウトブレイク隔離内ではなく、電子メール ポリシーの [アウトブレイク フィルタ（Outbreak Filters）] セクションで設定されます。

- 早期の有効期限切れ：メッセージは設定されている保留時間に到達する前に隔離から強制的に削除されます。これは次の場合に発生する可能性があります。
  - 「ポリシー、ウイルス、およびアウトブレイク隔離に対するディスク領域の割り当て」（P.8-10）に定義されているすべての隔離のサイズ制限に達した。

    サイズ制限に達すると、隔離に関係なく、最も古いメッセージが処理されメッセージごとのデフォルト アクションが、すべての隔離のサイズが再度サイズ制限未満になるまで実行されます。このポリシーは、First In First Out（FIFO; 先入れ先出し）です。最新の有効期限に基づいて複数の隔離内のメッセージが期限切れになります。

（任意）ディスク領域が十分でないために個々の隔離がリリースまたは削除から除外されるように設定することができます。すべての隔離が除外されディスク領域が容量に達するように設定すると、セキュリティ管理アプライアンスで領域が利用可能になるまで、メッセージが電子メール セキュリティ アプライアンスに保留されます。

セキュリティ管理アプライアンスはメッセージをスキャンしないため、集約アウトブレイク隔離内の各メッセージのコピーは、最初にメッセージを処理した電子メール セキュリティ アプライアンスに保存されます。これによって電子メール セキュリティ アプライアンスはアウトブレイク フィルタ ルールが更新されるたびに隔離されているメッセージを再スキャンし、もう脅威とは見なされないメッセージをセキュリティ管理アプライアンスに伝えることができます。アウトブレイク隔離の両方のコピーは同時にメッセージの同じセットを保持する必要があります。したがって、電子メール セキュリティ アプライアンスのディスク領域に空きがなくなるというまれな状況では、両方のアプライアンスのアウトブレイク隔離内のメッセージのコピーは集約隔離にまだ領域がある場合でも、早く期限切れとなります。

ディスク領域のマイルストーンについてアラートを受け取ります。「隔離用のディスク容量の使用率に関するアラート」（P.8-16）を参照してください。

- まだメッセージを保留している隔離を削除する。

メッセージが隔離から自動的に削除される場合、そのメッセージでのデフォルト アクションが実行されます。「自動的に処理される隔離メッセージのデフォルト アクション」（P.8-11）を参照してください。

保留時間の時間調整の影響

- 夏時間とアプライアンスの時間帯の変更は保留時間に影響しません。
- 隔離の保留時間を変更すると、新しいメッセージだけが新しい有効期限を持ちます。
- システム クロックを変更すると、過去に終了しているはずのメッセージが次の最も適切な時間に期限切れになります。
- システム クロックの変更は期限切れになる処理中のメッセージには適用されません。

自動的に処理される隔離メッセージのデフォルト アクション

「隔離内のメッセージの保留時間」（P.8-10）で説明された状況のどれかが発生するとポリシー、ウイルス、アウトブレイク隔離内のメッセージでデフォルト アクションが実行されます。

以下の 2 つのプライマリ デフォルト アクションがあります。

- 削除：メッセージが削除されます。
- リリース：メッセージは配信するためにリリースされます。

  リリースの際に、メッセージはウイルス対策またはスパム対策エンジンによって再スキャンされる場合があります。詳細については、「隔離されたメッセージの再スキャンについて」（P.8-23）を参照してください。

  さらに、予定の保留時間が過ぎる前にリリースされたメッセージは、X ヘッダーの追加など、その他の操作を行うことができます。詳細については、「ポリシー隔離の作成」（P.8-12）を参照してください。

  集約隔離からリリースされたメッセージは、処理のために発生元の電子メール セキュリティ アプライアンスに返されます。

システム作成隔離の設定の確認

隔離を使用する前に、分類されていない隔離も含めデフォルト隔離の設定をカスタマイズします。

ポリシー隔離の作成

はじめる前に

- 保留時間およびデフォルト アクションを含め、隔離内のメッセージが自動的に管理される方法を理解します。「隔離内のメッセージの保留時間」（P.8-10）および「自動的に処理される隔離メッセージのデフォルト アクション」（P.8-11）を参照してください。
- 各隔離にアクセスするユーザを決定し、ユーザおよびカスタム ユーザ ロールを適宜作成します。詳細は、「隔離にアクセスできるユーザ グループ」（P.8-17）を参照してください。

手順

ステップ 1　[メール（Email）] > [メッセージの隔離（Message Quarantine）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] を選択します。

ステップ 2　[ポリシー隔離を追加（Add Policy Quarantine）] をクリックします

ステップ 3　情報を入力します。

次の点を考慮してください。

- 隔離の名前は変更できません。
- 指定した保留期間の終了前にこの隔離内のメッセージを処理 *しない* ようにする場合は、隔離ディスク領域に空き領域がなくても、[容量オーバーフロー時にメッセージにデフォルトのアクションを適用して容量を解放します（Free up space by applying default action on messages upon space overflow）] を無効にします。

  すべての隔離でこのオプションを選択しないでください。少なくとも 1 つの隔離からメッセージを削除して、空き領域を作る必要があります。
- デフォルト アクションとして [リリース（Release）] を選択すると、保留期間が経過する前にリリースされるメッセージに適用される追加アクションを指定できます。

オプション	情報
件名の変更（Modify Subject）	テキストを入力し、元のメッセージの件名の先頭または末尾にそれを追加するかどうかを指定します。 たとえば、メッセージが不適切なコンテンツを含むかもしれないことを受信者に警告する場合があります。 **（注）**　非 ASCII 文字を含む件名を正しく表示するために、件名は RFC 2047 に従って表記されている必要があります。

オプション	情報
X-Header を追加（Add X-Header）	[X-Header を追加（Add X-Header）] では、メッセージの措置の記録を提供できます。これは、たとえば特定のメッセージが配信された理由に関する照会に対処するときなどに役に立ちます。 名前と値を入力します。 例： 名前 =「`Inappropriate-release-early `」 値 =「`True `」
添付ファイルを除去（Strip Attachments）	添付ファイルを除去することで、このようなファイルに内包する可能性のあるウイルスから保護します。

ステップ 4　この隔離にアクセスできる次のユーザを指定します。

ユーザ	情報
ローカルユーザ（Local Users）	ローカル ユーザ リストには隔離にアクセスできるロールを持つユーザだけが含まれます。 すべての管理者は隔離に自由にアクセスできるため、このリストでは管理権限を持つユーザを除外します。
外部認証されたユーザ（Externally Authenticated Users）	外部認証を設定する必要があります。
カスタム ユーザ ロール（Custom User Roles）	隔離へのアクセス権を持つカスタム ユーザ ロールを少なくとも 1 つ作成した場合にのみ、このオプションが表示されます。

ステップ 5　変更を送信し、保存します。

次の作業

- まだ電子メール セキュリティ アプライアンスから隔離を移行していない場合、次の手順に従います。

  移行処理の一部としてこれらの隔離をメッセージ フィルタやコンテンツ フィルタおよび DLP メッセージ アクションに割り当てます。

- すでに集約隔離に移行した場合は、次の手順に従います。

  お使いの電子メール セキュリティ アプライアンスに隔離にメッセージを移動するメッセージ フィルタやコンテンツ フィルタおよび DLP メッセージ アクションがあることを確認します。電子メール セキュリティ アプライアンスのユーザ ガイドまたはオンライン ヘルプを参照してください。

ポリシー、ウイルス、アウトブレイク隔離の設定の編集

（注）
- 隔離の名前は変更できません。

- 「保留時間の時間調整の影響」（P.8-11）も参照してください。

隔離の設定を変更するには、[メール（Email）] > [メッセージの隔離（Message Quarantine）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] を選択し、隔離の名前をクリックします。

隔離を割り当てるフィルタおよびメッセージ アクションの決定

隔離に関連付けられたメッセージ フィルタ、コンテンツ フィルタ、DLP メッセージ アクション、およびそれぞれが設定されている電子メール セキュリティ アプライアンスを表示できます。

手順

ステップ 1　[メール（Email）] > [メッセージの隔離（Message Quarantine）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] をクリックします。

ステップ 2　検査するポリシー隔離の名前をクリックします。

ステップ 3　ページの下部にスクロールして [関連付けられたメッセージ フィルタ / コンテンツ フィルタ /DLP メッセージ アクション（Associated Message Filters/Content Filters/DLP Message Actions）] を表示します。

ポリシー隔離の削除について

- ポリシー隔離を削除する前に、実行中のフィルタまたはメッセージ アクションと関連付けられているかどうかを確認します。「隔離を割り当てるフィルタおよびメッセージ アクションの決定」（P.8-14）を参照してください。
- フィルタまたはメッセージ アクションに割り当てられている場合でも、ポリシー隔離を削除できます。
- 空でない隔離を削除する場合、ディスクに空き領域がない場合にメッセージを削除しないというオプションを選択しても、隔離で定義されたデフォルト アクションがすべてのメッセージに適用されます。「自動的に処理される隔離メッセージのデフォルト アクション」（P.8-11）を参照してください。
- フィルタまたはメッセージ アクションと関連付けられた隔離を削除した後、このフィルタまたはメッセージ アクションにより引き続き隔離されたメッセージはすべて未分類隔離に送信されます。隔離を削除する前に、未分類隔離のデフォルト設定をカスタマイズする必要があります。
- 未分類隔離は削除できません。

隔離状態、容量、およびアクティビティのモニタリング

内容	手順
すべての非スパム隔離に割り当てられている領域の合計	[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] を選択し、ページの最初のセクションで確認します。 割り当てを変更するには、「ディスク使用量の管理」（P.14-56）を参照してください。
すべての非スパム隔離で現在使用できる領域	[メール（Email）] > [メッセージの隔離（Message Quarantine）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] を選択し、テーブルのすぐ下で確認します。
すべての隔離で現在使用中の合計容量	[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [システム ステータス（System Status）] を選択します。
各隔離で現在使用中の容量	[メール（Email）] > [メッセージの隔離（Message Quarantine）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] を選択し、隔離名をクリックして、テーブルの隔離名のすぐ下にある行でこの情報を確認します
すべての隔離内の現在のメッセージの総数	[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [システム ステータス（System Status）] を選択します。
各隔離内にある現在のメッセージ数	[メール（Email）] > [メッセージの隔離（Message Quarantine）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] を選択し、テーブルのその隔離の行を確認します。
すべての隔離による総 CPU 使用率	[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [システム ステータス（System Status）] を選択して [システム情報（System Information）] セクションで確認します。
最後のメッセージが各隔離に送信された日時（隔離間の移動を除く）	[メール（Email）] > [メッセージの隔離（Message Quarantine）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] を選択し、テーブルのその隔離の行を確認します。
ポリシー隔離が作成された日付 ポリシー隔離の作成者の名前	[メール（Email）] > [メッセージの隔離（Message Quarantine）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] を選択し、隔離名をクリックして、テーブルの隔離名のすぐ下にある行でこの情報を確認します 作成日および作成者の名前はシステムが作成した隔離では使用されません。
隔離に関連付けられたフィルタおよびメッセージ アクション	「隔離を割り当てるフィルタおよびメッセージ アクションの決定」（P.8-14）を参照してください。

隔離用のディスク容量の使用率に関するアラート

ポリシー、ウイルス、アウトブレイク隔離の合計サイズが容量の 75 パーセント、85 パーセント、95 パーセントに達するか超えると常にアラートが送信されます。このチェックは、メッセージが隔離エリアに入れられたときに実行されます。たとえば、隔離へのメッセージの追加でサイズが増加し総容量の 75 % になるかまたは超えると、アラートが送信されます。

アラートの詳細については、「アラートの管理」（P.14-33）を参照してください。

ポリシー隔離とロギング

AsyncOS により、隔離されるすべてのメッセージが個別にロギングされます。

```
Info: MID 482 quarantined to "Policy" (message filter:policy_violation)
```

括弧内には、メッセージを隔離させたメッセージ フィルタまたは Outbreak フィルタ機能のルールが出力されます。メッセージが入れられる隔離ごとに独立したログ エントリが生成されます。

また、AsyncOS により、隔離エリアから除去されるメッセージも個別にロギングされます。

```
Info: MID 483 released from quarantine "Policy" (queue full)
```

```
Info: MID 484 deleted from quarantine "Anti-Virus" (expired)
```

メッセージがすべての隔離から除去され、完全に削除されるか、配信用にスケジュールされると、それらのメッセージはシステムによって次のように個別にロギングされます。

```
Info: MID 483 released from all quarantines
```

```
Info: MID 484 deleted from all quarantines
```

メッセージが再注入されると、新しいメッセージ ID（MID）を持つ新しいメッセージ オブジェクトが作成されます。このことは、次のように「署名入り」の新しい MID を伴う既存のログ メッセージを使用してロギングされます。

```
Info: MID 483 rewritten to 513 by Policy Quarantine
```

メッセージ処理タスクの他のユーザへの配信について

メッセージのレビューおよび処理のタスクを他の管理者ユーザへ配信できます。次に例を示します。

- 人事部門はポリシー隔離をレビューし管理できます。
- 法務部門は社外秘マテリアル隔離を管理できます。

隔離の設定を指定するときに、これらのユーザにアクセス権限を割り当てます。隔離にユーザを追加するには、追加するユーザがすでに存在している必要があります。

各ユーザは、すべてまたは一部の隔離にアクセスできるようにすることも、まったくアクセスできないようにすることもできます。隔離の閲覧を許可されていないユーザに対しては、GUI または CLI の隔離のリスト表示のどこにも、その隔離の存在を示す証拠は一切表示されません。

関連項目

- 「隔離にアクセスできるユーザ グループ」（P.8-17）
- 第 13 章「管理タスクの分散」

隔離にアクセスできるユーザ グループ

ユーザが隔離にアクセスできるようにするときは、実行できるアクションは、次のユーザ グループごとに異なります。

- 管理者または電子メール管理者グループのユーザは、隔離の作成、設定、削除、および集約ができ、隔離メッセージを管理できます。
- オペレータ、ゲスト、読み込み専用オペレータ、およびヘルプ デスクのユーザ グループは、隔離管理権限を持つカスタム ユーザ ロール同様、隔離内のメッセージの検索、表示、および処理ができますが、隔離の設定を変更したり、隔離を作成、削除、または集約することはできません。それぞれの隔離にこれらのどのユーザがその隔離にアクセスするのかを指定します。
- Technicians グループに属するユーザは隔離にアクセスできません。

メッセージ トラッキングおよびデータ漏洩防止などの関連機能のアクセス権限も、[隔離（Quarantine）] ページに表示されるオプションおよび情報に影響します。たとえば、ユーザにメッセージ トラッキングへのアクセス権限がない場合、そのユーザは隔離されたメッセージに関するメッセージ トラッキング情報を確認できません。

（注）　セキュリティ管理アプライアンスに設定されたカスタム ユーザ ロールがフィルタおよび DLP メッセージ アクションのポリシー隔離を指定できるようにするには、「カスタム ユーザ ロールの集約隔離アクセスの設定」（P.8-8）を参照してください。

ポリシー、ウイルス、アウトブレイク隔離内のメッセージの操作方法

隔離内のメッセージの表示

目的	手順
隔離内のすべてのメッセージの表示	[メール（Email）] > [メッセージの隔離（Message Quarantine）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] を選択します。 関連する隔離の行で、表の [メッセージ（Messages）] 列の青い番号をクリックします。
アウトブレイク隔離内のメッセージの表示	• [メール（Email）] > [メッセージの隔離（Message Quarantine）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] を選択します。 関連する隔離の行で、表の [メッセージ（Messages）] 列の青い番号をクリックします。 • 「[ルール サマリで管理（Manage by Rule Summary）] リンク」（P.8-24）を参照してください。
隔離内のメッセージのリストのナビゲート	[前へ（Previous）]、[次へ（Next）]、ページ番号、または二重矢印のリンクをクリックします。二重矢印を使用すると、リストの先頭（[<<]）または最後（[>>]）のページに移動します。
隔離内のメッセージのリストのソート	列見出しをクリックします（複数の項目が含まれる可能性のある列または [その他の隔離（In other quarantines）] 列を除く）。
表の列のサイズ変更	列見出し間のディバイダをドラッグします。
メッセージが隔離された原因のコンテンツの表示	「一致した内容の表示」（P.8-22）を参照してください。

隔離されたメッセージおよび国際文字セット

メッセージの件名に国際文字セット（2 バイト、可変長、および非 ASCII の符号化）の文字が含まれる場合、[ポリシー隔離（Policy Quarantine）] ページでは、非 ASCII 文字の件名行が復号化された形式で表示されます。

ポリシー、ウイルス、アウトブレイク隔離内メッセージの検索

（注）
- ポリシー、ウイルス、アウトブレイク隔離内の検索では、スパム隔離内のメッセージは見つかりません。
- ユーザは、ユーザがアクセスできる隔離内のメッセージだけを探して確認することができます。

手順

ステップ 1　[メール（Email）] > [メッセージの隔離（Message Quarantine）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] を選択します。

ステップ 2　[複数の隔離を対象に検索（Search Across Quarantines）] ボタンをクリックします。

ヒント　アウトブレイク隔離では、アウトブレイク ルールによって隔離されたすべてのメッセージを検索することもできます。[アウトブレイク（Outbreak）] テーブル行の [ルール サマリで管理（Manage by Rule Summary）] リンクをクリックして、関連するルールをクリックします。

ステップ 3　検索を実施する隔離を選択します。

ステップ 4　（任意）他の検索条件を入力します。

- エンベロープ送信者およびエンベロープ受信者では、任意の文字を入力できます。入力の検証は実行されません。
- 検索結果には、指定した条件の *すべて* に一致するメッセージだけが含まれます。たとえば、エンベロープ受信者と件名を指定した場合は、エンベロープ受信者 *および* 件名両方で指定された条件に一致するメッセージだけが返されます。

次の作業

これらの検索結果は、隔離リストを使用するのと同様に使用できます。詳細については、「手動での隔離内のメッセージの処理」（P.8-19）を参照してください。

手動での隔離内のメッセージの処理

手動でメッセージを処理する場合は、[メッセージ アクション（Message Actions）] ページからメッセージのメッセージ アクションを手動で選択します。

（注）　RSA Enterprise Manager を使用する導入では、セキュリティ管理アプライアンス、または Enterprise Manager 上に隔離されたメッセージを表示できますが、メッセージでアクションを行うためには Enterprise Manager を使用する必要があります。Enterprise Manager の詳細については、電子メール セキュリティ アプライアンスのマニュアルの「Data Loss Prevention」の章を参照しください。

メッセージで次のアクションを行うことができます。

- 削除（Delete）
- リリース
- 隔離からの終了予定の遅延
- 指定した電子メール アドレスにメッセージのコピーを送信
- 1 つの隔離から別の隔離へのメッセージの移動

通常、次の作業を行うときに表示されるリスト内のメッセージ アクションを実施できます。ただし、すべての状況ですべてのアクションが使用可能なわけではありません。

- [メール（Email）] > [メッセージの隔離（Message Quarantine）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] ページの隔離のリストから、隔離内のメッセージ数をクリックします。
- [複数の隔離を対象に検索（Search Across Quarantines）] をクリックします。
- 隔離の名前をクリックし、隔離内を検索します。

次に、複数のメッセージで次の操作を同時に実行できます。

- メッセージ リストの先頭の選択リストからオプションを選択する。
- ページ上の各メッセージの横のチェックボックスを選択する。
- メッセージ リストの先頭の表見出し内のチェックボックスを選択する。これで画面に表示されているすべてのメッセージにアクションが適用されます。他のページのメッセージは影響を受けません。

アウトブレイク隔離内のメッセージに対しては追加のオプションが利用可能です。電子メール セキュリティ アプライアンスのオンライン ヘルプまたはユーザ ガイドの「Outbreak Filters」の章の [ルールサマリで管理（Manage by Rule Summary）] ビューについての情報を参照してください。

関連項目

- 「複数の隔離内のメッセージ」（P.8-21）
- 「自動的に処理される隔離メッセージのデフォルト アクション」（P.8-11）

メッセージのコピーの送信

メッセージのコピーは、管理者グループに属しているユーザだけが送信できます。

メッセージのコピーを送信するには、[コピーの送信先：（Send Copy To:）] フィールドに電子メール アドレスを入力し、[送信（Submit）] をクリックします。メッセージのコピーを送信しても、そのメッセージに対してその他のアクションが実行されることはありません。

ポリシー隔離間の移行メッセージについて

1 つのアプライアンス上で、1 つのポリシー隔離から別のポリシー隔離へ手動でメッセージを移動できます。

メッセージを別の隔離へ移動するには、次の手順に従ってください。

- 有効期限は変更されません。メッセージは、元の隔離の保留時間を維持します
- メッセージが隔離された原因は、コンテンツの一致やその他の関連する詳細も含め変更されません。
- メッセージが複数の隔離にあり、そのメッセージのコピーをすでに保留している宛先に移行する場合、メッセージの移動されるコピーの有効期限および隔離の原因が、宛先の隔離にもともとあるメッセージのコピーのそれらを上書きします。

複数の隔離内のメッセージ

メッセージが他の 1 つまたは複数の隔離内にある場合、隔離メッセージ リストの [その他の隔離（In other quarantines）] 列に、これらのほかの隔離にアクセスする許可があるかどうかに関係なく、[はい（Yes）] が表示されます。

複数の隔離内のメッセージ：

- 置かれていた隔離のすべてからメッセージがリリースされないかぎり配信されません。すべての隔離から削除されると、二度と配信できません。
- メッセージが置かれているすべての隔離から削除またはリリースされないかぎり、どの隔離からも削除されません。

メッセージをリリースしようとしているユーザがメッセージが置かれている隔離のすべてにアクセスできない可能性があるため、次のルールが適用されます。

- メッセージは、自身が存在するすべての隔離エリアから解放されるまで、どの隔離エリアからも解放されません。
- メッセージは、いずれかの隔離内で削除済みとマークされると、他の隔離からも配信できなくなります （ただし、リリースできます）。

したがって、メッセージが複数の隔離内にキューイングされ、ユーザがそのうちの 1 つまたは複数の隔離にアクセスできない場合は、次のことが起こります。

- ユーザは、ユーザがアクセスできる各隔離についてそのメッセージが存在するかどうか通知されます。
- GUI は、ユーザがアクセスできる隔離の保留期間の予定終了日時のみを表示します （同じメッセージに対して、隔離ごとに別々の終了日時が存在します）。
- ユーザは、そのメッセージを保管している他の隔離の名前を知らされません。
- ユーザは、ユーザがアクセス権限を持たない隔離にメッセージを置く原因となったコンテンツの一致を確認できません。
- メッセージのリリースは、ユーザがアクセスできるキューにだけ効果があります。
- ユーザがアクセスできない他の隔離にもメッセージがキューイングされている場合、残りの隔離にアクセスできるユーザによって処理されるまで（あるいは早期または通常の期限切れによって「正常に」リリースされるまで）、そのメッセージは変更されずに隔離内に残ります。

メッセージの詳細およびメッセージ コンテンツの表示

メッセージのコンテンツを表示したり、[隔離されたメッセージ（Quarantined Message）] ページにアクセスしたりするには、メッセージの件名行をクリックします。

[隔離されたメッセージ（Quarantined Message）] には、[隔離の詳細（Quarantine Details）] と [メッセージの詳細（Message Details）] の 2 つのセクションがあります。

[隔離されたメッセージ（Quarantined Message）] ページから、メッセージの読み取り、メッセージ アクションを選択したり、メッセージのコピーを送信したりできます。また、メッセージが隔離エリアから解放されるときに Encrypt on Delivery フィルタ アクションによって暗号化されるかどうかを確認することもできます。

[メッセージの詳細（Message Details）] セクションには、メッセージ本文、メッセージ ヘッダー、および添付ファイルが表示されます。メッセージ本文は最初の 100 KB だけが表示されます。メッセージがそれよりも長い場合は、最初の 100 KB が表示され、その後に省略記号（...）が続きます。実際のメッセージが切り捨てられることはありません。この処置は表示目的のためだけに行われます。[メッセージの詳細（Message Details）] の下部にある [メッセージ部分（Message Parts）] セクション内の

[message body] をクリックすることにより、メッセージ本文をダウンロードできます。また、添付ファイルのファイル名をクリックすることにより、メッセージの任意の添付ファイルをダウンロードすることもできます。

ウイルスの含まれるメッセージを表示する場合、ご使用のコンピュータにデスクトップ アンチウイルス ソフトウェアがインストールされていると、そのアンチウイルス ソフトウェアから、ウイルスが検出されたと警告される場合があります。これは、ご使用のコンピュータに対して脅威ではないため、無視しても問題ありません。

メッセージの詳細を表示するには、[メッセージ トラッキング（Message Tracking）] リンクをクリックします。

（注）　特別な Outbreak 隔離の場合、追加の機能を利用できます。「アウトブレイク隔離」（P.8-24）を参照してください。

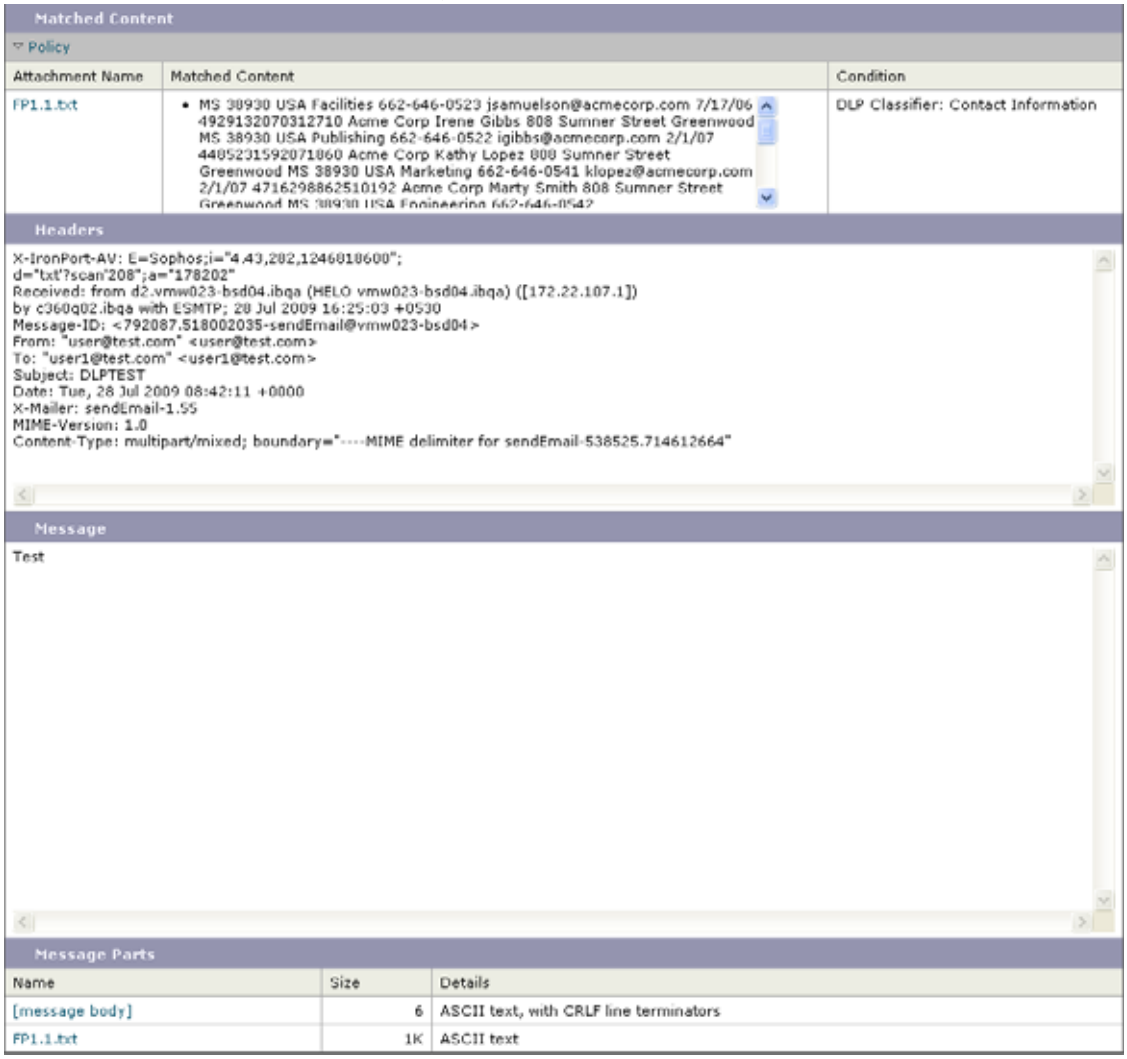
一致した内容の表示

Attachment Content 条件、Message Body または Attachment 条件、Message 本文条件、または Attachment 内容条件と一致するメッセージに対して隔離アクションを設定した場合、隔離されたメッセージ内の一致した内容を表示できます。メッセージ本文を表示する場合、DLP ポリシー違反の一致を除き、一致した内容が黄色で強調表示されます。また、$MatchedContent アクション変数を使用して、メッセージの一致した内容やコンテンツ フィルタの一致をメッセージの件名に含めることもできます。

一致した内容が添付ファイルに含まれる場合は、その判定結果が DLP ポリシー違反、コンテンツ フィルタ条件、メッセージ フィルタ条件、または画像解析のいずれによるものかに関係なく、添付ファイルの内容がその隔離理由とともに表示されます。

メッセージ フィルタまたはコンテンツ フィルタのルールをトリガーしたローカル隔離内のメッセージを表示すると、フィルタ アクションを実際にはトリガーしなかった内容が（フィルタ アクションをトリガーした内容とともに）GUI で表示されることがあります。GUI 表示は、内容の一致箇所を特定する際のガイドラインとして使用されますが、内容の一致リストを正確に反映しているとは限りません。これは、GUI で使用される内容一致ロジックが、フィルタで使用されるものほど厳密ではないため起こります。この問題は、メッセージ本文内での強調表示に対してのみ当てはまります。メッセージの各パート内の一致文字列をそれに対応するフィルタ ルールとともに一覧表示する表は正しく表示されます。

図 8-1　ポリシー隔離エリア内で表示された一致内容



添付ファイルのダウンロード

[メッセージ部分（Message Parts）] または [一致した内容 :（Matched Content）] セクション内の添付ファイルのファイル名をクリックすることにより、メッセージの添付ファイルをダウンロードできます。AsyncOS から、未知の送信元からの添付ファイルにはウイルスが含まれる可能性があることを示す警告が表示され、続行するかどうか尋ねられます。ウイルスを含むかもしれない添付ファイルを自己責任においてダウンロードします。[メッセージ部分（Message Parts）] セクション内の `[message body]` をクリックすることにより、メッセージ本文をダウンロードすることもできます。

隔離されたメッセージの再スキャンについて

隔離内にあるキューすべてからメッセージがリリースされると、アプライアンスで使用可能な機能に基づきおよびメッセージが最初に隔離されたメール ポリシーに対して、次の再スキャンが開始されます。

- ポリシーおよびウイルス隔離からリリースされるメッセージはウイルス対策エンジンによって再スキャンされます。

- アウトブレイク隔離からリリースされるメッセージはスパム対策およびウイルス対策エンジンによって再スキャンされます （アウトブレイク隔離中のメッセージの再スキャンの詳細については、電子メール セキュリティ アプライアンスのオンライン ヘルプまたはユーザ ガイドの「Outbreak Filters」の章を参照してください）。

再スキャンで、判定結果が前回そのメッセージを処理したときの判定結果と一致する場合、そのメッセージは再隔離されません。逆に、判定が異なると、そのメッセージは他の隔離に送信できます。

原理的に、メッセージの隔離が無限に繰り返されることはないようになっています。たとえば、メッセージが暗号化されていて、その結果、Virus 隔離に送信されるとします。管理者がそのメッセージをリリースしても、ウイルス対策エンジンはまだそのメッセージを復号化できません。しかし、そのメッセージは再隔離されない必要があるか、またはループ状態となりそのメッセージは二度と隔離からリリースされなくなります。2 回とも判定は同じ結果になるので、システムは 2 回めには Virus 隔離を無視します。

アウトブレイク隔離

アウトブレイク隔離は、アウトブレイク フィルタ機能の有効なライセンス キーが入力されている場合に存在します。アウトブレイク フィルタ機能では、しきい値セットに従ってメッセージがアウトブレイク隔離に送信されます。詳細については、の電子メール セキュリティ アプライアンスオンライン ヘルプまたはユーザ ガイドの「Outbreak Filters」の章を参照してください。

アウトブレイク隔離は、他の隔離と同じように運用され、メッセージの検索、メッセージのリリースまたは削除などができます。

アウトブレイク隔離には、他の隔離では使用できない追加の機能があります。これには、[ルール サマリで管理（Manage by Rule Summary）] リンク、メッセージの詳細を表示しているときの [シスコへ送信（Send to Cisco）] 機能、および [終了予定（Scheduled Exit）] の時間によって検索結果内のメッセージをソートするオプションがあります。

Outbreak フィルタ機能のライセンスの有効期限が切れると、メッセージをアウトブレイク隔離にそれ以上追加できなくなります。隔離エリア内に現在存在するメッセージの保存期間が終了してアウトブレイク隔離が空になると、GUI の隔離リストにアウトブレイク隔離は表示されなくなります。

アウトブレイク隔離内のメッセージの再スキャン

新しく発行されたルールによって、隔離されているメッセージがもう脅威ではないと考えられる場合にはアウトブレイク隔離に入れられたメッセージは自動的にリリースされます。

アプライアンス上でアンチスパムおよびアンチウイルスがイネーブルになっている場合、スキャン エンジンは、メッセージに適用されるメール フロー ポリシーに基づいて、アウトブレイク隔離から解放されたすべてのメッセージをスキャンします。

[ルール サマリで管理（Manage by Rule Summary）] リンク

隔離リストで Outbreak 隔離の横にある [ルール サマリで管理（Manage by Rule Summary）] リンクをクリックして、[ルール サマリで管理（Manage by Rule Summary）] ページを表示します。隔離エリア内のすべてのメッセージに対し、それらのメッセージを隔離させた感染防止ルールに基づいてメッセージ アクション（Release、Delete、Delay Exit）を実行できます。これは、アウトブレイク隔離から大量のメッセージを処理する場合に適しています。詳細については、電子メール セキュリティ アプライアンスのオンライン ヘルプまたはユーザ ガイドの「Outbreak Filters」の章の [ルール サマリで管理（Manage by Rule Summary）] ビューについての情報を参照してください。

誤検出または疑わしいメッセージのシスコへのレポート

アウトブレイク隔離内のメッセージのメッセージ詳細を表示したときに、誤検出または疑わしいメッセージをレポートするためにこのメッセージをシスコに送信できます。

手順

ステップ 1　アウトブレイク隔離内のメッセージに移動します。

ステップ 2　[メッセージの詳細（Message Details）] セクションで、[シスコにコピーを送信する（Send a Copy to Cisco Systems）] チェックボックスを選択します。

ステップ 3　[送信（Send）] をクリックします。

CHAPTER 9

Web セキュリティ アプライアンスの管理

中央集中型コンフィギュレーション管理について

集約設定管理を使用すると、シスコのコンテンツセキュリティ管理アプライアンスから関連する Web セキュリティ アプライアンスに設定を公開できるようになり、次のような利点が得られます。

- Web セキュリティ ポリシーの設定や設定の更新を個々の Web セキュリティ アプライアンスではなくセキュリティ管理アプライアンスで一度行うだけで済み、管理を簡便化および迅速化できます。
- 展開されているネットワーク全体で、ポリシーを均一に適用できます。

設定を Web セキュリティ アプライアンスに公開する方法は 2 つあります。

- Configuration Master を使用する
- Web セキュリティ アプライアンスからのコンフィギュレーション ファイルを使用する（拡張ファイル公開を使用する）

適切な設定公開方式の決定

セキュリティ管理アプライアンスから設定を公開するには異なる 2 つの方法があり、それぞれ異なる設定を公開します。設定の中には中央集中型で管理できないものもあります。

一般的には次のようになります。

- 次の設定に対しては、Configuration Master を使用します。

  Web セキュリティ アプライアンスの [Web セキュリティ マネージャ（Web Security Manager）] メニューに表示される機能。ポリシーやカスタム URL のカテゴリなど。

例外：L4 トラフィック モニタの（L4TM）の設定は、Configuration Master の対象に含まれません。

サポートの対象となる機能は、Configuration Master のバージョンによって変わります。このバージョンは AsyncOS for Web Security のバージョンに対応します。

Configuration Master で設定できる一部の機能は、動作させるために、Web セキュリティ アプライアンスでも直接設定する必要があります。たとえば、SOCKS ポリシーは Configuration Master で設定可能ですが、最初に SOCKS プロキシを Web セキュリティ アプライアンスで直接設定する必要があります。

- 次の設定に対しては、コンフィギュレーション ファイル（拡張ファイル公開）を使用します。

  アプライアンスの管理に関係する機能。たとえば、ログ サブスクリプションやアラートの設定、または管理責任の分散など。

  例外：

  セキュリティ管理アプライアンスを使用して、Web セキュリティ アプライアンスの次の機能を有効にすること、または設定することはできません: 連邦情報処理標準の FIPS モード、ネットワーク / インターフェイスの設定、DNS、Web Cache Communication Protocol（WCCP）、アップストリーム プロキシ グループ、証明書、プロキシ モード、NTP などの時間設定、L4 トラフィック モニタ（L4TM）設定、および認証リダイレクト ホスト名。

  これらの設定は、管理対象の Web セキュリティ アプライアンスで直接設定する必要があります。『*Cisco IronPort AsyncOS for Web Security User Guide*』を参照してください。

Configuration Master の設定

Configuration Master を使用して中央集中型コンフィギュレーション管理を設定するには、「Configuration Master の設定の概要」（P.9-2）で説明する手順を順序に従って実行してください。

拡張ファイル公開だけを使用するように準備するには、「拡張ファイル公開を使用するための設定」（P.9-14）を参照してください。

Configuration Master の設定の概要

Web セキュリティ アプライアンスを中央集中方式で管理するようにシステムを設定するには、次の手順に従ってください。

ステップ 1　**（任意）Web セキュリティ アプライアンス。**すべての Web セキュリティ アプライアンスの設定モデルとして動作している Web セキュリティ アプライアンスがすでにある場合は、その Web セキュリティ アプライアンスからコンフィギュレーション ファイルをダウンロードします。このファイルを使用すると、セキュリティ管理アプライアンスでの Configuration Master の設定を迅速に行うことができます。方法については、『*Cisco IronPort AsyncOS for Web Security User Guide* 』の「Saving and Loading the Appliance Configuration」を参照してください。

コンフィギュレーション ファイルと Configuration Master バージョンの互換性については、このリリースのリリース ノート（ http://www.cisco.com/en/US/products/ps10155/prod_release_notes_list.html）を参照してください。

ステップ 2　設定のための一般的な要件や注意事項を確認します。「Configuration Master を使用するための重要な注意事項」（P.9-3）を参照してください。

ステップ 3　各 Web セキュリティ アプライアンスに使用する Configuration Master のバージョンを確認します。「使用する Configuration Master のバージョンの確認」（P.9-3）を参照してください。

ステップ 4　**セキュリティ管理アプライアンス。**集約設定管理を有効にし、設定します。「セキュリティ管理アプライアンスでの中央集中型コンフィギュレーション管理のイネーブル化」（P.9-4）を参照してください。

ステップ 5　**セキュリティ管理アプライアンス。**Configuration Master を初期化します。「Configuration Master の初期化」（P.9-4）を参照してください。

ステップ 6　**セキュリティ管理アプライアンス。**Web セキュリティ アプライアンスを Configuration Master に関連付けます。「Web セキュリティ アプライアンスと Configuration Master の関連付けについて」（P.9-5）を参照してください。

ステップ 7　**セキュリティ管理アプライアンス。**ポリシー、カスタム URL カテゴリ、および Web プロキシ バイパス リストを Configuration Master にインポートするか、手動で設定します。「公開のための設定」（P.9-6）を参照してください。

ステップ 8　**セキュリティ管理アプライアンス。**それぞれの Web セキュリティ アプライアンスでイネーブルにされている機能が、そのアプライアンスに関連付けられている Configuration Master でイネーブルにされている機能と一致していることを確認します。「機能が常にイネーブルにされていることの確認」（P.9-11）を参照してください。

ステップ 9　**セキュリティ管理アプライアンス。**必要とする Configuration Master を設定し、必要な機能をイネーブルにしたら、Web セキュリティ アプライアンスに設定を公開します。「Configuration Master の公開」（P.9-14）を参照してください。

Configuration Master を使用するための重要な注意事項

（注）　中央集中型で管理する Web セキュリティ アプライアンスのそれぞれについて、同名のレルムに対する設定が同一である場合を除いて、[ネットワーク（Network）] > [認証（Authentication）] ですべての [レルム名（Realm Names）] がアプライアンス全体で一意になっていることを確認します。

使用する Configuration Master のバージョンの確認

セキュリティ管理アプライアンスには複数の設定マスターがあるため、複数の Web セキュリティ アプライアンスで異なる機能をサポートする異なるバージョンの AsyncOS for Web Security が実行されている異機種混在環境でも集約的に管理できます。

それぞれの Configuration Master には、AsyncOS for Web Security の特定のバージョンで使用する設定が行われています。

使用している AsyncOS for Web Security のバージョンで使用できる Configuration Master を判断するには、「SMA 互換性マトリクス」（P.2-2）を参照してください。

（注）　最善の結果を得るには、Configuration Master のバージョンが、Web セキュリティ アプライアンスの AsyncOS のバージョンと同じである必要があります。古いバージョンの Configuration Master から新しいバージョンの Web セキュリティ アプライアンスに対して公開を行うと、Web セキュリティ アプライアンスの設定が Configuration Master の設定と一致していない場合には、処理に失敗するおそれがあります。この問題は、[Web アプライアンス ステータスの詳細（Web Appliance Status Details）] ページに不一致が見られない場合でも発生することがあります。この場合は、各アプライアンスでの設定を手動で比較する必要があります。

セキュリティ管理アプライアンスでの中央集中型コンフィギュレーション管理のイネーブル化

手順

ステップ 1　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [Web] > [集中型設定マネージャ（Centralized Configuration Manager）] を選択します。

ステップ 2　[有効（Enable）] をクリックします。

ステップ 3　システム セットアップ ウィザードを実行してから初めて集約設定管理を有効にする場合は、エンド ユーザ ライセンス契約書を確認し、[承認（Accept）] をクリックします。

ステップ 4　変更を送信し、保存します。

Configuration Master の初期化

（注）　Configuration Master 7.1 を Configuration Master 7.5 および 7.7 にコピーしたり、インポートする前に、「Configuration Master 7.5 および 7.7 を設定する前の注意事項」（P.9-25）を参照してください。

手順

ステップ 1　メイン セキュリティ管理アプライアンスで、[Web] > [ユーティリティ（Utilities）] > [設定マスター（Configuration Masters）] を選択します。

ステップ 2　[オプション（Options）] カラムの [初期化（Initialize）] をクリックします。

ステップ 3　[Configuration Master の初期化（Initialize Configuration Master）] ページで、次の手順を実行します。

- 以前のリリース用の Configuration Master がすでにあり、新しい Configuration Master で同じ設定を適用したい場合は、[Configuration Master のコピー（Copy Configuration Master）] を選択します。

  また、後で既存の Configuration Master から設定をインポートすることもできます。
- 上記に該当しない場合は、[デフォルト設定を使用（Use default settings）] を選択します。

ステップ 4　[初期化（Initialize）] をクリックします。

これで Configuration Master が使用可能な状態になります。

ステップ 5　それぞれの Configuration Master のバージョンに対して初期化作業を繰り返します。

（注）　Configuration Master を初期化すると、[初期化（Initialize）] オプションは使用できなくなります。その代わりに、「公開のための設定」（P.9-6）で説明されている方法のいずれかを使用して Configuration Master を設定します。

Web セキュリティ アプライアンスと Configuration Master の関連付けについて

中央集中型で管理する Web セキュリティ アプライアンスのそれぞれにおいて、そのアプライアンスの AsyncOS バージョンと一致する Configuration Master にポリシー設定を関連付ける必要があります。たとえば、Web セキュリティ アプライアンスで AsyncOS 7.7 for Web を実行中の場合は、Configuration Master 7.7 に関連付ける必要があります。

このための最も単純な方法は、状況によって異なります。

条件	参照する手順
まだ Web セキュリティ アプライアンスをセキュリティ管理アプライアンス に追加していない	「Web セキュリティ アプライアンスの追加と Configuration Master のバージョンとの関連付け」（P.9-5）
すでに Web セキュリティ アプライアンスを追加済みである	「Configuration Master のバージョンと Web セキュリティ アプライアンスとの関連付け」（P.9-6）

Web セキュリティ アプライアンスの追加と Configuration Master のバージョンとの関連付け

まだ Web セキュリティ アプライアンスを中央集中管理の対象に追加していない場合は、この手順を実行してください。

手順

ステップ 1　使用している Web セキュリティ アプライアンスと、この AsyncOS for Security Management のリリースで使用できる Configuration Master のバージョンとの互換性を確認します。「SMA 互換性マトリクス」（P.2-2）を参照してください。

ステップ 2　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [セキュリティ アプライアンス（Security Appliances）] を選択します。

ステップ 3　[Web アプライアンスの追加（Add Web Appliance）] をクリックします。

ステップ 4　[アプライアンス名（Appliance Name）] および [IP アドレス（IP Address）] テキスト フィールドに、Web セキュリティ アプライアンスの管理インターフェイスのアプライアンス名と IP アドレスを入力します。

（注）　[IP アドレス（IP Address）] テキスト フィールドに DNS 名を入力した場合でも、[送信（Submit）] をクリックすると、すぐに IP アドレスに解決されます。

ステップ 5　Centralized Configuration Manager サービスが事前に選択されています。

ステップ 6　[接続の確立（Establish Connection）] をクリックします。

ステップ 7　管理対象となるアプライアンスの管理者アカウントのユーザ名とパスワードを入力し、[接続の確立（Establish Connection）] をクリックします。

（注）　ログイン資格情報を入力すると、セキュリティ管理アプライアンスからリモート アプライアンスへのファイル転送のための公開 SSH キーが渡されます。ログイン資格情報は、セキュリティ管理アプライアンスには保存されません。

ステップ 8　[成功（Success）] メッセージがページのテーブルの上に表示されるまで待機します。

ステップ 9　アプライアンスに関連付ける Configuration Master のバージョンを選択します。

ステップ 10　変更を送信し、保存します。

ステップ 11　中央集中型コンフィギュレーション管理をイネーブルにする Web セキュリティ アプライアンスごとに、この手順を繰り返します。

Configuration Master のバージョンと Web セキュリティ アプライアンスとの関連付け

Web セキュリティ アプライアンスをセキュリティ管理アプライアンスに追加済みの場合は、次の手順を使用して、Web セキュリティ アプライアンスを Configuration Master のバージョンに素早く関連付けることができます。

手順

ステップ 1　使用している Web セキュリティ アプライアンスと、この AsyncOS for Security Management のリリースで使用できる Configuration Master のバージョンとの互換性を確認します。「SMA 互換性マトリクス」（P.2-2）を参照してください。

ステップ 2　セキュリティ管理アプライアンスで、[Web] > [ユーティリティ（Utilities）] > [設定マスター（Configuration Masters）] を選択します。

（注）　Configuration Master が [無効（Disabled）] と表示されている場合にイネーブルにするには、[Web] > [ユーティリティ（Utilities）] > [セキュリティ サービス表示（Security Services Display）] の順にクリックし、次に [表示設定の編集（Edit Display Settings）] をクリックします。対象とする Configuration Master のチェックボックスを選択して、イネーブルにします。詳細については、「公開する機能のイネーブル化」（P.9-12）を参照してください。

ステップ 3　[アプライアンス割り当てリストの編集（Edit Appliance Assignment List）] をクリックします。

ステップ 4　関連付けるアプライアンスの行でクリックし、[マスター（Masters）] カラムにチェックマークを入れます。

ステップ 5　変更を送信し、保存します。

公開のための設定

公開する設定を Configuration Master に設定します。

Configuration Master の設定には、いくつかの方法があります。

- AsyncOS for Security Management の以前のリリースからアップグレードする場合 : 以前の既存の Configuration Master をコピーして新しい Configuration Master のバージョンを初期化していない場合は、古いバージョンをインポートすることができます。「既存の Configuration Master からのインポート」（P.9-7）を参照してください。
- Web セキュリティ アプライアンスを設定済みで、複数の Web セキュリティ アプライアンスで同じ設定を使用したい場合 : 保存されているコンフィギュレーション ファイルをアプライアンスから Configuration Master にインポートします （「Configuration Master の設定」（P.9-2）でコンフィギュレーション ファイルを保存した場合）。

  インポートの手順については、「Web セキュリティ アプライアンスからの設定のインポート」（P.9-7）を参照してください。
- インポートした設定を変更する場合は、「Configuration Master での Web セキュリティ機能の直接設定」（P.9-8）を参照してください。
- Web セキュリティ アプライアンスでポリシー、URL カテゴリ、バイパス設定をまだ設定していない場合は、セキュリティ管理アプライアンスでこれらの設定を対応する Configuration Master に設定します。

  詳細については、「Configuration Master での Web セキュリティ機能の直接設定」（P.9-8）を参照してください。

既存の Configuration Master からのインポート

既存の Configuration Master を新しい Configuration Master のバージョンにアップグレードすることができます。たとえば、Configuration Master 7.1 の設定を、Configuration Master 7.5 および 7.7 にインポートすることができます。

（注）　Configuration Master 7.5 および 7.7 にコピーまたはインポートする前に、「Configuration Master 7.5 および 7.7 を設定する前の注意事項」（P.9-25）を参照してください。

手順

ステップ 1　セキュリティ管理アプライアンスで、[Web] > [ユーティリティ（Utilities）] > [設定マスター（Configuration Masters）] を選択します。

ステップ 2　[オプション（Options）] カラムで、[設定のインポート（Import Configuration）] をクリックします。

ステップ 3　[設定ソースの選択（Select Configuration Source）] で、リストから [設定マスター（Configuration Master）] を選択します。

ステップ 4　この設定に、既存のカスタム ユーザ ロールを取り込むかどうかを選択します。

カスタム ユーザ ロールの詳細については、「Custom Web User ロールについて」（P.13-9）を参照してください。

ステップ 5　[インポート（Import）] をクリックします。

Web セキュリティ アプライアンスからの設定のインポート

使用中の Web セキュリティ アプライアンスで機能している既存の設定を使用する場合は、そのコンフィギュレーション ファイルをセキュリティ管理アプライアンスにインポートして、Configuration Master 用のデフォルトのポリシー設定を作成できます。

コンフィギュレーション ファイルと Configuration Master バージョンの互換性については、このリリースのリリース ノート（http://www.cisco.com/en/US/products/ps10155/prod_release_notes_list.html）を参照してください。

注意　管理対象の Web セキュリティ アプライアンスに設定をすでに公開してある場合でも、互換性のある Web コンフィギュレーション ファイルを何回でもインポートすることができます。ただし、コンフィギュレーション ファイルを Configuration Master にインポートすると、選択した Configuration Master に関連付けられている設定が上書きされることに注意してください。また、[セキュリティ サービス表示（Security Services Display）] ページのセキュリティ サービスの設定は、インポートしたファイルと一致するよう設定されます。

Configuration Master に Web コンフィギュレーション ファイルを取り込むには、次の手順を実行します。

手順

ステップ 1　Web セキュリティ アプライアンスから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　セキュリティ管理アプライアンスで、[Web] > [ユーティリティ（Utilities）] > [設定マスター（Configuration Masters）] を選択します。

ステップ 3　[オプション（Options）] カラムで、[設定のインポート（Import Configuration）] をクリックします。

ステップ 4　[設定の選択（Select Configuration）] ドロップダウン リストから、[Web 設定ファイル（Web Configuration File）] を選択します。

ステップ 5　[新しいマスターのデフォルト（New Master Defaults）] セクションで、[参照（Browse）] をクリックし、Web セキュリティ アプライアンスから有効なコンフィギュレーション ファイルを選択します。

ステップ 6　[ファイルをインポート（Import File）] をクリックします。

ステップ 7　[インポート（Import）] をクリックします。

Configuration Master での Web セキュリティ機能の直接設定

Configuration Master では、バージョンに応じて次の機能を設定できます。

Configuration Master 7.1	Configuration Master 7.5	Configuration Master 7.7
• ID • SaaS ポリシー • 復号ポリシー • ルーティング ポリシー • アクセス ポリシー • 全体の帯域幅の制限 • Cisco IronPort データ セキュリティ • 外部データ漏洩防止 • Outbound Malware Scanning • カスタム URL カテゴリ • 定義済みの時間範囲 • バイパス設定	• ID • SaaS ポリシー • 復号ポリシー • ルーティング ポリシー • アクセス ポリシー • 全体の帯域幅の制限 • Cisco IronPort データ セキュリティ • 外部データ漏洩防止 • Outbound Malware Scanning • カスタム URL カテゴリ • 定義済みの時間範囲 • バイパス設定	• ID • SaaS ポリシー • 復号ポリシー • ルーティング ポリシー • アクセス ポリシー • 全体の帯域幅の制限 • Cisco IronPort データ セキュリティ • 外部データ漏洩防止 • Outbound Malware Scanning • SOCKS ポリシー • カスタム URL カテゴリ • 定義済みの時間範囲 • バイパス設定

Configuration Master で各機能を直接設定するには、[Web] > [Configuration Master <*version*>] > <*feature*> を選択します。

「Configuration Master で機能を設定する場合の SMA 特有の違い」（P.9-9）で説明する一部の項目を除いて、Configuration Master で機能を設定する方法は、Web セキュリティ アプライアンスで同じ機能を設定する場合と同じです。各説明については、ご使用の Web セキュリティ アプライアンスのオンライン ヘルプ、または設定マスターのバージョンに対応する AsyncOS バージョンの『*Cisco IronPort AsyncOS for Web Security User Guide*』を参照してください。必要な場合は、「使用する Configuration Master のバージョンの確認」（P.9-3）を参照して、使用している Web セキュリティ アプライアンスに対応する正しい Configuration Master を判別してください。

Web セキュリティ ユーザ ガイドは、http://www.cisco.com/en/US/products/ps10164/products_user_guide_list.html ですべてのバージョンを入手できます。

Configuration Master で機能を設定する場合の SMA 特有の違い

Configuration Master で機能を設定するときには、以下で説明する Web セキュリティ アプライアンスで同じ機能を直接設定する場合との違いに注意してください。

表 9-1　機能の設定：Configuration Master と Web セキュリティ アプライアンスとの違い

機能またはページ	詳細
すべての機能、特に各リリースでの新機能	Configuration Master で設定する各機能について、セキュリティ管理アプライアンスで [Web] > [ユーティリティ（Utilities）] > [セキュリティ サービス表示（Security Services Display）] にある機能をイネーブルにする必要があります。詳細については、「機能が常にイネーブルにされていることの確認」（P.9-11）を参照してください。
ID	• 「Configuration Master で ID を使用する場合のヒント」（P.9-10）を参照してください。 • 同じ名前で、異なるプロトコルを使用する異なる Web セキュリティ アプライアンスにレルムがある場合、Configuration Master で目的のレルムごとに適切なスキームを選択します。 • トランスペアレント ユーザ ID をサポートする認証レルムがある 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ている場合、ID の追加または編集時に [ユーザを透過的に識別する（Identify Users Transparently）] オプションを使用できます。 この機能は、Configuration Master 7.5 で導入されました。
SaaS ポリシー	認証オプションの [透過的なユーザ識別によって検出された SaaS ユーザにプロンプトを出力する（Prompt SaaS users who have been discovered by transparent user identification）] は、トランスペアレント ユーザ ID をサポートする認証レルムが設定された 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ている場合のみ有効になります。
[アクセス ポリシー（Access Policies）] > [グループの編集（Edit Group）]	[ポリシー メンバの定義（Policy Member Definition）] セクションで [ID とユーザ（Identities and Users）] オプションを設定すると、外部ディレクトリ サーバを使用している場合には、以下が適用されます。 [グループの編集（Edit Group）] ページでグループを検索した場合、検索結果の最初の 500 項目しか表示されません。対象とするグループが見つからない場合は、そのグループを「Authorized Groups」に追加することができます。これを行うには、[ディレクトリ（Directory）] 検索フィールドにこのグループを入力して、[追加（Add）] ボタンをクリックします。
[アクセス ポリシー（Access Policies）] > [Web レピュテーションとマルウェア対策の設定（Web Reputation and Anti-Malware Settings）]	このページで指定できるオプションは、関連する Configuration Master に対して Adaptive Scanning がイネーブルにされているかどうかによって変わります。[Web] > [ユーティリティ（Utilities）] > [セキュリティ サービス表示（Security Services Display）] でこの設定を確認してください。 この機能は、Configuration Master 7.5 で導入されました。

Configuration Master で ID を使用する場合のヒント

セキュリティ管理アプライアンスで ID を作成する際には、特定のアプライアンスのみに適用されるオプションがあります。たとえば、セキュリティ管理アプライアンスを購入し、Web セキュリティ アプライアンスごとに作成された既存の Web セキュリティ アプライアンス コンフィギュレーションとポリシーを保持する場合は、1 つのファイルをマシンにロードし、次に他のマシンから手動でポリシーを追加する必要があります。

これを実行するための方法の 1 つとして、各アプライアンスに一連の ID を作成し、これらの ID を参照するポリシーを設定する方法があります。セキュリティ管理アプライアンスが設定を公開すると、これらの ID と、ID を参照するポリシーは自動的に削除され、ディセーブルになります。この方法を使用すると、手動で何も設定する必要がありません。これは基本的に「アプライアンスごと」の ID です。

この方法の唯一の問題は、デフォルトのポリシーまたは ID が、サイト間で異なる場合です。たとえば、あるサイトではポリシーを「default allow with auth」に設定し、別のサイトでは「default deny」に設定している場合です。この場合、アプライアンスごとの ID とポリシーをデフォルトのすぐ上に作成する必要があります。基本的には独自の「デフォルト」ポリシーを作成します。

機能が常にイネーブルにされていることの確認

Configuration Master を公開する前に、それが公開されることと、公開後に目的の機能がイネーブルになり、意図するように設定されていることを確認します。

このためには、次の両方を実行してください。

- 「イネーブルにされている機能の比較」（P.9-11）
- 「公開する機能のイネーブル化」（P.9-12）

（注）　異なる機能がイネーブルになっている複数の Web セキュリティ アプライアンスが同じ Configuration Master に割り当てられている場合は、各アプライアンスを別個に公開するようにし、公開前にこれらの手順を実行する必要があります。

イネーブルにされている機能の比較

それぞれの Web セキュリティ アプライアンスでイネーブルにされている機能が、そのアプライアンスに関連付けられている Configuration Master でイネーブルにされている機能と一致していることを確認します。

（注）　異なる機能を持つ複数の Web セキュリティ アプライアンスが同じ Configuration Master に割り当てられている場合は、各アプライアンスを別個に公開するようにし、公開前にこのチェックを実行する必要があります。

Web セキュリティ アプライアンスでイネーブルにされている機能を確認するには、次の手順を実行します。

手順

ステップ 1　セキュリティ管理アプライアンスで、[Web] > [ユーティリティ（Utilities）] > [Web アプライアンス ステータス（Web Appliances Status）] を選択します。

ステップ 2　Configuration Master を公開する Web セキュリティ アプライアンスの名前をクリックします。

ステップ 3　[セキュリティ サービス（Security Services）] テーブルまでスクロールします。

ステップ 4　イネーブルにされているすべての機能のライセンス キーがアクティブで、期限切れでないことを確認します。

ステップ 5　[サービス（Services）] カラムの設定を比較します。

[Web アプライアンス サービス（Web Appliance Service）] カラムと、[管理アプライアンスに表示されているサービス（Is Service Displayed on Management Appliance?）] カラムが同じである必要があります。

- [有効（Enabled）] = [はい（Yes）]

- [無効（Disabled）] および [未設定（Not Configured）] = [いいえ（No）] または [無効（Disabled）]
- N/A = 適用されません。たとえば、そのオプションは Configuration Master で設定できませんが、一覧には表示されて、ライセンス キーのステータスを確認することができます。

コンフィギュレーションが不一致の場合は、文字が赤色で表示されます。

ステップ 6　ある機能についてのイネーブルおよびディセーブルの設定が一致していない場合は、次のいずれかを実行します。

- Configuration Master の対応する設定を変更します。「公開する機能のイネーブル化」（P.9-12）を参照してください。
- Web セキュリティ アプライアンスの当該の機能をイネーブルまたはディセーブルにします。変更内容によっては、複数の機能に影響する場合があります。関連する機能については、『*Cisco IronPort AsyncOS for Web Security User Guide*』を参照してください。

公開する機能のイネーブル化

Configuration Master を使用して設定を公開する機能をイネーブルにします。

（注）　Configuration Master に対して機能をイネーブルにしても、その機能が Web セキュリティ アプライアンスでイネーブルになるわけではありません。

各 Configuration Master に対してイネーブルにした機能は、[セキュリティ サービス表示（Security Services Display）] ページに要約されます。「N/A」と表示されている場合は、その機能がその Configuration Master のバージョンで使用できないことを表します。

公開する機能をイネーブルにするには、次の手順を実行してください。

手順

ステップ 1　イネーブルにする機能とディセーブルにする機能を確認します。「イネーブルにされている機能の比較」（P.9-11）を参照してください。

ステップ 2　セキュリティ管理アプライアンスで、[Web] > [ユーティリティ（Utilities）] > [セキュリティ サービス表示（Security Services Display）] を選択します。

ステップ 3　[設定を編集（Edit Settings）] をクリックします。

[セキュリティ サービス表示の編集（Edit Security Services Display）] ページに、各 Configuration Master に表示される機能が一覧されます。

（注）　Web プロキシは機能として一覧されていません。これは、Web プロキシは Web セキュリティ アプライアンスで管理されているプロキシ タイプのいずれかを実行するためにイネーブルになっていると見なされているためです。Web プロキシをディセーブルにすると、Web セキュリティ アプライアンスに公開されたすべてのポリシーが無視されます。

ステップ 4　（任意）使用しない Configuration Master は非表示にします。意図しない影響が生じるのを避けるため、「使用しない Configuration Master のディセーブル化」（P.9-13）の「注」を参照してください。

ステップ 5　使用する各 Configuration Master について、イネーブルにする各機能に対する [はい（Yes）] チェックボックスを選択または選択解除します。

次の特定機能には特に注意してください（使用可能なオプションは、Configuration Master のバージョンによって異なります）。

- トランスペアレント モード。フォワード モードを使用した場合、プロキシ バイパス機能は使用できなくなります。
- HTTPS プロキシ。HTTPS プロキシは、復号ポリシーを実行するためにイネーブルにする必要があります。
- アップストリーム プロキシ グループ。ルーティング ポリシーを使用する場合は、Web セキュリティ アプライアンスでアップストリーム プロキシ グループが使用できるようになっている必要があります。

ステップ 6　使用する各 Configuration Master に対して変更を加えます。

ステップ 7　[送信（Submit）] をクリックします。セキュリティ サービスの設定に加えた変更が、Web セキュリティ アプライアンスで設定されたポリシーに影響する場合、GUI に特定の警告メッセージが表示されます。変更を送信することが確実な場合は、[続行（Continue）] をクリックします。

ステップ 8　[セキュリティ サービス表示（Security Services Display）] ページで、選択した各オプションの横に [はい（Yes）] と表示されることを確認します。

ステップ 9　変更を保存します。

ステップ 10　公開先のアプライアンスに対して、すべての機能が正しくイネーブルまたはディセーブルになっていることを確認します。「イネーブルにされている機能の比較」（P.9-11）を参照してください。

使用しない Configuration Master のディセーブル化

使用しない Configuration Master を表示しないようにすることができます。

たとえば、一部の Configuration Master をディセーブルにしたとき、[設定マスター（Configuration Master）] タブと [セキュリティ サービス表示（Security Services Display）] ページは次のように表示されます。

