AsyncOS 9.0 for Cisco Content Security Management Appliances ユーザ ガイド

２０１６ 年３月 ９ 日

Cisco Systems, Inc.
www.cisco.com

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

Text Part Number: N/A

CONTENTS

概要

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/c/en/us/support/security/content-security-management-appliance/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
仮想フォーム ファクタ	今回の Cisco コンテンツ セキュリティ管理仮想アプライアンス リリースは、電子メール セキュリティ アプライアンスをサポートします。 詳細については、『*Cisco Content Security Virtual Appliance Installation Guide*』（http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-installation-guides-list.html）を参照してください。
ディスク領域の管理の改善	• スパム隔離のサイズ制限が削除されました。 • 仮想アプライアンスでは、VMware ツールを使用してセキュリティ管理アプライアンスのインスタンスに利用できるディスク領域を拡張できます。2 TB を超える単一のパーティションがサポートされるようになりました。 既存の仮想アプライアンスをアップグレードする場合は、リリース ノートの「Upgrading a Virtual Appliance」に記載された重要な注意事項を参照してください。 • クォータ（その他のファイル）が追加されて、ログ ファイル、パケット キャプチャ、コンフィギュレーション ファイルに使用される領域を管理できるようになりました。 詳細については、ディスク領域の管理（14-53 ページ）を参照してください。

機能	説明
中央集中型ファイル分析の隔離	ファイル分析用に、送信されたファイルを Cisco コンテンツ セキュリティ管理アプライアンスで隔離できるようになりました。ただし電子メール セキュリティ アプライアンスとは異なり、この隔離ではファイル分析の判定に基づいて自動的にメッセージがリリースされることはありません。代わりに、指定した保持期間の間メッセージが保持されます。 この隔離は、本リリースへのアップグレード時に自動的に作成されます。「ポリシー、ウイルス、アウトブレイク隔離」と呼ばれる隔離グループの 1 つで、全般設定および動作はそれらの隔離と同じです。 詳細については、中央集中型ファイル分析隔離について（8-17 ページ）を参照してください。
アプライアンス管理者向けメッセージの表示	管理ユーザがアプライアンスにログインするときに表示するメッセージを作成できます。 現在、この機能はコマンドライン インターフェイス（CLI）を使用した場合にのみ利用できます。詳細については、管理ユーザ向けメッセージの表示（13-26 ページ）を参照してください。
アプライアンスへの最近のログインの表示	クレデンシャルを使用したアプライアンスへの最近のアクセス試行に関するショート リストを表示できます。 最近のログイン試行の表示（13-27 ページ）を参照してください。
ユーザ別のスパム通知	LDAP グループに基づいてスパム通知を受信するユーザを指定できます。
新機能のレポーティングおよびトラッキング	レポーティングおよびトラッキングが更新され、AsyncOS 9.0 for Cisco 電子メール セキュリティ アプライアンス の新機能をサポートするようになりました
新しいパスワード変更オプション	パスワード要件を変更した後など、手動でパスワード変更を要求する場合は、ユーザに強制するパスワード変更のタイミングを次回ログイン時にするか指定した期間後にするかを選択できます。 指定した期間後のパスワード変更を適用する場合は、パスワードの有効期限が切れてからパスワードをリセットするまでの猶予期間を設定できます。 スケジュール設定したパスワード変更の猶予期間も指定できます。
コンフィギュレーション ファイルのインポート	アプライアンス間の設定の移行を簡素化するコンフィギュレーション ファイルをインポートするときに、ネットワーク設定およびディスク クォータ設定を無視するように選択できるようになりました。 この機能は、AsyncOS 8.4 for Cisco Content Security Management Appliances（Web セキュリティ アプライアンスのみをサポート）でも利用できます。

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ーフェイスを提供します。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関するレポートを実行します。個々の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利用できます。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。
- **Web セキュリティ アプライアンスの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、複数の Web セキュリティ アプライアンスを対象にポリシー定義とポリシー導入を管理します。

（注） セキュリティ管理アプライアンスは、中央集中型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」とは関係ありません。

- **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。

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	詳細情報
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（2-2 ページ）
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	詳細情報
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。	『AsyncOS for Cisco Web Security Appliances 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」セクション（2-2 ページ）、「セットアップの準備」セクション（2-4 ページ）、および「システム セットアップ ウィザードの実行」セクション（2-8 ページ）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」セクション（2-14 ページ）から開始します。

SMA 互換性マトリクス

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 アプライアンスとのセキュリティ管理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コンフィギュレーション ファイルの互換性については、互換性マトリクス（http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-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（2-2 ページ）
- 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（2-3 ページ）
- クラスタ化された電子メール セキュリティ アプライアンスを使用した展開（2-4 ページ）

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

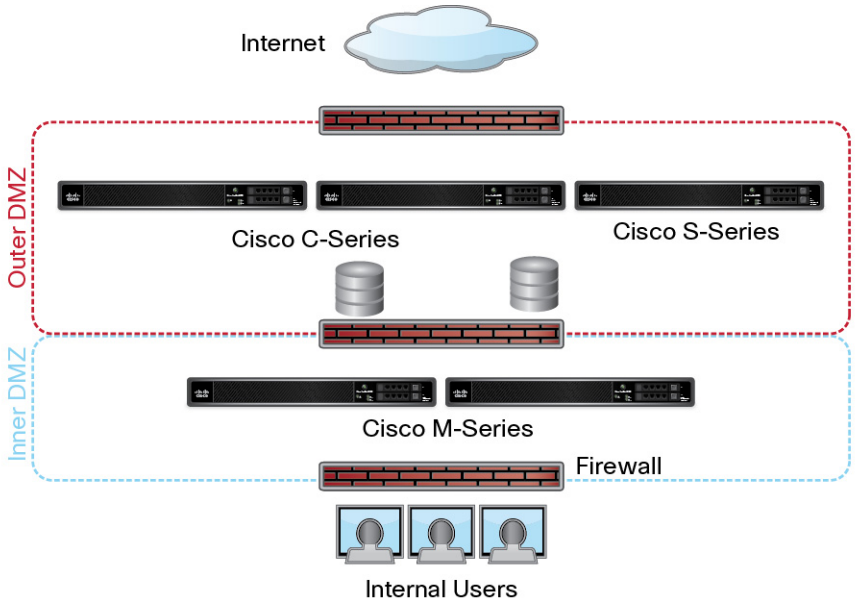


図 2-1 に、セキュリティ管理アプライアンスと複数の DMZ を含む一般的なネットワーク設定を示します。内部ネットワークで、DMZ の外側に セキュリティ管理アプライアンスを導入します。すべての接続は、セキュリティ管理アプライアンス（M シリーズ）から開始され、管理 電子メール セキュリティ アプライアンス（C シリーズ）および管理 Web セキュリティ アプライアンス（S シリーズ）で終わります。

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て、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とメッセージ 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。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こともできます。

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、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 マニュアルまたはオンライン ヘルプで、「Centralizing Services on a Cisco Content Security Management Appliance」の章を参照してください。

クラスタ化された電子メール セキュリティ アプライアンスを使用した展開

電子メール アプライアンスの中央集中型管理機能を使用する電子メール セキュリティ アプライアンスのクラスタに、セキュリティ管理アプライアンスを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て隔離できます。

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。

手順

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（E-1 ページ）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（2-2 ページ）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（2-2 ページ）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（2-4 ページ）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（2-4 ページ）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（2-5 ページ）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 アドレスと IP アドレスの割り当て」を参照してください。

（注） インターネットとコンテンツ 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電子メール メッセージの送受信には、セキュリティ管理アプライアンスで常に同じ IP アドレスを使用してください。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のメール フローに関する情報を参照してください。

Cisco コンテンツ セキュリティ管理アプライアンスとその管理対象アプライアンス間の通信では、IPv6 はサポートされていません。

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 アドレスと 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		AutoSupport を有効にする___ 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(2-6 ページ)
- Web インターフェイスへのアクセスについて(2-7 ページ)
- Web インターフェイスへのアクセス(2-7 ページ)
- コマンドライン インターフェイスへのアクセス(2-8 ページ)
- サポートされる言語(2-8 ページ)

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	—	—
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。スパム隔離 HTTPS インターフェイスを有効にすると、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 を介して管理者 Web インターフェイスにアクセスし、次に同じブラウザでポート 83 の HTTPS を介してスパム隔離エンド ユーザ Web インターフェイスにアクセスした場合、管理者 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（13-24 ページ）を参照してください。

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**

（注） Web インターフェイスまたはコマンドライン インターフェイスのいずれを使用した場合も、システム セットアップ ウィザードの完了後は、このパスワードは無効です。

コマンドライン インターフェイスへのアクセス

セキュリティ管理アプライアンスでコマンドライン インターフェイス（CLI）にアクセスする方法は、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 アクセスと同じですが、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リストについては、シスコ コンテンツ セキュリティ アプライアンスの『*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（14-58 ページ）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」セクション（2-4 ページ）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、この工場出荷時のデフォルト設定と競合していないことを確認してください。**

（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（13-24 ページ）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（13-24 ページ）を参照してください。

システム セットアップ ウィザードの概要

手順

ステップ 1　システム セットアップ ウィザードの起動（2-10 ページ）

ステップ 2　エンド ユーザ ライセンス契約書の確認（2-10 ページ）

ステップ 3　システムの設定（2-10 ページ）

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

ステップ 4　ネットワークの設定（2-11 ページ）

- 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 5　設定の確認（2-12 ページ）

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。

ステップ 6　次の手順（2-12 ページ）

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」セクション（2-7 ページ）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」セクション（14-34 ページ）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す。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」セクション（14-45 ページ）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」セクション（14-45 ページ）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」セクション（3-2 ページ）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。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 の有効化

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 AutoSupport」セクション（14-36 ページ）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（Network Settings）

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」セクション（14-41 ページ）を参照してください。

（注）　アプライアンスでは、着信接続のための DNS ルックアップを実行するために、稼働中の DNS サーバ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、[インターネット ルート DNS サーバを使用（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（2-1 ページ）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（2-2 ページ）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（4-3 ページ）
- 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（6-3 ページ）
- 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（7-4 ページ）
- 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（8-5 ページ）
- 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（5-4 ページ）
- 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（9-5 ページ）

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。

[セキュリティアプライアンス（Security Appliances）] ページ

- 管理対象アプライアンスの追加について（2-12 ページ）
- 管理対象アプライアンス設定の編集（2-13 ページ）
- 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（2-14 ページ）
- 管理対象アプライアンスの設定ステータスの表示（10-5 ページ）
- 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（8-8 ページ）

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「スパム隔離」
- 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(14-50 ページ)

CHAPTER 3

レポートの操作

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（3-3 ページ） • 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（4-45 ページ） • Web レポートのスケジュール設定（5-38 ページ）

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
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（4-48 ページ） • オンデマンドでの Web レポートの生成（5-42 ページ）。
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（3-10 ページ） • 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（3-12 ページ）
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（3-10 ページ）
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（4-48 ページ） • 電子メール レポートのスケジュール設定（4-45 ページ） • オンデマンドでの Web レポートの生成（5-42 ページ）。 • Web レポートのスケジュール設定（5-38 ページ）
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	アーカイブ済みの Web レポートの表示と管理（5-43 ページ）
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（3-9 ページ）

（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（15-1 ページ）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」セクション（14-45 ページ）を参照してください。

データには、IPv4 と IPv6 の両方に関係するトランザクションが含まれます。

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
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ローカル レポーティング	•	•	•	•	•	
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（3-4 ページ）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（3-5 ページ）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（3-6 ページ）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（3-6 ページ）を参照してください

目的	操作内容
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（4-6 ページ）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（14-58 ページ）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（3-7 ページ）を参照してください。

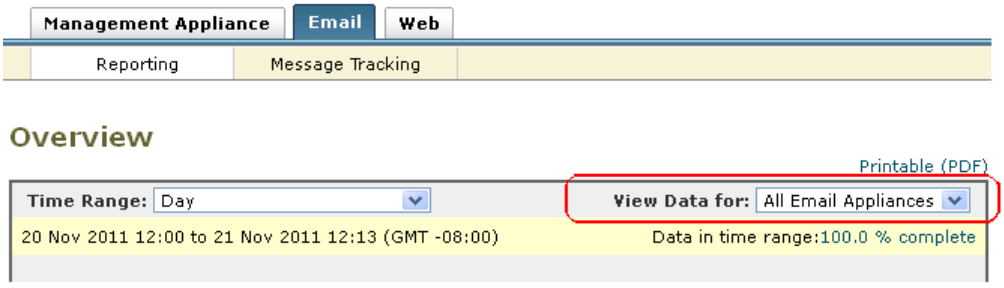
（注）　すべてのレポートにすべてのカスタマイズ機能を使用できるわけではありません。

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、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 レポーティング グループの作成（4-4 ページ）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
時間（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）	その月の最初の日の 00:00 ～その月の最後の日の 23:59	•	•	•	
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く日付および時刻情報が、グリニッジ標準時（GMT）オフセットで表示されます。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（14-58 ページ）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。

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	詳細情報
• 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。 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（4-10 ページ）も参照してください。
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	列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（14-58 ページ）を参照してください。

表 3-4　Web レポート ページのテーブルのカスタマイズ（続き）

目的	操作内容	詳細情報
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（3-9 ページ）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レポート（Web Reporting）] ページの説明（5-6 ページ）を参照してください。

カスタム レポート

ユーザは、既存のレポート 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 ページおよびカスタム Web セキュリティ レポート ページを作成できます。

目的	操作内容
カスタム レポート ページにモジュールを追加する。	参照先： • カスタム レポートに追加できないモジュール（3-8 ページ）。 • カスタム レポート ページの作成（3-8 ページ）
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. 表示する時間範囲を選択します。選択した時間範囲は [マイレポート（My Reports）] ページのすべてのモジュールを含むすべてのレポートに適用されます。 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 ページでのモジュールの再配置	目的の場所にモジュールをドラッグ アンド ドロップします。
カスタム レポート ページからのモジュールの削除	モジュールの右上にある [X] をクリックします。
カスタム レポートの PDF または CSV バージョンの生成	参照先： • オンデマンドでの電子メール レポートの生成（4-48 ページ） • オンデマンドでの Web レポートの生成（5-42 ページ）
カスタム レポートの PDF または CSV バージョンの定期的な生成	参照先： • 電子メール レポートのスケジュール設定（4-45 ページ） • Web レポートのスケジュール設定（5-38 ページ）

カスタム レポートに追加できないモジュール

- [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）] 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（Sender Profile）] 詳細レポート ページの、[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
- Web トラッキング検索結果を含む検索結果

カスタム レポート ページの作成

はじめる前に

- 追加するモジュールが追加可能であることを確認します。カスタム レポートに追加できないモジュール（3-8 ページ）を参照してください。
- 不要なデフォルト モジュールを削除するには、そのモジュールの右上にある [X] をクリックします。

手順

ステップ 1　次のいずれかの方法を使用して、カスタム レポート ページにモジュールを追加します。

（注） モジュールによっては、使用できる方法が 1 つのみである場合があります。ある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。

- [メール（Email）] タブまたは [Web] タブで、追加するモジュールを含むレポート ページに移動して、モジュールの上部にある [+] 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、**[+]**ボタンをクリックして、追加するレポート モジュールを選択します。

各モジュールは一度だけ追加できます。すでに特定のモジュールをレポートに追加している場合は、追加オプションが利用できなくなっています。

ステップ 2　カスタマイズした（たとえば、カラムの追加、削除、並べ替えや、チャートのデフォルト以外のデータの表示など）モジュールを追加する場合は、[マイレポート（My Reports）] ページでモジュールをカスタマイズします。

モジュールがデフォルト設定に追加されます。元のモジュールの時間範囲は保持されません。

ステップ 3　別に凡例を持つチャート（たとえば、[概要（Overview）] ページからのグラフ）を追加する場合は、別途凡例を追加します。必要に応じて、説明するデータの隣にドラッグ アンド ドロップします。

レポート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。

(一部のテーブルにのみ、これらのリンクはあります)。

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。

関連項目

- 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)(5-44 ページ)

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。

  - 内部ユーザ
  - Internal User Details
  - IP Addresses for Outgoing Senders
  - コンテンツ フィルタ

- **[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	注記
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。 参照先: • オンデマンドでの電子メール レポートの生成(4-48 ページ) • 電子メール レポートのスケジュール設定(4-45 ページ) • オンデマンドでの Web レポートの生成(5-42 ページ)。 • Web レポートのスケジュール設定(5-38 ページ)	—

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	注記
raw データ		•	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。
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（3-12 ページ）も参照してください。		•	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。参照先： • オンデマンドでの電子メール レポートの生成（4-48 ページ） • 電子メール レポートのスケジュール設定（4-45 ページ） • オンデマンドでの Web レポートの生成（5-42 ページ）。 • Web レポートのスケジュール設定（5-38 ページ）	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。
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、または韓国語の PDF を生成するには、Adobe.com から該当するフォント パックを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ことも必要です。
（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。

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	注記
（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（3-10 ページ）を参照してください。

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

表 3-6　raw データ エントリの表示（続き）

カテゴリ ヘッダー	値	説明
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。この問題を回避するには、ローカル マシンにファイルを保存し、[File] > [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でのサブドメインとセカンドレベル ドメイン

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。

すべてのレポートのトラブルシューティング

- バックアップ セキュリティ管理アプライアンスのレポート データを表示できない（3-14 ページ）
- レポーティングがディセーブルになっている（3-14 ページ）

関連項目：

- 電子メール レポートのトラブルシューティング（4-50 ページ）
- Web レポーティングおよびトラッキングのトラブルシューティング（5-52 ページ）

バックアップ セキュリティ管理アプライアンスのレポート データを表示できない

問題　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 アプライアンスを 1 つ選択してそのレポート データを表示することはできません。[データ参照（View Data For）] オプションはレポート ページには表示されません。

ソリューション　[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、中央で管理されている各アプライアンスを追加します（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）。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（3-4 ページ）を参照してください。

バックアップ中のサービスのアベイラビリティ（14-10 ページ）も参照してください。

レポーティングがディセーブルになっている

問題　進行中のバックアップをキャンセルすると、レポーティングがディセーブルになる場合があります。

ソリューション　レポーティング機能は、バックアップが完了すると回復します。

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

Cisco 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 リスクをモニタできるように、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。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。

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一元化されます。

中央集中型電子メール レポーティング機能では、全体的な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有効にした場合、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 レポーティングが有効でない場合、生成されるレポートはシステム ステータスとシステム キャパシティ関連に限定されます。

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 アプライアンスのマニュアルまたはオンライン ヘルプの「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 レポーティングの有効化（4-2 ページ）。
- 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（4-3 ページ）。
- 電子メール レポーティング グループの作成（4-4 ページ）
- 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 レポーティングの有効化（4-5 ページ）

（注） レポーティングとトラッキングを常に同時に有効にせず、かつそれらが適切に機能していない場合、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ていない場合は、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と、予想した結果は一致しません。これは、各機能（レポーティング、トラッキング）のデータが、その機能が有効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 レポーティングの有効化

はじめる前に

- 中央集中型レポーティングを有効にする前に、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 レポーティングを有効にする前に、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。「ディスク領域の管理」セクション（14-53 ページ）

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。

(注)　アプライアンスで電子メール レポーティングが有効になっていて、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、「ディスク領域の管理」セクション(14-53 ページ)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ます。

ステップ 6　変更を保存します。

電子メール レポーティング 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有効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（4-3 ページ）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　[グループの追加（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 リストに、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ても、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、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 レポーティングの有効化

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 レポーティングを有効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 アプライアンスのマニュアルまたはオンライン ヘルプで、「Configuring an Email Security Appliance to Use Centralized Reporting」のセクション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」セクション(3-1 ページ)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には、レポート データのビューのカスタマイズ(3-3 ページ)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(4-6 ページ)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(3-10 ページ)を参照してください。
- 各種インタラクティブ レポート ページについては、[メールレポート(Email Reporting)] ページの概要(4-6 ページ)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(4-48 ページ)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(4-45 ページ)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 メールレポート(Archived Email Reports)] の表示と管理(4-49 ページ)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(3-2 ページ)を参照してください。
- 大量のデータを処理する場合の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」セクション(3-9 ページ)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、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(許可されている場合)。この場合、メッセージ トラッキングで関連する検索が実行されます。下にスクロールして結果を表示します。

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
- 内部送信者ドメイン
- 内部送信者 IP アドレス
- 受信 TLS ドメイン
- 送信 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、Classless Inter-Domain Routing（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

（注） このリストは、AsyncOS for 電子メール セキュリティ アプライアンス の最新のサポート対象リリースで使用可能なレポートを示しています。電子メール セキュリティ アプライアンスで AsyncOS の以前のリリースを実行している場合、これらすべてのレポートを使用できるわけではありません。

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	操作
[電子メールレポーティングの概要（Email Reporting Overview）] ページ	[概要（Overview）] ページには、電子メール セキュリティ アプライアンスでのアクティビティの概要が表示されます。概要には、送受信メッセージに関するグラフおよび要約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（Email Reporting Overview）] ページ」セクション（4-13 ページ）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しているすべてのリモート ホストのリアルタイム情報に関するインタラクティブ レポートが表示されます。システムに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」セクション（4-16 ページ）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	[送信者グループ（Sender Groups）] レポート ページには、送信者グループ別およびメール フロー ポリシー アクション別に接続の要約が表示され、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ます。 詳細については、「[受信メール（Incoming Mail）] ページ」セクション（4-16 ページ）を参照してください。
[送信先（Outgoing Destinations）] ページ	[送信先（Outgoing Destinations）] ページには、組織がメールを送信する宛先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、送信脅威メッセージ別の上位の宛先、および送信クリーン 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、カラムが総受信者数別にソートされた（デフォルト設定）チャートが表示されます。 詳細については、「[送信先（Outgoing Destinations）] ページ」セクション（4-22 ページ）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」セクション（4-23 ページ）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	操作
[内部ユーザ（Internal Users）] ページ	[内部ユーザ（Internal Users）] には、内部ユーザによって送受信されたメールについての情報が*電子メール アドレス*ごとに表示されます。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 アドレスは結合されません。 詳細については、「[内部ユーザ（Internal Users）] ページ」セクション（4-24 ページ）を参照してください。
DLP インシデント（DLP Incidents）	[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）ポリシー違反のインシデントに関する情報が表示されます。 詳細については、「DLP インシデント（DLP Incidents）」セクション（4-26 ページ）を参照してください。
メッセージフィルタ（Message Filters）	[メッセージフィルタ（Message Filters）] ページには、送受信メッセージのメッセージ フィルタの上位一致（最も多くのメッセージに一致したメッセージ フィルタ）に関する情報が表示されます。
大容量のメール（High Volume Mail）	[大容量のメール（High Volume Mail）] ページでは、1 人の送信者から送られていたり、件名が同じであったりする、特定の 1 時間の間に送られた多数のメッセージに関係する攻撃が特定されます。 詳細については、「大容量のメール（High Volume Mail）」セクション（4-28 ページ）を参照してください。
[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」セクション（4-28 ページ）を参照してください。
DMARC 検証（DMARC Verification）	[DMARC 検証（DMARC Verification）] ページには、Domain-based Message Authentication, Reporting and Conformance（DMARC）検証に失敗した上位送信者のドメイン、および各ドメインからの受信メッセージに対して実行されたアクションの要約が表示されます。 詳細については、「DMARC 検証（DMARC Verification）」セクション（4-29 ページ）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	操作
[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するウイルス スキャン エンジンによって検出され、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」セクション（4-29 ページ）を参照してください。
[URLフィルタリング（URL Filtering）] ページ	メッセージ内で最も頻繁に使用される URL カテゴリ、スパム メッセージ内の最も一般的な URL、メッセージに表示される悪意のある URL および疑わしい URL の数を確認するには、このページを使用します。 詳細については、「[URLフィルタリング（URL Filtering）] ページ」セクション（4-30 ページ）を参照してください。
[高度なマルウェア防御（ファイルレピュテーション）（Advanced Malware Protection (File Reputation)）] および [高度なマルウェア防御（ファイル分析）（Advanced Malware Protection (File Analysis)）] レポート ページ	ファイル レピュテーションおよび分析データは 3 つのレポーティング ページに表示されます。 詳細については、「[高度なマルウェア防御（ファイルレピュテーション）（Advanced Malware Protection (File Reputation)）] および [高度なマルウェア防御（ファイル分析）（Advanced Malware Protection (File Analysis)）] レポート ページ」セクション（4-31 ページ）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」セクション（4-33 ページ）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」セクション（4-34 ページ）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、最近のアウトブレイク、およびアウトブレイク フィルタによって隔離されたメッセージに関する情報が表示されます。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」セクション（4-36 ページ）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	操作
[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」セクション（4-35 ページ）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」セクション（4-37 ページ）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」セクション（4-40 ページ）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」セクション（4-45 ページ）を参照してください。
[アーカイブ メールレポート（Archived Email Reports）] 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 メールレポート（Archived Email Reports）] の表示と管理」セクション（4-49 ページ）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」セクション（4-48 ページ）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

列名	説明
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。その代わりに、拒否された接続の数は、各時間間隔で最も顕著だった送信者についてのみ維持されます。
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。

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）

列名	説明
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による停止（Stopped by Reputation Filtering）] のコンポーネントです。HAT 上限値（1 時間当たりの最大受信者数、メッセージあたりの最大受信者数、または接続あたりの最大メッセージ数）のいずれかを超えたために、阻止された受信メッセージの数を表します。この値と、拒否されたか、TCP 拒否の接続に関連する受信メッセージの予測値とが合計されて、[レピュテーション フィルタによる停止（Stopped by Reputation Filtering）] が算出されます。
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「数が絞り込まれた」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。その代わりに、拒否された接続の数は、各時間間隔で最も顕著だった送信者についてのみ維持されます。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（レピュテーションにより阻止されたメッセージ、無効な受信者、スパム、およびウイルスとして阻止されたメッセージ）の総数
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。
ユーザ メールフローの詳細（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受信スパム。

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)

列名	説明
受信ウイルス検出(Incoming Virus Detected)	検出された受信ウイルス。
受信コンテンツフィルタの一致数(Incoming Content Filter Matches)	検出された受信コンテンツ 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)	設定したコンテンツ フィルタによって阻止された受信メッセージ。
正常な受信(Incoming Clean)	すべての受信クリーン メッセージ。
送信スパム検出(Outgoing Spam Detected)	検出された送信スパム。
送信ウイルス検出(Outgoing Virus Detected)	検出された送信ウイルス。
送信コンテンツフィルタの一致数(Outgoing Content Filter Matches)	検出された送信コンテンツ 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)	設定したコンテンツ フィルタによって阻止された送信メッセージ。
正常な送信(Outgoing Clean)	すべての送信クリーン メッセージ。
送受信TLS接続(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 接続の総数。
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	
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で発見された時刻。
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)	隔離に関連するメッセージ。

[電子メールレポーティングの概要（Email Reporting 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、送受信メッセージに関するグラフおよび要約テーブルが含まれます。

高レベルの [概要（Overview）] ページには、送受信メールのグラフと送受信メールの要約が表示されます。

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（Email Reporting 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（4-42 ページ）および[エグゼクティブサマリー（Executive Summary）] レポート（4-45 ページ）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含むドロップダウン リスト。詳細については、「レポートの時間範囲の選択」セクション（3-5 ページ）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E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（3-4 ページ）も参照してください。

受信メール メッセージの集計方法

AsyncOS は、メッセージごとの受信者数に応じて受信メールを集計します。たとえば、example.com から 3 人の受信者に送信された受信メッセージは、その送信者からの 3 通のメッセージとして集計されます。

送信者レピュテーション フィルタリングによってブロックされたメッセージは、実際にはワーク キューに入らないので、アプライアンスは、受信メッセージの受信者のリストに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、メッセージがスパムまたはウイルス確実とマークされ、コンテンツ フィルタにも一致することがあります。各種フィルタとスキャン アクティビティの優先順位は、メッセージ処理の結果に大きく影響します。

上記の例では、各種判定は次の優先ルールに従います。

- スパム陽性
- ウイルス陽性
- コンテンツ フィルタとの一致

これらのルールに従って、メッセージがスパム陽性とマークされた場合、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れば、このメッセージがドロップされてスパム 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パイプラインで処理するようにアンチスパム設定が設定されている場合、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、または隔離しても、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。

また、メッセージがアウトブレイク フィルタによって隔離された場合、隔離からリリースされてワーク キューで再度処理されるまで集計されません。

メッセージ処理の優先順位の詳細については、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 ヘルプまたはユーザ ガイドで、電子メール パイプラインに関する章を参照してください。

[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（「受信メール メッセージの集計方法」セクション（4-13 ページ）を参照）を掛け、その値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。
受信者が無効です（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）] カテゴリに集計されます。 • ウイルス スキャン結果が [修復（Repaired）] または [感染している（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集計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。
DMARCによる停止（Stopped by DMARC）	DMARC 検証に失敗し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。
承認された正常なメッセージ（Clean Messages Accepted）	このカテゴリは、承認され、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）を考慮に入れ、承認されたクリーン メッセージを最も正確に表したものです。 ただし、ウイルスまたはスパム確実としてマークされたにもかかわらず配信されたメッセージは集計されないので、実際のメッセージの配信数と、このクリーン メッセージの数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 [メール（Email）] > [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しているすべてのリモート ホストのリアルタイム情報に関するインタラクティブ レポートが表示されます。システムに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、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 テーブルという 2 つの主要なセクションで構成されます。

[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。いずれかの 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）] ページにアクセスするには、[受信メール（Incoming Mail）] ページの上部、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します。