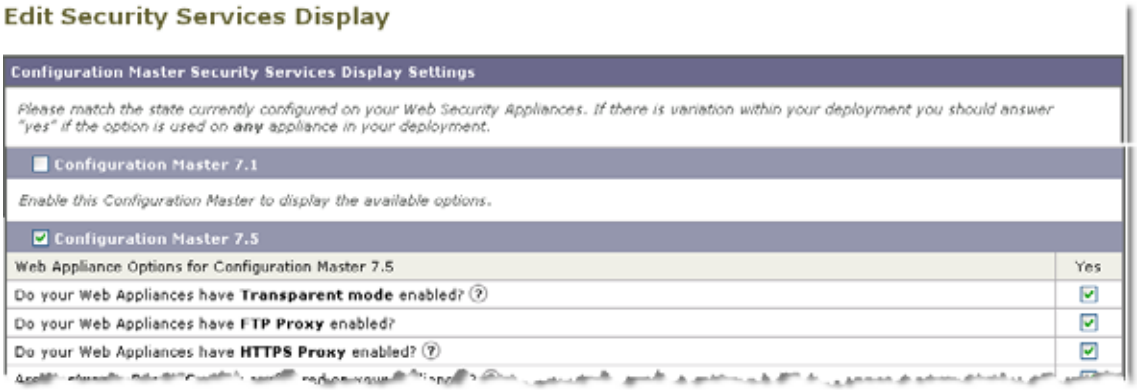
（注）　Configuration Master をディセーブルにすると、それに対するすべての参照が、対応する [設定マスター（Configuration Master）] タブを含めて GUI から削除されます。その Configuration Master を使用する保留中の公開ジョブは削除され、非表示の Configuration Master に割り当てられていたすべての Web セキュリティ アプライアンスが、割り当てられていないものとして再分類されます。少なくとも 1 つの Configuration Master をイネーブルにする必要があります。

手順

ステップ 1　セキュリティ管理アプライアンスで、[Web] > [ユーティリティ（Utilities）] > [セキュリティ サービス表示（Security Services Display）] を選択します。

ステップ 2　[設定を編集（Edit Settings）] をクリックします。

ステップ 3　使用しない Configuration Master に対するチェックボックスを選択解除します。



ステップ 4　変更を送信し、保存します。

拡張ファイル公開を使用するための設定

システムで Configuration Master を使用するよう設定されている場合は、拡張ファイル公開に対する設定も行われています。

そうでない場合は、次の項で説明する手順を実行してください。これらは、拡張ファイル公開だけでなく、Configuration Master の公開にも適用されます。

- 「セキュリティ管理アプライアンスでの中央集中型コンフィギュレーション管理のイネーブル化」（P.9-4）
- 「Configuration Master の初期化」（P.9-4）
- 「Web セキュリティ アプライアンスと Configuration Master の関連付けについて」（P.9-5）

Web セキュリティ アプライアンス への設定の公開

- 「Configuration Master の公開」（P.9-14）
- 「拡張ファイル公開による設定の公開」（P.9-18）

Configuration Master の公開

Configuration Master で設定を編集またはインポートした後、その設定を、Configuration Master に関連付けられている Web セキュリティ アプライアンスへ公開できます。

- 「Configuration Master を公開する前に」（P.9-15）
- 「Configuration Master の公開」（P.9-16）
- 「Configuration Master を後日公開」（P.9-17）
- 「コマンドライン インターフェイスによる Configuration Master の公開」（P.9-17）

Configuration Master を公開する前に

Configuration Master を公開すると、その Configuration Master に関連付けられている Web セキュリティ アプライアンスの既存のポリシー情報が上書きされます。

Configuration Master を使用して設定できる設定の詳細については、「適切な設定公開方式の決定」（P.9-1）を参照してください。

Configuration Master を公開する前に、次のことを確認します。

- 対象となる Web セキュリティ アプライアンスの AsyncOS のバージョンが、Configuration Master のバージョンと同じかそれより新しいものである必要があります。具体的な要件については、「SMA 互換性マトリクス」（P.2-2）を参照してください。AsyncOS 7.5 を実行している Web セキュリティ アプライアンスに対して公開するには、Configuration Master 7.5 を使用することを強く推奨します。
- （初回のみ）「Configuration Master の設定」（P.9-2）で説明する手順に従います。
- 対象とする各 Web セキュリティ アプライアンスからコンフィギュレーション ファイルを保存して、公開された設定によって問題が生じた場合に既存の設定を復元できるようにします。詳細については、『*Cisco IronPort AsyncOS for Web Security User Guide*』を参照してください。
- Configuration Master が公開を実施し、公開後に意図する機能がイネーブルになるようにするには、各 Web セキュリティ アプライアンスと、これに対応する Configuration Master の機能を確認し、必要に応じて変更を加えます。「イネーブルにされている機能の比較」（P.9-11）、および必要に応じて「公開する機能のイネーブル化」（P.9-12）を参照してください。

  同じ Configuration Master に割り当てられている複数の Web セキュリティ アプライアンスで異なる機能がイネーブルになっている場合は、各アプライアンスを別個に公開するようにし、それぞれの公開前に機能がイネーブルになっていることを確認する必要があります。
- 対象の Web セキュリティ アプライアンスで AsyncOS を復元した場合は、そのアプライアンスを異なる Configuration Master と関連付けなければならない場合があります。
- Configuration Master を、トランスペアレント ユーザ ID がイネーブルになったレルムを持たない Web セキュリティ アプライアンスに公開したものの、[ID（Identity）] または [SaaS ポリシー（SaaS Policy）] で [透過的なユーザ識別（Transparent User Identification）] を選択していると、次のようになります。
  - [ID（Identity）] の場合、[透過的なユーザ識別（Transparent User Identification）] はディセーブルになり、代わりに [認証が必要（Require Authentication）] オプションが選択されます。
  - [SaaS ポリシー（SaaS Policy）] の場合、[透過的なユーザ識別（Transparent User Identification）] オプションはディセーブルになり、代わりにデフォルトのオプション（SaaS ユーザに対して常にプロキシ認証を要求）が選択されます。
- Web セキュリティ アプライアンスでコミットしたときに Web プロキシの再起動が必要になる変更内容は、それを セキュリティ管理アプライアンスから公開したときにもプロキシの再起動が必要になります。この場合は、警告が発生します。

  プロキシの再起動が必要な変更を Web セキュリティ アプライアンスで行うと、公開時にもプロキシの再起動が発生することがあります。たとえば、Web セキュリティ アプライアンスで新しいグループをアクセス ポリシーのグループ認証設定に追加すると、次に Configuration Master が公開されるときに Web プロキシが再起動します。このような場合は、プロキシの再起動に関する警告は発生しません。

  Web プロキシの再起動により、Web セキュリティ サービスは一時的に中断されます。Web プロキシの再起動による影響の詳細については、『*Cisco IronPort for Web Security User Guide*』の「Checking for Web Proxy Restart on Commit」を参照してください。
- ID に対する変更を公開すると、すべてのエンド ユーザが再認証を受ける必要が生じます。

（注）　セキュリティ管理アプライアンスから、RSA サーバ用に設定されていない複数の Web セキュリティ アプライアンスに、外部 DLP ポリシーを公開しても問題ありません。公開しようとすると、セキュリティ管理アプライアンスから、次の公開ステータス警告が送信されます。「**The Security Services display settings configured for Configuration Master** <*version*> **do not currently reflect the state of one or more Security Services on Web Appliances associated with this publish request.The affected appliances are: "<***WSA Appliance Name***>".This may indicate a misconfiguration of the Security Services display settings for this particular Configuration Master.Go to the Web Appliance Status page for each appliance provides a detailed view to troubleshooting this issue.Do you want to continue publishing the configuration now?**」

公開を続行した場合、RSA サーバ用に設定されていない Web セキュリティ アプライアンスは、外部 DLP ポリシーを受信しますが、これらのポリシーはディセーブルにされます。外部 DLP サーバが設定されていない場合、Web セキュリティ アプライアンスの [外部 DLP（External DLP）] ページには公開されたポリシーが表示されません。

Configuration Master の公開

手順

ステップ 1　「Configuration Master を公開する前に」（P.9-15）の重要な要件と情報を参照してください。

ステップ 2　セキュリティ管理アプライアンスで、[Web] > [ユーティリティ（Utilities）] > [Web アプライアンスへの公開（Publish to Web Appliances）] を選択します。

ステップ 3　[今すぐ設定を公開する（Publish Configuration Now）] をクリックします。

ステップ 4　デフォルトでは [システム生成のジョブ名（System-generated job name）] が選択されています。あるいは、ユーザ定義のジョブ名（80 文字以下）を入力します。

ステップ 5　公開する Configuration Master を選択します。

ステップ 6　Configuration Master の公開先となる Web セキュリティ アプライアンスを選択します。Configuration Master に割り当てられているすべてのアプライアンスに設定を公開するには、[割り当てられたすべてのアプライアンス（All assigned appliances）] を選択します。

または

[リスト内のアプライアンスを選択してください（Select appliances in list）] を選択して、Configuration Master に割り当てられているアプライアンスの一覧を表示します。設定の公開先となるアプライアンスを選択します。

ステップ 7　[公開（Publish）] をクリックします。

[公開中（Publish in Progress）] ページに表示される赤色の経過表示バーとテキストは、公開中にエラーが発生したことを表します。別のジョブが現在公開中の場合、要求は前のジョブが完了すると実行されます。

（注）　進行中のジョブの詳細は、[Web] > [ユーティリティ（Utilities）] > [Web アプライアンスへの公開（Publish to Web Appliances）] ページにも表示されます。[公開中（Publish in Progress）] にアクセスするには、[進捗ステータスの確認（Check Progress）] をクリックします。

ステップ 8　公開が正しく完了したことを確認します。「公開履歴の表示」（P.9-20）を参照してください。完全に公開されなかった項目が表示されます。

Configuration Master を後日公開

手順

ステップ 1　「Configuration Master を公開する前に」（P.9-15）の重要な要件と情報を参照してください。

ステップ 2　セキュリティ管理アプライアンスで、[Web] > [ユーティリティ（Utilities）] > [Web アプライアンスへの公開（Publish to Web Appliances）] を選択します。

ステップ 3　[ジョブをスケジュールする（Schedule a Job）] をクリックします。

ステップ 4　デフォルトでは [システム生成のジョブ名（System-generated job name）] が選択されています。あるいは、ユーザ定義のジョブ名（80 文字以下）を入力します。

ステップ 5　Configuration Master を公開する日時を入力します。

ステップ 6　公開する Configuration Master を選択します。

ステップ 7　Configuration Master の公開先となる Web セキュリティ アプライアンスを選択します。Configuration Master に割り当てられているすべてのアプライアンスに設定を公開するには、[割り当てられたすべてのアプライアンス（All assigned appliances）] を選択します。

または

[リスト内のアプライアンスを選択してください（Select appliances in list）] を選択して、Configuration Master に割り当てられているアプライアンスの一覧を表示します。設定の公開先となるアプライアンスを選択します。

ステップ 8　[送信（Submit）] をクリックします。

ステップ 9　スケジュールされているジョブのリストは、[Web] > [ユーティリティ（Utilities）] > [Web アプライアンスへの公開（Publish to Web Appliances）] ページに表示されます。スケジュールされているジョブを編集するには、そのジョブの名前をクリックします。保留中のジョブをキャンセルするには、対応するごみ箱アイコンをクリックして、ジョブの削除を確認します。

ステップ 10　公開が正しく完了したことを確認するために、自分自身に対する覚え書きを（カレンダーなどに）作成することもできます。「公開履歴の表示」（P.9-20）を参照してください。完全に公開されなかった項目が表示されます。

（注）　スケジュールされた公開ジョブが発生する前に、アプライアンスをリブートまたはアップグレードした場合は、ジョブを再度スケジュールする必要があります。

コマンドライン インターフェイスによる Configuration Master の公開

（注）　「Configuration Master を公開する前に」（P.9-15）の重要な要件と情報を参照してください。

セキュリティ管理アプライアンスでは、次の CLI コマンドを使用して Configuration Master から変更を公開できます。

publishconfig config_master [*--job_name*] [*--host_list* | *host_ip*]

ここで、**config_master** は 7.1、7.5、または 7.7 です。このキーワードは必須です。*job_name* オプションは省略可能で、指定しなかった場合は生成されます。

host_list オプションは、公開する Web セキュリティ アプライアンスのホスト名または IP アドレスのリストで、指定しなかった場合は Configuration Master に割り当てられているすべてのホストに公開されます。*host_ip* オプションには、カンマで区切って複数のホスト IP アドレスを指定できます。

publishconfig コマンドが成功したことを確認するには、**smad_logs** ファイルを調べます。[Web] > [ユーティリティ（Utilities）] > [Web アプライアンス ステータス（Web Appliance Status）] を選択することで、セキュリティ管理アプライアンスの GUI から公開履歴が成功だったことを確認することもできます。このページから、公開履歴の詳細を調べる Web アプライアンスを選択します。また、[Web] > [ユーティリティ（Utilities）] > [公開（Publish）] > [公開履歴（Publish History）] により、[公開履歴（Publish History）] ページに進むことができます。

拡張ファイル公開による設定の公開

拡張ファイル公開を使用して、互換性のある XML コンフィギュレーション ファイルを、ローカル ファイル システムから管理対象の Web セキュリティ アプライアンスにプッシュします。

拡張ファイル公開を使用して設定できる設定の詳細については、「適切な設定公開方式の決定」（P.9-1）を参照してください。

（注）　Web セキュリティ アプライアンスでコミットしたときに Web プロキシの再起動が必要になる変更内容は、それを セキュリティ管理アプライアンスから公開したときにもプロキシの再起動が必要になります。拡張ファイル公開を使用するときには、プロキシの再起動に関する警告が発生します。

Web プロキシの再起動により、Web セキュリティ サービスは一時的に中断されます。Web プロキシの再起動による影響の詳細については、『*Cisco IronPort for Web Security User Guide*』の「Checking for Web Proxy Restart on Commit」を参照してください。

拡張ファイル公開を実行するには、次のいずれかを選択します。

- 「拡張ファイル公開：[今すぐ設定を公開する（Publish Configuration Now）]」（P.9-18）
- 「拡張ファイル公開：[後で公開（Publish Later）]」（P.9-19）

拡張ファイル公開：[今すぐ設定を公開する（Publish Configuration Now）]

手順

ステップ 1　元となる Web セキュリティ アプライアンスから、コンフィギュレーション ファイルを保存します。

ファイルの互換性については、「SMA 互換性マトリクス」（P.2-2）を参照してください。

Web セキュリティ アプライアンスからコンフィギュレーション ファイルを保存する方法については、『*Cisco IronPort AsyncOS for Web Security User Guide*』を参照してください。

ステップ 2　各宛先の Web セキュリティ アプライアンスにおいて、Web セキュリティ アプライアンスの既存の設定をコンフィギュレーション ファイルに保存します。詳細については、『*Cisco IronPort AsyncOS for Web Security User Guide*』を参照してください。

ステップ 3　セキュリティ管理アプライアンスのメイン ウィンドウで、[Web] > [ユーティリティ（Utilities）] > [Web アプライアンスへの公開（Publish to Web Appliances）] を選択します。

ステップ 4　[今すぐ設定を公開する（Publish Configuration Now）] をクリックします。

ステップ 5　デフォルトでは [システム生成のジョブ名（System-generated job name）] が選択されています。あるいはジョブ名（80 文字まで）を入力します。

ステップ 6　[公開する設定マスター（Configuration Master to Publish）] で、[詳細ファイル オプション（Advanced file options）] を選択します。

ステップ 7　[参照（Browse）] をクリックして、ステップ 1 で保存したファイルを選択します。

ステップ 8　[Web アプライアンス（Web Appliances）] ドロップダウン リストから、[リスト内のアプライアンスを選択してください（Select appliances in list）] または [すべてがマスターに割り当てられました（All assigned to Master）] を選択して、コンフィギュレーション ファイルの公開先となるアプライアンスを選択します。

ステップ 9　[公開（Publish）] をクリックします。

拡張ファイル公開：[後で公開（Publish Later）]

手順

ステップ 1　元となる Web セキュリティ アプライアンスから、コンフィギュレーション ファイルを保存します。

ファイルの互換性については、「SMA 互換性マトリクス」（P.2-2）を参照してください。

Web セキュリティ アプライアンスからコンフィギュレーション ファイルを保存する方法については、『*Cisco IronPort AsyncOS for Web Security User Guide*』を参照してください。

ステップ 2　各宛先の Web セキュリティ アプライアンスにおいて、Web セキュリティ アプライアンスの既存の設定をコンフィギュレーション ファイルに保存します。詳細については、『*Cisco IronPort AsyncOS for Web Security User Guide*』を参照してください。

ステップ 3　セキュリティ管理アプライアンスで、[Web] > [ユーティリティ（Utilities）] > [Web アプライアンスへの公開（Publish to Web Appliances）] を選択します。

ステップ 4　[ジョブをスケジュールする（Schedule a Job）] をクリックします。

ステップ 5　デフォルトでは [システム生成のジョブ名（System-generated job name）] が選択されています。あるいはジョブ名（80 文字まで）を入力します。

ステップ 6　設定を公開する日時を入力します。

ステップ 7　[公開する設定マスター（Configuration Master to Publish）] で、[詳細ファイルオプション（Advanced file options）] を選択し、次に [参照（Browse）] をクリックして、ステップ 1 で保存したコンフィギュレーション ファイルを選択します。

ステップ 8　[Web アプライアンス（Web Appliances）] ドロップダウン リストから、[リスト内のアプライアンスを選択してください（Select appliances in list）] または [すべてがマスターに割り当てられました（All assigned to Master）] を選択して、コンフィギュレーション ファイルの公開先となるアプライアンスを選択します。

ステップ 9　[公開（Publish）] をクリックします。

公開ジョブのステータスと履歴の表示

スケジュール設定された公開ジョブの表示

スケジュール設定されているものの、まだ実行されていない公開ジョブの一覧を確認するには、[Web] > [ユーティリティ（Utilities）] > [Web アプライアンスへの公開（Publish to Web Appliances）] を選択して、[保留中のジョブ（Pending Jobs）] セクションを確認します。

現在の公開ジョブのステータスの表示

現在進行中の公開ジョブのステータスを確認するには、[Web] > [ユーティリティ（Utilities）] > [Web アプライアンスへの公開（Publish to Web Appliances）] を選択して、[公開の進歩ステータス（Publishing Progress）] セクションを確認します。

公開履歴の表示

公開履歴を表示すると、公開中に発生した可能性のあるエラーのチェックに役立ちます。

手順

ステップ 1　セキュリティ管理アプライアンスで、[Web] > [ユーティリティ（Utilities）] > [公開履歴（Publish History）] を選択します。

[公開履歴（Publish History）] ページには、試行された最近のすべての公開ジョブがリストされます。カラム情報には、ジョブ名、ジョブ完了時刻、使用された Configuration Master（または、拡張ファイル公開を実行した場合は XML コンフィギュレーション ファイルの名前）、ジョブの公開先にしたアプライアンスの数、およびステータス（[成功（Success）] または [失敗（Failure）]）があります。

ステップ 2　特定のジョブに関してさらに詳細を表示するには、[ジョブ名（Job Name）] カラムで特定のジョブ名のハイパーテキスト リンクをクリックします。

ステップ 3　[公開履歴：ジョブの詳細（Publish History: Job Details）] ページでは、アプライアンス名をクリックすることにより、[Web] > [ユーティリティ（Utilities）] > [Web アプライアンス ステータス（Web Appliance Status）] ページを表示して、ジョブの特定のアプライアンスに関する追加の詳細を表示できます。ジョブの特定のアプライアンスに関するステータスの詳細を表示することもでき、対応する [詳細（Details）] リンクをクリックして [Web アプライアンス公開の詳細（Web Appliance Publish Details）] ページに詳細を表示します。

[Web アプライアンス ステータス（Web Appliance Status）] ページの [Web アプライアンス サービス（Web Appliance Service）] カラムのステータスと、[管理アプライアンスに表示されているサービス（Is Service Displayed on Management Appliance?）] カラムのステータスに不一致があると、公開処理が失敗します。両方のカラムで、機能がイネーブルになっているものの、対応するライセンス キーがアクティブになっていない場合（期限切れなど）にも、公開処理が失敗します。

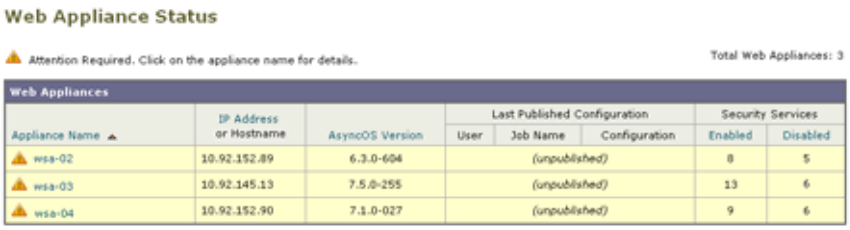
Web セキュリティ アプライアンスのステータスの表示

[Web アプライアンス ステータス（Web Appliances Status）] ページ

[Web] > [ユーティリティ（Utilities）] > [Web アプライアンス ステータス（Web Appliance Status）] ページには、ご使用のセキュリティ管理アプライアンスに接続されている Web セキュリティ アプライアンスの高レベルな概要が表示されます。

（注）　表示可能なデータがあるのは、集中管理をサポートするマシンのみです。

図 9-1　[Web アプライアンス ステータス（Web Appliances Status）] ページ



（注）　Web セキュリティ アプライアンスの Acceptable Use Control Engine の各種バージョンが、セキュリティ管理アプライアンスのバージョンと一致しない場合は、警告メッセージが表示されます。そのサービスが Web セキュリティ アプライアンスでディセーブルになっているか、そこに存在しない場合は、[N/A] と表示されます。

[Web アプライアンス ステータス（Web Appliance Status）] ページには、接続されている Web セキュリティ アプライアンスのリストが、アプライアンス名、IP アドレス、AsyncOS バージョン、最後に公開された設定情報（ユーザ、ジョブ名、コンフィギュレーション バージョン）、使用可能または使用不可にされているセキュリティ サービスの数、および接続しているアプライアンスの総数（最大 150）とともに表示されます。警告アイコンは、接続されたアプライアンスの 1 つに注意が必要なことを示しています。

（注）　Web セキュリティ アプライアンスで発生した最新の設定変更が [Web アプライアンス ステータス（Web Appliance Status）] ページに反映されるまでに、数分かかることがあります。データをすぐに更新するには、[データの更新（Refresh Data）] リンクをクリックします。ページのタイム スタンプは、データが最後にリフレッシュされた時刻を示しています。

[アプライアンス ステータス（Appliance Status）] ページ

[アプライアンス ステータス（Appliance Status）] ページには、接続されている各アプライアンスの状態が詳細に表示されます。

[Web アプライアンス ステータス（Web Appliance Status）] ページで管理対象 Web セキュリティ アプライアンスの詳細を表示するには、アプライアンスの名前をクリックします。

ステータス情報としては、接続されている Web セキュリティ アプライアンスに関する一般情報、それらの公開された設定、公開履歴、ライセンス キーのステータスなどがあります。

[アプライアンス ステータス（Appliance Status）] ページには、複数のセクションがあります。

- 「[Web アプライアンス ステータスの詳細（Web Appliance Status Details）] ページ：システム ステータス、設定の公開履歴、および中央集中型レポーティングのステータス」
- 「[Web アプライアンス ステータスの詳細（Web Appliance Status Details）] ページ：セキュリティ サービス セクション」
- 「[Web アプライアンス ステータスの詳細（Web Appliance Status Details）] ページ：AnyConnect セキュア モビリティ、プロキシ、および認証の設定」

図 9-2　[Web アプライアンス ステータスの詳細（Web Appliance Status Details）] ページ：システム ステータス、設定の公開履歴、および中央集中型レポーティングのステータス

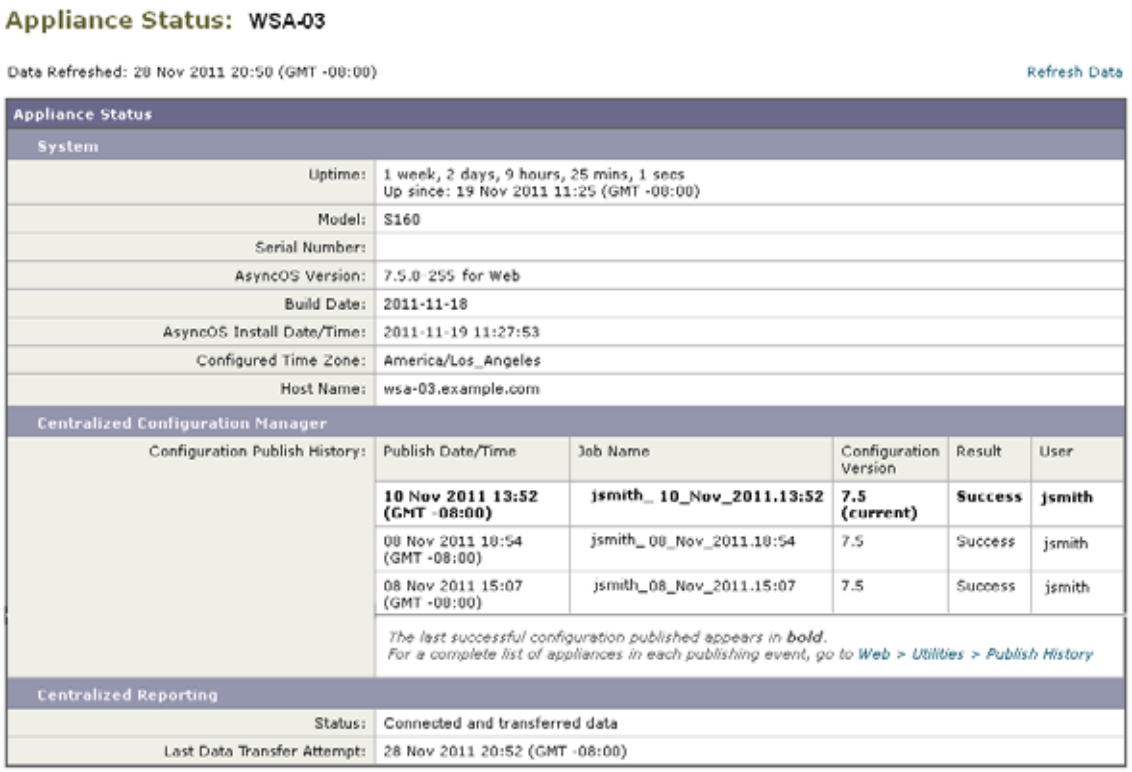


図 9-3　[Web アプライアンス ステータスの詳細（Web Appliance Status Details）] ページ：セキュリティ サービス セクション

Security Services

⚠ *One or more of the services on the Web Appliance does not match the corresponding Security Service Display setting on the Management Appliance.*

Description	Services		Feature Keys		
	Web Appliance Service	Is Service Displayed on Management Appliance?	Status	Time Remaining	Expiration Date
Cisco IronPort Web Proxy & DVS(TM) Engine	Enabled	Yes	Active	Perpetual	N/A
Cisco IronPort L4 Traffic Monitor	N/A	N/A	N/A	N/A	N/A
Proxy Mode	Forward	No (Bypass Proxy)			
FTP Proxy	Enabled	Yes			
Cisco IronPort HTTPS Proxy	Enabled	Yes	Active	Perpetual	N/A
SOCKS Proxy	Disabled	Yes			
Upstream Proxy Groups	Not Configured	No (Routing Policies)			
AnyConnect Secure Mobility	Cisco ASA	Yes (Cisco ASA)	Active	Perpetual	N/A
Cisco IronPort Web Usage Controls	Enabled	Yes	Active	Perpetual	N/A
Application Visibility and Control	Enabled	Yes			
Cisco IronPort Centralized Web Reporting	Enabled	Yes			
Cisco IronPort Web Reputation Filters	Enabled	Yes	Active	Perpetual	N/A
Adaptive Scanning	Disabled	No			
Webroot Anti-Malware	Enabled	Yes	Active	Perpetual	N/A
McAfee Anti-Malware	Enabled	Yes	Active	Perpetual	N/A
Sophos Antivirus	Enabled	Yes	Active	Perpetual	N/A
End-User Acknowledgement	Enabled	Yes			
Cisco IronPort Data Security Filters	Enabled	Yes			
External DLP Servers	Not Configured	No			
Credential Encryption	Disabled	No			
Identity Provider for SaaS	Not Configured	No			
Acceptable Use Controls Engine Updates					
Update Type	Web Appliance Version	Management Appliance Version			
Web Categorization Categories List	1337225318	1337225318			
Application Visibility and Control Data	1346296993	1346296993			

図 9-4　[Web アプライアンス ステータスの詳細（Web Appliance Status Details）] ページ：AnyConnect セキュア モビリティ、プロキシ、および認証の設定

AnyConnect Secure Mobility Settings

Cisco ASA:	[IP address and port go here]

Proxy Settings

Upstream Proxies:	*No upstream proxies configured.*
HTTP Ports to Proxy:	[Port goes here]

Authentication Service

Authentication Realms:	Name	Protocol	Servers	Support Transparent User Identification
	NTLM AUTH	NTLM	ad.example.com	No
	LDAP AUTH	LDAP	ad.example.com	No
Authentication Sequences:	Name		Order of Realms	
	All Realms		NTLMSSP: NTLM AUTH Basic: NTLM AUTH, LDAP AUTH	
Unreachable Authentication Service Action:	Block all traffic if authentication fails			

詳細には次の情報が含まれます。

- セキュリティ ステータス情報（稼働時間、アプライアンス モデル、シリアル番号、AsyncOS のバージョン、ビルド日、AsyncOS のインストール日時、ホスト名）
- 設定公開履歴（公開日時、ジョブ名、コンフィギュレーション バージョン、公開の結果、ユーザ）
- 直近に試行されたデータ転送の時刻など、中央集中型レポーティングのステータス
- Web セキュリティ機能のステータス（機能説明、設定のサマリー、セキュリティ サービスの設定、ライセンス キーのステータス）
- この情報は、使用するアプライアンスに中央集中型管理を設定する場合に使用します。
- 管理対象および管理側のアプライアンスの Acceptable Use Controls Engine のバージョン
- AnyConnect セキュア モビリティの設定
- プロキシ設定（アップストリーム プロキシとプロキシの HTTP ポート）
- 認証サービス（名前、プロトコル、認証レルムのサーバ、認証手順におけるレルムの名前と順序、トランスペアレント ユーザ ID のサポートの有無、認証に失敗した場合のトラフィックのブロックまたは許可）

ヒント　Web セキュリティ アプライアンスに変更を加えたときや、アプライアンスに対する情報を表示できないというメッセージが表示された場合に詳細をリフレッシュするには、[データの更新（Refresh Data）] リンクをクリックします。ページのタイム スタンプは、データが最後にリフレッシュされた時刻を示しています。

URL カテゴリ セットの更新と中央集中型コンフィギュレーション管理

URL カテゴリ セットの更新は、Configuration Master 7.5 以降に対してのみ適用されます。

システムで Web の使用率を管理するために事前定義されている URL カテゴリを最新の状態に維持するためには、Cisco IronPort Web Usage Controls（WUC）の URL カテゴリ セットを時折更新します。デフォルトでは、Web セキュリティ アプライアンスセキュリティ管理アプライアンスが URL カテゴリ セットをシスコから自動的にダウンロードし、Web セキュリティ アプライアンスがこれらの更新を管理対象のから数分以内に自動的に受信します。更新された URL カテゴリ セットは、Configuration Master 7.5 以降の ID とアプライアンス ポリシーにただちに表示されます。

以下のことを実施してください。

- 「URL カテゴリ セットの更新による影響の理解」（P.9-24）
- 「URL カテゴリ セットの更新に関するアラートを受信」（P.9-25）
- 「Configuration Master 7.5 および 7.7 を設定する前の注意事項」（P.9-25）
- 「新規または変更されたカテゴリのデフォルト設定の指定」（P.9-25）
- 「URL カテゴリ セットの更新時にポリシーと ID の設定を確認」（P.9-25）

URL カテゴリ セットの更新による影響の理解

URL カテゴリ セットの更新の前後に実行する手順の重要な説明については、「マニュアル」（P.1-4）のリンクに掲載されている、『*Cisco IronPort AsyncOS for Web Security User Guide*』の「Managing Updates to the Set of URL Categories」の章を参照してください。カテゴリについては、同じ章の「URL Category Descriptions」で説明されています。

URL カテゴリ セットの更新に関するアラートを受信

Configuration Master のポリシー設定に影響を及ぼす URL カテゴリ セットの更新について、アラートを受信するようにするには、[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [アラート（Alerts）] を選択し、[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設定します。アラートについての詳細は、「アラートの管理」（P.14-33）を参照してください。

Configuration Master 7.5 および 7.7 を設定する前の注意事項

Configuration Master 7.1 の設定を Configuration Master 7.5 または 7.7 にコピーまたはインポートすると、URL カテゴリを参照するすべての ID およびポリシーが Configuration Master 7.5 および 7.7 で変更されます。この代わりとして、正しく設定された Web セキュリティ アプライアンスからコンフィギュレーション ファイルをインポートすることができます。また、コピーまたはインポートする前に Configuration Master 7.1 の各ポリシーについて未分類の URL 設定を評価することもできます。

新規または変更されたカテゴリのデフォルト設定の指定

将来、URL カテゴリ セットが更新されると、既存の Configuration Master 7.5 以降のポリシーの動作が変化する可能性があります。URL カテゴリ セットを更新する前に、URL フィルタリングを行うポリシーの新規カテゴリやマージされたカテゴリにデフォルトの動作を指定するか、これらがすでに設定されている Web セキュリティ アプライアンスから設定をインポートする必要があります。

詳細については、『*User Guide for Cisco IronPort AsyncOS for Web Security*』の「URL Filters」の章にある「Choosing Default Settings for New and Changed Categories」項、または Web セキュリティ アプライアンスのオンライン ヘルプを参照してください。

URL カテゴリ セットの更新時にポリシーと ID の設定を確認

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

- カテゴリの変更についてのアラート
- カテゴリの変更によって変更された、またはディセーブルにされたポリシーについてのアラート

URL カテゴリ セットの変更に関するアラートを受信した場合は、Configuration Master 7.5 以降で既存の URL カテゴリに基づくポリシーと ID を確認して、それらが引き続きポリシーの目的を満たしていることを確認してください。

注意が必要な変更の詳細については、「マニュアル」（P.1-4）のリンクに掲載されている、『*Cisco IronPort for Web Security User Guide*』の「Responding to Alerts about URL Category Set Updates」を参照してください。

CHAPTER 10

システム ステータスのモニタリング

セキュリティ管理アプライアンス ステータスについて

デフォルトでは、[システム ステータス（System Status）] ページはブラウザからシスコ コンテンツセキュリティ管理アプライアンスにアクセスするときに最初に表示されるページです。（ランディング ページを変更するには、「プリファレンスの 設定」（P.14-58）を参照してください）

それ以外の場合に [システム ステータス（System Status）] ページにアクセスするには、[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] >[システム ステータス（System Status）] を選択します。

サービスのモニタリングをイネーブルにして、管理対象アプライアンスを追加するまでは、[システム情報（System Information）] セクションでのみステータス情報が提供されます。システム セットアップ ウィザードを実行し、集約管理サービスを有効にして、管理対象アプライアンスを追加すると、[集約管理サービス（Centralized Services）] セクションおよび [セキュリティアプライアンスデータ転送ステータス（Security Appliance Data Transfer Status）] セクションにデータが表示されます。

ステータス情報には、次の内容が含まれます。

- **集約管理サービス：**処理キューの使用状況などの各集約管理サービスの状態、
- **システム稼働時間：**アプライアンスが動作している時間の長さ
- **CPU 使用率：**各モニタリング サービスによって使用されている CPU 容量
- **システム バージョン情報：**モデル番号、AsyncOS（オペレーティング システム）バージョン、インストール日、およびシリアル番号

関連項目

- 「キューの処理のモニタリング」（P.10-2）
- 「CPU 使用率のモニタリング」（P.10-2）

セキュリティ管理アプライアンス容量のモニタリング

キューの処理のモニタリング

電子メールと Web レポート、およびアプライアンスが最適な容量で実行されているかを判断するためのトラッキング レポートに使用される処理キューの使用率を定期的に確認できます。

処理キューには、セキュリティ管理アプライアンスによる処理を待機している集中型レポーティング ファイルおよびトラッキング ファイルが保存されます。通常、セキュリティ管理アプライアンスは、処理対象のレポーティング ファイルとトラッキング ファイルのバッチを受信します。処理キューのレポーティング ファイルまたはトラッキング ファイルの割合は、通常、ファイルが管理アプライアンスから転送され、セキュリティ管理アプライアンスで処理されると変動します。

（注）　処理キューの割合は、キューにあるファイルの数で測定されます。ファイル サイズは考慮されません。割合は、セキュリティ管理アプライアンスの処理負荷の概算のみが表示されます。

手順

ステップ 1　[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [システム ステータス（System Status）] を選択します。

ステップ 2　ページ上部の [集約管理サービス（Centralized Services）] セクションで、次に対する処理キューの割合を参照してください.

- [集約管理レポート（Centralized Reporting）]（[E メール セキュリティ（Email Security）] サブセクション）
- 集約メッセージトラッキング（Centralized Message Tracking）
- [集約管理レポート（Centralized Reporting）]（[Web セキュリティ（Web Security）] サブ セクション）

ステップ 3　処理キューの使用率が数時間または数日にわたって高いままである場合は、システムが容量以上に稼働しています。

この場合は、セキュリティ管理アプライアンスから管理対象アプライアンスをいくつか削除するか、追加の セキュリティ管理アプライアンスをインストールするか、その両方を行うことを検討してください。

CPU 使用率のモニタリング

各集約管理サービスでセキュリティ管理アプライアンスが使用している CPU 容量の割合を表示するには、以下の手順に従ってください。

ステップ 1　[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [システム ステータス（System Status）] を選択します。

ステップ 2　[システム情報（System Information）] セクションまでスクロールし、[CPU 使用率（CPU Utilization）] サブ セクションを表示します。

[CPU 使用率（CPU Utilization）] の割合は、セキュリティ管理アプライアンスの主要な集約管理サービスそれぞれに使われる CPU 処理の割合を示します。いくつかのサービスの使用率の割合は統合されている可能性があります。たとえば、電子メールと Web レポーティングは、「レポーティング サービス」の下に結合され、スパム、ポリシー、ウイルス、およびアウトブレイク隔離は「隔離サービス」の下に結合されます。セキュリティ管理アプライアンスの操作は、「セキュリティ管理アプライアンス」の汎用見出しの下にグループ化されます。

ステップ 3　最新のデータを表示するには、ブラウザを更新します。

CPU 使用率の割合は、常に変化します。

管理アプライアンスからのデータ転送のステータスのモニタリング

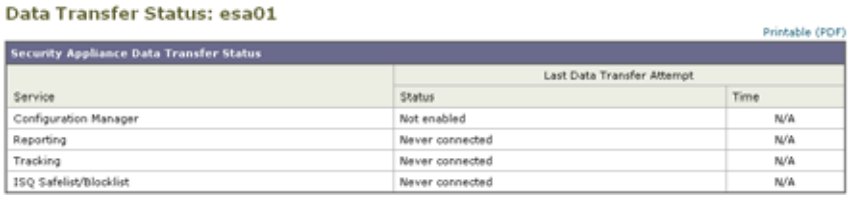
集中管理機能を実行するうえで、セキュリティ管理アプライアンスは、管理対象アプライアンスからセキュリティ管理アプライアンスにデータが正常に転送されることを前提としています。[セキュリティ アプライアンス データ転送ステータス（Security Appliance Data Transfer Status）] セクションでは、セキュリティ管理アプライアンスに管理される各アプライアンスのステータス情報が表示されます。

デフォルトで、[セキュリティ アプライアンス データ転送ステータス（Security Appliance Data Transfer Status）] セクションには最大 10 台のアプライアンスが表示されます。セキュリティ管理アプライアンスが 10 台を超えるアプライアンスを管理する場合、[表示されたアイテム（Items Displayed）] メニューを使用して表示するアプライアンスの数を選択できます。

（注）　[システム ステータス（System Status）] ページの [サービス（Services）] セクションに、データ転送ステータスの概要情報が表示されます。[セキュリティ アプライアンス データ転送ステータス（Security Appliance Data Transfer Status）] セクションには、アプライアンス固有のデータ転送ステータスが表示されます。

[システム ステータス（System Status）] ページの [セキュリティ アプライアンス データ転送ステータス（Security Appliance Data Transfer Status）] セクションで、特定のアプライアンスの接続ステータスの問題を表示できます。アプライアンスの各サービスのステータスに関する詳細情報については、アプライアンス名をクリックしてアプライアンスの [データ転送ステータス（Data Transfer Status）] ページを表示します。

図 10-1　[データ転送ステータス（Data Transfer Status）: <アプライアンス名>] ページ


Data Transfer Status: esa01

Printable (PDF)

Security Appliance Data Transfer Status		
	Last Data Transfer Attempt	
Service	Status	Time
Configuration Manager	Not enabled	N/A
Reporting	Never connected	N/A
Tracking	Never connected	N/A
ISQ Safelist/Blocklist	Never connected	N/A

[データ転送ステータス（Data Transfer Status）：*アプライアンス名*] ページには、各モニタリング サービスで最後にデータ転送が発生した時刻が表示されます。

電子メール セキュリティ アプライアンスのデータ転送ステータスは、次のいずれかの値になります。

- [無効（Not enabled）]：モニタリング サービスが 電子メール セキュリティ アプライアンスでイネーブルになっていません。
- [接続されていません（Never connected）]：モニタリング サービスは 電子メール セキュリティ アプライアンスでイネーブルになっていますが、電子メール セキュリティ アプライアンスと セキュリティ管理アプライアンスの間で接続が確立されていません。
- [データ待機中（Waiting for data）]：電子メール 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と接続されていて、データの受信を待機しています。
- [接続し、データ転送されました（Connected and transferred data）]：電子メール セキュリティ アプライアンスと セキュリティ管理アプライアンスの間で接続が確立され、データが正常に転送されました。
- [ファイル転送失敗（File transfer failure）]：電子メール セキュリティ アプライアンスと セキュリティ管理アプライアンスの間で接続が確立されましたが、データ転送に失敗しました。

Web セキュリティ アプライアンスのデータ転送ステータスは、次のいずれかの値になります。

- [無効（Not enabled）]：中央集中型コンフィギュレーション マネージャは、Web セキュリティ アプライアンスでイネーブルになっていません。
- [接続されていません（Never connected）]：中央集中型コンフィギュレーション マネージャは Web セキュリティ アプライアンスでイネーブルになっていますが、Web セキュリティ アプライアンスと セキュリティ管理アプライアンスの間で接続が確立されていません。
- [データ待機中（Waiting for data）]：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と接続されていて、データの受信を待機しています。
- [接続し、データ転送されました（Connected and transferred data）]：Web セキュリティ アプライアンスと セキュリティ管理アプライアンスの間で接続が確立され、データが正常に転送されました。
- [設定転送失敗（Configuration push failure）]：セキュリティ管理アプライアンスがコンフィギュレーション ファイルを Web セキュリティ アプライアンスにプッシュしようとしましたが、転送に失敗しました。
- [設定転送保留（Configuration push pending）]：セキュリティ管理アプライアンスが Web セキュリティ アプライアンスにコンフィギュレーション ファイルをプッシュする処理中です。
- [設定転送成功（Configuration push success）]：セキュリティ管理アプライアンスは Web セキュリティ アプライアンスにコンフィギュレーション ファイルを正常にプッシュしました。

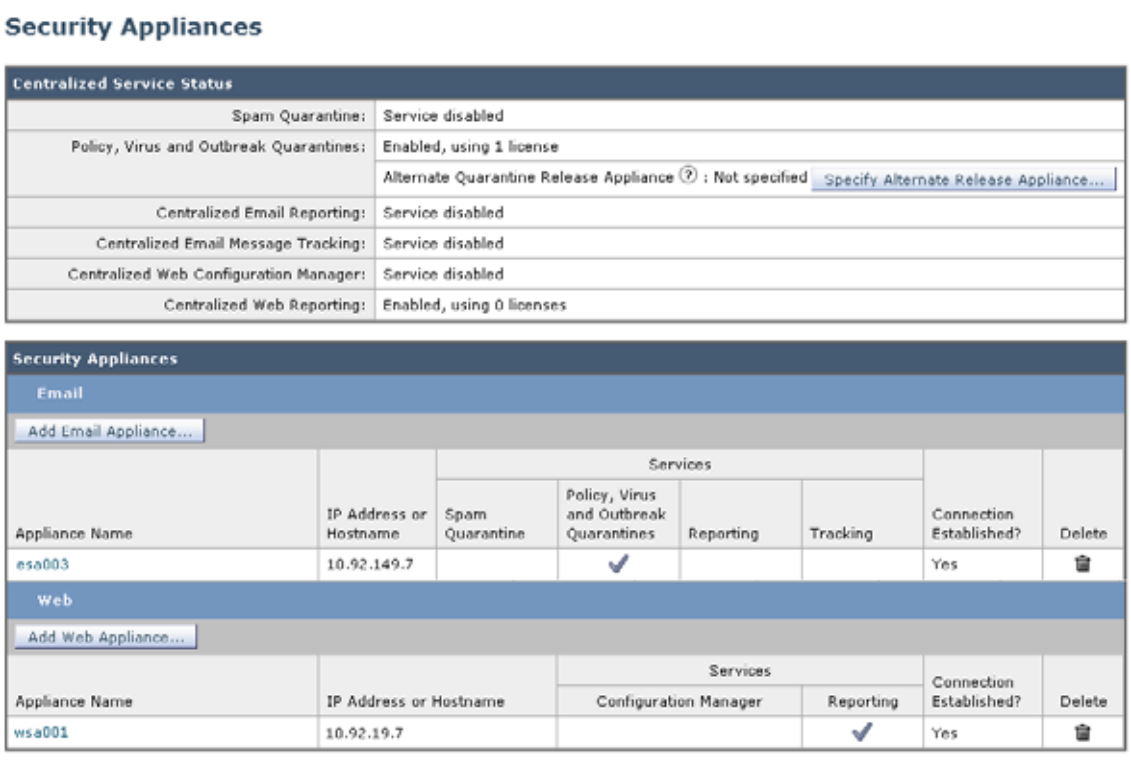
データ転送の問題は、一時的なネットワークの問題またはアプライアンスの設定の問題を反映していることがあります。ステータス [接続されていません（Never connected）] および [データ待機中（Waiting for data）] は、最初に管理対象アプライアンスをセキュリティ管理アプライアンスに追加し

たときの、通常の移行ステータスです。ステータスが最終的に [接続し、データ転送されました（Connected and transferred data）] に変化しなかった場合、このデータ転送ステータスは、設定の問題を示している可能性があります。

アプライアンスに [ファイル転送失敗（File transfer failure）] ステータスが表示された場合は、そのアプライアンスをモニタして、その失敗がネットワークの問題によるものなのか、アプライアンスの設定の問題によるものなのかを判断します。データを転送できない理由がネットワークの問題ではなく、ステータスが [接続し、データ転送されました（Connected and transferred data）] に変化しない場合、データ転送ができるようにアプライアンスの設定を変更する必要があります。

管理対象アプライアンスの設定ステータスの表示

セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [セキュリティ アプライアンス（Security Appliances）] を選択します。



[集約サービスのステータス（Centralized Service Status）] セクションに、有効化されているサービスと、サービスごとに使用中のライセンス数が表示されます。[セキュリティ アプライアンス（Security Appliances）] セクションには、追加したアプライアンスがリスト表示されます。チェック マークは、イネーブルになっているサービスを示し、[接続が確立されていますか？（Connection Established?）] カラムは、ファイル転送アクセスが正しく設定されているかどうかを示します。

関連項目

- 「リリースされたメッセージを処理する代替アプライアンスの指定」（P.8-8）
- 「管理対象アプライアンスの追加について」（P.2-12）

Web セキュリティ アプライアンスの追加ステータス情報

Web セキュリティ アプライアンスに関する追加ステータス情報については、「Web セキュリティ アプライアンスのステータスの表示」（P.9-21）を参照してください。

レポーティング データ アベイラビリティ ステータスのモニタリング

セキュリティ管理アプライアンスによって、指定された期間のレポーティング データのアベイラビリティをモニタできるようになります。アプライアンスに応じたセクションを参照してください。

- 「電子メール セキュリティ レポート データの可用性のモニタリング」（P.10-6）
- 「Web セキュリティ レポート データの可用性のモニタリング」（P.10-7）

電子メール セキュリティ レポート データの可用性のモニタリング

セキュリティ管理アプライアンスで電子メール セキュリティ アプライアンスからのレポーティング データをモニタするには、[メール（Email）] > [レポート（Reporting）] > [有効なレポート データ（Reporting Data Availability）] ページを表示します。

図 10-2　[有効なレポート データ（Reporting Data Availability）] ページ

[有効なレポート データ（Reporting Data Availability）] ページから、指定された期間に セキュリティ管理アプライアンスが 電子メール セキュリティ アプライアンスから受信したレポーティング データの割合を表示できます。棒グラフは、時間範囲内に受信したデータの完全性を示します。

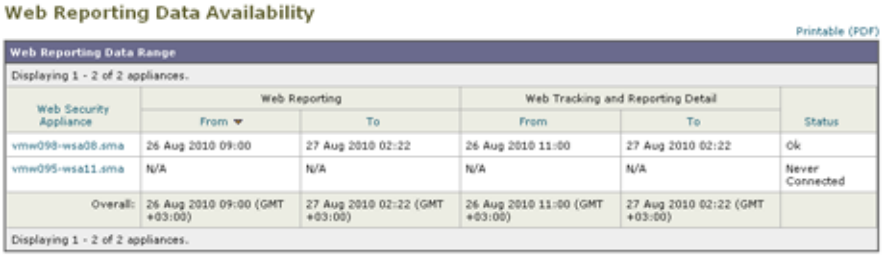
レポーティング データ アベイラビリティは、前の日、週、年についてモニタできます。セキュリティ管理アプライアンスが 電子メール セキュリティ アプライアンスから受信したレポーティング データが 100% 未満の場合は、データが不完全なことがすぐにわかります。データ アベイラビリティ情報を使用して、レポーティング データの検証およびシステムの問題のトラブルシューティングができます。

（注）　ハードウェア障害または他の理由で、電子メール セキュリティ アプライアンスの交換が必要になった場合、置き換えられた電子メール セキュリティ アプライアンスからのデータは失われませんが、そのデータはセキュリティ管理アプライアンスで正常に表示されません。

Web セキュリティ レポート データの可用性のモニタリング

セキュリティ管理アプライアンスで Web セキュリティ アプライアンスからのレポーティング データをモニタするには、[Web] > [レポート（Reporting）] > [使用可能なデータ（Data Availability）] ページを表示します。

[使用可能なデータ（Data Availability）] ページからデータの更新およびソートができ、リソース使用率および Web トラフィックの問題箇所をリアルタイムに表示できます。


Web Reporting Data Availability

Printable (PDF)

Web Reporting Data Range

Displaying 1 - 2 of 2 appliances.

Web Security Appliance	Web Reporting		Web Tracking and Reporting Detail		Status
	From	To	From	To	
vmw098-wsa08.sma	26 Aug 2010 09:00	27 Aug 2010 02:22	26 Aug 2010 11:00	27 Aug 2010 02:22	Ok
vmw095-wsa11.sma	N/A	N/A	N/A	N/A	Never Connected
Overall:	26 Aug 2010 09:00 (GMT +03:00)	27 Aug 2010 02:22 (GMT +03:00)	26 Aug 2010 11:00 (GMT +03:00)	27 Aug 2010 02:22 (GMT +03:00)	

Displaying 1 - 2 of 2 appliances.

（注）　[有効な Web レポート データ（Web Reporting Data Availability）] ウィンドウでは、Web Reporting と Email Reporting の**両方が**ディセーブルの場合にのみ、Web Reporting がディセーブルであると表示されます。

このページから、すべてのデータ リソース使用率および Web トラフィックの問題箇所を表示できます。リスト表示されている Web セキュリティ アプライアンス リンクのいずれかをクリックすると、そのアプライアンスのレポーティング データ アベイラビリティを表示できます。

レポーティング データ アベイラビリティは、前の日、週、年についてモニタできます。セキュリティ管理アプライアンスが Web セキュリティ アプライアンスから受信したレポーティング データが 100% 未満の場合は、データが不完全なことがすぐにわかります。データ アベイラビリティ情報を使用して、レポーティング データの検証およびシステムの問題のトラブルシューティングができます。

URL カテゴリに関するスケジュール設定されたレポート内でデータ アベイラビリティが使用されている場合に、いずれかのアプライアンスでデータに欠落があると、ページの下部に「この時間範囲の一部のデータは使用不可でした。(Some data in this time range was unavailable.)」というメッセージが表示されます。欠落がない場合は何も表示されません。

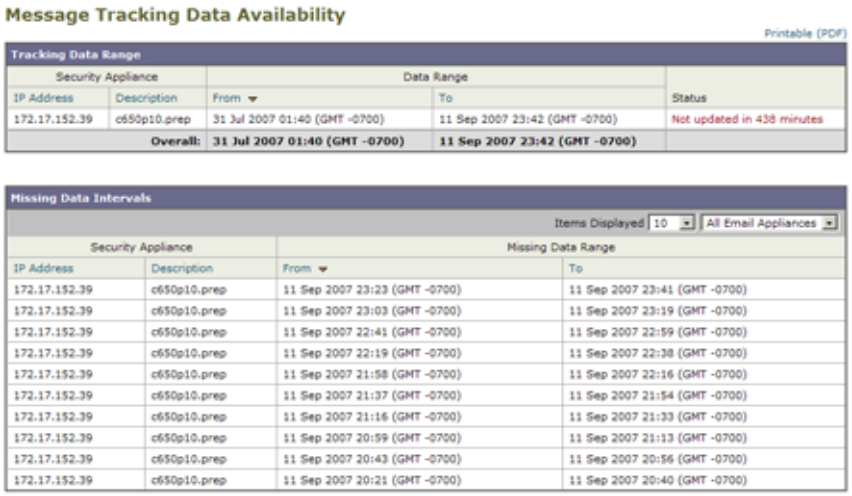
Web セキュリティ アプライアンスの [使用可能なデータ（Data Availability）] ページの詳細については、「[使用可能なデータ（Data Availability）] ページ」を参照してください。

電子メール トラッキング データ ステータスのモニタリング

電子メール トラッキング データのステータスをモニタするには、[メール（Email）] > [メッセージ トラッキング（Message Tracking）] > [有効なメッセージ トラッキング データ（Message Tracking Data Availability）] ページを表示します。

（注）　電子メール セキュリティ アプライアンスは、アプライアンスから取得したレポーティング データとトラッキング データのコピーを作成し、データ ファイルのコピーをデフォルト ディレクトリとは別の追加フォルダに保存します。次に、これらのフォルダのいずれかからデータを取り出すように、セキュリティ管理アプライアンスを設定できます。

図 10-3　[有効なメッセージ トラッキング データ（Message Tracking Data Availability）] ページ



[有効なメッセージ トラッキング データ（Message Tracking Data Availability）] ページによって、セキュリティ管理アプライアンスに対するデータ欠落インターバルを表示できるようになります。データ欠落インターバルは、セキュリティ管理アプライアンスが組織の電子メール セキュリティ アプライアンスからメッセージ トラッキング データを受信しなかった期間です。

特定の管理対象アプライアンス、またはシステムにあるすべての電子メール セキュリティ アプライアンスのデータ アベイラビリティをモニタできます。メッセージ トラッキング データのデータ欠落インターバルが検出された場合は、データが不完全なことがすぐにわかります。データ アベイラビリティ情報を使用して、メッセージ トラッキング データの検証およびシステムの問題のトラブルシューティングができます。

管理対象アプライアンスのキャパシティのモニタリング

セキュリティ管理アプライアンスからの管理対象アプライアンスの容量をモニタできます。すべての電子メールまたは Web セキュリティ アプライアンスの総合的な容量および個別のアプライアンスの容量を確認できます。

表示する容量	参照先
管理対象の Web セキュリティ アプライアンス	「[システム容量（System Capacity）] ページ」（P.5-61）
管理対象の電子メール セキュリティ アプライアンス	「[システム容量（System Capacity）] ページ」（P.4-44）

アクティブな TCP/IP サービスの識別

セキュリティ管理アプライアンスで使用されるアクティブな TCP/IP サービスを識別するには、コマンドライン インターフェイスで tcpservices コマンドを使用します。

CHAPTER 11

LDAP との統合

概要

企業の LDAP ディレクトリ（例：Microsoft Active Directory、SunONE Directory Server、または OpenLDAP ディレクトリなど）のエンド ユーザのパスワードおよび電子メール エイリアスを管理する場合、LDAP ディレクトリを使用して次のユーザを認証することができます。

- Cisco IronPort スパム隔離にアクセスするエンド ユーザおよび管理ユーザ。

  ユーザが Cisco IronPort スパム隔離の Web UI にログインする場合、LDAP サーバはログイン名とパスワードを検証し、AsyncOS は対応する電子メール エイリアスのリストを取得します。そのユーザの電子メール エイリアスのいずれかに送信された隔離メッセージは、アプライアンスが書き換えない限り Cisco IronPort スパム隔離で表示できます。

  「Cisco IronPort スパム隔離と連携させるための LDAP の設定」（P.11-1）を参照してください。

- 外部認証が有効に設定されている場合、シスコのコンテンツセキュリティ管理アプライアンスに署名する管理ユーザ。

  「LDAP を使用した管理ユーザの外部認証の設定」（P.11-14）を参照してください。

Cisco IronPort スパム隔離と連携させるための LDAP の設定

シスコ コンテンツ セキュリティ アプライアンスを LDAP ディレクトリと連携させるには、以下の手順に従って、受け入れ、ルーティング、エイリアシング、およびマスカレードを設定する必要があります。

手順

ステップ 1　**LDAP サーバ プロファイルを設定します。**

サーバ プロファイルの内容は、AsyncOS から LDAP サーバに接続するための、次のような情報です。

- サーバ名およびポート
- ベース DN
- サーバをバインディングするための認証要件

サーバ プロファイルの設定方法の詳細については、「LDAP サーバ プロファイルの作成」（P.11-2）を参照してください。

LDAP サーバ プロファイルを作成するときに、AsyncOS からの接続先となる LDAP サーバを複数設定できます。詳細については、「AsyncOS を複数の LDAP サーバと連携させるための設定」（P.11-11）を参照してください。

ステップ 2　**LDAP クエリーを設定します。**

LDAP サーバ プロファイル用に生成されたデフォルトのスパム隔離クエリーを使用するか、または実際に使用する LDAP の実装とスキーマに合わせて自分のクエリーを作成することができます。次に、スパム通知、および隔離へのエンドユーザ アクセス検証に使用するアクティブ クエリーを指定します。

クエリーの詳細については、「LDAP クエリーの設定」（P.11-4）を参照してください。

ステップ 3　**Cisco IronPort スパム隔離に対して、LDAP エンドユーザ アクセスおよびスパム通知をイネーブルにします。**

Cisco IronPort スパム隔離に対するエンドユーザ アクセスをイネーブルにして、エンドユーザが隔離メッセージを表示したり管理したりできるようにします。ユーザが複数の通知を受信しないように、スパム通知のエイリアス統合をイネーブルにすることもできます。

詳細については、「中央集中型スパム隔離の設定」（P.7-2）を参照してください。

LDAP サーバ プロファイルの作成

LDAP ディレクトリを使用するように AsyncOS を設定した場合は、LDAP サーバに関する情報を保存するために LDAP サーバ プロファイルを作成します。

手順

ステップ 1　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [LDAP] を選択します。

ステップ 2　[LDAP サーバ プロファイルを追加（Add LDAP Server Profile）] をクリックします。

ステップ 3　[LDAP サーバ プロファイル名（LDAP Server Profile Name）] テキスト フィールドにサーバ プロファイルの名前を入力します。

ステップ 4　[ホスト名（Host Name(s)）] テキスト フィールドに、LDAP サーバのホスト名を入力します。

複数のホスト名を入力すると、LDAP サーバのフェールオーバーやロード バランシングができるようになります。複数のエントリを指定する場合は、カンマで区切ります。詳細については、「AsyncOS を複数の LDAP サーバと連携させるための設定」（P.11-11）を参照してください。

ステップ 5　認証方式を選択します。匿名認証を使用することも、ユーザ名とパスワードを指定することもできます。

（注）　レポート上のクライアント IP アドレスではなくクライアント ユーザ ID を表示するには、LDAP 認証を設定する必要があります。LDAP 認証を使用しない場合、システムでは IP アドレスによるユーザの参照のみができます。[パスワードを使用（Use Password）] オプション ボタンを選択して、ユーザ名とパスワードを入力します。[内部ユーザのサマリー（Internal Users Summary）] ページにユーザ名が表示されます。

ステップ 6　LDAP サーバ タイプを、[Active Directory]、[OpenLDAP]、または [不明またはそれ以外（Unknown or Other）] から選択します。

ステップ 7　ポート番号を入力します。

デフォルト ポートは 3268 です。これは、複数台のサーバ環境でグローバル カタログへのアクセスをイネーブルにする Active Directory 用のデフォルト ポートです。

ステップ 8　LDAP サーバのベース DN（識別名）を入力します。

ユーザ名とパスワードで認証を行う場合、ユーザ名にはパスワードが含まれているエントリの完全 DN が含まれている必要があります。たとえば、電子メール アドレスが joe@example.com というユーザがマーケティング グループのユーザだとします。このユーザ用のエントリは、次のエントリのようになります。

```
uid=joe, ou=marketing, dc=example dc=com
```

ステップ 9　[拡張（Advanced）] で、LDAP サーバとの通信に SSL を使用するかどうかを選択します。

ステップ 10　キャッシュ存続可能時間を入力します。この値は、キャッシュを保持する時間の長さです。

ステップ 11　保持するキャッシュ エントリの最大数を入力します。

ステップ 12　同時接続の最大数を入力します。

ロード バランシングのために LDAP サーバ プロファイルを設定する場合、これらの接続はリストで指定された LDAP サーバ間で配分されます。たとえば、同時接続数を 10 と設定し、3 台のサーバを使用して接続のロード バランシングを行う場合は、AsyncOS によってサーバへの接続が 10 ずつ作成され、接続の総数は 30 となります。詳細については、「ロード バランシング」（P.11-13）を参照してください。

（注）　同時接続の最大数には、LDAP クエリーに使用される LDAP 接続が含まれます。ただし、Cisco IronPort スパム隔離のための LDAP 認証をイネーブルにする場合、アプライアンスはエンド ユーザ隔離に対して 20 の追加接続を許可し、接続の総数は 30 となります。

ステップ 13　サーバへの接続をテストするために、[テスト サーバ（Test Server(s)）] ボタンをクリックします。複数の LDAP サーバを指定した場合は、すべてのサーバのテストが実行されます。テストの結果が [接続ステータス（Connection Status）] フィールドに表示されます。詳細については、「LDAP サーバのテスト」（P.11-4）を参照してください。

ステップ 14　スパム隔離クエリーを作成します。該当するチェックボックスをオンにして、フィールドに入力します。

ユーザがエンドユーザ隔離にログインするときにそのユーザを検証する、隔離エンドユーザ認証クエリーを設定できます。エンドユーザが電子メール エイリアスごとに隔離通知を受け取らないように、エイリアス統合クエリーを設定できます。これらのクエリーを使用するには、[有効なクエリとして指定する（Designate as the active query）] チェックボックスをオンにします。詳細については、「LDAP クエリーの設定」（P.11-4）を参照してください。

ステップ 15　[クエリのテスト（Test Query）] ボタンをクリックして、スパム隔離クエリーをテストします。

テスト パラメータを入力して [テストの実行（Run Test）] をクリックします。テストの結果が [接続ステータス（Connection Status）] フィールドに表示されます。クエリーの定義や属性に変更を加えた場合は、[更新（Update）] をクリックします。

（注）　空パスワードでのバインドを許可するように LDAP サーバが設定されている場合は、パスワード フィールドが空でもクエリーのテストは合格となります。

ステップ 16　変更を送信し、保存します。

Active Directory サーバ設定では、Windows 2000 で TLS 経由の認証が許可されません。これは、Active Directory の既知の問題です。Active Directory および Windows 2003 の TLS 認証は、動作します。

（注）　サーバ設定の数は無制限ですが、サーバごとに、エンドユーザ認証クエリーを 1 つとエイリアス統合クエリーを 1 つだけ設定できます。

LDAP サーバのテスト

[LDAP サーバ プロファイルを追加/編集（Add/Edit LDAP Server Profile）] ページの [テスト サーバ（Test Server(s)）] ボタン（または CLI の `ldapconfig` コマンドの `test` サブコマンド）を使用して、LDAP サーバへの接続をテストします。サーバ ポートへの接続に成功したか失敗したかを示すメッセージが表示されます。複数の LDAP サーバを設定した場合は、AsyncOS によって各サーバがテストされ、結果が個別に表示されます。

LDAP クエリーの設定

次のセクションで、Cisco IronPort スパム隔離クエリーのタイプごとに、デフォルトのクエリー文字列と設定の詳細を示します。

- **スパム隔離へのエンドユーザ認証のクエリー。**詳細については、「スパム隔離へのエンドユーザ認証のクエリー」（P.11-5）を参照してください。
- **スパム隔離のエイリアス統合のクエリー。**詳細については、「スパム隔離のエイリアス統合クエリー」（P.11-7）を参照してください。

隔離でエンドユーザ アクセスまたはスパム通知の LDAP クエリーを使用するには、[有効なクエリとして指定する（Designate as the active query）] チェックボックスをオンにします。隔離アクセスを制御するエンドユーザ認証クエリーを 1 つと、スパム通知用のエイリアス統合クエリーを 1 つ指定できます。既存のアクティブ クエリーはすべてディセーブルになります。セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [LDAP] ページを選択します。アスタリスク（*）がアクティブ クエリーの横に表示されます。

ドメインベースのクエリーまたはチェーン クエリーも、アクティブなエンドユーザ アクセス クエリーまたはスパム通知クエリーとして指定できます。詳細については、「ドメインベース クエリー」（P.11-8）および「チェーン クエリー」（P.11-10）を参照してください。

（注）　[LDAP] ページの [クエリのテスト（Test Query）] ボタン（または **ldaptest** コマンド）を使用して、クエリーから返される結果が期待したとおりであることを確認します。

LDAP クエリーの構文

LDAP パス内でスペースを使用できます。引用符で囲む必要はありません。CN と DC の構文では、大文字と小文字は区別されません。

Cn=First Last,oU=user,dc=domain,DC=COM

クエリーに入力する変数名では、大文字と小文字が区別されます。また、正しく動作するためには、LDAP 実装と一致している必要があります。たとえば、プロンプトで **mailLocalAddress** と入力したときに実行されるクエリーは、**maillocaladdress** と入力したときとは異なります。

トークン

次のトークンを LDAP クエリー内で使用できます。

- {a} ユーザ名 @ ドメイン名
- {d} ドメイン
- {dn} 識別名
- {g} グループ名
- {u} ユーザ名
- {f} MAILFROM: アドレス

（注）　{f} トークンを使用できるのは、受け入れクエリーのみです。

たとえば、メールを受け入れるための Active Directory LDAP サーバに対するクエリーは、**(|(mail={a})(proxyAddresses=smtp:{a}))** になります。

（注）　作成したクエリーは、[LDAP] ページの [テスト（Test）] 機能（または **ldapconfig** コマンドの **test** サブコマンド）を使用してテストすることを強く推奨します。期待したとおりの結果が返されることを確認してから、リスナーに対して LDAP 機能をイネーブルにしてください。詳細については、「LDAP クエリーのテスト」（P.11-8）を参照してください。

スパム隔離へのエンドユーザ認証のクエリー

エンドユーザ認証のクエリーとは、ユーザが Cisco IronPort スパム隔離にログインするときにユーザを検証するためのクエリーです。トークン {u} は、ユーザを示します（ユーザのログイン名を表します）。トークン {a} は、ユーザの電子メール アドレスを示します。LDAP クエリーによって「SMTP:」が電子メール アドレスから除去されることはありません。ただし、AsyncOS はこの部分をアドレスから除去します。

サーバ タイプに基づいて、次のデフォルト クエリー文字列がエンドユーザ認証クエリーに使用されます。

- **Active Directory :** `(sAMAccountName={u})`

- **OpenLDAP：**(uid={u})
- [不明またはそれ以外（Unknown or Other）]：（ブランク）

デフォルトでは、プライマリ メール属性は **mail** です。独自のクエリーとメール属性を入力できます。クエリーを CLI で作成するには、**ldapconfig** コマンドの isqauth サブコマンドを使用します。

（注） ユーザのログイン時に各自の電子メール アドレス全体を入力させる場合は、(mail=smtp:{a}) というクエリー文字列を使用します。

Active Directory エンドユーザ認証の設定の例

ここでは、Active Directory サーバとエンドユーザ認証クエリーの設定の例を示します。この例では、Active Directory サーバのパスワード認証、Active Directory サーバのためのエンドユーザ認証のデフォルト クエリー文字列、mail および proxyAddresses メール属性を使用します。

表 11-1　LDAP サーバとスパム隔離へのエンドユーザ認証の設定例：Active Directory

認証方式	パスワードを使用 （検索用にバインドするための低特権のユーザを作成するか、匿名検索を設定する必要があります）
サーバ タイプ	Active Directory
ポート	3268
ベース DN	（ブランク）
接続プロトコル	（ブランク）
クエリー文字列	(sAMAccountName={u})
メール属性	mail,proxyAddresses

OpenLDAP エンドユーザ認証の設定の例

ここでは、OpenLDAP サーバとエンドユーザ認証クエリーの設定の例を示します。この例では、OpenLDAP サーバの匿名認証、OpenLDAP サーバのためのエンドユーザ認証のデフォルト クエリー文字列、mail および mailLocalAddress メール属性を使用します。

表 11-2　LDAP サーバとスパム隔離へのエンドユーザ認証の設定例：OpenLDAP

認証方式	匿名
サーバ タイプ	OpenLDAP
ポート	389
ベース DN	（ブランク）（古いスキーマでは具体的なベース DN の使用が要求されることがあります）
接続プロトコル	（ブランク）
クエリー文字列	(uid={u})
メール属性	mail,mailLocalAddress

スパム隔離のエイリアス統合クエリー

スパム通知を使用する場合は、スパム隔離のエイリアス統合クエリーを使用して電子メール エイリアスを 1 つにまとめると、受信者がエイリアスごとに隔離通知を受け取ることはなくなります。たとえば、ある受信者がメール アドレス john@example.com、jsmith@example.com、および john.smith@example.com のメールを受け取るとします。エイリアス統合を使用すると、受信者が受け取るスパム通知は 1 通だけとなります。送信先は、このユーザのエイリアスすべてに送信されるメッセージのプライマリ メール アドレスとして選択されたアドレスです。

メッセージを統合してプライマリ メール アドレスに送信するには、受信者の代替の電子メール エイリアスを検索するためのクエリーを作成してから、受信者のプライマリ メール アドレスを [メール属性（Email Attribute）] フィールドに入力します。

Active Directory サーバの場合は、デフォルトのクエリー文字列は `(|(proxyAddresses={a})(proxyAddresses=smtp:{a}))` で、デフォルトのメール属性は `mail` です。OpenLDAP サーバの場合は、デフォルトのクエリー文字列は `(mail={a})` で、デフォルトのメール属性は `mail` です。独自のクエリーとメール属性を定義することもできます。属性が複数の場合は、カンマで区切ります。入力するメール属性が複数ある場合は、最初のメール属性として、変動する可能性のある値を複数持つ属性（たとえば `proxyAddresses`）ではなく、値を 1 つだけ使用する一意の属性（たとえば `mail`）を入力することを推奨します。

クエリーを CLI で作成するには、`ldapconfig` コマンドの `isqalias` サブコマンドを使用します。

Active Directory エイリアス統合の設定の例

ここでは、Active Directory サーバとエイリアス統合クエリーの設定の例を示します。この例では、Active Directory サーバに対して匿名認証を使用し、Active Directory サーバに対するエイリアス統合用のクエリー文字列を指定し、メール属性は `mail` を使用します。

表 11-3　LDAP サーバとスパム隔離のエイリアス統合の設定例：Active Directory

認証方式	**匿名**
サーバ タイプ	Active Directory
ポート	3268
ベース DN	（ブランク）
接続プロトコル	Use SSL
クエリー文字列	(|(mail={a})(mail=smtp:{a}))
メール属性	`mail`

OpenLDAP エイリアス統合の設定の例

ここでは、OpenLDAP サーバとエイリアス統合クエリーの設定の例を示します。この例では、OpenLDAP サーバに対して匿名認証を使用し、OpenLDAP サーバに対するエイリアス統合用のクエリー文字列を指定し、メール属性は `mail` を使用します。

表 11-4　LDAP サーバとスパム隔離のエイリアス統合の設定例：OpenLDAP

認証方式	**匿名**
サーバ タイプ	OpenLDAP
ポート	389
ベース DN	（ブランク）（古いスキーマでは具体的なベース DN の使用が要求されることがあります）

表 11-4　LDAP サーバとスパム隔離のエイリアス統合の設定例 : OpenLDAP （続き）

接続プロトコル	Use SSL
クエリー文字列	`(mail={a}))`
メール属性	`mail`

LDAP クエリーのテスト

[LDAP サーバ プロファイルを追加/編集（Add/Edit LDAP Server Profile）] ページの [クエリのテスト（Test Query）] ボタン（または CLI の `ldaptest` コマンド）を使用して、クエリーをテストします。AsyncOS に、クエリー接続テストの各ステージの詳細が表示されます。たとえば、最初のステージの SMTP 認証に成功したか失敗したか、バインド照合の返された結果が true か false か、などです。

`ldaptest` コマンドは、次の例のようにバッチ コマンドとして使用できます。

```
ldaptest LDAP.isqalias foo@cisco.com
```

クエリーに入力する変数名では、*大文字と小文字が区別されます*。また、正しく動作するためには、LDAP 実装と一致している必要があります。たとえば、メール属性に `mailLocalAddress` と入力すると、`maillocaladdress` と入力する場合とは異なるクエリーを実行します。

クエリーをテストするには、テスト パラメータを入力して、[テストの実行（Run Test）] をクリックします。[テスト接続（Test Connection）] フィールドに結果が表示されます。エンドユーザ認証クエリーが成功した場合、「Success: Action: match positive」という結果が表示されます。エイリアス統合クエリーの場合は、統合されたスパム通知の電子メール アドレスと共に、「Success: Action: alias consolidation」という結果が表示されます。クエリーが失敗すると、一致する LDAP レコードが見つからない、一致したレコードにメール属性が含まれていないなど、失敗の原因が表示されます。複数の LDAP サーバを使用している場合、シスコ コンテンツ セキュリティ アプライアンスは、LDAP サーバごとにクエリーをテストします。

ドメインベース クエリー

ドメインベース クエリーとは、LDAP クエリーをタイプ別にグループ化し、ドメインに関連付けたものです。複数の別の LDAP サーバが異なるドメインに関連付けられているが、エンドユーザ隔離アクセスに対し、すべての LDAP サーバでクエリーを実行する必要がある場合、ドメインベース クエリーの使用を推奨します。たとえば、Bigfish という名前の会社が Bigfish.com、Redfish.com、および Bluefish.com というドメインを所持していて、それぞれのドメインに関連する従業員用に別の LDAP サーバを管理するとします。Bigfish は、ドメインベース クエリーを使用して、3 つのドメインすべての LDAP ディレクトリに対してエンドユーザを認証することができます。

ドメインベース クエリーを使用してエンドユーザ アクセスまたは Cisco IronPort スパム隔離の通知を制御するには、次の手順を実行します。

手順

ステップ 1　ドメインベース クエリーで使用する各ドメインについて LDAP サーバ プロファイルを作成します。各サーバ プロファイルでは、ドメインベース クエリーで使用するクエリーを設定します。詳細については、「LDAP サーバ プロファイルの作成」（P.11-2）を参照してください。

ステップ 2　ドメインベース クエリーを作成します。ドメインベース クエリーを作成するときに、各サーバ プロファイルからクエリーを選択し、ドメインベース クエリーを Cisco IronPort スパム隔離のアクティブ クエリーとして指定します。クエリーの作成方法の詳細については、「ドメインベース クエリーの作成」（P.11-9）を参照してください。

ステップ 3　Cisco IronPort スパム隔離に対して、エンドユーザ アクセスまたはスパム通知をイネーブルにします。詳細については、「中央集中型スパム隔離の設定」（P.7-2）を参照してください。

ドメインベース クエリーの作成

手順

ステップ 1　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [LDAP] を選択します。

ステップ 2　[LDAP] ページで、[拡張（Advanced）] をクリックします。

ステップ 3　ドメインベース クエリーの名前を入力します。

ステップ 4　クエリーのタイプを選択します。

（注）　ドメインベース クエリーを作成するときは、シングル クエリー タイプを指定します。クエリーのタイプを選択すると、該当するクエリーが LDAP サーバ プロファイルからクエリー フィールド ドロップダウン リストに含まれるようになります。

ステップ 5　[ドメイン割り当て（Domain Assignments）] フィールドに、ドメインを入力します。

ステップ 6　このドメインに関連付けるクエリーを選択します。

ステップ 7　行を追加して、ドメインベース クエリーのドメインごとにクエリーを選択します。

ステップ 8　どのクエリーにも一致しないときに実行する、デフォルトのクエリーを入力します。デフォルトのクエリーを入力しない場合は、[なし（None）] を選択します。

図 11-1　ドメインベース クエリーの例

ステップ 9　[クエリのテスト（Test Query）] ボタンをクリックし、[テスト パラメータ（Test Parameters）] フィールドにテストするユーザのログインとパスワード、または電子メール アドレスを入力して、クエリーをテストします。[接続ステータス（Connection Status）] フィールドに結果が表示されます。

ステップ 10　Cisco IronPort スパム隔離でドメインベース クエリーを使用するには、[有効なクエリとして指定する（Designate as the active query）] チェックボックスをオンにします。

（注）　ドメインベース クエリーが、指定されたクエリー タイプのアクティブ LDAP クエリーになります。たとえば、ドメインベース クエリーがエンドユーザ認証に使用されている場合は、Cisco IronPort スパム隔離のアクティブ エンドユーザ認証クエリーになります。

ステップ 11　[送信（Submit）] をクリックし、[確定する（Commit）] をクリックして変更を保存します。

（注）　同じ設定をコマンドライン インターフェイスで行うには、コマンド ライン プロンプトで、`ldapconfig` コマンドの `advanced` サブコマンドを入力します。

チェーン クエリー

チェーン クエリーは、AsyncOS が連続して実行する一連の LDAP クエリーです。AsyncOS は LDAP サーバから肯定的なレスポンスが返されると、または最後のクエリーで否定的なレスポンスが返されるか失敗するまで、シリーズ内の各クエリー、「チェーン」内の各クエリーを実行します。チェーン クエリーが役立つのは、LDAP ディレクトリ内のエントリにおいて、さまざまな属性に類似の（または同一の）値が格納されている場合です。たとえば、組織の各部門が、異なるタイプの LDAP ディレクトリを使用していることがあります。IT 部門が OpenLDAP を使用し、営業部門が Active Directory を使用しているとします。クエリーが両方のタイプの LDAP ディレクトリに対して実行されていることを確認するために、チェーン クエリーを使用できます。

チェーン クエリーを使用してエンドユーザ アクセスまたは Cisco IronPort スパム隔離の通知を制御するには、次の手順を実行します。

手順

ステップ 1　チェーン クエリーで使用するクエリーごとに 1 つずつ、LDAP サーバ プロファイルを作成します。このサーバ プロファイルのそれぞれについて、チェーン クエリーに使用するクエリーを設定します。詳細については、「LDAP サーバ プロファイルの作成」（P.11-2）を参照してください。

ステップ 2　チェーン クエリーを作成し、Cisco IronPort スパム隔離のアクティブ クエリーとして指定します。詳細については、「チェーン クエリーの作成」（P.11-10）を参照してください。

ステップ 3　Cisco IronPort スパム隔離に対して、LDAP エンドユーザ アクセスまたはスパム通知をイネーブルにします。スパム隔離の詳細については、「中央集中型スパム隔離の設定」（P.7-2）を参照してください。

チェーン クエリーの作成

ヒント　CLI から、`ldapconfig` コマンドの `advanced` サブコマンドも使用できます。

手順

ステップ 1　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [LDAP] > [LDAP サーバ（LDAP Server）] を選択します。

ステップ 2　[LDAP サーバ プロファイル（LDAP Server Profiles）] ページの [拡張（Advanced）] をクリックします。

ステップ 3　[連鎖クエリを追加（Add Chained Query）] をクリックします。

ステップ 4　チェーン クエリーの名前を入力します。

ステップ 5　クエリーのタイプを選択します。

チェーン クエリーを作成するときは、そのコンポーネントのクエリーすべてを同じクエリー タイプにします。クエリーのタイプを選択すると、該当するクエリーが LDAP からクエリー フィールド ドロップダウン リストに表示されます。

ステップ 6　チェーンの最初のクエリーを選択します。

シスコ コンテンツ セキュリティ アプライアンスによって、ここで設定した順にクエリーが実行されます。チェーン クエリーに複数のクエリーを追加する場合は、詳細なクエリーの後に広範なクエリーが続くように順序付けることを推奨します。

図 11-2　チェーン クエリーの例

ステップ 7　[クエリのテスト（Test Query）] ボタンをクリックし、[テスト パラメータ（Test Parameters）] フィールドにユーザのログインとパスワード、または電子メール アドレスを入力して、クエリーをテストします。[接続ステータス（Connection Status）] フィールドに結果が表示されます。

ステップ 8　Cisco IronPort スパム隔離でドメイン クエリーを使用するには、[有効なクエリとして指定する（Designate as the active query）] チェックボックスをオンにします。

（注）　チェーン クエリーが、指定されたクエリー タイプのアクティブ LDAP クエリーになります。たとえば、チェーン クエリーがエンドユーザ認証に使用されている場合は、Cisco IronPort スパム隔離のアクティブ エンドユーザ認証クエリーになります。

ステップ 9　変更を送信し、保存します。

（注）　同じ設定をコマンドライン インターフェイスで行うには、コマンド ライン プロンプトで、`ldapconfig` コマンドの `advanced` サブコマンドを入力します。

AsyncOS を複数の LDAP サーバと連携させるための設定

LDAP プロファイルを設定するときに、シスコ コンテンツ セキュリティ アプライアンスからの接続先となる複数の LDAP サーバをリストとして設定できます。複数の LDAP サーバを使用するには、格納されている情報、構造、使用する認証情報を同一にする必要があります。レコードを統合できる製品がサード パーティから提供されています。

次の機能を使用する場合は、冗長 LDAP サーバに接続するようにシスコ コンテンツ セキュリティ アプライアンスを設定します。

- **フェールオーバー**。シスコ コンテンツ セキュリティ アプライアンスが LDAP サーバに接続できない場合、リストで次に指定されているサーバに接続します。
- **ロード バランシング**。シスコ コンテンツ セキュリティ アプライアンスは、LDAP クエリーを実行するときに、リストで指定されている LDAP サーバの間で接続を分散します。

冗長 LDAP サーバを設定するには、[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [LDAP] ページまたは CLI の `ldapconfig` コマンドを使用します。

サーバとクエリーのテスト

[LDAP サーバ プロファイルを追加/編集（Add/Edit LDAP Server Profile）] ページの [テスト サーバ（Test Server(s)）] ボタン（または CLI の `test` サブコマンド）を使用して、LDAP サーバへの接続をテストします。複数の LDAP サーバを使用する場合は、各サーバのテストが実行されて、各サーバの結果が個別に表示されます。各 LDAP サーバでのクエリーのテストも実行されて、結果が個別に表示されます。

フェールオーバー

LDAP サーバで確実にクエリーを解決できるようにするには、フェールオーバー用に LDAP プロファイルを設定できます。

シスコ コンテンツ セキュリティ アプライアンスアプライアンスは、LDAP サーバ リスト内の最初のサーバへの接続を、所定の時間が経過するまで試行します。アプライアンスがリスト内の最初の LDAP サーバに接続できない場合は、リスト内の次の LDAP サーバへの接続が試行されます。シスコ コンテンツ セキュリティ アプライアンスが確実にプライマリ LDAP サーバにデフォルトで接続するようにするには、そのサーバが LDAP サーバ リストの先頭に入力されていることを確認してください。

シスコ コンテンツ セキュリティ アプライアンスが 2 番目の、または後続の LDAP サーバに接続する場合、そのサーバへの接続は所定の時間が経過するまで維持されます。この時間が経過すると、アプライアンスはリスト内の最初のサーバに対して再接続を試行します。

LDAP フェールオーバーのためのシスコのコンテンツ アプライアンスの設定

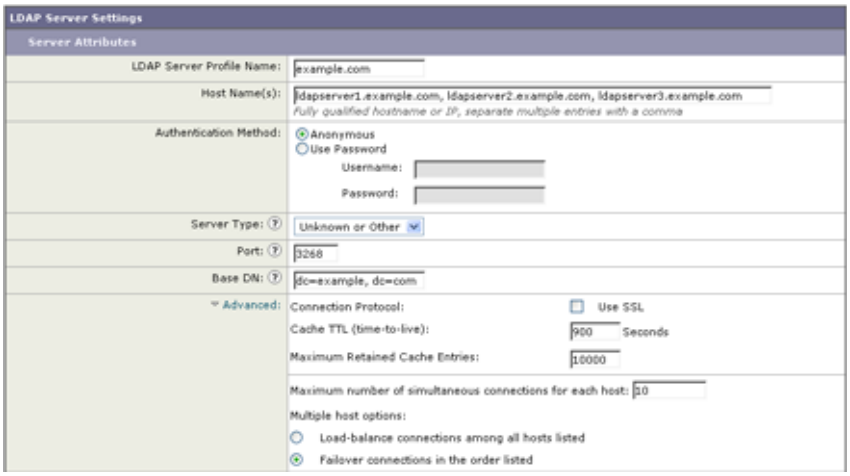
手順

ステップ 1　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [LDAP] を選択します。

ステップ 2　編集する LDAP サーバ プロファイルを選択します。

次の例で、LDAP サーバ名は example.com です。

図 11-3　　LDAP フェールオーバー コンフィギュレーションの例



ステップ 3　[ホスト名（Hostname）] テキスト フィールドに、LDAP サーバ（**ldapserver.example.com** など）を入力します。

ステップ 4　[各ホストの最大同時接続数（Maximum number of simultaneous connections for each host）] テキスト フィールドに、最大接続数を入力します。

この例では、最大接続数が **10** です。

ステップ 5　[一覧されている順序での接続のフェールオーバー（Failover connections in the order list）] の横にあるオプション ボタンをクリックします。

ステップ 6　その他の LDAP オプションを必要に応じて設定します。

ステップ 7　変更を送信し、保存します。

ロード バランシング

LDAP 接続をグループ内の LDAP サーバ間に分散させるには、ロード バランシングのための LDAP プロファイルを設定します。

ロード バランシングを使用した場合、シスコ コンテンツ セキュリティ アプライアンスからの接続はリスト内の LDAP サーバに分散されます。接続に失敗したときやタイムアウトしたときは、アプライアンスは使用可能な LDAP サーバを判断して、使用可能なサーバに再接続します。アプライアンスは、管理者が設定した最大同時接続数に基づいて、同時に確立する接続の数を決定します。

リストで指定された LDAP サーバの 1 つが応答しなくなった場合は、アプライアンスからの接続の負荷は残りの LDAP サーバに分散されます。

ロード バランシングのためのシスコのコンテンツ アプライアンスの設定

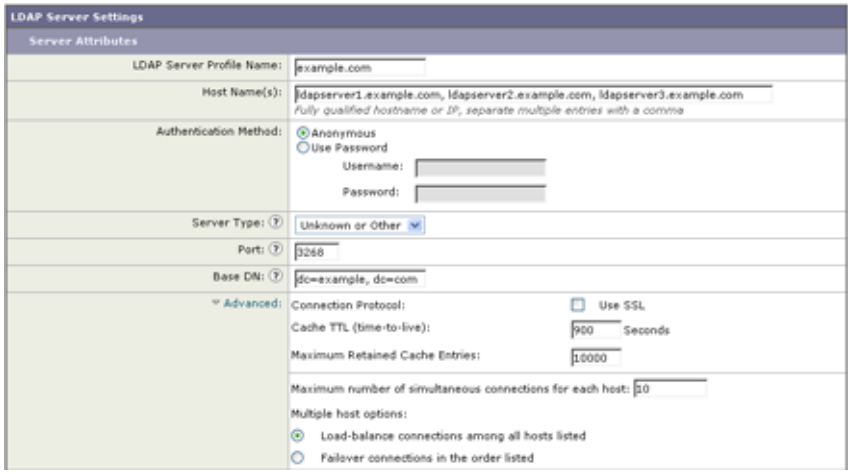
手順

ステップ 1　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [LDAP] を選択します。

ステップ 2　編集する LDAP サーバ プロファイルを選択します。

次の例で、LDAP サーバ名は example.com です。

図 11-4　　ロード バランシング コンフィギュレーションの例



ステップ 3　[ホスト名（Hostname）] テキスト フィールドに、LDAP サーバ（**ldapserver.example.com** など）を入力します。

ステップ 4　[各ホストの最大同時接続数（Maximum number of simultaneous connections for each host）] テキスト フィールドに、最大接続数を入力します。

この例では、最大接続数が **10** です。

ステップ 5　[すべてのホスト間での負荷分散接続（Load balance connections among all hosts）] の横にあるオプション ボタンをクリックします。

ステップ 6　その他の LDAP オプションを必要に応じて設定します。

ステップ 7　変更を送信し、保存します。

LDAP を使用した管理ユーザの外部認証の設定

ネットワーク上の LDAP ディレクトリを使用して管理ユーザを認証するようにアプライアンスを設定できます。このように設定すると、ユーザが各自の LDAP ユーザ名とパスワードを使用して、シスコ コンテンツ セキュリティ アプライアンスにログインできるようになります。

手順

ステップ 1　**LDAP サーバ プロファイルを設定します。**「LDAP サーバ プロファイルの作成」（P.11-2）を参照してください。

ステップ 2　**ユーザ アカウントを見つけるためのクエリーを作成します。**LDAP サーバ プロファイルの、[外部認証クエリ（External Authentication Queries）] セクションで、クエリーを作成して LDAP ディレクトリ内のユーザ アカウントを検索します。「管理ユーザの認証のためのユーザ アカウント クエリー」（P.11-15）を参照してください。

ステップ 3　**グループ メンバーシップ クエリーを作成します。**あるユーザがディレクトリ グループのメンバーであるかどうかを判断するクエリーを作成し、あるグループのすべてのメンバーを検索する別のクエリーを作成します。詳細ついては、「管理ユーザの認証のためのグループ メンバーシップ クエリー」（P.11-16）およびご使用の電子メール セキュリティ アプライアンスのマニュアルまたはオンライン ヘルプを参照してください。

（注）　そのページの [外部認証クエリ（External Authentication Queries）] セクションにある [テスト クエリ（Test Queries）] ボタン（または `ldaptest` コマンド）を使用して、クエリーから返される結果が期待したとおりであることを確認します。関連情報については、「LDAP クエリーのテスト」（P.11-8）を参照してください。

ステップ 4　**LDAP サーバを使用するように外部認証をセットアップします。**この LDAP サーバをユーザ認証に使用するようにアプライアンスを設定し、ユーザ ロールを LDAP ディレクトリ内のグループに割り当てます。詳細についてはの「管理ユーザの外部認証のイネーブル化」（P.11-17）および電子メール セキュリティ アプライアンスのマニュアルまたはオンライン ヘルプの「Adding Users」を参照してください。

管理ユーザの認証のためのユーザ アカウント クエリー

外部ユーザを認証するために、AsyncOS はクエリーを使用してそのユーザのレコードを LDAP ディレクトリ内で検出し、ユーザのフル ネームが格納されている属性を見つけます。管理者が選択したサーバ タイプに応じて、AsyncOS によってデフォルトのクエリーとデフォルトの属性が入力されます。アカウントが失効しているユーザは拒否するようにアプライアンスを設定することもできます。それには、RFC 2307 で規定されている属性が LDAP ユーザ レコード内で定義されている必要があります（**shadowLastChange**、**shadowMax**、および **shadowExpire**）。ユーザのレコードがあるドメイン レベルのベース DN が必要です。

表 11-5 に、AsyncOS がユーザ アカウントを Active Directory サーバ上で検索するときに使用されるデフォルトのクエリー文字列とユーザのフル ネーム属性を示します。

表 11-5　Active Directory サーバのデフォルト クエリー文字列

サーバ タイプ	Active Directory
ベース DN	（ブランク）（ユーザ レコードを見つけるには具体的なベース DN を使用する必要があります）
クエリー文字列	`(&(objectClass=user)(sAMAccountName={u}))`
ユーザのフル ネームが格納されている属性	`displayName`

表 11-6 に、AsyncOS がユーザ アカウントを OpenLDAP サーバ上で検索するときに使用されるデフォルトのクエリー文字列とユーザのフル ネーム属性を示します。

表 11-6　Open LDAP サーバのデフォルト クエリー文字列

サーバ タイプ	OpenLDAP
ベース DN	（ブランク）（ユーザ レコードを見つけるには具体的なベース DN を使用する必要があります）
クエリー文字列	`(&(objectClass=posixAccount)(uid={u}))`
ユーザのフル ネームが格納されている属性	`gecos`

管理ユーザの認証のためのグループ メンバーシップ クエリー

LDAP グループをアプライアンスにアクセスするためのユーザ ロールと関連付けることができます。

AsyncOS は、あるユーザがディレクトリ グループのメンバーであるかどうかを判断するクエリーや、あるグループのすべてのメンバーを検索する別のクエリーを使用することもできます。ディレクトリ グループ メンバーシップ内のメンバーシップによって、そのユーザのシステム内のアクセス許可が決まります。GUI の [管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザ（Users）] ページ（または CLI の `userconfig`）で外部認証をイネーブルにするときに、ユーザ ロールを LDAP ディレクトリ内のグループに割り当てます。ユーザ ロールによって、そのユーザがシステム内で持つアクセス許可が決まります。外部認証されたユーザの場合は、ロールは個々のユーザではなくディレクトリ グループに割り当てられます。たとえば、IT というディレクトリ グループ内のユーザに「Administrator」というロールを割り当て、「Support」というディレクトリ グループのユーザに「Help Desk User」というロールを割り当てます。

ユーザが異なるユーザ ロールを持つ複数の LDAP グループに属する場合は、AsyncOS がユーザに最も制限されたロールの権限を割り当てます。たとえば、ユーザが Operator 権限を持つグループと Help Desk User 権限を持つグループに属する場合、AsyncOS はユーザに Help Desk User ロールの権限を割り当てます。

グループ メンバーシップを問い合わせるための LDAP プロファイルを設定するときに、グループ レコードが格納されているディレクトリ レベルのベース DN を入力し、グループ メンバーのユーザ名が格納されている属性と、グループ名が格納されている属性を入力します。LDAP サーバ プロファイルに対して選択されたサーバ タイプに基づいて、ユーザ名とグループ名の属性のデフォルト値とデフォルト クエリー文字列が AsyncOS によって入力されます。

（注）　Active Directory サーバの場合は、ユーザが特定のグループのメンバーかどうかを判断するためのデフォルトのクエリー文字列は (&(objectClass=group)(member={u})) です。ただし、使用する LDAP スキーマにおいて、「memberof」のリストでユーザ名ではなく識別名が使用されている場合は、{dn} を {u} の代わりに使用できます。

表 11-7 に、AsyncOS が Active Directory サーバ上でグループ メンバーシップ情報を検索するときに使用されるデフォルトのクエリー文字列と属性を示します。

表 11-7　Active Directory サーバのデフォルト クエリー文字列および属性

クエリー文字列	Active Directory
ベース DN	（ブランク）（グループ レコードを見つけるには具体的なベース DN を使用する必要があります）
ユーザが特定のグループのメンバーかどうかを判断するためのクエリー文字列	`(&(objectClass=group)(member={u}))` **（注）** 使用する LDAP スキーマにおいてメンバーのリストの中でユーザ名ではなく識別名が使用されている場合は、`{u}` の代わりに `{dn}` を使用できます。
グループのすべてのメンバーを判別するクエリー文字列	`(&(objectClass=group)(cn={g}))`
各メンバーのユーザ名（またはそのユーザのレコードの DN）が格納されている属性	`member`
グループ名が格納されている属性	`cn`

表 11-8 に、AsyncOS が OpenLDAP サーバ上でグループ メンバーシップ情報を検索するときに使用されるデフォルトのクエリー文字列と属性を示します。

表 11-8　Open LDAP サーバのデフォルト クエリー文字列および属性

クエリー文字列	OpenLDAP
ベース DN	（ブランク）（グループ レコードを見つけるには具体的なベース DN を使用する必要があります）
ユーザが特定のグループのメンバーかどうかを判断するためのクエリー文字列	`(&(objectClass=posixGroup)(memberUid={u}))`
グループのすべてのメンバーを判別するクエリー文字列	`(&(objectClass=posixGroup)(cn={g}))`
各メンバーのユーザ名（またはそのユーザのレコードの DN）が格納されている属性	`memberUid`
グループ名が格納されている属性	`cn`

管理ユーザの外部認証のイネーブル化

LDAP サーバ プロファイルおよびクエリーを設定した後で、LDAP を使用する外部認証をイネーブルにすることができます。

手順

ステップ 1　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザ（Users）] ページを選択します。

ステップ 2　[有効（Enable）] をクリックします。

ステップ 3　[外部認証を有効にする（Enable External Authentication）] チェックボックスをオンにします。

ステップ 4　認証タイプとして [LDAP] を選択します。

ステップ 5　ユーザを認証する LDAP 外部認証クエリーを選択します。

ステップ 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　アプライアンスで認証する LDAP ディレクトリからのグループ名を入力し、グループのユーザに対するロールを選択します。

ステップ 8　また、[行の追加（Add Row）] をクリックして別のディレクトリ グループを追加することもできます。アプライアンスが認証する各ディレクトリ グループに対して、ステップ 7 とステップ 8 を繰り返します。

ステップ 9　変更を送信し、保存します。

CHAPTER 12

SMTP ルーティングの設定

この章では、シスコのコンテンツのセキュリティ管理アプライアンスを通過する電子メールのルーティングおよび配信に影響を与える機能、および [SMTP ルート（SMTP Routes）] ページと **smtproutes** コマンドの使用について説明します。

ローカル ドメインの電子メールのルーティング

セキュリティ管理アプライアンスは次のメールをルーティングします。

- ISQ によりリリースされた、SMTP ルーティングを無視するメッセージ
- アラート
- 指定した宛先にメールできるコンフィギュレーション ファイル
- 定義された受信者にも送信できるサポート要求メッセージ

  最後の 2 種類のメッセージは、宛先への配信に SMTP ルートが使用されます。

電子メール セキュリティ アプライアンスでは、メールをローカル ドメイン経由で、[管理アプライアンス（Management Appliance）] > [ネットワーク（Network）] > [SMTP ルート（SMTP Routes）] ページ（または **smtproutes** コマンド）を使用して指定されたホストにルーティングします。この機能は、sendmail の **mailertable** 機能に似ています。（[SMTP ルート（SMTP Routes）] ページと **smtproutes** コマンドは、AsyncOS 2.0 ドメイン リダイレクト機能を拡張したものです）。

（注） GUI のシステム設定ウィザードを完了し、変更を保存した場合、その時点で入力した各 RAT エントリに対してアプライアンス上の最初の SMTP ルート エントリを定義します。

SMTP ルートの概要

SMTP ルートでは、異なる Mail Exchange（MX）ホストへ特定のドメインのすべての電子メールをリダイレクトできます。たとえば、`example.com` から `groupware.example.com` へのマッピングを行うことができます。このマッピングによって、[エンベロープ受信者（Envelope Recipients）] アドレスに `@example.com` を持つすべての電子メールが、代わりに `groupware.example.com` に送られます。システムは、通常の電子メール配信のように、`groupware.example.com` で「MX」ルックアップを実行し、次にホストで「A」ルックアップを実行します。この代替 MX ホストは、DNS MX レコードにリストされている必要はなく、また、電子メールがリダイレクトされているドメインのメンバーになっている必要もありません。オペレーティング システムでは、最大 10,000 件の SMTP ルート マッピングをシスコ コンテンツ セキュリティ アプライアンスに設定できます。（「SMTP ルートの制限」（P.12-3）を参照）。

この機能では、ホストを「ひとかたまりにする」ことも可能です。example.com などの部分ドメインを指定すると、example.com で終わるすべてのドメインがエントリと一致します。たとえば、fred@foo.example.com と wilma@bar.example.com は、両方ともマッピングに一致します。

SMTP ルート テーブルにホストがない場合は、DNS を使用して MX ルックアップが実行されます。結果は、SMTP ルート テーブルに対して再チェックされません。foo.domain の DNS MX エントリが bar.domain の場合、foo.domain に送信されるすべての電子メールが bar.domain に配信されます。bar.domain から他のホストへのマッピングを作成した場合、foo.domain へ送信される電子メールは影響を受けません。

つまり、再帰的なエントリは続きません。a.domain から b.domain にリダイレクトされるエントリがあり、b.domain から a.domain にリダイレクトされるエントリがその後にある場合、メールのループは作成*されません*。この場合、a.domain に送信される電子メールは、b.domain で指定された MX ホストに配信されます。反対に、b.domain に送信される電子メールは、a.domain で指定された MX ホストに配信されます。

すべての電子メール配信で、SMTP ルート テーブルは、上から順に読み取られます。マッピングと一致する最も具体的なエントリが選択されます。たとえば、SMTP ルート テーブルに host1.example.com と example.com の両方のマッピングがある場合は、host1.example.com の方が具体的なエントリになっているため、こちらが使用されます。具体的でない方の example.com エントリが先にあっても、同じ結果になります。そうでない場合は、エンベロープ受信者のドメインで通常の MX ルックアップが実行されます。

デフォルトの SMTP ルート

特殊なキーワード ALL を使用して、デフォルトの SMTP ルートも定義できます。ドメインが SMTP ルート リストの以前のマッピングと一致しない場合、デフォルトでは、それが ALL エントリで指定される MX ホストにリダイレクトされます。

SMTP ルート エントリを印刷する場合、デフォルトの SMTP ルートは ALL: として一覧表示されます。デフォルトの SMTP ルートは削除できません。入力した値をクリアすることのみ可能です。

[管理アプライアンス（Management Appliance）] > [ネットワーク（Network）] > [SMTP ルート（SMTP Routes）] ページを使用するか、または **smtproutes** コマンドを使用して、デフォルトの SMTP ルートを設定します。

SMTP ルートの定義

電子メール セキュリティ アプライアンスはローカル ドメイン宛てのメールを、[管理アプライアンス（Management Appliance）] > [ネットワーク（Network）] > [SMTP ルート（SMTP Routes）] ページ（または **smtproutes** コマンド）を使用して指定されたホストにルーティングします。この機能は、sendmail の mailer table 機能に似ています。（[SMTP ルート（SMTP Routes）] ページと **smtproutes** コマンドは、AsyncOS 2.0 ドメイン リダイレクト機能を拡張したものです）。

[管理アプライアンス（Management Appliance）] > [ネットワーク（Network）] > [SMTP ルート（SMTP Routes）] ページ（または **smtproutes** コマンド）を使用してルートを作成します。新しいルートを作成するには、まず、永続的なルートを作成するドメインまたはドメインの一部を指定する必要があります。次に、宛先ホストを指定します。宛先ホストは、完全修飾ホスト名として入力することも、IP アドレスとして入力することもできます。エントリと一致するメッセージをドロップするために、特殊な宛先ホスト /dev/null を指定することもできます。（実際に /dev/null をデフォルト ルートに指定すると、アプライアンスが受信したメールは配信されなくなります）。

複数の宛先ホスト エントリに、完全修飾ホスト名と IP アドレスの両方を含めることができます。複数のエントリを指定する場合は、カンマで区切ります。

1 つまたは複数のホストが応答しない場合、メッセージは到達可能なホストの 1 つに配信されます。設定されたすべてのホストが応答しない場合、メールはそのホストのキューに格納されます（MX レコードの使用にフェールオーバーしません）。

SMTP ルートの制限

最大 10,000 ルートまで定義できます。最後のデフォルト ルート ALL は、この制限内のルートとしてカウントされます。したがって、定義できるのは最大 9,999 のカスタム ルートと、特殊キーワード ALL を使用する 1 つのルートです。

SMTP ルートと DNS

MX ルックアップを実行して、特定のドメインに対するネクスト ホップを決定するようアプライアンスに指示するには、特殊キーワード USEDNS を使用します。これは、サブドメインのメールを特定のホストにルーティングする必要がある場合に役立ちます。たとえば、example.com へのメールが企業の Exchange サーバに送信されることになっている場合、次のような SMTP ルートになっていることがあります。

```
example.com exchange.example.com
```

ただし、さまざまなサブドメイン（foo.example.com）宛のメールの場合は、次のような SMTP ルートを追加します。

```
.example.com USEDNS
```

SMTP ルート、メール配信、およびメッセージ分裂

着信：1 つのメッセージに 10 人の受信者がいて、全員が同じ Exchange サーバに属する場合、AsyncOS では TCP 接続を 1 つ開き、メール ストアには 10 の別々のメッセージではなく、メッセージを 1 つのみ配置します。

発信：同様に機能しますが、1 つのメッセージが 10 の異なるドメインの 10 人の受信者に送られる場合、AsyncOS では 10 の MTA に対する 10 の接続を開き、それぞれに 1 つずつ電子メール配信を行います。

分裂：1 つの着信メッセージに 10 人の受信者がいて、それぞれが別々の Incoming Policy グループ（10 グループ）に属する場合、10 人全員の受信者が同じ Exchange サーバを使用していても、メッセージは分裂します。つまり、10 の別々の電子メールが 1 つの TCP 接続で配信されます。

SMTP ルートと発信 SMTP 認証

発信 SMTP 認証プロファイルが作成されたら、SMTP ルートに適用できます。これによって、ネットワーク エッジにあるメール リレー サーバの背後にシスコ コンテンツ セキュリティ アプライアンスが配置されている場合に、発信メールを認証できます。

セキュリティ管理アプライアンスでの SMTP ルートの管理

手順

ステップ 1　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [ネットワーク（Network）] > [SMTP ルート（SMTP Routes）] を選択します。

このページを使用して、アプライアンスで SMTP ルートを管理します。このページから、テーブルのマッピングの追加、変更、および削除を行うことができます。SMTP ルート エントリをエクスポートまたはインポートすることができます。

SMTP ルートの追加

手順

ステップ 1　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [ネットワーク（Network）] > [SMTP ルート（SMTP Routes）] を選択します。

ステップ 2　[ルートを追加（Add Route）] をクリックします。

ステップ 3　受信側ドメインと宛先ホストを入力します。複数の宛先ホストを追加するには、[行の追加（Add Row）] をクリックし、新しい行に次の宛先ホストを入力します。

ステップ 4　ポート番号を指定するには、宛先ホストに「:<*port number*>」を追加します（例：`example.com:25`）。

ステップ 5　変更を送信し、保存します。

SMTP ルートの編集

手順

ステップ 1　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [ネットワーク（Network）] > [SMTP ルート（SMTP Routes）] を選択します。

ステップ 2　SMTP ルートのリストで、既存の SMTP ルートの名前をクリックします。

ステップ 3　ルートを編集します。

ステップ 4　変更を送信し、保存します。

SMTP ルートの削除

手順

ステップ 1　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [ネットワーク（Network）] > [SMTP ルート（SMTP Routes）] を選択します。

ステップ 2　削除する SMTP ルートの右側にあるチェックボックスを選択します。

ステップ 3　[削除（Delete）] をクリックします。

すべての SMTP ルートを削除するには、[すべて（All）] というラベルの付いたチェックボックスを選択して [削除（Delete）] をクリックします。

SMTP ルートのエクスポート

ホスト アクセス テーブル（HAT）および受信者アクセス テーブル（RAT）の場合と同様に、ファイルをエクスポートおよびインポートして SMTP ルート マッピングを変更することもできます。

手順

ステップ 1　[SMTP ルート（SMTP Routes）] ページの [SMTP ルートをエクスポート（Export SMTP Routes）] をクリックします。

ステップ 2　ファイルの名前を入力し、[送信（Submit）] をクリックします。

SMTP ルートのインポート

Host Access Table（HAT）および Recipient Access Table（RAT）の場合と同様に、ファイルをエクスポートおよびインポートして SMTP ルート マッピングを変更することもできます。

手順

ステップ 1　[SMTP ルート（SMTP Routes）] ページの [SMTP ルートをインポート（Import SMTP Routes）] をクリックします。

ステップ 2　エクスポートされた SMTP ルートが含まれているファイルを選択します。

ステップ 3　[送信（Submit）] をクリックします。インポートにより、既存の SMTP ルートがすべて置き換えられることが警告されます。テキスト ファイルにあるすべての SMTP ルートがインポートされます。

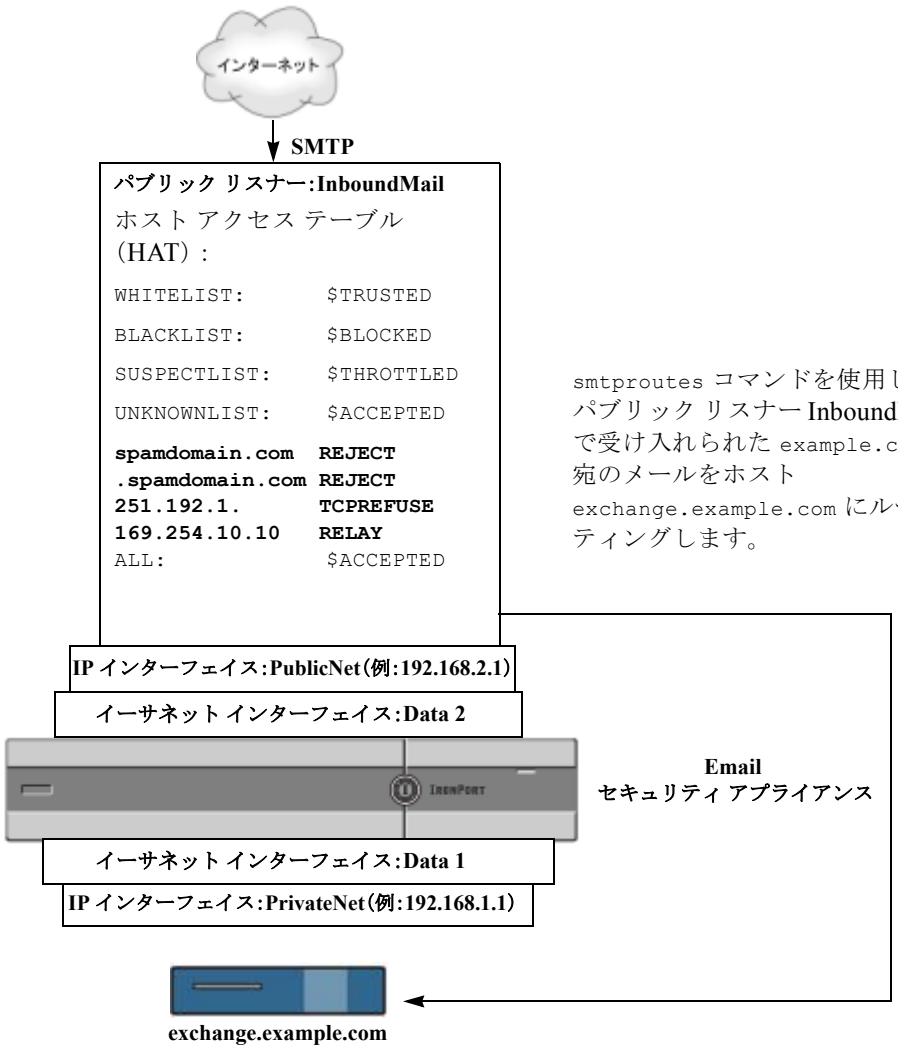
ステップ 4　[インポート（Import）] をクリックします。

ファイルには「コメント」を格納できます。文字「#」で始まる行はコメントと見なされ、AsyncOS によって無視されます。次に例を示します。

```
# this is a comment, but the next line is not
ALL:
```

この時点で、電子メール ゲートウェイの設定は次のようになります。

図 12-1　パブリック リスナー用に定義された SMTP ルート



smtproutes コマンドを使用して、パブリック リスナー InboundMail で受け入れられた example.com 宛のメールをホスト exchange.example.com にルーティングします。

CHAPTER 13

管理タスクの分散

管理タスクの分散について

ユーザ アカウントに割り当てたユーザ ロールに基づいて、他のユーザにシスコのコンテンツ セキュリティ管理アプライアンスの管理タスクを分散できます。

管理タスクが分散されるように設定するには、事前定義されたユーザ ロールがニーズを満たしているかどうかを判断して、必要なカスタム ユーザ ロールを作成します。次に、セキュリティ アプライアンスでローカルに管理ユーザの認証を行う、および（または）独自の中央集中型の LDAP や RADIUS システムを使用して外部で管理ユーザの認証を行うようにアプライアンスを設定します。

さらに、アプライアンスおよびアプライアンス上の特定の情報へのアクセスに追加の制御を指定できます。

ユーザ ロールの割り当て

セキュリティ管理アプライアンスには、電子メールと Web セキュリティ アプライアンスのモニタリングおよび管理を行うための、事前定義ユーザ ロールとカスタム ユーザ ロールの両方が用意されています。

事前定義ユーザ ロール

特記のない限り、次の表で説明されている権限を持つ事前設定ユーザ ロール、またはカスタム ユーザ ロールを各ユーザに割り当てることができます。

表 13-1　ユーザ ロールの説明

ユーザ ロール名	説明	Web レポーティング / 定期レポート機能
admin	**admin** ユーザはシステムのデフォルト ユーザ アカウントであり、すべての管理権限を持っています。便宜上、admin ユーザ アカウントをここに記載しましたが、これはユーザ ロールを使用して割り当てることはできず、パスワードの変更以外、編集や削除もできません。 **resetconfig** コマンドと **revert** コマンドを発行できるのは、**admin** ユーザだけです。	あり / あり
Administrator	Administrator ロールを持つユーザ アカウントはシステムのすべての設定に対する完全なアクセス権を持っています。	あり / あり
Operator	Operator ロールを持つユーザ アカウントは次のことができません。 • ユーザ アカウントの作成または編集 • アプライアンスのアップグレード • `resetconfig` コマンドの発行 • システム セットアップ ウィザードの実行 • ユーザ名とパスワード以外の LDAP サーバ プロファイル設定の変更（LDAP が外部認証に対してイネーブルになっている場合）。 • 隔離の設定、編集、削除、または集約。 これら以外は、Administrator ロールと同じ権限を持ちます。	あり / あり
Technician	Technician ロールを持つユーザ アカウントは、アップグレードおよびリブート、アプライアンスからのコンフィギュレーション ファイルの保存、ライセンス キーの管理などのシステム管理アクティビティを開始できます。	[メール（Email）] タブに表示されるシステム キャパシティ レポートへのアクセス
Read-Only Operator	Read-Only Operator ロールを持つユーザは、設定情報を参照するアクセス権を持っています。Read-Only Operator ロールを持つユーザは、機能の設定方法を確認するために大部分の変更を行って送信できますが、保存できません。または保存を必要としない変更を行うことができます。このロールのユーザは、アクセスが有効な場合、隔離内のメッセージを管理できます。 このロールのユーザは、以下にはアクセスできません。 • ファイル システム、FTP、SCP。 • 隔離を作成、編集、削除、または集中管理するための設定。	あり / なし

表 13-1　ユーザ ロールの説明 （続き）

ユーザ ロール名	説明	Web レポーティング / 定期レポート機能
Guest	ゲスト ロールを持つユーザ アカウントは、アクセス権限が有効であれば、隔離内のメッセージのステータス情報を確認し管理できます。Guest ロールを持つユーザはメッセージ トラッキングにアクセスできません。	あり / なし
Web Administrator	Web Administrator ロールを持つユーザ アカウントは、[Web] タブに表示されるすべての設定に対するアクセス権を持ちます。	あり / あり
Web Policy Administrator	Web Policy Administrator ロールを持つユーザ アカウントは、[Web アプライアンス ステータス（Web Appliance Status）] ページと、Configuration Master のすべてのページにアクセスできます。Web ポリシー管理者は、ID、アクセス ポリシー、暗号化ポリシー、ルーティング ポリシー、プロキシ バイパス、カスタム URL カテゴリ、および時間範囲を設定できます。Web ポリシー管理者は、設定を公開できません。	なし / なし
URL Filtering Administrator	URL Filtering Administrator ロールを持つユーザ アカウントは、URL フィルタリングだけを設定できます。	なし / なし
Email Administrator	メール管理者ロールを持つユーザ アカウントは、隔離など、[メール（Email）] メニューにあるすべての設定へのアクセス権のみを持ちます。	なし / なし

表 13-1　ユーザ ロールの説明 （続き）

ユーザ ロール名	説明	Web レポーティング / 定期レポート機能
Help Desk User	Help Desk User ロールを持つユーザがアクセスできるのは次のものに制限されます。 • メッセージ トラッキング • 隔離内のメッセージ管理 このロールを持つユーザは、CLI を含めたこれ以外のシステムにはアクセスできません。ユーザにこのロールを割り当てた後、このユーザがアクセスできるように隔離を設定する必要があります。	なし / なし
カスタム ロール	カスタム ユーザ ロールに割り当てられているユーザ アカウントは、ポリシー、機能、またはこのロールに特に与えられた特定のポリシーまたは機能インスタンスに対してのみ、表示および設定を行えます。 新しい Custom Email User ロールまたは新しい Custom Web User ロールは、[ローカル ユーザの追加（Add Local User）] ページから作成できます。ただし、ロールを使用できるようにするには、このカスタム ユーザ ロールに権限を割り当てる必要があります。権限を割り当てるには、[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザ ロール（User Roles）] に移動して、ユーザ名をクリックします。 **（注）** Custom Email User ロールに割り当てられているユーザは、CLI にアクセスできません。 詳細については、「カスタム ユーザ ロール」（P.13-5）を参照してください。	なし / なし

一部のロール（Administrator、Operator、Guest、Technician、および Read-Only Operator）は、GUI と CLI の両方にアクセスできます。他のロール（Help Desk User、Email Administrator、Web Administrator、Web Policy Administrator、URL Filtering Administrator、およびカスタム ユーザ）は GUI だけにアクセスできます。

ユーザを認証するために LDAP ディレクトリを使用する場合は、ユーザ ロールに個々のユーザではなくディレクトリ グループを割り当てます。ユーザ ロールにディレクトリ グループを割り当てると、そのグループの各ユーザはそのユーザ ロールで定義された権限を受け取ります。詳細については、「外部ユーザ認証」（P.13-18）を参照してください。

ユーザが隔離にアクセスする前にそのアクセスを有効にする必要があります。「Cisco IronPort スパム隔離への管理者ユーザ アクセスの設定」（P.7-8）および「ポリシー隔離の作成」（P.8-12）を参照してください。

カスタム ユーザ ロール

Administration 権限を持つユーザは、セキュリティ管理アプライアンスを使用してカスタム ロールに管理権限を委任できます。カスタム ロールは、事前定義されたユーザ ロールよりも、ユーザのアクセス権に対して柔軟な制御を行えます。

カスタム ユーザ ロールを割り当てたユーザは、アプライアンス、機能、またはエンド ユーザのサブセットに関して、ポリシーの管理またはレポートへのアクセスを行えます。たとえば、別の国にある組織の支社では、許容可能な使用ポリシーが組織の本社とは異なっている場合に、Web サービスに関して委任を受けた管理者に、支社のポリシーの管理を許可できます。カスタム ユーザ ロールを作成して、それらのロールにアクセス権を割り当てることで、管理を委任します。委任された管理者が表示および編集できるポリシー、機能、レポート、カスタム URL カテゴリなどを決定します。

詳細については、以下を参照してください。

- 「Custom Email User ロールについて」（P.13-5）
- 「Custom Web User ロールについて」（P.13-9）
- 「カスタム ユーザ ロールの削除」（P.13-11）

Custom Email User ロールについて

カスタム ロールを割り当てると、委任された管理者が セキュリティ管理アプライアンスにある次の項目にアクセスすることを許可できます。

- すべてのレポート（オプションでレポーティング グループによって制限）
- メール ポリシー レポート（オプションでレポーティング グループによって制限）
- DLP レポート（オプションでレポーティング グループによって制限）
- メッセージ トラッキング
- 隔離

これらの各項目の詳細については、以下のセクションで説明します。また、これらの権限を付与されたすべてのユーザは、[管理アプライアンス（Management Appliance）] タブ > [集約管理サービス（Centralized Services）] メニューを使用して、[システム ステータス（System Status）] を表示できます。Custom Email User ロールに割り当てられているユーザは、CLI にアクセスできません。

（注）　電子メール セキュリティ アプライアンスのカスタム ユーザ ロールは、セキュリティ管理アプライアンスのユーザ ロールよりも、より詳細なアクセス権を提供します。たとえば、メールおよび DLP ポリシーと、コンテンツ フィルタへのアクセス権を委任できます。詳細については、お使いの電子メール セキュリティ アプライアンスのマニュアルまたはオンライン ヘルプの「Common Administration」の章の「Managing Custom User Roles for Delegated Administration」のセクションを参照してください。

電子メール レポーティング

次のセクションで説明するように、電子メール レポートへのアクセス権をカスタム ユーザ ロールに付与できます。

セキュリティ管理アプライアンスの [メール セキュリティ モニタ（Email Security Monitor）] ページの詳細については、「中央集中型電子メール セキュリティ レポーティングの使用」の該当する章を参照してください。

すべてのレポート

カスタム ロールにすべてのレポートへのアクセス権を付与すると、このロールを割り当てられたユーザは、すべての 電子メール セキュリティ アプライアンス、または選択したレポーティング グループのいずれかに対する、次の [メール セキュリティ モニタ（Email Security Monitor）] ページを表示できます。

- 概要（Overview）
- 受信メール（Incoming Mail）
- 送信先（Outgoing Destinations）
- 送信メッセージ送信者（Outgoing Senders）
- 内部ユーザ（Internal Users）
- DLP インシデント（DLP Incidents）
- コンテンツ フィルタ（Content Filters）
- ウイルス タイプ（Virus Types）
- TLS 接続（TLS Connections）
- アウトブレイク フィルタ（Outbreak Filters）
- システム容量（System Capacity）
- 有効なレポート データ（Reporting Data Availability）
- 定期レポート（Scheduled Reports）
- アーカイブ レポート（Archived Reports）

メール ポリシー レポート（Mail Policy Reports）

カスタム ロールにメール ポリシー レポートへのアクセス権を付与すると、このロールを割り当てられたユーザは、すべての 電子メール セキュリティ アプライアンス、または選択したレポーティング グループのいずれかに対する、次の [メール セキュリティ モニタ（Email Security Monitor）] ページを表示できます。

- 概要（Overview）
- 受信メール（Incoming Mail）
- 送信先（Outgoing Destinations）
- 送信メッセージ送信者（Outgoing Senders）
- 内部ユーザ（Internal Users）
- コンテンツ フィルタ（Content Filters）
- ウイルス タイプ（Virus Types）
- アウトブレイク フィルタ（Outbreak Filters）
- 有効なレポート データ（Reporting Data Availability）
- アーカイブ レポート（Archived Reports）

DLP レポート（DLP Reports）

カスタム ロールに DLP レポートへのアクセス権を付与すると、このロールを割り当てられたユーザは、すべての 電子メール セキュリティ アプライアンス、または選択したレポーティング グループのいずれかに対する、次の [メール セキュリティ モニタ（Email Security Monitor）] ページを表示できます。

- DLP インシデント（DLP Incidents）

- 有効なレポート データ（Reporting Data Availability）
- アーカイブ レポート（Archived Reports）

メッセージ トラッキング（Message Tracking）

カスタム ロールにメッセージ トラッキングへのアクセス権を付与すると、このロールを割り当てられたユーザは、セキュリティ管理アプライアンスによってトラッキングされたすべてのメッセージのステータスを表示できます。

DLP ポリシーに違反するメッセージ内の機密情報へのアクセスを制御するには、「メッセージ トラッキングでの DLP 機密情報へのアクセスの制御」（P.13-24）を参照してください。

セキュリティ管理アプライアンスでメッセージ トラッキングへのアクセスをイネーブルにするためのアプライアンスの設定方法など、メッセージ トラッキングの詳細については、「電子メール メッセージのトラッキング」を参照してください。

隔離

カスタムロールに隔離へのアクセス権を付与すると、このロールを割り当てられたユーザは、このセキュリティ管理アプライアンスのすべての隔離メッセージを検索、表示、リリース、または削除できます。

ユーザが隔離にアクセスする前にそのアクセスを有効にする必要があります。「「Cisco IronPort スパム隔離への管理者ユーザ アクセスの設定」（P.7-8）」、「「ポリシー隔離の作成」（P.8-12）」、および「「カスタム ユーザ ロールの集約隔離アクセスの設定」（P.8-8）」を参照してください。

セキュリティ管理アプライアンスからこの隔離へのアクセスをイネーブルにするためのアプライアンスの設定方法など、スパム隔離の詳細については、「Cisco IronPort スパム隔離の管理」の章を参照してください。

Custom Email User ロールの作成

電子メール レポーティング、メッセージ トラッキング、および隔離へのアクセスに対して、カスタムのメール ユーザ ロールを作成できます。

これらの各オプションに許可されたアクセス権の詳細については、Custom Email User ロールについてとそのサブセクションを参照してください。

（注） より詳細なアクセス権、または他の機能、レポート、ポリシーへのアクセス権を付与するには、各 電子メール セキュリティ アプライアンスで直接カスタム ユーザ ロールを作成してください。

手順

ステップ 1　[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザ ロール（User Roles）] を選択します。

ステップ 2　[メール ユーザ ロールの追加（Add Email User Role）] をクリックします。

ヒント または、既存の Email User ロールを複製して、新しいロールを作成できます。それには、該当するテーブルの行で [重複（Duplicate）] アイコンをクリックし、生成されたコピーを編集します。

ステップ 3　ユーザ ロールの一意の名前（たとえば「dlp-auditor」）と説明を入力します。

- Email と Web のカスタム ユーザ ロール名を同じにしないでください。
- 名前には、小文字、数字、およびダッシュのみを使用してください。先頭をダッシュまたは数字にすることはできません。
- このロールのユーザに集約ポリシー隔離へのアクセス権限を許可し、このロールのユーザが電子メール セキュリティ アプライアンスのメッセージ フィルタやコンテンツ フィルタおよび DLP メッセージ アクション内にもこれらの集約隔離を指定できるようにする場合、カスタム ロールの名前を両方のアプライアンスで同じにする必要があります。

ステップ 4　このロールに対してイネーブルにするアクセス権限を選択します。

ステップ 5　[送信（Submit）] をクリックして [ユーザ ロール（User Roles）] ページに戻ると、新しいユーザ ロールが表示されます。

ステップ 6　レポーティング グループごとにアクセス権を制限する場合は、該当するユーザ ロールの [メール レポート（Email Reporting）] カラムにある [グループが選択されていません（no groups selected）] リンクをクリックして、少なくとも 1 つのレポーティング グループを選択します。

ステップ 7　変更を保存します。

ステップ 8　このロールに隔離へのアクセス権を付与する場合は、このロールに対してアクセス権を有効にします。

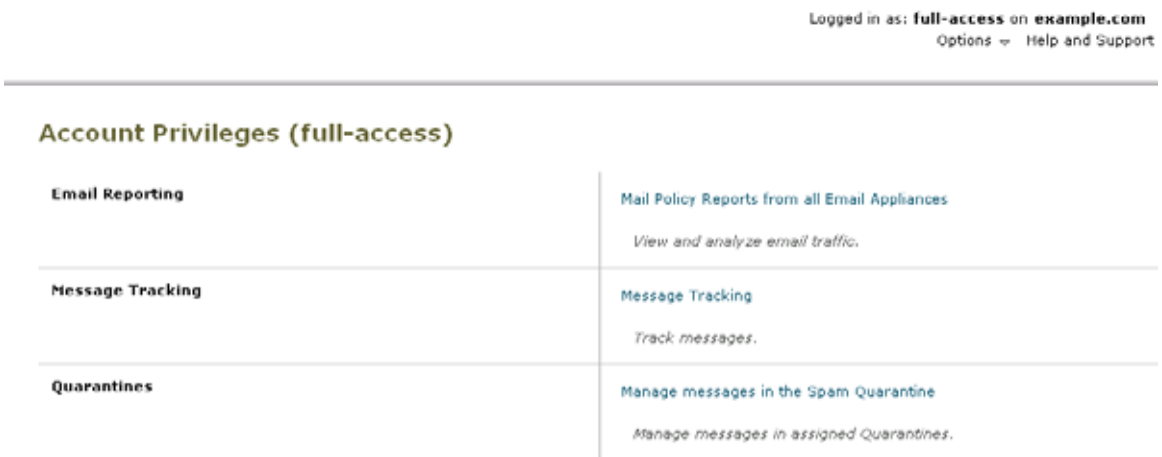
次を参照してください。

- 「Cisco IronPort スパム隔離への管理者ユーザ アクセスの設定」（P.7-8）。
- 「ポリシー隔離の作成」（P.8-12）.