[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メールを送信した送信者の 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（4-6 ページ）を参照）。
- 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」セクション（4-21 ページ）を参照してください。
- アプライアンスにメールを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（送信者レピュテーション 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を分析し、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（SBRS）、ドメインが直近に一致した送信者グループなど、送信者に関する詳細を SenderBase レピュテーション サービスから取得する。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
- ネットワーク所有者（Network Owners）

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、送信者の IP アドレス、ドメイン名、またはネットワーク オーナー情報をクリックすると、特定の送信者プロファイル情報を取得できます。送信者プロファイル情報の詳細については、「[送信者プロファイル（Sender Profile）] ページ」セクション（4-20 ページ）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。アプライアンスへのすべてのメール 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（4-21 ページ）を参照してください。

[受信メール（Incoming Mail）] ページにおける電子メール 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（Category）	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（「受信メール メッセージの集計方法」セクション（4-13 ページ）を参照）を掛け、その値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「数が絞り込まれた」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。その代わりに、拒否された接続の数は、各時間間隔で最も顕著だった送信者についてのみ維持されます。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。
受信者が無効です（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（Category）	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。
DMARCによる停止（Stopped by DMARC）	DMARC 検証に失敗し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。
承認された正常なメッセージ（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、承認されたクリーン メッセージを最も正確に表したものです。ただし、ウイルスまたはスパム確実としてマークされたにもかかわらず配信されたメッセージは集計されないので、実際のメッセージの配信数と、このクリーン メッセージの数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。

また、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。

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 [印刷可能な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（4-6 ページ）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）]、[ネットワーク所有者（Network Owners）]

[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」セクション（4-19 ページ）を参照してください。

[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」セクション（4-6 ページ）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」セクション（4-45 ページ）

[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外ホストを管理する方法は、送信者の検証によって制御できます。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。

[表示された項目（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

メールのグラフでは、さまざまな時間粒度でデータを表示できます。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」セクション（3-5 ページ）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 [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、電子メール セキュリティ アプライアンスのパブリック リスナーに接続した上位送信者がリスト表示されます。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 オーナーがテーブルに表示されます。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 アドレスを取得してその有効性を検証します。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、その送信者の詳細情報が表示されます。結果は、[送信者プロファイル（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（Sender Profile）]

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」セクション（4-20 ページ）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」セクション（4-21 ページ）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。いずれかの 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）] ページにアクセスするには、[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します。

*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（Sender Profile）] ページは、それぞれ多少異なります。各ページには、特定の送信者からの受信メールに関するグラフおよび要約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）] ページには、詳細なリストが含まれません）。[送信者プロファイル（Sender Profile）] ページには、送信者の現在の SenderBase、送信者グループ、およびネットワーク情報を示す情報セクションが表示されます。

- 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 オーナーに関連付けられたドメインや IP アドレスの情報が含まれます。
- ドメイン プロファイル ページには、ドメインおよびこのドメインに関連付けられた IP アドレスの情報が含まれます。
- 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 ページの下部にある最新情報テーブルには次のデータが含まれます。

- 次のような、SenderBase レピュテーション サービスからのグローバル情報。
  - 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。地震の測定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 を基数とする対数目盛を使用して算出されるメッセージの量の基準です。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 メッセージ量の 100% に相当します。対数目盛を使用した場合、1 ポイントのマグニチュードの増加は、実際の量の 10 倍の増加に相当します。

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 レピュテーション 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 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 レピュテーション 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 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 ページ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

[送信者グループ（Sender Groups）] レポート ページには、送信者グループ別およびメール フロー ポリシー アクション別に接続の要約が表示され、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、ホスト アクセス テーブル（HAT）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、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。

[送信者グループ（Sender Groups）] レポート ページを表示するには、[メール（Email）] > [レポート（Reporting）] > [送信者グループ（Sender Groups）] を選択します。

[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」セクション（4-6 ページ）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」セクション（4-45 ページ）

[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メールの量
- クリーン、スパム陽性、ウイルス陽性、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

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」セクション（3-5 ページ）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。脅威メッセージの総数には、スパム陽性かウイルス陽性、またはコンテンツ フィルタをトリガーした脅威メッセージが含まれます。
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」セクション（4-6 ページ）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」セクション（4-45 ページ）

[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合に処理される受信者の総数

[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。

[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、[送信メッセージ送信者（Outgoing Senders）] 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」セクション（3-5 ページ）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）。
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）	組織によって送信されたすべての発信メッセージの送信者（IP アドレス別またはドメイン別）のすべての詳細情報。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 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」セクション（4-6 ページ）を参照してください。

（注）　[送信メッセージ送信者（Outgoing Senders）] 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」セクション（4-45 ページ）

[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 アドレスは結合されません。

[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。

- 最も多くの外部電子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がコンテンツ フィルタによって阻止されたかどうか

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」セクション（3-5 ページ）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）。
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）。

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
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」セクション（4-25 ページ）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」セクション（4-6 ページ）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」セクション（4-45 ページ）

[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（4-28 ページ）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（DLP Incidents）

[メール（Email）] > [レポート（Reporting）] > [DLPインシデント（DLP Incidents）]（[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）] テーブルで有効になっている 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

[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」セクション（3-5 ページ）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。
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 ポリシーで現在有効になっている 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。

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
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 Incidents 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 インシデントの総数に加えて、重大度レベル別の内訳、メッセージ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」セクション（4-27 ページ）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 インシデントの総数に加えて、重大度レベル別の内訳、メッセージ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確認するには、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」セクション（4-27 ページ）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すると、[DLPポリシー詳細（DLP Policy Detail）] ページが開き、そのポリシーの 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。

また、ページ下部の [送信者別インシデント（Incidents by Sender）] テーブルに、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が表示されます。このテーブルには、このポリシーのユーザごとの 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、ドロップされたかも示されます。[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特定できます。

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」セクション（4-24 ページ）を参照してください。

メッセージフィルタ（Message Filters）

[メッセージフィルタ（Message Filters）] ページには、送受信メッセージのメッセージ フィルタの上位一致（最も多くのメッセージに一致したメッセージ フィルタ）に関する情報が表示されます。

大容量のメール（High Volume Mail）

このページのレポートは、次の目的で使用します。

- 1 人の送信者から送られていたり、件名が同じであったり、1 時間の間に送られたりした、多数のメッセージが関係する攻撃を特定します。
- このような攻撃が独自のドメイン内で発生しないように上位ドメインをモニタします。この状況が生じると、組織の 1 つ以上のアカウントが侵害される可能性があります。
- フィルタを適宜調整できるように、誤検出を特定します。

このページのレポートには、ヘッダー反復ルールを使用し、そのルールで設定されたメッセージ数のしきい値を超えるメッセージ フィルタからのデータのみが表示されます。他のルールと組み合わせた場合、ヘッダー反復ルールの評価は最後になります。また、先行する条件によってメッセージの処理が決定されると評価は行われません。同様に、レート制限で検出されたメッセージはヘッダー反復メッセージ フィルタに達しません。したがって、別の状況では大容量のメールと見なされるメッセージが、これらのレポートに含まれない場合があります。特定のメッセージをホワイトリストに追加するようにフィルタを設定している場合は、それらのメッセージもレポートから除外されます。

メッセージ フィルタおよびヘッダー反復ルールの詳細については、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 ヘルプまたはユーザ ガイドを参照してください。

関連項目

- [レート制限（Rate Limits）] ページ（4-35 ページ）

[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」セクション（4-29 ページ）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」セクション（4-6 ページ）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」セクション（4-45 ページ）

[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（4-25 ページ）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。

DMARC検証（DMARC Verification）

[DMARC検証（DMARC Verification）] ページには、Domain-based Message Authentication, Reporting and Conformance（DMARC）検証に失敗した上位送信者のドメイン、および各ドメインからの受信メッセージに対して実行されたアクションの要約が表示されます。このレポートを使用して DMARC 設定を最適化し、次のような情報を取得できます。

- DMARC 検証に失敗したメッセージを最も多く送信したドメイン
- 各ドメインで、DMARC 検証に失敗したメッセージに対して実行されたアクション

DMARC 検証の詳細については、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 ヘルプまたはユーザ ガイドで「Email Authentication」の章を参照してください。

[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するウイルス スキャン エンジンによって検出され、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）　アウトブレイク フィルタでは、ユーザが操作しなくても、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。

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、有効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」セクション（3-5 ページ）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」セクション（4-6 ページ）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」セクション（4-45 ページ）

[URLフィルタリング（URL Filtering）] ページ

- URL フィルタリング レポート モジュールは、URL フィルタリングが有効の場合にのみ入力されます。
- URL フィルタリング レポートは、送受信メッセージに対して使用できます。
- URL フィルタリング エンジンによって（アンチスパム/アウトブレイク フィルタ スキャンの一部として、またはメッセージ/コンテンツ フィルタを使用して）スキャンされるメッセージのみが、これらのモジュールに含まれます。ただし、必ずしもすべての結果が URL フィルタリング機能のみに起因するわけではできません。

- [上位URLカテゴリ（Top URL Categories）] モジュールには、コンテンツ フィルタまたはメッセージ フィルタに一致するかどうかにかかわらず、スキャンされたメッセージで検出されたすべてのカテゴリが含まれます。
- 各メッセージを関連付けることができるレピュテーション レベルは 1 つのみです。メッセージに複数の URL がある場合、メッセージ内の URL の最も低いレピュテーションが統計情報に反映されます。
- [セキュリティサービス（Security Services）] > [URLフィルタリング（URL Filtering）] で設定したグローバル ホワイトリストの URL は、レポートに含まれません。

  個別のフィルタで使用されるホワイトリストの URL はレポートに含まれます。
- 悪意のある URL とは、アウトブレイク フィルタによってレピュテーションが低いと判定された URL です。疑わしい URL とは、アウトブレイク フィルタによってクリック時の保護が必要であると判定された URL です。したがって、疑わしい URL は Cisco Web セキュリティ プロキシにリダイレクトするために書き換えられています。
- URL カテゴリ ベースのフィルタの結果はコンテンツおよびメッセージ フィルタ レポートに反映されます。
- Cisco Web セキュリティ プロキシによるクリック時の URL 評価の結果は、レポートに反映されません。

[高度なマルウェア防御（ファイルレピュテーション）（Advanced Malware Protection (File Reputation)）] および [高度なマルウェア防御（ファイル分析）（Advanced Malware Protection (File Analysis)）] レポート ページ

ファイル分析レポートの詳細の要件

ファイル分析レポートの詳細を取得するには、アプライアンスがポート 443 経由でファイル分析サーバに接続できる必要があります。詳細については、付録 C「ファイアウォール情報」を参照してください。

Cisco コンテンツ セキュリティ管理アプライアンスがインターネットに直接接続していない場合は、このトラフィック用にプロキシ サーバを設定します（アップグレードとアップデートの設定（14-23 ページ）を参照）。プロキシを使用してアップグレードおよびサービス アップデートを入手するようにアプライアンスを設定済みの場合は、既存の設定が使用されます。

HTTPS プロキシを使用する場合は、そのプロキシでトラフィックを復号化しません。パススルー機能を使用してファイル分析サーバと通信するようにしてください。プロキシ サーバはファイル分析サーバからの証明書を信頼する必要がありますが、ファイル分析サーバに自身の証明書を提供する必要はありません。

追加の要件については、お使いのセキュリティ管理アプライアンス リリースのリリース ノート（http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html で入手可能）を参照してください。

SHA-256 ハッシュによるファイルの識別

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

ほとんどのレポートでは、ファイルがその SHA-256 値（短縮形式）別に表示されます。

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

レポート	説明
高度なマルウェア防御（Advanced Malware Protection）	ファイル レピュテーション サービスによって特定されたファイル ベースの脅威を示します。 判定が変更されたファイルについては、[AMP判定のアップデート（AMP Verdict Updates）] レポートを参照してください。これらの判定は、[高度なマルウェア防御（Advanced Malware Protection）] レポートに反映されません。 圧縮ファイルまたはアーカイブ済みファイルから悪意のあるファイルが抽出された場合、圧縮ファイルまたはアーカイブ済みファイルの SHA 値のみが [高度なマルウェア防御（Advanced Malware Protection）] レポートに含まれます。
ファイル分析（File Analysis）	分析用に送信された各ファイルの時間と判定（または中間判定）を表示します。 1000 を超えるファイル分析結果を表示するには、データを .csv ファイルとしてエクスポートします。 ドリル ダウンすると、各ファイルの脅威の特性を含む詳細な分析結果が表示されます。 SHA の追加情報についてクラウド サービスを検索することもできます。リンクは結果の詳細ページにあります。 ファイル分析の詳細を表示するには、ファイル分析レポートの詳細の要件（4-31 ページ）を参照してください。 圧縮ファイルまたはアーカイブ済みファイルから抽出したファイルが分析用に送信されると、抽出されたファイルの SHA 値のみが [ファイル分析（File Analysis）] レポートに含まれます。

レポート	説明
AMP判定のアップデート（AMP Verdict Updates）	高度なマルウェア防御は対象を絞ったゼロデイ脅威に焦点を当てるため、集約データでより詳細な情報が提供されると、脅威の判定が変わる可能性があります。 [AMP判定のアップデート（AMP Verdict Updates）] レポートには、このアプライアンスで処理され、メッセージ受信後に判定が変わったファイルが表示されます。この状況の詳細については、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を参照してください。 1000 を超える判定アップデートを表示するには、データを .csv ファイルとしてエクスポートします。 1 つの SHA-256 に対して判定が複数回変わった場合は、判定履歴ではなく最新の判定のみがこのレポートに表示されます。 使用可能な最大時間範囲内（レポートに選択された時間範囲に関係なく）に特定の SHA-256 の影響を受けるすべてのメッセージを表示するには、SHA-256 リンクをクリックします。

他のレポートのファイル レピュテーション フィルタリング データの表示

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

[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

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」セクション（3-5 ページ）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。

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
受信TLS接続数サマリー（Incoming TLS Connections Summary）	このテーブルには、受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メッセージ数サマリー（Incoming TLS Messages Summary）	このテーブルには、受信メッセージの総量の要約が表示されます。
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。
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）	このテーブルには、送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。
送信TLSメッセージ数サマリー（Outgoing TLS Messages Summary）	このテーブルには、送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。

[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。

[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（Mail Flow Policies）] で設定します。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。

関連項目

- 大容量のメール（High Volume Mail）（4-28 ページ）

[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、最近のアウトブレイクやアウトブレイク フィルタによって隔離されたメッセージに関する情報が表示されます。このページを使用して、対象を絞ったウイルス、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。

- アウトブレイク 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
- ウイルス発生に対するアウトブレイク フィルタ機能のリード タイム
- グローバル発生と比較したローカル発生の状況
- メッセージがアウトブレイク隔離にとどまる期間
- 最も頻繁に表示される悪意のある可能性がある URL

[タイプ別脅威（Threats By Type）] セクションには、アプライアンスによって受信された脅威メッセージのさまざまなタイプが示されます。[脅威サマリー（Threat Summary）] セクションには、[ウイルス（Virus）]、[フィッシング（Phish）]、および [Scam] によるメッセージの内訳が示されます。

[過去 1 年間のアウトブレイク サマリー（Past Year Outbreak Summary）] には、この 1 年間にわたるグローバル発生およびローカル発生が表示されるので、ローカル ネットワークのトレンドとグローバルな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。ローカル感染発生データには、ウイルス以外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、Threat Operations Center によって検出されたすべての発生を表します。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発生を表します。[ローカル保護の合計時間（Total Local Protection Time）] は、Threat Operations Center による各ウイルス発生の検出と、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、アウトブレイク フィルタの隔離状況の概要が示されます。これは、アウトブレイク 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、メッセージはアンチウイルスおよびアンチスパム ルールが使用可能になる前に隔離されます。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、陽性か、クリーンかを判定されます。発生トラッキングの動的性質により、メッセージが隔離エリア内にあるときでも、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。（隔離エリア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）、脅威の名前、脅威の説明、識別されたメッセージの数などの、特定の発生に関する情報が表示されます。ウイルス発生の場合は [過去 1 年間のウイルス アウトブレイク（Past Year Virus Outbreaks）] に、発生の名前と ID、ウイルス発生が初めてグローバルに検出された日時、アウトブレイク フィルタによって提供される保護時間、および隔離されたメッセージの数が含まれます。グローバル発生またはローカル発生のどちらを表示するかを選択できます。

[最初にグローバルで確認した日時（First Seen Globally）] の時間は、世界最大の電子メールおよび Web トラフィック モニタリング ネットワークである SenderBase のデータに基づいて、Threat Operations Center によって決定されます。[保護時間（Protection Time）] は、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。

このページの他のモジュールには次の情報が表示されます。

- 選択した期間にアウトブレイク フィルタによって処理された受信メッセージの数。

  ウイルス以外の脅威には、外部 Web サイトへのリンクを使用したフィッシング電子メール、詐欺、およびマルウェア配布が含まれます。

- アウトブレイク フィルタで検出された脅威の重大度。

  レベル 5 の脅威が範囲または影響において重大であるのに対し、レベル 1 は脅威のリスクが低いことを示します。脅威レベルの説明については、お使いの電子メール セキュリティ アプライアンスのオンライン ヘルプまたはユーザ ガイドを参照してください。

- メッセージがアウトブレイク隔離にとどまっていた時間。

  この期間は、潜在的な脅威の安全性の判定に必要なデータを収集するためにかかる時間によって決まります。通常、ウイルス脅威を含むメッセージはアンチウイルス プログラムの更新を待機する必要があるため、ウイルス以外の脅威を含む場合よりも隔離に長くとどまります。各メール ポリシーで指定した最大保存期間も反映されます。

- サイトのクリック時評価（受信者がメッセージ内の悪意のある可能性があるリンクをクリックした場合）用に、メッセージ受信者を Cisco Web セキュリティ プロキシにリダイレクトするために最も頻繁に書き換えられた URL。

  いずれかの URL が悪意のある URL と見なされると、そのメッセージ内のすべての URL が書き換えられるため、このリストには悪質でない URL が含まれる場合があります。

（注） [アウトブレイクフィルタ（Outbreak Filters）] レポート ページにテーブルが正しく表示されるためには、アプライアンスが、で指定した Cisco アップデート サーバと通信できる必要があります。[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [アップデート設定（Update Settings）]

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 ヘルプまたはユーザ ガイドの「Outbreak Filters」の章を参照してください。

[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、ワークキュー内のメッセージ数、送受信メッセージ（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超える時期を特定します。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必要なタイミングがわかります。
- 今後発生するキャパシティの問題を示す、システム動作の履歴トレンドを特定します。
- 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。

お使いの電子メール 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、ワーク 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）]（4-39 ページ）および[システム容量（System Capacity）]：[送信メール（Outgoing Mail）]（4-39 ページ）を参照してください。
- **ワーク キュー:** ワーク 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、ワーク 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、頻繁なワーク 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、ワーク 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）]（4-39 ページ）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、指定された期間内の最大値を示します。[平均（Average）] 値は指定された期間内のすべての値の平均です。集計期間は、レポートに対して選択された間隔に応じて異なります。たとえば、月単位のチャートの場合は、日付ごとの [平均（Average）] 値と [最大（Maximum）] 値を表示することができます。

特定のグラフの [詳細の表示（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、指定された期間のワーク キュー内のメッセージ量が表示されます。また、同じ期間のワーク 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できます。[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。[Workqueue] ページを確認するときは、ワーク 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ワーク キュー バックアップに注意することが推奨されます。

[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、受信メッセージの総数、平均メッセージ サイズ、受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。受信メール 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確認することもできます。

（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。

[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、送信メッセージの総数、平均メッセージ サイズ、送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。送信メール データと送信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確認することもできます。

[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 アプライアンスの全体的な 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を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、調整や無効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）。

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 スワッピングは予想される正常な動作です（特に C1x0 アプライアンスの場合）。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。

[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。

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タイプ

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」セクション（4-28 ページ）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（DLP Incidents）」セクション（4-26 ページ）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は仮想ゲートウェイ 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(Email Reporting 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」セクション(4-42 ページ)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(Email Reporting 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」セクション(4-42 ページ)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」セクション(4-16 ページ)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」セクション(4-24 ページ)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」セクション(4-36 ページ)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」セクション(4-22 ページ)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」セクション(4-23 ページ)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」セクション(4-23 ページ)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」セクション(4-21 ページ)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」セクション(4-37 ページ)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」セクション(4-33 ページ)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」セクション(4-29 ページ)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。[スケジュールされたレポート（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（3-10 ページ）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 メールレポート（Archived Email Reports）] の表示と管理（4-49 ページ）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 つ以上のドメインの送受信メッセージ アクティビティ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)] レポートと送信者レピュテーション フィルタリングによってブロックされたメッセージ

送信者レピュテーション フィルタリングによってブロックされたメッセージはワーク 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、メッセージが受信者レベル(RCPT TO)に達するまでセキュリティ管理アプライアンスでの HAT 拒否を遅らせます。そうすることで、AsyncOS が受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** を有効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** を有効にするには、**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 configuration 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 ドメイン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。アプライアンスでコンフィギュレーション ファイルを更新する場合は、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)] > [スケジュールされたレポート(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　レポートに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。

- [ドメインを個別に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 configuration 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(4-43 ページ)を参照してください。

(注)　レポートを外部アカウント(Yahoo!　メールや Gmail など)に送信する場合は、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、送信メール 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、デフォルトのシスコ 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（3-10 ページ）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送受信電子メール メッセージ アクティビティの全体的な概要です。セキュリティ管理アプライアンスで表示できます。

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（Email Reporting 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（Email Reporting Overview）] ページ」セクション（4-13 ページ）を参照してください。

[スケジュールされたレポート（Scheduled Reports）] ページ

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（4-40 ページ）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

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）] > [スケジュールされたレポート（Scheduled Reports）] を選択します。

ステップ 2　[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（4-40 ページ）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（4-42 ページ）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　[行数（Number of Rows）] では、レポートに応じて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（3-10 ページ）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）] > [スケジュールされたレポート（Scheduled Reports）] を選択します。

ステップ 2　[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）] > [スケジュールされたレポート（Scheduled Reports）] を選択します。

ステップ 2　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オンにします。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オンにします。

ステップ 3　[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（4-50 ページ）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（4-6 ページ）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（4-40 ページ）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（4-40 ページ）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（4-42 ページ）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（3-10 ページ）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 メールレポート（Archived Email Reports）] ページ

- 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（4-40 ページ）
- オンデマンドでの電子メール レポートの生成（4-48 ページ）
- [アーカイブ メールレポート（Archived Email Reports）] の表示と管理（4-49 ページ）

[アーカイブ メールレポート（Archived Email Reports）] 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 30 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。30 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、生成済みでまだ消去されていない、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。

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 メールレポート（Archived Email Reports）] の表示と管理（4-49 ページ）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 つ以上のレポートのチェックボックスをオンにします。

ステップ 3　[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（4-47 ページ）を参照してください。

電子メール レポートのトラブルシューティング

- アウトブレイク フィルタ レポートに情報が正しく表示されない（4-51 ページ）
- レポートのリンクをクリックした後のメッセージ トラッキング結果がレポート結果と一致しない（4-51 ページ）
- [高度なマルウェア保護判定のアップデート（Advanced Malware Protection Verdict Updates）] レポートの結果が異なる（4-51 ページ）
- ファイル分析レポートの詳細の表示に関する問題（4-51 ページ）

すべてのレポートのトラブルシューティング（3-13 ページ）も参照してください。

アウトブレイク フィルタ レポートに情報が正しく表示されない

問題　アウトブレイク フィルタ レポートに脅威情報が正しく表示されません。

ソリューション　アプライアンスが、で指定した Cisco アップデート サーバと通信できることを確認します。[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）]

レポートのリンクをクリックした後のメッセージ トラッキング結果がレポート結果と一致しない

問題　レポートからドリルダウンしたときのメッセージ トラッキング結果が、予期した結果に一致しません。

ソリューション　これは、レポーティングとトラッキングが常に同時に有効にならずに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に発生する可能性があります。各機能（レポーティング、トラッキング）のデータは、その機能が有効になっている間だけキャプチャされます。

関連項目

- 有効なメッセージ トラッキング データの検査（6-4 ページ）

[高度なマルウェア保護判定のアップデート（Advanced Malware Protection Verdict Updates）] レポートの結果が異なる

問題　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 アプライアンスが同じファイルを分析用に送信し、Web および電子メールの [AMP判定のアップデート（AMP Verdict Updates）] レポートに、そのファイルの異なる判定が表示されます。

ソリューション　これは一時的な違いです。すべての判定アップデートがダウンロードされると、結果は一致します。一致するまでに最大で 30 分かかります。

ファイル分析レポートの詳細の表示に関する問題

- ファイル分析レポートの詳細を使用できない（4-51 ページ）
- ファイル分析レポートの詳細を表示する際のエラー（4-52 ページ）

ファイル分析レポートの詳細を使用できない

問題　ファイル分析レポートの詳細を使用できません。

ソリューション　ファイル分析レポートの詳細の要件（4-31 ページ）を参照してください。

ファイル分析レポートの詳細を表示する際のエラー

問題　ファイル分析レポートの詳細を表示しようとすると、**使用可能なクラウド サーバ構成がありません**(No cloud server configuration is available)エラーが表示されます。

ソリューション　[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)] に移動して、ファイル分析機能が有効になっている電子メール セキュリティ アプライアンスを少なくとも 1 つ追加します。

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 レポーティングおよびトラッキングの概要

Cisco コンテンツ セキュリティ管理アプライアンスは、複数の Web セキュリティ アプライアンスのセキュリティ機能から情報を収集し、Web トラフィック パターンとセキュリティ 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、管理者は全体的な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 URL 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

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」というタイトルのユーザ 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

URL カテゴリ

URL カテゴリについては、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」というカテゴリのレポート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」セクション（15-1 ページ）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有効な場合、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 レポーティングが有効になっていない場合、生成されるレポートはシステム ステータスとシステム キャパシティ関連に限定されます。

セキュリティ管理アプライアンスで Web レポーティング データを表示する方法は複数あります。

- インタラクティブ レポート ページを表示する場合は、[Webレポート（Web Reporting）] ページの説明（5-6 ページ）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（5-42 ページ）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（5-37 ページ）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、アーカイブ済みの Web レポートの表示と管理（5-43 ページ）を参照してください。

- 個々のトランザクションに関する情報を表示するには、Webトラッキング（Web Tracking）（5-44 ページ）を参照してください。

中央集中型 Web レポーティングおよびトラッキングの設定

中央集中型 Web レポーティングおよび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 Web レポーティングの有効化（5-3 ページ）
  - Web レポートでのユーザ名の匿名化
- 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有効化（5-4 ページ）
- 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（5-4 ページ）
- Web レポートでのユーザ名の匿名化（5-5 ページ）

セキュリティ管理アプライアンスでの中央集中型 Web レポーティングの有効化

手順

ステップ 1　中央集中型 Web レポーティングを有効にする前に、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。ディスク領域の管理（14-53 ページ）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有効にする場合は、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無効にし、その後有効にする場合は、次の手順を実行します。

a. [設定の編集（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（5-5 ページ）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。

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有効化

中央集中型レポーティングを有効にする前に、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有効にする必要があります。

『AsyncOS for Cisco Web Security Appliances User Guide』の「Enabling Centralized Reporting」のセクション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有効にする各 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。

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　[設定の編集（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。

Web セキュリティ レポートの使用

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

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（3-1 ページ）
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（3-3 ページ）
データ内の特定のトランザクションに関する情報を検索する	Webトラッキング（Web Tracking）（5-44 ページ）

目的	参照先
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（3-10 ページ）
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レポート（Web Reporting）] ページの説明（5-6 ページ）
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（5-37 ページ）
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（5-37 ページ）
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	アーカイブ済みの Web レポートの表示と管理（5-43 ページ）
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（3-2 ページ）

[Webレポート（Web Reporting）] ページの説明

（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」セクション（5-37 ページ）を参照してください。

表 5-1　[Web レポート（Web Reporting）] タブの詳細

[Web レポート（Web Reporting）] メニュー	操作
Web レポーティングの概要	[概要（Overview）] ページには、Web セキュリティ アプライアンスでのアクティビティの概要が表示されます。これには、着信および発信トランザクションに関するグラフおよび要約テーブルが含まれます。詳細については、「Web レポーティングの概要」セクション（5-10 ページ）を参照してください。

表 5-1　[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	操作
[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）」セクション（5-12 ページ）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）」セクション（5-13 ページ）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」セクション（5-15 ページ）を参照してください。
[URLカテゴリ（URL Categories）] 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（URL Categories）] レポート」セクション（5-16 ページ）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」セクション（5-19 ページ）を参照してください。

表 5-1　[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	操作
[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」セクション（5-21 ページ）を参照してください。
[高度なマルウェア防御（ファイルレピュテーション）（Advanced Malware Protection (File Reputation)）] および [高度なマルウェア防御（ファイル分析）（Advanced Malware Protection (File Analysis)）] レポート ページ	ファイル レピュテーションおよび分析データは 3 つのレポーティング ページに表示されます。 詳細については、「[高度なマルウェア防御（ファイルレピュテーション）（Advanced Malware Protection (File Reputation)）] および [高度なマルウェア防御（ファイル分析）（Advanced Malware Protection (File Analysis)）] レポート」セクション（5-25 ページ）を参照してください。
[クライアントマルウェアリスク（Client Malware Risk）] 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」セクション（5-27 ページ）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」セクション（5-29 ページ）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」セクション（5-31 ページ）を参照してください。
[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」セクション（5-33 ページ）を参照してください。
ユーザの場所別のレポート（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、「ユーザの場所別のレポート（Reports by User Location）」セクション（5-34 ページ）を参照してください。

表 5-1　[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	操作
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る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）」セクション（5-44 ページ）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」セクション（5-35 ページ）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」セクション（5-37 ページ）を参照してください。
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」セクション（5-37 ページ）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、「アーカイブ済みの Web レポートの表示と管理」セクション（5-43 ページ）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」セクション（5-37 ページ）を参照してください。