Custom Email User ロールの使用

Custom Email User ロールに割り当てられているユーザがアプライアンスにログインすると、そのユーザには、ユーザがアクセス権を持つセキュリティ機能へのリンクだけが表示されます。そのユーザは、[オプション（Options）] メニューで [アカウント権限（Account Privileges）] を選択することで、いつでもこのメインページに戻ることができます。これらのユーザは、Web ページの上部にあるメニューを使用して、アクセス権を持つ機能にアクセスすることもできます。次の例では、ユーザは Custom Email User ロールによって、セキュリティ管理アプライアンスで使用可能なすべての機能へのアクセス権を持ちます。

図 13-1　Custom Email User ロールが割り当てられている委任管理者の [アカウント権限（Account Privileges）] ページ



Custom Web User ロールについて

Custom Web User ロールでは、ユーザがポリシーを別の Web セキュリティ アプライアンスに公開することができ、カスタム設定を編集したり、別のアプライアンスに公開できるようになります。

セキュリティ管理アプライアンスの [Web] > [設定マスター（Configuration Master）] > [カスタム URL カテゴリ（Custom URL Categories）] ページでは、管理および公開できる URL カテゴリとポリシーを表示できます。また、[Web] > [ユーティリティ（Utilities）] > [今すぐ設定を公開する（Publish Configuration Now）] ページに移動して、可能な設定を表示することもできます。

（注） 公開権限を持つカスタム ロールを作成した場合、ユーザがログインすると、使用可能なメニューが表示されないことに注意してください。URL やポリシー タブが機能を持たないため、このようなユーザには公開メニューが表示されず、編集不可の固定画面が表示されます。つまり、どのカテゴリまたはポリシーも公開または管理できないユーザを作ってしまうことになります。

この問題の回避策としては、ユーザが公開はできるが、どのカテゴリまたはポリシーも管理できないようにする場合、どのポリシーでも使用されていないカスタム カテゴリを作成し、そのユーザに、そのカスタム カテゴリを管理する権限と公開する権限を付与する**必要があります**。このようにすると、ユーザがそのカテゴリで URL を追加または削除しても、他に影響が及びません。

カスタム ユーザ ロールを作成および編集して、Web 管理を委任できます。

- Custom Web User ロールの作成
- Custom Web User ロールの編集

Custom Web User ロールの作成

手順

ステップ 1　[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザ ロール（User Roles）] を選択します。

ステップ 2　[Web ユーザ ロールの追加（Add Web User Role）] をクリックします。

ヒント または、既存の Web User ロールを複製して、新しいロールを作成できます。それには、該当するテーブルの行で [重複（Duplicate）] アイコンをクリックし、生成されたコピーを編集します。

ステップ 3　ユーザ ロールの一意の名前（たとえば「canadian-admins」）と説明を入力します。

（注） 名前には、小文字、数字、およびダッシュのみを使用してください。先頭をダッシュにすることはできません。

ステップ 4　デフォルトで、ポリシーとカスタム URL カテゴリを表示するか、非表示にするかを選択します。

ステップ 5　公開権限をオンにするか、オフにするかを選択します。

この権限を持つユーザは、ユーザがアクセス ポリシーまたは URL カテゴリを編集できるすべての Configuration Master を公開できます。

ステップ 6　新しい（空の）設定で始めるか、既存のカスタム ユーザ ロールをコピーするかを選択します。既存のユーザ ロールをコピーする場合は、コピーするロールをリストから選択します。

ステップ 7　[送信（Submit）] をクリックして [ユーザ ロール（User Roles）] ページに戻ると、新しいユーザ ロールが表示されます。

（注）　Web レポーティングで匿名機能をイネーブルにしていた場合、Web レポーティングへのアクセス権を持つすべてのユーザ ロールには、インタラクティブなレポート ページで認識できないユーザ名とロールが表示されるようになります。第 5 章「中央集中型 Web レポーティングおよびトラッキングの使用」の Web レポートのスケジュール設定のセクションを参照してください。Administrator ロールの場合は例外的に、スケジュール設定されたレポートで実際のユーザ名を確認できます。匿名機能がイネーブルになっている場合、オペレータおよび Web 管理者によって作成されたスケジュール設定されたレポートは匿名になります。

（注）　[Web] > [ユーティリティ（Utilities）] > [セキュリティ サービス表示（Security Services Display）] > [セキュリティ サービス表示の編集（Edit Security Services Display）] ページを使用して Configuration Master の 1 つを非表示にしている場合、[ユーザ ロール（User Roles）] ページでも対応する [設定マスター（Configuration Master）] カラムが非表示になりますが、非表示になっている Configuration Master に対する権限設定は保持されます。

Custom Web User ロールの編集

手順

ステップ 1　[ユーザ ロール（User Roles）] ページでロール名をクリックし、[ユーザ ロールの編集（Edit User Role）] ページを表示します。

ステップ 2　名前、説明、およびポリシーとカスタム URL カテゴリを表示するかどうかなどの設定を編集します。

ステップ 3　[送信（Submit）] をクリックします。

カスタム ユーザ ロールの権限を編集するには、次の手順を実行します。

[ユーザ ロール（User Roles）] ページに移動します。

- アクセス ポリシー権限を編集するには、[アクセス ポリシー（Access policies）] をクリックして、Configuration Master に設定されているアクセス ポリシーのリストを表示します。[含める（Include）] カラムで、ユーザ編集アクセス権を付与するポリシーのチェックボックスをオンにします。[送信（Submit）] をクリックして、[ユーザ ロール（User Roles）] ページに戻ります。

または

- カスタム URL カテゴリ権限を編集するには、カスタム URL カテゴリをクリックして、Configuration Master に定義されているカスタム URL カテゴリのリストを表示します。[含める（Include）] カラムで、ユーザ編集アクセス権を付与するカスタム URL カテゴリのチェックボックスをオンにします。[送信（Submit）] をクリックして、[ユーザ ロール（User Roles）] ページに戻ります。

カスタム ユーザ ロールの削除

1 人以上のユーザに割り当てられているカスタム ユーザ ロールを削除する場合、エラーは受信しません。

管理ユーザの認証の管理

許可されたユーザをアプライアンスでローカルに定義したり、外部認証を使用することで、アプライアンスに対するアクセスを制御できます。

- 「管理者ユーザのパスワード変更」（P.13-11）
- 「Locally-Defined 管理ユーザの管理」（P.13-11）
- 「外部ユーザ認証」（P.13-18）

管理者ユーザのパスワード変更

「管理者」ユーザのパスワードは GUI または CLI から変更できます。

GUI を使用してパスワードを変更するには、[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザ（Users）] ページを選択して、管理ユーザを選択します。

管理者ユーザのパスワードを CLI から変更するには `password` コマンドを使用します。パスワードは 6 文字以上である必要があります。`password` コマンドでは、セキュリティのために古いパスワードの入力が必要です。

管理者ユーザ アカウントのパスワードを忘れた場合は、パスワードをリセットするためにカスタマー サポート プロバイダーにご連絡ください。

（注）　パスワードの変更はすぐに有効になり、変更を送信する必要がありません。

Locally-Defined 管理ユーザの管理

- 「Locally-Defined ユーザの追加」（P.13-12）
- 「Locally-Defined ユーザの編集」（P.13-12）
- 「Locally-Defined ユーザの削除」（P.13-13）
- 「ローカルに定義されたユーザのリストの表示」（P.13-13）
- 「パスワードの設定と変更」（P.13-13）
- 「パスワードの設定およびログインの要件」（P.13-13）
- 「ユーザに対する次回ログイン時のパスワード変更の義務付け」（P.13-16）
- 「ローカル ユーザ アカウントのロックおよびロック解除」（P.13-17）

Locally-Defined ユーザの追加

外部認証を使用していない場合は、次の手順に従って、ユーザを セキュリティ管理アプライアンスに直接追加します。または、CLI で **userconfig** コマンドを使用します。

（注）　外部認証もイネーブルである場合は、ローカル ユーザ名が外部認証されたユーザ名と重複しないことを確認してください。

アプライアンスに作成できるユーザ アカウントの数に制限はありません。

手順

ステップ 1　カスタム ユーザ ロールを割り当てる場合は、そのロールを先に定義しておくことを推奨します。「カスタム ユーザ ロール」（P.13-5）を参照してください。

ステップ 2　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザ（Users）] を選択します。

ステップ 3　[ユーザを追加（Add User）] をクリックします。

ステップ 4　ユーザの一意の名前を入力します。システムで予約されている語（「operator」や「root」など）を入力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。

ステップ 5　ユーザの氏名を入力します。

ステップ 6　事前定義されたロールまたはカスタム ロールを選択します。ユーザ ロールの詳細については、表 13-1 を参照してください。

新しい Email ロールまたは Web ロールをここに追加する場合は、ロールの名前を入力します。命名上の制限については、「Custom Email User ロールの作成」（P.13-7）または「Custom Web User ロールの作成」（P.13-9）を参照してください。

ステップ 7　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 8　変更を送信し、保存します。

ステップ 9　このページにカスタム ユーザ ロールを追加する場合は、この時点でそのロールに権限を割り当てます。「カスタム ユーザ ロール」（P.13-5）を参照してください。

Locally-Defined ユーザの編集

たとえば、パスワードを変更するには、次の手順を実行します。

手順

ステップ 1　[ユーザ（Users）] 一覧でユーザの名前をクリックします。

ステップ 2　ユーザに対して変更を行います。

ステップ 3　変更を送信し、保存します。

Locally-Defined ユーザの削除

手順

ステップ 1　[ユーザ（Users）] 一覧でユーザの名前に対応するゴミ箱のアイコンをクリックします。

ステップ 2　表示される警告ダイアログで [削除（Delete）] をクリックして削除を確認します。

ステップ 3　[確定する（Commit）] をクリックして変更を保存します。

ローカルに定義されたユーザのリストの表示

ローカルに定義されたユーザのリストを表示するには、[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザ（Users）] を選択します。

（注）　アスタリスクは、委任された管理に応じてユーザに割り当てられたカスタム ユーザ ロールを示します。ユーザのカスタム ロールが削除された場合は、[割り当てなし（Unassigned）] と赤く表示されます。カスタム ユーザ ロールの詳細については、「カスタム ユーザ ロール」（P.13-5）を参照してください。

パスワードの設定と変更

- ユーザを追加する場合は、そのユーザに初期パスワードを指定します。
- システムに設定されたユーザのパスワードを変更するには、GUI の [ユーザの編集（Edit User）] ページを使用します（詳細は、「Locally-Defined ユーザの編集」（P.13-12）を参照してください）。
- システムのデフォルト管理ユーザ アカウントのパスワードを変更するには、「管理者ユーザのパスワード変更」（P.13-11）を参照してください。
- ユーザにパスワードの変更を強制するには、「ユーザに対する次回ログイン時のパスワード変更の義務付け」（P.13-16）を参照してください。
- GUI 右側上部の [オプション（Options）] メニューをクリックして、[パスワードの変更（Change Password）] オプションを選択することで、ユーザは自分のパスワードを変更できます。

  [パスワードの変更（Change Password）] ページで、古いパスワードを入力してから、新しいパスワードを入力し、確認のため、その新しいパスワードを再入力します。[送信（Submit）] をクリックして、ログアウトします。ログイン画面が表示されます。

パスワードの設定およびログインの要件

ユーザ アカウントとパスワードの制限を定義して、組織全体にパスワード ポリシーを強制的に適用することができます。ユーザ アカウントとパスワードの制限は、セキュリティ管理アプライアンスで定義されているローカル ユーザに適用されます。次の設定値を設定できます。

- **ユーザ アカウントのロック。**ユーザがアカウントからロックアウトされるまでの、ログイン試行の失敗回数を定義できます。
- **パスワード期限の規則。**ログイン後にユーザがパスワードの変更を要求されるまでの、パスワードの使用期間を定義できます。
- **パスワードの規則。**どの文字が任意で、どの文字が必須かなど、ユーザが選択できるパスワードの種類を定義できます。

手順

ステップ 1　[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザ（Users）] を選択します。

ステップ 2　[ローカル ユーザ アカウントとパスワードの設定（Local User Account and Password Settings）] セクションまでページを下にスクロールします。

ステップ 3　[設定を編集（Edit Settings）] をクリックします。

ステップ 4　表 13-2 に示す設定値を設定します。

表 13-2　ローカル ユーザ アカウントとパスワードの設定

設定	説明
ユーザ アカウントのロック（User Account Lock）	ユーザが正常にログインできない場合に、ユーザ アカウントをロックするかどうかを決定します。アカウントがロックされるまでの、ログイン失敗回数を指定します。1 ～ 60 の範囲で任意の数字を入力できます。デフォルト値は 5 です。 アカウントのロックを設定する場合は、ログインしようとしているユーザに表示されるメッセージを入力します。7 ビットの ASCII 文字を使用して、テキストを入力します。このメッセージは、ユーザがロックされたアカウントに正しいパスワードを入力した場合だけ表示されます。 ユーザ アカウントがロックされた場合は、管理者が GUI の [ユーザの編集（Edit User）] ページか、`userconfig` CLI コマンドを使用して、ロック解除できます。 ユーザが接続に使用したマシン、または接続の種類（SSH または HTTP）に関係なく、失敗したログイン試行はユーザごとに追跡されます。ユーザが正常にログインすると、失敗したログイン試行回数はゼロ（0）にリセットされます。 失敗したログイン試行の最大数に達したためにユーザ アカウントがロックアウトされた場合、アラートが管理者に送信されます。このアラートは「Info」重大度レベルに設定されます。 **（注）**　個々のユーザ アカウントを手動でロックすることもできます。「手動によるユーザ アカウントのロック」（P.13-17）を参照してください。

表 13-2　ローカル ユーザ アカウントとパスワードの設定 （続き）

設定	説明
パスワードのリセット（Password Reset）	管理者がユーザのパスワードを変更後、ユーザにパスワードの変更を強制するかどうかを決定します。 また、パスワードの有効期限が切れた後に、ユーザにパスワードの変更を強制するかどうかを決定することもできます。ユーザによるパスワードの変更が必要になるまでの、パスワードの有効日数を入力します。1 ～ 366 の範囲で任意の数字を入力できます。デフォルトは 90 です。スケジュール外の時間に、ユーザにパスワードの変更を強制するには、「ユーザに対する次回ログイン時のパスワード変更の義務付け」（P.13-16）を参照してください。 パスワードの期限が切れた後、ユーザにパスワードの変更を強制する場合は、次回のパスワード期限切れについての通知を表示できます。期限切れの何日前に通知が行われるかを選択します。 パスワードが期限切れになると、ユーザは次回のログイン時にアカウント パスワードの変更を強制されます。 **（注）** ユーザ アカウントがパスワード チャレンジではなく SSH キーを使用している場合も、パスワードのリセット規則は適用されます。SSH キーを持つユーザ アカウントが期限切れになると、そのユーザは古いパスワードを入力するか、管理者に依頼して、パスワードを手動で変更し、アカウントに関連付けられたキーを変更してもらう必要があります。
パスワードルール：（Password Rules:） <number> 文字以上必要です。（Require at least <number> characters.）	パスワードに含める最小文字数を入力します。 ゼロ（0）以上のどんな数字も入力できます。
パスワードルール：（Password Rules:） 数字（0 ～ 9）が 1 文字以上必要です。（Require at least one number (0-9).）	パスワードに 1 文字以上の数字を含める必要があるかどうかを決定します。
パスワードルール：（Password Rules:） 特殊文字が 1 文字以上必要です。（Require at least one special character.）	パスワードに 1 文字以上の特殊文字を含める必要があるかどうかを決定します。パスワードには、次の特殊文字を使用できます。 ~ ?!@ # $ % ^ & * - _ + = \ | / [ ] ( ) < > { } ` ' " ; : , .

表 13-2　ローカル ユーザ アカウントとパスワードの設定 （続き）

設定	説明
パスワードルール：（Password Rules:） ユーザ名とその変化形をパスワードとして使用することはできません。（Ban usernames and their variations as passwords.）	対応するユーザ名またはユーザ名の変化形と同じものを、パスワードに使用できるかどうかを決定します。ユーザ名の変化形の使用を禁止する場合、次の規則がパスワードに適用されます。 • 大文字か小文字かに関係なく、パスワードはユーザ名と同じであってはならない。 • 大文字か小文字かに関係なく、パスワードはユーザ名を逆にしたものと同じであってはならない。 • パスワードは、次の文字置換が行われたユーザ名、またはユーザ名を逆にしたものと同じであってはならない。 – 「a」の代わりに「@」または「4」 – 「e」の代わりに「3」 – 「i」の代わりに「|」、「!」、または「1」 – 「o」の代わりに「0」 – 「s」の代わりに「$」または「5」 – 「t」の代わりに「+」または「7」
パスワードルール：（Password Rules:） 直近 <number> 個のパスワードを再使用することはできません。（Ban reuse of the last <number> passwords.）	ユーザにパスワードの変更を強制する場合に、最近使用したパスワードを選択できるかどうかを決定します。最近のパスワードの再利用を禁止した場合、再利用を禁止する最近のパスワードの個数を入力します。 1 ～ 15 の範囲で任意の数字を入力できます。デフォルトは 3 です。

ステップ 5　変更を送信し、保存します。

ユーザに対する次回ログイン時のパスワード変更の義務付け

すべての、または選択したユーザに、次回セキュリティ管理アプライアンスにアクセスしたときにパスワードを変更するように要求するには、次の手順を実行します。これは 1 回限りのアクションです。

パスワードを変更するための定期的な要求を自動化するには、「パスワードの設定およびログインの要件」（P.13-13）で説明されている [パスワードのリセット（Password Reset）] オプションを使用します。

手順

ステップ 1　[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザ（Users）] を選択します。

ステップ 2　[ユーザ（Users）] セクションで、次回のログインでパスワードの変更が必要なユーザの横のチェックボックスを選択します。

ステップ 3　[パスワードのリセット（Password Reset）] をクリックします。

ローカル ユーザ アカウントのロックおよびロック解除

ユーザ アカウントのロックは、ローカル ユーザがアプライアンスにログインするのを防止します。ユーザ アカウントは、次のいずれかの場合にロックされることがあります。

- すべてのローカル ユーザ アカウントを、設定した試行回数の後にユーザが正常なログインに失敗するとロックするように、設定することができます。「パスワードの設定およびログインの要件」（P.13-13）を参照してください。
- 管理者はユーザ アカウントを手動でロックできます。「手動によるユーザ アカウントのロック」（P.13-17）を参照してください。

[ユーザの編集（Edit User）] ページでユーザ アカウントを表示すると、AsyncOS によりユーザ アカウントがロックされた理由が表示されます。

手動によるユーザ アカウントのロック

手順

ステップ 1　初回のみ：アプライアンスを設定して、ユーザ アカウントのロックをイネーブルにします。

a. [管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザ（Users）] に移動します。

b. [ローカル ユーザ アカウントとパスワードの設定（Local User Account & Password Settings）] セクションで、[設定を編集（Edit Settings）] をクリックします。

c. [管理者が手動でユーザ アカウントをロックしている場合、ロックされているアカウント メッセージを表示する（Display Locked Account Message if Administrator has manually locked a user account）] に対するチェックボックスを選択して、メッセージを入力します。

d. 変更を送信します。

ステップ 2　[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザ（Users）] に移動して、ユーザ名をクリックします。

（注）　admin アカウントをロックする前に、ロック解除できることを確認してください。「ユーザ アカウントのロック解除」（P.13-17）の（注）を参照してください。

ステップ 3　[アカウントのロック（Lock Account）] をクリックします。

AsyncOS は、ユーザがアプライアンスにログインできなくなるというメッセージを表示し、継続するかどうかを問い合わせてきます。

ユーザ アカウントのロック解除

ユーザ アカウントをロック解除するには、[ユーザ（Users）] 一覧でユーザ名をクリックしてユーザ アカウントを開き、[アカウントのロック解除（Unlock Account）] をクリックします。

（注）　admin アカウントをロックした場合は、シリアル コンソール ポートへのシリアル通信接続経由で admin としてログインしてロック解除するしかありません。admin ユーザは、admin アカウントがロックされた場合でも、シリアル コンソール ポートを使用して常にアプライアンスにアクセスできます。シリアル コンソール ポートを使用してアプライアンスにアクセスする方法の詳細については、お使いの電子メール セキュリティ アプライアンスのマニュアルまたはオンライン ヘルプの「Setup and Installation」の章を参照してください。

外部ユーザ認証

ネットワークの LDAP または RADIUS ディレクトリにユーザ情報を保存する場合は、外部ディレクトリを使用してアプライアンスにログインするユーザを認証するよう セキュリティ管理アプライアンスを設定できます。

（注）
- 「ビューのカスタマイズ」（P.14-57）で説明されている一部の機能は、外部認証ユーザには使用できません。
- 展開でローカル認証と外部認証の両方を使用している場合、ローカル ユーザ名と外部認証ユーザ名を同じにしないでください。
- アプライアンスが外部ディレクトリと通信できない場合、外部アカウントとローカル アカウントの両方を持つユーザは、ローカル ユーザ アカウントを使用してアプライアンスにログインできます。

LDAP 認証の設定

LDAP 認証を設定するには、「LDAP を使用した管理ユーザの外部認証の設定」（P.11-14）を参照してください。

RADIUS 認証のイネーブル化

ユーザを認証し、アプライアンスを管理しているユーザ ロールにユーザ グループを割り当てるために RADIUS ディレクトリを使用できます。RADIUS サーバは CLASS 属性をサポートする必要があります（AsyncOS は RADIUS ディレクトリのユーザをユーザ ロールに割り当てるために CLASS 属性を使用します）。

（注）　外部ユーザが RADIUS グループのユーザ ロールを変更する場合、外部ユーザはアプライアンスからログアウトし、再びログインする必要があります。このユーザは新しいロールの権限を持ちます。

はじめる前に

RADIUS サーバへの共有シークレット キーの長さは 48 文字以下でなければなりません。

手順

ステップ 1　[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザ（Users）] ページで、[有効（Enable）] をクリックします。

ステップ 2　[外部認証を有効にする（Enable External Authentication）] チェックボックスをオンにします。

ステップ 3　認証タイプとして RADIUS を選択します。

ステップ 4　RADIUS サーバのホスト名を入力します。

ステップ 5　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 6　RADIUS サーバの共有シークレット キーを入力します。

（注）　電子メール セキュリティ アプライアンスのクラスタに対して外部認証を有効にするには、クラスタ内のすべてのアプライアンスで同じ共有シークレット キーを入力します。

ステップ 7　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 8　認証プロトコルとして、パスワード認証プロトコル（PAP）を使用するか、またはチャレンジ ハンドシェイク認証プロトコル（CHAP）を使用するか選択します。

ステップ 9　（任意）[行の追加（Add Row）] をクリックして別の RADIUS サーバを追加します。認証のためにアプライアンスで使用する各 RADIUS サーバに対してステップ 6 とステップ 7 を繰り返します。

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。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場合があります。

ステップ 10　Web ユーザ インターフェイスで、外部認証クレデンシャルを保存する時間を入力します。

（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 11　グループ マッピングの設定

設定	説明
外部認証されたす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）（推奨）	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。 • Administrator • Email Administrator • Web Administrator • Web Policy Administrator • URL Filtering Administrator • カスタム ユーザ ロール（電子メールまたは Web） ユーザにカスタム ユーザ ロールにマッピングされた複数のクラス属性が割り当てられている場合、RADIUS サーバのリストの最後のクラス属性が使用されます。 • Technician • Operator • Read-Only Operator • Help Desk User • Guest
外部認証されたすべてのユーザを管理者に割り当てます（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 12　（任意）[行の追加（Add Row）] をクリックして別のグループを追加します。アプライアンスが認証するユーザの各グループに対してステップ 11 を繰り返します。

ステップ 13　変更を送信し、保存します。

セキュリティ管理アプライアンスへのアクセスに対する追加の制御

IP ベースのネットワーク アクセスの設定

組織がリモート ユーザに逆プロキシを使用する場合、アプライアンスに直接接続するユーザ、および逆プロキシを介して接続するユーザのためのアクセス リストを作成することで、ユーザがどの IP アドレスからセキュリティ管理アプライアンスにアクセスするのかを制御できます。

直接接続

セキュリティ管理アプライアンスに接続できるマシンの IP アドレス、サブネット、または CIDR アドレスを指定できます。ユーザは、アクセス リストの IP アドレスを持つすべてのマシンから、アプライアンスにアクセスできます。リストに含まれていないアドレスからアプライアンスに接続しようとするユーザは、アクセスを拒否されます。

プロキシ経由の接続

組織のネットワークで、リモート ユーザのマシンとセキュリティ管理アプライアンスの間で逆プロキシが使用されている場合、AsyncOS では、アプライアンスに接続できるプロキシの IP アドレスのアクセス リストを作成できます。

逆プロキシを使用している場合でも、AsyncOS は、ユーザ接続が許可されている IP アドレスのリストと照合して、リモート ユーザのマシンの IP アドレスを検証します。リモート ユーザの IP アドレスを電子メール セキュリティ アプライアンスに送信するには、プロキシで `x-forwarded-for` HTTP ヘッダーをアプライアンスへの接続要求に含める必要があります。

`x-forwarded-for` ヘッダーは非 RFC 標準 HTTP ヘッダーであり、形式は次のとおりです。

```
x-forwarded-for: client-ip, proxy1, proxy2,... CRLF.
```

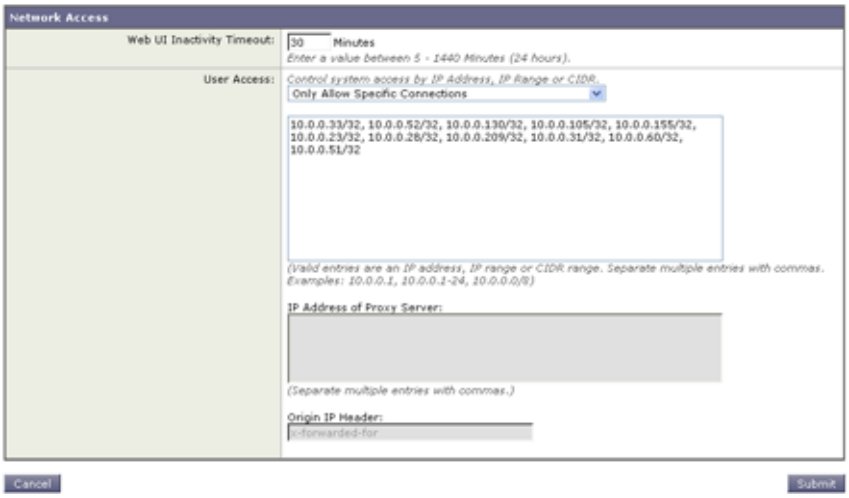
このヘッダーの値はカンマ区切りの IP アドレスのリストであり、左端のアドレスがリモート ユーザ マシンのアドレスで、その後に、接続要求を転送した一連の各プロキシのアドレスが続きます。（ヘッダー名は設定可能です）。セキュリティ管理アプライアンスは、ヘッダーから取得したリモート ユーザの IP アドレスおよび接続プロキシの IP アドレスを、アクセス リスト内の許可されたユーザ IP アドレスおよびプロキシ IP アドレスと照合します。

（注）　AsyncOS は、`x-forwarded-for` ヘッダーで IPv4 アドレスだけをサポートします。

アクセス リストの作成

GUI の [ネットワーク アクセス（Network Access）] ページまたは CLI の **adminaccessconfig > ipaccess** コマンドから、ネットワーク アクセス リストを作成できます。図 13-2 は、セキュリティ管理アプライアンスへの直接的な接続が許可されているユーザ IP アドレスのリストが表示された [ネットワークアクセス（Network Access）] ページを示しています。

図 13-2　ネットワーク アクセス設定の例



AsyncOS には、アクセス リストに対する次の 4 つの異なる制御モードが用意されています。

- [すべてを許可（Allow All）]。このモードでは、アプライアンスへのすべての接続が許可されます。これが、デフォルトの動作モードです。
- [特定の接続のみを許可（Only Allow Specific Connections）]。このモードは、ユーザの IP アドレスが、アクセス リストに含まれている IP アドレス、IP 範囲、または CIDR 範囲と一致する場合に、ユーザのアプライアンスへの接続を許可します。
- [特定のプロキシ経由接続のみを許可（Only Allow Specific Connections Through Proxy）]。このモードは、次の条件が満たされた場合に、逆プロキシを介したユーザのアプライアンスへの接続を許可します。
  - 接続プロキシの IP アドレスが、[プロキシ サーバ（Proxy Server）] フィールドのアクセス リストの IP アドレスに含まれている。
  - プロキシで、接続要求に `x-forwarded-header` HTTP ヘッダーが含まれている。
  - `x-forwarded-header` の値が空ではない。
  - リモート ユーザの IP アドレスが `x-forwarded-header` に含まれ、それがアクセス リスト内の IP アドレス、IP 範囲、または CIDR 範囲と一致する。
- [特定の直接またはプロキシ経由接続のみを許可（Only Allow Specific Connections Directly or Through Proxy）]。このモードは、ユーザの IP アドレスが、アクセス リストに含まれている IP アドレス、IP 範囲、または CIDR 範囲と一致する場合に、ユーザの逆プロキシを介した、あるいは直接的なアプライアンスへの接続を許可します。プロキシを介した接続の条件は、[特定のプロキシ経由接続のみを許可（Only Allow Specific Connections Through Proxy）] モードの場合と同じです。

次のいずれかの条件に該当する場合、変更をサブミットおよびコミットした後に、アプライアンスにアクセスできなくなる可能性があります。

- [特定の接続のみを許可（Only Allow Specific Connections）] を選択し、現在のマシンの IP アドレスがリストに含まれていない場合。
- [特定のプロキシ経由接続のみを許可（Only Allow Specific Connections Through Proxy）] を選択し、アプライアンスに現在接続されているプロキシの IP アドレスがプロキシ リストになく、元の IP ヘッダーの値が許可された IP アドレスのリストにない場合。
- [特定の直接またはプロキシ経由接続のみを許可（Only Allow Specific Connections Directly or Through Proxy）] を選択し、次が当てはまる場合。
  - 元の IP ヘッダーの値が許可される IP アドレスのリストにない

    または
  - 元の IP ヘッダーの値が許可される IP アドレスのリストになく、アプライアンスに接続されているプロキシの IP アドレスが許可されるプロキシのリストにない。

アクセス リストを修正せずに続行した場合、ユーザが変更を確定すると、AsyncOS はアプライアンスからユーザのマシンまたはプロキシを切断します。

手順

ステップ 1　[システム管理（System Administration）] > [ネットワーク アクセス（Network Access）] を選択します。

ステップ 2　[設定を編集（Edit Settings）] をクリックします。

ステップ 3　アクセス リストの制御モードを選択します。

ステップ 4　ユーザがアプライアンスへの接続が許可される IP アドレスを入力します。

IP アドレス、IP アドレス範囲または CIDR 範囲を入力できます。複数のエントリを区切るには、カンマを使用します。

ステップ 5　プロキシ経由の接続が許可されている場合は、次の情報を入力します。

- アプライアンスへの接続が許可されているプロキシの IP アドレス。複数のエントリを区切るには、カンマを使用します。
- プロキシがアプライアンスに送信する発信元の IP ヘッダーの名前。これには、リモート ユーザ マシンの IP アドレスと、要求を転送したプロキシ サーバの IP アドレスが含まれます。デフォルトでは、ヘッダーの名前が `x-forwarded-for` です。

ステップ 6　変更を送信し、保存します。

Web UI セッション タイムアウトの設定

セキュリティ管理アプライアンスの Web UI から AsyncOS が、非アクティブなユーザをログアウトするまでの時間を指定できます。この Web UI セッション タイムアウトは、admin を含めて、すべてのユーザに適用され、また HTTP セッションと HTTPS セッションの両方に使用されます。

AsyncOS によってユーザがログアウトされると、アプライアンスはユーザの Web ブラウザをログイン ページにリダイレクトします。

（注）　Web UI セッション タイムアウトは IronPort スパム隔離セッションには適用されません。このセッションには 30 分のタイムアウトが設定されており、変更できません。

手順

ステップ 1　[システム管理（System Administration）] > [ネットワーク アクセス（Network Access）] ページを使用します。

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　ユーザが非アクティブ状態になった後、何分経過後にログアウトされるかを入力します。タイムアウト時間には 5 ～ 1440 分を定義できます。

ステップ 4　変更を送信し、保存します。

メッセージ トラッキングでの DLP 機密情報へのアクセスの制御

データ漏洩防止（DLP）ポリシーに違反するメッセージには、通常、企業の機密情報や個人情報（クレジット カード番号や健康診断結果など）といった機密情報が含まれています。デフォルトで、この内容はメッセージ トラッキング結果に表示されているメッセージの [メッセージの詳細（Message Details）] ページにある [DLP に一致した内容（DLP Matched Content）] タブに表示されます。

このタブとその内容は、割り当てられている事前定義されたロールまたはカスタム ロールに基づいて、セキュリティ管理アプライアンスのユーザには表示されないようにすることができます。

手順

ステップ 1　[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザ（Users）] ページに移動します。

ステップ 2　[DLP トラッキング権限（DLP Tracking Privileges）] セクションで、[設定を編集（Edit Settings）] をクリックします。

ステップ 3　メッセージ トラッキングでの DLP データへのアクセス権を付与するロールを選択します。

メッセージ トラッキングへのアクセス権を持つカスタム ロールだけが一覧表示されます。

ステップ 4　変更を送信し、保存します。

この設定を有効にするには、[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] で中央集中型電子メール メッセージ トラッキング機能をイネーブルにする必要があります。

管理ユーザ アクティビティの表示

- 「Web を使用したアクティブなセッションの表示」（P.13-25）
- 「コマンドライン インターフェイスを介した管理ユーザ アクティビティの表示」（P.13-25）

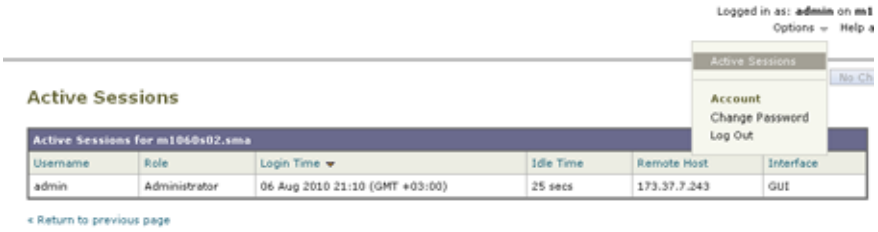
Web を使用したアクティブなセッションの表示

セキュリティ管理アプライアンスでは、すべてのアクティブなセッションと、アプライアンスにログインしているユーザを表示できます。

手順

ステップ 1　ウィンドウの右上から、[オプション（Options）] > [アクティブなセッション（Active Sessions）] を選択します。

図 13-3　[アクティブなセッション（Active Sessions）] メニュー



[アクティブなセッション（Active Sessions）] ページから、ユーザ名、ユーザが持っているロール、ユーザのログイン時間、アイドル時間、およびユーザがコマンドラインと GUI のどちらからログインしたかを表示できます。

コマンドライン インターフェイスを介した管理ユーザ アクティビティの表示

次に、アプライアンスへの複数ユーザ アクセスをサポートするコマンドを示します。

- **who** コマンドは、CLI からシステムにログインしたすべてのユーザ、ログイン時間、アイドル時間、およびユーザがログインしたリモート ホストを一覧表示します。

```
mail3.example.com> who

Username  Login Time  Idle Time  Remote Host  What
========  ==========  =========  ===========  ====
admin     03:27PM     0s         10.1.3.201   cli
```

- `whoami` コマンドは、現在ログインしているユーザのユーザ名および氏名と、ユーザが属しているグループを表示します。

```
mail3.example.com> whoami

Username: admin
Full Name: Administrator
Groups: admin, operators, config, log, guest
```

- `last` コマンドは、アプライアンスに最近ログインしたユーザを表示します。リモート ホストの IP アドレス、ログイン、ログアウト、および合計時間も表示されます。

```
mail3.example.com> last

Username  Remote Host  Login Time        Logout Time       Total Time
```

```
========  ===========  ================  ================  ==========
admin     10.1.3.67    Sat May 15 23:42  still logged in   15m
admin     10.1.3.67    Sat May 15 22:52  Sat May 15 23:42  50m
admin     10.1.3.67    Sat May 15 11:02  Sat May 15 14:14  3h 12m
admin     10.1.3.67    Fri May 14 16:29  Fri May 14 17:43  1h 13m
shutdown                                 Fri May 14 16:22
shutdown                                 Fri May 14 16:15
admin     10.1.3.67    Fri May 14 16:05  Fri May 14 16:15  9m
admin     10.1.3.103   Fri May 14 16:12  Fri May 14 16:15  2m
admin     10.1.3.103   Thu May 13 09:31  Fri May 14 14:11  1d 4h 39m
admin     10.1.3.135   Fri May 14 10:57  Fri May 14 10:58  0m
admin     10.1.3.67    Thu May 13 17:00  Thu May 13 19:24  2h 24m
```

CHAPTER 14

一般的な管理タスク

管理タスクの実行

システム管理タスクのほとんどは、グラフィカル ユーザ インターフェイス（GUI）の [システム管理（System Administration）] メニューを使用して実行できます。ただし、一部のシステム管理機能は、コマンドライン インターフェイス（CLI）からのみ実行できます。

また、第 10 章「システム ステータスのモニタリング」で説明されているように、[モニタ（Monitor）] メニューでアプライアンスのステータス モニタリング機能を使用することができます。

（注） この章で説明する機能やコマンドの中には、ルーティングの優先順位に影響を及ぼすものがあります。詳細については、「IP アドレス、インターフェイス、およびルーティング」（P.B-3）を参照してください。

ライセンス キーでの作業

セキュリティ管理アプライアンスで、GUI を使用して [管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ライセンス キー（Feature Keys）] を選択して（またはコマンドライン プロンプトから **featurekey** コマンドで）キーを入力し、関連する機能を有効にします。

キーは、アプライアンスのシリアル番号に固有のものであり、またイネーブルにする機能にも固有です。1 つのシステムのキーを、別のシステムで再利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。

Cisco カスタマー サポートは、システム上で特定の機能を有効にするキーを提供する場合があります。

[ライセンス キー（Feature Keys）] ページと [ライセンス キーの設定（Feature Key Settings）] ページの 2 つのページで、ライセンス キーの機能が提供されます。

[ライセンス キー（Feature Keys）] ページ

セキュリティ管理アプライアンスにログインし、[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ライセンス キー（Feature Keys）] を選択します。[ライセンス キー（Feature Keys）] ページでは、次の作業を実行します。

- アプライアンスのアクティブなライセンス キーをすべて表示する。
- アクティベーションを保留中のすべてのライセンス キーを表示する。
- 発行された新しいキーを検索する。
- ライセンス キーをインストールする。

[ライセンスキーの状態　シリアル番号: <*Serial Number*>（Feature Keys for Serial Number: <*Serial Number*>）] セクションには、アプライアンスに対してイネーブルとなっている機能の一覧が表示されます。[保留中のライセンス（Pending Activation）] セクションには、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ライセンス キーの一覧が表示されます。デフォルトでは、アプライアンスは、新しいキーを定期的に確認します。アプライアンス設定を変更すると、この動作を変更できます。さらに、[新しいキーをチェック（Check for New Keys）] ボタンをクリックして、保留中のキーの一覧をリフレッシュできます。

新しいライセンス キーを手動で追加するには、[ライセンス キー（Feature Key）] フィールドにキーを貼り付けるか、または入力し、[キーを設定（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（たとえば、キーが正しくない場合など）。それ以外の場合は、ライセンス キーがリストに追加されます。

[保留中のライセンス（Pending Activation）] リストの新しいライセンス 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選択）、[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）] リスト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

[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ライセンス キーの設定（Feature Key Settings）] ページを使用して、アプライアンスが新しいライセンス キーがあるか確認し、ダウンロードするかどうか、またキーが自動的にアクティベートされるかどうかを制御します。

期限切れライセンス キー

アクセスしようとしている機能のライセンス キーの有効期限が切れている場合は、シスコ担当者または他のカスタマー サポート組織までご連絡ください。

CLI コマンドを使用したメンテナンス作業の実行

ここで説明する操作とコマンドを利用すると、セキュリティ管理アプライアンス上でメンテナンスに関連する作業を実行できます。ここでは、次の操作とコマンドについて説明します。

- **shutdown**
- **reboot**
- **suspend**
- **offline**
- **resume**
- **resetconfig**
- **version**

セキュリティ管理アプライアンスのシャットダウン

セキュリティ管理アプライアンスをシャットダウンするには、[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [シャットダウン / 再起動（Shutdown/Reboot）] ページを使用するか、コマンドライン プロンプトで **shutdown** コマンドを使用します。

アプライアンスをシャットダウンすると、AsyncOS が終了し、アプライアンスの電源を安全にオフにできます。アプライアンスは、配信キューのメッセージを失わずに後で再起動できます。アプライアンスをシャットダウンする遅延値を入力する必要があります。デフォルト遅延値は 30 秒です。AsyncOS では、その遅延値の間はオープン中の接続を完了できます。その遅延値を超えると、オープン中の接続が強制的に閉じられます。

セキュリティ管理アプライアンスのリブート

セキュリティ管理アプライアンスをリブートするには、GUI の [システム管理（System Administration）] メニューで利用可能な [シャットダウン / 再起動（Shutdown/Reboot）] ページを使用するか、CLI で `reboot` コマンドを使用します。

アプライアンスをリブートすると、AsyncOS が再起動されるため、アプライアンスの電源を安全にオフにし、アプライアンスをリブートできます。アプライアンスをシャットダウンする遅延値を入力する必要があります。デフォルト遅延値は 30 秒です。AsyncOS では、その遅延値の間はオープン中の接続を完了できます。その遅延値を超えると、オープン中の接続が強制的に閉じられます。アプライアンスを再起動しても、配信キューのメッセージは失われません。

セキュリティ管理アプライアンスをメンテナンス状態にする

システム メンテナンスを行う場合は、セキュリティ管理アプライアンスをオフライン状態にします。suspend および offline コマンドは、AsyncOS をオフライン状態にします。オフライン状態では、次のようになります。

- 着信電子メール接続は受け入れられません。
- 発信電子メール配信は停止されます。
- ログ転送は停止されます。
- CLI はアクセス可能のままになります。

オフライン状態にするアプライアンスの遅延値を入力する必要があります。デフォルト遅延値は 30 秒です。AsyncOS では、その遅延値の間はオープン中の接続を完了できます。その遅延値を超えると、オープン中の接続が強制的に閉じられます。オープン中の接続がない場合は、すぐにオフライン状態になります。

（注）　**suspend** コマンドと **offline** コマンドの相違点は、**suspend** コマンドはマシンがリブートされた後でもその状態を保つことです。**suspend** コマンドを発行してからアプライアンスをリブートする場合は、**resume** コマンドを使用してシステムをオンライン状態に戻す必要があります。

関連項目：

- お使いの電子メール セキュリティ アプライアンスのマニュアルまたはオンライン ヘルプの「Suspending Email Delivery」、「Resuming Email Delivery」、「Suspending Receiving」、および「Resuming Receiving」。

suspend および offline コマンド

```
mail3.example.com> suspend

Enter the number of seconds to wait before abruptly closing connections.
[30]> 45

Waiting for listeners to exit...
Receiving suspended.
Waiting for outgoing deliveries to finish...
Mail delivery suspended.

mail3.example.com> offline

Enter the number of seconds to wait before abruptly closing connections.
[30]> 45

Waiting for listeners to exit...
Receiving suspended.
Waiting for outgoing deliveries to finish...
Mail delivery suspended.
```

オフライン状態からの再開

resume コマンドは、**suspenddel** コマンドまたは **suspend** コマンドを使用した後に、AsyncOS を通常の動作状態に戻します。

resume コマンド

```
mail3.example.com> resume

Receiving resumed.
Mail delivery resumed.
mail3.example.com>
```

出荷時の初期状態への設定のリセット

アプライアンスを物理的に転送するとき、または構成の問題を解決する最後の手段として、出荷時の初期状態にアプライアンスをリセットすることもできます。

注意　設定をリセットすると CLI から切り離すことになり、アプライアンス（FTP、Telnet、SSH、HTTP、HTTPS）への接続に使用しているサービスが無効になり、ユーザ アカウントが削除されます。

目的	操作内容
• 出荷時の初期状態へすべての設定をリセット • すべてのレポート カウンタをクリア ただし、 • ログ ファイルを保持 • 隔離メッセージを保持	1. デフォルトの管理ユーザ アカウントとパスワードを使用し、シリアル インターフェイスを使用して CLI に接続するかまたはデフォルト設定を使用して管理ポートに接続して、リセット後にアプライアンスに接続できることを確認します。デフォルト設定のアプライアンスへのアクセスの詳細については、第 2 章「セットアップ、インストール、および基本設定」を参照してください。 2. オフラインでアプライアンスを取得します。 3. [管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [設定ファイル（Configuration File）] を選択し、[リセット（Reset）] をクリックします。 **（注）** リセット後、アプライアンスがオフライン状態に自動的に戻ります。リセット前に電子メールの送信が中断されている場合、配信はリセット後に再試行されます。
• 出荷時の初期状態へすべての設定をリセット • すべてのデータを削除	`diagnostic > reload` CLI コマンドを使用します。 **注意**　このコマンドは、シスコのルータまたはスイッチで使用される類似のコマンドと同じではありません。

resetconfig コマンド

```
mail3.example.com> offline

Delay (seconds, minimum 30):
[30]> 45
```

```
Waiting for listeners to exit...
Receiving suspended.
Waiting for outgoing deliveries to finish...
Mail delivery suspended.

mail3.example.com> resetconfig

Are you sure you want to reset all configuration values? [N]> Y

All settings have been restored to the factory default.
```

AsyncOS のバージョン情報の表示

手順

ステップ 1　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliances）] > [集約管理サービス（Centralized Services）] > [システム ステータス（System Status）] を選択します。

ステップ 2　ページの下部までスクロールして、[バージョン情報（Version Information）] で、現在インストールされている AsyncOS のバージョンを確認します。

あるいは、コマンドライン プロンプトで **version** コマンドを使用することもできます。

リモート電源管理のイネーブル化

リモートからアプライアンス シャーシの電源をリセットする機能は、M380 および M680 ハードウェアでのみ使用できます。

リモートからアプライアンスの電源をリセットできるようにするには、ここで説明する手順を使用して、事前にこの機能をイネーブルにして設定する必要があります。

はじめる前に

- ケーブルを使用して、専用のリモート電源管理ポートをセキュアなネットワークに直接接続します。詳細については、ハードウェア インストレーション ガイドを参照してください。
- アプライアンスがリモートからアクセスできることを確認します。たとえば、ファイアウォールを通過するために必要なポートを開きます。
- この機能は、専用のリモート電源管理インターフェイスに固有の IPv4 アドレスが必要です。このインターフェイスは、ここで説明する手順でのみ設定可能です。`ipconfig` コマンドを使用して設定することはできません。
- アプライアンスの電源を一度切ってから再投入するには、Intelligent Platform Management Interface（IPMI）バージョン 2.0 をサポートするデバイスを管理できるサードパーティ製ツールが必要です。これらのツールを使用する準備ができていることを確認します。
- コマンドライン インターフェースへのアクセスに関する詳細については、CLI リファレンス ガイドを参照してください。

手順

ステップ 1　SSH、Telnet、またはシリアル コンソール ポートを使用して、コマンドライン インターフェイスにアクセスします。

ステップ 2　管理者アクセス権を持つアカウントを使用してログインします。

ステップ 3　次のコマンドを入力します。

```
remotepower
setup
```

ステップ 4　プロンプトに従って、次のことを指定します。

- この機能専用の IP アドレス、およびネットマスクとゲートウェイ。
- power-cycle コマンドを実行するために必要なユーザ名とパスワード。

  これらのクレデンシャルは、アプライアンスへのアクセスに使用する他のクレデンシャルとは関係ありません。

ステップ 5　`commit` を入力して変更を保存します。

ステップ 6　設定をテストし、リモートからアプライアンスの電源を管理できることを確認します。

ステップ 7　入力したクレデンシャルが今後無期限に利用可能であることを確認します。たとえば、この情報を安全な場所に保管し、このタスクの実行が必要になる場合がある管理者が必要なクレデンシャルにアクセスできることを確認します。

関連項目

- 「リモートからのアプライアンス電源のリセット」（P.16-6）

セキュリティ管理アプライアンスのデータのバックアップ

バックアップされるデータ

すべてのデータをバックアップすること、または次のデータの任意の組み合わせをバックアップすることを選択できます。

- メッセージ、メタデータを含むスパム隔離
- メッセージ、メタデータを含む電子メール トラッキング（メッセージ トラッキング）
- Web トラッキング
- レポーティング（電子メールおよび Web）
- セーフリスト / ブロックリスト

- メッセージおよびメタ データを含んでいる集約ポリシー、ウイルス、およびアウトブレイク隔離

データの転送が完了すると、2 つのアプライアンスのデータが同一になります。

この処理を行っても、設定とログはバックアップされません。これらのアイテムをバックアップする方法については、「その他の重要なバックアップ タスク」（P.14-14）を参照してください。

最初のバックアップ後の各バックアップは、前回のバックアップ後に生成された情報のみをコピーします。

バックアップの制約事項および要件

バックアップをスケジュール設定する前に、次の制約事項および要件を考慮してください。

制約事項	要件
AsyncOS バージョン	ソースのおよびターゲットのセキュリティ管理アプライアンスの AsyncOS バージョンが同じである必要があります。バージョンの非互換性がある場合、バックアップをスケジュールする前に、同じリリースにアプライアンスをアップグレードします。
ネットワーク上のターゲット アプライアンス	ターゲット アプライアンスがネットワーク上に設定されている必要があります。 ターゲット アプライアンスが新規の場合は、システム セットアップ ウィザードを実行して必要な情報を入力します。手順については、第 2 章「セットアップ、インストール、および基本設定」を参照してください。
アプライアンス間の通信	ソースおよびターゲット セキュリティ管理アプライアンスは、SSH を使用して通信できるようになっている必要があります。このため次のようになります。 • 両方のアプライアンスのポート 22 を開いておく必要があります。デフォルトでは、このポートはシステム セットアップ ウィザードを実行すると開きます。 • ドメイン ネーム サーバ（DNS）で、A レコードと PTR レコードの両方を使用して、両方のアプライアンスのホスト名を解決できる必要があります。

制約事項	要件
アプライアンス キャパシティ	ターゲット アプライアンスのキャパシティが、ソース アプライアンスのキャパシティと同等以上である必要があります。ターゲット アプライアンスのデータの各タイプに割り当てられているディスク領域は、ソース アプライアンスの対応する割り当て未満にできません。 **（注）** すべてのデータのバックアップに十分なスペースがターゲット上にあれば、大きいソースから小さいターゲット セキュリティ管理アプライアンスへのバックアップをスケジュール設定できます。たとえば、ソース アプライアンスが M1060 で、小さいほうの M650 がターゲットの場合、大きいほうの M1060 で割り当てられているスペースを削減して、小さいほうの M650 アプライアンスで使用可能なスペースと一致するようにしてください。ディスク領域の割り当てについては、「ディスク使用量の管理」（P.14-56）を参照してください。
複数、同時、および チェーン バックアップ	バックアップ プロセスは一度に 1 つだけ実行できます。前のバックアップが完了する前に実行がスケジュールされているバックアップはスキップされ、警告が送信されます。 セキュリティ管理アプライアンスからのデータは、1 つのセキュリティ管理アプライアンスにバックアップできます。 チェーン バックアップ（バックアップへのバックアップ）はサポートされていません。

バックアップ期間

最初の完全バックアップでは、800GB のバックアップに最大 10 時間かかります。毎日のバックアップは、それぞれ最大 3 時間かかります。毎週または毎月のバックアップはより長くかかる場合があります。これらの数は場合によって異なります。

初期バックアップ後のバックアップ プロセスでは、最後のバックアップから変更されたファイルのみが転送されます。このため、その後のバックアップにかかる時間は初期バックアップの場合よりも短くなります。後続のバックアップに必要な時間は、累積されたデータ量、変更されたファイル数、および最後のバックアップ以降どの程度のファイルが変更されたかによって異なります。

バックアップ中のサービスのアベイラビリティ

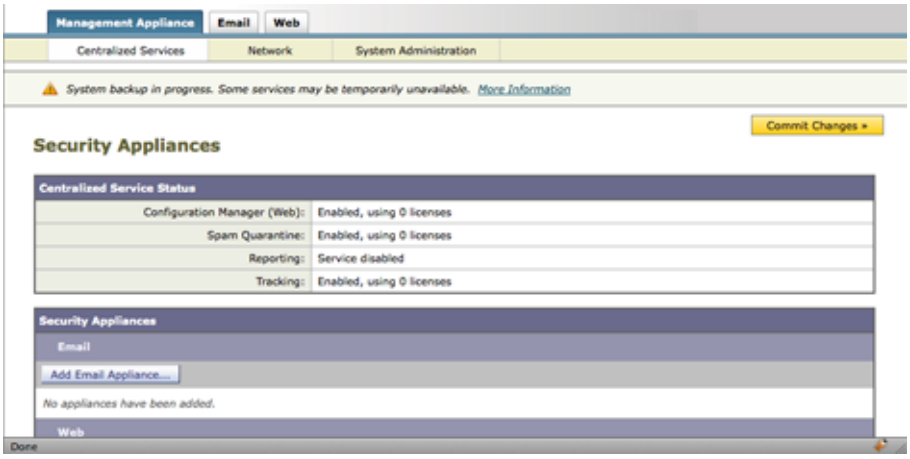
セキュリティ管理アプライアンスをバックアップすると、「ソース」セキュリティ管理アプライアンスから「ターゲット」セキュリティ管理アプライアンスにアクティブ データ セットがコピーされます。このとき、コピー元の「ソース」アプライアンスの中断は最小限に抑えられます。

バックアップ プロセスのフェーズと、それらがサービスのアベイラビリティに及ぼす影響は次のとおりです。

- フェーズ 1：バックアップ プロセスのフェーズ 1 は、ソース アプライアンスとターゲット アプライアンス間のデータの転送で開始されます。データの転送中、ソース アプライアンスでのサービスは実行されたままになるため、データ収集をそのまま継続できます。ただし、ターゲット アプライアンスではサービスがシャットダウンされます。ソースからターゲット アプライアンスへのデータの転送が完了すると、フェーズ 2 が開始されます。
- フェーズ 2：フェーズ 2 が始まると、ソース アプライアンスでサービスがシャットダウンされます。最初のシャットダウンから、ソースおよびターゲット アプライアンスの間でのデータ転送中に収集された相違点がターゲット アプライアンスにコピーされ、サービスがソースとターゲットの両方のバックアップに戻されます。これにより、ソース アプライアンス上で最大の稼働時間を維持でき、いずれかのアプライアンスのデータが損失することがなくなります。

バックアップ中に、データのアベイラビリティ レポートが機能しなくなる場合があります。また、メッセージ トラッキング結果を表示すると、各メッセージのホスト名に「未解決」というラベルが付くことがあります。

レポートをスケジュール設定しようとしているときに、バックアップが進行中であることを忘れていた場合は、[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] を選択して、システムのステータスを確認できます。このウィンドウには、システムのバックアップが進行中であるという警告が表示されます。



バックアップ プロセスの中断

（注）　バックアップの実行中にソース アプライアンスの予期しないリブートがあっても、ターゲット アプライアンスはこの停止を認識しません。ターゲット アプライアンスでバックアップをキャンセルする必要があります。

バックアップ プロセスの中断があり、そのバックアップ プロセスが完了していない場合、バックアップを次に試行したときに、セキュリティ管理アプライアンスは停止した部分からバックアップ プロセスを開始できます。

進行中のバックアップをキャンセルすることは推奨されません。これは、既存のデータが不完全になり、エラーが発生した場合は、次のバックアップが完了するまで使用できないことがあります。進行中のバックアップのキャンセルが必要な場合は、できるだけ早く完全バックアップを実行し、常に使用可能な現在のバックアップを確保してください。

単一または定期バックアップのスケジュール設定

単一または定期バックアップを事前設定した時間に行うようにスケジュール設定できます。

はじめる前に

ソース アプライアンスの設定に一致するコンフィギュレーション ファイルをターゲット アプライアンスにロードします。

（注） リモート マシンに実行中のバックアップがある場合、バックアップ プロセスは開始されません。

手順

ステップ 1 管理者として SSH セッションにログインします。

ステップ 2 コマンド プロンプトで **backupconfig** と入力し、Enter を押します。

実行する操作を選択します。

- [View]：スケジュール設定したバックアップを確認できます。
- [Verify]：バックアップをリモート マシンでスケジュール設定できるかどうかを確認します。
- [Schedule]：アプライアンスにバックアップをスケジュール設定します。
- [Cancel]：スケジュール設定されたバックアップをキャンセルします。
- [Status]：実行中のバックアップのステータスを表示します。
- [Setup]：バックアップ パラメータを設定します。

ステップ 3 ソース アプライアンスおよびターゲット アプライアンス間の接続が低速である場合は、データ圧縮をオンにします。

setup と入力して、Y を押します。

ステップ 4 **Schedule** と入力して、Enter を押します。

ステップ 5 ターゲットセキュリティ管理アプライアンスの IP アドレスを入力します。

ステップ 6 ターゲット アプライアンスを識別する有効な名前を入力します（最大 20 文字）。

ステップ 7 ターゲット アプライアンスの管理ユーザの名前およびパスワードを入力します。

ステップ 8 バックアップするデータに関するプロンプトに応答します。

これで、セキュリティ管理アプライアンスはターゲット マシンの存在を確認し、ターゲット マシンにデータを受けるのに十分なスペースがあるかどうかを判別します。

ターゲット マシンのスペースが不十分な場合は、次のエラー メッセージが表示されます。「Backup cannot be scheduled.Reason: There is not enough space for Spam Quarantine, Email Tracking, Web Tracking, Reporting.Please increase disk allocation for these services on the target machine」。データは転送されません。

ターゲット マシンが検証されると、次の選択肢が表示されます。

1. [Setup Repeating Backup Schedule]：定期バックアップをスケジュール設定できます。
2. [Schedule a single backup]：単一バックアップをスケジュール設定できます。
3. [Start a Single Backup Now]：即時バックアップを開始できます。

ステップ 9 単一バックアップをスケジュール設定する場合は、2 を入力して、Enter を押します。

ステップ 10 定期バックアップをスケジュール設定する場合は、次の手順を実行します。

a. **1** を入力して、Enter を押します。

b. 次の選択肢が表示されます。1.[Daily]、2.[Weekly]、3.[Monthly]。

c. 定期バックアップの時間枠を選択し、Enter を押します。

ステップ 11　バックアップを開始する特定の日付または日および時間を入力して、Enter を押します。

ステップ 12　バックアップ プロセスの名前を入力します。

ステップ 13　バックアップが正常にスケジュール設定されたことを確認します。コマンド プロンプトで **View** と入力して、Enter を押します。

ステップ 14　「その他の重要なバックアップ タスク」（P.14-14）も参照してください。

即時バックアップの開始

はじめる前に

ソース アプライアンスの設定に一致するコンフィギュレーション ファイルをターゲット アプライアンスにロードします。

（注）　リモート マシンに実行中のバックアップがある場合、バックアップ プロセスは開始されません。

手順

ステップ 1　管理者として SSH セッションにログインします。

ステップ 2　コマンド プロンプトで **backupconfig** と入力し、Enter を押します。

実行する操作を選択します。

- [View]：スケジュール設定したバックアップを確認できます。
- [Verify]：バックアップをリモート マシンでスケジュール設定できるかどうかを確認します。
- [スケジュール（Schedule）]：アプライアンスにバックアップをスケジュール設定できます。
- [Cancel]：スケジュール設定されたバックアップをキャンセルします。
- [Status]：実行中のバックアップのステータスを確認できます。
- [Setup]：バックアップ パラメータを設定します。

ステップ 3　ソース アプライアンスおよびターゲット アプライアンス間の接続が低速である場合は、データ圧縮をオンにします。

setup と入力して、Y を押します。

ステップ 4　**Schedule** と入力して、Enter を押します。

ステップ 5　ターゲットセキュリティ管理アプライアンスの IP アドレスを入力します。

ステップ 6　ターゲット アプライアンスを識別する有効な名前を入力します（最大 20 文字）。

ステップ 7　ターゲット アプライアンスの管理ユーザの名前およびパスワードを入力します。

ステップ 8　バックアップするデータに関するプロンプトに応答します。

これで、セキュリティ管理アプライアンスはターゲット マシンの存在を確認し、ターゲット マシンにデータを受けるのに十分なスペースがあるかどうかを判別します。

ターゲット マシンのスペースが不十分な場合は、次のエラー メッセージが表示されます。「Backup cannot be scheduled.Reason: There is not enough space for Spam Quarantine, Email Tracking, Web Tracking, Reporting.Please increase disk allocation for these services on the target machine」。データは転送されません。

ターゲット マシンが検証されると、コンソールに次の選択肢が表示されます。

1. [Setup Reoccurring Backup]：定期バックアップをスケジュール設定できます。
2. [Schedule a Single backup]：単一バックアップをスケジュール設定できます。
3. [Start a Single Backup Now]：即時バックアップを開始できます。

ステップ 9　**3** と入力して、Enter を押します。

ステップ 10　バックアップ ジョブの有効な名前を入力します。

バックアップ プロセスが数分で開始し、ソース マシンからターゲット マシンへのデータの転送が開始されます。即時バックアップが開始されると、次のメッセージが表示されます。「Backup has been initiated and will begin in a few seconds」。

ステップ 11　（任意）バックアップの進捗状況を表示するには、コマンドライン プロンプトで **Status** と入力します。

ステップ 12　「その他の重要なバックアップ タスク」（P.14-14）も参照してください。

バックアップ ステータスの確認

ログ ファイルの確認

バックアップ ログはバックアップ プロセスを開始から終了まで記録します。

バックアップ スケジューリングに関する情報は、SMA ログ内にあります。

スケジュールされたバックアップの確認

手順

ステップ 1　管理者として SSH セッションにログインします。

ステップ 2　コマンド プロンプトで **backupconfig** と入力し、Enter を押します。

ステップ 3　View 操作を選択します。

進行中のバックアップのステータスの確認

手順

ステップ 1　管理者として SSH セッションにログインします。

ステップ 2　コマンド プロンプトで **backupconfig** と入力し、Enter を押します。

ステップ 3　Status 操作を選択します。

その他の重要なバックアップ タスク

ここで説明されているバックアップ プロセスではバックアップされない項目が失われることを防止するため、およびアプライアンスの障害が発生した場合にセキュリティ管理アプライアンスの交換を速めるため、次のことを検討してください。

- プライマリ セキュリティ管理アプライアンスから設定を保存するには、「コンフィギュレーション設定の保存とインポート」（P.14-48）を参照してください。プライマリ セキュリティ管理アプライアンスとは別の安全な場所にコンフィギュレーション ファイルを保存します。
- セキュリティ管理アプライアンスから別の場所にログ ファイルを保存する方法については、「ログ サブスクリプション」（P.15-21）を参照してください。

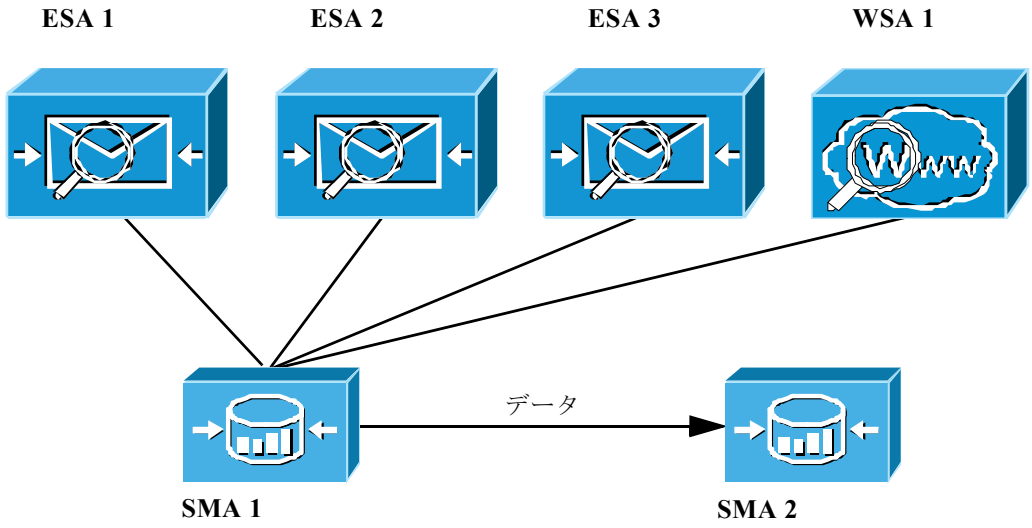
  さらに、バックアップ ログのログ サブスクリプションを設定できます。「GUI でのログ サブスクリプションの作成」（P.15-23）を参照してください。

セキュリティ管理アプライアンスでのディザスタ リカバリ

セキュリティ管理アプライアンスが予期せず失敗した場合は、次の手順を使用して、セキュリティ管理サービスおよびバックアップしたデータを復元します。これは「セキュリティ管理アプライアンスのデータのバックアップ」（P.14-7）の情報を使用して定期的に保存しています。

一般的なアプライアンス設定は図 14-1 のようになります。

図 14-1　　ディザスタ リカバリ：一般的な環境



この環境で、SMA 1 は ESA 1 ～ 3 および WSA 1 からデータを受信しているプライマリ セキュリティ管理アプライアンスです。SMA 2 は SMA1 からバックアップ データを受信しているバックアップ セキュリティ管理アプライアンスです。

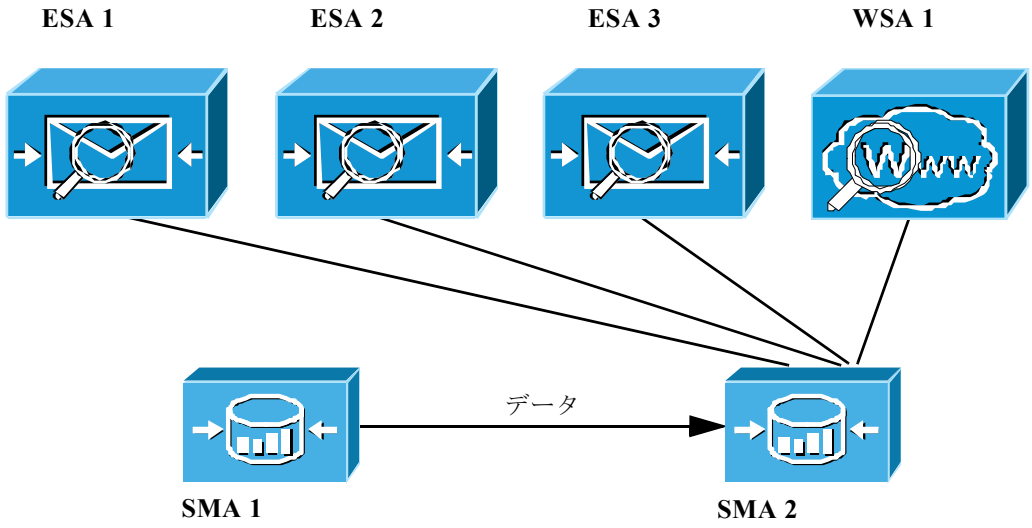
失敗した場合は、SMA 2 がプライマリ セキュリティ管理アプライアンスになるように設定する必要があります。

SMA 2 を新しいプライマリ セキュリティ管理アプライアンスとして設定し、サービスを復元するには、次の手順を実行します。

ステップ	操作内容	追加情報
ステップ 1	集約ポリシー、ウイルス、およびアウトブレイク隔離を使用している場合は以下を実行します。 各電子メール セキュリティ アプライアンスで、集約隔離を無効にします。	電子メール セキュリティ アプライアンスのマニュアルで集約ポリシー、ウイルス、およびアウトブレイク隔離を無効にする方法を参照してください。 これは、後で新しいセキュリティ管理アプライアンスに移行するそれぞれの電子メール セキュリティ アプライアンスの内部隔離を作成します。
ステップ 2	バックアップ セキュリティ管理アプライアンス（SMA2）に、プライマリ セキュリティ管理アプライアンス（SMA1）から保存したコンフィギュレーション ファイルをロードします。	「コンフィギュレーション ファイルのロード」（P.14-50）を参照してください。
ステップ 3	障害が発生した SMA 1 から IP アドレスを再作成し、SMA 2 の IP アドレスに設定します。	1. SMA 2 で、[ネットワーク（Network）] > [IP インターフェイス（IP Interfaces）] > [IP インターフェイスの追加（Add IP Interfaces）] を選択します。 2. [IP インターフェイスの追加（Add IP Interfaces）] ページで、障害が発生した SMA1 のすべての関連 IP 情報をテキスト フィールドに入力して、SMA 2 のインターフェイスを再作成します。 IP インターフェイスの追加の詳細については、「IP インターフェイスの設定」（P.A-2）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。	—
ステップ 5	新しいセキュリティ管理アプライアンス（SMA 2）で、適用可能なすべての中央集中型サービスをイネーブルにします。	「セキュリティ管理アプライアンスでのサービスの設定」（P.2-14）を参照してください。
ステップ 6	すべてのアプライアンスを新しい セキュリティ管理アプライアンス（SMA 2）に追加します。 アプライアンスへの接続を確立し、その接続をテストすることで、各アプライアンスがイネーブルとなり、機能していることをテストして確認します。	「管理対象アプライアンスの追加について」（P.2-12）を参照してください。
ステップ 7	集約ポリシー、ウイルス、およびアウトブレイク隔離を使用している場合、新しいセキュリティ管理アプライアンス上に隔離の移行を設定し、その後必要な電子メール セキュリティ アプライアンスごとに移行を有効にして設定します。	「ポリシー、ウイルス、およびアウトブレイク隔離の集約」（P.8-3）を参照してください。
ステップ 8	必要に応じて、追加データを復元します。	「その他の重要なバックアップ タスク」（P.14-14）を参照してください。

このプロセスが完了した後、SMA 2 がプライマリ セキュリティ管理アプライアンスになります。これで、図 14-2 に示すように、ESA 1 ～ 3 と WSA 1 からもすべてのデータが SMA 2 に送られるようになりました。

図 14-2　　ディザスタ リカバリ：最終結果



アプライアンス ハードウェアのアップグレード

古いセキュリティ管理アプライアンスから新しいモデルにアップグレードする場合、次の手順を実行して、古いアプライアンスから新しいアプライアンスにデータを正常に転送します。

（注） 異なるサイズの セキュリティ管理アプライアンス間でデータを転送することはできますが、新しいアプライアンスには同等以上のサイズが割り当てられている必要があります。

図 14-3　　新しいセキュリティ管理アプライアンス ハードウェアのアップグレード

はじめる前に

- 「セキュリティ管理アプライアンスのデータのバックアップ」（P.14-7）の情報を理解します。
- 「バックアップの制約事項および要件」（P.14-8）で説明されている前提条件を満たします。

- ソース アプライアンスのコンフィギュレーション ファイルのコピーを、ターゲット アプライアンスから到達できる場所に保存します。「コンフィギュレーション設定の保存とインポート」（P.14-48）を参照してください。
- コンフィギュレーション ファイルを新しいアプライアンスにインポートする前に、場合により編集する必要があります。たとえば、インターフェイス IP アドレスを変更して、そのアドレスがネットワークで一意になるようにします。また、新しいアプライアンスのインターフェイス名が、古いアプライアンスの対応するインターフェイス名に一致するようにします。

手順

ステップ 1　新しいアプライアンスでシステム セットアップ ウィザードを実行します。

ステップ 2　アプライアンスを設定するか、コンフィギュレーション ファイルをインポートします。

ステップ 3　管理者として SSH セッションにログインします。

ステップ 4　コマンド プロンプトで **backupconfig** と入力し、Enter を押します。

実行する操作を選択します。

- [View]：スケジュール設定したバックアップを確認できます。
- [Verify]：バックアップをリモート マシンでスケジュール設定できるかどうかを確認します。
- [Schedule]：アプライアンスにバックアップをスケジュール設定できます。
- [Cancel]：スケジュール設定されたバックアップをキャンセルします。
- [Status]：実行中のバックアップのステータスを確認できます。

ステップ 5　**Schedule** と入力して、Enter を押します。

ステップ 6　ターゲット セキュリティ管理アプライアンスの IP アドレスと名前を入力します。

これで、セキュリティ管理アプライアンスはターゲット マシンが存在するかどうか、およびターゲット マシンにデータを受けるのに十分なスペースがあるかどうかを確認します。

異なるサイズの セキュリティ管理アプライアンス間でデータを転送することはできますが、新しいアプライアンスには同等以上のサイズが割り当てられている可能性があります。ターゲット マシンのスペースが不十分な場合は、次のエラー メッセージが表示されます。「**Backup cannot be scheduled.Reason: There is not enough space for isq, tracking, reporting, slbl.Please increase disk allocation for these services on the target machine**」。データは転送されません。

ターゲット マシンが検証されると、コンソールに次の選択肢が表示されます。

- 1. [Setup Reoccurring Backup]：定期バックアップをスケジュール設定できます。
- 2. [Schedule a Single backup]：単一バックアップをスケジュール設定できます。
- 3. [Start a Single Backup Now]：即時バックアップを開始できます。

ステップ 7　**3** と入力して、Enter を押します。

バックアップ プロセスが開始し、ソース マシンからターゲット マシンへのデータの転送がすぐに開始されます。即時バックアップが開始されると、次のメッセージが表示されます。「`Backup has been initiated and will begin in a few seconds`」。

ステップ 8　コマンドライン プロンプトに **suspendtransfers** コマンドを入力し、ソース アプライアンスと新しいターゲット アプライアンス間のすべてのデータ転送を一時停止します。

suspendtransfers コマンドによって、古いソース セキュリティ管理アプライアンスのデータ受信が停止されます。

ステップ 9　上記のステップ 2 から 5 を繰り返して、ソース マシンで新しいインスタント バックアップを実行します。

次の作業

`resumetransfers` コマンドを使用してデータ転送を再開します。

データ転送のステータスを確認するには、[集約管理サービス（Centralized Services）] > [システム ステータス（System Status）] に移動します。

AsyncOS のアップグレード

アップグレード用のバッチ コマンド

アップグレード手順用のバッチ コマンドの詳細については、『CLI Reference Guide for AsyncOS for Email』（http://www.cisco.com/en/US/products/ps10154/prod_command_reference_list.html）を参照してください。

アップグレードとアップデートのネットワーク要件の決定

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。厳格なファイアウォール ポリシーを適用している場合は、AsyncOS のアップグレード用に静的な場所の設定が必要になることがあります。アップグレードに関して、ファイアウォール設定にスタティック IP が必要であると判断した場合は、Cisco カスタマー サポートに連絡して、必要な URL アドレスを取得してください。

（注）　既存のファイアウォール ルールで `upgrades.cisco.com` ポート（22、25、80、4766 など）からのレガシー アップグレードのダウンロードが許可されている場合は、それらを削除するか、修正したファイアウォール ルールに置き換える必要があります。

アップグレード方式：リモートまたは ストリーミング

シスコはアプライアンスでの AsyncOS のアップグレード用に、以下の 2 種類の方法（または「ソース」）を提供しています。

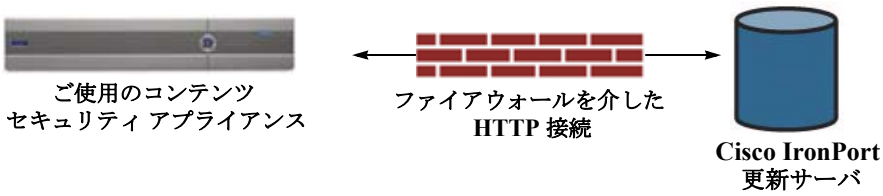
- ストリーミング アップグレード：各アプライアンスは Cisco IronPort アップグレード サーバから HTTP を介して AsyncOS アップグレードを直接ダウンロードします。
- リモート アップグレード：シスコからアップグレード イメージを 1 回だけダウンロードし、アプライアンスに保存します。次に、アプライアンスは、ネットワーク内のサーバから AsyncOS アップグレードをダウンロードします。

「アップグレードおよびサービス アップデートの設定」（P.14-22）にある、アップグレード方式を設定します。オプションで、CLI で **updateconfig** コマンドを使用します。

ストリーミング アップグレードの概要

ストリーミング アップグレードでは、次のように各シスコ コンテンツ セキュリティ アプライアンスが直接 Cisco IronPort アップデート サーバに接続して、アップグレードを検索してダウンロードします。

図 14-4　　ストリーミング アップデート方式

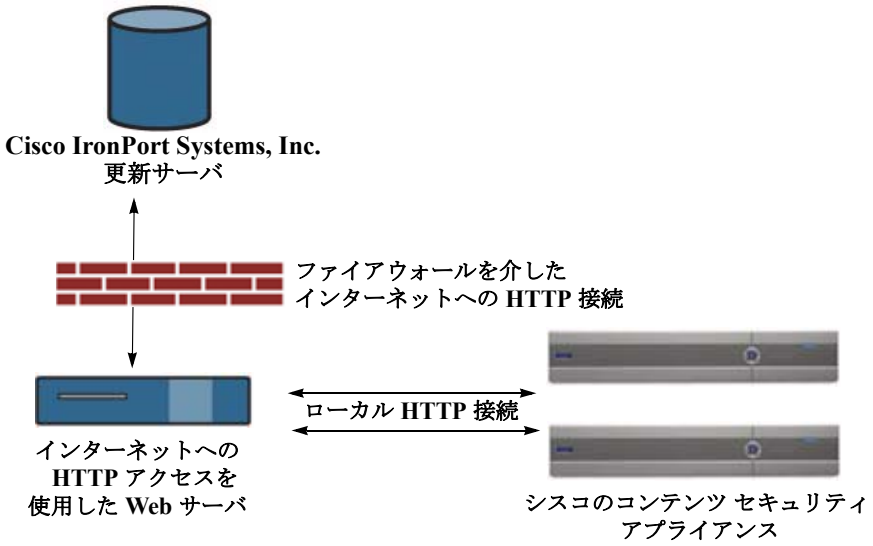


この方式では、アプライアンスが Cisco IronPort アップデート サーバにネットワークから直接接続する必要があります。

リモート アップグレードの概要

また、Cisco IronPort のアップデート サーバから直接アップデートを取得する（ストリーミング アップグレード）のではなく、ネットワーク内からローカルで AsyncOS にアップデートをダウンロードおよびホスト（リモート アップグレード）することもできます。この機能を使用して、インターネットにアクセスできるネットワーク上のすべてのサーバに HTTP で暗号化されたアップデート イメージをダウンロードします。アップデート イメージをダウンロードする場合は、内部 HTTP サーバ（アップデート マネージャ）を設定し、セキュリティ管理アプライアンスで AsyncOS イメージをホスティングすることができます。

図 14-5　リモート アップデート方式



基本的なプロセスは、次のとおりです。

手順

ステップ 1　「リモート アップグレードのハードウェア要件およびソフトウェア要件」（P.14-20）および「リモート アップグレード イメージのホスティング」（P.14-21）の情報をお読みください。

ステップ 2　アップグレード ファイルを取得して処理するように、ローカル サーバを設定します。

ステップ 3　アップグレード ファイルをダウンロードします。

ステップ 4　[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [アップデート設定（Update Settings）] を選択します。

このページで、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することを指定します。

ステップ 5　[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [システム アップグレード（System Upgrade）] を選択します。

ステップ 6　[使用可能なアップグレード（Available Upgrades）] をクリックします。

（注）　コマンドライン プロンプトから、次を行うこともできます。
updateconfig コマンドを実行してから **upgrade** コマンドを実行する。

詳細については、「AsyncOS のアップグレード」（P.14-18）を参照してください。

リモート アップグレードのハードウェア要件およびソフトウェア要件

AsyncOS アップグレード ファイルを *ダウンロード* するには、内部ネットワークに次を持つシステムが必要です。

- Cisco IronPort アップデート サーバへのインターネット アクセス。
- Web ブラウザ。

（注）　今回のリリースでアップデート サーバのアドレスへの HTTP アクセスを許可するファイアウォール設定値を設定する必要がある場合、特定の IP アドレスではなく DNS 名を使用する必要があります。

AsyncOS アップデート ファイルを*ホスティング*するには、内部ネットワークに次を持つサーバが必要です。

- Web サーバ。たとえば、次のような Microsoft IIS（Internet Information Services）または Apache オープン ソース サーバ。
  - 24 文字を超えた、ディレクトリまたはファイル名の表示をサポート
  - ディレクトリ参照に対応
  - 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 イメージに対して少なくとも 350MB の空きディスク領域がある

リモート アップグレード イメージのホスティング

ローカル サーバの設定が完了したら、**http://updates.ironport.com/fetch_manifest.html** にアクセスしてアップグレード イメージの zip ファイルをダウンロードします。イメージをダウンロードするには、シスコ コンテンツ セキュリティ アプライアンスのシリアル番号と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。アップグレード イメージの zip ファイルを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。AsyncOS アップグレードのアップグレード イメージを使用するには、ローカル サーバの基本 URL を [アップデート設定を編集（Edit Update Settings）] ページに入力します（または CLI の `updateconfig` を使用します）。

ネットワーク上のシスコ コンテンツ セキュリティ アプライアンスに使用可能なアップグレードを、`http://updates.ironport.com/fetch_manifest.html` で選択したバージョンに限定する XML ファイルを、ローカル サーバでホスティングすることもできます。シスコ コンテンツ セキュリティ アプライアンスはまだ、Cisco IronPort アップデート サーバからアップグレードをダウンロードします。アップグレード リストをローカル サーバにホスティングする場合は、zip ファイルをダウンロードして、`asyncos/phoebe-my-upgrade.xml` ファイルをローカル サーバのルート ディレクトリに展開します。AsyncOS アップグレードのアップグレード リストを使用するには、XML ファイルの完全 URL を [アップデート設定を編集（Edit Update Settings）] ページに入力します（または CLI の `updateconfig` を使用します）。

リモート アップグレードの詳細については、ナレッジ ベース（「ナレッジ ベース」（P.1-5）を参照）を確認するか、サポート プロバイダーにお問い合わせください。

リモート アップグレード方式における重要な違い

ストリーミング アップグレード方式と比較して、AsyncOS をローカル サーバからアップグレード（リモート 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。

- ダウンロード*中に*、アップグレードによるインストールがすぐに実行されます。
- アップグレード プロセスの最初の 10 秒間、バナーが表示されます。このバナーが表示されている間は、Ctrl を押した状態で C を押すと、ダウンロードの開始前にアップグレード プロセスを終了できます。

アップグレードおよびサービス アップデートの設定

シスコ コンテンツ 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（時間帯ルールなど）および AsyncOS アップグレードをダウンロードする方法を設定できます。たとえば、Cisco IronPort サーバまたはローカル サーバからイメージを利用できる場所にアップグレードおよびアップデートを動的にダウンロードするかどうか、アップデート間隔を設定するかどうか、自動アップデートをディセーブルにするかどうかを選択できます。

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。

アップグレードおよびアップデート設定は、GUI（次の 2 つの項を参照）で、または CLI で `updateconfig` コマンドを使用して設定できます。

アップグレードおよびアップデートの設定

表 14-1 に、設定可能なアップデートおよびアップグレード設定を示します。

表 14-1　セキュリティ サービスのアップデート設定

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、Cisco IronPort AsyncOS アップグレードおよびサービス アップデート ソフトウェア イメージ（時間帯ルールやライセンス キーのアップデートなど）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、アップグレードおよびアップデートの両方で Cisco IronPort アップデート サーバです。 次の場合、ローカル Web サーバを使用する場合があります。 • スタティック アドレスからアプライアンスにイメージをダウンロードする必要がある。「厳格なファイアウォール ポリシーを適用している環境のスタティック アップグレードおよびアップデート サーバ設定」（P.14-23）を参照してください。 • 適宜、アプライアンスに Cisco IronPort AsyncOS アップグレード イメージをダウンロードする。（この場合でも、Cisco Ironport アップデート サーバからサービス アップデート イメージを動的にダウンロードできます）。 ローカル アップデート サーバを選択した場合は、アップグレードとアップデートのダウンロードに使用するサーバの基本 URL とポート番号を入力します。サーバが認証を必要とする場合、有効なユーザ名とパスワードも入力します。 詳細については、「アップグレード方式：リモートまたは ストリーミング」（P.14-18）および「リモート アップグレードの概要」（P.14-19）を参照してください。

表 14-1　セキュリティ サービスのアップデート設定 （続き）

設定	説明
アップデートサーバ（リスト）（Update Servers (lists)）	利用可能なアップグレードおよびサービス アップデートのリスト（マニフェスト XML ファイル）を、Cisco IronPort アップデート サーバまたはローカル Web サーバのどちらからダウンロードするかを選択します。 デフォルトは、アップグレードおよびアップデートの両方で Cisco IronPort アップデート サーバです。アップグレードとアップデートには、それぞれ異なる設定を選択できます。 該当する場合は、「厳格なファイアウォール ポリシーを適用している環境のスタティック アップグレードおよびアップデート サーバ設定」（P.14-23）を参照してください。 ローカル アップデート サーバを選択した場合、サーバのファイル名およびポート番号を含む、各リストのマニフェスト XML ファイルのフル パスを入力します。ポートのフィールドを空のままにした場合、AsyncOS はポート 80 を使用します。サーバが認証を必要とする場合、有効なユーザ名とパスワードも入力します。 詳細については、「アップグレード方式：リモートまたは ストリーミング」（P.14-18）および「リモート アップグレードの概要」（P.14-19）を参照してください。
自動アップデート（Automatic Updates）	時間帯ルールの自動アップデートを有効にするかどうかを選択します。イネーブルにする場合は、アップデートを確認する間隔を入力します。分の場合は **m**、時間の場合は **h**、日の場合は **d** を末尾に追加します。
インターフェイス（Interface）	時間帯ルールや AsyncOS アップグレードなどをアップデート サーバに問い合わせるときに、どのネットワーク インターフェイスを使用するかを選択します。使用可能なプロキシ データ インターフェイスが表示されます。デフォルトでは、使用するインターフェイスがアプライアンスにより選択されます。
HTTP プロキシ サーバ（HTTP Proxy Server）	アップストリームの HTTP 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。 プロキシ サーバを指定すると、GUI にリストされているサービスへのアクセスおよびアップデートにそれが使用されます。
HTTPS プロキシ サーバ（HTTPS Proxy Server）	アップストリームの HTTPS 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。 プロキシ サーバを指定すると、GUI にリストされているサービスへのアクセスおよびアップデートにそれが使用されます。

厳格なファイアウォール ポリシーを適用している環境のスタティック アップグレードおよびアップデート サーバ設定

AsyncOS アップデート サーバは、ダイナミック IP アドレスを使用します。環境にスタティック IP アドレスが必要な厳格なファイアウォール ポリシーを適用している場合は、[アップデート設定（Update Settings）] ページで次の設定を使用します。

図 14-6　[アップデート サーバ（イメージ）（Update Servers (images)）] 設定のスタティック URL

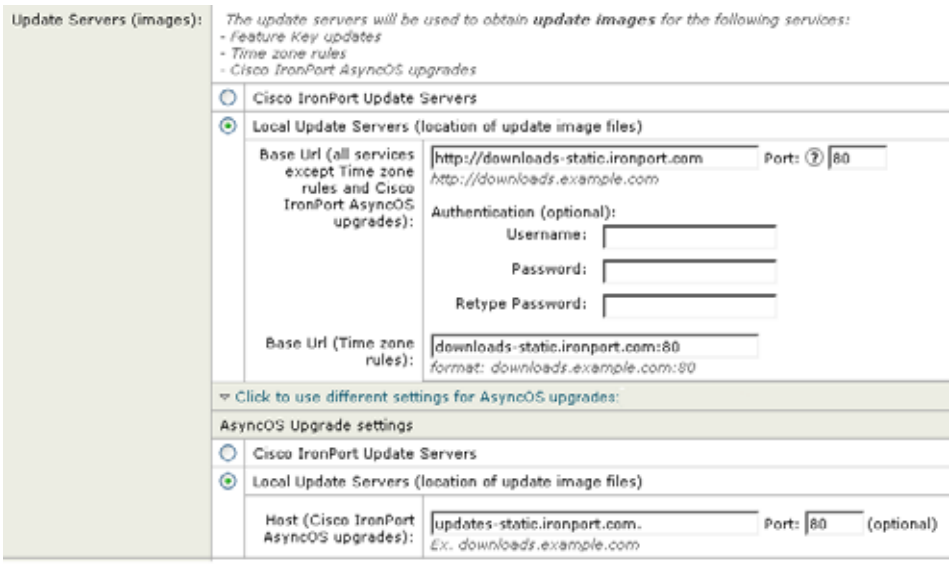


図 14-7　[アップデート サーバ（リスト）（Update Servers (list)）] 設定のスタティック URL

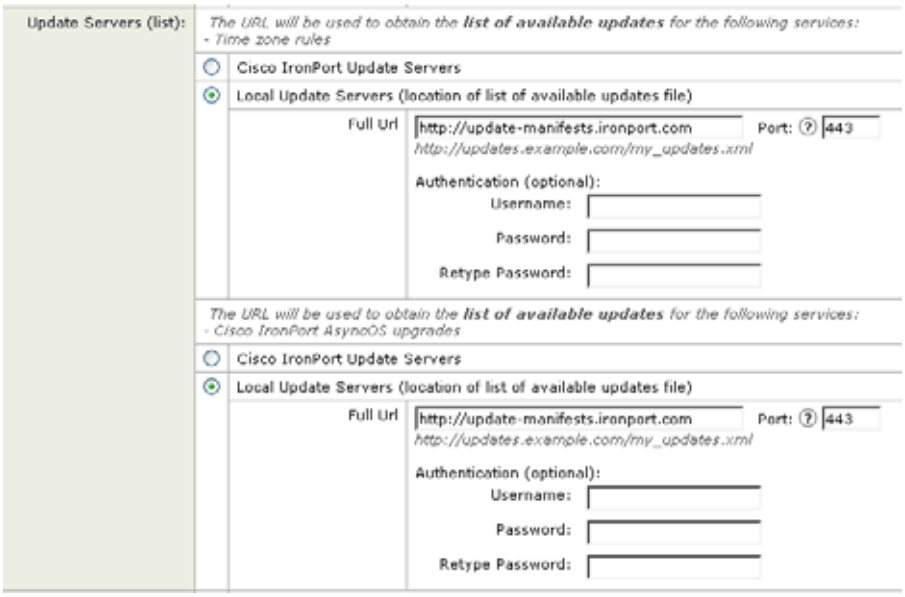


表 14-2　厳格なファイアウォール ポリシーを適用している環境のスタティック アドレス

セクション	設定	スタティック URL/IP アドレスおよびポート
アップデート サーバ（イメージ）（Update Servers (images)）	Base Url (all services except Time zone rules and Cisco IronPort AsyncOS upgrades)	http://downloads-static.ironport.com 204.15.82.8 Port 80
	Base Url (Time zone rules)	downloads-static.ironport.com 204.15.82.8 Port 80
	Host (Cisco IronPort AsyncOS upgrades)	updates-static.ironport.com 208.90.58.25 Port 80
アップデート サーバ（リスト）：（Update Servers (list):）	For updates: Full Url	update-manifests.ironport.com 208.90.58.5 Port 443
	For upgrades: Full Url	update-manifests.ironport.com 208.90.58.5 Port 443

GUI 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

手順

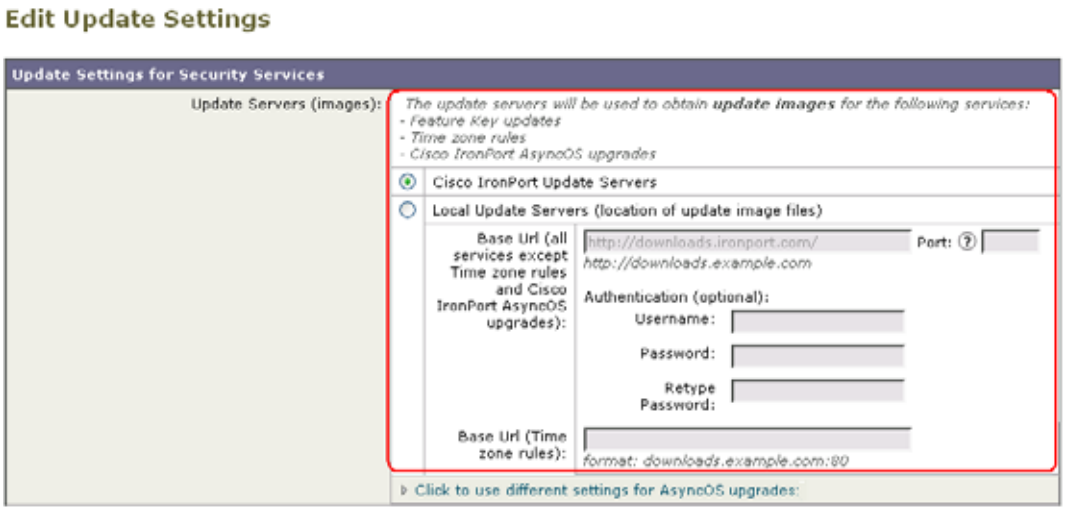
ステップ 1　[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [アップデート設定（Update Settings）] を選択します。

ステップ 2　[アップデート設定を編集（Edit Update Settings）] をクリックします。

「アップグレードおよびアップデートの設定」（P.14-22）の説明を使用して、この手順の設定を構成します。

ステップ 3　[アップデート サーバ（イメージ）（Update Servers (images)）] セクションで、アップデートのイメージのダウンロード元のサーバを指定します。

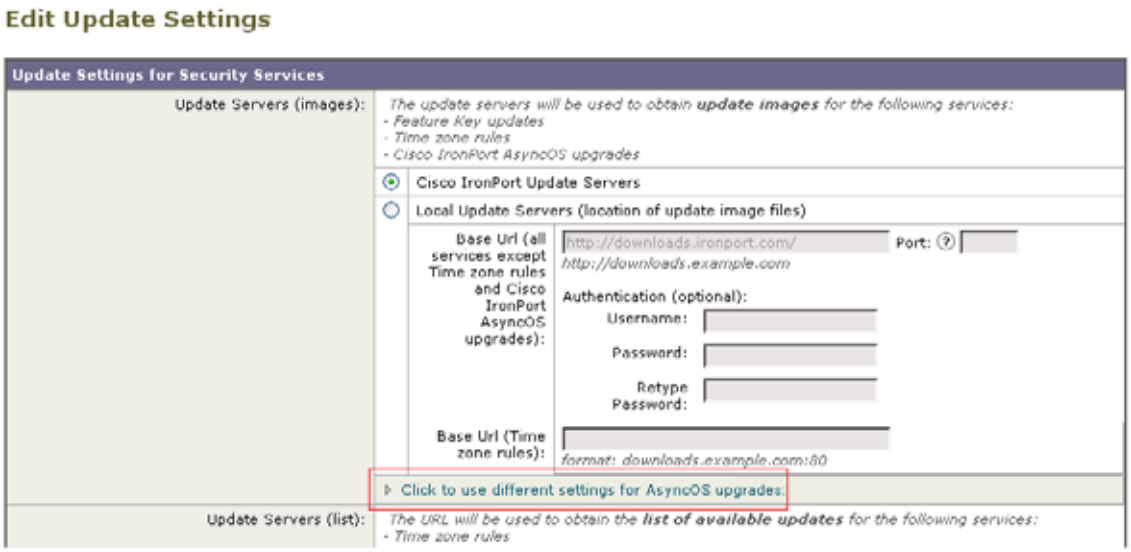
図 14-8　アップデート イメージのサーバ設定



ステップ 4　AsyncOS アップグレードのイメージをダウンロードする元のサーバを指定します。

a.　同じセクションの下部で、[クリックして AsyncOS アップグレードの異なる設定を使用する（Click to use different settings for AsyncOS upgrades）] リンクをクリックします。

図 14-9　アップグレード イメージのサーバ設定を指定するリンク



b.　AsyncOS アップグレードのイメージをダウンロードするためのサーバ設定を指定します。

ステップ 5　[アップデート サーバ（リスト）（Update Servers (list)）] セクションで、使用可能なアップデートおよび AsyncOS アップグレードのリストを取得するサーバを指定します。

上部のサブセクションはアップデートに適用されます。下部のサブセクションはアップグレードに適用されます。

ステップ 6　時間帯ルールおよびインターフェイスの設定を指定します。

ステップ 7　（任意）プロキシ サーバの設定を指定します。

ステップ 8　変更を送信し、保存します。

ステップ 9　結果が予定通りか確認します。

[アップデート設定（Update Settings）] ページが表示されていない場合は、[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [アップデート設定（Update Settings）] を選択します。

一部の URL では、サーバ URL に「asyncos」ディレクトリが追加されます。この不一致は無視してかまいません。

アップグレードする前に：重要な手順

はじめる前に

「アップグレードとアップデートのネットワーク要件の決定」（P.14-18）でネットワーク要件を参照してください。

手順

ステップ 1　次のようにして、データの消失を防止する、または最小限に抑えます。

- 新しいアプライアンスに十分なディスク容量があり、転送される各データ タイプに同等以上のサイズが割り当てられていることを確認します。「最大ディスク領域と割り当て」（P.14-56）を参照してください。
- ディスク領域についての何らかの警告を受け取った場合は、アップグレードを開始する前に、ディスク領域に関する問題をすべて解決してください。

ステップ 2　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。「現在のコンフィギュレーション ファイルの保存およびエクスポート」（P.14-50）で説明する警告を参照してください。

ステップ 3　セーフリスト/ブロックリスト機能を使用している場合は、リストをボックスからエクスポートします。

[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [設定ファイル（Configuration File）] をクリックしてスクロール ダウンします。詳細については、お使いのリリースのマニュアルを参照してください。

ステップ 4　CLI からアップグレードを実行している場合は、**suspendlistener** コマンドを使用してリスナーを停止します。GUI からアップグレードを実行した場合は、自動的にリスナーの一時停止が発生します。

ステップ 5　メール キューとデリバリ キューを解放します。

ステップ 6　アップグレード設定が希望どおりに設定されていることを確認します。「アップグレードおよびサービス アップデートの設定」（P.14-22）を参照してください。

AsyncOS のアップグレード

ダウンロードとインストールを単一の操作でできます。またはバックグラウンドでダウンロードしあとでインストールすることもできます。

（注）　Cisco IronPort サーバからの代わりにローカル サーバから単一の操作で AsyncOS をダウンロードしてアップグレードする場合、アップグレードは*ダウンロード中*にすぐにインストールされます。アップグレード プロセスの開始時に、バナーが 10 秒間表示されます。このバナーが表示されている間は、Ctrl を押した状態で C を押すと、ダウンロードの開始前にアップグレード プロセスを終了できます。

はじめる前に

- アップグレードをシスコから直接ダウンロードするのか、またはお使いのネットワーク上のサーバのアップグレード イメージをホストにするのかを選択します。その後、選択した方式をサポートするようにネットワークを設定します。次に、選択したソースからアップグレードを取得するようにアプライアンスを設定します。「アップグレード方式：リモートまたは ストリーミング」（P.14-18）および「アップグレードおよびサービス アップデートの設定」（P.14-22）を参照してください。
- アップグレードをすぐにインストールする場合でも、「アップグレードする前に：重要な手順」（P.14-27）の手順に従ってください。

手順

ステップ 1　[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [システム アップグレード（System Upgrade）] を選択します。

ステップ 2　[アップグレード（Upgrade）] オプションをクリックします。

ステップ 3　次のオプションを選択します。

目的	操作内容
単一の操作でアップグレードをダウンロードしてインストール	[ダウンロードとインストール（Download and Install）] をクリックします。 すでにインストーラをダウンロードしている場合、既存のダウンロードを上書きするように促されます。
アップグレード インストーラをダウンロード	[ダウンロードのみ（Download only）] をクリックします。 すでにインストーラをダウンロードしている場合、既存のダウンロードを上書きするように促されます。 インストーラはサービス中断のないバックグラウンドでダウンロードを行います。
ダウンロードしたアップグレード インストーラをインストールします。	[インストール（Install）] をクリックします。 このオプションは、インストーラがダウンロードされた場合にだけ表示されます。 インストールする AsyncOS バージョンは [インストール（Install）] オプションの下に表示されます。

ステップ 4　以前にダウンロードされたインストーラをインストールしていないのであれば、利用可能なアップグレードのリストから AsyncOS バージョンを選択します。

ステップ 5　インストールしている場合：

a.　現在の設定をアプライアンスの `configuration` ディレクトリに保存するかどうかを選択します。

b.　設定ファイルのパスワードをマスクするかどうかを選択します。

（注）　マスクされたパスワードが記載された設定ファイルは、GUI の [設定（Configuration File）] ページや CLI の `loadconfig` コマンドからロードできません。

c. 設定ファイルのコピーを電子メールで送信する場合は、ファイルを電子メールで送信する電子メール アドレスを入力します。複数の電子メール アドレスを指定する場合は、カンマで区切ります。

ステップ 6　[続行（Proceed）] をクリックします。

ステップ 7　インストールしている場合：

a. 処理中はプロンプトに答えられるようにしていてください。

応答まで処理が中断します。

ページの上部に経過表示バーが表示されます。

b. プロンプトで、[今すぐ再起動（Reboot Now）] をクリックしてください。

（注）　リブートしてから少なくとも 20 分経過するまで、いかなる理由があっても（アップグレードの問題をトラブルシューティングするためであっても）アプライアンスの電源を中断しないでください。

c. 約 10 分後、アプライアンスにアクセスし、ログインします。

次の作業

- プロセスが中断された場合、プロセスを再開します。
- アップグレードをダウンロードし、インストールしていない場合は、次の指示に従います。

  アップグレードをインストールする準備ができたら、「はじめる前に」の項の前提条件を含めて最初からこれらの手順に従います。しかしインストールのオプションも選択します。
- アップグレードをインストールしている場合は、「アップグレード後」（P.14-30）を参照してください。
- アップグレード後オンライン ヘルプを表示するには、ブラウザ キャッシュをクリアし、ブラウザを終了してもう一度開きます。これにより、期限切れのコンテンツのブラウザ キャッシュがクリアされます。

バックグラウンド ダウンロードのステータスの表示、キャンセル、または削除

手順

ステップ 1　[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [システム アップグレード（System Upgrade）] を選択します。

ステップ 2　[アップグレード（Upgrade）] オプションをクリックします。

ステップ 3　次のオプションを選択します。

目的	操作内容
ダウンロードの状態を表示	ページの中央に見てください。 進行中のダウンロードおよびインストール待ちのダウンロードが完了してないダウンロードがない場合、ダウンロード ステータス情報が表示されません。 アップグレードのステータスは upgrade_logs でも見ることができます。
ダウンロードをキャンセル	ページの中央にある [ダウンロードをキャンセル（Cancel Download）] ボタンをクリックします。 このオプションは、ダウンロードが実行中の場合のみ表示されます。
ダウンロードされたインストーラを削除	ページの中央にある [ファイルを削除（CDelete File）] ボタンをクリックします。 このオプションは、インストーラがダウンロードされた場合にだけ表示されます。

アップグレード後

アップグレードが完了したら、次の手順を実行します。

- （関連する電子メール セキュリティ アプライアンスのある導入環境の場合）リスナーを再度イネーブルにします。
- （Web セキュリティ アプライアンス関連の導入の場合）最新の設定マスターをサポートするようにシステムを設定します。「Configuration Master の設定の概要」（P.9-2）を参照してください。
- 設定を保存するかどうか判断します。詳細については、「コンフィギュレーション設定の保存とインポート」（P.14-48）を参照してください。

AsyncOS の以前のバージョンへの復元について

緊急時には、前の認定バージョンの AsyncOS に戻すことができます。

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始める場合は、現在実行中のビルドに戻すこともできます。

復元による影響に関する重要な注意事項

シスコ コンテンツ セキュリティ アプライアンスにおける `revert` コマンドの使用は、非常に破壊的な操作になります。このコマンドはすべての設定ログおよび既存データを永久破壊します。さらに、復元ではアプライアンスが再設定されるまでメール処理が中断されます。このコマンドはすべての設定を破壊するため、`revert` コマンドを発行する場合は、シスコ コンテンツ セキュリティ アプライアンスへの物理的なローカル アクセスを必ず用意するようにしてください。

警告　**戻し先のバージョンのコンフィギュレーション ファイルが必要です。コンフィギュレーション ファイルには、後方互換性が*ありません*。**

AsyncOS の復元

はじめる前に

お使いの電子メール セキュリティ アプライアンスで集約ポリシー、ウイルス、およびアウトブレイク隔離が有効になっている場合、それらのアプライアンス内部でメッセージが隔離されるように集約化を無効にします。

手順

ステップ 1　戻し先のバージョンのコンフィギュレーション ファイルがあることを確認してください。コンフィギュレーション ファイルには、後方互換性がありません。

ステップ 2　アプライアンスの現在の設定のバックアップ コピーを、（パスワードをマスクしない状態で）別のマシンに保存します。それには、電子メールで自分に送信したり、ファイルを FTP で転送します。簡単に行うには、`mailconfig` CLI コマンドを実行すると、アプライアンスの現在のコンフィギュレーション ファイルが指定したメール アドレスに送信されます。

（注）　復元後にロードするのは、この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 3　セーフリスト/ブロックリスト機能を使用する場合は、セーフリスト/ブロックリスト データベースを別のマシンにエクスポートします。

ステップ 4　電子メール セキュリティ アプライアンスで、すべてのリスナーを一時停止します。

ステップ 5　メール キューが空になるまで待ちます。

ステップ 6　バージョンを戻すアプライアンスの CLI にログインします。

`revert` コマンドを実行すると、いくつかの警告プロンプトが出されます。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、復元前の手順を完了するまで、復元プロセスを開始しないでください。

ステップ 7　コマンドライン プロンプトから **revert** コマンドを入力し、プロンプトに応答します。

次に、**revert** コマンドの例を示します。

```
m650p03.prep> revert

This command will revert the appliance to a previous version of AsyncOS.

WARNING: Reverting the appliance is extremely destructive.
The following data will be destroyed in the process:
- all configuration settings (including listeners)
- all log files
- all databases (including messages in Virus Outbreak and Policy
quarantines)
- all reporting data (including saved scheduled reports)
- all message tracking data
- all Cisco IronPort Spam Quarantine message and end-user safelist/blocklist data

Only the network settings will be preseved.
```

```
Before running this command, be sure you have:
- saved the configuration file of this appliance (with passwords
unmasked)
- exported the Cisco IronPort Spam Quarantine safelist/blocklist database
   to another machine (if applicable)
- waited for the mail queue to empty

Reverting the device causes an immediate reboot to take place.
After rebooting, the appliance reinitializes itself and reboots again to the desired
version.

Do you want to continue? yes

Are you sure you want to continue? yes

Available versions
==================
 1. 7.2.0-390
 2. 6.7.6-020

Please select an AsyncOS version: 1

You have selected "7.2.0-390".

Reverting to "testing" preconfigure install mode.

The system will now reboot to perform the revert operation.
```

ステップ 8　アプライアンスが 2 回リブートするまで待ちます。

ステップ 9　CLI を使用してアプライアンスにログインします。

ステップ 10　アプライアンスが AsyncOS 7.5 以降を実行する Web セキュリティ アプライアンスを管理する場合は、これらのアプライアンスの少なくとも 1 つを追加してから数分待機して、URL カテゴリ アップデートが Web セキュリティ アプライアンスからダウンロードされるようにします。

ステップ 11　URL カテゴリのアップデートが完了したら、戻し先のバージョンのコンフィギュレーション ファイルをロードします。

ステップ 12　セーフリスト/ブロックリスト機能を使用する場合は、セーフリスト/ブロックリスト データベースをインポートして復元します。

ステップ 13　電子メール セキュリティ アプライアンスで、すべてのリスナーを再びイネーブルにします。

ステップ 14　変更を保存します。

復元が完了したシスコ コンテンツ セキュリティ アプライアンスは、選択された AsyncOS バージョンを使用して稼働します。

（注）　復元が完了して、シスコ コンテンツ セキュリティ 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。

アップデートについて

サービス アップデートは定期的にダウンロード可能にできます。これらのダウンロードの設定を指定するには、「アップグレードおよびサービス アップデートの設定」（P.14-22）を参照してください。

Cisco IronPort Web 使用率制御の URL カテゴリ セット アップデートについて

- 「URL カテゴリ セットの更新と中央集中型コンフィギュレーション管理」（P.9-24）
- 「URL カテゴリ セットの更新とレポート」（P.5-28）

生成されたメッセージの返信アドレスの設定

次の場合に対して、AsyncOS で生成されたメールのエンベロープ送信者を設定できます。

- バウンス メッセージ
- レポート

返信アドレスの表示、ユーザ、およびドメイン名を指定できます。ドメイン名に仮想ゲートウェイ ドメインの使用を選択することもできます。

GUI の [システム管理（System Administration）] メニューから利用できる [返信先アドレス（Return Addresses）] ページを使用するか、CLI で **addressconfig** コマンドを使用します。

システムで生成された電子メール メッセージの返信アドレスを GUI で変更するには、[返信先アドレス（Return Addresses）] ページで [設定を編集（Edit Settings）] をクリックします。1 つまたは複数のアドレスを変更して [送信（Submit）] をクリックし、変更を確定します。

アラートの管理

アラートとは、アプライアンスで発生しているイベントに関する情報が記載されている、電子メールによる通知のことです。これらのイベントにはマイナーからメジャーまでの重要度（または重大度）レベルがあり、一般的にアプライアンスの特定のコンポーネントまたは機能に関連しています。アラートは、アプライアンスで生成されます。どのアラート メッセージがどのユーザに送信され、イベントの重大度がどの程度である場合にアラートが送信されるかは、非常にきめ細かなレベルで指定できます。アラートの管理は、GUI の [管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [アラート（Alerts）] ページで行います（または、CLI で `alertconfig` コマンドを使用します）。

アラートの概要

次の機能によって、電子メール通知の動作が制御されます。

- **アラート**：電子メール通知を受け取るアラートを作成します。アラートは、アラートの受信者（受信アラートの電子メール アドレス）と、アラート通知（重大度とアラート タイプを含む）で構成されています。
- **アラート設定**：アラート機能の全般的な動作を指定します。たとえば、アラートの送信者（差出人：（FROM:））のアドレス、重複アラートを送信する秒間隔、および [オートサポート（AutoSupport）] を有効にするかどうか（および、オプションで週次でオートレポートを送信するかどうか）などを指定します。

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、ハードウェア問題などの特定の機能についての情報が含まれている電子メール メッセージまたは通知であり、アラートの受信者に送信されます。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、アラートの分類と重大度によって決まります。どのアラート分類を、どの重大度で、特定のアラート受信者に送信するかを指定できます。アラート エンジンを使用して、受信者に送信されるアラートを詳細に制御できます。たとえば、重大度レベルが Critical であり、アラート タイプが System の場合など、特定のタイプのアラートのみが受信者に送信されるようにシステムを設定できます。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.14-37）を参照してください）。すべてのアラートのリストについては、「アラート リスト」（P.14-38）を参照してください。

アラートの分類

AsyncOS では、次のアラート分類を送信します。

- システム
- ハードウェア

重大度

アラートは、次の重大度に従って送信されます。

- Critical：すぐに対処が必要な問題
- 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
- Info：この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 レベルのシステム 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 の週次ステータス 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、待機時間が 5 秒間の場合、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、送信間隔は非常に長くなります。[重複アラート送信時の最大待ち時間（秒）（Maximum Number of Seconds to Wait Before Sending a Duplicate Alert）] 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。

アラートの配信

アラート メッセージはシスコ コンテンツ セキュリティ アプライアンス内の問題の通知に使用されるため、送信に AsyncOS の標準メール配信システムを使用しません。代わりに、アラート メッセージは AsyncOS で重大なシステム故障が発生しても動作するように設計された、個別に並行動作する電子メール システムで処理されます。

アラート メール システムは、AsyncOS と同一の設定を共有しません。このため、アラート メッセージは、次のように他のメール配信とは若干異なる動作をする可能性があります。

- アラート メッセージは、標準の DNS MX レコードおよび A レコードのルックアップを使用して配信されます。
  - 5.X よりも前の AsyncOS バージョンでは、アラート メッセージに SMTP ルートが使用されません。
  - アラート メッセージは DNS エントリを 30 分間キャッシュし、そのキャッシュは 30 分ごとにリフレッシュされます。このため、DNS 障害時にもアラートが出力されます。
- アラート メッセージはワーク キューを通過しないため、ウイルスまたはスパムのスキャン対象外です。メッセージ フィルタまたはコンテンツ フィルタの処理対象にも含まれません。
- アラート メッセージは配信キューを通過しないため、バウンスのプロファイルまたは送信先制御の制限には影響を受けません。

最新アラートの表示

目的	操作内容
最近のアラートのリストを表示	管理者およびオペレータのアクセス権のあるユーザは、[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [アラート（Alerts）] を選択し、[上位アラートを表示（View Top Alerts）] ボタンをクリックします。 アラートは、電子メールで通知する問題があっても表示されます。
リストをソート	列の見出しをクリックします。
このリストに保存するアラートの最大数を指定	コマンドライン インターフェイス（CLI）で `alertconfig` コマンドを使用します。
この機能を無効にする	コマンドライン インターフェイス（CLI）で `alertconfig` コマンドを使用してアラートの最大数をゼロ（0）に設定します。

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

Header From: アドレスは、GUI で [設定を編集（Edit Settings）] ボタンをクリックするか、CLI（『*Cisco IronPort AsyncOS CLI Reference Guide*』を参照）を使用して設定できます。

アラートの件名

アラート メッセージの件名は、次の形式になります。

```
Subject: [severity]-[hostname]: ([class]) short message
```

アラート メッセージの例

```
Date: 23 Mar 2007 21:10:19 +0000
To: joe@example.com
From: Cisco IronPort M670 Alert [alert@example.com]
Subject: Critical-example.com: (AntiVirus) update via http://newproxy.example.com failed

The Critical message is:

update via http://newproxy.example.com failed

Version: 6.0.0-419
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 need further information, contact your support provider.
```

アラート受信者の管理

（注） システムのセットアップ時に AutoSupport をイネーブルにした場合、指定した電子メール アドレスはデフォルトで、すべての重大度およびクラスのアラートを受信します。この設定はいつでも変更できます。

手順

ステップ 1　[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [アラート（Alerts）] を選択します。

ステップ 2　[受信者を追加 ...（Add Recipient）] をクリックします。

ステップ 3　受信者の電子メール アドレスを入力します。複数のアドレスをカンマで区切って入力することもできます。

ステップ 4　アラート受信者が受信するアラート重大度を選択します。

ステップ 5　[送信（Submit）] をクリックして、アラート受信者を追加します。

ステップ 6　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、セキュリティ管理アプライアンスが送信するすべてのアラートに適用されます。

手順

ステップ 1　[アラート（Alerts）] ページで [設定を編集（Edit Settings）] をクリックします。

ステップ 2　アラートの送信に使用する Header From: アドレスを入力するか、[自動生成（Automatically generated）]（「alert@<hostname>」）を選択します。

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.14-34）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　必要に応じて、[Cisco IronPort AutoSupport] オプションを選択して、AutoSupport をイネーブルにします。AutoSupport の詳細については、「Cisco IronPort オートサポート」（P.14-37）を参照してください。

AutoSupport がイネーブルの場合、Information レベルのシステム 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、週次 AutoSupport レポートが送信されます。チェックボックスを使用して、これを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。

次の作業

[上位アラート（Top Alerts）] リストに表示するアラートの最大数を設定、または [上位アラート（Top Alerts）] 機能を無効にするには、「最新アラートの表示」（P.14-35）を参照してください。

Cisco IronPort オートサポート

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シスコ コンテンツ セキュリティ アプライアンスを設定できます。「オートサポート」と呼ばれるこの機能は、カスタマー サポート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、オートサポート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、この設定を無効にできます。この機能を有効または無効にするには、「アラート設定値の設定」（P.14-37）を参照してください。

アラート リスト

次の表に、アラート名、説明、および重大度など、アラートを分類別に示します。

ハードウェア アラート

表 14-3 には、アラートの説明やアラートの重大度など、AsyncOS によって生成される可能性のあるさまざまなハードウェア アラートを示してあります。

表 14-3　ハードウェア アラートのリスト

アラート名	説明	重大度
INTERFACE.ERRORS	インターフェイス エラーを検出した場合に送信されます。	Warning
MAIL.MEASUREMENTS_ FILESYSTEM	ディスク パーティションが 75 % の使用率に近づいた場合に送信されます。	Warning
MAIL.MEASUREMENTS_ FILESYSTEM.CRITICAL	ディスク パーティションが 90 % の使用率に達した場合（95 %、96 %、97 % など）に送信されます。	Critical
SYSTEM.RAID_EVENT_ ALERT	重大な RAID-event が発生した場合に送信されます。	Warning
SYSTEM.RAID_EVENT_ ALERT_INFO	RAID-event が発生した場合に送信されます。	Information

システム アラート

表 14-4 には、アラートの説明やアラートの重大度など、AsyncOS によって生成される可能性のあるさまざまなシステム アラートを示してあります。

表 14-4　システム アラートのリスト

アラート名	説明	重大度
COMMON.APP_FAILURE	不明なアプリケーション障害が発生した場合に送信されます。	Critical
COMMON.KEY_EXPIRED_AL ERT	ライセンス キーの有効期限が切れた場合に送信されます。	Warning
COMMON.KEY_EXPIRING_A LERT	ライセンス キーの有効期限が切れる場合に送信されます。	Warning
COMMON.KEY_FINAL_ EXPIRING_ALERT	ライセンス キーの有効期限が切れる場合の最後の通知として送信されます。	Warning
DNS.BOOTSTRAP_FAILED	アプライアンスがルート DNS サーバに問い合わせることができない場合に送信されます。	Warning
INTERFACE. FAILOVER.FAILURE_ BACKUP_DETECTED	バックアップ NIC ペアリング インターフェイスが故障した場合に送信されます。	Warning
INTERFACE. FAILOVER.FAILURE_ BACKUP_RECOVERED	NIC ペアのフェールオーバーが復旧した場合に送信されます。	Information
INTERFACE.FAILOVER. FAILURE_DETECTED	インターフェイス故障により、NIC ペアリング フェールオーバーが検出された場合に送信されます。	Critical

表 14-4　システム アラートのリスト （続き）

アラート名	説明	重大度
INTERFACE.FAILOVER. FAILURE_DETECTED_NO_ BACKUP	インターフェイス故障により NIC ペアリング フェールオーバーは検出されたけれども、バック アップ インターフェイスが利用できない場合に送信されます。	Critical
INTERFACE.FAILOVER. FAILURE_RECOVERED	NIC ペアのフェールオーバーが復旧した場合に送信されます。	Information
INTERFACE.FAILOVER. MANUAL	別の NIC ペアへの手動フェールオーバーが検出された場合に送信されます。	Information
COMMON.INVALID_FILTER	無効なフィルタが存在する場合に送信されます。	Warning
LDAP.GROUP_QUERY_ FAILED_ALERT	LDAP グループ クエリーに失敗した場合に送信されます。	Critical
LDAP.HARD_ERROR	LDAP クエリーが（すべてのサーバで試行した後）完全に失敗した場合に送信されます。	Critical
LOG.ERROR.*	さまざまなロギング エラー。	Critical
MAIL.PERRCPT.LDAP_ GROUP_QUERY_FAILED	各受信者のスキャン時に LDAP グループ クエリーに失敗した場合に送信されます。	Critical
MAIL.QUEUE.ERROR.*	メール キューのさまざまなハード エラー。	Critical
MAIL.RES_CON_START_ ALERT.MEMORY	メモリ使用率がシステム リソース節約しきい値を超過した場合に送信されます。	Critical
MAIL.RES_CON_START_ ALERT.QUEUE_SLOW	メール キューが過負荷となり、システム リソース節約がイネーブルになった場合に送信されます。	Critical
MAIL.RES_CON_START_ ALERT.QUEUE	キュー使用率がシステム リソース節約しきい値を超過した場合に送信されます。	Critical
MAIL.RES_CON_START_ ALERT.WORKQ	ワーク キューのサイズが大きすぎるため、リスナーが一時停止された場合に送信されます。	Critical
MAIL.RES_CON_START_ ALERT	アプライアンスが「リソース節約」モードに入った場合に送信されます。	Critical
MAIL.RES_CON_STOP_ ALERT	アプライアンスの「リソース節約」モードが解除された場合に送信されます。	Critical
MAIL.WORK_QUEUE_ PAUSED_NATURAL	ワーク キューが中断された場合に送信されます。	Critical
MAIL.WORK_QUEUE_ UNPAUSED_NATURAL	ワーク キューが再開された場合に送信されます。	Critical
NTP.NOT_ROOT	root として NTP が実行されていないためにアプライアンスが時刻を調整できない場合に送信されます。	Warning
PERIODIC_REPORTS. DOMAIN_REPORT. DOMAIN_FILE_ERRORS	ドメイン指定ファイルでエラーが検出された場合に送信されます。	Critical
PERIODIC_REPORTS. DOMAIN_REPORT.FILE_ EMPTY	ドメイン指定ファイルが空の場合に送信されます。	Critical

表 14-4　システム アラートのリスト （続き）

アラート名	説明	重大度
PERIODIC_REPORTS. DOMAIN_REPORT.FILE_ MISSING	ドメイン指定ファイルが見つからない場合に送信されます。	Critical
REPORTD.DATABASE_ OPEN_FAILED_ALERT	レポート エンジンがデータベースを開けない場合に送信されます。	Critical
REPORTD.AGGREGATION_DI SABLED_ALERT	システムのディスク領域が不足している場合に送信されます。ログ エントリに関するディスク使用率がログ使用率のしきい値を超過すると、reportd は集約をディセーブルにし、アラートを送信します。	Warning
REPORTING.CLIENT. UPDATE_FAILED_ALERT	レポート エンジンがレポート データを保存できなかった場合に送信されます。	Warning
REPORTING.CLIENT. JOURNAL.FULL	レポート エンジンが新規データを保存できない場合に送信されます。	Critical
REPORTING.CLIENT. JOURNAL.FREE	レポート エンジンが再び新規データを保存できるようになった場合に送信されます。	Information
PERIODIC_REPORTS. REPORT_TASK.BUILD_ FAILURE_ALERT	レポート エンジンがレポートを作成できない場合に送信されます。	Critical
PERIODIC_REPORTS. REPORT_TASK.EMAIL_ FAILURE_ALERT	レポートを電子メールで送信できなかった場合に送信されます。	Critical
PERIODIC_REPORTS. REPORT_TASK.ARCHIVE_FA ILURE_ALERT	レポートをアーカイブできなかった場合に送信されます。	Critical
SENDERBASE.ERROR	SenderBase からの応答を処理中にエラーが発生した場合に送信されます。	Information
SMAD.ICCM.ALERT_PUSH_F AILED	1 台以上のホストでコンフィギュレーションのプッシュに失敗した場合に送信されます。	Warning
SMAD.TRANSFER. TRANSFERS_STALLED	SMA ログがトラッキング データを 2 時間取得できなかった場合、またはレポーティング データを 6 時間取得できなかった場合に送信されます。	Warning
SMTPAUTH.FWD_SERVER_F AILED_ALERT	SMTP 認証転送サーバが到達不能である場合に送信されます。	Warning
SMTPAUTH.LDAP_QUERY_F AILED	LDAP クエリーが失敗した場合に送信されます。	Warning
SYSTEM.HERMES_ SHUTDOWN_FAILURE. REBOOT	リブート中のシステムをシャットダウンしている際に問題が発生した場合に送信されます。	Warning
SYSTEM.HERMES_ SHUTDOWN_FAILURE. SHUTDOWN	システムをシャットダウンしている際に問題が発生した場合に送信されます。	Warning
SYSTEM. RCPTVALIDATION.UPDATE_F AILED	受信者検証のアップデートに失敗した場合に送信されます。	Critical

表 14-4　システム アラートのリスト （続き）

アラート名	説明	重大度
SYSTEM.SERVICE_ TUNNEL.DISABLED	Cisco IronPort サポート サービス用に作成されたトンネルがディセーブルの場合に送信されます。	Information
SYSTEM.SERVICE_ TUNNEL.ENABLED	Cisco IronPort サポート サービス用に作成されたトンネルがイネーブルの場合に送信されます。	Information

ネットワーク設定値の変更

このセクションでは、アプライアンスのネットワーク操作の設定に使用する機能について説明します。これらの機能では、「システム セットアップ ウィザードの実行」（P.2-8）でシステム セットアップ ウィザードを利用して設定したホスト名、DNS、およびルーティングの設定値に直接アクセスできます。

ここでは、次の機能について説明します。

- sethostname
- DNS 設定（GUI で設定。および CLI で dnsconfig コマンドを使用して設定）
- ルーティング設定（GUI で設定。および CLI で routeconfig コマンドと setgateway コマンドを使用して設定）
- dnsflush
- パスワード

システム ホスト名の変更

ホスト名は、CLI プロンプトでシステムを識別する際に使用されます。完全修飾ホスト名を入力する必要があります。sethostname コマンドは、コンテンツ セキュリティ アプライアンスの名前を設定します。新規ホスト名は、commit コマンドを発行して初めて有効になります。

sethostname コマンド

```
oldname.example.com> sethostname

[oldname.example.com]> mail3.example.com

oldname.example.com>
```

ホスト名の変更を有効にするには、commit コマンドを入力する必要があります。ホスト名の変更を確定すると、CLI プロンプトに新しいホスト名が表示されます。

```
oldname.example.com> commit

Please enter some comments describing your changes:
[]> Changed System Hostname
Changes committed: Mon Jan 04 12:00:01 2010
```

プロンプトに新規ホスト名が次のように表示されます。mail3.example.com>

ドメイン ネーム システムの設定

コンテンツ セキュリティ アプライアンスのドメイン ネーム システム（DNS）は、GUI の [管理アプライアンス（Management Appliance）] > [ネットワーク（Network）] > [DNS] ページ、または `dnsconfig` コマンドを使用して設定できます。

次の設定値を設定できます。

- インターネットの DNS サーバまたはユーザ独自の DNS サーバを利用するか、および使用するサーバ
- DNS トラフィックに使用するインターフェイス
- 逆引き DNS ルックアップがタイムアウトするまで待機する秒数
- DNS キャッシュのクリア

DNS サーバの指定

AsyncOS では、インターネットのルート DNS サーバ、ユーザ独自の DNS サーバ、インターネットのルート DNS サーバ、または指定した権威 DNS サーバを使用できます。インターネットのルート サーバを使用するときは、特定のドメインに使用する代替サーバを指定することもできます。代替 DNS サーバは単一のドメインに適用されるため、該当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）になっている必要があります。

AsyncOS では、インターネットの DNS サーバを使用しない場合に「スプリット」DNS サーバをサポートしています。ユーザ独自の内部サーバを使用している場合は、例外のドメインおよび関連する DNS サーバを指定することもできます。

「スプリット」DNS を設定しているときは、in-addr.arpa（PTR）エントリも同様に設定する必要があります。このため、たとえば「.eng」クエリーをネームサーバ 1.2.3.4 にリダイレクトする際に、すべての .eng エントリが 172.16 ネットワークにある場合、スプリット DNS 設定に「eng,16.172.in-addr.arpa」をドメインとして指定する必要があります。

複数エントリとプライオリティ

入力する各 DNS サーバに、数値でプライオリティを指定できます。AsyncOS では、プライオリティが 0 に最も近い DNS サーバの使用を試みます。その 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、さらにそれよりわずかに長い秒数待機するという動作を続けます。待機時間の長さは、DNS サーバの実際の総数と、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。プライオリティが 3 つの場合、タイムアウトは 5 秒、10 秒、45 秒になります。

たとえば、4 つの DNS サーバを設定し、2 つにプライオリティ 0 を、1 つにプライオリティ 1 を、もう 1 つにプライオリティ 2 を設定したとします。