[滞留時間（Time Spent）] について

さまざまなテーブルの [滞留時間（Time Spent）] カラムは、Web ページでユーザが費やした時間を表します。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。

Web レポーティングの概要

[Web] > [レポート（Reporting）] > [概要（Overview）] ページには、Web セキュリティ アプライアンスでのアクティビティの概要が表示されます。これには、着信および発信トランザクションに関するグラフと要約テーブルが含まれます。

[概要（Overview）] ページの上部には、URL とユーザの使用量に関する統計情報、Web プロキシ アクティビティ、および各種トランザクション サマリーが表示されます。トランザクション サマリーには、さらに詳細なトレンド情報が示されます。たとえば、疑わしいトランザクションと、そのグラフの隣にそれらのトランザクションがブロックされた数、およびブロックされた方法が表示されます。

[概要（Overview）] ページの下半分は、使用状況に関する情報に使用されます。つまり、表示されている上位 URL カテゴリ、ブロックされている上位アプリケーション タイプおよびカテゴリ、これらのブロックまたは警告を生成している上位ユーザが表示されます。

表 5-2　[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」セクション（3-5 ページ）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（3-4 ページ）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 プロキシの概要（Web Proxy Summary）	このセクションでは、疑わしい Web プロキシ アクティビティまたは正常なプロキシ アクティビティの比率を、トランザクションの総数も含めて表示できます。
L4 トラフィック モニタの概要（L4 Traffic Monitor Summary）	この項には、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概要（Suspect Transactions Summary）	このセクションでは、ブロックまたは警告された疑わしいトランザクションの比率を表示できます。また、検出されてブロックされたトランザクションのタイプ、およびそのトランザクションが実際にブロックされた回数を確認できます。
総トランザクション数別上位 URL カテゴリ（Top URL Categories by Total Transactions）	このセクションには、ブロックされている上位 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（5-18 ページ）を参照してください。

表 5-2　[Web] > [レポート（Reporting）] > [概要（Overview）] ページの詳細（続き）

セクション	説明
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。
検出された上位マルウェア カテゴリ（Top Malware Categories Detected）	このセクションには、検出されたすべてのマルウェア カテゴリが表示されます。
ブロックまたは警告されたトランザクション上位ユーザ（Top Users Blocked or Warned Transactions）	このセクションには、ブロックされたトランザクションまたは警告が発行されたトランザクションを生成している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（5-5 ページ）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。

[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 5-3　[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」セクション（3-5 ページ）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 レポーティングの有効化」セクション（5-3 ページ）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」セクション（5-5 ページ）を参照してください。

表 5-3　[Web] > [レポート（Reporting）] > [ユーザ（Users）] ページの詳細（続き）

セクション	説明
使用した帯域幅別上位ユーザ（Top Users by Bandwidth Used）	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 テーブル（Users Table）	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）」セクション（5-13 ページ）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「LDAP サーバ プロファイルの作成」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、Web セキュリティ レポートの使用（5-5 ページ）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」セクション（D-1 ページ）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」セクション（5-37 ページ）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）] テーブルでそのユーザをクリックします。

[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 5-4　[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」セクション（3-5 ページ）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（5-18 ページ）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（5-18 ページ）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 5-4　[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」セクション（D-1 ページ）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。

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

表 5-5　[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」セクション（3-5 ページ）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。
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。 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」セクション（D-3 ページ）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、Web セキュリティ レポートの使用（5-5 ページ）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」セクション（5-37 ページ）を参照してください。

[URLカテゴリ（URL Categories）] 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。

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

表 5-6　[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」セクション（3-5 ページ）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。
ブロックまたは警告を受けたトランザクション数別上位 URL カテゴリ（Top URL Categories by Blocked and Warned Transactions）	このセクションには、トランザクションごとに発生するブロック アクションまたは警告アクションをトリガーした上位 URL がグラフ形式で表示されます。たとえば、ユーザがある URL にアクセスしたが、特定のポリシーが適用されているために、ブロック アクションまたは警告がトリガーされたとします。この URL は、ブロックまたは警告されたトランザクションとしてこのグラフに追加されます。
一致した URL カテゴリ（URL Categories Matched）	[一致した URL カテゴリ（URL Categories Matched）] セクションには、指定した時間範囲内における URL カテゴリ別のトランザクションの処理、使用された帯域幅、各カテゴリで費やされた時間が表示されます。 未分類の URL が多数ある場合は、未分類の URL の削減（5-17 ページ）を参照してください。
URL フィルタリングのバイパス（URL Filtering Bypassed）	URL フィルタリングの前に実行されるポリシー、ポートおよび管理ユーザ エージェントのブロッキングを示します。

ヒント　このレポートのビューをカスタマイズするには、Web セキュリティ レポートの使用（5-5 ページ）を参照してください。

メモ

- 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）（5-40 ページ）を参照してください。
- 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。

未分類の URL の削減

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。これらのトランザクションは、代わりに [URL フィルタリングバイパス（URL Filtering Bypassed）] 統計情報に含まれるようになります。方法については、『AsyncOS for Cisco Web Security Appliances User Guide』でカスタム URL カテゴリに関する情報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（5-19 ページ）を参照してください。

URL カテゴリ セットの更新とレポート

URL カテゴリ セットの更新の準備および管理（9-22 ページ）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（URL Categories）] 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：アクセス数上位の URL カテゴリの調査」セクション（D-4 ページ）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、今後のルール更新への組み込みに活用されます。

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、『AsyncOS for Cisco Web Security Appliances User Guide』の「Understanding Application Visibility and Control」の章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、『AsyncOS for Cisco Web Security Appliances User Guide』の「Understanding Application Visibility and Control」の章を参照してください。

[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 5-7　[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」セクション（3-5 ページ）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、「Web セキュリティ レポートの使用」セクション（5-5 ページ）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、Web セキュリティ レポートの使用（5-5 ページ）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」セクション（5-37 ページ）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、有効なスキャン 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」セクション（5-31 ページ）を参照してください。

[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 5-8　[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」セクション（3-5 ページ）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（5-23 ページ）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。

表 5-8　[Web] > [レポート（Reporting）] > [マルウェア対策（Anti-Malware）] ページの詳細（続き）

セクション	説明
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（5-23 ページ）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。 「アウトブレイク（Outbreak）」のラベルと番号が付いている脅威は、他のスキャン エンジンとは別に、Adaptive Scanning 機能によって特定された脅威です。 **（注）**　[マルウェア脅威（Malware Threats）] でテーブルを昇順にソートすると、リストの最上部に [名前のないマルウェア（Unnamed Malware）] が表示されます。

ヒント　このレポートのビューをカスタマイズするには、Web セキュリティ レポートの使用（5-5 ページ）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。

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、Web セキュリティ レポートの使用（5-5 ページ）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 Threats）] レポート ページには、特定の脅威にさらされているクライアント、および感染した可能性があるクライアントのリストが表示され、[クライアントの詳細（Client Detail）] ページへのリンクがあります。レポート上部のトレンド グラフには、指定した時間範囲内で脅威に関してモニタされたトランザクションおよびブロックされたトランザクションが表示されます。下部のテーブルには、指定した時間範囲内で脅威に関してモニタされたトランザクションおよびブロックされたトランザクションの実際の数が表示されます。

このレポートを表示するには、[マルウェア対策（Anti-Malware）] レポート ページの [マルウェアのカテゴリ] カラムでカテゴリをクリックします。

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」セクション（5-37 ページ）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。

マルウェアのタイプ	説明
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。
トロイのフィッシャ	トロイのフィッシャは、感染したコンピュータに潜んで特定の Web ページがアクセスされるのを待つか、または感染したマシンをスキャンして銀行サイト、オークション サイト、あるいはオンライン支払サイトに関係するユーザ名とパスワードを探します。
ウィルス	ウイルスは、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。

[高度なマルウェア防御（ファイルレピュテーション）（Advanced Malware Protection (File Reputation)）] および [高度なマルウェア防御（ファイル分析）（Advanced Malware Protection (File Analysis)）] レポート

ファイル分析レポートの詳細の要件

ファイル分析レポートの詳細を取得するには、アプライアンスがポート 443 経由でファイル分析サーバに接続できる必要があります。詳細については、付録 C「ファイアウォール情報」を参照してください。

Cisco コンテンツ セキュリティ管理アプライアンスがインターネットに直接接続していない場合は、このトラフィック用にプロキシ サーバを設定します（アップグレードとアップデートの設定（14-23 ページ）を参照）。プロキシを使用してアップグレードおよびサービス アップデートを入手するようにアプライアンスを設定済みの場合は、既存の設定が使用されます。

HTTPS プロキシを使用する場合は、そのプロキシでトラフィックを復号化しません。パススルー機能を使用してファイル分析サーバと通信するようにしてください。プロキシ サーバはファイル分析サーバからの証明書を信頼する必要がありますが、ファイル分析サーバに自身の証明書を提供する必要はありません。

追加の要件については、お使いのセキュリティ管理アプライアンス リリースのリリース ノート（http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html で入手可能）を参照してください。

SHA-256 ハッシュによるファイルの識別

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

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

[高度なマルウェア防御（ファイルレピュテーション）（Advanced Malware Protection (File Reputation)）] および [高度なマルウェア防御（ファイル分析）（Advanced Malware Protection (File Analysis)）] レポート ページ

レポート	説明
高度なマルウェア防御（Advanced Malware Protection）	ファイル レピュテーション サービスによって特定されたファイル ベースの脅威を示します。 各 SHA にアクセスしようとしたユーザ、およびその SHA-256 に関連付けられたファイル名を表示するには、テーブルの SHA-256 リンクをクリックします。 [マルウェア脅威ファイルの詳細（Malware Threat File Details）] レポート ページの下部にあるリンクをクリックすると、レポート用に選択された時間範囲に関係なく使用可能な最大時間範囲内に検出された、Web トラッキング内のファイルのすべてのインスタンスが表示されます。 判定が変更されたファイルについては、[AMP判定のアップデート（AMP Verdict Updates）] レポートを参照してください。これらの判定は、[高度なマルウェア防御（Advanced Malware Protection）] レポートに反映されません。 圧縮ファイルまたはアーカイブ済みファイルから悪意のあるファイルが抽出された場合、圧縮ファイルまたはアーカイブ済みファイルの SHA 値のみが [高度なマルウェア防御（Advanced Malware Protection）] レポートに含まれます。
ファイル分析（File Analysis）	分析用に送信された各ファイルの時間と判定（または中間判定）を表示します。 1000 を超えるファイル分析結果を表示するには、データを .csv ファイルとしてエクスポートします。 ドリル ダウンすると、各ファイルの脅威の特性およびスコアを含む詳細な分析結果が表示されます。 SHA の追加情報についてクラウド サービスを検索することもできます。リンクは結果の詳細ページにあります。 ファイル分析レポートの詳細の要件（5-25 ページ）も参照してください。 圧縮ファイルまたはアーカイブ済みファイルから抽出したファイルが分析用に送信されると、抽出されたファイルの SHA 値のみが [ファイル分析（File Analysis）] レポートに含まれます。

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

他のレポートのファイル レピュテーション フィルタリング データの表示

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

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

[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。

表 5-9 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 5-9　[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（3-5 ページ）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（5-31 ページ）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）（5-13 ページ）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（5-31 ページ）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、Web セキュリティ レポートの使用（5-5 ページ）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 Security appliance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 User Guide*』の「Web Reputation Filters」を参照してください。

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

表 5-10　[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」セクション（3-5 ページ）を参照してください。
Web レピュテーション アクション（トレンド）（Web Reputation Actions (Trend)）	このセクションには、指定した時間（横方向の時間軸）に対する Web レピュテーション アクションの総数（縦方向の目盛り）が、グラフ形式で表示されます。このセクションでは、時間の経過に伴う Web レピュテーション アクションの潜在的なトレンドを確認できます。
Web レピュテーション アクション（ボリューム）（Web Reputation Actions (Volume)）	このセクションには、Web レピュテーション アクションのボリュームがトランザクション数の比率で表示されます。
ブロックされたトランザクション別 Web レピュテーション脅威タイプ（Web Reputation Threat Types by Blocked Transactions）	このセクションには、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。
詳細にスキャンされたトランザクション別 Web レピュテーション脅威タイプ（Web Reputation Threat Types by Scanned Further Transactions）	Adaptive Scanning が有効の場合、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 が有効でない場合、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「詳細なスキャン（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（スコア別明細）（Web Reputation Actions (Breakdown by Score)）	Adaptive Scanning が有効でない場合、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、Web セキュリティ レポートの使用（5-5 ページ）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 を有効または無効にしたりできます。Web レピュテーションの設定の詳細については、『AsyncOS for Cisco Web Security Appliances User Guide』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、Web セキュリティ レポートの使用（5-5 ページ）を参照してください。

表 5-11　[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（3-5 ページ）を参照してください。
上位クライアント IP（Top Client IPs）	このセクションには、組織内で最も頻繁にマルウェア サイトに接続しているコンピュータの IP アドレスがグラフ形式で表示されます。 チャートの下の [チャート オプション（Chart Options）] リンクをクリックすると、表示を総合的な [検出されたマルウェア接続] から [モニタされたマルウェア接続（Malware Connections Monitored）] または [ブロックされたマルウェア接続（Malware Connections Blocked）] に変更できます。 このチャートは、[クライアントマルウェアリスク（Client Malware Risk）] レポート（5-27 ページ）の [L4トラフィックモニタ：検出されたマルウェア接続（L4 Traffic Monitor: Malware Connections Detected）] チャートと同じです。
上位マルウェア サイト（Top Malware Sites）	このセクションには、L4 トラフィック モニタによって検出された上位のマルウェア ドメインがグラフ形式で表示されます。 チャートの下の [チャート オプション（Chart Options）] リンクをクリックすると、表示を総合的な [検出されたマルウェア接続] から [モニタされたマルウェア接続（Malware Connections Monitored）] または [ブロックされたマルウェア接続（Malware Connections Blocked）] に変更できます。

表 5-11　[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 [ブロックされたマルウェア接続（Malware Connections Blocked）] が高い数値を示している場合、そのカラムの数値をクリックすると、ブロックされた各接続のリストが表示されます。このリストは、[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（5-49 ページ）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（5-27 ページ）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、[検出された上位マルウェア接続（Total Malware Connections Detected）] の数値をクリックすると、そのポートの各接続の詳細情報が表示されます。このリストは、[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（5-49 ページ）を参照してください。

表 5-11　[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
検出されたマルウェア サイト（Malware Sites Detected）	このテーブルには、L4 トラフィック モニタによって最も頻繁にマルウェアが検出されたドメインが表示されます。 特定のポートのデータだけを含めるには、テーブル下部のボックスにポート番号を入力し、[ポート別にフィルタ（Filter by Port）] をクリックします。この機能を使用して、サイトまたはポートをブロックするかどうかを判断できます。 詳細を表示するには、テーブル内のエントリをクリックします。たとえば、[ブロックされたマルウェア接続（Malware Connections Blocked）] の数値をクリックすると、特定のサイトに対してブロックされた各接続のリストが表示されます。このリストは、[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（5-49 ページ）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、Web セキュリティ レポートの使用（5-5 ページ）を参照してください。

関連項目

- L4 トラフィック モニタ レポートのトラブルシューティング（5-54 ページ）

[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手順については、『AsyncOS for Cisco Web Security Appliances User Guide』を参照してください。

関連項目

- SOCKS プロキシによって処理されるトランザクションの検索（5-49 ページ）

ユーザの場所別のレポート（Reports by User Location）

[Web] > [レポート（Reporting）] > [ユーザの場所別のレポート（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。

[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 5-12　[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」セクション（3-5 ページ）を参照してください。
Web プロキシ アクティビティ総数：リモート ユーザ（Total Web Proxy Activity: Remote Users）	このセクションには、指定した時間（横方向）におけるリモート ユーザのアクティビティ（縦方向）が、グラフ形式で表示されます。
Web プロキシの概要（Web Proxy Summary）	このセクションには、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。
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。
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。
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。
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。
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。

[ユーザの場所別レポート（Reports by User Location）] ページでは、ローカル ユーザとリモート ユーザのアクティビティを示すレポートを生成できます。これにより、ユーザのローカル アクティビティとリモート アクティビティを簡単に比較できます。

ヒント　このレポートのビューをカスタマイズするには、Web セキュリティ レポートの使用（5-5 ページ）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」セクション（5-37 ページ）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）] レポートの表示

手順

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

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

（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）]：[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、調整や無効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。

[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）]（5-36 ページ）で説明されているチャートと同じページで、それらのチャートの下に表示されます。

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予想される正常な動作です。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。

（注）　Web レポーティングが無効になると、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。

[Webレポート(Web Reporting)] の [開始(From)] カラムと [終了(To)] カラム、および [Webレポートとトラッキング(Web Reporting and Tracking)] の [開始(From)] カラムと [終了(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。

データの消去の詳細については、「ディスク領域の管理」セクション(14-53 ページ)を参照してください。

（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 レポーティングの概要」セクション(5-10 ページ)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)」セクション(5-12 ページ)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」セクション(5-15 ページ)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(URL Categories)] レポート」セクション(5-16 ページ)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）（5-40 ページ）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」セクション（5-19 ページ）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）（5-41 ページ）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」セクション（5-21 ページ）を参照してください。
- [クライアント マルウェア リスク（Client Malware Risk）]：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」セクション（5-27 ページ）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」セクション（5-29 ページ）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」セクション（5-31 ページ）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、「ユーザの場所別のレポート（Reports by User Location）」セクション（5-34 ページ）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」セクション（5-35 ページ）を参照してください。

Web レポートのスケジュール設定

このセクションの内容は次のとおりです。

（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（5-5 ページ）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。

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。

スケジュール設定された Web レポートの保存

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 30 の最新インスタンスで、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。

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。30 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、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）。

関連項目

- アーカイブ済みの Web レポートの表示と管理（5-43 ページ）

スケジュール設定された Web 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 Web 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 Web 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 Web 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。

メモ

- 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（5-18 ページ）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 Web レポート（5-40 ページ）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Webレポート（Archived Web Reports）] ページ

- 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
- オンデマンドでの Web レポートの生成
- アーカイブ済みの Web レポートの表示と管理

アーカイブ済みの Web レポートの表示と管理

ここでは、スケジュール設定されたレポートとして生成されたレポートの使用方法について説明します。

手順

ステップ 1　[Web] > [レポート（Reporting）] > [アーカイブレポート（Archived Reports）] に移動します。

ステップ 2　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。

ステップ 3　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。

関連項目

- スケジュール設定された Web レポートの保存（5-39 ページ）
- スケジュール設定された Web レポートの追加（5-39 ページ）
- オンデマンドでの Web レポートの生成（5-42 ページ）

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（5-44 ページ）
- L4 トラフィック モニタによって処理されたトランザクションの検索（5-49 ページ）
- SOCKS プロキシによって処理されるトランザクションの検索（5-49 ページ）
- Web トラッキングの検索結果の使用（5-50 ページ）
- Web トラッキング検索結果のトランザクションの詳細の表示（5-50 ページ）

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

関連項目

- Web トラッキングおよびアップグレードについて（5-52 ページ）

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。このデータには、L4 トラフィック モニタリング データ、および SOCKS プロキシによって処理されたトランザクションは含まれません。

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」セクション（D-1 ページ）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」セクション（5-18 ページ）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] > [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 5-13　[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」セクション（3-5 ページ）を参照してください。
ユーザ/クライアント IPv4 または IPv6（User/Client IPv4 or IPv6）	レポートに表示される認証ユーザ名、または追跡対象のクライアント IP アドレスを任意で入力します。IP 範囲を 172.16.0.0/16 のような CIDR 形式で入力することもできます。 このフィールドを空にしておくと、すべてのユーザに関する検索結果が返されます。
Web サイト（Website）	追跡対象の Web サイトを任意で入力します。このフィールドを空にしておくと、すべての Web サイトに関する検索結果が返されます。
トランザクション タイプ（Transaction Type）	追跡対象のトランザクションのタイプを [すべてのトランザクション（All Transactions）]、[完了したもの（Completed）]、[ブロック対象（Blocked）]、[モニタ対象（Monitored）]、または [警告対象（Warned）] から選択します。

表 5-13　[プロキシ サービス（Proxy Services）] タブの Web トラッキング検索条件（続き）

オプション	説明
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「廃止予定（Deprecated）」のラベルが付けられる場合があります。廃止予定のカテゴリは、少なくとも 1 つの管理対象 Web セキュリティ アプライアンスで新しいトランザクションに使用されなくなります。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（5-18 ページ）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、[アプリケーション別フィルタ（Filter by Application）] を選択し、フィルタリングに使用するアプリケーションを選択します。 アプリケーション タイプでフィルタリングするには、[アプリケーション タイプ別フィルタ（Filter by Application Type）] を選択し、フィルタリングに使用するアプリケーション タイプを選択します。
ポリシー（Policy）	ポリシー グループでフィルタリングするには、[ポリシーでフィルタ（Filter by Policy）] を選択し、フィルタリングに使用するポリシー グループ名を入力します。 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。
マルウェア脅威（Malware Threat）	特定のマルウェアの脅威でフィルタリングするには、[マルウェア脅威でフィルタ（Filter by Malware Threat）] を選択し、フィルタリングに使用するマルウェアの脅威名を入力します。 マルウェア カテゴリでフィルタリングするには、[マルウェア カテゴリ別フィルタ（Filter by Malware Category）] を選択し、フィルタリングに使用するマルウェア カテゴリを選択します。説明については、マルウェアのカテゴリについて（5-48 ページ）を参照してください。

表 5-13　[プロキシ サービス（Proxy Services）] タブの Web トラッキング検索条件（続き）

オプション	説明
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別フィルタ（Filter by Reputation Threat）] を選択し、フィルタリングに使用する Web レピュテーションの脅威を入力します。 WBRS スコアの詳細については、『*Cisco IronPort AsyncOS for Web 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）。
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。
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：**このフィルタを有効にすると、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。

ステップ 5　[検索（Search）] をクリックします。

関連項目

- 詳細な Web トラッキング検索結果の表示（5-50 ページ）
- Web トラッキング検索結果について（5-50 ページ）
- Web トラッキング検索結果のトランザクションの詳細の表示（5-50 ページ）
- Web トラッキング機能および高度なマルウェア防御機能について（5-51 ページ）

マルウェアのカテゴリについて

マルウェアのタイプ	説明
アドウェア	アドウェアには、販売目的でユーザを製品に誘導する、すべてのソフトウェア実行可能ファイルおよびプラグインが含まれます。また、これらのプログラムによってセキュリティ設定が変更されて、ユーザがシステム設定を変更できなくなる場合もあります。
ブラウザ ヘルパー オブジェクト	ブラウザ ヘルパー オブジェクトは、広告の表示やユーザ設定の乗っ取りに関連するさまざまな機能を実行するおそれがあるブラウザ プラグインです。
商用システム モニタ	商用システム モニタは、正当な手段によって正規のライセンスで取得できる、システム モニタの特性を備えたソフトウェアです。
ダイヤラ	ダイヤラは、モデムあるいは別のタイプのインターネット アクセスを利用して、ユーザの完全な承諾なしに、長距離通話料のかかる電話回線またはサイトにユーザを接続するプログラムです。
一般的なスパイウェア	スパイウェアはコンピュータにインストールされるタイプのマルウェアで、ユーザに知られることなくその詳細情報を収集します。
ハイジャッカー	ハイジャッカーは、ユーザの承諾なしにユーザを Web サイトに誘導したりプログラムを実行したりできるように、システム設定を変更したり、ユーザのシステムに不要な変更を加えたりします。
既知の悪意のある高リスク ファイル	これらは、高度なマルウェア防御ファイル レピュテーション サービスによって脅威と判定されたファイルです。
その他のマルウェア	このカテゴリは、定義済みのどのカテゴリにも当てはまらないマルウェアと疑わしい動作に使用されます。
フィッシング URL	フィッシング URL は、ブラウザのアドレス バーに表示されます。場合によっては、正当なドメインを模倣したドメイン名が使用されます。
PUA	望ましくないアプリケーションのこと。PUA は、悪質ではないが望ましくないと見なされるアプリケーションです。
システム モニタ	システム モニタには、次のいずれかを実行するソフトウェアが含まれます。 • 公然と、または密かに、システム プロセスやユーザ アクションを記録する。 • これらの記録を後で取得して確認できるようにする。
トロイのダウンローダ	トロイのダウンローダは、インストール後にリモート ホスト/サイトにアクセスして、リモート ホストからパッケージやアフィリエイトをインストールするトロイの木馬です。
トロイの木馬	トロイの木馬は、安全なアプリケーションを装う有害なプログラムです。ウイルスとは異なり、トロイの木馬は自己複製しません。
トロイのフィッシャ	トロイのフィッシャは、感染したコンピュータに潜んで特定の Web ページがアクセスされるのを待ったり、感染したマシンをスキャンしてユーザ名とパスワードを探したりします。
ウィルス	ウイルスは、ユーザが気付かない間にコンピュータにロードされるプログラムまたはコードです。
ワーム	ワームは、コンピュータ ネットワーク上で自己を複製し、悪質なアクションを実行するプログラムまたはアルゴリズムです。

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
- トランザクションを開始したマシンの IP アドレス（IPv4 または IPv6）
- 接続先 Web サイトのドメインまたは IP アドレス（IPv4 または IPv6）
- 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（5-31 ページ）を参照してください。

関連項目

- [L4トラフィックモニタ（L4 Traffic Monitor）] レポート（5-31 ページ）

SOCKS プロキシによって処理されるトランザクションの検索

ブロックまたは完了したトランザクション、トランザクションを開始したクライアント マシンの IP アドレス、および宛先ドメイン、IP アドレス、またはポートなど、さまざまな条件に一致するトランザクションを検索できます。カスタム URL カテゴリ、一致するポリシー、およびユーザの場所（ローカルまたはリモート）により、結果をフィルタリングすることもできます。IPv4 および IPv6 アドレスがサポートされます。

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、[詳細（Advanced）] をクリックします。

ステップ 4　検索条件を入力します。

ステップ 5　[検索（Search）] をクリックします。

関連項目

- [SOCKSプロキシ（SOCKS Proxy）] レポート（5-33 ページ）

Web トラッキングの検索結果の使用

詳細な Web トラッキング検索結果の表示

手順

ステップ 1　返された結果のページをすべて確認してください。

ステップ 2　現在表示されている数よりも多くの結果を各ページに表示するには、[表示された項目（Items Displayed）] メニューからオプションを選択します。

ステップ 3　条件に一致するトランザクションが、[表示された項目（Items Displayed）] メニューで選択できる最大トランザクション数より多い場合は、[印刷可能なダウンロード（Printable Download）] リンクをクリックし、一致するすべてのトランザクションを含む CSV ファイルを取得すると、完全な結果を確認できます。

この CSV ファイルには、関連トランザクションの詳細を除く、raw データ一式が含まれます。

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。

検索結果に表示される情報：

- URL がアクセスされた時刻。
- 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。関連トランザクションの数は、カラム見出しの [すべての詳細を表示(Display All Details)] リンクの下の各行に表示されます。
- 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）。

Web トラッキング検索結果のトランザクションの詳細の表示

内容	操作内容
リスト内の短縮 URL の完全な URL	トランザクションを処理したホスト Web セキュリティ アプライアンスをメモして、そのアプライアンスのアクセスログを確認します。
個々のトランザクションの詳細	[Webサイト（Website）] カラムの URL をクリックします。

内容	操作内容
すべてのトランザクションの詳細	[Webサイト（Website）] カラム見出しの [すべての詳細を表示 ...(Display All Details...)] リンクをクリックします。
500 件までの関連トランザクションのリスト	関連トランザクションの数は、検索結果リストのカラム見出しにある [詳細を表示（Display Details）] リンクの下のカッコ内に表示されます。 トランザクションの [詳細（Details）] ビューで [関連トランザクション（Related Transactions）] リンクをクリックします。

Web トラッキング機能および高度なマルウェア防御機能について

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

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

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

  トラッキングの詳細に表示される [AMP脅威スコア（AMP Threat Score）] は、ファイルを明確に判定できないときにクラウド レピュテーション サービスが提示するベスト エフォート型のスコアです。この場合のスコアは 1 ～ 100 です（AMP 判定が返された場合、またはスコアがゼロの場合は [AMP脅威スコア（AMP Threat Score）] を無視してください）。アプライアンスはこのスコアをしきい値スコア（[セキュリティサービス（Security Services）] > [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] ページで設定）と比較して、実行するアクションを決定します。デフォルトでは、スコアが 60 ～ 100 の場合に悪意のあるファイルと見なされます。デフォルトのしきい値スコアを変更することはお勧めしません。WBRS スコアはファイルのダウンロード元となったサイトのレピュテーションです。このスコアはファイル レピュテーションとは関係ありません。
- 判定のアップデートは [AMP判定のアップデート（AMP Verdict Updates）] レポートでのみ使用できます。Web トラッキングの元のトランザクションの詳細は、判定が変更されても更新されません。特定のファイルが関係するトランザクションを表示するには、判定アップデート レポートで SHA-256 をクリックします。
- 分析結果や分析用にファイルが送信済みかどうかといった、ファイル分析に関する情報は [ファイル分析（File Analysis）] レポートにのみ表示されます。

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

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

関連項目

- SHA-256 ハッシュによるファイルの識別（5-25 ページ）

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。

Web レポーティングおよびトラッキングのトラブルシューティング

- 中央集中型レポーティングが適切に有効化されているのに機能しない（5-52 ページ）
- [高度なマルウェア保護判定のアップデート（Advanced Malware Protection Verdict Updates）] レポートの結果が異なる（5-52 ページ）
- ファイル分析レポートの詳細の表示に関する問題（5-53 ページ）
- 予想されるデータがレポーティングまたはトラッキングの結果に表示されない（5-53 ページ）
- PDF に Web トラッキング データのサブセットのみが表示される（5-54 ページ）
- L4 トラフィック モニタ レポートのトラブルシューティング（5-54 ページ）