表 14-5　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。

インターネット ルート サーバの使用

AsyncOS DNS リゾルバは、高性能な電子メール配信に必要な大量の同時 DNS 接続を収容できるように設計されています。

（注）　デフォルト DNS サーバにインターネット ルート サーバ以外を設定することを選択した場合、設定されたサーバは権威サーバとなっていないドメインのクエリーを再帰的に解決できる必要があります。

逆引き DNS ルックアップのタイムアウト

シスコ コンテンツ セキュリティ アプライアンスは電子メールの送受信の際、リスナーに接続しているすべてのリモート ホストに対して「二重 DNS ルックアップ」の実行を試みます つまり、ダブル DNS ルックアップを実行することで、システムはリモート ホストの IP アドレスの正当性を確保および検証します。これは、接続元ホストの IP アドレスに対する逆引き DNS（PTR）ルックアップと、それに続く PTR ルックアップ結果に対する正引き DNS（A）ルックアップからなります。その後、システムは A ルックアップの結果が PTR ルックアップの結果と一致するかどうかをチェックします。結果が一致しないか、A レコードが存在しない場合、システムはホスト アクセス テーブル（HAT）内のエントリと一致する IP アドレスのみを使用します。この特別なタイムアウト時間はこのルックアップにのみ適用され、「複数エントリとプライオリティ」（P.14-42）で説明されている一般的な DNS タイムアウトには適用されません。

デフォルト値は、20 秒です。秒数に「0」を入力することで、すべてのリスナーに対してグローバルに逆引き DNS ルックアップのタイムアウトをディセーブルにできます。値を 0 秒に設定した場合、逆引き DNS ルックアップは試行されず、代わりに標準のタイムアウト応答がすぐに返されます。

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」が付与されたアラートが生成される場合がまれにあります。このメッセージは、システムによるプライマリ DNS サーバへの問い合わせができなかったことを示しています。この事象は、ネットワーク接続が確立される前に

DNS サブシステムがオンラインになった場合、ブートのタイミングで発生します。このメッセージが別のタイミングで表示された場合、ネットワーク問題が発生しているか、または DNS 設定で有効なサーバが指定されていないことを示しています。

DNS キャッシュのクリア

GUI の [キャッシュをクリア（Clear Chashe）] ボタン、または `dnsflush` コマンドを使用して、DNS キャッシュのすべての情報をクリアします（`dnsflush` コマンドの詳細については、『*Cisco IronPort AsyncOS CLI Reference Guide*』を参照してください）。ローカル DNS システムが変更された際に、この機能を使用できます。コマンドはすぐに実行され、キャッシュの再投入中に一時的に性能が低下する可能性があります。

グラフィカル ユーザ インターフェイスを使用した DNS 設定値の設定

手順

ステップ 1　[管理アプライアンス（Management Appliance）] > [ネットワーク（Network）] > [DNS] ページで、[設定を編集（Edit Settings）] ボタンをクリックします。

ステップ 2　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 サーバのどちらを使用するかを選択して、権威 DNS サーバを指定します。

ステップ 3　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 [行の追加（Add Row）] をクリックします。各サーバでこの作業を繰り返します。ユーザ独自の DNS サーバを入力する場合は、プライオリティも同時に指定します。詳細については、「DNS サーバの指定」（P.14-42）を参照してください。

ステップ 4　DNS トラフィック用のインターフェイスを選択します。

ステップ 5　逆引き DNS ルックアップをキャンセルするまでに待機する秒数を入力します。

ステップ 6　必要に応じて、[キャッシュをクリア（Clear Chashe）] をクリックして、DNS キャッシュをクリアします。

ステップ 7　変更を送信し、保存します。

TCP/IP トラフィック ルートの設定

一部のネットワーク環境では、標準のデフォルト ゲートウェイ以外のトラフィック ルートを使用する必要があります。スタティック ルートの管理は、GUI の [管理アプライアンス（Management Appliance）] > [ネットワーク（Network）] > [ルーティング（Routing）] ページ、または CLI の `routeconfig` コマンドを使用して行います。

GUI でのスタティック ルートの管理

[管理アプライアンス（Management Appliance）] > [ネットワーク（Network）] > [ルーティング（Routing）] ページを使用して、スタティック ルートの作成、編集、または削除を行えます。このページからデフォルト ゲートウェイの変更もできます。

スタティック ルートの追加

手順

ステップ 1　[管理アプライアンス（Management Appliance）] > [ネットワーク（Network）] > [ルーティング（Routing）] ページで、ルート リストの [ルートを追加（Add Route）] をクリックします。ルートの名前を入力します。

ステップ 2　宛先 IP アドレスを入力します。

ステップ 3　ゲートウェイの IP アドレスを入力します。

ステップ 4　変更を送信し、保存します。

スタティック ルートの削除

手順

ステップ 1　[スタティッ クルート（Static Routes）] のリストから、スタティック ルート名に対応するゴミ箱アイコンをクリックします。

ステップ 2　表示される警告ダイアログで [削除（Delete）] をクリックして削除を確認します。

ステップ 3　変更を保存します。

スタティック ルートの編集

手順

ステップ 1　[スタティック ルート（Static Routes）] のリストでルートの名前をクリックします。

ステップ 2　ルートの設定を変更します。

ステップ 3　変更を送信し、保存します。

デフォルト ゲートウェイの変更（GUI）

手順

ステップ 1　[ルーティング（Routing）] ページのルート リストで [デフォルト ルート（Default Route）] をクリックします。

ステップ 2　ゲートウェイの IP アドレスを変更します。

ステップ 3　変更を送信し、保存します。

デフォルト ゲートウェイの設定

GUI の [管理アプライアンス（Management Appliance）] > [ネットワーク（Network）] > [ルーティング（Routing）] ページ（「デフォルト ゲートウェイの変更（GUI）」（P.14-45）を参照してください）、または CLI の `setgateway` コマンドを使用して、デフォルト ゲートウェイを設定できます。

システム時刻の設定

アプライアンスのシステム時刻を設定し、時間帯を指定できます。GUI の [管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [タイム ゾーン（Time Zone）] ページと、[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [時刻設定（Time Settings）] ページを使用します。または、CLI で `ntpconfig`、`settime`、および `settz` コマンドを使用します。

[タイム ゾーン（Time Zone）] ページ

[時間帯（Time Zone）] ページ（GUI の [システム管理（System Administration）] メニューから利用可能）では、コンテンツ セキュリティ アプライアンスの時間帯が表示されます。特定の時間帯または GMT オフセットを選択できます。

時間帯の選択

アプライアンスの時間帯を設定するには、次の手順を実行します。

手順

ステップ 1　[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [タイム ゾーン（Time Zone）] を選択します。

ステップ 2　[設定を編集（Edit Settings）] をクリックします。

ステップ 3　地域、国、および時間帯を選択します。

ステップ 4　変更を送信し、保存します。

GMT オフセットの選択

シスコ コンテンツ セキュリティ アプライアンスの GMT オフセットを設定するには、次の手順に従います。

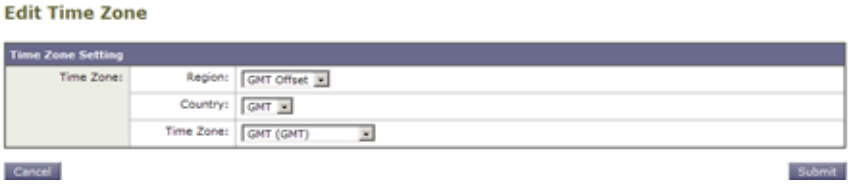
手順

ステップ 1　[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [タイム ゾーン（Time Zone）] を選択します。

ステップ 2　[設定を編集（Edit Settings）] をクリックします。

ステップ 3　地域のリストから [GMT オフセット（GMT Offset）] を選択します。[タイム ゾーン設定（Time Zone Setting）] ページが更新され、[タイム ゾーン（Time Zone）] フィールドに GMT オフセットが含まれるようになります。

図 14-10　　GMT オフセットの設定



ステップ 4　[タイム ゾーン（Time Zone）] フィールドでオフセットを選択します。オフセットとは、グリニッジ子午線のローカル時間であるグリニッジ標準時（GMT）に、加算または減算する時間のことです。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西側にあたります。プラス記号（「+」）の場合、グリニッジ子午線の東側にあたります。

ステップ 5　変更を送信し、保存します。

（注）　セキュリティ管理アプライアンスは、レポートのデータを収集する際に、セキュリティ管理アプライアンス上で時間設定を行った際に設定した情報からタイム スタンプを適用します。詳細については、「セキュリティ アプライアンスによるレポート用データの収集方法」（P.3-2）を参照してください。

時間帯ファイルの更新

いずれかの国の時間帯に変更があった場合は必ず、アプライアンスでこれらの時間帯ファイルを更新する必要があります。

時間帯ファイルの自動更新

手順

ステップ 1　[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [アップデート設定（Update Settings）] を選択します。

ステップ 2　[タイム ゾーン ルールの自動アップデートを有効にする（Enable automatic updates for Time zone rules）] チェックボックスをオンにします。

ステップ 3　間隔を入力します。重要な情報については、ページ上の [?] ヘルプをクリックします。

ステップ 4　まだ実行していない場合は、このページの他の設定値を設定します。「アップグレードおよびサービス アップデートの設定」（P.14-22）を参照してください。

時間帯ファイルの手動更新

手順

ステップ 1　[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [時刻設定（Time Settings）] を選択します。

ステップ 2　[タイム ゾーン ファイルの更新（Time Zone File Updates）] セクションを確認します。

ステップ 3　使用可能な時間帯ファイルの更新がある場合、[今すぐ更新（Update Now）] をクリックします。

システム時刻設定の編集

手動でシステム時刻を設定するか、または使用しているネットワーク上またはインターネット上の他のコンピュータとセキュリティ管理アプライアンスシステム クロックを同期するために Network Time Protocol (NTP) サーバを使用できます。

デフォルトの NTP サーバは `time.sco.cisco.com` です。

はじめる前に

デフォルトの NTP サーバを含め、外部 NTP サーバを使用する場合は、ファイアウォールを通過する必要なポートを開きます。第 C 章「ファイアウォール情報」を参照してください。

手順

ステップ 1　[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [時刻設定（Time Settings）] ページで、[設定を編集（Edit Settings）] をクリックします。

ステップ 2　時刻の設定方式を選択します。

ステップ 3　変更を送信し、必要に応じてコミットします。

コンフィギュレーション設定の保存とインポート

（注）　ここで説明されているコンフィギュレーション ファイルは、セキュリティ管理アプライアンスの設定に使用されます。第 9 章「Web セキュリティ アプライアンスの管理」で説明されているコンフィギュレーション ファイルおよび Configuration Master は、Web セキュリティ アプライアンスの設定に使用されます。

セキュリティ管理アプライアンスの大部分の設定は、1 つのコンフィギュレーション ファイルで管理できます。このファイルは Extensible Markup Language（XML）フォーマットで保持されます。

次のように、このファイルはさまざまな用途に使用できます。

- プライマリ セキュリティ管理アプライアンスで予期しない障害が発生した場合に、2 番目のセキュリティ管理アプライアンスをすばやく設定し、サービスを復元できます。
- コンフィギュレーション ファイルを別のシステムに保存し、重要な設定データをバックアップおよび保持できます。アプライアンスの設定中に間違いを犯した場合、保存した最新のコンフィギュレーション ファイルにロールバックできます。
- 既存のコンフィギュレーション ファイルをダウンロードし、アプライアンスの全体の設定を素早く確認できます（新しいブラウザの多くには XML ファイルを直接レンダリングする機能が含まれています）。これは、現在の設定にある可能性のあるマイナー エラー（誤植など）のトラブルシューティングに役立つ場合があります。

- 既存のコンフィギュレーション ファイルをダウンロードして、変更を行い、同じアプライアンスにアップロードできます。この場合は、実質的に設定の変更を行うために CLI と GUI の両方が「バイパス」されます。
- FTP を介してコンフィギュレーション ファイル全体をアップロードしたり、コンフィギュレーション ファイルの一部を CLI に直接貼り付けたりすることができます。
- このファイルは XML 形式になっているため、コンフィギュレーション ファイルのすべての XML エンティティが記述された、関連する文書型定義（DTD）も提供されます。XML コンフィギュレーション ファイルをアップロードする前にこの DTD をダウンロードして XML コンフィギュレーション ファイルを検証できます（XML 検証ツールはインターネットで簡単に入手できます）。

XML コンフィギュレーション ファイルを使用した複数のアプライアンスの管理

警告　ある セキュリティ管理アプライアンスから別の セキュリティ管理アプライアンスにコンフィギュレーション ファイルをインポートする場合は、次の点に注意してください。

元の設定内のすべて（IP アドレスを含む）が、コンフィギュレーション ファイルに含まれています。コンフィギュレーション ファイルを編集して IP アドレスを変更するか、元の セキュリティ管理アプライアンスがオフラインになっていることを確認します。

また、SSH 認証接続が終了することに注意してください。そうなった場合は、接続されたすべての Web セキュリティ アプライアンスおよび 電子メール セキュリティ アプライアンスとの接続を再確立する必要があります。

- あるアプライアンスから既存の設定ファイルをダウンロードし、変更を行い、別のアプライアンスにアップロードできます。これにより、複数のアプライアンスのインストールを簡単に管理できるようになります。ただし、電子メール セキュリティ アプライアンスからセキュリティ管理アプライアンスに、設定ファイルをロードすることはできません。
- あるアプライアンスからダウンロードされた既存のコンフィギュレーション ファイルを、複数のサブセクションに分割できます。（複数のアプライアンス環境の）すべてのアプライアンスで共通するこれらのセクションを変更し、サブセクションの更新時にこれらのセクションを他のアプライアンスにロードできます。

  たとえば、Global Unsubscribe コマンドをテストするためにテスト環境でアプライアンスを使用できます。グローバル配信停止リストを適切に設定した場合は、テスト アプライアンスのグローバル配信停止設定セクションをすべての実稼働アプライアンスにロードできます。

コンフィギュレーション ファイルの管理

アプライアンスでコンフィギュレーション ファイルを管理するには、[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [設定ファイル（Configuration File）] を選択します。

[設定ファイル（Configuration File）] ページには、次のセクションが含まれています。

- [現在の設定（Current Configuration）] : 現在のコンフィギュレーション ファイルを保存およびエクスポートするために使用します
- [設定をロード（Load Configuration）] : コンフィギュレーション ファイルの全体または一部をロードするために使用します

- [エンドユーザ セーフリスト/ブロックリスト データベース（Cisco IronPort スパム隔離）（End-User Safelist/Blocklist Database (Cisco IronPort Spam Quarantine)]：セーフリスト/ブロックリスト データベースの管理に使用します
- [設定情報のリセット（Reset Configuration）]：現在の設定を出荷時デフォルト値にリセットするために使用します（リセット前に設定を保存する必要があります）

関連項目

- 「以前コミットしたコンフィギュレーションへのロールバック」（P.14-52）

現在のコンフィギュレーション ファイルの保存およびエクスポート

[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [設定ファイル（Configuration File）] ページの [現在の設定（Current Configuration）] セクションを使用すると、現在のコンフィギュレーション ファイルを、ローカル マシンに保存したり、アプライアンスで保存したり（FTP/SCP ルートの `configuration` ディレクトリに保存されます）、指定されたアドレスに電子メールで送信したりできます。

パスワードのマスク

必要に応じて、チェックボックスをオンにして、ユーザのパスワードをマスクします。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。

（注）　パスワードがマスクされたコンフィギュレーション ファイルをロードして AsyncOS に戻すことはできません。

コンフィギュレーション ファイルのロード

設定ファイルは、設定をロードするアプライアンスと同じバージョンの AsyncOS を実行しているアプライアンスから保存される必要があります。

[管理アプライアンス（Management Appliance）] > [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、新しい設定情報をアプライアンスにロードします。情報は次の 3 つのいずれかの方法でロードできます。

- `configuration` ディレクトリに情報を格納し、アップロードする
- 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
- GUI に設定情報を直接貼り付ける

パスワードがマスクされたコンフィギュレーション ファイルはロードできません。

どの方法の場合でも、設定の上部に次のタグを含める必要があります。

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<config>
 ... your configuration information in valid XML
</config>
```

`</config>` 閉じタグは設定情報の後に指定する必要があります。XML 構文の値は、シスコ コンテンツ セキュリティ アプライアンスの `configuration` ディレクトリにある DTD を使用して解析および検証されます。DTD ファイルの名前は `config.dtd` です。`loadconfig` コマンドを使用したときにコマンド

ラインで検証エラーが報告された場合、変更はロードされません。コンフィギュレーション ファイルをアップロードする前に、アプライアンスの外部で DTD をダウンロードし、コンフィギュレーション ファイルを検証できます。

いずれの方法の場合でも、コンフィギュレーション ファイル全体（最上位のタグである <config></config> 間で定義された情報）またはコンフィギュレーション ファイルの *complete* および *unique* サブセクション（上記の宣言タグが含まれ、<config></config> タグ内に存在する場合）をインポートできます。

「complete（完全）」とは、DTD で定義されたサブセクションの開始タグおよび終了タグ全体が含まれることを意味します。たとえば、次のコードをアップロードまたは貼り付けると、検証エラーが発生します。

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<config>
  <autosupport_enabled>0</autosu
</config>
```

しかし、次のコードをアップロードまたは貼り付けても、検証エラーは発生しません。

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<config>
  <autosupport_enabled>0</autosupport_enabled>
</config>
```

「unique（一意）」とは、アップロードまたは貼り付けられるコンフィギュレーション ファイルのサブセクションが、設定として多義的でないことを意味します。たとえば、システムは 1 つのホスト名しか持てないため、次のコード（宣言および <config></config> タグを含む）をアップロードすることは可能です。

```
<hostname>mail4.example.com</hostname>
```

しかし、システムにはそれぞれ異なる受信者アクセス テーブルが定義された複数のリスナーが定義されている可能性があるため、次のコードのみをアップロードすることは多義的であると見なされます。

```
<rat>
   <rat_entry>
     <rat_address>ALL</rat_address>
     <access>RELAY</access>
   </rat_entry>
 </rat>
```

多義的であるため、「完全」な構文であっても許可されません。

警告　コンフィギュレーション ファイルまたはコンフィギュレーション ファイルのサブセクションをアップロードまたは貼り付ける場合は、待機中の可能性がある、保存されていない変更が破棄されることがあります。

空のタグと省略されたタグ

コンフィギュレーション ファイルのセクションをアップロードまたは貼り付ける場合は注意が必要です。タグを含めないと、コンフィギュレーション ファイルのアップロード時に設定の値が変更されません。ただし、空白タグを含めると、設定の問題が解消されます。

たとえば、次のコードをアップロードすると、システムからすべてのリスナーが削除されます。

```
<listeners></listeners>
```

警告　**コンフィギュレーション ファイルのサブセクションをアップロードしたり、貼り付けたりした場合、GUI または CLI から切断され、大量の設定データが破壊されることがあります。別のプロトコル、シリアル インターフェイス、または管理ポートのデフォルト設定を使用してアプライアンスに再接続できない場合は、このコマンドでサービスをディセーブルにしないでください。また、DTD で定義された設定構文がよくわからない場合は、このコマンドを使用しないでください。新しいコンフィギュレーション ファイルをロードする前に、必ず設定データをバックアップしてください。**

ログ サブスクリプションのパスワードのロードについての注意事項

パスワードが必要なログ サブスクリプションを含むコンフィギュレーション ファイルをロードしようとしても（たとえば、FTP プッシュを使用）、`loadconfig` コマンドは不明なパスワードについて警告しません。FTP プッシュが失敗し、`logconfig` コマンドを使用して正しいパスワードを設定するまで警告が生成されます。

文字セット エンコーディングについての注意事項

XML コンフィギュレーション ファイルの「encoding」属性は、ファイルをオフラインで操作するために使用している文字セットに関係なく、「`ISO-8859-1`」である必要があります。`showconfig` コマンド、`saveconfig` コマンド、または `mailconfig` コマンドを発行するたびに、エンコーディング属性がファイルで指定されます。

```
<?xml version="1.0" encoding="ISO-8859-1"?>
```

現時点では、このエンコーディングを持つコンフィギュレーション ファイルだけをロードできます。

現在の設定のリセット

現在の設定をリセットすると、シスコ コンテンツ セキュリティ アプライアンスが出荷時の初期状態に設定も戻します。リセットする前に設定を保存してください。

「出荷時の初期状態への設定のリセット」（P.14-5）を参照してください。

以前コミットしたコンフィギュレーションへのロールバック

以前コミットされた設定にロール バックできます。

コマンドライン インターフェイスで `rollbackconfig` コマンドを使用して、直近の 10 件のコミットから 1 件を選択します。

ロール バックをコミットすることを促されたときに [いいえ（No）] を入力した場合、変更をコミットする次回をこのロール バックがコミットします。

管理者アクセス権を持つユーザだけが `rollbackconfig` コマンドを使用できます。

（注）　以前の設定が復元するとログ メッセージまたはアラートは生成されません。

（注）　既存のデータを保持する十分なサイズにディスク領域を再割り当てするなどの一部のコミットでは、データ漏洩が発生する可能性があります。

コンフィギュレーション ファイル用の CLI コマンド

次のコマンドを使用すると、コンフィギュレーション ファイルを操作できます。

- showconfig
- mailconfig
- saveconfig
- loadconfig
- rollbackconfig
- resetconfig（「出荷時の初期状態への設定のリセット」（P.14-5）を参照）
- publishconfig
- backupconfig（参照「セキュリティ管理アプライアンスのデータのバックアップ」（P.14-7））

showconfig、mailconfig、および saveconfig コマンド

コンフィギュレーション コマンドの showconfig、mailconfig、および saveconfig の場合は、電子メールで送信されるファイルまたは表示されるファイルにパスワードを含めるかどうか選択することを求められます。パスワードを含めないことを選択すると、パスワード フィールドが空白のままになります。セキュリティの問題を心配する場合は、パスワードを含めないことを選択できます。ただし、loadconfig コマンドを使用してロードされた場合、パスワードがないコンフィギュレーション ファイルは失敗します。「ログ サブスクリプションのパスワードのロードについての注意事項」（P.14-52）を参照してください。

（注）　パスワードを含めることを選択した場合（「Do you want to include passwords?」に「yes」と回答します）にコンフィギュレーション ファイルを保存、表示、または電子メールで送信するとき、パスワードは暗号化されます。ただし、秘密キーと証明書は暗号化されていない PEM フォーマットで含まれます。

Showconfig コマンドは現在の設定を画面に出力します。

```
mail3.example.com> showconfig

Do you want to include passwords? Please be aware that a configuration without passwords
will fail when reloaded with loadconfig.

<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">

<!--
  Product: Cisco IronPort model number Messaging Gateway Appliance(tm)
  Model Number: model number
  Version: version of AsyncOS installed
  Serial Number: serial number
  Current Time: current time and date
[The remainder of the configuration file is printed to the screen.]
```

mailconfig コマンドを使用して、現在の設定をユーザに電子メールで送信します。メッセージには config.xml という名前の XML 形式のコンフィギュレーション ファイルが添付されます。

```
mail3.example.com> mailconfig

Please enter the email address to which you want to send
the configuration file.
[]> administrator@example.com
```

```
Do you want to include passwords? Please be aware that a configuration without passwords
will fail when reloaded with loadconfig.  [N]> y

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

セキュリティ管理アプライアンスで saveconfig コマンドを使用すると、一意のファイル名を使用して、すべての設定マスター ファイル（ESA および WSA）が configuration ディレクトリに保存されます。

```
mail3.example.com> saveconfig

Do you want to include passwords? Please be aware that a configuration without passwords
will fail when reloaded with loadconfig.  [N]> y

The file C650-00065B8FCEAB-31PM121-20030630T130433.xml has been saved in the configuration
directory.
mail3.example.com>
```

loadconfig コマンド

アプライアンスに新しい設定情報をロードするには、loadconfig コマンドを使用します。情報は次の 2 つのいずれかの方法でロードできます。

- configuration ディレクトリに情報を格納し、アップロードする
- CLI に設定情報を直接貼り付ける。

詳細については、「コンフィギュレーション ファイルのロード」（P.14-50）を参照してください。

rollbackconfig コマンド

「以前コミットしたコンフィギュレーションへのロールバック」（P.14-52）を参照してください。

publishconfig コマンド

変更を Configuration Master に公開するには、publishconfig コマンドを使用します。構文は次のとおりです。

publishconfig *config_master* [*job_name*] [*host_list* | *host_ip*

ここで、*config_master* は、サポートされている Configuration Master です。これらの Configuration Master のリストは、このリリースのリリース ノートの「Compatibility Matrix」（http://www.cisco.com/en/US/products/ps10155/prod_release_notes_list.html）にあります。このキーワードは必須です。キーワード *job_name* は省略可能で、指定しなかった場合は生成されます。

キーワード *host_list* は、公開される WSA アプライアンスのホスト名または IP アドレスのリストで、指定しなかった場合は、Configuration Master に割り当てられているすべてのホストに公開されます。オプションの *host_ip* には、カンマで区切って複数のホスト IP アドレスを指定できます。

publishconfig コマンドが成功したことを確認するには、smad_logs ファイルを調べます。[Web] > [ユーティリティ（Utilities）] > [Web アプライアンス ステータス（Web Appliance Status）] を選択することで、セキュリティ管理アプライアンスの GUI から公開履歴が成功だったことを確認することもできます。このページから、公開履歴の詳細を調べる Web アプライアンスを選択します。また、[Web] > [ユーティリティ（Utilities）] > [公開（Publish）] > [公開履歴（Publish History）] により、[公開履歴（Publish History）] ページに進むことができます。

CLI を使用した設定変更のアップロード

手順

ステップ 1　CLI の外部で、アプライアンスの configuration ディレクトリにアクセスできることを確認します。詳細については、付録 A「IP インターフェイスおよびアプライアンスへのアクセス」を参照してください。

ステップ 2　コンフィギュレーション ファイル全体またはコンフィギュレーション ファイルのサブセクションをアプライアンスの configuration ディレクトリに格納するか、saveconfig コマンドで作成した既存の設定を編集します。

ステップ 3　CLI 内で、loadconfig コマンドを使用して、ステップ 2 で示されたディレクトリに格納したコンフィギュレーション ファイルをロードするか、テキスト（XML 構文）を CLI に直接貼り付けます。

この例では、changed.config.xml という名前のファイルがアップロードされ、変更が保存されます。

```
mail3.example.com> loadconfig

1. Paste via CLI
2. Load from file
[1]> 2

Enter the name of the file to import:
[]> changed.config.xml

Values have been loaded.
Be sure to run "commit" to make these settings active.
mail3.example.com> commit
```

この例では、新しいコンフィギュレーション ファイルをコマンド ラインに直接貼り付けます（空白行で Ctrl を押した状態で D を押すと貼り付けコマンドが終了します）。次に、システム セットアップ ウィザードを使用して、デフォルトのホスト名、IP アドレス、およびゲートウェイ情報を変更します。（詳細は、「システム セットアップ ウィザードの実行」（P.2-8）を参照してください）。これで、変更が確定されます。

```
mail3.example.com> loadconfig

1. Paste via CLI
2. Load from file
[1]> 1

Paste the configuration file now. Press CTRL-D on a blank line when done.

[The configuration file is pasted until the end tag </config>. Control-D is entered on a
separate line.]

Values have been loaded.
Be sure to run "commit" to make these settings active.

mail3.example.com> commit

Please enter some comments describing your changes:
[]> pasted new configuration file and changed default settings
```

ディスク使用量の管理

セキュリティ管理アプライアンスのモニタリング サービスに割り当てられているディスク領域および現在使用されているディスク領域の大きさを表示するには、[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ディスク管理（Disk Management）] を選択します。

現在使用されている隔離のクォータの割合を表示するには、[管理アプライアンス（Management Appliance）] > [集約サービス（Centralized Services）] > [システム ステータス（System Status）] を選択し、[集約サービス（Centralized Services）] セクションを確認します。

最大ディスク領域と割り当て

組織で使用する各機能に、使用可能な最大量まで、使用可能なディスク領域を割り当てることができます。

表 14-6　使用可能な最大ディスク領域（GB 単位）

	ハードウェア プラットフォーム							
	M160	M170	M380	M660	M670	M680	M1060	M1070
隔離などのすべての機能に対して使用可能な合計	165	165	968	681	681	1805	1039	1407
スパム隔離の最大量	70	70	150	150	150	265	265	265

表 14-7　機能別のデフォルト ディスク領域割り当て（パーセント単位）

機能	割り当てられたディスク領域 デフォルト（概算）
中央集中型レポーティング（電子メールおよび Web）	10 %
電子メール トラッキング	22.5%
Web トラッキング	22.5%
スパム隔離	22.5%
ポリシー、ウイルス、アウトブレイク隔離をまとめて	22.5%

（注）

- レポーティング（単なるカウンター）や、トラッキング（限定的な量のヘッダー情報だけを保存）とは異なり、スパム隔離では、隔離されたメッセージのメッセージ本文全体が保存されるため、他の機能よりも、メッセージごとの使用ディスク領域が大幅に多くなります。このように大量の領域が使用されるため、アプライアンスがロックされるのを防ぐために、スパム隔離のディスク クォータには、単なる使用可能なディスク領域よりも厳しい制限があります。
- セキュリティ管理アプライアンスの中央集中型レポーティング ディスク領域は、電子メールと Web の両方のデータに使用されます。中央集中型電子メール レポーティングと中央集中型 Web レポーティングのどちらか一方をイネーブルにすると、すべての領域がイネーブルにした機能専用になります。両方をイネーブルにした場合、電子メールおよび Web レポーティング データは領域を共有し、領域はファースト カム ベースで割り当てられます。

- 中央集中型 Web レポーティングをイネーブルにしているが、レポーティングにディスク領域が割り当てられていない場合、ディスク領域が割り当てられるまで、中央集中型 Web レポーティングが機能しません。
- 既存の割り当て量を少なくした場合、新しい割り当て量内にすべてのデータが収まるようになるまで、最も古いデータから削除されます。新しいクォータが現在使用されているディスク領域よりも大きい場合、データは失われません。
- 割り当て量をゼロに設定すると、データは保持されなくなります。
- 非スパム隔離でのディスク領域管理方法の詳細については、「ポリシー、ウイルス、およびアウトブレイク隔離に対するディスク領域の割り当て」（P.8-10）および「隔離内のメッセージの保留時間」（P.8-10）を参照してください。

ディスク領域量の再割り当て

アプライアンスで、特定機能用のディスク領域が頻繁に不足し、一方で他の機能用のディスク領域が余分にある場合、ディスク領域を再割り当てすることで、この問題を緩和できます。すべての機能により多くの領域が必要な場合は、ハードウェアのアップグレードを検討してください。

はじめる前に

- ディスク割り当てを変更すると、既存のデータまたは機能のアベイラビリティに影響する場合があります。「最大ディスク領域と割り当て」（P.14-56）で情報を参照してください。
- 隔離からメッセージを手動で解放または削除することで、隔離用の領域を一時的に作成できます。

手順

ステップ 1　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ディスク管理（Disk Management）] を選択します。

ステップ 2　[ディスク クォータの編集（Edit Disk Quotas）] をクリックします。

ステップ 3　[ディスク クォータの編集（Edit Disk Quotas）] ページで、各サービスに割り当てるディスク領域の量（ギガバイト単位）を入力します。

スパム隔離以外のすべてのサービスに対して、0 からディスク領域の合計量までの値を入力できます。

ステップ 4　[送信（Submit）] をクリックします。

ステップ 5　確認ダイアログボックスで、[新しいクオータの設定（Set New Quotas）] をクリックします。

ステップ 6　[確定する（Commit）] をクリックして変更を保存します。

ビューのカスタマイズ

お気に入りページの使用

（ローカル認証された管理ユーザだけ）もっともよく使用するページへ簡単にアクセスするリストを作成できます。

目的	操作内容
お気に入りリストにページを追加	追加するページに移動し、ウィンドウの右上角の近くの [お気に入り（My Favorites）] メニューから [このページをお気に入りに追加（Add This Page To My Favorites）] を選択します。 お気に入りの変更ではコミットは必要ありません。
お気に入りの順序を変更	[お気に入り（My Favorites）] > [すべてのお気に入りを表示（View All My Favorites）] を選択しお気に入りを希望の順番にドラッグします。
お気に入りを削除	[お気に入り（My Favorites）] > [すべてのお気に入りを表示（View All My Favorites）] を選択し、お気に入りを削除します。
お気に入りのページに移動	ウィンドウの右上隅付近に**ある** [お気に入り（My Favorites）] メニューからページを選択します。
カスタム レポートのページを表示または作成	「カスタム レポート」（P.3-7）を参照してください。
メイン インターフェイスに戻る	お気に入りを選択するか、ページ下部の [前のページに戻る（Return to previous page）] をクリックします。

プリファレンスの 設定

セキュリティ管理アプライアンス上で設定されている管理ユーザ

ローカル認証されたユーザは次のプリファレンスを選択できます。このプリファレンスは、ユーザがセキュリティ管理アプライアンスにログインするたびに適用されます。

- 言語（GUI および PDF レポートに適用）
- ランディング ページ（ログイン後に表示されるページ）
- レポート ページのデフォルトの時間範囲（使用可能なオプションは、電子メールおよび Web レポーティング ページのサブセットです）
- レポート ページの表に表示する行数

実際のオプションは、ユーザ ロールによって異なります。

これらのプリファレンスを設定するには、[オプション（Options）] > [環境設定（Preferences）] を設定します。([オプション（Options）] メニューは GUI ウィンドウの上部右側にあります)。完了したら変更を送信します。確定する必要はありません。

ヒント　[環境設定（Preferences）] ページにアクセスする前に表示していたページに戻るには、ページ下部の [前のページに戻る（Return to previous page）] リンクをクリックします。

外部認証されたユーザ

外部認証されたユーザは、[オプション（Options）] メニューで表示言語を直接選択できます。

CHAPTER 15

ロギング

ロギングの概要

ログ ファイルには、システムのアクティビティの例外に加えて、通常の操作が記録されます。シスコ コンテンツ セキュリティ アプライアンスのモニタリング、トラブルシューティング、およびシステム パフォーマンスの評価のためにログを使用します。

ほとんどのログは、プレーン テキスト（ASCII）形式で記録されますが、トラッキング ログはリソースの効率性を保つためにバイナリ形式で記録されます。ASCII テキスト情報は、任意のテキスト エディタで読むことができます。

ロギングとレポーティング

ロギング データは、メッセージ フローのデバッグ、基本的な日常の動作に関する情報の確認（FTP 接続の詳細、HTTP ログ ファイルなど）、アーカイブのコンプライアンスの目的に使用します。

このロギング データには、電子メール セキュリティ アプライアンスから直接アクセスすることも、任意の外部 FTP サーバに送信してアーカイブまたは読み取ることもできます。アプライアンスに FTP 接続してログにアクセスすることも、バックアップの目的でプレーン テキストのログを外部サーバにプッシュすることもできます。

レポーティング データを表示するには、アプライアンスのグラフィカル ユーザ インターフェイスの [レポート（Report）] ページを使用します。元データにはアクセスできません。また、シスコのコンテンツセキュリティ管理アプライアンス以外には送信できません。

（注） セキュリティ管理アプライアンスは、Cisco IronPort スパム隔離（ISQ）データの例外を含む、すべてのレポーティングおよびトラッキング情報を取り出します。ISQ データは、ESA から渡されます。

ログの取得

ログ ファイルは、表 15-1 に示すファイル転送プロトコルを使用して取得できます。プロトコルは、グラフィカル ユーザ インターフェイスでサブスクリプションを作成または編集するときに設定するか、CLI の logconfig コマンドを使用して設定します。

表 15-1　ログ転送プロトコル

FTP ポーリング	このタイプのファイル転送では、リモート FTP クライアントは管理者レベルまたはオペレータ レベルのユーザのユーザ名およびパスワードを使用して、アプライアンスにアクセスし、ログ ファイルを取得します。FTP ポーリング方法を使用するようにログ サブスクリプションを設定する場合は、保持するログ ファイルの最大数を指定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。
FTP プッシュ	このタイプのファイル転送では、シスコ コンテンツ セキュリティ アプライアンスがリモート コンピュータの FTP サーバに、定期的にログ ファイルをプッシュします。サブスクリプションには、ユーザ名、パスワード、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、設定されたロールオーバー スケジュールに基づいて転送されます。
SCP プッシュ	このタイプのファイル転送では、シスコ コンテンツ セキュリティ アプライアンスがリモート コンピュータの 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、設定されたロールオーバー スケジュールに基づいて転送されます。
Syslog プッシュ	このタイプのファイル転送では、シスコ コンテンツ セキュリティ アプライアンスがリモート Syslog サーバにログ メッセージを送信します。この方法は、RFC 3164 に準拠しています。Syslog サーバのホスト名を指定し、ログの送信に UDP または TCP を使用する必要があります。使用するポートは 514 です。ログのファシリティは選択できますが、ログ タイプのデフォルトはドロップダウン メニューであらかじめ選択されています。syslog プッシュを使用して転送できるのは、テキストベースのログだけです。

ファイル名およびディレクトリ構造

AsyncOS はログ サブスクリプションで指定したログ名に基づいて、各ログ サブスクリプションのディレクトリを作成します。ディレクトリ内のログのファイル名は、ログ サブスクリプションで指定されたファイル名、ログ ファイルが開始されたタイムスタンプ、および単一文字のステータス コードで構成されています。次に、ディレクトリおよびファイル名の規則の例を示します。

```
/<Log_Name>/<Log_Filename>.@<timestamp>.<statuscode>
```

ステータス コードは、.c（「current（現在）」の意味）、または .s（「saved（保存済み）」の意味）です。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。

ログのロールオーバーおよび転送スケジュール

ログ サブスクリプションを作成するときに、ログのロールオーバー、古いファイルの転送、および新しいファイルの作成のトリガーを指定します。

次のトリガーのいずれかを選択します。

- ファイル サイズ
- 時間
  - 指定した間隔で（秒、分、時間、または日数）

値を入力するときは、画面の例に従います。

2 時間半など、複合間隔を入力するには、例 2h30m に従います。

または

- 毎日、指定した時刻に

または

- 選択した週の曜日の指定した時刻に

時刻を指定する場合は、24 時間形式を使用します。たとえば 11pm は 23:00 です。

1 日に複数のロールオーバー時間をスケジュール設定するには、時間をカンマで区切ります。たとえば、深夜と正午にログをロールオーバーするには、00:00, 12:00 と入力します。

アスタリスク（*）をワイルドカードとして使用できます。
たとえば、正確に毎時および 30 分ごとにログをロールオーバーするには、*:00, *:30 と入力します。

指定した制限に達すると（またはサイズおよび時間の両方に基づいた制限を設定している場合は最初の制限に達すると）、ログ ファイルがロールオーバーされます。FTP ポーリング転送メカニズムに基づいたログ サブスクリプションでは、ファイルが作成されると、それらのファイルが取得されるか、システムでログ ファイル用にさらにスペースが必要になるまで、アプライアンスの FTP ディレクトリにそれらのファイルが保存されます。

（注）　次の制限に達したときにロールオーバーが実行中の場合、新しいロールオーバーはスキップされます。エラーが記録され、アラートが送信されます。

ログ ファイル内のタイムスタンプ

次のログ ファイルには、ログ自体の開始日と終了日、AsyncOS のバージョン、および GMT オフセット（ログの開始時からの秒数）が含まれています。

- メール ログ
- セーフリスト/ブロックリスト ログ
- システム ログ

デフォルトでイネーブルになるログ

セキュリティ管理アプライアンスには、有効な次のログ サブスクリプションが事前設定されています。

表 15-2　事前設定されたログ サブスクリプション

ログ名	ログ タイプ	取得方法
cli_logs	CLI 監査ログ	FTP ポーリング
euq_logs	Cisco IronPort スパム隔離ログ	FTP ポーリング
euqgui_logs	Cisco IronPort スパム隔離 GUI ログ	FTP ポーリング
gui_logs	HTTP ログ	FTP ポーリング
mail_logs	Cisco IronPort テキスト メール ログ	FTP ポーリング
reportd_logs	レポーティング ログ	FTP ポーリング
reportqueryd_logs	レポーティング クエリー ログ	FTP ポーリング

表 15-2　事前設定されたログ サブスクリプション （続き）

ログ名	ログ タイプ	取得方法
slbld_logs	セーフリスト/ブロックリスト ログ	FTP ポーリング
smad_logs	SMA ログ	FTP ポーリング
system_logs	システム ログ	FTP ポーリング
trackerd_logs	トラッキング ログ	FTP ポーリング

事前定義されているすべてのログ サブスクリプションでは、ログ レベルが Information に設定されています。ログ レベルの詳細については、「ログ レベルの設定」（P.15-22）を参照してください。

適用されているライセンス キーによっては、追加のログ サブスクリプションを設定できます。ログ サブスクリプションの作成および編集については、「ログ サブスクリプション」（P.15-21）を参照してください。

ログ タイプ

ログ タイプの概要

ログ サブスクリプションはログ タイプを名前、ログ レベル、およびファイル サイズや宛先情報などのその他の特性に関連付けます。コンフィギュレーション履歴ログ以外のすべてのログ タイプで、複数のサブスクリプションを使用できます。ログ タイプによってログに記録されるデータが決まります。ログ サブスクリプションを作成するときにログ タイプを選択します。詳細については、「ログ サブスクリプション」（P.15-21）を参照してください。

AsyncOS では、次のログ タイプが生成されます。

表 15-3　ログ タイプ

ログ タイプ	説明
認証ログ	認証ログには、ローカルまたは外部認証されたユーザおよびセキュリティ管理アプライアンスへの GUI および CLI の両方のアクセスについて、成功したログインと失敗したログイン試行が記録されます。 外部認証がオンの場合、デバッグおよびより詳細なモードでは、すべての LDAP クエリーがこれらのログに表示されます。
バックアップ ログ	バックアップ ログはバックアップ プロセスを開始から終了まで記録します。 バックアップ スケジューリングに関する情報は、SMA ログ内にあります。
CLI 監査ログ	CLI 監査ログには、システム上のすべての CLI アクティビティが記録されます。
コンフィギュレーション履歴ログ	コンフィギュレーション履歴ログは、どのようなセキュリティ管理アプライアンスの変更がいつ行われたかの情報を記録します。ユーザが変更をコミットするたびに、新しいコンフィギュレーション履歴ログが作成されます。
FTP サーバ ログ	FTP ログには、インターフェイスでイネーブルになっている FTP サービスの情報が記録されます。接続の詳細とユーザ アクティビティが記録されます。
GUI ログ	GUI ログには、Web インターフェイスでのページ更新の履歴、セッション データ、およびユーザがアクセスしたページが記録されます。GUI ログを使用して、ユーザ アクティビティを追跡することや、GUI でユーザに表示されたエラーを調査することができます。エラー トレースバックは、通常、このログに記録されます。 GUI ログには、SMTP トランザクションに関する情報（たとえば、アプライアンスから電子メールで送信されるスケジュール済みレポートに関する情報）も記録されます。
HTTP ログ	HTTP ログには、インターフェイスでイネーブルになっている HTTP サービスおよびセキュア HTTP サービスに関する情報が記録されます。HTTP を介してグラフィカル ユーザ インターフェイス（GUI）にアクセスするため、HTTP ログは基本的に、CLI 監査ログの GUI 版になっています。セッション データ（新規セッション、期限切れセッションなど）、およびグラフィカル ユーザ インターフェイスでアクセスされたページが記録されます。
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。
テキスト メール ログ	テキスト メール ログには、電子メール システムの動作（メッセージの受信、メッセージの配信試行、接続の開始と終了、メッセージのバウンスなど）に関する情報が記録されます。 メール ログに添付ファイル名が含まれる場合に関する重要な情報については、「トラッキング サービスの概要」（P.6-1）を参照してください。
LDAP デバッグ ログ	[システム管理（System Administration）] > [LDAP] で LDAP を設定している場合は、これらのログを問題のデバッグに使用します。 たとえば、これらのログには、[テスト サーバ（Test Server）] ボタンや [テスト クエリ（Test Queries）] ボタンをクリックした結果が記録されます。 失敗した LDAP 認証の詳細については、認証ログを参照してください。
NTP ログ	NTP ログには、アプライアンスと任意の設定済みネットワーク タイム プロトコル（NTP）サーバとの通信が記録されます。NTP サーバの設定の詳細については、「システム時刻の設定」（P.14-46）を参照してください。

表 15-3　ログ タイプ （続き）

ログ タイプ	説明
レポーティング ログ	レポーティング ログには、中央集中型レポーティング サービスのプロセスに関連付けられたアクションが記録されます。
レポーティング クエリー ログ	レポーティング クエリー ログには、アプライアンスで実行された、レポーティング クエリーに関連付けられたアクションが記録されます。
SMA ログ	SMA ログには、一般的なセキュリティ管理アプライアンスプロセスに関連付けられたアクションが記録されます。集約管理レポート、集約管理トラッキング、Cisco IronPort スパム隔離サービスのプロセスは含まれません。 これらのログには、バックアップ スケジューリングに関する情報が含まれます。
SNMP ログ	SNMP ログには、SNMP ネットワーク管理エンジンに関連するデバッグ メッセージが記録されます。トレースまたはデバッグ モードでは、セキュリティ管理アプライアンスへの SNMP 要求が含まれます。
セーフリスト/ブロックリスト ログ	セーフリスト/ブロックリスト ログには、セーフリスト/ブロックリストの設定およびデータベースに関するデータが記録されます。
スパム隔離 GUI ログ	Cisco IronPort スパム隔離 GUI ログには、GUI を介した隔離設定、エンド ユーザ認証、エンド ユーザ アクション（例：電子メールの解放）など、Cisco IronPort スパム隔離 GUI に関連するアクションが記録されます。
スパム隔離ログ	Cisco IronPort スパム隔離ログには、Cisco IronPort スパム隔離プロセスに関連付けられたアクションが記録されます。
ステータス ログ	ステータス ログには、`status detail` および `dnsstatus` などの CLI ステータス コマンドで検出されたシステム統計情報が記録されます。記録期間は、`logconfig` の `setup` サブコマンドを使用して設定します。ステータス ログでレポートされるカウンタまたはレートは、前回カウンタがリセットされた時点からの値です。
システム ログ	システム ログには、ブート情報、DNS ステータス情報、および `commit` コマンドを使用してユーザが入力したコメントが記録されます。システム ログは、アプライアンスの状態のトラブルシューティングに役立ちます。
トラッキング ログ	トラッキング ログには、トラッキング サービスのプロセスに関連付けられたアクションが記録されます。トラッキング ログは、メール ログのサブセットになっています。
アップデータ ログ	時間帯のアップデートなど、サービス アップデートに関する情報。
アップグレード ログ	アップグレードのダウンロードとインストールに関するステータス情報。

ログ タイプの比較

表 15-4 に、各ログ タイプの特徴をまとめます。

表 15-4　　ログ タイプの比較

						次の情報を格納					
	トランザクション	ステートレス	テキストとして記録	バイナリとして記録	ヘッダー ロギング	定期的なステータス情報	メッセージ受信情報	配信情報	個々のハード バウンス	個々のソフト バウンス	設定情報
認証ログ	•		•								
バックアップ ログ	•		•								
CLI 監査ログ	•		•			•					
コンフィギュレーション履歴ログ	•		•								•
FTP サーバ ログ	•		•			•					
HTTP ログ	•		•			•					
Haystack ログ	•		•								
テキスト メール ログ	•		•		•	•	•	•	•	•	
LDAP デバッグ ログ	•		•								
NTP ログ	•		•			•					
レポーティング ログ	•		•			•					
レポーティング クエリー ログ	•		•			•					
SMA ログ	•		•			•					
SNMP ログ	•		•								
セーフリスト/ブロックリスト ログ	•		•			•					
スパム隔離 GUI	•		•			•					
スパム隔離	•		•			•					
ステータス ログ		•	•			•					
システム ログ	•		•			•					
トラッキング ログ	•			•	•		•	•	•	•	
アップデータ ログ	•		•								

コンフィギュレーション履歴ログの使用

コンフィギュレーション履歴ログは、コンフィギュレーション ファイルで構成され、ユーザの名前、ユーザが変更を行った設定の場所の説明、変更を保存するときにユーザが入力したコメントがリストされた追加のセクションがあります。ユーザが変更をコミットするたびに、変更後のコンフィギュレーション ファイルを含む新しいログが作成されます。

コンフィギュレーション履歴ログの例

次のコンフィギュレーション履歴ログの例は、システムにログインできるローカル ユーザを定義するテーブルに、ユーザ（admin）がゲスト ユーザを追加したことを示しています。

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<!--
  XML generated by configuration change.
  Change comment: added guest user
  User: admin
  Configuration are described as:
    This table defines which local users are allowed to log into the system.
  Product: Cisco IronPort M160 Messaging Gateway(tm) Appliance
  Model Number: M160
  Version: 6.7.0-231
  Serial Number: 000000000ABC-D000000
  Number of CPUs: 1
  Memory (GB): 4
  Current Time: Thu Mar 26 05:34:36 2009
  Feature "Centralized Configuration Manager": Quantity = 10, Time Remaining = "25 days"
  Feature "Centralized Reporting": Quantity = 10, Time Remaining = "9 days"
  Feature "Centralized Tracking": Quantity = 10, Time Remaining = "30 days"
  Feature "Centralized Spam Quarantine": Quantity = 10, Time Remaining = "30 days"
  Feature "Receiving": Quantity = 1, Time Remaining = "Perpetual"
-->
<config>
```

CLI 監査ログの使用

表 15-5 に、CLI 監査ログに記録される統計情報を示します。

表 15-5　CLI 監査ログの統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
PID	コマンドが入力された特定の CLI セッションのプロセス ID。
メッセージ	メッセージは、入力された CLI コマンド、CLI 出力（メニュー、リストなど）、および表示されるプロンプトで構成されます。

CLI 監査ログの例

次の CLI 監査ログの例は、`who` および `textconfig` CLI コマンドが入力された PID 16434 の情報を示しています。

```
Thu Sep  9 14:35:55 2004 Info: PID 16434: User admin entered 'who'; prompt was
'\nmail3.example.com> '
Thu Sep  9 14:37:12 2004 Info: PID 16434: User admin entered 'textconfig'; prompt was
'\nUsername  Login Time  Idle Time  Remote Host  What\n
========  ==========  =========  ===========  ====\n
admin     Wed 11AM    3m 45s     10.1.3.14    tail\nadmin     02:32PM     0s
10.1.3.14    cli\nmail3.example.com> '
Thu Sep  9 14:37:18 2004 Info: PID 16434: User admin entered ''; prompt was '\nThere are
no text resources currently defined.\n\n\nChoose the operation you want to perform:\n- NEW
- Create a new text resource.\n- IMPORT - Import a text resource from a file.\n[]> '
```

FTP サーバ ログの使用

表 15-6 に、FTP サーバ ログに記録される統計情報を示します。

表 15-6　FTP サーバ ログの統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
ID	接続 ID。FTP 接続ごとの別個の ID。
メッセージ	ログ エントリのメッセージ セクションは、ログファイルのステータス情報、または FTP 接続情報（ログイン、アップロード、ダウンロード、ログアウトなど）になります。

FTP サーバ ログの例

次の FTP サーバ ログの例には、接続（ID:1）が記録されています。着信接続の IP アドレスのほか、アクティビティ（ファイルのアップロードとダウンロード）およびログアウトが示されています。

```
Wed Sep  8 18:03:06 2004 Info: Begin Logfile
Wed Sep  8 18:03:06 2004 Info: Version: 4.0.0-206 SN: 00065BF3BA6D-9WFWC21
Wed Sep  8 18:03:06 2004 Info: Time offset from UTC: 0 seconds
Wed Sep  8 18:03:06 2004 Info: System is coming up
Fri Sep 10 08:07:32 2004 Info: Time offset from UTC: -25200 seconds
Fri Sep 10 08:07:32 2004 Info: ID:1 Connection from 10.1.3.14 on 172.19.0.86
Fri Sep 10 08:07:38 2004 Info: ID:1 User admin login SUCCESS
Fri Sep 10 08:08:46 2004 Info: ID:1 Upload wording.txt 20 bytes
Fri Sep 10 08:08:57 2004 Info: ID:1 Download words.txt 1191 bytes
Fri Sep 10 08:09:06 2004 Info: ID:1 User admin logout
```

HTTP ログの使用

表 15-7 に、HTTP ログに記録される統計情報を示します。

表 15-7　HTTP ログに記録される統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
ID	セッション ID。
req	接続元マシンの IP アドレス。
user	接続ユーザのユーザ名。
メッセージ	実行されたアクションに関する情報。GET コマンド、POST コマンド、またはシステム ステータスなどが含まれる場合があります。

HTTP ログの例

次の HTTP ログの例は、管理者ユーザによるグラフィカル ユーザ インターフェイスの使用（システム セットアップ ウィザードの実行など）を示しています。

```
Wed Sep  8 18:17:23 2004 Info: http service on 192.168.0.1:80 redirecting to https port
443
Wed Sep  8 18:17:23 2004 Info: http service listening on 192.168.0.1:80
Wed Sep  8 18:17:23 2004 Info: https service listening on 192.168.0.1:443
```

```
Wed Sep  8 11:17:24 2004 Info: Time offset from UTC: -25200 seconds
Wed Sep  8 11:17:24 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg POST
/system_administration/system_setup_wizard HTTP/1.1 303
Wed Sep  8 11:17:25 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/system_administration/ssw_done HTTP/1.1 200
Wed Sep  8 11:18:45 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/monitor/incoming_mail_overview HTTP/1.1 200
Wed Sep  8 11:18:45 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/monitor/mail_flow_graph?injector=&width=365&interval=0&type=recipientsin&height=190
HTTP/1.1 200
Wed Sep  8 11:18:46 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/monitor/classification_graph?injector=&width=325&interval=0&type=recipientsin&height=190
HTTP/1.1 200
Wed Sep  8 11:18:49 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/monitor/quarantines HTTP/1.1 200
```

Cisco IronPort スパム隔離ログの使用

表 15-8 に、Cisco IronPort スパム隔離ログに記録される統計情報を示します。

表 15-8　Cisco IronPort スパム隔離ログの統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
メッセージ	メッセージは、実行されたアクション（メッセージの隔離、隔離領域からの解放など）で構成されます。

Cisco IronPort スパム隔離ログの例

次のログの例は、隔離から admin@example.com に 2 個のメッセージ（MID 8298624 と MID 8298625）が解放されたことを示しています。

```
Mon Aug 14 21:41:47 2006 Info: ISQ: Releasing MID [8298624, 8298625] for all
Mon Aug 14 21:41:47 2006 Info: ISQ: Delivering released MID 8298624 (skipping work queue)
Mon Aug 14 21:41:47 2006 Info: ISQ: Released MID 8298624 to admin@example.com
Mon Aug 14 21:41:47 2006 Info: ISQ: Delivering released MID 8298625 (skipping work queue)
Mon Aug 14 21:41:47 2006 Info: ISQ: Released MID8298625 to admin@example.com
```

Cisco IronPort スパム隔離 GUI ログの使用

表 15-9 に、Cisco IronPort スパム隔離 GUI ログに記録される統計情報を示します。

表 15-9　Cisco IronPort スパム隔離 GUI ログの統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
メッセージ	メッセージは、ユーザ認証など、実行されたアクションで構成されます。

Cisco IronPort スパム隔離 GUI ログの例

次のログの例は、成功した認証、ログイン、およびログアウトを示しています。

表 15-10　Cisco IronPort スパム隔離 GUI ログの例

```
Fri Aug 11 22:05:28 2006 Info: ISQ: Serving HTTP on 192.168.0.1, port 82
Fri Aug 11 22:05:29 2006 Info: ISQ: Serving HTTPS on 192.168.0.1, port 83
Fri Aug 11 22:08:35 2006 Info: Authentication OK, user admin
Fri Aug 11 22:08:35 2006 Info: logout:- user:pqufOtL6vyI5StCqhCfO
session:10.251.23.228
Fri Aug 11 22:08:35 2006 Info: login:admin user:pqufOtL6vyI5StCqhCfO
session:10.251.23.228
Fri Aug 11 22:08:44 2006 Info: Authentication OK, user admin
```

Cisco IronPort テキスト メール ログの使用

これらのログには、電子メールの受信、電子メールの配信、およびバウンスの詳細が記録されます。ステータス情報も、1 分ごとにメール ログに書き込まれます。これらのログは、特定のメッセージの配信を理解し、システム パフォーマンスを分析するうえで有益な情報源となります。

これらのログに、特別な設定は必要ありません。ただし、添付ファイル名を表示するには、適切なシステムの設定が必要です。添付ファイル名は、常に記録されるわけではありません。詳細については、「トラッキング サービスの概要」（P.6-1）を参照してください。

表 15-11 に、テキスト メール ログに表示される情報を示します。

表 15-11　テキスト メール ログの統計情報

統計	説明
ICID	Injection Connection ID（インジェクション接続 ID）。システムに対する個々の SMTP 接続を表す数値 ID です。システムへの 1 つの SMTP 接続で、単一のメッセージまたは多数のメッセージを送信できます。
DCID	Delivery Connection ID（配信接続 ID）。別のサーバに対する個々の SMTP 接続を表す数値 ID であり、この接続で 1 個から数千個のメッセージが配信されます。1 つのメッセージ送信で一部または全部の RID が一緒に配信されます。
RCID	RPC Connection ID（RPC 接続 ID）。Cisco IronPort スパム隔離に対する個々の RPC 接続を表す数値 ID です。この ID を使用して、Cisco IronPort スパム隔離との間で送受信されるメッセージを追跡します。
MID	メッセージ ID。この ID を使用して、メッセージのフローをログで追跡します。
RID	受信者 ID。各メッセージ受信者には、ID が割り当てられます。
New	新規の接続が開始されました。
Start	新規のメッセージが開始されました。

例

ログ ファイルを解釈するためのガイドとして、次のサンプルを使用してください。

（注）　ログ ファイルの各行には、番号が*割り当てられません*。ここでは、単にサンプル用として番号が割り当てられています。

表 15-12　テキスト メール ログの詳細

1	`Mon Apr 17 19:56:22 2003 Info: New SMTP ICID 5 interface Management (10.1.1.1) address 10.1.1.209 reverse dns host remotehost.com verified yes`
2	`Mon Apr 17 19:57:20 2003 Info: Start MID 6 ICID 5`
3	`Mon Apr 17 19:57:20 2003 Info: MID 6 ICID 5 From: <sender@remotehost.com>`
4	`Mon Apr 17 19:58:06 2003 Info: MID 6 ICID 5 RID 0 To: <mary@yourdomain.com>`
5	`Mon Apr 17 19:59:52 2003 Info: MID 6 ready 100 bytes from <sender@remotehost.com>`
6	`Mon Apr 17 19:59:59 2003 Info: ICID 5 close`
7	`Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 8 interface 192.168.42.42 address 10.5.3.25`
8	`Mon Mar 31 20:10:58 2003 Info: Delivery start DCID 8 MID 6 to RID [0]`
9	`Mon Mar 31 20:10:58 2003 Info: Message done DCID 8 MID 6 to RID [0]`
10	`Mon Mar 31 20:11:03 2003 Info: DCID 8 close`

前述のログ ファイルを読み取るためのガイドとして、表 15-13 を使用してください。

表 15-13　テキスト メール ログの例の詳細

行番号	説明
1	システムに対して新しい接続が開始され、インジェクション ID（ICID）「5」が割り当てられました。この接続は管理 IP インターフェイスで受信され、10.1.1.209 のリモート ホストで開始されました。
2	クライアントから `MAIL FROM` コマンドが実行された後、メッセージにメッセージ ID（MID）「6」が割り当てられました。
3	送信者アドレスが識別され、受け入れられます。
4	受信者が識別され、受信者 ID（RID）「0」が割り当てられました。
5	MID 5 が受け入れられ、ディスクに書き込まれ、確認応答されました。
6	受信が成功し、受信接続が終了しました。
7	メッセージ配信プロセスが開始されました。192.168.42.42 から 10.5.3.25 への配信に、配信接続 ID（DCID）「8」が割り当てられました。
8	RID「0」へのメッセージ配信が開始されました。
9	RID「0」への MID 6 の配信に成功しました。
10	配信接続が終了しました。

テキスト メール ログ エントリの例

次の例で、さまざまなケースに基づくログ エントリを示します。

メッセージ受信

1 人の受信者に対するメッセージがアプライアンスにインジェクトされます。メッセージは正常に配信されます。

```
Wed Jun 16 21:42:34 2004 Info: New SMTP ICID 282204970 interface mail.example.com
(1.2.3.4) address 2.3.4.5 reverse dns host unknown verified no
Wed Jun 16 21:42:34 2004 Info: ICID 282204970 SBRS None
Wed Jun 16 21:42:35 2004 Info: Start MID 200257070 ICID 282204970
Wed Jun 16 21:42:35 2004 Info: MID 200257070 ICID 282204970 From: <someone@foo.com>
Wed Jun 16 21:42:36 2004 Info: MID 200257070 ICID 282204970 RID 0 To: <user@example.com>
Wed Jun 16 21:42:38 2004 Info: MID 200257070 Message-ID '<37gva9$5uvbhe@mail.example.com>'
Wed Jun 16 21:42:38 2004 Info: MID 200257070 Subject 'Hello'
Wed Jun 16 21:42:38 2004 Info: MID 200257070 ready 24663 bytes from <someone@foo.com>
Wed Jun 16 21:42:38 2004 Info: MID 200257070 antivirus negative
Wed Jun 16 21:42:38 2004 Info: MID 200257070 queued for delivery
Wed Jun 16 21:42:38 2004 Info: New SMTP DCID 2386069 interface 1.2.3.4 address 1.2.3.4
Wed Jun 16 21:42:38 2004 Info: Delivery start DCID 2386069 MID 200257070 to RID [0]
Wed Jun 16 21:42:38 2004 Info: ICID 282204970 close
Wed Jun 16 21:42:38 2004 Info: Message done DCID 2386069 MID 200257070 to RID [0]
[('X-SBRS', 'None')]
Wed Jun 16 21:42:38 2004 Info: MID 200257070 RID [0] Response 2.6.0
<37gva9$5uvbhe@mail.example.com> Queued mail for delivery
Wed Jun 16 21:42:43 2004 Info: DCID 2386069 close
```

正常なメッセージ配信の例

```
Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 5 interface 172.19.0.11 address
63.251.108.110
Mon Mar 31 20:10:58 2003 Info: Delivery start DCID 5 MID 4 to RID [0]
Mon Mar 31 20:10:58 2003 Info: Message done DCID 5 MID 4 to RID [0]
Mon Mar 31 20:11:03 2003 Info: DCID 5 close
```

失敗したメッセージ配信（ハード バウンス）

2 人の受信者が指定されたメッセージがアプライアンスにインジェクトされます。配信時に、宛先ホストが *5XX* エラーを返しました。これは、メッセージをどちらの受信者にも配信できなかったことを示します。アプライアンスは、送信者に通知して、キューからそれらの受信者を削除します。

```
Mon Mar 31 20:00:23 2003 Info: New SMTP DCID 3 interface 172.19.0.11 address 64.81.204.225
Mon Mar 31 20:00:23 2003 Info: Delivery start DCID 3 MID 4 to RID [0, 1]
Mon Mar 31 20:00:27 2003 Info: Bounced: DCID 3 MID 4 to RID 0 - 5.1.0 - Unknown address
error ('550', ['<george@yourdomain.com>... Relaying denied']) []
Mon Mar 31 20:00:27 2003 Info: Bounced: DCID 3 MID 4 to RID 1 - 5.1.0 - Unknown address
error ('550', ['<jane@yourdomain.com>... Relaying denied']) []
Mon Mar 31 20:00:32 2003 Info: DCID 3 close
```

最終的に正常に配信されるソフト バウンスの例

メッセージがアプライアンスにインジェクトされます。最初の配信試行で、メッセージはソフト バウンスして、その後の配信キューに入れられます。2 回めの試行でメッセージは正常に配信されます。

```
Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 5 interface 172.19.0.11 address
63.251.108.110
Mon Mar 31 20:00:23 2003 Info: Delivery start DCID 3 MID 4 to RID [0, 1]
Mon Mar 31 20:00:23 2003 Info: Delayed: DCID 5 MID 4 to RID 0 - 4.1.0 - Unknown address
error ('466', ['Mailbox temporarily full.'])[]
Mon Mar 31 20:00:23 2003 Info: Message 4 to RID [0] pending till Mon Mar 31 20:01:23 2003
```