すべてのレポートのトラブルシューティング（3-13 ページ）も参照してください。

中央集中型レポーティングが適切に有効化されているのに機能しない

問題　指示どおりに中央集中型 Web レポーティングを有効にしても機能しません。

ソリューション　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 レポーティングは機能しません。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、「ディスク領域の管理」セクション（14-53 ページ）を参照してください。

[高度なマルウェア保護判定のアップデート（Advanced Malware Protection Verdict Updates）] レポートの結果が異なる

問題　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 アプライアンスが同じファイルを分析用に送信し、Web および電子メールの [AMP判定のアップデート（AMP Verdict Updates）] レポートに、そのファイルの異なる判定が表示されます。

ソリューション　これは一時的な違いです。すべての判定アップデートがダウンロードされると、結果は一致します。一致するまでに最大で 30 分かかります。

ファイル分析レポートの詳細の表示に関する問題

ファイル分析レポートの詳細を使用できない

問題　ファイル分析レポートの詳細を使用できません。

ソリューション　ファイル分析レポートの詳細の要件（5-25 ページ）を参照してください。

ファイル分析レポートの詳細を表示する際のエラー

問題　ファイル分析レポートの詳細を表示しようとすると、**使用可能なクラウドサーバ構成がありません**（No cloud server configuration is available）エラーが表示されます。

ソリューション　[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）] に移動して、ファイル分析機能が有効になっている Web セキュリティ アプライアンスを少なくとも 1 つ追加します。

予想されるデータがレポーティングまたはトラッキングの結果に表示されない

問題　予想されるデータがレポーティングまたはトラッキングの結果に表示されません。

ソリューション　考えられる原因：

- 目的の時間範囲を選択したことを確認します。
- トラッキング結果の場合は、一致したすべての結果が表示されていることを確認します。詳細な Web トラッキング検索結果の表示（5-50 ページ）を参照してください。
- Web セキュリティ アプライアンスとCisco コンテンツ セキュリティ管理アプライアンス間のデータ転送が中断されたか、データが消去された可能性があります。[使用可能なデータ（Data Availability）] ページ（5-37 ページ）を参照してください。
- アップグレードによって情報のレポート方法または追跡方法が変更された場合は、アップグレード前に発生したトランザクションが想定どおりに表示されないことがあります。お使いのリリースでこのような変更が行われたかどうかを確認するには、マニュアル（E-1 ページ）に示された場所で該当するリリース ノートを参照してください。
- Web プロキシ サービスのトラッキング検索結果に表示されない結果については、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（5-44 ページ）を参照してください。
- 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リング時の予期しない結果については、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（5-44 ページ）の表の「ユーザ要求（User Request）」行を参照してください。

PDF に Web トラッキング データのサブセットのみが表示される

問題　PDF に [Webトラッキング（Web Tracking）] ページに表示されるデータの一部だけが表示されます。

ソリューション　PDF および CSV ファイルで表示されるデータと除外されるデータについては、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（3-10 ページ）の表で Web トラッキングの情報を参照してください。

L4 トラフィック モニタ レポートのトラブルシューティング

Web プロキシが転送プロキシとして設定され、L4 トラフィック モニタがすべてのポートをモニタするように設定されている場合、プロキシのデータ ポートの IP アドレスが記録され、クライアント IP アドレスとしてレポートに表示されます。Web プロキシがトランスペアレント プロキシとして設定されている場合は、クライアント IP アドレスが正しく記録され、表示されるように IP スプーフィングを有効にします。方法については、『*Cisco IronPort AsyncOS for Web User Guide*』を参照してください。

関連項目

- [クライアントマルウェアリスク（Client Malware Risk）] レポート（5-27 ページ）
- L4 トラフィック モニタによって処理されたトランザクションの検索（5-49 ページ）

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

Cisco 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 か所で追跡できます。

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：**指定された日時の間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。または拒否された接続を検索結果に表示します。
- **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。名前に対してクエリーが実行された少なくとも 1 つの添付ファイルを含む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。

トラッキングできない添付ファイルもあります。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、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の、他のスキャン操作の一部としてのみ実行されます。添付ファイル名は、添付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に対してのみ使用できます。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いるときに、メッセージがドロップされるか、またはその添付ファイルがアンチスパムまたはアンチウイルス フィルタによって削除された場合
  - 本文スキャンが実行される前に、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削除された場合

- **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 トラッキングの有効化（6-2 ページ）
- 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（6-3 ページ）
- 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（6-3 ページ）

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 トラッキングの有効化

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ール トラッキング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。

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　[設定の編集（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、有効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 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　中央集中型メッセージ トラッキング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、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（13-25 ページ）を参照してください。

有効なメッセージ トラッキング データの検査

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。

手順

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）[詳細設定（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。エントリ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。エントリ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。

  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済みのメッセージのみが検索結果に表示されます。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、拒否された接続のみ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 アドレスは、コロンで区切られた 8 セットの 16 ビット 16 進数値で構成されます。1 か所で、*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、[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）]、[含まれている悪意のあるURL（contained malicious URLs）]、[指定されたカテゴリに含まれているURL（contained URL in specified category）]、[DLP違反（DLP Violations）]（DLP ポリシーの名前を入力して、違反の重大度または実行アクションを選択できます）、[DMARC違反（DMARC violations）]、[送信完了（Delivered）]、[高度なマルウェア保護ポジティブ（Advanced Malware Protection Positive）]（添付ファイルで検出されるマルウェア用）、[ハードバウンス（Hard Bounced）]、[ソフトバウンス（Soft Bounced）]、[現在、ポリシー隔離に隔離（currently in policy quarantine）]、[現在、ウイルス隔離に隔離（currently in virus quarantine）]、[現在、アウトブレイク隔離に隔離（currently in outbreak quarantine）]、[メッセージフィルタで検出（caught by message filters）]、[コンテンツフィルタで検出（caught by content filters）]、[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 minutes）]、[2分（2 minutes）]、[5分（5 minutes）]、[10分（10 minutes）]、および [時間制限なし（No time limit）] です。また、クエリーが返す結果の最大数を選択します（最大 1000）。
- [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。

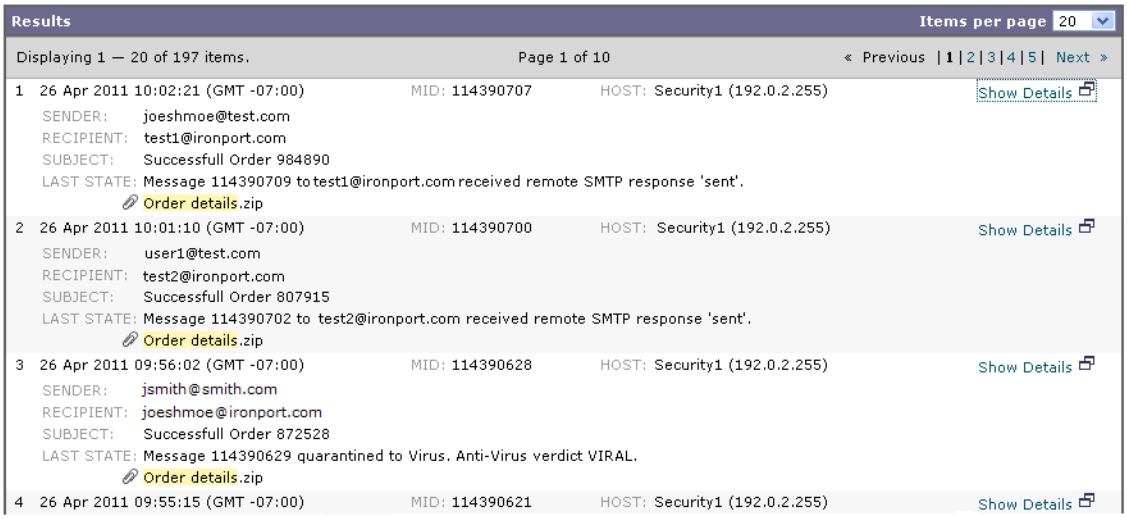
  SHA-256 ハッシュに基づいたファイルの識別方法については、SHA-256 ハッシュによるファイルの識別（4-32 ページ）を参照してください。

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 [ページ当たりの項目数（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。

関連項目

- 結果セットの絞り込み（6-7 ページ）
- メッセージ トラッキングおよび高度なマルウェア防御機能について（6-8 ページ）
- トラッキング クエリー結果について（6-9 ページ）

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、検索精度を高めます。

- Date and time
- Message ID（MID）
- ホスト（電子メール セキュリティ アプライアンス）
- 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、検索精度を高めます。

[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、さらに検索精度を高めます。

（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。

メッセージ トラッキングおよび高度なマルウェア防御機能について

メッセージ トラッキングのファイル脅威情報を検索する際は、次の点に注意してください。

- ファイル レピュテーション サービスで検出された悪質なファイルを検索するには、メッセージ トラッキングの [詳細設定（Advanced）] セクションで、[メッセージイベント（Message Event）] オプションの [高度なマルウェア保護ポジティブ（Advanced Malware Protection Positive）] を選択します。
- メッセージ トラッキングにはファイル レピュテーション処理についての情報と、メッセージが処理されたときに返された元のファイル レピュテーションの判定のみが含まれます。たとえば最初にファイルがクリーンであると判断され、その後、判定のアップデートでそのファイルが悪質であると判断された場合、クリーンの判定のみがトラッキング結果に表示されます。

  メッセージ トラッキングの詳細の [処理詳細（Action Details）] セクションには、次の情報が表示されます。

  - メッセージの各添付ファイルの SHA-256
  - メッセージ全体に対する高度なマルウェア防御の最終判定
  - マルウェアが検出された添付ファイル

    クリーンな添付ファイルおよびスキャンできない添付ファイルの情報は表示されません。
- 判定のアップデートは [AMP判定のアップデート（AMP Verdict Updates）] レポートでのみ使用できます。メッセージ トラッキングの元のメッセージの詳細は、判定が変更されても更新されません。特定の添付ファイルを含むメッセージを表示するには、判定アップデート レポートで SHA-256 をクリックします。

- 分析結果や分析用にファイルが送信済みかどうかといった、ファイル分析に関する情報は [ファイル分析（File Analysis）] レポートにのみ表示されます。

  分析済みファイルのその他の情報は、クラウドから入手できます。ファイルの使用可能なファイル分析情報を表示するには、[モニタ（Monitor）] > [ファイル分析（File Analysis）] を選択して、ファイルを検索する SHA-256 を入力します。ファイル分析サービスによってソースのファイルが分析されると、その詳細を表示できます。分析されたファイルの結果だけが表示されます。

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

関連項目

- SHA-256 ハッシュによるファイルの識別（4-32 ページ）

トラッキング クエリー結果について

結果が予期したものでない場合は、メッセージ トラッキングのトラブルシューティング（6-11 ページ）を参照してください。

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」セクション（6-10 ページ）を参照してください。

メモ

- 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に、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有効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（3-10 ページ）を参照してください。

関連項目

- メッセージの詳細（6-10 ページ）

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（Envelope and Header Summary）

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。表示される情報は次のとおりです。

[受信時刻（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「なし（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（Sending Host Summary）

[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「なし（None）」の場合、そのメッセージが処理された時点で、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（Processing Details）

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無効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（13-25 ページ）を参照してください。

メッセージ トラッキングのトラブルシューティング

予想されるメッセージが検索結果に表示されない

問題　条件に一致するメッセージが検索結果に含まれていません。

ソリューション

- 多くの検索（特にメッセージ イベント検索）は、アプライアンスの設定によって結果が異なります。たとえばフィルタ処理していない URL カテゴリを検索すると、メッセージにそのカテゴリの URL が含まれていても、結果には表示されません。意図した動作を実現するように電子メール セキュリティ アプライアンスが正しく設定されていることを確認します。メール ポリシー、コンテンツ フィルタおよびメッセージ フィルタ、隔離の設定などを確認してください。
- 有効なメッセージ トラッキング データの検査（6-4 ページ）を参照してください。
- レポートのリンクをクリックしても予想される情報が表示されない場合は、電子メール レポートのトラブルシューティング（4-50 ページ）を参照してください。

添付ファイルが検索結果に表示されない

問題　添付ファイル名が検出されず、検索結果に表示されません。

ソリューション　設定要件（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 トラッキングの有効化（6-2 ページ））および添付ファイル名検索の制約事項（トラッキング サービスの概要（6-1 ページ））を参照してください。

スパム隔離

スパム隔離の概要

スパム隔離（別名 ISQ、エンドユーザ隔離、および EUQ）は、「誤検出」（アプライアンスが正規の電子メール メッセージをスパムと見なすこと）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。アプライアンスによって、スパムまたはその疑いがあるメッセージであると判断された場合、そのメッセージを配信または削除する前に受信者または管理者にメッセージを確認してもらうことをお勧めします。スパム隔離はこのためにメッセージを保存します。

電子メール セキュリティ アプライアンスの管理ユーザは、スパム隔離内のすべてのメッセージを閲覧できます。一般的にメッセージの受信者であるエンド ユーザは、若干異なる Web インターフェイスで自身の隔離されたメッセージを閲覧できます。

スパム隔離は、ポリシー、ウイルス、アウトブレイク隔離とは異なります。

ローカルのスパム隔離と外部のスパム隔離

ローカルのスパム隔離では、Web Security applianceでスパムおよびスパムの疑いがあるメッセージなどを保存します。外部のスパム隔離は、別の Cisco コンテンツ セキュリティ管理アプライアンスでこれらのメッセージを保存できます。

次の場合は外部のスパム隔離の使用を検討してください。

- 複数の電子メール セキュリティ アプライアンスからのスパムを一元化して保存および管理する必要がある。

- 電子メール セキュリティ アプライアンスで保持可能な量より多くのスパムを保存する必要がある。
- スパム隔離とそのメッセージを定期的にバックアップする必要がある。

関連項目

- スパム隔離の有効化と設定（7-3 ページ）
- スパム隔離へのブラウザ アクセス用 IP インターフェイスの設定（7-6 ページ）
- スパム隔離への管理ユーザ アクセスの設定（7-6 ページ）
- 隔離対象のメールの受信者の制限（7-7 ページ）
- メッセージ テキストが正しく表示されることの確認（7-8 ページ）
- スパム隔離の言語（7-8 ページ）

中央集中型スパム隔離の設定

	操作内容	詳細情報
ステップ 1	セキュリティ管理アプライアンスで、中央集中型スパム隔離サービスを有効にします。	スパム隔離の有効化と設定（7-3 ページ）
ステップ 2	セキュリティ管理アプライアンスで、中央集中型スパム隔離に含める電子メール セキュリティ アプライアンスを指定します。	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（7-4 ページ）
ステップ 3	通知およびリリースされたスパムの送信用にセキュリティ管理アプライアンスを設定します。	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（7-5 ページ）
ステップ 4	セキュリティ管理アプライアンスで、スパム隔離のブラウザ インターフェイスを設定します。	スパム隔離へのブラウザ アクセス用 IP インターフェイスの設定（7-6 ページ）
ステップ 5	電子メール セキュリティ アプライアンスがスパム隔離にメールを送信するように設定されていることを確認します。	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で、アンチスパムおよびメール ポリシーの設定に関する情報を参照してください。関連するセクションへのリンクは、ローカルのスパム隔離の設定に関するセクションの表に記載されています。
ステップ 6	電子メール セキュリティ アプライアンスで外部のスパム隔離を有効にし、設定します。	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を参照してください。
ステップ 7	電子メール セキュリティ アプライアンスでローカル隔離を無効にします。	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で、外部のスパム隔離をアクティブ化するためのローカルのスパム隔離の無効化に関する情報を参照してください。

スパム隔離の有効化と設定

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）] > [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、スパム隔離を初めて有効にする場合は、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。

スパム隔離の設定を編集する場合は、[設定の編集（Edit Settings）] をクリックします。

ステップ 3　次のオプションを指定します。

オプション	説明
隔離IPインターフェイス（Quarantine IP Interface） 隔離ポート（Quarantine Port）	デフォルトでは、スパム隔離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。
次を使用してメッセージを配信（Deliver Messages Via）	隔離関係のすべての送信電子メール（スパム通知やスパム隔離からリリースされたメッセージなど）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信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 サーバを使用してルーティングできます。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 Data 2 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。
次の日数の経過後に削除（Schedule Delete After）	メッセージを削除する前に保持する日数を指定します。 隔離エリアの容量が満杯になるのを防ぐために、古いメッセージから削除するように隔離を設定することを推奨します。自動削除をスケジュールしないという選択も可能です。
メッセージのリリース時にシスコに通知（Notify Cisco Upon Message Release）	—

オプション	説明
スパム隔離のアピアランス（Spam Quarantine Appearance）	**ロゴ（Logo）** デフォルトでは、ユーザがログインして隔離されたメッセージを確認するときに、スパム隔離のページの最上部にシスコ ロゴが表示されます。 代わりにカスタム ロゴを使用するには、そのロゴをアップロードします。ロゴは、高さ 50 ピクセル、幅 500 ピクセルまでの .jpg、.gif、または .png ファイルにする必要があります。
	ログインページのメッセージ（Login page message） （任意）ログイン ページ メッセージを指定します。このメッセージは、隔離を閲覧するためにエンド ユーザおよび管理者がログインするときに表示されます。 メッセージを指定しない場合、次のメッセージが表示されます。 ログイン情報を入力してください。入力する情報がわからない場合は、管理者に問い合わせてください。（Enter your login information below. If you are unsure what to enter, please contact your administrator.）
管理ユーザ（Administrative Users）	スパム隔離への管理ユーザ アクセスの設定（7-6 ページ）を参照してください。

ステップ 4　変更を送信し、保存します。

次の作業

- 中央集中型スパム隔離の設定（7-2 ページ）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（Appliance Name）] および [IPアドレス（IP Address）] テキスト フィールドに、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. 成功の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　スパム隔離を有効にする電子メール 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。

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。

はじめる前に

発信インターフェイスに使用する 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、次をを参照してください。付録 B「ネットワーク アドレスと IP アドレスの割り当て」

手順

ステップ 1　この手順は、次のセクションの説明と併せて実行してください。付録 B「ネットワーク アドレスと IP アドレスの割り当て」

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（Name）
- イーサネット ポート（Ethernet Port）

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、[次を使用してメッセージを配信（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（IP Address）

  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（Netmask）
- ホスト名（Hostname）

  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。

スパム隔離へのブラウザ アクセス用 IP インターフェイスの設定

管理者およびエンド ユーザがスパム隔離にアクセスするときには、別のブラウザ ウィンドウが開きます。

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　**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。

- デフォルトでは、HTTP がポート 82 を使用し、HTTPS がポート 83 を使用します。
- 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。

  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エンド ユーザに表示したくない場合は、代わりのホスト名を指定できます。

ステップ 4　変更を送信し、保存します。

次の作業

スパム隔離アクセス用に指定したホスト名を DNS サーバが解決できることを確認します。

スパム隔離への管理ユーザ アクセスの設定

管理者権限を持つすべてのユーザは、スパム隔離設定を変更したり、スパム隔離内のメッセージを表示および管理したりすることができます。管理者ユーザに対してスパム隔離アクセスを設定する必要はありません。

次のロールのユーザに対してスパム隔離へのアクセスを設定すると、これらのユーザはスパム隔離内のメッセージを表示、リリース、削除できます。

- メール管理者（Email administrator）
- オペレータ（Operator）
- 読み取り専用オペレータ（Read-Only operator）
- ヘルプ デスク ユーザ（Help Desk user）
- ゲスト（Guest）
- スパム隔離権限を持つカスタム ユーザ ロール

これらのユーザはスパム隔離設定にアクセスできません。

はじめる前に

スパム隔離にアクセスできるユーザまたはカスタム ユーザ ロールを作成します。詳細については、第 13 章「管理タスクの分散について」でカスタム ユーザ ロールの隔離へのアクセス（13-7 ページ）に関する情報を参照してください。

手順

ステップ 1　スパム隔離設定ページをまだ編集していない場合は、次の手順を実行します。

a. [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。

b. [設定の編集（Edit Settings）] をクリックします。

ステップ 2　追加するユーザ タイプ（ローカル、外部認証、またはカスタム ロール）のリンクをクリックします。

ユーザまたはロールを追加済みの場合は、ユーザ名かロールをクリックすると、すべての対象ユーザまたはロールが表示されます。

ステップ 3　追加するユーザまたはロールを選択します。

管理者権限を持つユーザは（電子メール管理者を含む）、自動的にスパム隔離への完全なアクセス権が付与されるため表示されません。

ステップ 4　[OK] をクリックします。

ステップ 5　変更を送信し、保存します。

関連項目

- スパム隔離へのエンドユーザ アクセスの設定（7-19 ページ）

隔離対象のメールの受信者の制限

電子メール セキュリティ アプライアンスで複数のメール ポリシーを使用して（[メールポリシー（Mail Policies）] > [受信メールポリシー（Incoming Mail Policy）]）、メールの隔離対象から除外する受信者アドレスのリストを指定できます。そのメール ポリシーにアンチスパムを設定する際、隔離の代わりに [配信（Deliver）] または [ドロップ（Drop）] を選択します。

メッセージ テキストが正しく表示されることの確認

AsyncOS では、メッセージ ヘッダーに指定されたエンコーディングに基づいてメッセージの文字セットが決定されます。しかし、ヘッダーに指定されたエンコーディングが実際のテキストと一致していないと、そのメッセージは、スパム隔離内で閲覧される際に正しく表示されません。このような状況は、スパム メッセージの場合に発生することがよくあります。

これらのメッセージのメッセージ テキストが適切に表示されるようにするには、お使いの電子メール セキュリティ アプライアンスに関するマニュアルの「スパム隔離」の章に記載されたデフォルト エンコーディングを指定する手順を参照してください。

スパム隔離の言語

各ユーザは、ウィンドウの右上にある [オプション(Options)] メニューからスパム隔離の言語を選択します。

[スパム隔離の編集(Edit Spam Quarantine)] ページ

- スパム隔離の有効化と設定(7-3 ページ)
- ローカルのスパム隔離と外部のスパム隔離(7-1 ページ)
- スパム隔離の有効化と設定(7-3 ページ)
- スパム隔離へのエンドユーザ アクセスの設定(7-19 ページ)
- エンド ユーザへの隔離されたメッセージに関する通知(7-20 ページ)

セーフリストおよびブロックリストを使用した送信者に基づく電子メール配信の制御

管理者およびエンド ユーザは、メッセージがスパムであるかどうかを判断するためにセーフリストとブロックリストを使用できます。セーフリストでは、スパムとして処理しない送信者およびドメインが指定されます。ブロックリストでは、常にスパムとして処理する送信者およびドメインが指定されます。

エンド ユーザ(電子メール ユーザ)に各自の電子メール アカウントのセーフリストとブロックリストの管理を許可することができます。たとえば、エンド ユーザは、もう興味のないメーリング リストから電子メールを受信している場合があります。そのようなユーザは、このメーリング リストからの電子メールが自分の受信箱に送信されないように、その送信者を自分のブロックリストに追加できます。また、エンド ユーザは、スパムではない特定の送信者からの電子メールが自分のスパム隔離に送信されていることに気づくこともあります。これらの送信者からのメッセージが隔離されないようにするために、エンド ユーザはそれらの送信者を自分のセーフリストに追加できます。

エンド ユーザおよび管理者が行った変更はお互いに表示され、両者が変更できます。

関連項目

- セーフリストとブロックリストのメッセージ処理(7-9 ページ)
- セーフリストとブロックリストの有効化(7-10 ページ)

セーフリストとブロックリストのメッセージ処理

セーフリストまたはブロックリストに送信者を追加しても、アプライアンスでは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が行われます。受信者のセーフリストにメッセージの送信者が含まれていても、他のスキャン設定と結果によってはメッセージが配信されない場合があります。

セーフリストとブロックリストを有効にすると、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。アプライアンスがセーフリストまたはブロックリストのエントリに一致する送信者またはドメインを検出した場合、受信者が複数存在すると（かつ各受信者のセーフリスト/ブロックリスト設定が異なると）、そのメッセージは分裂します。たとえば、受信者 A と受信者 B の両方に送信されるメッセージがあるとします。受信者 A のセーフリストにはこの送信者のエントリがありますが、受信者 B のセーフリストおよびブロックリストには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 に送信されるメッセージは、セーフリストに一致していることが *X-SLBL-Result-Safelist* ヘッダーによってマークされ、アンチスパム スキャンをスキップします。一方、受信者 B 宛のメッセージは、アンチスパム スキャン エンジンによってスキャンされます。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の配信の動作は、セーフリスト/ブロックリスト機能を有効にするときに指定したブロックリスト アクション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。隔離を実行するようにブロックリスト アクションが設定されている場合、そのメッセージはスキャンされ、最終的に隔離されます。削除するようにブロックリスト アクションが設定されている場合、そのメッセージは、セーフリスト/ブロックリスト スキャンの直後にドロップされます。

セーフリストとブロックリストはスパム隔離内に保持されているため、配信の動作は、他のアンチスパム設定にも左右されます。たとえば、アンチスパム スキャンをスキップするようにホスト アクセス テーブル（HAT）で「承認（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は、自分のセーフリストとブロックリストの設定がそのリスナー上で受信されたメールに適用されなくなります。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。

関連項目

- セーフリストとブロックリストの有効化（7-10 ページ）
- 外部スパム隔離およびセーフリスト/ブロックリスト（7-10 ページ）

セーフリストとブロックリストの有効化

はじめる前に

- スパム隔離を有効にする必要があります。中央集中型スパム隔離の設定（7-2 ページ）を参照してください。
- 外部セーフリスト/ブロックリストを使用するように電子メール セキュリティ アプライアンスを設定します。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で外部スパム隔離を設定する手順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）] > [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　[エンドユーザセーフリスト/ブロックリスト（スパム隔離）（End-User Safelist/Blocklist (Spam Quarantine)）] セクションで [有効（Enable）] を選択します。

ステップ 3　[エンドユーザセーフリスト/ブロックリスト機能を有効にする（Enable End User Safelist/Blocklist Feature）] を選択します。

ステップ 4　[ユーザごとの最大一覧項目数（Maximum List Items Per User）] を指定します。

これは、各受信者のリストごとのアドレスまたはドメインの最大数です。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 5　更新頻度を選択します。この値によって、外部スパム隔離を使用する電子メール セキュリティ アプライアンスのセーフリスト/ブロックリストを AsyncOS が更新する頻度が決まります。この設定の意味については、外部スパム隔離およびセーフリスト/ブロックリスト（7-10 ページ）で説明します。

ステップ 6　変更を送信し、保存します。

外部スパム隔離およびセーフリスト/ブロックリスト

電子メール セキュリティ アプライアンスは受信メールの処理時にセーフリストとブロックリスト内の送信者を評価するため、セキュリティ管理アプライアンスに保存されているセーフリストおよびブロックリストが受信メールに適用されるように、これらを電子メール セキュリティ アプライアンスに送信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セーフリスト/ブロックリスト機能を設定する際に、その更新頻度を設定します。

セーフリストおよびブロックリストへの送信者とドメインの追加（管理者）

スパム隔離のインターフェイスでセーフリストとブロックリストを管理します。

多数の受信者（組織のエンド ユーザ）が特定の送信者またはドメインをホワイトリストまたはブラックリストに追加しているかどうかも確認できます。

管理者は、各エンド ユーザが表示および操作する同じエントリのスーパーセットを表示して操作します。

はじめる前に

- スパム隔離にアクセスできることを確認します。スパム隔離へのアクセス（管理ユーザ）（7-24 ページ）を参照してください。
- セーフリスト/ブロックリストへのアクセスを有効にします。セーフリストとブロックリストの有効化（7-10 ページ）を参照してください。
- （任意）このセクションの手順を使用してこれらのリストを作成する代わりに、セーフリスト/ブロックリストをインポートするには、セーフリスト/ブロックリストのバックアップと復元（7-14 ページ）で説明する手順を使用します。
- セーフリストとブロックリストのエントリの必須形式を把握します。セーフリスト エントリとブロックリスト エントリの構文（7-12 ページ）を参照してください。

手順

ステップ 1　ブラウザを使用してスパム隔離にアクセスします。

ステップ 2　ログインします。

ステップ 3　ページの右上にある [オプション（Options）] ドロップダウン メニューを選択します。

ステップ 4　[セーフリスト（Safelist）] または [ブロックリスト（Blocklist）] を選択します。

ステップ 5　（任意）送信者または受信者を検索します。

ステップ 6　次の 1 つまたは複数の操作を実行します。

目的	操作内容
1 人の受信者に対して複数の送信者を追加する	1. [表示方法：受信者（View by: Recipient）] を選択します。 2. [追加（Add）] をクリックするか、受信者の [編集（Edit）] をクリックします。 3. 受信者の電子メール アドレスを入力または編集します。 4. 送信者の電子メール アドレスおよびドメインを入力します。 各エントリを別の行に入力するか、各エントリをカンマで区切ります。 5. [送信（Submit）] をクリックします。
1 人の送信者に対して複数の受信者を追加する	1. [表示方法：送信者（View by: Sender）] を選択します。 2. [追加（Add）] をクリックするか、または送信者の [編集（Edit）] をクリックします。 3. 送信者アドレスまたはドメインを入力または編集します。 4. 受信者の電子メール アドレスを入力します。 各エントリを別の行に入力するか、各エントリをカンマで区切ります。 5. [送信（Submit）] をクリックします。

目的	操作内容
受信者に関連付けられたすべての送信者を削除する 送信者に関連付けられたすべての受信者を削除する	1. [表示方法(View by)] オプションを選択します。 2. ゴミ箱アイコンをクリックしてテーブル行全体を削除します。
受信者の個々の送信者を削除する 送信者の個々の受信者を削除する	1. [表示方法(View by)] オプションを選択します。 2. 個々の受信者または送信者の [編集(Edit)] をクリックします。 3. テキスト ボックスでエントリを追加または削除します。少なくとも 1 つはエントリを残す必要があります。 4. [送信(Submit)] をクリックします。

関連項目

- セーフリスト エントリとブロックリスト エントリの構文(7-12 ページ)
- すべてのセーフリストおよびブロックリストのクリア(7-12 ページ)

セーフリスト エントリとブロックリスト エントリの構文

送信者を次の形式でセーフリストとブロックリストに追加できます。

- user@domain.com
- server.domain.com
- domain.com
- [10.1.1.0]
- [ipv6:2001:DB8:1::1]
- user@[1.2.3.4]
- user@[ipv6:2001:db8::1]

送信者アドレスやドメインなどの同一エントリを、セーフリストとブロックリストの両方に同時に追加することはできません。ただし、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送信者の電子メール アドレスをブロックリストに追加すること(またはその逆)は可能です。両方のルールが適用されます。たとえば *example.com* がセーフリストに含まれている場合、*george@example.com* をブロックリストに追加することができます。この場合アプライアンスは、スパムとして処理される *george@example.com* からのメールを除いて、*example.com* からのすべてのメールをスパムのスキャンなしで配信します。

.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、ブロックしたりすることはできません。ただし、*server.domain.com* のような構文を使用して、特定のドメインをブロックすることはできます。

すべてのセーフリストおよびブロックリストのクリア

すべての送信者と受信者を含む、セーフリストおよびブロックリストのすべてのエントリを削除する必要がある場合は、セーフリスト/ブロックリストのバックアップと復元(7-14 ページ)の手順を使用してエントリなしでファイルをインポートします。

セーフリストおよびブロックリストへのエンドユーザ アクセスについて

エンド ユーザはスパム隔離から各自のセーフリストとブロックリストにアクセスします。スパム隔離へのエンドユーザ アクセスを設定するには、Web ブラウザからのスパム隔離へのエンドユーザ アクセスの設定（7-18 ページ）を参照してください。

必要に応じて、スパム隔離の URL と下記の手順をエンド ユーザに提供してください。

関連項目

- セーフリストへのエントリの追加（エンド ユーザ）（7-13 ページ）
- ブロックリストへの送信者の追加（エンド ユーザ）（7-14 ページ）

セーフリストへのエントリの追加（エンド ユーザ）

（注）　セーフリストに登録されている送信者からのメッセージの配信は、システムの他の設定によって異なります。セーフリストとブロックリストのメッセージ処理（7-9 ページ）を参照してください。

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。

- 隔離されたメッセージの送信者のセーフリストへの追加（7-13 ページ）
- 隔離されたメッセージのない送信者のセーフリストへの追加（7-13 ページ）

隔離されたメッセージの送信者のセーフリストへの追加

エンド ユーザは、スパム隔離に送信されたメッセージの送信者をセーフリストに追加できます。

手順

ステップ 1　スパム隔離から、メッセージの横にあるチェックボックスをオンにします。

ステップ 2　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）] を選択します。

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 パイプライン内のワーク 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。

隔離されたメッセージのない送信者のセーフリストへの追加

手順

ステップ 1　ブラウザからスパム隔離にアクセスします。

ステップ 2　ページの右上にある [オプション（Options）] ドロップダウン メニューを選択します。

ステップ 3　[セーフリスト（Safelist）] を選択します。

ステップ 4　[セーフリスト(Safelist)] ダイアログボックスから、電子メール アドレスまたはドメインを入力します。ドメインと電子メール アドレスは、コンマで区切って複数入力できます。

ステップ 5　[一覧に追加(Add to List)] をクリックします。

ブロックリストへの送信者の追加(エンド ユーザ)

ブロックリストに登録されている送信者からのメッセージは、管理者が定義したセーフリスト/ブロックリスト アクション設定に応じて、拒否または隔離されます。

(注)　この手順でのみブロックリスト エントリを追加できます。

手順

ステップ 1　スパム隔離にログインします。

ステップ 2　ページの右上にある [オプション(Options)] ドロップダウン メニューを選択します。

ステップ 3　ブロックリストに追加するドメインまたは電子メール アドレスを入力します。ドメインと電子メール アドレスは、コンマで区切って複数入力できます。

ステップ 4　[一覧に追加(Add to List)] をクリックします。

セーフリスト/ブロックリストのバックアップと復元

アプライアンスのアップグレード前またはインストール ウィザードの実行前に、セーフリスト/ブロックリスト データベースをバックアップする必要があります。セーフリスト/ブロックリストの情報は、アプライアンスの設定が格納されるメインの XML コンフィギュレーション ファイルには含まれていません。

セーフリスト/ブロックリスト エントリは、セキュリティ管理アプライアンスの他のデータとともにバックアップすることもできます。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(14-8 ページ)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)] > [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。

目的	操作内容
セーフリスト/ブロックリストをエクスポートする	.csv ファイルのパスおよびファイル名をメモし、必要に応じて変更します。 [今すぐバックアップ（Backup Now）] をクリックします。 アプライアンスは次の命名規則を使用して、アプライアンスの /configuration ディレクトリに .csv ファイルを保存します。 *slbl<serial number><timestamp>.csv*
セーフリスト/ブロックリストをインポートする	⚠ **注意**　このプロセスによって、すべてのユーザのセーフリストおよびブロックリストの既存のエントリがすべて上書きされます。 [リストアするファイルを選択（Select File to Restore）] をクリックします。 configuration ディレクトリ内のファイル リストから目的のファイルを選択します。 復元するセーフリスト/ブロックリスト バックアップ ファイルを選択します。 [復元（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

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_log ファイルまたはアンチスパム ログ ファイルに記録されます。セーフリストに含まれる電子メールは、セーフリストに一致していることが *X-SLBL-Result-セーフリスト* ヘッダーによってマークされます。ブロックリストに含まれる電子メールは、ブロックリストに一致していることが *X-SLBL-Result-ブロックリスト* ヘッダーによってマークされます。

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（14-34 ページ）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。

関連項目

- セーフリストに登録されている送信者からのメッセージが配信されない（7-15 ページ）

セーフリストに登録されている送信者からのメッセージが配信されない

問題　セーフリストに登録されている送信者からのメッセージが配信されませんでした。

ソリューション　考えられる原因：

- マルウェアまたはコンテンツ違反のためメッセージがドロップされました。セーフリストとブロックリストのメッセージ処理（7-9 ページ）を参照してください。

- アプライアンスが複数あり、その送信者をセーフリストに最近追加した場合、メッセージが処理された時点ではセーフリスト/ブロックリストが同期されていなかった可能性があります。外部スパム隔離およびセーフリスト/ブロックリスト（7-10 ページ）を参照してください。

エンド ユーザのためのスパム管理機能の設定

目的	参照先
スパム管理機能へのエンドユーザ アクセスのさまざまな認証方式について、利点と制限事項を把握します。	スパム隔離へのエンドユーザ アクセスの設定（7-19 ページ）およびサブセクション
エンド ユーザがブラウザから直接スパム隔離にアクセスすることを許可します。	スパム管理機能にアクセスするエンド ユーザの認証オプション（7-16 ページ）
メッセージがスパム隔離にルーティングされたときに、その宛先のユーザに通知を送信します。 通知にはスパム隔離へのリンクを含めることができます。	エンド ユーザへの隔離されたメッセージに関する通知（7-20 ページ）
ユーザが、安全であると判断した送信者、およびスパムまたはその他の無用なメールを送信すると判断した送信者の電子メール アドレスとドメインを指定できるようにします。	セーフリストおよびブロックリストを使用した送信者に基づく電子メール配信の制御（7-8 ページ）

関連項目

- スパム管理機能にアクセスするエンド ユーザの認証オプション（7-16 ページ）
- Web ブラウザからのスパム隔離へのエンドユーザ アクセスの設定（7-18 ページ）
- エンド ユーザへの隔離されたメッセージに関する通知（7-20 ページ）

スパム管理機能にアクセスするエンド ユーザの認証オプション

（注） メールボックス認証では、ユーザが電子メール エイリアス宛てのメッセージを表示することはできません。

エンド ユーザの場合 スパム隔離へのアクセス	操作内容
Web ブラウザから直接アクセス、認証必須 および 通知内のリンク経由でアクセス、認証必須	1. [エンドユーザ隔離アクセス（End User Quarantine Access）] 設定で、[LDAP] または [メールボックス（IMAP/POP）（Mailbox (IMAP/POP)）] を選択します。 2. [スパム通知（Spam Notifications）] 設定で、[隔離へのアクセスに証明書なしのログインを有効にする（Enable login without credentials for quarantine access）] の選択を解除します。

エンド ユーザの場合 スパム隔離へのアクセス	操作内容
Web ブラウザから直接アクセス、認証必須 および 通知内のリンク経由でアクセス、認証不要	1. [エンドユーザ隔離アクセス（End User Quarantine Access）] 設定で、[LDAP] または [メールボックス(IMAP/POP)（Mailbox (IMAP/POP)）] を選択します。 2. [スパム通知（Spam Notifications）] 設定で、[隔離アクセスにクレデンシャルなしのログインを有効にする（Enable login without credentials for quarantine access）] をオンにします。
通知内のリンク経由でのみアクセス、認証不要	[エンドユーザ隔離アクセス（End User Quarantine Access）] 設定で、認証方式として [なし（None）] を選択します。
アクセスなし	[エンドユーザ隔離アクセス（End User Quarantine Access）] 設定で、[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）] の選択を解除します。

関連項目

- LDAP 認証プロセス（7-17 ページ）
- IMAP/POP 認証プロセス（7-18 ページ）
- スパム隔離へのエンドユーザ アクセスの設定（7-19 ページ）
- エンド ユーザへの隔離されたメッセージに関する通知（7-20 ページ）
- スパム隔離と連携させるための LDAP の設定（11-1 ページ）
- セーフリストおよびブロックリストへのエンドユーザ アクセスについて（7-13 ページ）

LDAP 認証プロセス

1. ユーザが自分のユーザ名とパスワードを Web UI ログイン ページに入力します。
2. スパム隔離は、匿名検索を実行するように、または指定された「サーバ ログイン」DN とパスワードによる認証ユーザとして、指定された LDAP サーバに接続します。Active Directory の場合、一般に「グローバル カタログ ポート」（6000 番台）上でサーバ接続を確立する必要があり、検索を実行するために、スパム隔離がバインドできる低い特権 LDAP ユーザを作成する必要があります。
3. 次に、スパム隔離は、指定された BaseDN とクエリー ストリングを使用してユーザを検索します。ユーザの LDAP レコードが見つかると、スパム隔離は、そのレコードの DN を抽出し、ユーザ レコードの DN と最初にユーザが入力したパスワードを使用してディレクトリへのバインドを試みます。このパスワード チェックに成功すると、ユーザは正しく認証されます。しかしまだ、スパム隔離は、そのユーザに対してどのメールボックスの内容を表示するのか決定する必要があります。
4. メッセージは、受信者のエンベロープ アドレスを使用してスパム隔離に保管されます。ユーザのパスワードが LDAP に対して検証された後、スパム隔離は、「プライマリ電子メール属性」を LDAP レコードから取得して、どのエンベロープ アドレスの隔離されたメッセージを表示する必要があるのか決定します。「プライマリ電子メール属性」には、電子メール アドレスが複数格納されている場合があり、これらのアドレスを使用して、隔離からどのエンベロープ アドレスが認証ユーザに対して表示される必要があるのか決定されます。

関連項目

- 第 11 章「LDAP との統合」

IMAP/POP 認証プロセス

1. メール サーバ設定に応じて、ユーザは、自分のユーザ名（joe）または電子メール アドレス（joe@example.com）と、パスワードを Web UI ログイン ページに入力します。ユーザに電子メール アドレスをフルに入力する必要があるのか、ユーザ名だけを入力すればよいのか知らせるために、ログイン ページ メッセージを変更できます（スパム隔離へのエンドユーザ アクセスの設定（7-19 ページ）を参照）。
2. スパム隔離は、IMAP サーバまたは POP サーバに接続し、入力されたログイン名（ユーザ名または電子メール アドレス）とパスワードを使用して IMAP/POP サーバへのログインを試みます。パスワードが受け入れられると、そのユーザは認証されたと見なされ、スパム隔離はただちに IMAP/POP サーバからログアウトします。
3. ユーザが認証された後、スパム隔離は、ユーザの電子メール アドレスに基づいて、そのユーザ宛の電子メールのリストを作成します。
   - スパム隔離の設定において、修飾のないユーザ名（joe など）に追加するドメインを指定している場合は、このドメインを後ろに追加してできる完全修飾電子メール アドレスを使用して、隔離エリア内の一致するエンベロープが検索されます。
   - それ以外の場合、スパム隔離は、入力された電子メール アドレスを使用して、一致するエンベロープを検索します。

IMAP の詳細については、ワシントン大学の Web サイトを参照してください。

http://www.washington.edu/imap/

Web ブラウザからのスパム隔離へのエンドユーザ アクセスの設定

	操作内容	詳細情報
ステップ 1	スパム管理機能へのエンドユーザ アクセスのさまざまな認証方式について、利点と制限事項を把握します。	スパム管理機能にアクセスするエンド ユーザの認証オプション（7-16 ページ）
ステップ 2	LDAP を使用してエンド ユーザを認証する場合は、[システム管理（System Administration）] > [LDAP] > [LDAPサーバプロファイル（LDAP Server Profile）] ページの [スパム隔離エンドユーザ認証クエリ（Spam Quarantine End-User Authentication Query）] 設定などで、LDAP サーバ プロファイルを設定します。	第 11 章「LDAP との統合」
ステップ 3	スパム隔離へのエンドユーザ アクセスを設定します。	スパム隔離へのエンドユーザ アクセスの設定（7-19 ページ）
ステップ 4	スパム隔離へのエンドユーザ アクセスの URL を決定します。	スパム隔離へのエンドユーザ アクセス用 URL の決定（7-20 ページ）

関連項目

- スパム隔離へのエンドユーザ アクセスの設定（7-19 ページ）
- スパム隔離へのエンドユーザ アクセス用 URL の決定（7-20 ページ）
- エンド ユーザに表示されるメッセージ（7-20 ページ）

スパム隔離へのエンドユーザ アクセスの設定

管理ユーザは、エンドユーザ アクセスが有効であるかどうかにかかわらずスパム隔離にアクセスできます。

はじめる前に

スパム管理機能にアクセスするエンド ユーザの認証オプション（7-16 ページ）で要件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）] > [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　[設定の編集（Edit Settings）] をクリックします。

ステップ 3　[エンドユーザ隔離へのアクセスを有効にする（Enable 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）] を選択します。

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 ユーザの認証に使用する方式を指定します。

選択オプション	詳細情報
なし	—
メールボックス（IMAP/POP）	認証に LDAP ディレクトリを使用しないサイトの場合、隔離は、ユーザの電子メール アドレスとパスワードの正当性を、それらのユーザのメールボックスが保持されている標準ベースの IMAP または POP サーバに対して検証することもできます。 スパム隔離にログインするとき、エンド 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。 POP サーバがバナー内で APOP サポートをアドバタイズしている場合、セキュリティ上の理由から（つまり、パスワードが平文で送信されるのを回避するために）、Cisco IronPort アプライアンスは APOP のみを使用します。一部またはすべてのユーザに対して 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 サーバを設定する必要があります。 サーバで SSL を使用するように設定している場合は、SSL を選択します。ユーザがユーザ名だけを入力した場合に、電子メール アドレスを自動入力するために追加するドメインを指定できます。「権限のないユーザ名にドメインを追加（Append Domain to Unqualified Usernames）」するには、ログインするユーザ用のエンベロープのドメインを入力します。
LDAP	このトピックの「はじめる前に」で触れたセクションの説明に従って、LDAP を設定します。

ステップ 6　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をオンにすると、ユーザは、スパム隔離ページからメッセージ本文を表示できなくなります。この場合、隔離されたメッセージの本文を表示するには、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。

次の作業

（任意）ユーザがスパム隔離にアクセスしたときに表示されるページをカスタマイズします（まだ行っていない場合）。スパム隔離の有効化と設定（7-3 ページ）の設定の説明を参照してください。

スパム隔離へのエンドユーザ アクセス用 URL の決定

エンド ユーザがスパム隔離に直接アクセスするために使用できる URL は、マシンのホスト名と、隔離が有効になっている IP インターフェイス上の設定（HTTP/S とポート番号）から作成されます。たとえば、`HTTP://mail3.example.com:82` となります。

エンド ユーザに表示されるメッセージ

通常、エンド ユーザにはスパム隔離内にある自身のメッセージだけが表示されます。

アクセス方法（通知経由または Web ブラウザから直接）と認証方式（LDAP または IMAP/POP）によっては、スパム隔離内にある複数の電子メール アドレス宛のメールが表示される場合があります。

LDAP 認証を使用する場合、LDAP ディレクトリ内でプライマリ電子メール属性に複数の値が設定されていると、それらの値（アドレス）のすべてがユーザに関連付けられます。したがって、隔離エリア内には、LDAP ディレクトリでエンド ユーザに関連付けられたすべての電子メール アドレス宛の隔離されたメッセージが存在します。

認証方式が IMAP/POP の場合、またはユーザが通知から直接隔離にアクセスした場合は、そのユーザの電子メール アドレス（または通知の送信先アドレス）宛のメッセージのみが隔離に表示されます。

メンバーになっているエイリアスに送信されたメッセージについては、受信者の電子メールのメーリング リスト エイリアスおよびスパム通知（7-22 ページ）を参照してください。

関連項目

- スパム隔離へのエンドユーザ アクセスの設定（7-19 ページ）
- 受信者の電子メールのメーリング リスト エイリアスおよびスパム通知（7-22 ページ）

エンド ユーザへの隔離されたメッセージに関する通知

特定またはすべてのユーザに、スパム隔離内にスパムまたはその疑いのあるメッセージがあることを通知する電子メールを送信するように、システムを設定できます。

デフォルトでは、そのユーザの隔離されたメッセージがスパム通知に表示されます。ユーザがスパム隔離内の隔離されたメッセージを表示できるように、リンクを通知に含めることもできます。このリンクに有効期限はありません。ユーザは隔離されたメッセージを確認し、自分の受信箱に配信するか、削除するかを決定できます。

はじめる前に

- エンド ユーザが通知に表示されるメッセージを管理するには、スパム隔離にアクセスできる必要があります。スパム隔離へのエンドユーザ アクセスの設定（7-19 ページ）を参照してください。
- 通知を使用してスパムを管理するための認証オプションを把握します。スパム管理機能にアクセスするエンド ユーザの認証オプション（7-16 ページ）を参照してください。
- エンド ユーザが複数のエイリアスで電子メールを受信する場合については、受信者の電子メールのメーリング リスト エイリアスおよびスパム通知（7-22 ページ）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）] > [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　[設定の編集（Edit Settings）] をクリックします。

ステップ 3　[スパム通知（Spam Notifications）] セクションまでスクロールします。

ステップ 4　[スパム通知を有効にする（Enable Spam Notification）] を選択します。

ステップ 5　オプションを指定します。

メッセージ本文をカスタマイズするには、次の手順を実行します。

a. （任意）デフォルトのテキストおよび変数をカスタマイズします。

次のメッセージ変数は特定のエンド ユーザに対応した実際の値に展開されます。

- [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%`）：スパム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%`）：隔離にログインし、メッセージを表示するための URL。
- [ユーザ名（Username）]（`%username%`）
- [新規メッセージテーブル（New Message Table）]（`%new_quarantine_messages%`）：隔離内にあるこのユーザの新しいメッセージのリスト。

変数を挿入するには、挿入する位置にカーソルを置いて、右側のメッセージ変数リストで変数の名前をクリックします。または変数を入力します。

b. このページの [エンドユーザ隔離アクセス（End User Quarantine Access）] セクションで認証方式を有効にしている場合は、次を実行します。

- 通知内のリンクをクリックしてアクセスしたユーザを自動的にスパム隔離にログインさせるには、[隔離へのアクセスに証明書なしのログインを有効にする（Enable login without credentials for quarantine access）] を選択します。エンド ユーザは、通知の [リリース（Release）] リンクをクリックするだけでメッセージをリリースできます。
- 通知内のリンクをクリックしてアクセスしたユーザにスパム隔離へのログインを要求する場合は、このオプションの選択を解除します。エンド ユーザは、通知の [リリース（Release）] リンクをクリックするだけではメッセージをリリースできません。

c. [メッセージのプレビュー（Preview Message）] をクリックして、メッセージの内容を確認します。

ステップ 6　変更を送信し、保存します。

次の作業

これらの通知を確実に受信できるように、エンド ユーザにスパム隔離からの通知電子メールの差出人アドレスを各自のメール アプリケーション（Microsoft Outlook、Mozilla Thunderbird など）の迷惑メール設定にある「ホワイトリスト」に追加することを推奨してください。

関連項目

- 受信者の電子メールのメーリング リスト エイリアスおよびスパム通知（7-22 ページ）
- 通知のテスト（7-23 ページ）
- スパム通知のトラブルシューティング（7-23 ページ）

受信者の電子メールのメーリング リスト エイリアスおよびスパム通知

電子メールが隔離されている各エンベロープ受信者（メーリング リストおよびその他のエイリアスを含む）に通知を送信できます。各メーリング リストは、単一の要約を受信します。メーリング リストに通知を送信すると、リストの購読者全員に通知が届きます。複数の電子メール エイリアスに属するユーザ、通知を受信する LDAP グループに属するユーザ、または複数の電子メール アドレスを使用するユーザは、複数のスパム通知を受信する場合があります。次の表に、ユーザが複数の通知を受け取る状況の例を示します。

表 7-1　アドレス/エイリアスに応じた通知数

ユーザ	電子メール アドレス	エイリアス	通知
Sam	sam@example.com	—	1
Mary	mary@example.com	dev@example.com qa@example.com pm@example.com	4
Joe	joe@example.com、 admin@example.com	hr@example.com	3

LDAP 認証を使用する場合、メーリング リスト エイリアスに通知を送信しないように選択することができます。または、メーリング リスト エイリアスにスパム通知を送信することを選択した場合、複数の通知が送信されないようにすることができます。スパム隔離エイリアス統合クエリー（11-7 ページ）を参照してください。

アプライアンスが電子メール通知にスパム隔離のエイリアス統合クエリーを使用していない限り、通知内のリンクをクリックしてスパム隔離にアクセスしたユーザに、そのエンドユーザが所有する他のエイリアス宛の隔離対象メッセージは表示されません。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。

つまり、各メーリング リストの購読者は、全員が同じ通知を受信することになり、その隔離にログインしてメッセージを解放したり、削除したりできます。この場合、エンド ユーザが隔離にアクセスして、通知に示されたメッセージを表示しようとしても、それらのメッセージは他のユーザによってすでに削除されている可能性もあります。

（注） LDAP を使用していない場合で、エンド ユーザが複数の電子メール通知を受信することがないようにする必要がある場合は、通知をディセーブルにすることを検討します。この場合、代わりとして、エンド ユーザが隔離に直接アクセスできるようにし、LDAP または POP/IMAP で認証します。

通知のテスト

テスト用のメール ポリシーを設定し、単一のユーザに対してのみスパムを隔離することで通知をテストできます。その後、スパム隔離の通知設定で、[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、[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フにします。これにより、[バウンスされたメッセージの送信先（Deliver Bounced Messages To）] フィールドに設定された管理者だけが、隔離内の新しいスパムについて通知されます。

スパム通知のトラブルシューティング

関連項目

- ユーザが複数の通知を受信する（7-23 ページ）
- 受信者に通知が届かない（7-23 ページ）
- ユーザが複数の通知を受信する（7-23 ページ）
- 受信者に通知が届かない（7-23 ページ）

ユーザが複数の通知を受信する

問題　ユーザが 1 つのメッセージに対して複数のスパム通知を受信します。

ソリューション　考えられる原因:

- ユーザが複数の電子メール アドレスを所有し、スパム メッセージがその内の 2 つ以上のアドレスに送信されました。
- ユーザが、スパム メッセージを受信した 1 つ以上の電子メール エイリアスのメンバーです。重複を最小限にするための詳細については、受信者の電子メールのメーリング リスト エイリアスおよびスパム通知（7-22 ページ）を参照してください。

受信者に通知が届かない

問題　受信者にスパム通知が届きません。

ソリューション

- スパム受信者ではなく [バウンスメッセージの送信先:（Deliver Bounce Messages To:）] のアドレスに通知が送信される場合は、スパム通知が有効になっていても、スパム隔離へのアクセスが有効になっていないことを意味します。スパム管理機能にアクセスするエンド ユーザの認証オプション（7-16 ページ）を参照してください。
- ユーザに各自の電子メール クライアントの迷惑メール設定を確認してもらいます。
- スパム隔離の有効化と設定（7-3 ページ）で [次を使用してメッセージを配信（Deliver Messages Via）] に指定したアプライアンスまたはサーバに問題がないかを確認します。

スパム隔離内のメッセージの管理

ここでは、ローカルまたは外部のスパム隔離内にあるメッセージの操作方法について説明します。

管理ユーザはスパム隔離内のすべてのメッセージを表示および管理できます。

関連項目

- スパム隔離へのアクセス（管理ユーザ）（7-24 ページ）
- スパム隔離内でのメッセージの検索（7-24 ページ）
- スパム隔離内のメッセージの表示（7-25 ページ）
- スパム隔離内のメッセージの配信（7-25 ページ）
- スパム隔離からのメッセージの削除（7-25 ページ）

スパム隔離へのアクセス（管理ユーザ）

ステップ 1　[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、[スパム隔離（Spam Quarantine）] リンクをクリックします。

スパム隔離が別のブラウザ ウィンドウで開きます。

スパム隔離内でのメッセージの検索

手順

ステップ 1　エンベロープ受信者を指定します。

（注）　アドレスの一部を入力できます。

ステップ 2　入力した受信者に検索結果が厳密に一致する必要があるか、あるいは入力した値が検索結果のアドレスの一部、先頭、または末尾のいずれと一致する必要があるかを選択します。

ステップ 3　検索の対象期間を入力します。カレンダー アイコンをクリックして、日付を選択します。

ステップ 4　差出人アドレスを指定し、入力した値が検索結果のアドレスの一部、全体、先頭、または末尾のいずれと一致する必要があるかを選択します。

ステップ 5　[検索（Search）] をクリックします。検索基準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。

関連項目

- 大量メッセージの検索（7-24 ページ）

大量メッセージの検索

スパム隔離内に大量のメッセージが収集されている場合、および検索条件が絞り込まれていない場合、クエリーの結果が返されるまでに非常に長い時間がかかる可能性があり、場合によってはタイムアウトします。

その場合、検索を再実行するかどうか確認されます。大量の検索が同時に複数実行されると、パフォーマンスに悪影響を与える可能性があることに注意してください。

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、スパム隔離内のメッセージが表示されます。一度に表示されるメッセージの件数を選択できます。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。同じカラムを再びクリックすると、逆順にソートされます。

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。メッセージは、[メッセージの詳細（Message Details）] ページに表示されます。メッセージの最初の 20 KB が表示されます。メッセージがそれよりも長い場合、表示は 20 KB で打ち切られ、メッセージの最後にあるリンクからメッセージをダウンロードできます。

[メッセージの詳細（Message Details）] ページから、メッセージを削除したり（[削除（Delete）] を選択）、[リリース（Release）] を選択してメッセージを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。

メッセージについてさらに詳細な情報を表示するには、[メッセージトラッキング（Message Tracking）] リンクをクリックします。

次の点に注意してください。

- **添付ファイルを含むメッセージの表示**

  添付ファイルを含むメッセージを表示すると、メッセージの本文が表示された後、添付ファイルのリストが続いて表示されます。

- **HTML メッセージの表示**

  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。画像は表示されません。

- **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。

スパム隔離内のメッセージの配信

メッセージを解放して配信するには、解放する 1 つまたは複数のメッセージの隣にあるチェックボックスをクリックし、ドロップダウン メニューから [リリース（Release）] を選択します。その後、[送信（Submit）] をクリックします。

ページに現在表示されているすべてのメッセージを自動で選択するには、見出し行にあるチェックボックスをクリックします。

解放されたメッセージは、それ以降の電子メール パイプライン内のワーク 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。

スパム隔離からのメッセージの削除

スパム隔離では、メッセージが一定時間後に自動で削除されるように設定できます。また、スパム隔離が最大サイズに達したら、古いものから順にメッセージが自動で削除されるように設定することもできます。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隣にあるチェックボックスをクリックし、ドロップダウン メニューから [削除（Delete）] を選択します。その後、[送信（Submit）] をクリックします。ページに現在表示されているすべてのメッセージを自動で選択するには、見出し行にあるチェックボックスをクリックします。

スパム隔離内のすべてのメッセージを削除するには、その隔離を無効にし（外部スパム隔離の無効化について（7-26 ページ）を参照）、[すべてのメッセージを削除（Delete All Messages）] リンクをクリックします。リンクの末尾にある括弧内の数字は、スパム隔離内のメッセージの件数です。

スパム隔離のディスク領域

隔離に使用できるディスク領域は、アプライアンス モデルによって異なります。ディスク クォータおよび使用状況の表示（14-54 ページ）を参照してください。

デフォルトでは、スパム隔離内のメッセージは一定期間後に自動的に削除されます。隔離エリアが満杯になった場合は、古いスパムから削除されます。この設定を変更するには、スパム隔離の有効化と設定（7-3 ページ）を参照してください。