```
Mon Mar 31 20:01:28 2003 Info: DCID 5 close
Mon Mar 31 20:01:28 2003 Info: New SMTP DCID 16 interface PublicNet address 172.17.0.113
Mon Mar 31 20:01:28 2003 Info: Delivery start DCID 16 MID 4 to RID [0]
Mon Mar 31 20:01:28 2003 Info: Message done DCID 16 MID 4 to RID [0]
Mon Mar 31 20:01:33 2003 Info: DCID 16 close
```

メッセージ スキャン結果（scanconfig）

次のプロンプトで、メッセージの構成要素を分解できない場合（添付ファイルを削除する場合）の動作を scanconfig コマンドを使用して決定した場合、

```
If a message could not be deconstructed into its component parts in order to remove
specified attachments, the system should:
1. Deliver
2. Bounce
3. Drop
[3]>
```

メール ログに以下が表示されます。

scanconfig で、メッセージを分解できない場合に配信するように設定した場合。

```
Tue Aug 3 16:36:29 2004 Info: MID 256 ICID 44784 From: <test@virus.org>
Tue Aug 3 16:36:29 2004 Info: MID 256 ICID 44784 RID 0 To: <joe@example.com>
Tue Aug 3 16:36:29 2004 Info: MID 256 Message-ID '<137398.@virus.org>'
Tue Aug 3 16:36:29 2004 Info: MID 256 Subject 'Virus Scanner Test #22'
Tue Aug 3 16:36:29 2004 Info: MID 256 ready 1627 bytes from <test@virus.org>
Tue Aug 3 16:36:29 2004 Warning: MID 256, Message Scanning Problem: Continuation line seen
before first header
Tue Aug 3 16:36:29 2004 Info: ICID 44784 close
Tue Aug 3 16:36:29 2004 Info: MID 256 antivirus positive 'EICAR-AV-Test'
Tue Aug 3 16:36:29 2004 Info: Message aborted MID 256 Dropped by antivirus
Tue Aug 3 16:36:29 2004 Info: Message finished MID 256 done
```

scanconfig で、メッセージを分解できない場合にドロップするように設定した場合。

```
Tue Aug 3 16:38:53 2004 Info: Start MID 257 ICID 44785
Tue Aug 3 16:38:53 2004 Info: MID 257 ICID 44785 From: test@virus.org
Tue Aug 3 16:38:53 2004 Info: MID 257 ICID 44785 RID 0 To: <joe@example.com>
Tue Aug 3 16:38:53 2004 Info: MID 257 Message-ID '<392912.@virus.org>'
Tue Aug 3 16:38:53 2004 Info: MID 25781 Subject 'Virus Scanner Test #22'
Tue Aug 3 16:38:53 2004 Info: MID 257 ready 1627 bytes from <test@virus.org>
Tue Aug 3 16:38:53 2004 Warning: MID 257, Message Scanning Problem: Continuation line seen
before first header
Tue Aug 3 16:38:53 2004 Info: Message aborted MID 25781 Dropped by filter 'drop_zip_c'
Tue Aug 3 16:38:53 2004 Info: Message finished MID 257 done
Tue Aug 3 16:38:53 2004 Info: ICID 44785 close
```

添付ファイルのあるメッセージ

この例では、添付ファイル名の識別をイネーブルにするように、条件「Message Body Contains」を含むコンテンツ フィルタが設定されています。

```
Sat Apr 23 05:05:42 2011 Info: New SMTP ICID 28 interface Management (192.0.2.10)
address 224.0.0.10 reverse dns host test.com verified yes
Sat Apr 23 05:05:42 2011 Info: ICID 28 ACCEPT SG UNKNOWNLIST match sbrs[-1.0:10.0]
SBRS 0.0
Sat Apr 23 05:05:42 2011 Info: Start MID 44 ICID 28
Sat Apr 23 05:05:42 2011 Info: MID 44 ICID 28 From: <sender1@example.com>
Sat Apr 23 05:05:42 2011 Info: MID 44 ICID 28 RID 0 To: <recipient1@example.org>
```

```
Sat Apr 23 05:05:42 2011 Info: MID 44 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>'
Sat Apr 23 05:05:42 2011 Info: MID 44 Subject 'Message 001'
Sat Apr 23 05:05:42 2011 Info: MID 44 ready 240129 bytes from <sender1@example.com>
Sat Apr 23 05:05:42 2011 Info: MID 44 matched all recipients for per-recipient
policy DEFAULT in the inbound table
Sat Apr 23 05:05:42 2011 Info: ICID 28 close
Sat Apr 23 05:05:42 2011 Info: MID 44 interim verdict using engine: CASE
spam negative
Sat Apr 23 05:05:42 2011 Info: MID 44 using engine: CASE spam negative
Sat Apr 23 05:05:43 2011 Info: MID 44 attachment 'Banner.gif'
Sat Apr 23 05:05:43 2011 Info: MID 44 attachment '=D1=82=D0=B5=D1=81=D1=82.rst'
Sat Apr 23 05:05:43 2011 Info: MID 44 attachment 'Test=20Attachment.docx'
Sat Apr 23 05:05:43 2011 Info: MID 44 queued for delivery
```

3 つの添付ファイルの 2 番目が Unicode であることに注意してください。Unicode を表示できない端末では、このような添付ファイルは quoted-printable 形式で表示されます。

生成またはリライトされたメッセージ

リライト/リダイレクト アクションなどの一部の機能（`alt-rcpt-to` フィルタ、アンチスパム RCPT リライト、`bcc()` アクション、アンチウイルス リダイレクションなど）によって、新しいメッセージが作成されます。ログに目を通して結果を確認し、必要に応じて MID や、場合によっては DCID を追加します。次のようなエントリが可能です。

```
Tue Jun  1 20:02:16 2004 Info: MID 14 generated based on MID 13 by bcc filter 'nonetest'
```

または

```
Tue Jan  6 15:03:18 2004 Info: MID 2 rewritten to 3 by antispam
Fri May 14 20:44:43 2004 Info: MID 6 rewritten to 7 by alt-rcpt-to-filter filter
'testfilt'
```

（注）　「Rewritten」エントリは、新しい MID の使用を示すログの行の後に表示されます。

Cisco IronPort スパム隔離へのメッセージの送信

メッセージを隔離領域に送信すると、メール ログでは、RPC 接続を識別する RPC 接続 ID（RCID）を使用して、隔離領域との間の移動が追跡されます。次のメール ログでは、メッセージにスパムのタグが付けられ、Cisco IronPort スパム隔離に送信されています。

```
Wed Feb 14 12:11:40 2007 Info: Start MID 2317877 ICID 15726925
Wed Feb 14 12:11:40 2007 Info: MID 2317877 ICID 15726925 From: <HLD@chasehf.bfi0.com>
Wed Feb 14 12:11:40 2007 Info: MID 2317877 ICID 15726925 RID 0 To:
<stevel@healthtrust.org>
Wed Feb 14 12:11:40 2007 Info: MID 2317877 Message-ID
'<W1TH05606E5811BEA0734309D4BAF0.323.14460.pimailer44.DumpShot.2@email.chase.com>'
Wed Feb 14 12:11:40 2007 Info: MID 2317877 Subject 'Envision your dream home - Now make it
a reality'
Wed Feb 14 12:11:40 2007 Info: MID 2317877 ready 15731 bytes from <HLD@chasehf.bfi0.com>
Wed Feb 14 12:11:40 2007 Info: MID 2317877 matched all recipients for per-recipient policy
DEFAULT in the inbound table
Wed Feb 14 12:11:41 2007 Info: MID 2317877 using engine: CASE spam suspect
Wed Feb 14 12:11:41 2007 Info: EUQ: Tagging MID 2317877 for quarantine
Wed Feb 14 12:11:41 2007 Info: MID 2317877 antivirus negative
Wed Feb 14 12:11:41 2007 Info: MID 2317877 queued for delivery
Wed Feb 14 12:11:44 2007 Info: RPC Delivery start RCID 756814 MID 2317877 to local Cisco
IronPort Spam Quarantine
```

```
Wed Feb 14 12:11:45 2007 Info: EUQ: Quarantined MID 2317877
Wed Feb 14 12:11:45 2007 Info: RPC Message done RCID 756814 MID 2317877
Wed Feb 14 12:11:45 2007 Info: Message finished MID 2317877 done
```

NTP ログの使用

表 15-14 に、NTP ログに記録される統計情報を示します。

表 15-14　NTP ログに記録される統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
メッセージ	メッセージは、サーバへの簡易ネットワーク タイム プロトコル（SNTP）クエリーまたは adjust: メッセージで構成されます。

NTP ログの例

次の NTP ログの例は、アプライアンスから NTP ホストへの 2 度のポーリングを示しています。

```
Thu Sep  9 07:36:39 2004 Info: sntp query host 10.1.1.23 delay 653 offset -652
Thu Sep  9 07:36:39 2004 Info: adjust: time_const: 8 offset: -652us next_poll: 4096
Thu Sep  9 08:44:59 2004 Info: sntp query host 10.1.1.23 delay 642 offset -1152
Thu Sep  9 08:44:59 2004 Info: adjust: time_const: 8 offset: -1152us next_poll: 4096
```

レポーティング ログの使用

表 15-15 に、レポーティング ログに記録される統計情報を示します。

表 15-15　レポーティング ログの統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
メッセージ	メッセージは、ユーザ認証など、実行されたアクションで構成されます。

レポーティング ログの例

次のレポーティング ログの例は、情報ログ レベルに設定されたアプライアンスを示しています。

```
Wed Oct  3 13:39:53 2007 Info: Period minute using 0 (KB)
Wed Oct  3 13:39:53 2007 Info: Period month using 1328 (KB)
Wed Oct  3 13:40:02 2007 Info: Update 2 registered appliance at 2007-10-03-13-40
Wed Oct  3 13:40:53 2007 Info: Pages found in cache: 1304596 (99%). Not found: 1692
Wed Oct  3 13:40:53 2007 Info: Period hour using 36800 (KB)
Wed Oct  3 13:40:53 2007 Info: Period day using 2768 (KB)
Wed Oct  3 13:40:53 2007 Info: Period minute using 0 (KB)
Wed Oct  3 13:40:53 2007 Info: Period month using 1328 (KB)
Wed Oct  3 13:40:53 2007 Info: HELPER checkpointed in 0.00580507753533 seconds
Wed Oct  3 13:41:02 2007 Info: Update 2 registered appliance at 2007-10-03-13-41
Wed Oct  3 13:41:53 2007 Info: Pages found in cache: 1304704 (99%). Not found: 1692
Wed Oct  3 13:41:53 2007 Info: Period hour using 36800 (KB)
Wed Oct  3 13:41:53 2007 Info: Period day using 2768 (KB)
Wed Oct  3 13:41:53 2007 Info: Period minute using 0 (KB)
Wed Oct  3 13:41:53 2007 Info: Period month using 1328 (KB)
```

```
Wed Oct  3 13:42:03 2007 Info: Update 2 registered appliance at 2007-10-03-13-42
```

レポーティング クエリー ログの使用

表 15-16 に、レポーティング クエリー ログに記録される統計情報を示します。

表 15-16　レポーティング クエリー ログの統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
メッセージ	メッセージは、ユーザ認証など、実行されたアクションで構成されます。

レポーティング クエリー ログの例

次のレポーティング クエリー ログの例は、アプライアンスによって、2007 年 8 月 29 日から 10 月 10 日までの期間で毎日の発信メール トラフィック クエリーが実行されていることを示しています。

```
Tue Oct  2 11:30:02 2007 Info: Query: Closing interval handle 811804479.
Tue Oct  2 11:30:02 2007 Info: Query: Closing interval handle 811804480.
Tue Oct  2 11:30:02 2007 Info: Query: Closing query handle 302610228.
Tue Oct  2 11:30:02 2007 Info: Query: Merge query with handle 302610229 for
['MAIL_OUTGOING_TRAFFIC_SUMMARY.
DETECTED_SPAM', 'MAIL_OUTGOING_TRAFFIC_SUMMARY.DETECTED_VIRUS',
'MAIL_OUTGOING_TRAFFIC_SUMMARY.THREAT_CONTEN
T_FILTER', 'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_CLEAN_RECIPIENTS',
'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_RECI
PIENTS_PROCESSED'] for rollup period "day" with interval range 2007-08-29 to 2007-10-01
with key constraints
 None sorting on ['MAIL_OUTGOING_TRAFFIC_SUMMARY.DETECTED_SPAM'] returning results from 0
to 2 sort_ascendin
g=False.
Tue Oct  2 11:30:02 2007 Info: Query: Closing query handle 302610229.
Tue Oct  2 11:30:02 2007 Info: Query: Merge query with handle 302610230 for
['MAIL_OUTGOING_TRAFFIC_SUMMARY.
TOTAL_HARD_BOUNCES', 'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_RECIPIENTS_DELIVERED',
'MAIL_OUTGOING_TRAFFIC_SUMM
ARY.TOTAL_RECIPIENTS'] for rollup period "day" with interval range 2007-08-29 to
2007-10-01 with key constra
ints None sorting on ['MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_HARD_BOUNCES'] returning
results from 0 to 2 sort
_ascending=False.
Tue Oct  2 11:30:02 2007 Info: Query: Closing query handle 302610230.
```

セーフリスト/ブロックリスト ログの使用

表 15-17 に、セーフリスト/ブロックリスト ログに記録される統計情報を示します。

表 15-17　セーフリスト/ブロックリスト ログの統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
メッセージ	メッセージは、ユーザ認証など、実行されたアクションで構成されます。

セーフリスト/ブロックリスト ログの例

次のセーフリスト/ブロックリスト ログの例は、アプライアンスによって 2 時間ごとにデータベースのスナップショットが作成されていることを示しています。送信者がデータベースに追加された時刻も表示されます。

```
Fri Sep 28 14:22:33 2007 Info: Begin Logfile Fri Sep 28 14:22:33 2007 Info: Version:
6.0.0-425 SN: XXXXXXXXXXX-XXX Fri Sep 28 14:22:33 2007 Info: Time offset from UTC: 10800
seconds Fri Sep 28 14:22:33 2007 Info: System is coming up.
Fri Sep 28 14:22:33 2007 Info: SLBL: The database snapshot has been created.
Fri Sep 28 16:22:34 2007 Info: SLBL: The database snapshot has been created.
Fri Sep 28 18:22:34 2007 Info: SLBL: The database snapshot has been created.
Fri Sep 28 20:22:34 2007 Info: SLBL: The database snapshot has been created.
Fri Sep 28 22:22:35 2007 Info: SLBL: The database snapshot has been created.
.........................
Mon Oct  1 14:16:09 2007 Info: SLBL: The database snapshot has been created.
Mon Oct  1 14:37:39 2007 Info: SLBL: The database snapshot has been created.
Mon Oct  1 15:31:37 2007 Warning: SLBL: Adding senders to the database failed.
Mon Oct  1 15:32:31 2007 Warning: SLBL: Adding senders to the database failed.
Mon Oct  1 16:37:40 2007 Info: SLBL: The database snapshot has been created.
```

SMA ログの使用

表 15-18 に、SMA ログに記録される統計情報を示します。

表 15-18　SMA ログの統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
メッセージ	メッセージは、ユーザ認証など、実行されたアクションで構成されます。

次の SMA ログの例は、電子メール セキュリティ アプライアンスからトラッキング ファイルをダウンロードする中央集中型トラッキング サービスと、電子メール セキュリティ アプライアンスからレポーティング ファイルをダウンロードする中央集中型レポーティング サービスを示しています。

```
Wed Oct  3 13:26:39 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from
172.29.0.17 - /export/tracki
ng/tracking.@20071003T202244Z_20071003T202544Z.s
Wed Oct  3 13:28:11 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from
172.29.0.15 - /export/tracki
ng/tracking.@20071003T202443Z_20071003T202743Z.s
Wed Oct  3 13:28:46 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from
172.29.0.17 - /export/tracki
ng/tracking.@20071003T202544Z_20071003T202844Z.s
Wed Oct  3 13:31:27 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from
172.29.0.15 - /export/tracki
ng/tracking.@20071003T202743Z_20071003T203043Z.s
Wed Oct  3 13:31:28 2007 Info: TRANSFER: Plugin REPORTINGPLUGIN downloading from
172.29.0.15 - /reporting/ou
tgoing_queue/rpx.2007-10-03-20-15Z.000F1F6ECA7C-2RWDB51.v1.tgz
Wed Oct  3 13:31:53 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from
172.29.0.17 - /export/tracki
ng/tracking.@20071003T202844Z_20071003T203144Z.s
Wed Oct  3 13:32:31 2007 Info: TRANSFER: Plugin REPORTINGPLUGIN downloading from
172.29.0.17 - /reporting/ou
tgoing_queue/rpx.2007-10-03-20-15Z.0019B9B316E4-JZ41PC1.v1.tgz
Wed Oct  3 13:34:40 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from
172.29.0.15 - /export/tracki
```

```
ng/tracking.@20071003T203043Z_20071003T203343Z.s
```

ステータス ログの使用

ステータス ログには、status、status detail、および dnsstatus を含む CLI ステータス コマンドで検出されたシステム統計情報が記録されます。記録期間は、logconfig の setup サブコマンドを使用して設定します。ステータス ログでレポートされるカウンタまたはレートは、前回カウンタがリセットされた時点からの値です。

ステータス ログの読み取り

表 15-19 に、ステータス ログ ラベル、およびそれと一致するシステム統計情報を示します。

表 15-19　ステータス ログの統計情報

統計	説明
CPULd	CPU 使用率。
DskIO	ディスク I/O 使用率。
RAMUtil	RAM 使用率。
QKUsd	使用されているキュー（キロバイト単位）。
QKFre	空いているキュー（キロバイト単位）。
CrtMID	メッセージ ID（MID）。
CrtICID	インジェクション接続 ID（ICID）。
CRTDCID	配信接続 ID（DCID）。
InjMsg	インジェクトされたメッセージ。
InjRcp	インジェクトされた受信者。
GenBncRcp	生成されたバウンス受信者。
RejRcp	拒否された受信者。
DrpMsg	ドロップされたメッセージ。
SftBncEvnt	ソフト バウンスされたイベント。
CmpRcp	完了した受信者。
HrdBncRcp	ハード バウンスされた受信者。
DnsHrdBnc	DNS ハード バウンス。
5XXHrdBnc	5XX ハード バウンス。
FltrHrdBnc	フィルタ ハード バウンス。
ExpHrdBnc	期限切れハード バウンス。
OtrHrdBnc	その他のハード バウンス。
DlvRcp	配信された受信者。
DelRcp	削除された受信者。
GlbUnsbHt	グローバル配信停止リストとの一致数。
ActvRcp	アクティブ受信者。
UnatmptRcp	未試行受信者。
AtmptRcp	試行受信者。

表 15-19　ステータス ログの統計情報 （続き）

統計	説明
CrtCncIn	現在の着信接続。
CrtCncOut	現在の発信接続。
DnsReq	DNS 要求。
NetReq	ネットワーク要求。
CchHit	キャッシュ ヒット。
CchMis	キャッシュ ミス。
CchEct	キャッシュ例外。
CchExp	キャッシュ期限切れ。
CPUTTm	アプリケーションが使用した合計 CPU 時間。
CPUETm	アプリケーションが開始されてからの経過時間。
MaxIO	メール プロセスに対する 1 秒あたりの最大ディスク I/O 動作。
RamUsd	割り当て済みのメモリ（バイト単位）。
SwIn	スワップインされたメモリ
SwOut	スワップアウトされたメモリ
SwPgIn	ページインされたメモリ
SwPgOut	ページアウトされたメモリ
MMLen	システム内の合計メッセージ数。
DstInMem	メモリ内の宛先オブジェクト数。
ResCon	リソース保持の tarpit 値 （大量のシステム負荷により、着信メールの受け入れがこの秒数だけ遅延します）。
WorkQ	作業キューにある現在のメッセージ数。
QuarMsgs	システム隔離にある個々のメッセージ数（複数の隔離領域に存在するメッセージは一度だけカウントされます）。
QuarQKUsd	システム隔離メッセージによって使用されたキロバイト数。
LogUsd	使用されたログ パーティションの割合。
CASELd	CASE スキャンで使用された CPU の割合。
TotalLd	CPU の合計消費量。
LogAvail	ログ ファイルに使用できるディスク領域の大きさ。
EuQ	Cisco IronPort スパム隔離内のメッセージ数。
EuqRls	Cisco IronPort スパム隔離解放キュー内のメッセージ数。

ステータス ログの例

```
Fri Feb 24 15:14:39 2006 Info: Status: CPULd 0 DskIO 0 RAMUtil 2 QKUsd 0 QKFre 8388608
CrtMID 19036 CrtICID 35284 CrtDCID 4861 InjMsg 13889 InjRcp 14230 GenBncRcp 12 RejRcp 6318
DrpMsg 7437 SftBncEvnt 1816 CmpRcp 6813 HrdBncRcp 18 DnsHrdBnc 2 5XXHrdBnc 15 FltrHrdBnc 0
ExpHrdBnc 1 OtrHrdBnc 0 DlvRcp 6793 DelRcp 2 GlbUnsbHt 0 ActvRcp 0 UnatmptRcp 0 AtmptRcp 0
CrtCncIn 0 CrtCncOut 0 DnsReq 143736 NetReq 224227 CchHit 469058 CchMis 504791 CchEct
```

```
15395 CchExp 55085 CPUTTm 228 CPUETm 181380 MaxIO 350 RAMUsd 21528056 MMLen 0 DstInMem 4
ResCon 0 WorkQ 0 QuarMsgs 0 QuarQKUsd 0 LogUsd 3 AVLd 0 BMLd 0 CASELd 3 TotalLd 3 LogAvail
17G EuQ 0 EuqRls 0
```

システム ログの使用

表 15-20 に、システム ログに記録される統計情報を示します。

表 15-20　システム ログの統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
メッセージ	ログに記録されたイベント。

システム ログの例

次のシステム ログの例は、commit を実行したユーザの名前と入力されたコメントを含む、いくつかの commit エントリを示しています。

```
Wed Sep  8 18:02:45 2004 Info: Version: 6.0.0-206 SN: XXXXXXXXXXXX-XXX
Wed Sep  8 18:02:45 2004 Info: Time offset from UTC: 0 seconds
Wed Sep  8 18:02:45 2004 Info: System is coming up
Wed Sep  8 18:02:49 2004 Info: bootstrapping DNS cache
Wed Sep  8 18:02:49 2004 Info: DNS cache bootstrapped
Wed Sep  8 18:13:30 2004 Info: PID 608: User admin commit changes: SSW:Password
Wed Sep  8 18:17:23 2004 Info: PID 608: User admin commit changes: Completed Web::SSW
Thu Sep  9 08:49:27 2004 Info: Time offset from UTC: -25200 seconds
Thu Sep  9 08:49:27 2004 Info: PID 1237: User admin commit changes: Added a second CLI log
for examples
Thu Sep  9 08:51:53 2004 Info: PID 1237: User admin commit changes: Removed example CLI
log.
```

トラッキング ログについて

トラッキング ログには、AsyncOS の電子メール動作に関する情報が記録されます。ログ メッセージは、メール ログに記録されたメッセージのサブセットです。

トラッキング ログは、メッセージ トラッキング データベースを作成するため、メッセージ トラッキング コンポーネントで使用されます。ログ ファイルはデータベースの作成プロセスで消費されるので、トラッキング ログは一過性のものになります。トラッキング ログの情報は、人による読み取りや解析を目的とした設計になっていません。

トラッキング ログは、リソースの効率性を保つためにバイナリ形式で記録され、転送されます。情報は、論理的にレイアウトされ、シスコが提供するユーティリティを使用して変換した後は人による読み取りが可能になります。変換ツールは、次の URL にあります。

`http://tinyurl.com/3c5l8r`

ログ サブスクリプション

- 「ログ サブスクリプションの設定」（P.15-22）
- 「GUI でのログ サブスクリプションの作成」（P.15-23）

- 「ロギングに対するグローバル設定」（P.15-24）
- 「ログ サブスクリプションのロールオーバー」（P.15-26）
- 「ホスト キーの設定」（P.15-28）

ログ サブスクリプションの設定

ログ サブスクリプションによって、シスコ コンテンツ セキュリティ アプライアンスに、またはリモートに保存される個々のログ ファイルが作成されます。ログ サブスクリプションは、プッシュ（別のコンピュータに配信）またはプル（アプライアンスから取得）されます。一般に、ログ サブスクリプションには次の属性があります。

表 15-21　ログ ファイルの属性

属性	説明
Log Type	記録される情報のタイプと、ログ サブスクリプションの形式を定義します。詳細については、「ログ タイプの概要」（P.15-4）を参照してください。
Name	後で参照するための、ログ サブスクリプションのわかりやすい名前。
Log Filename	ディスクに書き込むときのファイルの物理名。システムに複数のコンテンツ セキュリティ アプライアンスがある場合、ログ ファイルを生成したアプライアンスを識別できる一意のログ ファイル名を使用します。
Rollover by File Size	ファイルの最大サイズ。このサイズに到達すると、ロールオーバーされます。
Rollover by Time	時間に基づいてログ ファイルをロールオーバーするタイミング。「ログのロールオーバーおよび転送スケジュール」（P.15-2）のオプションを参照してください。
Log Level	各ログ サブスクリプションの詳細レベル。
Retrieval Method	ログ ファイルをアプライアンスから転送するときに使用する方式。

[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ログ設定（Log Subscriptions）] ページ（または CLI の `logconfig` コマンド）を使用して、ログ サブスクリプションを設定します。ログ タイプを入力するプロンプトが表示されます（「ログ タイプの概要」（P.15-4）を参照）。ほとんどのログ タイプで、ログ サブスクリプションの *ログ レベル*の入力も要求されます。

（注） コンフィギュレーション履歴ログのみ：コンフィギュレーション履歴ログからコンフィギュレーションをロードする可能性がある場合は、コンフィギュレーションにマスクされたパスワードが含まれているとロードできないことに注意してください。[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ログ設定（Log Subscriptions）] ページで、パスワードをログに含めるかどうかを尋ねるプロンプトが表示されたら、[はい（Yes）] を選択します。CLI の `logconfig` コマンドを使用する場合は、プロンプトで `y` を入力します。

ログ レベルの設定

ログ レベルによって、ログに送信される情報量が決定します。ログには、5 つの詳細レベルのいずれかを設定できます。詳細なログ レベルを設定すると、省略されたログ レベルを設定した場合と比べて、大きなログ ファイルが作成され、システム パフォーマンスに大きな影響を与えます。詳細なログ レベル設定には、省略されたログ レベル設定に含まれるすべてのメッセージと、追加のメッセージが含まれます。詳細レベルを上げるほど、システムのパフォーマンスは低下します。

（注）　ログ タイプごとに異なるログ レベルを指定できます。

表 15-22　ログ レベル

ログ レベル	説明
Critical	エラーだけがログに記録されます。最も省略されたログ レベル設定です。このログ レベルでは、パフォーマンスおよび重要なアプライアンスのアクティビティをモニタすることはできません。ただし、詳細ログ レベルのように、ログ ファイルがすぐに最大サイズに達することはありません。このログ レベルは、syslog レベル Alert と同等です。
Warning	すべてのシステム エラーと警告が記録されます。このログ レベルでは、パフォーマンスおよび重要なアプライアンスのアクティビティをモニタすることはできません。Critical ログ レベルよりは早く、ログ ファイルが最大サイズに達します。このログ レベルは、syslog レベル Warning と同等です。
Information	システムの動作が逐次記録されます。たとえば、接続のオープンや配信試行が記録されます。Information レベルは、ログに推奨される設定です。このログ レベルは、syslog レベル Info と同等です。
Debug	Information ログ レベルよりも詳細な情報が記録されます。エラーをトラブルシューティングするときは、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。
Trace	使用可能なすべての情報が記録されます。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。

GUI でのログ サブスクリプションの作成

手順

ステップ 1　[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ログ設定（Log Subscriptions）] ページで、[ログ設定を追加（Add Log Subscription）] をクリックします。

ステップ 2　ログ タイプを選択し、ログ名（ログ ディレクトリ用）とログ ファイル自体の名前を入力します。

ステップ 3　該当する場合は、最大ファイル サイズを指定します。

ステップ 4　該当する場合は、ログをロールオーバーする日、時刻、または時間間隔を指定します。詳細については、「ログのロールオーバーおよび転送スケジュール」（P.15-2）を参照してください。

ステップ 5　該当する場合は、ログ レベルを指定します。

ステップ 6　（コンフィギュレーション履歴ログのみ）パスワードをログに含めるかどうかを選択します。

（注）　マスクされたパスワードが含まれているコンフィギュレーションはロードできません。コンフィギュレーション履歴ログからコンフィギュレーションをロードする可能性がある場合は、[はい（Yes）] を選択してパスワードをログに含めます。

ステップ 7　ログの取得方法を設定します。

ステップ 8　変更を送信し、保存します。

ログ サブスクリプションの編集

手順

ステップ 1　[ログ設定（Log Subscriptions）] ページの [ログ名（Log Name）] カラムにあるログ名をクリックします。

ステップ 2　ログ サブスクリプションを更新します。

ステップ 3　変更を送信し、保存します。

ロギングに対するグローバル設定

システムは、テキスト メール ログおよびステータス ログ内にシステム メトリックを定期的に記録します。[ログ設定（Log Subscriptions）] ページの [グローバル設定（Global Settings）] セクションにある [設定を編集（Edit Settings）] ボタン（または、CLI の `logconfig -> setup` コマンド）を使用して、次の情報を設定します。

- システムが測定を記録するまで待機する時間（秒単位）
- メッセージ ID ヘッダーを記録するかどうか
- リモート応答ステータス コードを記録するかどうか
- 元のメッセージのサブジェクト ヘッダーを記録するかどうか
- メッセージごとにログに記録するヘッダー

すべてシスコ コンテンツ セキュリティ アプライアンスのログには、次の 3 項目を任意で記録できます。

- [メッセージ ID（Message-ID）] : このオプションを設定すると、可能な場合はすべてのメッセージのメッセージ ID ヘッダーがログに記録されます。このメッセージ ID は、受信したメッセージから取得される場合と、AsyncOS で生成される場合があります。次に例を示します。

  ```
  Tue Apr 6 14:38:34 2004 Info: MID 1 Message-ID Message-ID-Content
  ```

- [リモート応答（Remote Response）] : このオプションを設定すると、可能な場合はすべてのメッセージのリモート応答ステータス コードがログに記録されます。次に例を示します。

  ```
  Tue Apr 6 14:38:34 2004 Info: MID 1 RID [0] Response 'queued as 9C8B425DA7'
  ```

  リモート応答文字列は、SMTP 会話配信時の DATA コマンドへの応答後に受信される、人が読み取ることのできるテキストです。この例では、接続ホストが data コマンドを実行した後のリモート応答が、「queued as 9C8B425DA7」となります。

  ```
  [...]
  250 ok hostname
  250 Ok: queued as 9C8B425DA7
  ```

文字列の先頭にある空白や句読点、および 250 応答の OK 文字は除去されます。文字列の末尾については、空白だけが除去されます。たとえば、シスコ コンテンツ セキュリティ アプライアンスはデフォルトで、DATA コマンドに対して「250 Ok: Message MID accepted」という文字列で応答します。したがって、リモート ホストが別のシスコ コンテンツ セキュリティ アプライアンスである場合は、エントリ「Message MID accepted」がログに記録されます。

- [オリジナルの件名（Original Subject Header）]：このオプションをイネーブルにすると、各メッセージの元のサブジェクト ヘッダーがログに記録されます。

```
Tue May 31 09:20:27 2005 Info: Start MID 2 ICID 2
Tue May 31 09:20:27 2005 Info: MID 2 ICID 2 From: <mary@example.com>
Tue May 31 09:20:27 2005 Info: MID 2 ICID 2 RID 0 To: <joe@example.com>
Tue May 31 09:20:27 2005 Info: MID 2 Message-ID '<44e4n$2@example.com>'
Tue May 31 09:20:27 2005 Info: MID 2 Subject 'Monthly Reports Due'
```

メッセージ ヘッダーのロギング

場合によっては、メッセージがシステムを通過するときに、メッセージのヘッダーの存在と内容を記録する必要があります。[ログ設定のグローバル設定（Log Subscriptions Global Settings）] ページ（または、CLI の logconfig -> logheaders サブコマンド）で、記録するヘッダーを指定します。アプライアンスは、指定されたメッセージ ヘッダーをテキスト メール ログおよびトラッキング ログに記録します。ヘッダーが存在する場合、システムはヘッダーの名前と値を記録します。ヘッダーが存在しない場合は、ログに何も記録されません。

（注） システムは、ロギングに指定したヘッダーに関係なく、メッセージの記録処理中に随時、メッセージに存在するすべてのヘッダーを評価します。

（注） SMTP プロトコルについての RFC は、http://www.faqs.org/rfcs/rfc2821.html にあります。この RFC には、ユーザ定義のヘッダーが規定されています。

（注） logheaders コマンドを使用してヘッダーをログに記録するように設定している場合、ヘッダー情報は配信情報の後に表示されます。

表 15-23　ログ ヘッダー

ヘッダー名	ヘッダーの名前
値	ログに記録されるヘッダーの内容

たとえば、ログに記録するヘッダーとして「date, x-subject」を指定すると、メール ログに次の行が表示されます。

```
Tue May 31 10:14:12 2005 Info: Message done DCID 0 MID 3 to RID [0] [('date', 'Tue, 31 May
2005 10:13:18 -0700'), ('x-subject', 'Logging this header')]
```

GUI を使用したロギングのグローバル設定

手順

ステップ 1　[ログ設定（Log Subscriptions）] ページの [グローバル設定（Global Settings）] セクションにある [設定を編集（Edit Settings）] ボタンをクリックします。

ステップ 2　システム メトリクスの頻度、メール ログにメッセージ ID ヘッダーを加えるかどうか、リモート応答を加えるかどうか、および各メッセージの元のサブジェクト ヘッダーを加えるかどうかを指定します。

これらの設定の詳細については、「ロギングに対するグローバル設定」（P.15-24）を参照してください。

ステップ 3　ログに加えるその他のヘッダーを入力します。各エントリはカンマで区切ります。

ステップ 4　変更を送信し、保存します。

ログ サブスクリプションのロールオーバー

AsyncOS がログ ファイルをロールオーバーすると、次のことが行われます。

- ロールオーバーのタイムスタンプで新規のログ ファイルが作成され、文字「`c`」の拡張子によって現在のファイルとして指示されます。
- 現在のログ ファイルが、保存済みを示す文字「`s`」の拡張子付きに名前変更されます。
- 新たに保存されたログ ファイルがリモート ホストに転送されます（プッシュ ベースの場合）。
- 同じサブスクリプションから以前に失敗したログ ファイルが転送されます（プッシュ ベースの場合）。
- 保持するファイルの合計数を超えた場合は、ログ サブスクリプション内の最も古いファイルが削除されます（ポーリング ベースの場合）。

ログ サブスクリプション内のログのロールオーバー

「ログのロールオーバーおよび転送スケジュール」（P.15-2）を参照してください。

GUI を使用したログの即時ロールオーバー

手順

ステップ 1　[ログ設定（Log Subscriptions）] ページで、ロールオーバーするログの右側のチェックボックスをオンにします。

ステップ 2　[すべて（All）] チェックボックスをオンにして、すべてのログをロールオーバー対象として選択することもできます。

ステップ 3　[今すぐロールオーバー（Rollover Now）] ボタンをクリックします。

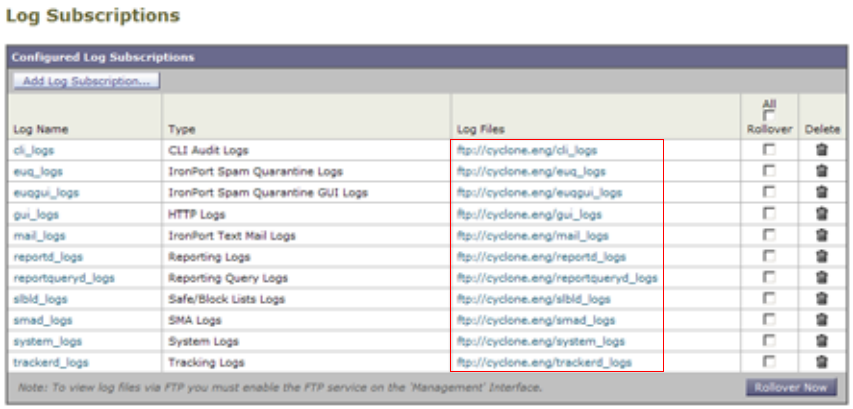
CLI を介したログの即時ロールオーバー

rollovernow コマンドを使用して、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 ファイルを選択します。

グラフィカル ユーザ インターフェイスでの最近のログ エントリの表示

GUI を介してログ ファイルを表示するには、[ログ設定（Log Subscriptions）] ページのテーブルの [ログ ファイル（Log Files）] カラムにあるログ サブスクリプションをクリックします。ログ サブスクリプションへのリンクをクリックすると、パスワードを入力するプロンプトが表示されます。次に、そのサブスクリプションのログ ファイルのリストが表示されます。いずれかのログ ファイルをクリックして、ブラウザに表示したり、ディスクに保存したりすることができます。グラフィカル ユーザ インターフェイスを介してログを表示するには、管理インターフェイスで FTP サービスをイネーブルにしておく必要があります。

図 15-1　　グラフィカル ユーザ インターフェイスでのログ ファイルの表示



最新のログ エントリの表示（tail コマンド）

AsyncOS では、アプライアンスに設定されたログの最新エントリを表示する tail コマンドをサポートしています。tail コマンドを実行し、現在設定されているログのうち、表示するログの番号を選択します。Ctrl を押した状態で C を押して、tail コマンドを終了します。

（注）　コンフィギュレーション履歴ログは、tail コマンドを使用して表示することができません。FTP または SCP を使用する必要があります。

例

次に、tail コマンドを使用してシステム ログを表示する例を示します tail コマンドは、次の例のように、表示するログの名前をパラメータとして指定することもできます。

```
tail system_logs

Welcome to the Cisco IronPort M600 Messaging Gateway(tm) Appliance
example.srv> tail

Currently configured logs:
```

```
1. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
2. "euq_logs" Type: "Cisco IronPort Spam Quarantine Logs" Retrieval: FTP Poll
3. "euqgui_logs" Type: "Cisco IronPort Spam Quarantine GUI Logs" Retrieval: FTP Poll
4. "gui_logs" Type: "HTTP Logs" Retrieval: FTP Poll
5. "mail_logs" Type: "Cisco IronPort Text Mail Logs" Retrieval: FTP Poll
6. "reportd_logs" Type: "Reporting Logs" Retrieval: FTP Poll
7. "reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: FTP Poll
8. "slbld_logs" Type: "Safe/Block Lists Logs" Retrieval: FTP Poll
9. "smad_logs" Type: "SMA Logs" Retrieval: FTP Poll
10. "system_logs" Type: "System Logs" Retrieval: FTP Poll
11. "trackerd_logs" Type: "Tracking Logs" Retrieval: FTP Poll
Enter the number of the log you wish to tail.
[]> 10

Press Ctrl-C to stop.
Thu Sep 27 00:18:56 2007 Info: Begin Logfile
Thu Sep 27 00:18:56 2007 Info: Version: 6.0.0-422 SN: 001143583D73-FT9GP61
Thu Sep 27 00:18:56 2007 Info: Time offset from UTC: 0 seconds
Thu Sep 27 00:18:47 2007 Info: System is coming up.
Thu Sep 27 00:23:05 2007 Warning: DNS query network error '[Errno 64] Host is down' to
'172.16.0.3' looking up 'downloads.cisco.com'
Fri Sep 28 22:20:08 2007 Info: PID 688: User admin commit changes:
Fri Sep 28 23:06:15 2007 Info: PID 688: User admin commit changes:
^Cexample.srv>
.
```

ホスト キーの設定

`logconfig -> hostkeyconfig` サブ コマンドを使用して、シスコ コンテンツ セキュリティ アプライアンスから他のサーバにログをプッシュするときに、SSH で使用するホスト キーを管理します。SSH サーバには、秘密キーと公開キーの 2 つのホスト キーが必要です。秘密ホスト キーは SSH サーバにあり、リモート マシンから読み取ることはできません。公開ホスト キーは、SSH サーバと対話する必要のある任意のクライアント マシンに配信されます。

（注） ユーザ キーを管理するには、お使いの電子メール セキュリティ アプライアンスのユーザ ガイドまたはオンライン ヘルプの「Managing Secure Shell (SSH) Keys」を参照してください。

`hostkeyconfig` サブコマンドによって、次の機能が実行されます。

表 15-24　ホスト キーの管理：サブコマンドのリスト

コマンド	説明
New	新しいキーを追加します。
Edit	既存のキーを変更します。
Delete	既存のキーを削除します。
Scan	ホスト キーを自動的にダウンロードします。
Print	キーを表示します。
Host	システム ホスト キーを表示します。これは、リモート システムの「known_hosts」ファイルに配置される値です。
Fingerprint	システム ホスト キーのフィンガープリントを表示します。
User	リモート マシンにログをプッシュするシステム アカウントの公開キーを表示します。これは、SCP プッシュ サブスクリプションを設定するときに表示されるキーと同じです。これは、リモート システムの「authorized_keys」ファイルに配置される値です。

次の例では、コマンドによってホスト キーがスキャンされ、ホストに追加されます。

```
mail3.example.com> logconfig

Currently configured logs:
[ list of logs ]

Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
[]> hostkeyconfig

Currently installed host keys:
1. mail3.example.com ssh-dss [ key displayed ]

Choose the operation you want to perform:
- NEW - Add a new key.
- EDIT - Modify a key.
- DELETE - Remove a key.
- SCAN - Automatically download a host key.
- PRINT - Display a key.
- HOST - Display system host keys.
- FINGERPRINT - Display system host key fingerprints.
- USER - Display system user keys.
[]> scan

Please enter the host or IP address to lookup.
[]> mail3.example.com

Choose the ssh protocol type:
1. SSH2:rsa
2. SSH2:dsa
3. All
[3]>

SSH2:dsa
mail3.example.com ssh-dss
[ key displayed ]

SSH2:rsa
mail3.example.com ssh-rsa
[ key displayed ]


Add the preceding host key(s) for mail3.example.com? [Y]>

Currently installed host keys:
1. mail3.example.com ssh-dss [ key displayed ]
2. mail3.example.com ssh-rsa [ key displayed ]
3. mail3.example.com 1024 35 [ key displayed ]

Choose the operation you want to perform:
- NEW - Add a new key.
- EDIT - Modify a key.
- DELETE - Remove a key.
- SCAN - Automatically download a host key.
- PRINT - Display a key.
- HOST - Display system host keys.
- FINGERPRINT - Display system host key fingerprints.
- USER - Display system user keys.
```

```
[]>

Currently configured logs:
[ list of configured logs ]

Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
[]>

mail3.example.com> commit
```

CHAPTER 16

トラブルシューティング

システム情報の収集

シリアル番号などのアプライアンスとそのステータスに関する情報を取得する方法は、第 10 章「システム ステータスのモニタリング」に説明します。

テクニカル サポートの使用方法

アプライアンスからのサポート ケースのオープンおよび更新

はじめる前に

（注） 問題が緊急な場合は、この方法は使用しないでください。代わりに、「シスコのテクニカル サポート」（P.1-6）に一覧表示されている他の方法の 1 つを使ってサポートに連絡してください。

- この項の手順は、情報要求など、または回避策が見つかった問題だが代替ソリューションを知りたい場合に使用してください。
- ヘルプを得るために以下の他のオプションを検討してください。
  - 「ナレッジ ベース」（P.1-5）
  - 「シスコ サポート コミュニティ」（P.1-6）
- この手順を使用して、サポート ケースを開くと、アプライアンスの設定ファイルがシスコのカスタマー サポートに送信されます。アプライアンスの設定を送信しない場合、ほかの方式を使用して、カスタマー サポートにお問い合わせください。

- アプライアンスはインターネットに接続しているはずですので、電子メールを送信できます。
- 既存のケースに関する情報を送信する場合は、ケース番号を使用してください。

手順

ステップ 1　アプライアンスにログインします。

ステップ 2　[ヘルプとサポート（Help and Support）] > [テクニカルサポートに問い合わせる（Contact Technical Support）] を選択します。

ステップ 3　サポート リクエストの受信者を次のように設定します。

要求をシスコのカスタマー サポートに送信する	[Cisco IronPort カスタマーサポート（Cisco IronPort Customer Support）] チェックボックスを選択します。
要求を内部サポート デスクにのみ送信する	• [Cisco IronPort カスタマーサポート（Cisco IronPort Customer Support）] チェックボックスを選択解除します。 • サポート デスクの電子メール アドレスを入力します。
（任意）他の受信者を追加する	電子メール アドレスを入力します。

ステップ 4　フォームに入力します。

ステップ 5　[送信（Send）] をクリックします。

シスコのテクニカル サポート担当者へのリモート アクセスのイネーブル化

シスコのカスタマー サポートだけが、次の方法を使用してアプライアンスにアクセスできます。

- 「インターネット接続を備えたアプライアンスへのリモート アクセスの有効化」（P.16-2）
- 「インターネットの直接接続のないアプライアンスへのリモート アクセスの有効化」（P.16-3）
- 「テクニカル サポートのトンネルの無効化」（P.16-4）
- 「リモート アクセスの無効化」（P.16-4）
- 「サポートの接続ステータスの確認」（P.16-4）

インターネット接続を備えたアプライアンスへのリモート アクセスの有効化

サポートは、この手順でアプライアンスと `upgrades.ironport.com` のサーバ間で作成される SSH トンネル経由でアプライアンスにアクセスします。

はじめる前に

インターネットから到達可能なポートを識別します。デフォルトは、ほとんどの環境で機能するポート 25 です。このポート経由の接続は、ほとんどのファイアウォール設定で許可されます。

手順

ステップ 1　アプライアンスへのログイン

ステップ 2　GUI ウィンドウの右上で、[ヘルプとサポート（Help and Support）] > [リモート アクセス（Remote Access）] を選択します。

ステップ 3　[有効（Enable）] をクリックします。

ステップ 4　情報を入力します。

オプション	説明
カスタマー サポート パスワード	この仮パスワードとアプライアンスのシリアル番号（物理アプライアンスの場合）または VLAN（仮想アプライアンスの場合）はサポート アクセスのパスワードを生成するために使用されます。
セキュア トンネル	リモート アクセス接続にセキュア トンネルを使用する場合に、このチェックボックスを選択します。 接続用のポートを入力します。 デフォルトは、ほとんどの環境で機能するポート 25 です。

ステップ 5　[送信（Submit）] をクリックします。

次の作業

サポート担当者へのリモート アクセスが必要なくなったときは、「テクニカル サポートのトンネルの無効化」（P.16-4）を参照してください。

インターネットの直接接続のないアプライアンスへのリモート アクセスの有効化

インターネットに直接接続のないアプライアンスの場合、アクセスは、インターネットに接続されている 2 番目のアプライアンスを介して行われます。

はじめる前に

- アプライアンスは、インターネットに接続されている 2 番目のアプライアンスにポート 22 で接続できる必要があります。
- インターネット接続が設定されたアプライアンスで、「インターネット接続を備えたアプライアンスへのリモート アクセスの有効化」（P.16-2）の手順に従ってそのアプライアンスへのサポート トンネルを作成します。

手順

ステップ 1　サポートが必要なアプライアンスのコマンドライン インターフェイスから、`techsupport` コマンドを入力します。

ステップ 2　`sshaccess` を入力します。

ステップ 3　プロンプトに従ってください。

次の作業

サポート担当者へのリモート アクセスが必要なくなったときは、次のを参照してください。

- 「リモート アクセスの無効化」（P.16-4）
- 「テクニカル サポートのトンネルの無効化」（P.16-4）

テクニカル サポートのトンネルの無効化

有効な techsupport トンネルは、7 日間は upgrades.ironport.com に接続したままです。その後は、確立された接続は切断されませんが、いったん切断されたトンネルを再度開通することはできません。

手順

ステップ 1　アプライアンスへのログイン

ステップ 2　GUI ウィンドウの右上で、[ヘルプとサポート（Help and Support（Help and Support）] > [リモート アクセス（Remote Access）] を選択します。

ステップ 3　[無効（Disable）] をクリックします。

リモート アクセスの無効化

techsupport コマンドを使用して作成したリモート アクセス アカウントは非アクティブ化されるまでアクティブのままです。

手順

ステップ 1　コマンドライン インターフェイスから、techsupport コマンドを入力します。

ステップ 2　sshaccess を入力します。

ステップ 3　disable を入力します。

サポートの接続ステータスの確認

手順

ステップ 1　コマンドライン インターフェイスから、techsupport コマンドを入力します。

ステップ 2　status を入力してください。

パケット キャプチャの実行

パケット キャプチャはサポート担当者がアプライアンスから出入りする TCP/IP データおよびその他のパケットを確認できるようにします。これによって、サポートはネットワーク設定をデバッグでき、どのネットワーク トラフィックがアプライアンスに届きアプライアンスから出て行くのかを検出できます。

手順

ステップ 1　[ヘルプとサポート（Help and Support（Help and Support）] > [パケット キャプチャ（Packet Capture）] を選択します。

ステップ 2　次の手順で、パケット キャプチャ設定を指定します。

a. [パケットキャプチャ設定（Packet Capture Settings）] セクションで、[設定を編集（Edit Settings）] をクリックします。

b. （任意）パケット キャプチャの期間、制限、およびフィルタを入力します。

サポートは、これらの設定の基準を示すことがあります。

時間の単位を指定せずにキャプチャの期間を入力すると、AsyncOS ではデフォルトで秒が使用されます。

[フィルタ（Filters）] セクションは、次のようになります。

- カスタム フィルタでは UNIX の `tcpdump` コマンドでサポートされる `host 10.10.10.10 && port 80` のような構文を使用できます。
- クライアント IP は、電子メール セキュリティ アプライアンスを介してメッセージを送信するメール クライアントなどのアプライアンスに接続しているマシンの IP アドレスです。
- サーバ IP は、アプライアンスがメッセージを配信する Exchange サーバなどのアプライアンスが接続しているマシンの IP アドレスです。

  クライアントとサーバの IP アドレスを使用して、中間に電子メール セキュリティ アプライアンスがある特定のクライアントと特定のサーバ間のトラフィックを追跡できます。

c. [送信（Submit）] をクリックします。

ステップ 3　[キャプチャを開始（Start Capture）] をクリックします。

- キャプチャは一度に 1 つだけ実行できます。
- パケット キャプチャが実行されている場合、[パケット キャプチャ（Packet Capture）] ページには、実行中のキャプチャのステータス（ファイル サイズや経過時間などの現在の統計情報）が表示されます。
- GUI に表示されるのは GUI で開始されたパケット キャプチャだけで、CLI で開始されたパケット キャプチャは表示されません。同様に、CLI には CLI で開始された現在のパケット キャプチャのステータスだけが表示されます。
- パケット キャプチャ ファイルは 10 個の部分に分割されます。全体の時間が経過する前にパケット キャプチャ ファイルが最大サイズ制限に到達した場合は、そのファイルの最も古い部分が削除され（データが破棄されます）、現在のパケット キャプチャ データで新しい部分が開始されます。パケット キャプチャ ファイルは一度に 1/10 だけ破棄されます。
- GUI で開始されたキャプチャはセッション間で維持されます。（CLI で開始した実行中のキャプチャはセッションが終了したときに停止します）。

ステップ 4　キャプチャを指定した期間実行させるか、または無期限に実行させて [キャプチャ停止（Stop Capture）] をクリックして手動で停止します。

ステップ 5　パケット キャプチャ ファイルへのアクセス：

- [パケットキャプチャファイルの管理（Manage Packet Capture Files）] リスト内のファイルをクリックし [ファイルのダウンロード（Download File）] をクリックします。
- アプライアンスの `captures` サブ ディレクトリ内のファイルにアクセスするために FTP または SCP を使用します。

次の作業

サポートするファイルを使用できるようにします。

- アプライアンスへのリモート アクセスを許可している場合、技術者が FTP または SCP を使用してパケット キャプチャ ファイルにアクセスできます。「シスコのテクニカル サポート担当者へのリモート アクセスのイネーブル化」（P.16-2）を参照してください。
- サポートにファイルを電子メールで送信します。

リモートからのアプライアンス電源のリセット

アプライアンスでハード リセットが必要な場合、サードパーティ製の Intelligent Platform Management Interface（IPMI）ツールを使用して、リモートからアプライアンス シャーシをリブートできます。

制約事項

- リモート電源管理は、特定のハードウェアでのみ使用できます。

  詳細については、「リモート電源管理のイネーブル化」（P.14-6）を参照してください。
- この機能を使用可能にするには、事前にイネーブルにする必要があります。

  詳細は、「リモート電源管理のイネーブル化」（P.14-6）を参照してください。
- 次の IPMI コマンドのみサポートされます。

  `status`、`on`、`off`、`cycle`、`reset`、`diag`、`soft`

  サポート対象外のコマンドを発行すると、「特権が不十分」エラーが生成されます。

はじめる前に

- IPMI バージョン 2.0 を使用して、デバイスを管理できるユーティリティを取得し、設定します。
- サポートされる IPMI コマンドを使用する方法を理解します。お使いの IPMI ツールのマニュアルを参照してください。

手順

ステップ 1　IPMI を使用して、必要なクレデンシャルとともに、以前に設定したリモート電源管理ポートに割り当てられる IP アドレスに対して、サポートされている電源の再投入コマンドを発行します。

たとえば、IPMI をサポートする UNIX タイプのマシンから次のコマンドを発行できます。

```
ipmitool -I lan -H 192.0.2.1 -U remoteresetuser -P password chassis power reset
```

ここで、`192.0.2.1` はリモート電源管理ポートに割り当てられた IP アドレス、`remoteresetuser` と `password` は、この機能をイネーブルにする際に入力したクレデンシャルです。

ステップ 2　アプライアンスがリブートするまで、少なくとも 5 分間待ちます。

APPENDIX A

IP インターフェイスおよびアプライアンスへのアクセス

シスコ コンテンツ セキュリティ アプライアンスで作成する任意の IP インターフェイスには、さまざまなサービスを通してアクセスできます。

デフォルトでは、各インターフェイスに対して次のサービスがイネーブルまたはディセーブルに設定されています。

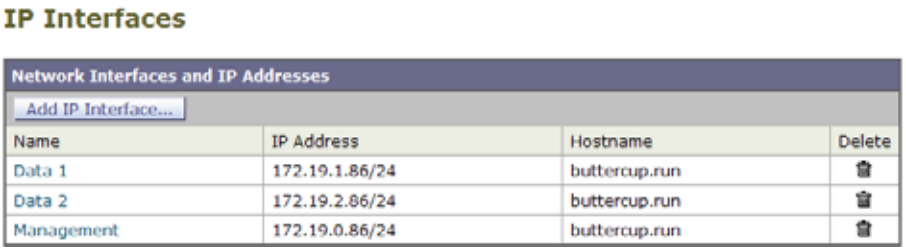
表 A-1　IP インターフェイスに対してデフォルトでイネーブルになるサービス

		デフォルトでイネーブルかどうか	
サービス	**デフォルト ポート**	**管理インターフェイス**	**新規作成された IP インターフェイス**
FTP	21	No	No
Telnet	23	Yes	No
SSH	22	Yes	No
HTTP	80	Yes	No
HTTPS	443	Yes	No

IP インターフェイス

IP インターフェイスには、ネットワークへの個別の接続に必要なネットワーク設定データが含まれています。1 つの物理イーサネット インターフェイスに対して複数の IP インターフェイスを設定できます。IP インターフェイス経由の Cisco IronPort スパム隔離へのアクセスも設定できます。電子メール配信および仮想ゲートウェイの場合、各 IP インターフェイスは特定の IP アドレスおよびホスト名を持つ 1 つの仮想ゲートウェイ アドレスとして機能します。また、インターフェイスは個別のグループに（CLI を介して）「参加」させることもできます。その場合、システムは、電子メールの配信時にこれらのグループを順番に繰り返して使用します。仮想ゲートウェイの参加またはグループ化は、大規模な電子メール キャンペーンを複数のインターフェイス間でロード バランシングする際に役立ちます。
VLAN を作成し、他のインターフェイスと同様に（CLI を介して）設定することもできます。詳細については、お使いの電子メール セキュリティ アプライアンスのユーザ ガイドまたはのオンライン ヘルプの「Advanced Networking」の章を参照してください。

図 A-1　[IP インターフェイス（IP Interfaces）] ページ



IP インターフェイスの設定

[管理アプライアンス（Management Appliance）] > [ネットワーク（Network）] > [IP インターフェイス（IP Interfaces）] ページ（および `interfaceconfig` コマンド）では、IP インターフェイスを追加、編集、または削除できます。

（注）　セキュリティ管理アプライアンス上の管理インターフェイスに関連付けられた名前またはイーサネットポートを変更することはできません。さらに、セキュリティ管理アプライアンスは後述のすべての機能をサポートしているわけではありません（たとえば、仮想ゲートウェイ）。

IP インターフェイスを設定する場合は、次の情報が必要です。

表 A-2　IP インターフェイス コンポーネント

名前	インターフェイスのニックネーム。
IP アドレス	同じサブネットに含まれる IP アドレスを、別々の物理イーサネット インターフェイスには設定できません。
ネットマスク（サブネットマスク）	ネットマスクを標準のドット付きオクテット形式（たとえば、255.255.255.0）または 16 進形式（たとえば、0xffffff00）で入力できます。デフォルトのネットマスクは 255.255.255.0、一般的なクラス C 値です。
ブロードキャスト アドレス	AsyncOS はデフォルトのブロードキャスト アドレスを IP アドレスおよびネットマスクから自動的に計算します。
ホスト名	インターフェイスに関連するホスト名。ホスト名は、SMTP カンバセーション中のサーバの特定に使用されます。各 IP アドレスに関連付けられた有効なホスト名を入力する必要があります。ソフトウェアは、DNS によってホスト名が一致する IP アドレスに正しく解決されたり、または逆引き DNS によって所定のホスト名が解決されることをチェックしません。
許可されるサービス	FTP、SSH、Telnet、Cisco IronPort スパム隔離、HTTP、および HTTPS はインターフェイス上でイネーブルまたはディセーブルにできます。サービスごとにポートを設定できます。Cisco IronPort スパム隔離の HTTP/HTTPS、ポート、および URL も設定できます。

（注）　第 2 章「セットアップ、インストール、および基本設定」の説明に従ってシステム セットアップ ウィザードを完了し、変更を保存している場合は、アプライアンス上に管理インターフェイスがすでに設定されているはずです。

GUI を使用した IP インターフェイスの作成

手順

ステップ 1　[管理アプライアンス（Management Appliance）] > [ネットワーク（Network）] > [IP インターフェイス（IP Interfaces）] を選択します。

ステップ 2　[IP インターフェイスの追加（Add IP Interface）] をクリックします。

ステップ 3　インターフェイスの名前を入力します。

ステップ 4　イーサネット ポートを選択し、IP アドレスを入力します。

ステップ 5　IP アドレスに対応するネットマスクを入力します。

ステップ 6　インターフェイスのホスト名を入力します。

ステップ 7　この IP インターフェイス上でイネーブルにする各サービスの横にあるチェックボックスをオンにします。必要に応じて、対応するポートを変更します。

ステップ 8　アプライアンス管理用にインターフェイスで HTTP から HTTPS へのリダイレクトをイネーブルにするかどうかを選択します。

ステップ 9　Cisco IronPort スパム隔離を使用している場合は、HTTP、HTTPS、またはその両方を選択し、それぞれにポート番号を指定できます。HTTP 要求を HTTPS にリダイレクトするかどうかも選択できます。最後に、IP インターフェイスが Cisco IronPort スパム隔離のデフォルト インターフェイスであるかどうか、およびホスト名を URL として使用するかまたはカスタム URL を指定するかを指定できます。

ステップ 10　変更を送信し、保存します。

FTP 経由でのアプライアンスへのアクセス

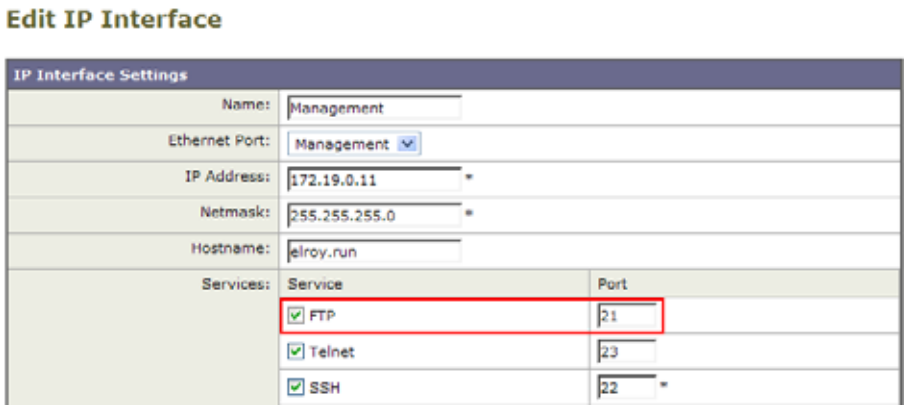
警告　**[管理アプライアンス（Management Appliance）] > [ネットワーク（Network）] > [IP インターフェイス（IP Interfaces）] ページまたは `interfaceconfig` コマンドからサービスをディセーブルにすることにより、アプライアンスへの接続方法に応じて、GUI または CLI から切断できます。別のプロトコル、シリアル インターフェイス、または管理ポートのデフォルト設定を使用してアプライアンスに再接続できない場合は、このコマンドでサービスをディセーブルにしないでください。**

手順

ステップ 1　[管理アプライアンス（Management Appliance）] > [ネットワーク（Network）] > [IP インターフェイス（IP Interfaces）] ページ（または `interfaceconfig` コマンド）を使用して、インターフェイスに対して FTP アクセスをイネーブルにします。

この例では、管理インターフェイスはポート 21（デフォルト ポート）上での FTP アクセスをイネーブルにするように編集されています。

図 A-2　[IP インターフェイスを編集（Edit IP Interface）] ページ



（注）　次のステップに移る前に、変更を保存することを忘れないでください。

ステップ 2　FTP 経由でインターフェイスにアクセスします。インターフェイスに対して正しい IP アドレスを使用していることを確認します。

例：

```
ftp 192.168.42.42
```

ブラウザの多くは、FTP 経由でもインターフェイスにアクセスできます。

例：

```
ftp://192.10.10.10
```

ステップ 3　実行しようとする特定のタスクのディレクトリを参照します。FTP 経由でインターフェイスにアクセスしたら、次のディレクトリを参照してファイルをコピーおよび追加（「GET」および「PUT」）できます。表 A-3 を参照してください。

表 A-3　アクセスできるディレクトリ

ディレクトリ名	説明
/avarchive **/bounces** **/cli_logs** **/delivery** **/error_logs** **/ftpd_logs** **/gui_logs** **/mail_logs** **/rptd_logs** **/sntpd.logs** **/status** **/system_logs**	[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ログ設定（Log Subscriptions）] ページまたは、`logconfig` および `rollovernow` コマンドを使用したロギング用に、自動的に作成されます。各ログの詳しい説明については、お使いの電子メール セキュリティ アプライアンスのユーザ ガイドまたはオンライン ヘルプの「Logging」の章を参照してください。 各ログ ファイル タイプの違いについては、「Logging」章の「Log File Type Comparison」を参照してください。
/configuration	次のページおよびコマンドからのデータのエクスポート先ディレクトリ、またはインポート元（保存）ディレクトリ。 • 仮想ゲートウェイ マッピング（`altsrchost`） • XML 形式の設定データ（`saveconfig`、`loadconfig`） • [ホスト アクセス テーブル（HAT）（Host Access Table (HAT)）] ページ（`hostaccess`） • [受信者アクセス テーブル（RAT）（Recipient Access Table (RAT)）] ページ（`rcptaccess`） • [SMTP ルート（SMTP Routes）] ページ（`smtproutes`） • エイリアス テーブル（`aliasconfig`） • マスカレード テーブル（`masquerade`） • メッセージ フィルタ（`filters`） • グローバル配信停止データ（`unsubscribe`） • `trace` コマンドのテスト メッセージ

表 A-3　アクセスできるディレクトリ （続き）

ディレクトリ名	説明
/MFM	メール フロー モニタリング データベース ディレクトリには、GUI から使用できるメール フロー モニタ機能のデータが含まれます。各サブディレクトリには、各ファイルのレコード形式を文書化した README ファイルが含まれます。 記録を残すためにこれらのファイルを異なるマシンにコピーしたり、ファイルをデータベースにロードして独自の分析アプリケーションを作成することができます。レコード形式は、すべてのディレクトリ内にあるすべてのファイルで同じです。この形式は今後のリリースで変更される場合があります。
/periodic_reports	システムで設定されているすべてのアーカイブ済みレポートが保管されます。

ステップ 4　ご使用の FTP プログラムを使用して、適切なディレクトリに対するファイルのアップロードおよびダウンロードを行います。

セキュア コピー（scp）アクセス

クライアント オペレーティング システムでセキュア コピー（scp）コマンドがサポートされている場合は、表 A-3（P.A-5）に示すディレクトリ間でファイルをコピーできます。たとえば、次の例では、ファイル /tmp/test.txt は、クライアント マシンからホスト名 mail3.example.com を持つアプライアンスの configuration ディレクトリにコピーされます。

（注）　このコマンドでは、ユーザ（admin）のパスワードを求めるプロンプトが表示されます。この例を参考用としてだけ示します。オペレーティング システムのセキュア コピーの実装方法によって異なる場合があります。