外部スパム隔離の無効化について

スパム隔離を無効にする場合は、次を参照してください。

- 無効になっているスパム隔離内にメッセージが存在する場合は、すべてのメッセージの削除を選択できます。
- 電子メール セキュリティ アプライアンスでメール ポリシーの調整が必要になる場合があります。
- 外部スパム隔離を完全に無効にするには、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 アプライアンスのみで外部スパム隔離を無効にしても、外部隔離またはそのメッセージとデータは削除されません。

スパム隔離機能のトラブルシューティング

- 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（7-15 ページ）
- スパム通知のトラブルシューティング（7-23 ページ）
- メッセージ テキストが正しく表示されることの確認（7-8 ページ）

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、セキュリティ リスクを減らすために、DMZ の代わりに、ファイアウォールの内側に保存されます。
- 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。

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。

隔離の詳細については、お使いの電子メール セキュリティ アプライアンスのドキュメントを参照してください。

隔離のタイプ

隔離タイプ	隔離名	システムにデフォルトで作成されるか	説明	詳細情報
高度なマルウェア防御（Advanced Malware Protection）	ファイル分析（File Analysis）	はい	ファイル分析用に送信されるメッセージを保持します。 特性については、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 マニュアルまたはオンライン ヘルプ	• ポリシー、ウイルス、およびアウトブレイク隔離の管理（8-9 ページ） • ポリシー、ウイルス、またはアウトブレイク隔離のメッセージの操作（8-17 ページ）
ウィルス	ウィルス	はい	アンチウイルス エンジンによる判定に従って、マルウェアを送信する可能性のあるメッセージを保持します。	
アウトブレイク	Outbreak	はい	アウトブレイク フィルタによってスパムまたはマルウェアの可能性があると検出されたメッセージを保持します。	
ポリシー（Policy）	ポリシー	はい	メッセージ フィルタ、コンテンツ フィルタ、DLP メッセージ アクションによって検出されたメッセージを保持します。 デフォルトのポリシー隔離が作成されています。	
	未分類	はい	メッセージ フィルタ、コンテンツ フィルタ、DLP メッセージ アクションで指定した隔離が削除された場合にのみ、メッセージを保持します。 この隔離をフィルタまたはメッセージ アクションに対して割り当てることはできません。	
	（自分で作成するポリシー隔離）	いいえ	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	Spam	はい	メッセージの受信者または管理者が確認できるように、スパムおよびその疑いのあるメッセージを保持します。	第 7 章「スパム隔離」

一元化されたポリシー、ウイルス、アウトブレイク隔離

	操作内容	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（8-4 ページ）
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。	ディスク領域の管理（14-53 ページ）
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、およびデフォルトのポリシー隔離を設定します。 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（8-12 ページ） • システムが作成した隔離の設定の確認（8-12 ページ）。
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（8-5 ページ）
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（8-6 ページ）

	操作内容	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」 • 「一元化されたポリシー、ウイルス、アウトブレイク隔離」
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（8-12 ページ）
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（8-8 ページ）
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（8-9 ページ）

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

一元化されたポリシー、ウイルス、アウトブレイク隔離（8-3 ページ）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

一元化されたポリシー、ウイルス、アウトブレイク隔離(8-3 ページ)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

一元化されたポリシー、ウイルス、アウトブレイク隔離(8-3 ページ)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

一元化されたポリシー、ウイルス、アウトブレイク隔離（8-3 ページ）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

- 一元化されたポリシー、ウイルス、アウトブレイク隔離（8-3 ページ）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	選択項目	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　[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

一元化されたポリシー、ウイルス、アウトブレイク隔離(8-3 ページ)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一元化されたポリシー、ウイルス、アウトブレイク隔離(8-3 ページ)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 アプライアンスを使用できないときのメッセージのリリース(8-9 ページ)

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（13-7 ページ）

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 アプライアンスを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場合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（8-8 ページ）

ポリシー、ウイルス、およびアウトブレイク隔離の管理

関連項目

- 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（8-10 ページ）
- 隔離内のメッセージの保存期間（8-10 ページ）
- 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（8-11 ページ）
- システムが作成した隔離の設定の確認（8-12 ページ）

- ポリシー隔離の作成（8-12 ページ）
- ポリシー、ウイルス、アウトブレイク隔離の設定の編集方法（8-14 ページ）
- フィルタおよびメッセージ アクションに割り当てる隔離を決定する（8-14 ページ）
- ポリシー隔離の削除について（8-14 ページ）
- 隔離のステータス、容量、アクティビティのモニタリング（8-15 ページ）
- 隔離のディスク領域の使用状況についてのアラート（8-16 ページ）
- ポリシー隔離とロギング（8-16 ページ）
- メッセージ処理作業の他のユーザへの分配（8-16 ページ）

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、ディスク領域の管理（14-53 ページ）を参照してください。

複数の隔離のメッセージは、1 つの隔離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Web Security appliance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。
- 特定の管理対象Web Security applianceから隔離された、アウトブレイク隔離内のメッセージに使用できるセキュリティ管理アプライアンスのディスク領域は、そのWeb Security applianceで隔離メッセージに使用できるディスク領域の量によって制限される場合があります。
- この状況の詳細については、隔離内のメッセージの保存期間（8-10 ページ）を参照してください。

関連項目

- 隔離のステータス、容量、アクティビティのモニタリング（8-15 ページ）
- 隔離のディスク領域の使用状況についてのアラート（8-16 ページ）
- 隔離内のメッセージの保存期間（8-10 ページ）

隔離内のメッセージの保存期間

メッセージは次のタイミングで隔離から自動的に削除されます。

- 通常の期限切れ：隔離エリア内のメッセージが保存期間を満了する場合です。各隔離エリアのメッセージの保存期間を指定します。各メッセージには、それぞれ独自の有効期限があり、隔離のリストに表示されます。このトピックで説明され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が経過するまで保管されます。

（注）　アウトブレイク フィルタ隔離エリアでのメッセージの通常の保存期間は、アウトブレイク隔離ではなく各メールの アウトブレイク フィルタ セクションで設定します。

- 早期の期限切れ：設定した保存期間に到達する前にメッセージが隔離エリアから強制的に削除される場合です。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（8-10 ページ）で定義した、すべての隔離エリアのサイズ制限に達する。

    サイズ制限に到達すると、隔離に関係なく、古いメッセージから処理されます。すべての隔離エリアのサイズがサイズ制限未満に戻るまで、各メッセージに対してデフォルト アクションが実行されます。このポリシーは、先入れ先出し（FIFO）です。複数の隔離のメッセージは、最新の有効期限に基づいて期限切れになります。

    （任意）ディスク容量不足によるリリースまたは削除から除外するように、個々の隔離を設定できます。除外するようにすべての隔離を設定して、ディスク領域が満杯になった場合、セキュリティ管理アプライアンスの領域が利用可能になるまでメッセージはWeb Security applianceに保持されます。

    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Web Security appliance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、Web Security appliance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。

    ディスク容量のマイルストーンについてアラートが送信されます。隔離のディスク領域の使用状況についてのアラート（8-16 ページ）を参照してください。
  - まだメッセージを保持している隔離を削除します。

メッセージが隔離から自動的に削除される場合、デフォルト アクションがメッセージに対して実行されます。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（8-11 ページ）を参照してください。

保存期間への時間調整の影響

- サマータイムとアプライアンスのタイムゾーンの変更は保存期間に影響しません。
- 隔離の保存期間を変更すると、新しいメッセージにだけ新しい有効期限が適用されます。
- システム クロックを変更すると、以前期限切れになるはずだった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の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

デフォルト アクションは、隔離内のメッセージの保存期間（8-10 ページ）に記述されるいずれかの状況が発生した場合、ポリシー、ウイルス、アウトブレイク隔離エリア内のメッセージに対して実行されます。

2 つの主要なデフォルト アクションがあります。

- [削除（Delete）]：メッセージが削除されます。
- [リリース（Release）]：メッセージが解放されて配信されます。

  メッセージのリリース時に、脅威に対する再スキャンが実行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（8-24 ページ）を参照してください。

さらに、予定される保存期間よりも前にリリースされるメッセージには、X-Header の追加などの操作が行われる場合があります。詳細については、ポリシー隔離の作成（8-12 ページ）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Web Security applianceに返されます。

システムが作成した隔離の設定の確認

隔離を使用する前に、未分類隔離などのデフォルトの隔離設定をカスタマイズします。

関連項目

- ポリシー、ウイルス、アウトブレイク隔離の設定の編集方法（8-14 ページ）

ポリシー隔離の作成

はじめる前に

- 保存期間やデフォルト アクションなど、隔離エリア内のメッセージが自動的に管理される方法を確認します。隔離内のメッセージの保存期間（8-10 ページ）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（8-11 ページ）を参照してください。
- 各隔離エリアにアクセスできるユーザを決め、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、ポリシー、ウイルス、およびアウトブレイク隔離にアクセスできるユーザ グループ（8-17 ページ）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　[ポリシー隔離の追加（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。
- 隔離ディスク領域が一杯になった場合でも、指定した保存期間の終了前にこの隔離メッセージを*処理されたくない*場合、[メッセージに対してデフォルトのアクションを適用して空き容量を増やす（Free up space by applying default action on messages upon space overflow）] の選択を解除します。

  このオプションはすべての隔離では選択しないでください。システムは、少なくとも 1 つの隔離エリアからメッセージを削除して、領域を確保する必要があります。
- デフォルト アクションとして [リリース（Release）] を選択すると、保存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の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）	追加するテキストを入力し、そのテキストを元のメッセージの件名の前と後ろのどちらに追加するかを選択します。 たとえば、受信者に不適切なコンテンツを含む可能性があるメッセージであることを警告します。 **（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。
X-Header を追加（Add X-Header）	X-Header ではメッセージで実行されたアクションを記録できます。これはたとえば、特定のメッセージが配信された理由についての照会を処理する際に役立つ場合があります。 名前と値を入力します。 例: Name =`Inappropriate-release-early` Value = `True`
添付ファイルの削除（Strip Attachments）	添付ファイルを削除すると、このようなファイル中に存在する可能性のあるウイルスから保護します。

ステップ 4　この隔離エリアにアクセス可能なユーザを指定してください。

ユーザ	情報
ローカル ユーザ	ローカル ユーザ リストには、隔離エリア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すべてのアクセス権限を持つため、リストでは管理者権限を持つユーザを除外します。
外部認証されたユーザ	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	このオプションは、隔離へのアクセス権限を持つ少なくとも 1 つのカスタム ユーザ ロールを作成している場合にのみ表示されます。

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Web Security appliance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。Web Security appliance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方法

メモ

- 隔離の名前は変更できません。
- 保存期間への時間調整の影響（8-11 ページ）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。

フィルタおよびメッセージ アクションに割り当てる隔離を決定する

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Web Security appliance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　確認するポリシー隔離の名前をクリックします。

ステップ 3　ページの下部までスクロールし、[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）] を照会します。

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、アクティブな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。フィルタおよびメッセージ アクションに割り当てる隔離を決定する（8-14 ページ）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、ディスクがいっぱいになった際にメッセージを削除しないオプションを選択した場合でも、隔離で定義されたデフォルト アクションは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（8-11 ページ）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、フィルタまたはメッセージ アクションにより隔離されたメッセージは未分類隔離に送られます。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。

隔離のステータス、容量、アクティビティのモニタリング

内容	操作内容
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、ディスク領域の管理（14-53 ページ）を参照してください。
スパム隔離以外のすべての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。
現在すべての隔離が使用している合計容量	[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。
現在各隔離に使用されている容量	[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。
現在すべての隔離にあるメッセージの総数	[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。
現在各隔離にあるメッセージ数	[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時 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	フィルタおよびメッセージ アクションに割り当てる隔離を決定する（8-14 ページ）を参照してください。

隔離のディスク領域の使用状況についてのアラート

ポリシー、ウイルスおよびアウトブレイク隔離エリアの合計容量が 75% 以上、85% 以上および 95% 以上になると、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、メッセージが隔離に追加されたときにそのサイズが合計容量の 75% 以上に増加すると、アラートが送信されますも参照してください。