```
% scp /tmp/test.txt admin@mail3.example.com:configuration
The authenticity of host 'mail3.example.com (192.168.42.42)' can't be established.
DSA key fingerprint is 69:02:01:1d:9b:eb:eb:80:0c:a1:f5:a6:61:da:c8:db.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'mail3.example.com ' (DSA) to the list of known hosts.
admin@mail3.example.com's password: (type the password)
test.txt             100% |***************************|  1007       00:00
%
```

この例では、同じファイルがアプライアンスからクライアント マシンにコピーされます。

```
% scp admin@mail3.example.com:configuration/text.txt .
admin@mail3.example.com's password: (type the password)
test.txt             100% |***************************|  1007       00:00
```

コンテンツ セキュリティ アプライアンスに対するファイルの転送および取得には、secure copy（scp）を FTP に代わる方法として使用できます。

（注）　operators グループおよび administrators グループのユーザだけが、アプライアンスへのアクセスにセキュア コピー（scp）を使用できます。詳細については、「AsyncOS の以前のバージョンへの復元について」（P.14-30）を参照してください。

シリアル接続によるアクセス

シリアル接続を使用してアプライアンスに接続している場合、図 A-3 にシリアル ポート コネクタのピン番号を示し、表 A-4 にシリアル ポート コネクタのピン割り当ておよびインターフェイス信号を定義します。

図 A-3　　シリアル ポートのピン番号

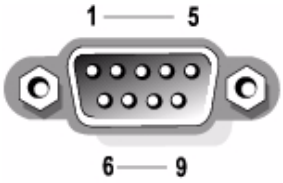


表 A-4　　シリアル ポートのピン割り当て

ピン	信号	I/O	定義
1	DCD	I	データ キャリア検出
2	SIN	I	シリアル入力
3	SOUT	O	シリアル出力
4	DTR	O	データ ターミナル レディ
5	GND	n/a	信号用接地
6	DSR	I	データ セット レディ
7	RTS	I	送信要求
8	CTS	O	送信可
9	RI	I	リング インジケータ
シェル	n/a	n/a	シャーシ アース

APPENDIX B

ネットワークと IP アドレスの割り当て

この付録では、ネットワーク アドレスと IP アドレスの割り当てに関する一般的なルールについて説明し、ネットワークに シスコ コンテンツ セキュリティ アプライアンスを接続するための戦略の一部を示します。

この付録の内容は、次のとおりです。

イーサネット インターフェイス

シスコのコンテンツ セキュリティ アプライアンスには、構成により（任意選択の光ネットワーク インターフェイスがあるかどうか）システムの背面パネルに最大 4 つのイーサネット インターフェイスがあります。次のラベルが付いています。

- Management
- Data1
- Data2
- Data3
- Data4

IP アドレスとネットマスクの選択

ネットワークを設定するとき、コンテンツ セキュリティ アプライアンスは発信パケットを送信するために一意のインターフェイスを選択できなければなりません。この要件によって、イーサネット インターフェイスの IP アドレスとネットマスクの選択に関して、いくつかのことが決まります。単一のネットワークに配置できるインターフェイスは 1 つのみというのがルールです（ネットマスクがインターフェイスの IP アドレスに適用されることでそのように定められます）。

IP アドレスは、指定されたネットワークの物理インターフェイスを識別します。物理イーサネット インターフェイスは、パケットを受け取る IP アドレスを複数持つことができます。複数の IP アドレスを持つイーサネット インターフェイスは、パケットの送信元アドレスとしていずれか 1 つの IP アドレスを使用して、インターフェイスからパケットを送信できます。このプロパティは、仮想ゲートウェイ テクノロジーの実装で使用されます。

ネットマスクの目的は、IP アドレスをネットワーク アドレスとホスト アドレスに分割することです。ネットワーク アドレスは、IP アドレスのネットワーク部分（ネットマスクと一致するビット）と見なすことができます。ホスト アドレスは、IP アドレスの残りのビットです。4 オクテット アドレス内の有効なビット数は、クラスレス ドメイン間ルーティング（CIDR）形式で表現されることがあります。これは、スラッシュ記号、後にビット数（1 ～ 32）が続きます。

ネットマスクは、単純にバイナリの 1 を数える方法で表現できます。255.255.255.0 は「/24」になり、255.255.240.0 は「/20」になります。

インターフェイス設定のサンプル

ここでは、いくつかの代表的なネットワークに基づいたインターフェイスの設定例を示します。この例では、Int1 と Int2 の 2 つのインターフェイスを使用します。コンテンツ セキュリティ アプライアンスの場合、これらのインターフェイス名は、3 つのインターフェイス（Management、Data1、Data2）の中の 2 つのインターフェイスを示します。

ネットワーク 1：

個別のインターフェイスは別のネットワーク上に存在するように示す必要があります。

インターフェイス	IP アドレス	ネットマスク	ネット アドレス
Int1	192.168.1.10	255.255.255.0	192.168.1.0/24
Int2	192.168.0.10	255.255.255.0	192.168.0.0/24

192.168.1.x にアドレス指定されたデータ（ここで X は 1 ～ 255 の任意の番号。ただし、自身のアドレス（この場合は 10）を除く）は、Int1 から送出されます。192.168.0.x にアドレス指定されたデータは、Int2 から送出されます。この形式ではない他のアドレス（最も考えられるのは WAN またはインターネット上）に向かうパケットは、デフォルト ゲートウェイに送信されます。デフォルト ゲートウェイはこれらのネットワークのどちらかの上に存在する必要があります。その後、デフォルト ゲートウェイがパケットを転送します。

ネットワーク 2：

2 つの異なるインターフェイスのネットワーク アドレス（IP アドレスのネットワーク部分）は同じにすることができません。

イーサネット インターフェイス	IP アドレス	ネットマスク	ネット アドレス
Int1	192.168.1.10	255.255.0.0	192.168.0.0/16
Int2	192.168.0.10	255.255.0.0	192.168.0.0/16

これは、2 つのイーサネット インターフェイスが同じネットワーク アドレスを持つという、競合した状態を表しています。コンテンツ セキュリティ アプライアンスからのパケットが 192.168.1.11 に送信された場合、パケットの配信にどのイーサネット インターフェイスを使用する必要があるかを決定する方法はありません。2 つのイーサネット インターフェイスが 2 つの物理ネットワークに別々に接続されている場合、パケットは誤ったネットワークに配信される可能性があり、そうするとそのパケットの送信先を見つけることはできません。コンテンツ セキュリティ アプライアンスでは、競合するネットワークを設定できません。

2 つのイーサネット インターフェイスを同じ物理ネットワークに接続することはできますが、コンテンツ セキュリティ アプライアンスが一意の配信インターフェイスを選択できるように IP アドレスとネットマスクを設定する必要があります。

IP アドレス、インターフェイス、およびルーティング

GUI または CLI で、インターフェイスを選択可能なコマンドや関数を実行する際にインターフェイスを選択した場合（たとえば、AsyncOS のアップグレードや DNS の設定など）、ルーティング（デフォルト ゲートウェイ）が選択した内容よりも優先されます。

たとえば、3 つのネットワーク インターフェイスがそれぞれ別のネットワーク セグメントに設定された次のようなコンテンツ セキュリティ アプライアンスがあるとします（すべて /24 と仮定）。

イーサネット	IP
Management	192.19.0.100
Data1	192.19.1.100
Data2	192.19.2.100

デフォルト ゲートウェイは 192.19.0.1 です。

ここで、AsyncOS のアップグレード（またはインターフェイスを選択できる他のコマンドや関数）を実行し、Data1 上の IP（192.19.1.100）を選択した場合、すべての TCP トラフィックが Data1 イーサネット インターフェイス経由になると予想されることと思います。しかし、実際には、デフォルト ゲートウェイとして設定されているインターフェイス（ここでは Management）からトラフィックが送出されます。ただし、トラフィックの送信元アドレスには Data1 の IP が設定されています。

サマリー

コンテンツ セキュリティ アプライアンスは、配信可能なパケットが経由する一意のインターフェイスを常に識別できなければなりません。この決定を行うために、コンテンツ セキュリティ アプライアンスは、パケットの宛先 IP アドレスと、そのイーサネット インターフェイスのネットワークおよび IP アドレス設定を組み合わせて使用します。次の表に、ここまで説明してきた例をまとめます。

	同じネットワーク	異なるネットワーク
同じ物理インターフェイス	許可	許可
異なる物理インターフェイス	不可	許可

コンテンツ セキュリティ アプライアンスを接続するための戦略

アプライアンスを接続する際には、次の点に留意してください。

- 通常、管理トラフィック（CLI、Web インターフェイス、ログ配信）は、電子メール トラフィックよりもはるかに少量です。
- 2 つのイーサネット インターフェイスが同じネットワーク スイッチに接続されているが最終的にダウンストリームの別のホスト上の単一インターフェイスと通信するだけの場合、あるいはすべてのデータがすべてのポートにエコーされるネットワーク ハブにそれらが接続されている場合、2 つのインターフェイスを使用しても得られる利点はありません。

- 1000Base-T で動作しているインターフェイスでの SMTP カンバセーションは、100Base-T で動作している同じインターフェイスでのカンバセーションよりも少し高速ですが、速くなるのは理想的な条件下でのみです。
- 配信ネットワークの別の箇所にボトルネックがある場合、ネットワークへの接続を最適化しても意味はありません。ボトルネックは、インターネットへの接続および接続プロバイダーのさらにアップストリームで最も頻繁に発生します。

接続に使用するインターフェイスの数とそれらへのアドレス指定の方法は、基礎となるネットワークの複雑性によって決める必要があります。複数インターフェイスの接続は、ネットワーク トポロジやデータ ボリュームで要求されなければ必要ありません。また、最初は単純な接続にしておき、ゲートウェイに慣れてきたら、ボリュームやネットワーク トポロジでの必要に応じて接続を増やすこともできます。

APPENDIX C

ファイアウォール情報

次の表は、シスコ コンテンツ セキュリティ アプライアンスを正常に動作させるために開けなければならないことがあるポートのリストです（デフォルト値を示す）。

表 C-1　　ファイアウォール ポート

デフォルト ポート	プロトコル	In/Out	ホスト名	目的
20/21	TCP	In または Out	AsyncOS IP、FTP サーバ	ログ ファイルのアグリゲーションの FTP。 データ ポート TCP 1024 およびそれ以上もすべて開いている必要があります。 詳細については、ナレッジ ベースの FTP ポート情報を検索してください。「ナレッジ ベース」（P.1-5）を参照してください。
22	SSH	Out	AsyncOS IP	中央集中型コンフィギュレーション マネージャのコンフィギュレーションの配信。 バックアップにも使用されます。
22	TCP	In	AsyncOS IP	CLI への SSH アクセス、ログ ファイルのアグリゲーション。
22	TCP	Out	SCP サーバ	ログ サーバへの SCP 配信。
23	Telnet	In	AsyncOS IP	CLI への Telnet アクセス。
23	Telnet	Out	Telnet サーバ	Telnet アップグレード。
25	TCP	Out	Any	電子メール送信用 SMTP。
25	TCP	In	AsyncOS IP	バウンスされた電子メールを受信する SMTP または外部のファイアウォールから電子メールをインジェクトする場合。
80	HTTP	In	AsyncOS IP	システム モニタリングのための GUI への HTTP アクセス。
80	HTTP	Out	downloads.cisco.com	サービス アップデート、AsyncOS アップグレードを除く。
80	HTTP	Out	updates.cisco.com	AsyncOS アップグレード。
82	HTTP	In	AsyncOS IP	Cisco IronPort スパム隔離の表示に使用。
83	HTTPS	In	AsyncOS IP	Cisco IronPort スパム隔離の表示に使用。

表 C-1　ファイアウォール ポート （続き）

デフォルト ポート	プロトコル	In/Out	ホスト名	目的
53	UDP/TCP	Out	DNS サーバ	インターネット ルート サーバまたはファイアウォール外部の DNS サーバを使用するように設定されている場合の DNS。また、SenderBase クエリーの場合。
110	TCP	Out	POP サーバ	Cisco IronPort スパム隔離のためのエンドユーザの POP 認証。
123	UDP	Out	NTP サーバ	タイム サーバがファイアウォール外部の場合、NTP。
143	TCP	Out	IMAP サーバ	Cisco IronPort スパム隔離のためのエンドユーザの IMAP 認証。
161	UDP	In	AsyncOS IP	SNMP クエリー。
162	UDP	Out	管理ステーション	SNMP トラップ。
389 3268	LDAP	Out	LDAP サーバ	LDAP ディレクトリ サーバがファイアウォール外部の場合、LDAP。Cisco IronPort スパム隔離のための LDAP 認証。
636 3269	LDAPS	Out	LDAPS	LDAPS：ActiveDirectory のグローバル カタログ サーバ。
443	TCP	In	AsyncOS IP	システム モニタリングのための GUI への HTTP（https）アクセス。
443	TCP	Out	update-static.cisco.com	アップデート サーバの最新のファイルを確認します。
443	TCP	Out	phonehome.senderbase.org	アウトブレイク フィルタの受信 / 送信。
514	UDP/TCP	Out	Syslog サーバ	Syslog ロギング。
1024 以降	—	—	—	ポート 21（FTP）については、上記の情報を参照してください。
2222	CCS	In および Out	AsyncOS IP	クラスタ通信サービス（中央集中型管理用）。
6025	TCP	In	AsyncOS IP	外部 Cisco IronPort スパム隔離がイネーブルの場合、Cisco IronPort スパム隔離データをセキュリティ管理アプライアンスに送信。
7025	TCP	In および Out	AsyncOS IP	この機能が集約されると電子メール セキュリティ アプライアンスのセキュリティ管理アプライアンス間でポリシー、ウイルス、アウトブレイク隔離データを渡します。

APPENDIX D

例

この付録は、シスコのコンテンツ セキュリティ管理アプライアンス機能を導入する一般的な方法について数例を説明しています。これらには、次の項を含みます。

Web セキュリティ アプライアンスの例

ここでは、セキュリティ管理アプライアンスおよび Web セキュリティ アプライアンスを使用した例について説明します。

（注） これらのシナリオはすべて、セキュリティ管理アプライアンスおよびWeb セキュリティ アプライアンスで Web レポーティングおよび Web トラッキングをイネーブルがイネーブルにされていることを前提としています。Web トラッキングおよび Web レポーティングをイネーブルにする方法については、第 5 章「中央集中型 Web レポーティングおよびトラッキングの使用」を参照してください。

例 1：ユーザの調査

次に、システム管理者が会社で特定のユーザを調査する例を示します。

このシナリオでは、ある従業員が勤務中に不適切な Web サイトにアクセスしている、という苦情を管理者が受け取っています。それを調査するには、システム管理者が Web アクティビティの詳細をトラッキングする必要があります。

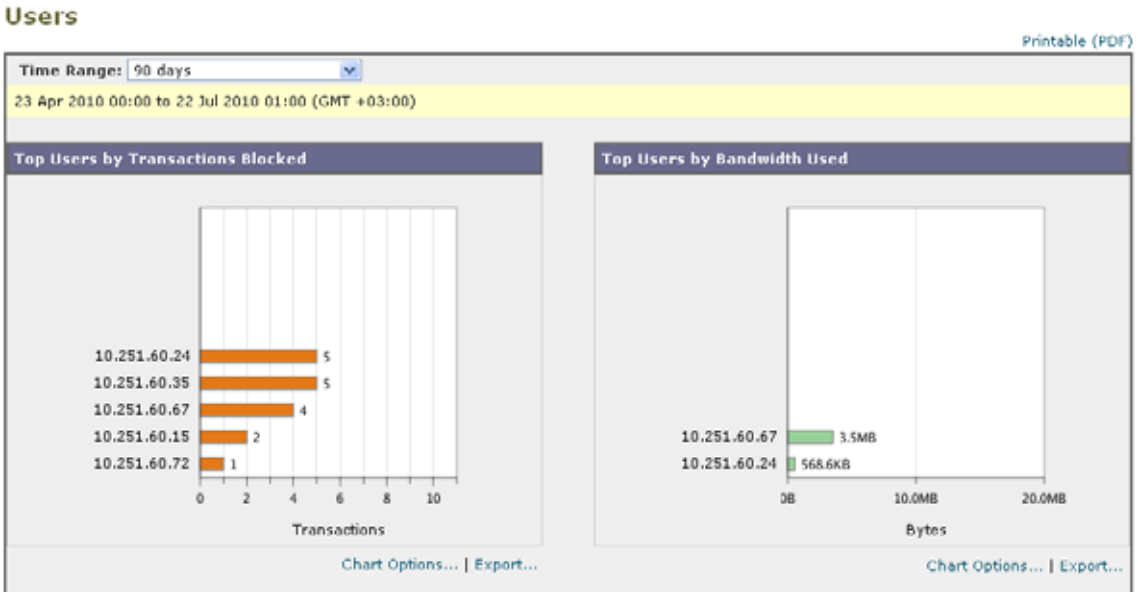
Web アクティビティがトラッキングされると、従業員の参照履歴に関する情報が記載された Web レポートが作成されます。

ステップ 1 セキュリティ管理アプライアンスで、[Web] > [レポート（Reporting）] > [ユーザ（Users）] を選択します。

ステップ 2 [ユーザ（Users）] テーブルで、調査する [ユーザ ID（User ID）] または [クライアント IP アドレス（Client IP address）] をクリックします。

ユーザ ID またはクライアント IP アドレスがわからない場合は、ユーザ ID またはクライアント IP アドレスをわかる範囲でテキスト フィールドに入力し、[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）] をクリックします。IP アドレスが正確に一致していなくても

結果は返されます。[ユーザ（Users）] テーブルに、指定したユーザ ID およびクライアント IP アドレスが入力されます。この例では、クライアント IP アドレス 10.251.60.24 の情報について検索しています。



ステップ 3　IP アドレス [10.251.60.24] をクリックします。

10.251.60.24 のユーザの詳細ページが表示されます。

Users > 10.251.60.24

Printable (PDF)

Time Range: 90 days

31 Aug 2011 00:00 to 29 Nov 2011 15:00 (GMT -08:00)

URL Categories by Total Transactions

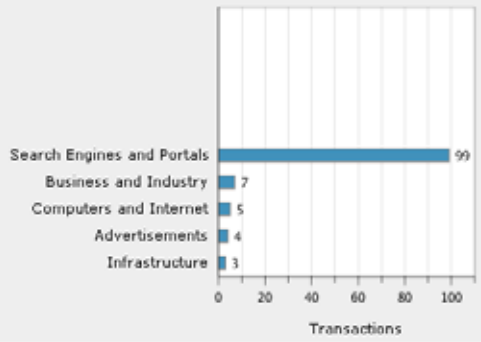


Chart Options... | Export...

Trend by Total Transactions

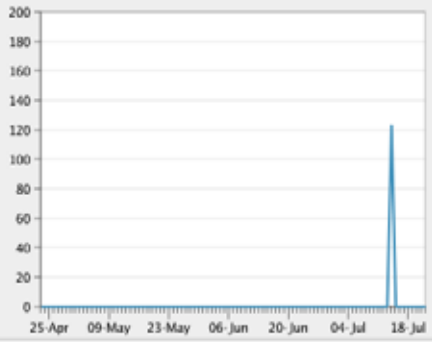


Chart Options... | Export...

URL Categories Matched

URL Category	Bandwidth Used	Time Spent	Blocked URL Category	Transactions Completed	Total Transactions
Search Engines and Portals	447.4KB	00:21	0	99	99
Business and Industry	15.5KB	00:06	0	7	7
Computers and Internet	84.4KB	00:06	0	5	5
Advertisements	16.9KB	00:00	0	4	4
Infrastructure	4,540B	00:00	0	3	3
Totals (all available data):	568.6KB	00:33	0	118	118

Find URL Category

Columns... | Export...

Domains Matched

Domain or IP	Bandwidth Used	Time Spent	Transactions Completed	Transactions Blocked	Total Transactions
[redacted].com	464.5KB	00:36	101	5	106
[redacted].com	83.1KB	00:06	4	0	4
[redacted].com	8,272B	00:00	4	0	4
[redacted].net	15.1KB	00:00	3	0	3
[redacted].com	6,391B	00:06	2	0	2
[redacted].com	1,365B	00:00	1	0	1
[redacted].com	1,231B	00:00	1	0	1
[redacted].com	1,047B	00:00	1	0	1
[redacted]	2,021B	00:00	1	0	1

Find Domain or IP

Columns... | Export...

Applications Matched

No data was found in the selected time range

Malware Threats Detected

No data was found in the selected time range

Policies Matched

Policy Name	Policy Type	Bandwidth Used	Completed Transactions	Blocked Transactions	Total Transactions

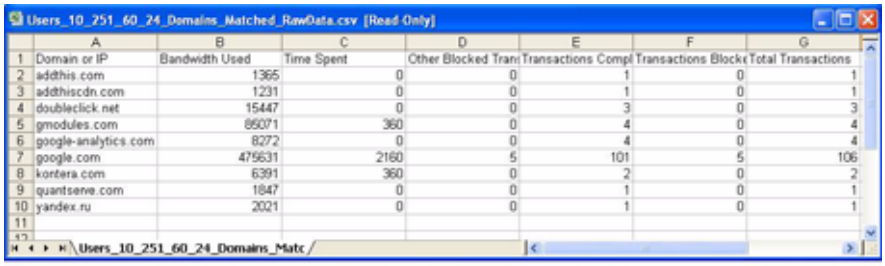
ユーザの詳細ページから総トランザクション別の URL カテゴリ、総トランザクション別のトレンド、一致する URL カテゴリ、一致するドメイン、一致するアプリケーション、検出されたマルウェアの脅威、および一致するポリシーを確認できます。

これらのカテゴリによって、10.251.60.24 のユーザがブロックされている URL（ページの [ドメイン（Domains）] セクションに含まれる [ブロックされたトランザクション（Transactions Blocked）] カラムに表示）にアクセスしようとしていたことなどがわかります。

ステップ 4　[一致したドメイン（Domains Matched）] テーブルの下の [エクスポート（Export）] をクリックし、ユーザがアクセスしようとしていたドメインおよび URL のリストを表示します。

図 D-1 に、ユーザからエクスポートされた情報のリストを示します。

図 D-1　　エクスポート データの例



ここから Web トラッキング機能を使用して、この特定のユーザの Web 使用状況をトラッキングし、表示することができます。

（注）　Web レポーティングでは、アクセスされる特定の URL に限らず、ユーザがアクセスするすべてのドメイン情報を取得できる点に注意してください。ユーザがアクセスしている特定の URL、その URL にアクセスした時刻、その URL が許可されているかどうかなどの情報を得るには、[Web トラッキング（Web Tracking）] ページの [プロキシ サービス（Proxy Services）] タブを使用します。

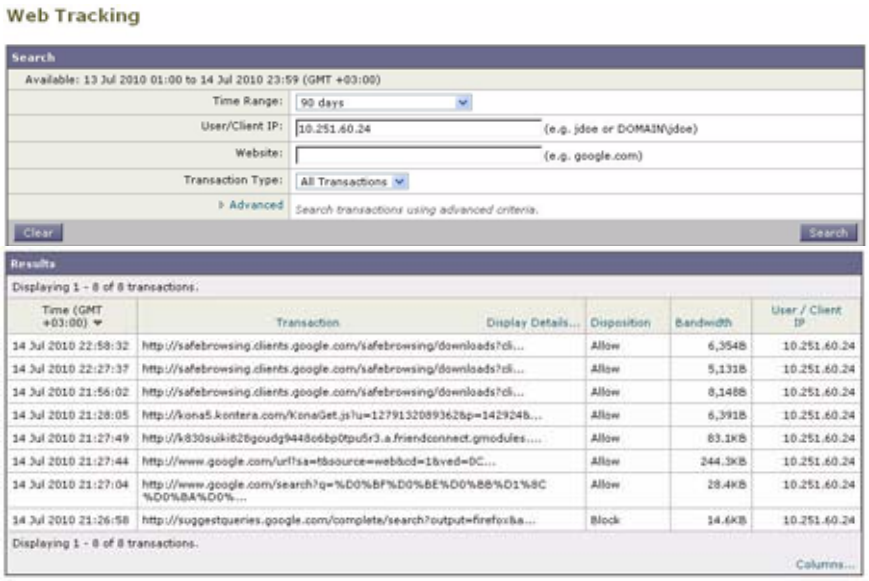
ステップ 5　[Web] > [レポート（Reporting）] > [Web トラッキング（Web Tracking）] を選択します。

ステップ 6　[プロキシ サービス（Proxy Services）] タブをクリックします。

ステップ 7　[ユーザ / クライアント IP アドレス（User/Client IP Address）] テキスト フィールドにユーザ名または IP アドレスを入力します。

この例では、ユーザ 10.251.60.24 の Web トラッキング情報を検索します。

検索結果が表示されます。



このページから、IP アドレス 10.251.60.24 に割り当てられているコンピュータのユーザがアクセスしたトランザクションおよび URL のすべてのリストを確認できます。

関連項目

表 D-1 に、この例で説明した項目を示します。各項目の詳細については、リンクをクリックしてください。

表 D-1　　ユーザの調査の関連項目

機能名	機能情報
[ユーザ（User）] ページ	「[ユーザ（Users）] レポート（Web）」（P.5-17）
[ユーザの詳細（User Details）] ページ	「[ユーザの詳細（User Details）]（Web レポーティング）」（P.5-20）
レポート データのエクスポート	「レポーティング データおよびトラッキング データの印刷およびエクスポート」（P.3-10）
[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	「Web プロキシ サービスによって処理されたトランザクションの検索」（P.5-56）

例 2：URL のトラッキング

このシナリオでは、セールス マネージャが、会社のサイトへのアクセスで、先週の上位 5 位を知りたい場合を考えます。さらに、どのユーザがこれらの Web サイトにアクセスしているかについても知りたいとします。

ステップ 1　セキュリティ管理アプライアンスで、[Web] > [レポート（Reporting）] > [Web サイト（Web Sites）] を選択します。

ステップ 2　[時間範囲（Time Range）] ドロップダウン リストから [週（Week）] を選択します。

ステップ 3　[ドメイン（Domains）] セクションをスクロール ダウンすると、アクセスされているドメインまたは Web サイトが表示されます。

アクセス上位 25 位までの Web サイトは、[一致したドメイン（Domains Matched）] テーブルに表示されます。同じテーブルで [ドメイン（Domain）] または [IP] カラムのリンクをクリックすると、特定のアドレスまたはユーザが参照した実際の Web サイトを確認できます。

関連項目

表 D-2 に、この例で説明した項目を示します。各項目の詳細については、リンクをクリックしてください。

表 D-2　URL のトラッキングの関連項目

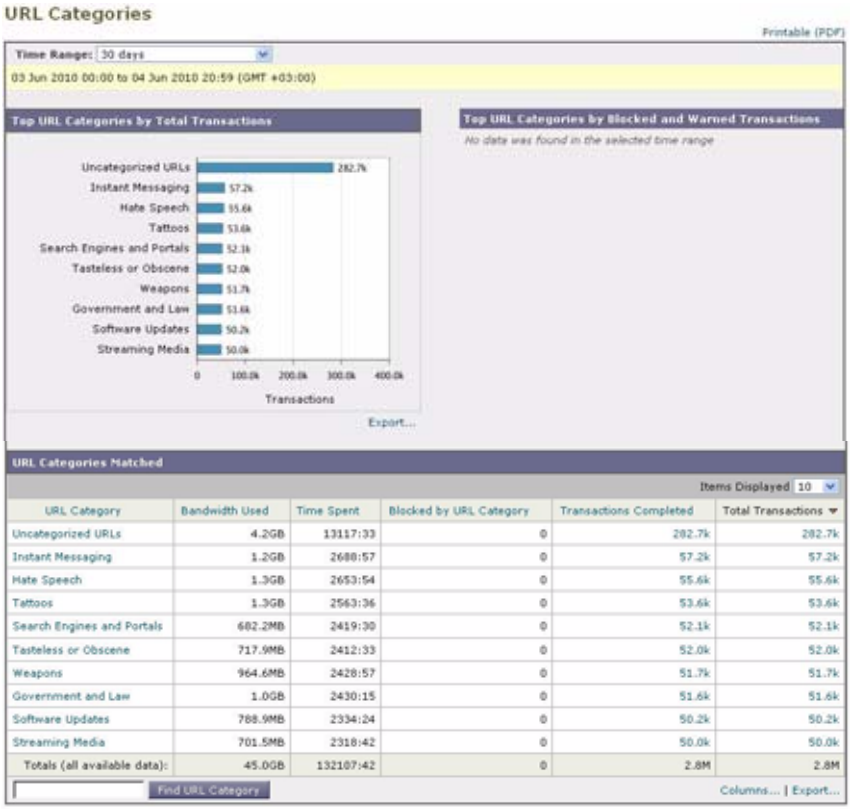
機能名	機能情報
[Web サイト（Web Sites）] ページ	「[Web サイト（Web Sites）] レポート」（P.5-24）

例 3：アクセス数の多い URL カテゴリの調査

このシナリオでは、従業員が最近 30 日間にアクセスした上位 3 位までの URL を、人事部長が知りたい場合を考えます。また、ネットワーク管理者が、帯域幅の使用上をモニタしたり、ネットワークで最も帯域幅を使用している URL を特定したりするためにこの情報を取得するとします。

次の例は、複数の観点を持つ複数の人のためにデータを収集するが、生成するレポートは 1 つだけで済む方法を示します。

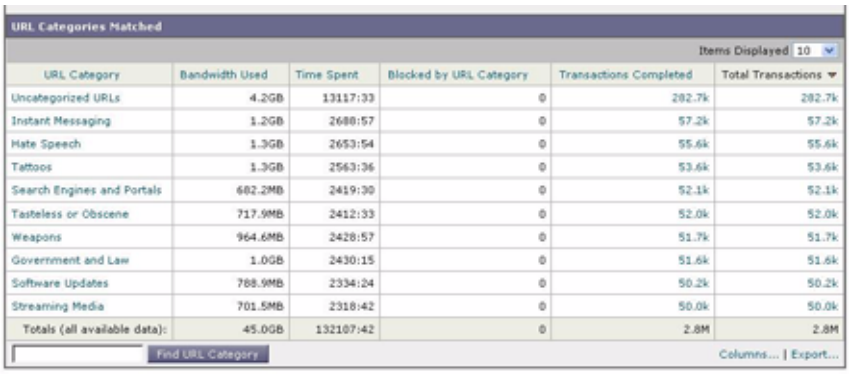
ステップ 1　セキュリティ管理アプライアンスで、[Web] > [レポート（Reporting）] > [URL カテゴリ（URL Categories）] を選択します。



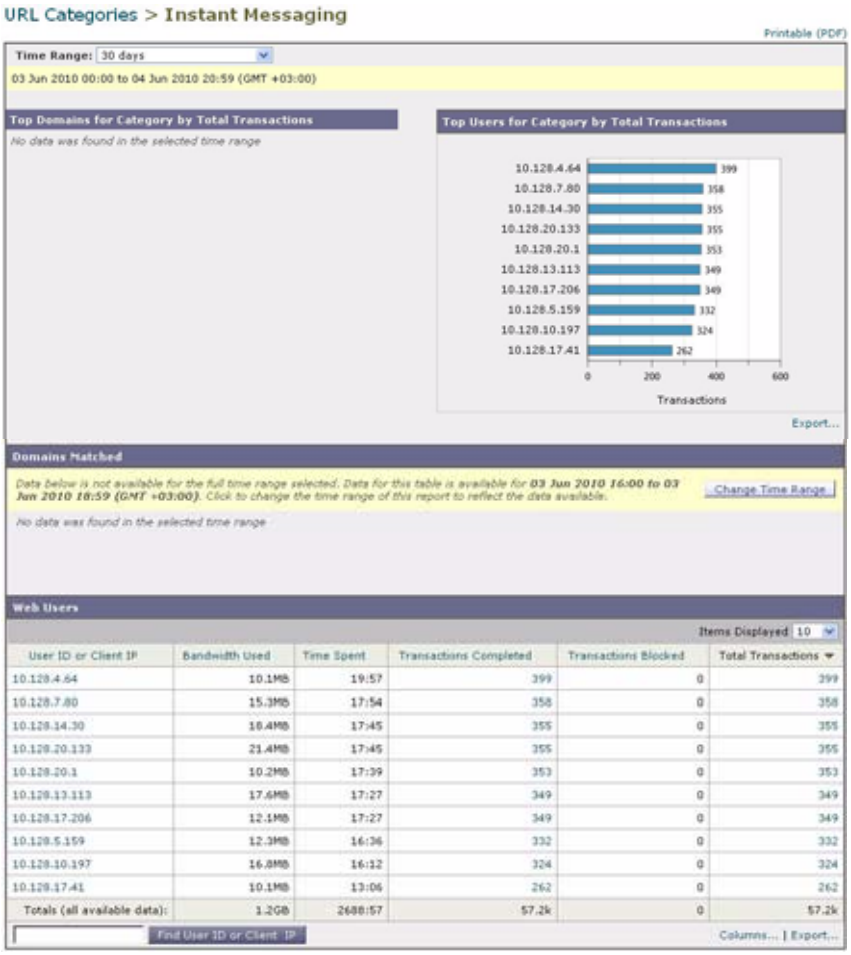
この例の [URL カテゴリ（URL Categories）] ページによると、総トランザクション別の上位 10 の URL カテゴリ グラフから、Instant Messaging、Hate Speech、Tattoo サイトなどの他に、282 k の未分類の URL にアクセスしていることがわかります。

ここで、[エクスポート（Export）] リンクをクリックして raw データを Excel スプレッドシートにエクスポートすると、このファイルを人事部長に送信できます。ネットワーク マネージャに URL ごとの帯域幅の使用量を知らせる必要があります。

ステップ 2　[一致した URL カテゴリ（URL Categories Matched）] テーブルをスクロールダウンし、[使用済み帯域幅（Bandwidth Used）] カラムを表示します。



[一致した URL カテゴリ（URL Categories Matched）] テーブルで、すべての URL カテゴリの帯域幅の使用量を確認することができます。もう一度 [エクスポート（Export）] リンクをクリックして、このファイルをネットワーク管理者に送信します。さらに細かく調べるには、[インスタント メッセージ（Instant Messaging）] リンクをクリックすると、どのユーザが帯域幅を大量に使用しているかが特定されます。次のページが表示されます。



このページから、ネットワーク管理者が Instant Messaging サイトの上位 10 ユーザを知ることができます。

このページから、最近 30 日間で 10.128.4.64 のユーザが Instant Messaging サイトに 19 時間 57 分アクセスしており、この期間の帯域幅の使用量が 10.1 MB であることがわかります。

関連項目

表 D-3 に、この例で説明した項目を示します。各項目の詳細については、リンクをクリックしてください。

表 D-3　アクセスの多い URL カテゴリの調査の関連項目

機能名	機能情報
[URL カテゴリ（URL Categories）] ページ	「URL カテゴリ レポート」（P.5-26）
レポート データのエクスポート	「レポーティング データおよびトラッキング データの印刷およびエクスポート」（P.3-10）

APPENDIX E

End User License Agreement

Cisco Systems End User License Agreement

IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY.IT IS VERY IMPORTANT THAT YOU CHECK THAT YOU ARE PURCHASING CISCO SOFTWARE OR EQUIPMENT FROM AN APPROVED SOURCE AND THAT YOU, OR THE ENTITY YOU REPRESENT (COLLECTIVELY, THE "CUSTOMER") HAVE BEEN REGISTERED AS THE END USER FOR THE PURPOSES OF THIS CISCO END USER LICENSE AGREEMENT.IF YOU ARE NOT REGISTERED AS THE END USER YOU HAVE NO LICENSE TO USE THE SOFTWARE AND THE LIMITED WARRANTY IN THIS END USER LICENSE AGREEMENT DOES NOT APPLY.ASSUMING YOU HAVE PURCHASED FROM AN APPROVED SOURCE, DOWNLOADING, INSTALLING OR USING CISCO OR CISCO-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.

CISCO SYSTEMS, INC. OR ITS SUBSIDIARY LICENSING THE SOFTWARE INSTEAD OF CISCO SYSTEMS, INC. ("CISCO") IS WILLING TO LICENSE THIS SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU PURCHASED THE SOFTWARE FROM AN APPROVED SOURCE AND THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS END USER LICENSE AGREEMENT PLUS ANY ADDITIONAL LIMITATIONS ON THE LICENSE SET FORTH IN A SUPPLEMENTAL LICENSE AGREEMENT ACCOMPANYING THE PRODUCT OR AVAILABLE AT THE TIME OF YOUR ORDER (COLLECTIVELY THE "AGREEMENT").TO THE EXTENT OF ANY CONFLICT BETWEEN THE TERMS OF THIS END USER LICENSE AGREEMENT AND ANY SUPPLEMENTAL LICENSE AGREEMENT, THE SUPPLEMENTAL LICENSE AGREEMENT SHALL APPLY.BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU ARE REPRESENTING THAT YOU PURCHASED THE SOFTWARE FROM AN APPROVED SOURCE AND BINDING YOURSELF TO THE AGREEMENT.IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED CD PACKAGE AND ANY WRITTEN MATERIALS) FOR A FULL REFUND, OR, IF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND.YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM AN APPROVED SOURCE, AND APPLIES ONLY IF YOU ARE THE ORIGINAL AND REGISTERED END USER PURCHASER.FOR THE PURPOSES OF THIS END USER LICENSE AGREEMENT, AN "APPROVED SOURCE" MEANS (A) CISCO; OR (B) A DISTRIBUTOR OR SYSTEMS INTEGRATOR AUTHORIZED BY CISCO TO DISTRIBUTE / SELL CISCO EQUIPMENT, SOFTWARE AND SERVICES WITHIN YOUR TERRITORY TO END USERS; OR (C) A RESELLER AUTHORIZED BY ANY SUCH DISTRIBUTOR OR SYSTEMS INTEGRATOR

IN ACCORDANCE WITH THE TERMS OF THE DISTRIBUTOR'S AGREEMENT WITH CISCO TO DISTRIBUTE / SELL THE CISCO EQUIPMENT, SOFTWARE AND SERVICES WITHIN YOUR TERRITORY TO END USERS.

THE FOLLOWING TERMS OF THE AGREEMENT GOVERN CUSTOMER'S USE OF THE SOFTWARE (DEFINED BELOW), EXCEPT TO THE EXTENT: (A) THERE IS A SEPARATE SIGNED CONTRACT BETWEEN CUSTOMER AND CISCO GOVERNING CUSTOMER'S USE OF THE SOFTWARE, OR (B) THE SOFTWARE INCLUDES A SEPARATE "CLICK-ACCEPT" LICENSE AGREEMENT OR THIRD PARTY LICENSE AGREEMENT AS PART OF THE INSTALLATION OR DOWNLOAD PROCESS GOVERNING CUSTOMER'S USE OF THE SOFTWARE.TO THE EXTENT OF A CONFLICT BETWEEN THE PROVISIONS OF THE FOREGOING DOCUMENTS, THE ORDER OF PRECEDENCE SHALL BE (1)THE SIGNED CONTRACT, (2) THE CLICK-ACCEPT AGREEMENT OR THIRD PARTY LICENSE AGREEMENT, AND (3) THE AGREEMENT.FOR PURPOSES OF THE AGREEMENT, "SOFTWARE" SHALL MEAN COMPUTER PROGRAMS, INCLUDING FIRMWARE AND COMPUTER PROGRAMS EMBEDDED IN CISCO EQUIPMENT, AS PROVIDED TO CUSTOMER BY AN APPROVED SOURCE, AND ANY UPGRADES, UPDATES, BUG FIXES OR MODIFIED VERSIONS THERETO (COLLECTIVELY, "UPGRADES"), ANY OF THE SAME WHICH HAS BEEN RELICENSED UNDER THE CISCO SOFTWARE TRANSFER AND RE-LICENSING POLICY (AS MAY BE AMENDED BY CISCO FROM TIME TO TIME) OR BACKUP COPIES OF ANY OF THE FOREGOING.

License.Conditioned upon compliance with the terms and conditions of the Agreement, Cisco grants to Customer a nonexclusive and nontransferable license to use for Customer's internal business purposes the Software and the Documentation for which Customer has paid the required license fees to an Approved Source."Documentation" means written information (whether contained in user or technical manuals, training materials, specifications or otherwise) pertaining to the Software and made available by an Approved Source with the Software in any manner (including on CD-Rom, or on-line).In order to use the Software, Customer may be required to input a registration number or product authorization key and register Customer's copy of the Software online at Cisco's website to obtain the necessary license key or license file.

Customer's license to use the Software shall be limited to, and Customer shall not use the Software in excess of, a single hardware chassis or card or such other limitations as are set forth in the applicable Supplemental License Agreement or in the applicable purchase order which has been accepted by an Approved Source and for which Customer has paid to an Approved Source the required license fee (the "Purchase Order").

Unless otherwise expressly provided in the Documentation or any applicable Supplemental License Agreement, Customer shall use the Software solely as embedded in, for execution on, or (where the applicable Documentation permits installation on non-Cisco equipment) for communication with Cisco equipment owned or leased by Customer and used for Customer's internal business purposes.No other licenses are granted by implication, estoppel or otherwise.

For evaluation or beta copies for which Cisco does not charge a license fee, the above requirement to pay license fees does not apply.

General Limitations.This is a license, not a transfer of title, to the Software and Documentation, and Cisco retains ownership of all copies of the Software and Documentation.Customer acknowledges that the Software and Documentation contain trade secrets of Cisco or its suppliers or licensors, including but not limited to the specific internal design and structure of individual programs and associated interface information.Except as otherwise expressly provided under the Agreement, Customer shall only use the Software in connection with the use of Cisco equipment purchased by the Customer from an Approved Source and Customer shall have no right, and Customer specifically agrees not to:

(i) transfer, assign or sublicense its license rights to any other person or entity (other than in compliance with any Cisco relicensing/transfer policy then in force), or use the Software on Cisco equipment not purchased by the Customer from an Approved Source or on secondhand Cisco equipment, and Customer acknowledges that any attempted transfer, assignment, sublicense or use shall be void;

(ii) make error corrections to or otherwise modify or adapt the Software or create derivative works based upon the Software, or permit third parties to do the same;

(iii) reverse engineer or decompile, decrypt, disassemble or otherwise reduce the Software to human-readable form, except to the extent otherwise expressly permitted under applicable law notwithstanding this restriction or except to the extent that Cisco is legally required to permit such specific activity pursuant to any applicable open source license;

(iv) publish any results of benchmark tests run on the Software;

(v) use or permit the Software to be used to perform services for third parties, whether on a service bureau or time sharing basis or otherwise, without the express written authorization of Cisco; or

(vi) disclose, provide, or otherwise make available trade secrets contained within the Software and Documentation in any form to any third party without the prior written consent of Cisco.Customer shall implement reasonable security measures to protect such trade secrets.

To the extent required by applicable law, and at Customer's written request, Cisco shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of Cisco's applicable fee, if any.Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Cisco makes such information available.

Software, Upgrades and Additional Copies.NOTWITHSTANDING ANY OTHER PROVISION OF THE AGREEMENT: (1) CUSTOMER HAS NO LICENSE OR RIGHT TO MAKE OR USE ANY ADDITIONAL COPIES OR UPGRADES UNLESS CUSTOMER, AT THE TIME OF MAKING OR ACQUIRING SUCH COPY OR UPGRADE, ALREADY HOLDS A VALID LICENSE TO THE ORIGINAL SOFTWARE AND HAS PAID THE APPLICABLE FEE TO AN APPROVED SOURCE FOR THE UPGRADE OR ADDITIONAL COPIES; (2) USE OF UPGRADES IS LIMITED TO CISCO EQUIPMENT SUPPLIED BY AN APPROVED SOURCE FOR WHICH CUSTOMER IS THE ORIGINAL END USER PURCHASER OR LESSEE OR OTHERWISE HOLDS A VALID LICENSE TO USE THE SOFTWARE WHICH IS BEING UPGRADED; AND (3) THE MAKING AND USE OF ADDITIONAL COPIES IS LIMITED TO NECESSARY BACKUP PURPOSES ONLY.

Proprietary Notices.Customer agrees to maintain and reproduce all copyright, proprietary, and other notices on all copies, in any form, of the Software in the same form and manner that such copyright and other proprietary notices are included on the Software.Except as expressly authorized in the Agreement, Customer shall not make any copies or duplicates of any Software without the prior written permission of Cisco.

Term and Termination.The Agreement and the license granted herein shall remain effective until terminated.Customer may terminate the Agreement and the license at any time by destroying all copies of Software and any Documentation.Customer's rights under the Agreement will terminate immediately without notice from Cisco if Customer fails to comply with any provision of the Agreement.Upon termination, Customer shall destroy all copies of Software and Documentation in its possession or control.All confidentiality obligations of Customer, all restrictions and limitations imposed on the Customer under the section titled "General Limitations" and all limitations of liability and disclaimers and restrictions of warranty shall survive termination of this Agreement.In addition, the provisions of the sections titled "U.S.Government End User Purchasers" and "General Terms Applicable to the Limited Warranty Statement and End User License Agreement" shall survive termination of the Agreement.

Customer Records.Customer grants to Cisco and its independent accountants the right to examine Customer's books, records and accounts during Customer's normal business hours to verify compliance with this Agreement.In the event such audit discloses non-compliance with this Agreement, Customer shall promptly pay to Cisco the appropriate license fees, plus the reasonable cost of conducting the audit.

Export, Re-Export, Transfer and Use Controls.The Software, Documentation and technology or direct products thereof (hereafter referred to as Software and Technology), supplied by Cisco under the Agreement are subject to export controls under the laws and regulations of the United States (U.S.) and any other applicable countries' laws and regulations.Customer shall comply with such laws and regulations governing export, re-export, transfer and use of Cisco Software and Technology and will obtain all required U.S.and local authorizations, permits, or licenses.Cisco and Customer each agree to provide the other information, support documents, and assistance as may reasonably be required by the other in connection with securing authorizations or licenses.Information regarding compliance with export, re-export, transfer and use may be located at the following URL:

http://www.cisco.com/web/about/doing_business/legal/global_export_trade/general_export/contract_compliance.html.

U.S.Government End User Purchasers.The Software and Documentation qualify as "commercial items," as that term is defined at Federal Acquisition Regulation ("FAR") (48 C.F.R.) 2.101, consisting of "commercial computer software" and "commercial computer software documentation" as such terms are used in FAR 12.212.Consistent with FAR 12.212 and DoD FAR Supp.227.7202-1 through 227.7202-4, and notwithstanding any other FAR or other contractual clause to the contrary in any agreement into which the Agreement may be incorporated, Customer may provide to Government end user or, if the Agreement is direct, Government end user will acquire, the Software and Documentation with only those rights set forth in the Agreement.Use of either the Software or Documentation or both constitutes agreement by the Government that the Software and Documentation are "commercial computer software" and "commercial computer software documentation," and constitutes acceptance of the rights and restrictions herein.

Identified Components; Additional Terms.The Software may contain or be delivered with one or more components, which may include third-party components, identified by Cisco in the Documentation, readme.txt file, third-party click-accept or elsewhere (e.g. on www.cisco.com) (the "Identified Component(s)") as being subject to different license agreement terms, disclaimers of warranties, limited warranties or other terms and conditions (collectively, "Additional Terms") than those set forth herein.You agree to the applicable Additional Terms for any such Identified Component(s)."

Limited Warranty

Subject to the limitations and conditions set forth herein, Cisco warrants that commencing from the date of shipment to Customer (but in case of resale by an Approved Source other than Cisco, commencing not more than ninety (90) days after original shipment by Cisco), and continuing for a period of the longer of (a) ninety (90) days or (b) the warranty period (if any) expressly set forth as applicable specifically to software in the warranty card accompanying the product of which the Software is a part (the "Product") (if any): (a) the media on which the Software is furnished will be free of defects in materials and workmanship under normal use; and (b) the Software substantially conforms to the Documentation.The date of shipment of a Product by Cisco is set forth on the packaging material in which the Product is shipped.Except for the foregoing, the Software is provided "AS IS".This limited warranty extends only to the Software purchased from an Approved Source by a Customer who is the first registered end user.Customer's sole and exclusive remedy and the entire liability of Cisco and its suppliers under this limited warranty will be (i) replacement of defective media and/or (ii) at Cisco's option, repair, replacement, or refund of the purchase price of the Software, in both cases subject to the condition that any error or defect constituting a breach of this limited warranty is reported to the Approved Source supplying the Software to Customer, within the warranty period.Cisco or the Approved Source supplying the Software to Customer may, at its option, require return of the Software and/or Documentation as a condition to the remedy.In no event does Cisco warrant that the Software is error free or that Customer will be able to operate the Software without problems or interruptions.In addition, due to the continual development of new techniques for intruding upon and attacking networks, Cisco does not warrant that the Software or any equipment, system or network on which the Software is used will be free of vulnerability to intrusion or attack.

Restrictions.This warranty does not apply if the Software, Product or any other equipment upon which the Software is authorized to be used (a) has been altered, except by Cisco or its authorized representative, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Cisco, (c) has been subjected to abnormal physical or electrical stress, abnormal environmental conditions, misuse, negligence, or accident; or (d) is licensed for beta, evaluation, testing or demonstration purposes.The Software warranty also does not apply to (e) any temporary Software modules; (f) any Software not posted on Cisco's Software Center; (g) any Software that Cisco expressly provides on an "AS IS" basis on Cisco's Software Center; (h) any Software for which an Approved Source does not receive a license fee; and (i) Software supplied by any third party which is not an Approved Source.

DISCLAIMER OF WARRANTY

EXCEPT AS SPECIFIED IN THIS WARRANTY SECTION, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, SATISFACTORY QUALITY, NON-INTERFERENCE, ACCURACY OF INFORMATIONAL CONTENT, OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW AND ARE EXPRESSLY DISCLAIMED BY CISCO, ITS SUPPLIERS AND LICENSORS.TO THE EXTENT THAT ANY OF THE SAME CANNOT BE EXCLUDED, SUCH IMPLIED CONDITION, REPRESENTATION AND/OR WARRANTY IS LIMITED IN DURATION TO THE EXPRESS WARRANTY PERIOD REFERRED TO IN THE "LIMITED WARRANTY" SECTION ABOVE.BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY IN SUCH STATES.THIS WARRANTY GIVES CUSTOMER SPECIFIC LEGAL RIGHTS, AND CUSTOMER MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. This disclaimer and exclusion shall apply even if the express warranty set forth above fails of its essential purpose.

Disclaimer of Liabilities - Limitation of Liability.IF YOU ACQUIRED THE SOFTWARE IN THE UNITED STATES, LATIN AMERICA, CANADA, JAPAN OR THE CARIBBEAN, NOTWITHSTANDING ANYTHING ELSE IN THE AGREEMENT TO THE CONTRARY, ALL LIABILITY OF CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS COLLECTIVELY, TO CUSTOMER, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), BREACH OF WARRANTY OR OTHERWISE, SHALL NOT EXCEED THE PRICE PAID BY CUSTOMER TO ANY APPROVED SOURCE FOR THE SOFTWARE THAT GAVE RISE TO THE CLAIM OR IF THE SOFTWARE IS PART OF ANOTHER PRODUCT, THE PRICE PAID FOR SUCH OTHER PRODUCT.THIS LIMITATION OF LIABILITY FOR SOFTWARE IS CUMULATIVE AND NOT PER INCIDENT (I.E. THE EXISTENCE OF TWO OR MORE CLAIMS WILL NOT ENLARGE THIS LIMIT).

IF YOU ACQUIRED THE SOFTWARE IN EUROPE, THE MIDDLE EAST, AFRICA, ASIA OR OCEANIA, NOTWITHSTANDING ANYTHING ELSE IN THE AGREEMENT TO THE CONTRARY, ALL LIABILITY OF CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS COLLECTIVELY, TO CUSTOMER, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), BREACH OF WARRANTY OR OTHERWISE, SHALL NOT EXCEED THE PRICE PAID BY CUSTOMER TO CISCO FOR THE SOFTWARE THAT GAVE RISE TO THE CLAIM OR IF THE SOFTWARE IS PART OF ANOTHER PRODUCT, THE PRICE PAID FOR SUCH OTHER PRODUCT.THIS LIMITATION OF LIABILITY FOR SOFTWARE IS CUMULATIVE AND NOT PER INCIDENT (I.E. THE EXISTENCE OF TWO OR MORE CLAIMS WILL NOT ENLARGE THIS LIMIT).NOTHING IN THE AGREEMENT SHALL LIMIT (I) THE LIABILITY OF CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND

LICENSORS TO CUSTOMER FOR PERSONAL INJURY OR DEATH CAUSED BY THEIR NEGLIGENCE, (II) CISCO'S LIABILITY FOR FRAUDULENT MISREPRESENTATION, OR (III) ANY LIABILITY OF CISCO WHICH CANNOT BE EXCLUDED UNDER APPLICABLE LAW.

Disclaimer of Liabilities - Waiver of Consequential Damages and Other Losses.IF YOU ACQUIRED THE SOFTWARE IN THE UNITED STATES, LATIN AMERICA, THE CARIBBEAN OR CANADA, REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE OR OTHERWISE, IN NO EVENT WILL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR LOST OR DAMAGED DATA, BUSINESS INTERRUPTION, LOSS OF CAPITAL, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY OR WHETHER ARISING OUT OF THE USE OF OR INABILITY TO USE SOFTWARE OR OTHERWISE AND EVEN IF CISCO OR ITS SUPPLIERS OR LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

IF YOU ACQUIRED THE SOFTWARE IN JAPAN, EXCEPT FOR LIABILITY ARISING OUT OF OR IN CONNECTION WITH DEATH OR PERSONAL INJURY, FRAUDULENT MISREPRESENTATION, AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE OR OTHERWISE, IN NO EVENT WILL CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR LOST OR DAMAGED DATA, BUSINESS INTERRUPTION, LOSS OF CAPITAL, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY OR WHETHER ARISING OUT OF THE USE OF OR INABILITY TO USE SOFTWARE OR OTHERWISE AND EVEN IF CISCO OR ANY APPROVED SOURCE OR THEIR SUPPLIERS OR LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IF YOU ACQUIRED THE SOFTWARE IN EUROPE, THE MIDDLE EAST, AFRICA, ASIA OR OCEANIA, IN NO EVENT WILL CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS, BE LIABLE FOR ANY LOST REVENUE, LOST PROFIT, OR LOST OR DAMAGED DATA, BUSINESS INTERRUPTION, LOSS OF CAPITAL, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES, HOWSOEVER ARISING, INCLUDING, WITHOUT LIMITATION, IN CONTRACT, TORT (INCLUDING NEGLIGENCE) OR WHETHER ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF, IN EACH CASE, CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS, HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT FULLY APPLY TO YOU.THE FOREGOING EXCLUSION SHALL NOT APPLY TO ANY LIABILITY ARISING OUT OF OR IN CONNECTION WITH: (I) DEATH OR PERSONAL INJURY, (II) FRAUDULENT MISREPRESENTATION, OR (III) CISCO'S LIABILITY IN CONNECTION WITH ANY TERMS THAT CANNOT BE EXCLUDED UNDER APPLICABLE LAW.

Customer acknowledges and agrees that Cisco has set its prices and entered into the Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the parties.

Controlling Law, Jurisdiction.If you acquired, by reference to the address on the purchase order accepted by the Approved Source, the Software in the United States, Latin America, or the Caribbean, the Agreement and warranties ("Warranties") are controlled by and construed under the laws of the State

of California, United States of America, notwithstanding any conflicts of law provisions; and the state and federal courts of California shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties.If you acquired the Software in Canada, unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of the Province of Ontario, Canada, notwithstanding any conflicts of law provisions; and the courts of the Province of Ontario shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties.If you acquired the Software in Europe, the Middle East, Africa, Asia or Oceania (excluding Australia), unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of England, notwithstanding any conflicts of law provisions; and the English courts shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties.In addition, if the Agreement is controlled by the laws of England, no person who is not a party to the Agreement shall be entitled to enforce or take the benefit of any of its terms under the Contracts (Rights of Third Parties) Act 1999.If you acquired the Software in Japan, unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of Japan, notwithstanding any conflicts of law provisions; and the Tokyo District Court of Japan shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties.If you acquired the Software in Australia, unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of the State of New South Wales, Australia, notwithstanding any conflicts of law provisions; and the State and federal courts of New South Wales shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties.If you acquired the Software in any other country, unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of the State of California, United States of America, notwithstanding any conflicts of law provisions; and the state and federal courts of California shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties.

For all countries referred to above, the parties specifically disclaim the application of the UN Convention on Contracts for the International Sale of Goods.Notwithstanding the foregoing, either party may seek interim injunctive relief in any court of appropriate jurisdiction with respect to any alleged breach of such party's intellectual property or proprietary rights.If any portion hereof is found to be void or unenforceable, the remaining provisions of the Agreement and Warranties shall remain in full force and effect.Except as expressly provided herein, the Agreement constitutes the entire agreement between the parties with respect to the license of the Software and Documentation and supersedes any conflicting or additional terms contained in any Purchase Order or elsewhere, all of which terms are excluded.The Agreement has been written in the English language, and the parties agree that the English version will govern.

Product warranty terms and other information applicable to Cisco products are available at the following URL:

http://www.cisco.com/go/warranty

Supplemental End User License Agreement for Cisco Systems Content Security Software

IMPORTANT: READ CAREFULLY

This Supplemental End User License Agreement ("SEULA") contains additional terms and conditions for the Software product licensed under the End User License Agreement ("EULA") between You ("You" as used herein means You and the business entity you represent or "Company") and Cisco (collectively, the "Agreement").Capitalized terms used in this SEULA but not defined will have the meanings assigned to them in the EULA.To the extent that there is a conflict between the terms and conditions of the EULA and this SEULA, the terms and conditions of this SEULA will take precedence.

In addition to the limitations set forth in the EULA on your access and use of the Software, you agree to comply at all times with the terms and conditions provided in this SEULA.

DOWNLOADING, INSTALLING, OR USING THE SOFTWARE CONSTITUTES ACCEPTANCE OF THE AGREEMENT, AND YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT TO THE AGREEMENT.IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED CD PACKAGE AND ANY WRITTEN MATERIALS) FOR A FULL REFUND, OR, IF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND.YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM CISCO OR AN AUTHORIZED CISCO RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL END USER PURCHASER.

For purposes of this SEULA, the Product name and the Product description You have ordered is any of the following Cisco Systems Email Security Appliance ("ESA"), Cisco Systems Web Security Appliance ("WSA") and Cisco Systems Security Management Application ("SMA") (collectively, "Content Security") and their Virtual Appliance equivalent ("Software"):

Cisco AsyncOS for Email

Cisco AsyncOS for Web

Cisco AsyncOS for Management

Cisco Email Anti-Spam, Sophos Anti-Virus

Cisco Email Outbreak Filters

Cloudmark Anti-Spam

Cisco Image Analyzer

McAfee Anti-Virus

Cisco Intelligent Multi-Scan

Cisco RSA Data Loss Prevention

Cisco Email Encryption

Cisco Email Delivery Mode

Cisco Web Usage Controls

Cisco Web Reputation

Sophos Anti-Malware

Webroot Anti-Malware

McAfee Anti-Malware

Cisco Email Reporting

Cisco Email Message Tracking

Cisco Email Centralized Quarantine

Cisco Web Reporting

Cisco Web Policy and Configuration Management

Cisco Advanced Web Security Management with Splunk

Email Encryption for Encryption Appliances

Email Encryption for System Generated Bulk Email

Email Encryption and Public Key Encryption for Encryption Appliances

Large Attachment Handling for Encryption Appliances

Secure Mailbox License for Encryption Appliances

Definitions

For purposes of this SEULA, the following definitions apply:

"Company Service" means the Company's email, Internet, security management services provided to End Users for the purposes of conducting Company's internal business.

"End User" means: (1) for the WSA and SMA, the employee, contractor or other agent authorized by Company to access the Internet and the SMA via the Company Service; and (2) for the ESA, the email boxes of the employees, contractors, or other agent authorized by Company to access or use the email services via the Company Service.

"Ordering Document" means the purchase agreement, evaluation agreement, beta, pre-release agreement or similar agreement between the Company and Cisco or the Company and a Cisco reseller, or the valid terms of any purchase order accepted by Cisco in connection therewith, containing the purchase terms for the Software license granted by this Agreement.

"Personally Identifiable Information" means any information that can be used to identify an individual, including, but not limited to, an individual's name, user name, email address and any other personally identifiable information.

"Server" means a single physical computer or devices on a network that manages or provides network resources for multiple users.

"Services" means Cisco Software Subscription Services.

"Service Description" means the description of the Software Subscription Support Services at http://www.cisco.com/web/about/doing_business/legal/service_descriptions/index.html

"Telemetry Data" means samples of Company's email and web traffic, including data on email message and web request attributes and information on how different types of email messages and web requests were handled by Company's Cisco hardware products.Email message metadata and web requests included in Telemetry Data are anonymized and obfuscated to remove any Personally Identifiable Information.

"Term" means the length of the Software subscription You purchased, as indicated in your Ordering Document.

"Virtual Appliance" means the virtual version of Cisco's email security appliances, web security appliances, and security management appliances.

"Virtual Machine" means a software container that can run its own operating system and execute applications like a Server.

Additional License Terms and Conditions

LICENSE GRANTS AND CONSENT TO TERMS OF DATA COLLECTION

License of Software.

By using the Software and the Documentation, Company agrees to be bound by the terms of this Agreement, and so long as Company is in compliance with this Agreement, Cisco hereby grants to Company a nonexclusive, non-sublicensable, non-transferable, worldwide license during the Term to use the Software only on Cisco's hardware products, or in the case of the Virtual Appliances, on a Virtual Machine, solely in connection with the provision of the Company Service to End Users.The number of End Users licensed for the use of the Software is limited to the number of End Users specified in the Ordering Documents.In the event that the number of End Users in connection with the provision of the

Company Service exceeds the number of End Users specified in the Ordering Documents, Company shall contact an Approved Source to purchase additional licenses for the Software.The duration and scope of this license(s) is further defined in the Ordering Document.The Ordering Document supersedes the EULA with respect to the term of the Software license.Except for the license rights granted herein, no right, title or interest in any Software is granted to the Company by Cisco, Cisco's resellers or their respective licensors.Your entitlement to Upgrades to the Software is subject to the Service Description.This Agreement and the Services are co-terminus.

Consent and License to Use Data.

Subject to the Cisco Privacy Statement at http://www.cisco.com/web/siteassets/legal/privacy.html, Company hereby consents and grants to Cisco a license to collect and use Telemetry Data from the Company.Cisco does not collect or use Personally Identifiable Information in the Telemetry Data.Cisco may share aggregated and anonymous Telemetry Data with third parties to assist us in improving your user experience and the Software and other Cisco security products and services.Company may terminate Cisco's right to collect Telemetry Data at any time by disabling SenderBase Network Participation in the Software.Instructions to enable or disable SenderBase Network Participation are available in the Software configuration guide.

Description of Other Rights and Obligations

Please refer to the Cisco Systems, Inc. End User License Agreement, Privacy Statement and Service Description of Software Subscription Support Services.

INDEX

記号

A

C

D

F

G

H

I

L

M

N

O

P

R

S

T

U

W

X

あ

い

う

え

お

か

き

く

け

こ

さ

し

す

せ

そ

た

ち

つ

て

ろ

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/