アラートの詳細については、アラートの管理（14-34 ページ）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 フィルタまたはアウトブレイク 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エリアから除去され、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 オブジェクトがシステムによって作成されます。これは、次のように新しい MID「by 行」がある既存のログ 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 System Quarantine
```

メッセージ処理作業の他のユーザへの分配

メッセージの処理および確認タスクを、他の管理者ユーザへ分配することができます。次に例を示します。

- 人事部門のチームはポリシー隔離の確認と管理ができます。
- 法務部門のチームは Confidential Material 隔離を管理できます。

隔離の設定を指定する際に、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の場所でも、その隔離の存在は一切表示されません。

関連項目

- ポリシー、ウイルス、およびアウトブレイク隔離にアクセスできるユーザ グループ（8-17 ページ）
- 第 13 章「管理タスクの分散」

ポリシー、ウイルス、およびアウトブレイク隔離にアクセスできるユーザ グループ

管理ユーザに隔離へのアクセスを許可した場合、実行できるアクションはそれぞれのユーザ 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 ユーザ グループに属するユーザに加え、隔離管理権限を持つカスタム ユーザ ロールのユーザは、隔離エリア内のメッセージの検索、閲覧および処理が可能ですが、隔離の設定変更、作成、削除、または集約はできません。各隔離にどのユーザがアクセスできるかを指定します。
- 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。

また、メッセージ トラッキングおよびデータ消失防止など、関連機能のアクセス権限によって、[隔離（Quarantine）] ページで管理ユーザに表示されるオプションおよび情報が変わります。たとえば、メッセージ トラッキングにアクセスできないユーザの場合、そのユーザにはメッセージ トラッキング 隔離されたメッセージに関する情報が表示されません。

（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（8-9 ページ）を参照してください。

エンド ユーザにはポリシー、ウイルス、およびアウトブレイク隔離に対する閲覧権限とアクセス権限はありません。

中央集中型ファイル分析隔離について

- 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を有効にすると、メッセージはCisco コンテンツ セキュリティ管理アプライアンスの中央集中型ファイル分析隔離に隔離されます。
- 電子メール セキュリティ アプライアンスの場合とは異なり、中央集中型ファイル分析隔離で、ファイル分析の判定に基づいて自動的にメッセージがリリースされることはありません。代わりに、設定した保持期間が経過するとメッセージは集約隔離からリリースされます。デフォルトの保持期間は 1 時間です。
- 電子メール セキュリティ アプライアンスの場合とは異なり、中央集中型ファイル分析隔離からリリースされるメッセージはリリース時に再スキャンされません。

ポリシー、ウイルス、またはアウトブレイク隔離のメッセージの操作

関連項目

- 隔離エリア内のメッセージの表示（8-18 ページ）
- ポリシー、ウイルスおよびアウトブレイク隔離のメッセージの検索（8-19 ページ）
- 隔離内のメッセージの手動による処理（8-19 ページ）
- 複数の隔離エリアにあるメッセージ（8-21 ページ）

- メッセージの詳細およびメッセージ コンテンツの表示（8-22 ページ）
- 隔離されたメッセージの再スキャンについて（8-24 ページ）
- アウトブレイク隔離（8-24 ページ）

隔離エリア内のメッセージの表示

目的	操作内容
隔離エリアのすべてのメッセージを表示する	[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。 表の関連する隔離の行で、[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エリアのメッセージを表示する	• [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。 表の関連する隔離の行で、[メッセージ（Messages）] 列の青い番号をクリックします。 • [ルールサマリー管理（Manage by Rule Summary）] リンク（8-25 ページ）を参照してください。
隔離エリアのメッセージのリスト内で移動する	[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。
隔離エリアのメッセージのリストをソートする	カラム見出しをクリックします（カラムに複数の項目が含まれる場合と [その他の隔離（In other quarantines）] カラムを除く）。
テーブルカラムのサイズを変更する	カラム見出し間の境界線をドラッグします。
メッセージの隔離の原因となるコンテンツを表示する	一致した内容の表示（8-22 ページ）を参照してください。

関連項目

- 隔離されたメッセージおよび国際文字セット（8-18 ページ）

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、ウイルスおよびアウトブレイク隔離のメッセージの検索

メモ
- ポリシー、ウイルスおよびアウトブレイク隔離の検索では、スパム隔離メッセージは見つかりません。
- ユーザは、アクセスできる隔離メッセージだけを検索および表示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　[隔離全体を検索（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に対して、各アウトブレイク ルールによって隔離されたすべてのメッセージも検索できます。アウトブレイク テーブル行で [ルール サマリーによる管理（anage by Rule Summary）] リンクをクリックします

ステップ 3　検索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（Envelope Sender）] および [エンベロープ受信者（Envelope Recipient）] には任意の文字を入力できます。エントリ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（Envelope Recipient）] および [件名（Subject）] を指定した場合は、[エンベロープ受信者（Envelope Recipient）] *および* [件名（Subject）] に指定された単語の両方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、隔離の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、隔離内のメッセージの手動による処理（8-19 ページ）を参照してください。

隔離内のメッセージの手動による処理

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 を使用する展開では、セキュリティ管理アプライアンスまたは Enterprise Manager で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」の章を参照してください。

メッセージで次の処理を実行することができます。

- 削除（Delete）
- リリース
- 隔離エリアで予定していた終了の遅延
- 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する
- ある隔離エリアから別の隔離エリアにメッセージを移動する

通常、次の実行時に表示されたリストのメッセージに処理を行うことができます。ただし、すべての状況ですべてのアクションが使用できる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。
- [隔離全体を検索（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。

次の手順で、これらの操作を複数のメッセージで同時に実行できます。

- メッセージ リストの上部の選択リストからオプションを選択する。
- ページ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 リストの上部のテーブル見出しでチェックボックスを選択する。これは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を適用されます。他のページのメッセージは影響を受けません。

その他のオプションもアウトブレイク隔離エリアのメッセージに利用可能です。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 ガイドで、「Outbreak Filters」の章の [ルールサマリー管理（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

- メッセージのコピーの送信（8-20 ページ）
- ポリシー隔離エリア間のメッセージの移動について（8-21 ページ）
- 複数の隔離エリアにあるメッセージ（8-21 ページ）
- 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（8-11 ページ）

メッセージのコピーの送信

メッセージのコピーは、Administrators 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。

ポリシー隔離エリア間のメッセージの移動について

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。

別の隔離にメッセージを移動する場合次のようになります。

- 有効期限は変わりません。メッセージは、元の隔離の保持期限が適応されます。
- 一致したコンテンツおよび他の関連情報を含め、メッセージが隔離された理由は変更されません。
- あるメッセージが複数の隔離にあり、すでにメッセージのコピーを保持している場所にメッセージを移動した場合、移動したメッセージのコピーの有効期限および隔離の理由は、移動先の隔離エリアに元からあるメッセージのコピーを上書きします。

複数の隔離エリアにあるメッセージ

メッセージが他の 1 つ以上の隔離エリア内にも存在する場合、他の隔離エリアへのアクセス権限があるかどうかにかかわらず、隔離メッセージ リストの [その他の隔離（In other quarantines）] カラムに [はい（Yes）] と表示されます。

複数の隔離エリアにあるメッセージ

- メッセージが存在するすべての隔離エリアから解放されるまで、配信されません。特定の隔離エリアから削除されても、配信されません。
- メッセージが存在するすべての隔離エリアから削除または解放されるまで、どの隔離エリアからも削除されません。

メッセージを解放しようとするユーザはそれらのメッセージが存在する隔離の一部にしかアクセスできない場合があるため、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、いずれかの隔離エリア内で削除済みとマークされると、他の隔離エリアからも配信できなくなります。（ただし、解放はできます）。

メッセージが複数の隔離エリア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スケジュールされた保存期間の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。
- ユーザには、一致したコンテンツでアクセスできない隔離エリアにメッセージが格納されているものは表示されません。
- メッセージの解放は、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エリア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」メッセージが解放されるまで）、そのメッセージは変更されずに隔離エリア内に残ります。

メッセージの詳細およびメッセージ コンテンツの表示

メッセージの内容を表示したり、[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、メッセージを読んだり、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 [メッセージ本文（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。

メッセージについてさらに詳細な情報を表示するには、[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） 特別なアウトブレイク隔離の場合、追加の機能を利用できます。アウトブレイク隔離（8-24 ページ）を参照してください。

関連項目

- 一致した内容の表示（8-22 ページ）
- 添付ファイルのダウンロード（8-24 ページ）

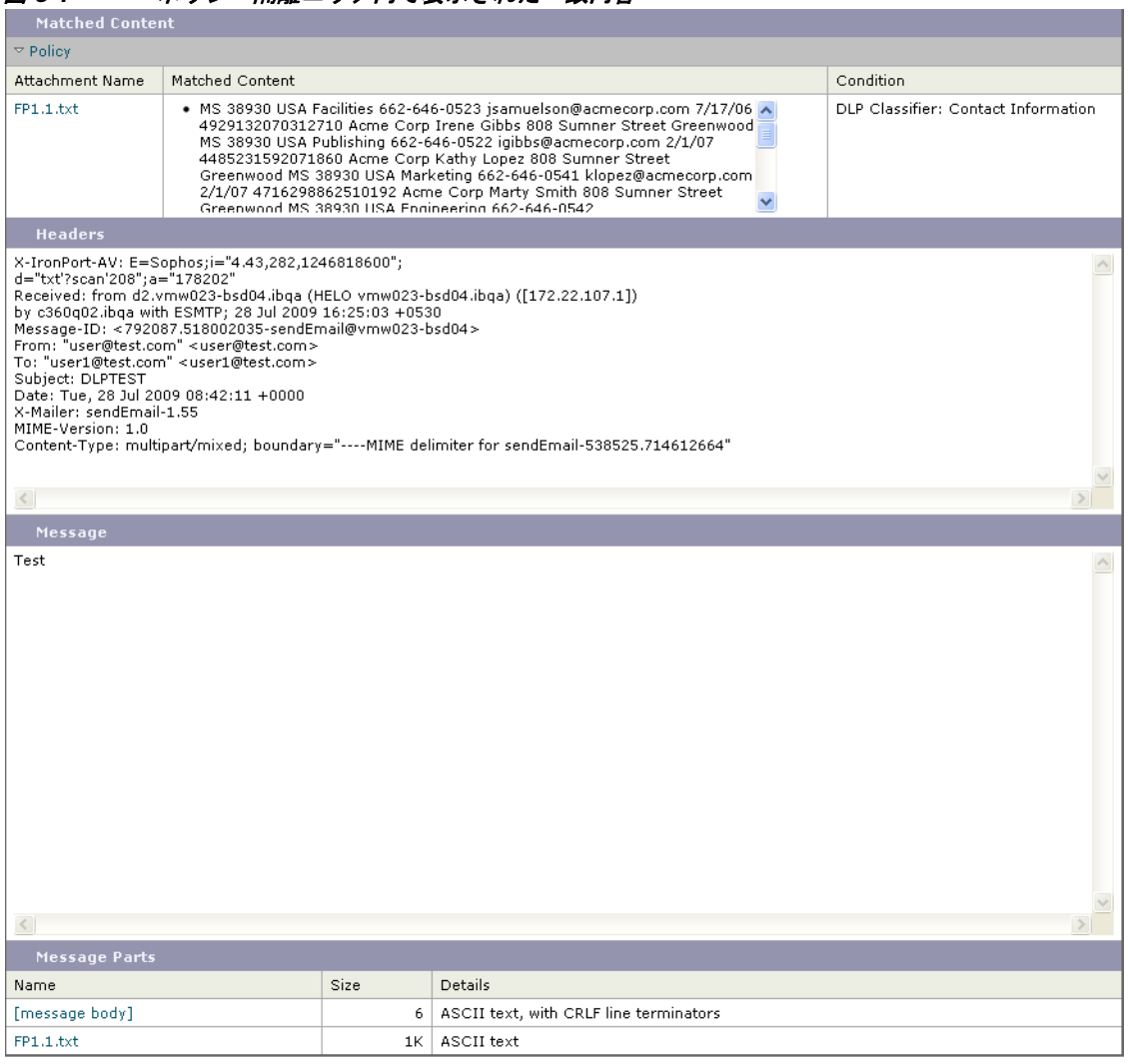
一致した内容の表示

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 の表示は、該当コンテンツを特定するための目安として使用するもので、該当コンテンツの完全なリストであるとは限りません。この現象が発生するのは、GUI でコンテンツの照合に使用しているロジックがフィルタと比べて厳密でないためです。この問題はメッセージ本文での検索についてのみ発生します。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テーブル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。ウイルスが含まれる可能性がある添付ファイルは、ユーザ自身の自己責任においてダウンロードしてください。[メッセージ部分（Message Parts）] セクション内の [メッセージ本文（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

隔離されたすべてのキューからメッセージが解放されるとき、アプライアンスおよび最初にメッセージを隔離したメール ポリシーでイネーブルにされている機能によって、次の再スキャンが発生します。

- ポリシーおよびウイルス隔離から解放されるメッセージはアンチウイルス 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エリアから解放されたメッセージは、アンチスパムおよびアンチウイルス 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）。
- 添付ファイルを含むメッセージは、ポリシー、ウイルス、およびアウトブレイク隔離から解放されるときにファイル レピュテーション サービスによって再スキャンされます。

再スキャン時に、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、そのメッセージは別の隔離に送信される可能性があります。

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解放しても、アンチウイルス 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ります。再隔離されるとループ状態となり、そのメッセージは隔離エリアからまったく解放されなくなります。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、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。

アウトブレイク隔離は、他の隔離と同様の機能を持ち、メッセージを検索したり、メッセージを解放または削除したりなどできます。

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（[ルール サマリーによる管理（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の送信機能、およびスケジュールされた保存期間の終了日時で検索結果内のメッセージを並べ替えるオプション）。

アウトブレイク 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。

関連項目

- アウトブレイク隔離のメッセージの再スキャン（8-25 ページ）
- [ルールサマリー管理（Manage by Rule Summary）] リンク（8-25 ページ）
- シスコへの偽陽性または不審なメッセージの報告（8-25 ページ）

アウトブレイク隔離のメッセージの再スキャン

アウトブレイク隔離に入れられたメッセージは、新しく公開されたルールによってもう脅威ではないと見なされると、自動的に解放されます。

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。

[ルールサマリー管理（Manage by Rule Summary）] リンク

隔離リストでアウトブレイク隔離の横にある [ルール サマリーによる管理（Manage by Rule Summary）] リンクをクリックして、[ルール サマリーによる管理（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多数のメッセージを片付け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 [ルールサマリー管理（Manage by Rule Summary）] ビューについての情報を参照してください。

シスコへの偽陽性または不審なメッセージの報告

アウトブレイク隔離内のメッセージについてメッセージの詳細を表示しているとき、偽陽性または不審なメッセージを報告するためにそのメッセージをシスコへ送信できます。

手順

ステップ 1　アウトブレイク隔離エリア内のメッセージの移動

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。

集約ポリシー隔離のトラブルシューティング

- 管理ユーザがフィルタおよび DLP メッセージ アクションの隔離を選択できない（8-26 ページ）
- 集約アウトブレイク隔離から解放されたメッセージが再スキャンされない（8-26 ページ）

管理ユーザがフィルタおよび DLP メッセージ アクションの隔離を選択できない

問題　管理ユーザが、電子メール セキュリティ アプライアンスでコンテンツ フィルタおよびメッセージ フィルタまたは DLP アクションの隔離を表示することも選択することもできません。

ソリューション　カスタム ユーザ ロールの集約隔離アクセスの設定（8-9 ページ）を参照してください。

集約アウトブレイク隔離から解放されたメッセージが再スキャンされない

問題　アウトブレイク隔離から解放されたメッセージは配信前に再スキャンされるはずですが、一部の汚染されたメッセージが隔離から配信されました。

ソリューション　これは、隔離されたメッセージの再スキャンについて（8-24 ページ）で説明した状況で発生する可能性があります。

Web セキュリティ アプライアンスの管理

中央集中型コンフィギュレーション管理について

中央集中型コンフィギュレーション管理を使用すると、シスコ コンテンツ セキュリティ管理アプライアンスから最大 150 の関連する 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。

設定の対象	操作内容
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(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 を公開します。 Configuration Master で設定できる機能の多くは、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。
アプライアンスの管理(ログ サブスクリプションまたはアラートの設定、管理責任の分散など)に関係する機能。	拡張ファイル公開を使用します。
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。	管理対象の Web セキュリティ アプライアンスで直接設定します。 次のマニュアルを参照してください。『*AsyncOS for Cisco Web Security Appliances User Guide*』

中央集中型で Webセキュリティ アプライアンスを管理する Configuration Master の設定

対象アプライアンス	操作内容	詳細情報
—	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(9-3 ページ)を参照してください。
—	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(9-3 ページ)を参照してください。
Web セキュリティ アプライアンス	**(任意)**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 アプライアンスがある場合は、その Web セキュリティ アプライアンスのコンフィギュレーション 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。	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する手順については、『*AsyncOS for Cisco Web Security Appliances User Guide*』の「Saving and Loading the Appliance Configuration」を参照してください。
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有効化(9-4 ページ)を参照してください。
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(9-4 ページ)を参照してください。
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(9-5 ページ)を参照してください。

対象アプライアンス	操作内容	詳細情報
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（9-7 ページ）を参照してください
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 アプライアンスで有効化されている機能が、そのアプライアンスに関連付けられている Configuration Master で有効化されている機能と一致していることを確認します。	機能が常に有効化されていることの確認（9-11 ページ）を参照してください。
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、必要な機能を有効にしたら、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（9-14 ページ）を参照してください。
セキュリティ管理アプライアンス	既存の Configuration Master 設定が変更される可能性がある、URL カテゴリ セットの更新のために事前に準備します。	URL カテゴリ セットの更新の準備および管理（9-22 ページ）

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各 Web セキュリティ アプライアンスで、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）] のすべてのレルム名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 Configuration Master があるため、異なる機能をサポートするさまざまなバージョンの AsyncOS for Web Security を実行する Web セキュリティ アプライアンスを中央集中型で管理できます。

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。

お使いの 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、互換性マトリクス（http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html）を参照してください。

（注）　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 のバージョンと一致している必要があります。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有効化

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 の初期化と設定

Configuration Master の初期化

（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（9-7 ページ）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。

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。

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 8.0 for Web を実行中の場合は、Configuration Master 8.0 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（9-5 ページ）
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（9-6 ページ）

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。

はじめる前に

まだ追加していない場合は、各 Web セキュリティ アプライアンスに適した Configuration Master のバージョンを選択してください。使用する Configuration Master のバージョンの確認（9-3 ページ）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　[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 3　[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 アドレスまたは解決可能なホスト名を入力します。

（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。

ステップ 4　Centralized Configuration Manager サービスが事前に選択されています。

ステップ 5　[接続の確立(Establish Connection)] をクリックします。

ステップ 6　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 7　[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 8　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 9　変更を送信し、保存します。

ステップ 10　中央集中型コンフィギュレーション管理を有効にする 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。

はじめる前に

まだ追加していない場合は、各 Web セキュリティ アプライアンスに適した Configuration Master のバージョンを選択してください。使用する Configuration Master のバージョンの確認(9-3 ページ)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。

(注)　Configuration Master が [無効(Disabled)] と表示されている場合に有効にするには、[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、有効にします。詳細については、公開する機能の有効化(9-12 ページ)を参照してください。

ステップ 2　[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 3　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 4　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。

条件	操作内容
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 および 新しい Configuration Master のバージョンを初期化（以前の既存の Configuration Master を新しいバージョンにコピー）していない場合	古いバージョンをインポートします。既存の Configuration Master からのインポート（9-7 ページ）を参照してください。
Web セキュリティ アプライアンスを設定済みで、同じ設定を複数の Web セキュリティ アプライアンスで使用する場合	その Web セキュリティ アプライアンスから保存したコンフィギュレーション ファイルを Configuration Master にインポートします （中央集中型で Webセキュリティ アプライアンスを管理する Configuration Master の設定（9-2 ページ）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（9-8 ページ）を参照してください。
インポートした設定を変更する必要がある場合	Configuration Masters での Web セキュリティ機能の直接設定（9-9 ページ）を参照してください。
ポリシー設定、URL カテゴリ、バイパス設定を Web セキュリティ アプライアンスでまだ設定していない場合	これらの設定をセキュリティ管理アプライアンスの該当する Configuration Master に直接設定します。 Configuration Masters での Web セキュリティ機能の直接設定（9-9 ページ）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 7.7 の設定を、Configuration Master 8.0 および 8.5 にインポート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、[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。

ステップ 5　[インポート（Import）] をクリックします。

関連項目

- Custom Web User ロールについて（13-8 ページ）

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

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 にポリシー設定を作成できます。

はじめる前に

コンフィギュレーション ファイルと Configuration Master のバージョンの互換性を確認してください。使用する Configuration Master のバージョンの確認（9-3 ページ）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公開済みであっても、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。Configuration Master にコンフィギュレーション ファイルをインポートすると、選択した Configuration Master に関連付けられた設定がすべて上書きされます。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。

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 Masters 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。

- アイデンティティ（Identities）
- SaaS ポリシー（SaaS Policies）
- 復号化ポリシー（Decryption Policies）
- ルーティング ポリシー（Routing Policies）
- アクセス ポリシー（Access Policies）
- 全体の帯域幅制限（Overall Bandwidth Limits）
- Cisco データ セキュリティ（Cisco Data Security）
- 発信マルウェア スキャン（Outbound Malware Scanning）
- 外部データ消失防止（External Data Loss Prevention）
- SOCKS ポリシー
- カスタム URL カテゴリ（Custom URL Categories）
- 時間範囲およびクォータの定義（Define Time Ranges and Quotas）
- バイパス設定（Bypass Settings）
- L4 トラフィック モニタ

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（9-9 ページ）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。手順については、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 Configuration Master のバージョンに対応する AsyncOS バージョンの『*AsyncOS for Cisco Web Security Appliances 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（9-3 ページ）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/c/en/us/support/security/web-security-appliance/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）] にある機能を有効にする必要があります。詳細については、機能が常に有効化されていることの確認（9-11 ページ）を参照してください。

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
アイデンティティ（Identities）	• Configuration Master で ID を使用する場合のヒント（9-10 ページ）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。
SaaS ポリシー（SaaS Policies）	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。目的のグループが見つからない場合は、そのグループを [ディレクトリ（Directory）] 検索フィールドに入力して、[追加（Add）] ボタンをクリックすると、[承認済みグループ（Authorized Groups）] リストに追加することができます。
[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）]	このページで使用できるオプションは、Adaptive Scanning が関連する Configuration Master に対して有効になっているかどうかによって異なります。[Web] > [ユーティリティ（Utilities）] > [セキュリティ サービス表示（Security Services Display）] でこの設定を確認してください。

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、無効になります。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。

機能が常に有効化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有効になり、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。

- 有効化されている機能の比較（9-11 ページ）
- 公開する機能の有効化（9-12 ページ）

（注）　異なる機能が有効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。

有効化されている機能の比較

それぞれの Web セキュリティ アプライアンスで有効化されている機能が、そのアプライアンスに関連付けられている Configuration Master で有効化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。

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　有効化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上でサービスを表示しますか?（Is Service Displayed on Management Appliance?）] カラムが一致している必要があります。

- [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。

次の作業

ある機能についての有効および無効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。公開する機能の有効化（9-12 ページ）を参照してください。
- Web セキュリティ アプライアンスの当該の機能を有効または無効にします。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。『*AsyncOS for Cisco Web Security Appliances User Guide*』で該当する機能に関する情報を参照してください。

公開する機能の有効化

Configuration Master を使用して設定を公開する機能を有効にします。

はじめる前に

有効にする機能と無効にする機能を確認します。有効化されている機能の比較（9-11 ページ）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）] > [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　[設定の編集（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。

横に [なし（N/A）] と表示されている機能は、その Configuration Master のバージョンで使用できないことを意味します。

（注）　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るポリシー タイプのいずれかを実行するために有効になっていると見なされるため、機能としてリストされません。Web プロキシを無効にすると、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 3　（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 の無効化（9-13 ページ）の「注」を参照してください。

ステップ 4　使用する各 Configuration Master について、有効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有効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 5　使用する各 Configuration Master に対して変更を加えます。

ステップ 6　[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 アプライアンスに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。変更を送信しても問題ない場合は [続行（Continue）] をクリックします。

ステップ 7　[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 8　変更を保存します。

次の作業

- 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有効または無効になっていることを確認します。有効化されている機能の比較（9-11 ページ）を参照してください。
- 公開先の各 Web セキュリティ アプライアンスで、Configuration Master に対して有効にした機能と一致する機能が有効になっていることを確認します。

使用しない Configuration Master の無効化

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。

ただし、少なくとも 1 つの Configuration Master は有効にする必要があります。

（注）　Configuration Master を無効にすると、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。

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　[設定の編集（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。

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

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

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（9-1 ページ）を参照してください。

すべての公開ジョブ

- 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（2-2 ページ）を参照してください。
- （初回のみ）中央集中型で Webセキュリティ アプライアンスを管理する Configuration Master の設定（9-2 ページ）で説明する手順に従います。
- Configuration Master が公開を実施し、公開後に意図する機能が有効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。有効化されている機能の比較（9-11 ページ）、および必要に応じて公開する機能の有効化（9-12 ページ）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有効になっている場合は、各アプライアンスに個別に公開する必要があります。それぞれの公開前に機能が有効になっていることを確認してください。
- 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、『*AsyncOS for Cisco Web Security Appliances User Guide*』を参照してください。

- 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については、『*AsyncOS for Cisco Web Security Appliances 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。

特殊な状況

- 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 が有効化され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）] は無効になり、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）] オプションは無効になり、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。
- RSA サーバ用に設定されていない複数の Web セキュリティ アプライアンスにセキュリティ管理アプライアンスから外部 DLP ポリシーを公開すると、セキュリティ管理アプライアンスによって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 Names*>". 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無効化されます。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 に、Kerberos スキームを使用するレルムを使ってユーザを識別および認証する ID がある場合、次の警告が適用されます。
  - AsyncOS 8.0 for Web にアップグレードする前に Web セキュリティ アプライアンスで作成した Active Directory レルムは、Kerberos 認証スキームに対応していません。
  - 同じ名前でも Kerberos に対応していないレルムがある Web セキュリティ アプライアンスに Configuration Master 8.0 を公開すると、次の状況が発生します。

Configuration Master の アイデンティティのスキーム	Web セキュリティ アプライアンスの アイデンティティのスキーム
Kerberos 認証を使用	NTLMSSP 認証または Basic 認証を使用
Kerberos 認証または NTLMSSP 認証を使用	NTLMSSP 認証を使用
Kerberos 認証、NTLMSSP 認証、または Basic 認証を使用	NTLMSSP 認証または Basic 認証を使用

Configuration Master の公開

はじめる前に

Configuration Master を公開する前に（9-14 ページ）の重要な要件と情報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）] > [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 2　[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 3　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 4　公開する Configuration Master を選択します。

ステップ 5　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 6　[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。

次の作業

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（9-20 ページ）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

はじめる前に

Configuration Master を公開する前に（9-14 ページ）の重要な要件と情報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）] > [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 2　[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 3　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 4　Configuration Master を公開する日時を入力します。

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　[送信（Submit）] をクリックします。

ステップ 8　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 9　スケジュールされた公開時刻の後に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。

（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。

次の作業

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（9-20 ページ）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。

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（9-14 ページ）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*]

config_master は、サポートされている Configuration Master のバージョンです。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（9-1 ページ）を参照してください。

拡張ファイル公開を実行するには、次を参照してください。

- 拡張ファイル公開：[今すぐ設定を公開する（Publish Configuration Now）]（9-18 ページ）
- 拡張ファイル公開：[後で公開（Publish Later）]（9-19 ページ）

拡張ファイル公開：[今すぐ設定を公開する（Publish Configuration Now）]

はじめる前に

- 公開するコンフィギュレーション バージョンが、公開先アプライアンスの AsyncOS バージョンと互換性があることを確認します。互換性マトリクス（http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html）を参照してください。
- 各宛先の Web セキュリティ アプライアンスで、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 ファイルにバックアップします。詳細については、『*AsyncOS for Cisco Web Security Appliances User Guide*』を参照してください。

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。

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、『*AsyncOS for Cisco Web Security Appliances User Guide*』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のウィンドウで、[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 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。あるいはジョブ名（80 文字まで）を入力します。

ステップ 5　[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 6　[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 7　[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 8　[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）]

はじめる前に

- 公開するコンフィギュレーション バージョンが、公開先アプライアンスの AsyncOS バージョンと互換性があることを確認します。互換性マトリクス（http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html）を参照してください。
- 各宛先の Web セキュリティ アプライアンスで、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 ファイルにバックアップします。詳細については、『*AsyncOS for Cisco Web Security Appliances User Guide*』を参照してください。

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。

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、『*AsyncOS for Cisco Web Security Appliances User Guide*』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。あるいはジョブ名（80 文字まで）を入力します。

ステップ 5　設定を公開する日時を入力します。

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、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 7　[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 8　[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

内容	操作内容
スケジュール済みで実行されていない公開ジョブのリスト	[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、[保留中のジョブ（Pending Jobs）] セクションを確認してください。
各アプライアンスで最後に公開された設定のリスト	[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）] を選択し、[最新公開設定（Last Published Configuration）] の情報を参照してください。
現在進行中の公開ジョブのステータス	[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、[公開の進歩ステータス（Publishing Progress）] セクションを確認してください。
すべてまたは一部のアプライアンスに対するすべてまたは一部の公開ジョブの履歴	公開履歴の表示（9-20 ページ）を参照してください

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。

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をクリックします。

ステップ 3　ジョブの特定のアプライアンスに関する詳細を表示するには、アプライアンス名をクリックします。

[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）] ページが表示されます。

ステップ 4　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には、対応する [詳細（Details）] リンクをクリックします。

[Webアプライアンス公開の詳細（Web Appliance Publish Details）] ページが表示されます。

Web セキュリティ アプライアンス ステータスの表示

Web アプライアンス ステータスの概要の表示

[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 アプライアンスの全体的な概要が表示されます。

[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。

個々の Web セキュリティ アプライアンスのステータスの表示

[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。

(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。

(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 アプライアンスで無効になっているか、そこに存在しない場合は、[なし(N/A)] と表示されます。

ヒント Web セキュリティ アプライアンスで実行され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。すぐにデータを更新するには、[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。

Web アプライアンス ステータスの詳細

[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。

- 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 アプライアンスの各機能のステータス（各機能が有効になっているかどうか、ライセンス キーのステータス）
- 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
- Web セキュリティ アプライアンスの AnyConnect セキュア モビリティ設定
- Web セキュリティ アプライアンスのプロキシ設定（アップストリーム プロキシとプロキシの HTTP ポート）
- 認証サービス情報（サーバ、スキーム、レルム、シーケンス、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）

URL カテゴリ セットの更新の準備および管理

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、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 アプライアンスが URL カテゴリ セットの更新をシスコから自動的にダウンロードし、セキュリティ管理アプライアンスがこれらの更新を管理対象の Web セキュリティ アプライアンスから数分以内に自動的に受信します。

これらの更新は既存の設定およびアプライアンスの動作に影響を与える可能性があるので、事前に準備して更新後に対処する必要があります。

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（9-22 ページ）
- URL カテゴリ セットの更新に関する通知およびアラートの受信（9-23 ページ）
- 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（9-23 ページ）
- 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（9-23 ページ）

URL カテゴリ セットの更新による影響の理解

URL カテゴリ セットが更新されると、Configuration Master の既存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 セットの更新前後に必要となる処理の重要情報については、マニュアル（E-1 ページ）に掲載されているリンクで、『*AsyncOS for Cisco Web Security Appliances User Guide*』の「URL Filters」の章の「Managing Updates to the Set of URL Categories」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通知およびアラートの受信

受信対象	操作内容
URL カテゴリ セットの更新の事前通知	シスコ コンテンツ セキュリティ アプライアンスに関する通知（URL カテゴリ セットの更新に関する通知を含む）を受け取るには今すぐサインアップしてください。Cisco 通知サービス（E-1 ページ）を参照してください。
URL カテゴリ セットの更新が既存のポリシー設定に影響する場合のアラート	[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [アラート（Alerts）] に移動し、[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に設定されていることを確認します。アラートについての詳細は、アラートの管理（14-34 ページ）を参照してください。

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

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、『*AsyncOS for Cisco Web Security Appliances User Guide*』の「URL Filters」の章の「Choosing Default Settings for New and Changed Categories」セクション、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

URL 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、または無効化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、既存の URL カテゴリに基づくポリシーと ID 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、『*AsyncOS for Cisco Web Security Appliances User Guide*』の「Responding to Alerts about URL Category Set Updates」を参照してください。

コンフィギュレーション管理上の問題のトラブルシューティング

[Configuration Master] > [ID（Identities）] に [グループ（Groups）] が表示されない

問題　[Web] > [Configuration Master] > [ID（Identities）] のポリシー メンバーシップの定義ページで、[選択されたグループとユーザ（Selected groups and Users）] に [グループ（Groups）] オプションが表示されません。

ソリューション　複数の Web セキュリティ アプライアンスがある場合、すべての設定が同名のレルムに対して同一でない限り、各 WSA の [ネットワーク（Network）] > [認証（Authentication）] で、レルム名がすべての WSA で一意であることを確認します。

ヒント：各 WSA についてレルム名を確認するには、[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）] に移動して、各アプライアンス名をクリックし、詳細ページの下部までスクロールします。

[Configuration Master] > [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）] ページの設定が想定とは異なる

問題　Configuration Master の [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）] ページに、Web レピュテーション スコアのしきい値設定やアンチマルウェア スキャン エンジンを選択する機能など、想定される設定が表示されません。または、Web セキュリティ アプライアンスで Adaptive Security を使用している場合にこれらの設定が含まれます。

ソリューション　使用可能なオプションは、[Web] > [ユーティリティ（Utilities）] > [セキュリティ サービス表示（Security Services Display）] で、Adaptive Security がその Configuration Master に対して選択されているかどうかによって異なります。

設定公開失敗のトラブルシューティング

問題　設定を公開できません。

ソリューション　[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）] ページを確認します。公開が失敗する理由は次のとおりです。

- [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上でサービスを表示しますか？（Is Service Displayed on Management Appliance?）] カラムのステータスとの間に不一致があります。

- 両方のカラムで、機能が有効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ません（期限切れなど）。
- 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 のバージョンと一致している必要があります。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（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。

関連項目

- 公開履歴の表示（9-20 ページ）
- 有効化されている機能の比較（9-11 ページ）
- 公開する機能の有効化（9-12 ページ）

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（14-58 ページ）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有効にして、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

- 処理キューのモニタリング（10-2 ページ）
- CPU 使用率のモニタリング（10-3 ページ）
- 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（10-3 ページ）

セキュリティ管理アプライアンス容量のモニタリング

処理キューのモニタリング

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。

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　[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、主要な集約管理サービスのそれぞれに使われるセキュリティ管理アプライアンスの 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、[レポート サービス（Reporting Service）] 下で統合され、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（Quarantine Services）] 下で統合されます。セキュリティ管理アプライアンスのその他の動作は、汎用見出し [セキュリティ管理アプライアンス（Security Management appliance）] 以下にまとめられます。

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。

[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 アプライアンスで有効になっていません。
- [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 アプライアンスで有効になっていますが、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 アプライアンスで有効になっていません。
- [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 アプライアンスで有効になっていますが、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 マークは有効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（8-8 ページ）
- 管理対象アプライアンスの追加について（2-12 ページ）

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 ステータスの表示（9-21 ページ）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（10-5 ページ）
- 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（10-6 ページ）

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。

[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。

（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**無効の場合にのみ、Web Reporting が無効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。

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。

[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（5-35 ページ）
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（4-37 ページ）

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。

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。

- 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スパム隔離で表示できます。

  スパム隔離と連携させるための LDAP の設定（11-1 ページ）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に、Cisco コンテンツ セキュリティ管理アプライアンスにサインインする管理ユーザ。

  LDAP を使用した管理ユーザの外部認証の設定（11-15 ページ）を参照してください。

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 プロファイルには、AsyncOS が LDAP サーバに接続できるように次のような情報が含まれます。

- サーバ名およびポート
- ベース DN（Base DN）
- サーバにバインド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（11-2 ページ）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（11-12 ページ）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（11-4 ページ）を参照してください。

ステップ 3　**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有効にします。**

スパム隔離への LDAP エンドユーザ アクセスを有効にして、エンドユーザが隔離内のメッセージを表示および管理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有効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（7-2 ページ）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 を設定するには、LDAP サーバに関する情報を保存する 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（11-12 ページ）を参照してください。

ステップ 5　認証方法を選択します。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。[パスワードの使用（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るようになります。

ステップ 6　LDAP サーバのタイプを、[Active Directory]、[OpenLDAP]、[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 Active Directory のデフォルト ポートであり、複数サーバ環境のグローバル カタログへのアクセスが可能になります。

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。このユーザのエントリは、次のようになります。

```
uid=joe, ou=marketing, dc=example dc=com
```

ステップ 9　[詳細設定（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 バランシング用に LDAP サーバ プロファイルを設定した場合は、指定された LDAP サーバにこれらの接続が振り分けられます。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（11-14 ページ）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 接続も含まれます。ただし、スパム隔離の LDAP 認証を有効にした場合、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　[テスト サーバ（Test Server(s)）] ボタンをクリックしてサーバへの接続をテストします。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（11-4 ページ）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。

エンドユーザ隔離へのログイン時にユーザを検証する、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（11-4 ページ）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、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。

- **スパム隔離エンドユーザ認証クエリー。**詳細については、「スパム隔離エンドユーザ認証クエリー」セクション（11-5 ページ）を参照してください。
- **スパム隔離エイリアス統合クエリー。**詳細については、スパム隔離エイリアス統合クエリー（11-7 ページ）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 クエリーはすべて無効化されます。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（11-8 ページ）およびチェーン クエリー（11-10 ページ）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（11-5 ページ）
- トークン（11-5 ページ）

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 機能を有効にしてください。詳細については、「LDAP クエリーのテスト」セクション（11-8 ページ）を参照してください。

スパム隔離エンドユーザ認証クエリー

エンドユーザ認証クエリーとは、スパム隔離にログインする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 サーバのエンドユーザ認証用デフォルト 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エンドユーザ認証の設定例：Active Directory

認証方式（Authentication Method）	**[パスワードの使用（Use Password）]（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（Server Type）	Active Directory
ポート（Port）	3268
ベース DN（Base DN）	（ブランク）
接続プロトコル（Connection Protocol）	（ブランク）
クエリー文字列（Query String）	(sAMAccountName={u})
メール属性（Email Attribute(s)）	mail,proxyAddresses

OpenLDAP エンドユーザ認証の設定例

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 サーバのエンドユーザ認証用デフォルト 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エンドユーザ認証の設定例：OpenLDAP

認証方式（Authentication Method）	**匿名**
サーバ タイプ（Server Type）	OpenLDAP
ポート（Port）	389
ベース DN（Base 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（Connection Protocol）	（ブランク）
クエリー文字列（Query String）	(uid={u})
メール属性（Email Attribute(s)）	mail,mailLocalAddress

スパム隔離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 エイリアスを統合すると、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、ある受信者が電子メール 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 アドレスの属性を [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、デフォルト クエリー文字列(実際の展開では異なることもあります)は `(|(proxyAddresses={a})(proxyAddresses=smtp:{a}))` で、デフォルト メール属性は `mail` です。OpenLDAP サーバの場合は、デフォルト クエリー文字列が `(mail={a})` で、デフォルト メール属性が `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例(11-7 ページ)
- OpenLDAP エイリアス統合の設定例(11-8 ページ)

Active Directory エイリアス統合の設定例

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 サーバの匿名認証、Active Directory サーバのエイリアス統合用クエリー文字列、`mail` メール属性を使用します。

表 11-3　LDAP サーバとスパム隔離エイリアス統合の設定例:Active Directory

認証方式(Authentication Method)	**匿名**
サーバ タイプ(Server Type)	Active Directory
ポート(Port)	3268
ベース DN(Base DN)	(ブランク)
接続プロトコル(Connection Protocol)	SSL を使用する(Use SSL)
クエリー文字列(Query String)	(|(mail={a})(mail=smtp:{a}))
メール属性(Email Attribute)	メール アドレス

OpenLDAP エイリアス統合の設定例

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 サーバの匿名認証、OpenLDAP サーバのエイリアス統合用クエリー文字列、mail メール属性を使用します。

表 11-4　LDAP サーバとスパム隔離エイリアス統合の設定例：OpenLDAP

認証方式（Authentication Method）	**匿名**
サーバ タイプ（Server Type）	OpenLDAP
ポート（Port）	389
ベース DN（Base 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（Connection Protocol）	SSL を使用する（Use SSL）
クエリー文字列（Query String）	`(mail={a})`
メール属性（Email Attribute）	メール アドレス

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。詳細には、最初のステージの SMTP 認証に成功したか失敗したか、バインド照合で返された結果が true か false かなどが含まれます。

`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。

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、「成功：アクション：一致ポジティブ（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用の電子メール アドレスと共に、「成功：アクション：エイリアス統合（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スパム隔離のエンドユーザ アクセスまたは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（11-2 ページ）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（11-9 ページ）を参照してください。

ステップ 3　スパム隔離に対して、エンドユーザ アクセスおよびスパム通知を有効にします。詳細については、中央集中型スパム隔離の設定（7-2 ページ）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、[詳細設定（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 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、クエリー タイプを 1 つだけ指定します。クエリー 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。

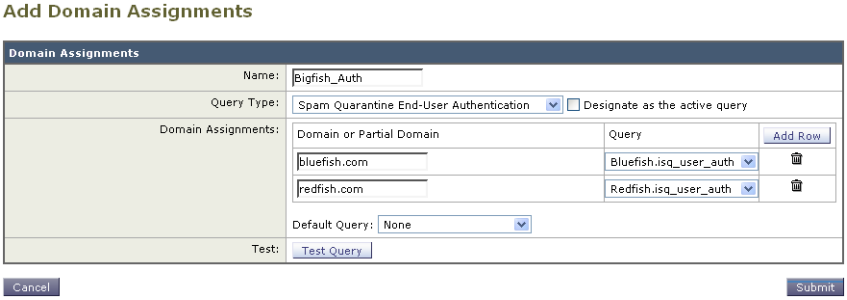
ステップ 5　[ドメイン割り当て（Domain Assignments）] フィールドに、ドメインを入力します。

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　他のすべてのクエリーが失敗したときに実行するデフォルト クエリーを入力します。デフォルト 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　クエリーをテストします。[クエリのテスト（Test Query）] ボタンをクリックし、テストするユーザ ログインとパスワードまたは電子メール アドレスを [テストパラメータ（Test Parameters）] のフィールドに入力します。結果が [接続ステータス（Connection Status）] フィールドに表示されます。

ステップ 10　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、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まで、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スパム隔離のエンドユーザ アクセスまたは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、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（11-2 ページ）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、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（11-11 ページ）を参照してください。

ステップ 3　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有効にします。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（7-2 ページ）を参照してください。

チェーン クエリーの作成

ヒント　CLI で `ldapconfig` コマンドの `advanced` サブコマンドを使用することもできます。

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 [詳細設定（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。

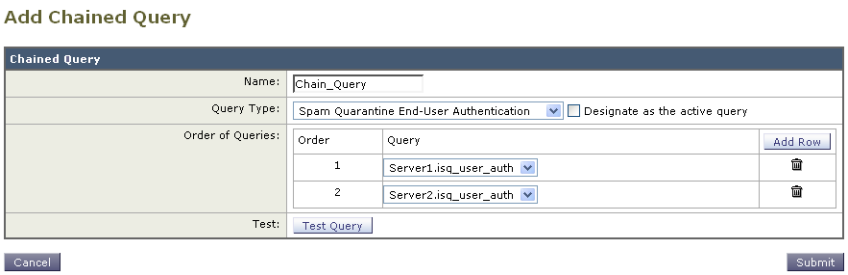
ステップ 5　クエリー タイプを選択します。

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 クエリーをすべて同じクエリー タイプにします。クエリー 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　クエリーをテストするには、[クエリのテスト（Test Query）] ボタンをクリックし、ユーザ ログインとパスワードまたは電子メール アドレスを [テストパラメータ（Test Parameters）] のフィールドに入力します。結果が [接続ステータス（Connection Status）] フィールドに表示されます。

ステップ 8　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、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 サーバ 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（または編集）（Add (or 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、そのサーバを LDAP サーバ リストの先頭に入力してください。

シスコ コンテンツ セキュリティ アプライアンスが 2 番目または後続の LDAP サーバに接続した場合、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 コンテンツ セキュリティ アプライアンスの設定

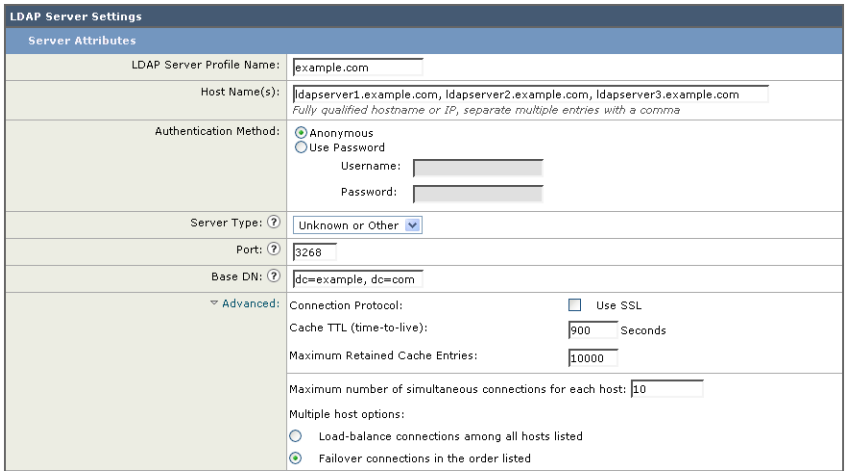
手順

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 フェールオーバーの設定例



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 コンテンツ セキュリティ アプライアンスの設定

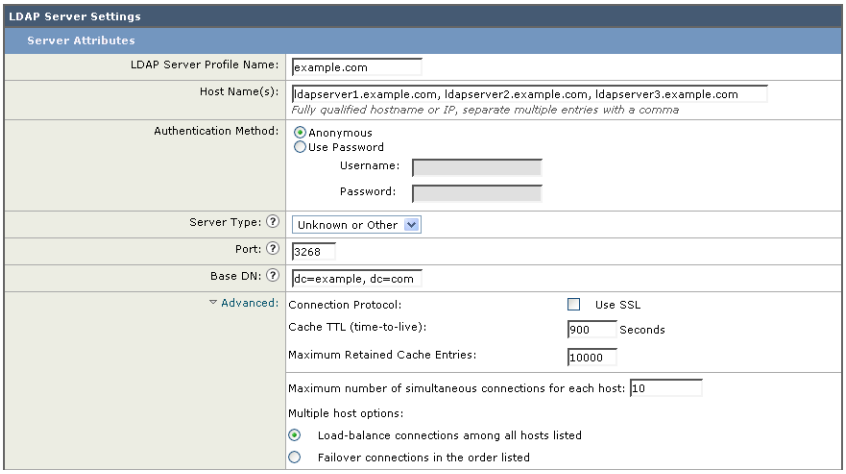
手順

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 バランシングの設定例



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。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、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（11-2 ページ）を参照してください。

ステップ 2　**ユーザ アカウントを検索す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、LDAP ディレクトリ内のユーザ アカウントを検索するクエリーを作成します。管理ユーザの認証のためのユーザ アカウント クエリー（11-15 ページ）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。**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、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（11-16 ページ）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（11-8 ページ）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、管理ユーザの外部認証の有効化（11-18 ページ）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索し、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。選択したサーバ タイプに応じて、AsyncOS によってデフォルト クエリーとデフォルト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 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 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（Server Type）	Active Directory
ベース DN（Base 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（Query String）	`(&(objectClass=user)(sAMAccountName={u}))`
ユーザのフル ネームが格納されている属性（Attribute containing the user's full name）	`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 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（Server Type）	OpenLDAP
ベース DN（Base 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（Query String）	`(&(objectClass=posixAccount)(uid={u}))`
ユーザのフル ネームが格納されている属性（Attribute containing the user's full name）	`gecos`

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、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、グループのすべてのメンバーを検索する別のクエリーも使用します。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`）で外部認証を有効にするときに、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 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 ロールを割り当てます。

1 人のユーザが複数の LDAP グループに属しており、それぞれユーザ ロールが異なる場合は、最も限定的なロールのアクセス許可が AsyncOS によってそのユーザに付与されます。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、グループ メンバーのユーザ名が格納されている属性、および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 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（Query String）	Active Directory
ベース DN（Base 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（Query String）	OpenLDAP
ベース DN（Base 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有効化

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有効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、[行を追加（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。

SMTP ルーティングの設定

SMTP ルートの概要

この章では、Cisco コンテンツ 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。

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` へのマッピングを作成できます。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（12-4 ページ）を参照）。

この機能を使用すると、ホストを「ひとかたまりにする」ことができます。`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に一致します。たとえば、`fred@foo.example.com` と `wilma@bar.example.com` は、いずれ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はホストの `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。

電子メールの配信時は、SMTP ルート テーブルは必ず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、host1.example.com のエントリがより具体的であるため、こちらが使用されます。具体的ではない example.com エントリが先であっても、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。

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。

分割：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 サーバを使用してる場合でも、メッセージは分割されます。つまり、1 つの TCP 接続により、10 通の別々の電子メールが配信されます。

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。

ローカル ドメインにおける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（Alerts）
- 指定した宛先にメール送信され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され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 アプライアンスは、[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）を使用して指定したホストに、ローカル ドメイン宛てのメールを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て変更を保存した場合、そのときに入力した RAT エントリごとに、アプライアンスで最初の SMTP ルート エントリが定義されています。

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、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 SMTP ルートは ALL: として記載されます。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)] ページまたは **smtproutes** コマンドを使用して、デフォルト SMTP ルートを設定します。

SMTP ルートの管理

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)を使用して指定し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。そのため、定義できるのは最大 9,999 個のカスタム ルートと、特殊なキーワード ALL を使用するルート 1 個です。

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

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　エクスポートした SMTP ルートを含む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。インポートによって既存の 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。

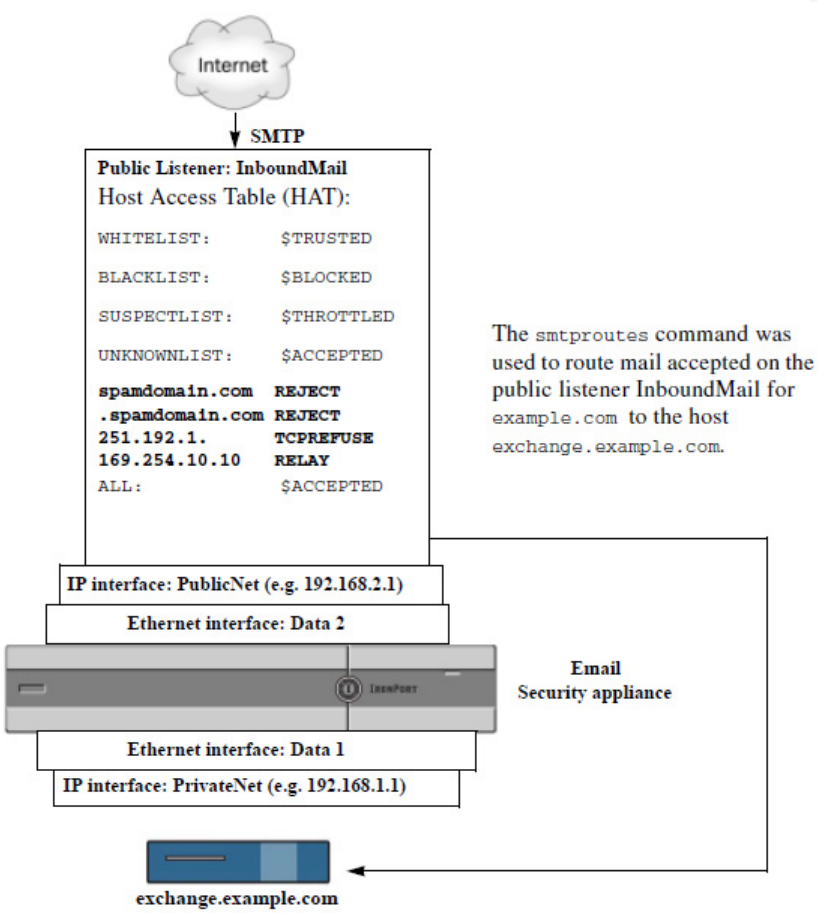
ステップ 4　[インポート（Import）] をクリックします。

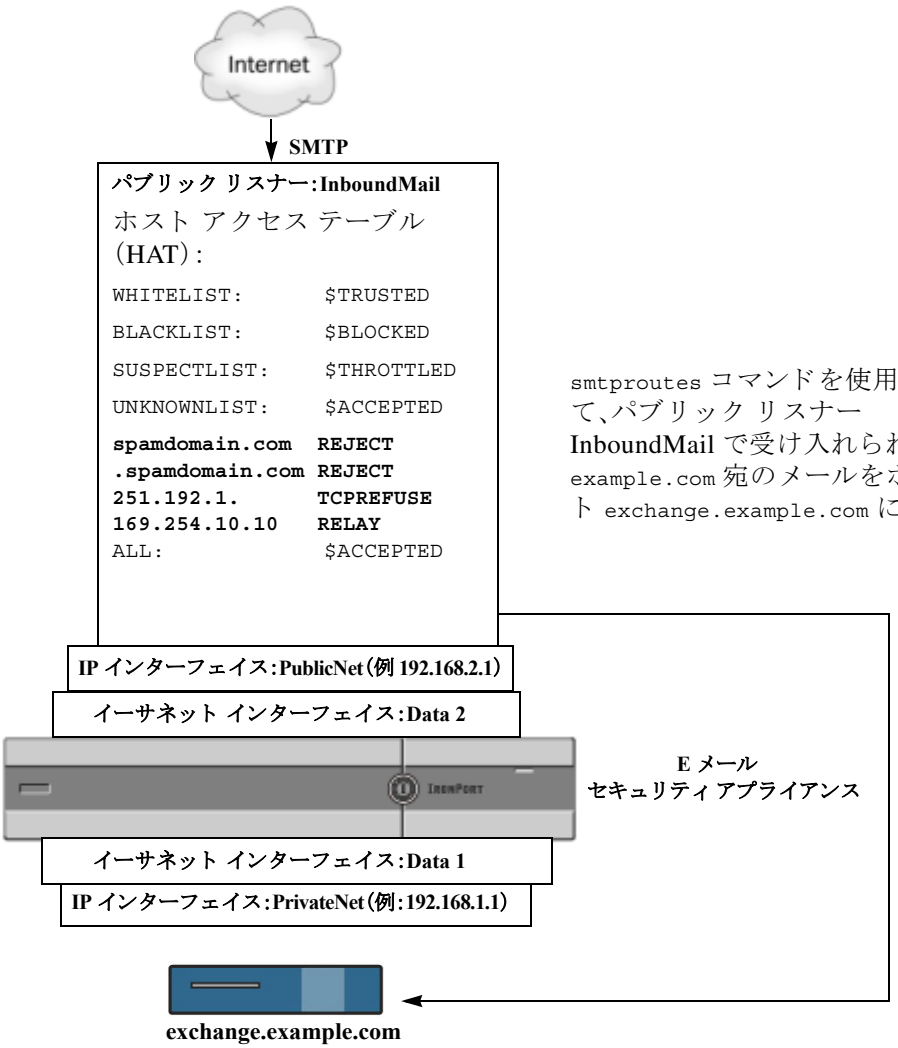
ファイル内に「コメント」を配置できます。文字「#」で始まる行はコメントと見なされ、AsyncOS によって無視されます。次に例を示します。

```
# 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

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
```

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

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（Scheduled Reports）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
管理者（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
オペレータ（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有効になっている場合）。 • 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
専門技術者（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。	[Web] および [メール（Email）] タブのシステム キャパシティ レポートへのアクセス

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（Scheduled Reports）機能
読み取り専用オペレータ（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。 • 隔離の作成、編集、削除、または集約の設定。	あり/なし
ゲスト（Guest）	Guest 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、レポートおよび Web トラッキングを含むステータス情報を表示し、隔離内のメッセージを管理できます。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 管理者（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 ポリシー管理者（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 フィルタリング管理者（URL Filtering Administrator）	URL フィルタリング管理者ロールを持つユーザ アカウントは、Web セキュリティの URL フィルタリングのみ設定できます。	なし/なし
メール管理者（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（Scheduled Reports）機能
ヘルプ デスク ユーザ（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の管理 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（13-4 ページ）を参照してください。	なし/なし

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（13-5 ページ）
- Custom Web User ロールについて（13-8 ページ）
- カスタム ユーザ ロールの削除（13-10 ページ）

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 レポーティングへのアクセス

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
- 受信メール（Incoming Mail）
- 発信先
- 送信メッセージ送信者（Outgoing Senders）
- 内部ユーザ

- DLP インシデント（DLP Incidents）
- コンテンツ フィルタ
- ウイルスの種類
- TLS 接続
- アウトブレイク フィルタ
- 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
- 受信メール（Incoming Mail）
- 発信先
- 送信メッセージ送信者（Outgoing Senders）
- 内部ユーザ
- コンテンツ フィルタ
- ウイルスの種類
- アウトブレイク フィルタ
- 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 データへのアクセス

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（13-25 ページ）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有効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。

カスタム ユーザ ロールの隔離へのアクセス

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。隔離へのアクセス（13-11 ページ）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有効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。

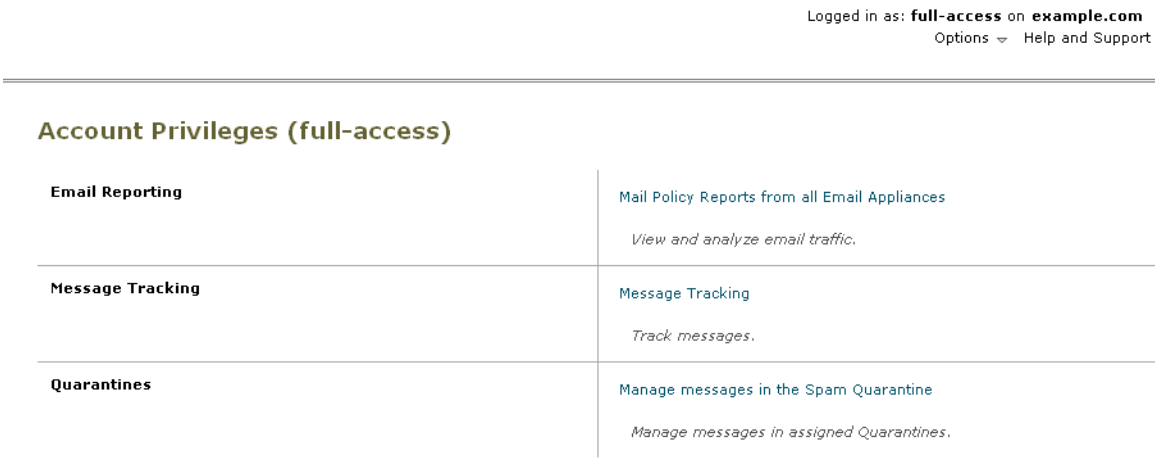
参照先:

- スパム隔離への管理ユーザ アクセスの設定（7-6 ページ）。
- ポリシー隔離の作成（8-12 ページ）。

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
- カスタム ユーザ ロールの削除（13-10 ページ）

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有効にしていた場合、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。匿名機能が有効になっている場合、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 ロールを削除しても、エラーは受信しません。

CLI へのアクセス権を持つユーザ ロール

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(ヘルプ デスク ユーザ、メール管理者、Web 管理者、Web ポリシー管理者、URL フィルタリング管理者(Web セキュリティ)、およびカスタム ユーザ)は GUI だけにアクセスできます。

LDAP の使用

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、個々のユーザではなくユーザ ロールにディレクトリ 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(13-19 ページ)を参照してください。

隔離へのアクセス

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。次の情報を参照してください。

- スパム隔離への管理ユーザ アクセスの設定(7-6 ページ)、
- ポリシー隔離の作成(8-12 ページ)(ポリシー隔離)、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(8-9 ページ)。

[ユーザ(Users)] ページ

次のセクションの詳細について	参照先
ユーザ(Users)	管理タスクの分散について ローカルに定義された管理ユーザの管理
[パスワードのリセット(Reset Passwords)] ボタン	オン デマンドでの次回ログイン時のユーザに対するパスワード変更の義務付け
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)	パスワードの設定およびログインの要件
外部認証(External Authentication)	外部ユーザ認証
DLP トラッキング権限(DLP Tracking Privileges)	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

管理ユーザの認証について

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。

- admin ユーザのパスワードの変更(13-12 ページ)
- ローカルに定義された管理ユーザの管理(13-12 ページ)
- 外部ユーザ認証(13-19 ページ)

admin ユーザのパスワードの変更

管理者レベルのユーザは、GUI または CLI を使用して「admin」ユーザのパスワードを変更できます。

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。

admin ユーザのパスワードを CLI から変更するには、password コマンドを使用します。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。

「admin」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。

ローカルに定義された管理ユーザの管理

ローカルに定義されたユーザの追加

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）　外部認証も有効である場合は、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（13-4 ページ）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　[ユーザの追加（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（13-7 ページ）またはCustom Web User ロールの作成（13-9 ページ）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（13-4 ページ）を参照してください。

ローカルに定義されたユーザの編集

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。

ローカルに定義されたユーザの削除

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 ロールが削除されている場合は、[未定義（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（13-4 ページ）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、ローカルに定義されたユーザの編集（13-13 ページ）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、admin ユーザのパスワードの変更（13-12 ページ）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、オン デマンドでの次回ログイン時のユーザに対するパスワード変更の義務付け（13-17 ページ）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。
- **パスワード存続期間のルール。**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。
- **パスワードのルール。**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　設定を行います。

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、ログインを試みているユーザに表示するメッセージを入力します。テキストは 7 ビット ASCII 文字を使用して入力します。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、管理者は GUI で [ユーザの編集（Edit User）] ページを使用するか、`userconfig` CLI コマンドを使用してロックを解除できます。 失敗したログインの試行は、ユーザが接続しているマシンや、接続のタイプ（SSH または HTTP など）に関係なく、ユーザ別に追跡されます。ユーザがログインに成功すると、失敗ログイン試行の回数は 0 にリセットされます。 失敗ログイン試行の最大回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ると、管理者にアラートが送信されます。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（13-18 ページ）を参照してください。
Password Reset（パスワードのリセット）	管理者がユーザのパスワードを変更した後で、ユーザにパスワードを強制的に変更させるかどうかを選択します。 パスワードが期限切れになった後で、ユーザにパスワードを強制的に変更させるかどうかを選択することもできます。ユーザがパスワードを変更するまでのパスワードの存続日数を入力します。1 から 366 までの任意の数を入力できます。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、オン デマンドでの次回ログイン時のユーザに対するパスワード変更の義務付け（13-17 ページ）を参照してください。 期限切れ後にユーザにパスワードを強制的に変更させる場合は、次回のパスワード期限に関する通知を表示できます。期限切れの何日前にユーザに通知するかを選択します。 **（注）**　ユーザ アカウントがパスワード チャレンジの代わりに SSH キーを使用している場合でも、Password Reset ルールが適用されます。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。
パスワードの規則（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。 0（ゼロ）から 128 までの数字を入力してください。 デフォルトは 8 です。 パスワードには、ここで指定した数以上の文字を使用できます。

設定	説明
パスワードの規則（Password Rules）： 数字(0 ～ 9)が 1 文字以上必要です。（Require at least one number (0-9). ）	パスワードに数字を少なくとも 1 文字含める必要があるかどうかを選択します。

パスワードの規則（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。
	`~ ? ! @ # $ % ^ and * - _+ =`
	`\ | / [ ] ( ) < > { } ` ' " ; : , 。`

パスワードの規則（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」
パスワードの規則（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。
パスワードの規則（Password Rules）： パスワードで許可しない単語の一覧（List of words to disallow in passwords）	パスワードでの使用を禁止する語のリストを作成できます。 このファイルは、許可しない語ごとに行を分けたテキスト ファイルにします。ファイルに名前 `forbidden_password_words.txt` を付けて保存し、SCP または FTP を使用してファイルをアプライアンスにアップロードします。 この制限を選択しても語のリストをアップロードしないと、この制限は無視されます。

設定	説明
パスワードの強度（Password Strength）	管理者またはユーザが新しいパスワードを入力したときに、パスワード強度インジケータを表示できます。 この設定は強固なパスワードの作成を強制するものではありません。入力されたパスワードがどの程度簡単に推測されるかを示すだけです。 インジケータを表示するロールを選択します。次に、選択した各ロールに対して、0 よりも大きい数値を入力します。数値が大きいほど、強力なパスワードとして登録されたパスワードが推測困難であることを意味します。この設定に最大値はありません。 次に、例を示します。 • `30` と入力した場合は、少なくとも 1 つの大文字と小文字、数字、特殊文字を含む 8 文字のパスワードが強力なパスワードとして登録されます。 • `18` と入力した場合は、すべて小文字で数字と特殊文字を含まない 8 文字のパスワードが強力なパスワードとして登録されます。 パスワードの強度は対数目盛で測定されます。評価は、付録 A の NIST SP 800-63 で定義されているエントロピーの米国立標準技術研究所のルールに基づいています。 一般的に、強固なパスワードは次のような特徴を備えています。 • 長い • 大文字、小文字、数字、特殊文字が含まれている • どのような言語であれ辞書にある単語が含まれていない このような特徴を持つパスワードを強制するには、このページの他の設定を使用します。

ステップ 5　変更を送信し、保存します。

次の作業

ユーザに新しい要件を満たす新しいパスワードへの変更を要求します。オン デマンドでの次回ログイン時のユーザに対するパスワード変更の義務付け（13-17 ページ）を参照してください

オン デマンドでの次回ログイン時のユーザに対するパスワード変更の義務付け

アドホック ベースで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、すべてまたは選択したユーザにパスワードの変更を要求するには、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（13-14 ページ）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、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オンにします。

ステップ 3　[パスワードの変更を実施（Enforce Password Changes）] を選択します。

ステップ 4　オプションを選択します。

猶予期間のグローバル設定は [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）] で設定します。

ステップ 5　[OK] 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（13-14 ページ）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（13-18 ページ）を参照してください。

[ユーザ役割の編集（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：ユーザ アカウントのロックを有効にするようにアプライアンスを設定します。

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（13-19 ページ）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。

メモ

- ビューのカスタマイズ（14-57 ページ）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。

参照先:

- LDAP を使用した管理ユーザの外部認証の設定（11-15 ページ）
- RADIUS 認証の有効化（13-20 ページ）

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（11-15 ページ）を参照してください。

RADIUS 認証の有効化

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は、アプライアンスからログアウトして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）[行を追加（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必要がある場合があります。

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 • メール管理者 • Web 管理者 • Web ポリシー管理者 • URL フィルタリング管理者（Web セキュリティ） • カスタム ユーザ ロール（電子メールまたは Web） 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ユーザに割り当てられている場合、RADIUS サーバのリストにある最後のクラス属性が使用されます。 • Technician • Operator • Read-Only Operator • ヘルプ デスク ユーザ • 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 サーバ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.
```

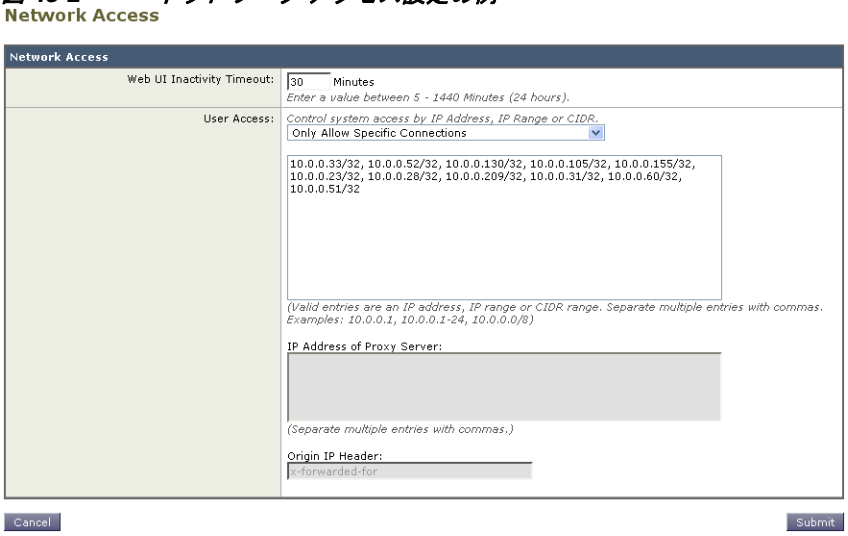
このヘッダーの値はカンマ区切りの IP アドレスのリストです。左端のアドレスがリモート ユーザ マシンのアドレスで、その後に、接続要求を転送した一連の各プロキシのアドレスが続きます（ヘッダー名は設定可能です）。セキュリティ管理アプライアンスは、ヘッダーから取得したリモート ユーザの IP アドレスおよび接続プロキシの IP アドレスを、アクセス リスト内の許可されたユーザ IP アドレスおよびプロキシ IP アドレスと照合します。

（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。
- **[Only Allow Specific Connections Through Proxy（特定のプロキシ経由接続のみを許可）]** 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、アクセス リストの [プロキシサーバのIPアドレス（IP Address of Proxy Server）] フィールドに含まれている。
  - プロキシで、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 リスト内のユーザに対して定義された IP アドレス、IP 範囲、または CIDR 範囲と一致する。
- **[特定の直接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。プロキシ経由接続の条件は、[特定のプロキシ経由接続のみを許可（Only Allow Specific Connections Through Proxy）] モードと同じです。

次のいずれかの条件が true の場合、変更を送信して確定した後、アプライアンスにアクセスできなくなることがありますので注意してください。

- [特定の接続のみを許可（Only Allow Specific Connections）] を選択し、現在のマシンの IP アドレスがリストに含まれていない場合。
- [特定のプロキシ経由接続のみを許可（Only Allow Specific Connections Through Proxy）] を選択し、現在アプライアンスに接続されているプロキシの IP アドレスがプロキシ リストに存在せず、許可されている IP アドレスのリストに送信元 IP ヘッダーの値が存在しない場合。
- [特定の直接またはプロキシ経由接続のみを許可（Only Allow Specific Connections Directly or Through Proxy）] を選択し、
  - 許可されている IP アドレスのリストに送信元 IP ヘッダーの値が存在しない場合

    または
  - 許可されている IP アドレスのリストに送信元 IP ヘッダーの値が存在せず、アプライアンスに接続されたプロキシの IP アドレスが許可されているプロキシのリストに存在しない場合。

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　[設定の編集（Edit Settings）] をクリックします。

ステップ 3　アクセス リストの制御モードを選択します。

ステップ 4　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、ヘッダーの名前は `x-forwarded-for` です。

ステップ 6　変更を送信し、保存します。

Web UI セッション タイムアウトの設定

AsyncOS が、セキュリティ管理アプライアンスの Web UI から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　[設定の編集（Edit Settings）] をクリックします。

ステップ 3　ログアウトになるまでの非アクティブ時間を分単位で入力します。5 ～ 1440 分のタイムアウト期間を定義できます。

ステップ 4　変更を送信し、保存します。

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有効にする必要があります。

管理ユーザ向けメッセージの表示

管理ユーザがアプライアンスにサインインするときにメッセージを表示できます。

メッセージを設定またはクリアするには、次の手順を実行します。

ステップ 1　テキスト ファイルをインポートする場合は、アプライアンスの `/data/pub/configuration` ディレクトリにインポートします。

ステップ 2　コマンドライン インターフェイス（CLI）にアクセスします。

ステップ 3　`adminaccessconfig > BANNER` コマンドとサブコマンドを使用します。

ステップ 4　変更を確定します。

管理ユーザ アクティビティの表示

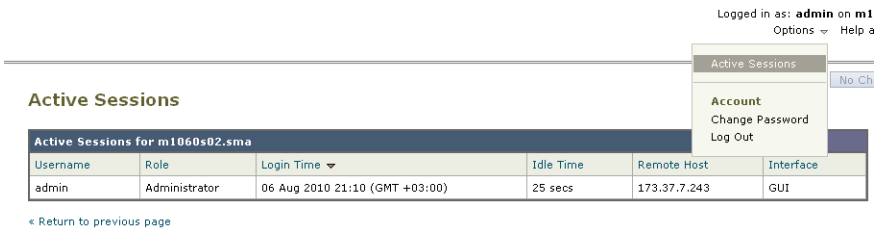
Web を使用したアクティブなセッションの表示

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。

最近のログイン試行の表示

Web インターフェイス、SSH、または FTP を介した直近数回のログイン試行を表示するには、次の手順を実行します。

ステップ 1　ログインします。

ステップ 2　画面の右上部付近にある [次のユーザとしてログイン（Logged in as）] の横の アイコンをクリックします。

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 または Web ユーザ インターフェイスを介してシステムにログインしたすべてのユーザ、ユーザのロール、ログイン時刻、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。
- `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
```

管理ユーザ アクセスのトラブルシューティング

エラー:ユーザにアクセス権限が割り当てられていません（User Has No Access Privileges Assigned）

問題　管理を委任されたユーザはセキュリティ管理アプライアンスにログインできますが、アクセス権限が割り当てられていないというメッセージが表示されます。

ソリューション

- このユーザに割り当てられたカスタム ユーザ ロールに権限を割り当てたことを確認します。[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザ（Users）] を表示して、割り当てられているユーザ ロールを特定してから、[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、ユーザ ロールの名前をクリックしてロールに権限を割り当てます。
- レポーティング グループに基づいてアクセスを割り当てた場合は、[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）] ページで、そのユーザのレポーティング グループが選択されていることを確認します。グループを割り当てるには、[委任管理用のユーザ役割（User Roles for Delegated Administration）] テーブルの [メールレポート（Email Reporting）] カラムで [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ます。

アクティブ メニューがありません（User Has No Active Menus）

問題　公開権限を付与されたユーザのログイン時に、アクティブ メニューがありません。

ソリューション　少なくとも 1 つのアクセス ポリシーまたはカスタム URL カテゴリにアクセス権を付与したことを確認します。いずれかを編集できるこのユーザ権限を付与しない場合は、どのポリシーでも使用されていないカスタム URL カテゴリを作成し、[カスタムユーザ役割（Custom User Role）] ページでこのカテゴリにこのユーザ ロール権限を付与します。

外部認証されたユーザに設定オプションが表示されます（Externally-Authenticated Users See Preferences Option）

問題　外部認証されたユーザに設定オプションが表示されます。

ソリューション　セキュリティ管理アプライアンスで直接追加するユーザのユーザ名が、外部認証データベースで使用されていない一意のユーザ名であることを確認します。

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（B-3 ページ）を参照してください。

ライセンス キーの使用

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、また有効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。

ここで説明するタスクをコマンドライン プロンプトから実行するには、`featurekey` コマンドを使用します。

目的	操作内容
• 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 キーを手動でインストールする • ライセンス キーをアクティブ化する	[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。 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。 発行されたときに自動的に新しいキーを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した場合、[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 キーの自動ダウンロードおよびアクティベーションを有効または無効にする	[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）] を選択します。 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。
期限切れライセンス キーを更新する	シスコの担当者にお問い合わせください。

仮想アプライアンスのライセンスおよびライセンス キー

ライセンスおよびライセンス キーの期限が切れたときのアプライアンスの動作については、http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-installation-guides-list.html から入手できる『*Cisco Content Security Virtual Appliance Installation Guide*』を参照してください。

ライセンス情報を表示するには、コマンドライン インターフェイス（CLI）で `showlicense` コマンドを使用します。

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`
- `suspendtransfers`
- `resume`
- `resumetransfers`
- `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の停止

システム メンテナンスを実行する場合など、アプライアンスをオフラインにするには、次のコマンドのいずれかを使用します。

コマンド	説明	パーシステンス
suspend	• 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の隔離されたメッセージの転送を一時停止します。 • 隔離からリリースされたメッセージの配信を一時停止します。 • 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。 • ログ転送が停止されます。 • CLI はアクセス可能のままになります。	リブート後も維持されます。
suspendtransfers	管理対象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コンテンツ セキュリティ管理アプライアンスへのレポーティング データおよびトラッキング データの転送を一時停止します。 このコマンドでは、電子メール セキュリティ アプライアンスからの隔離されたメッセージの受信も一時停止されます。 バックアップ アプライアンスをプライマリ アプライアンスとして再開するための準備段階でこのコマンドを使用します。	リブート後も維持されます。

これらのコマンドの使用時には、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存在しない場合は、すぐにサービスが停止されます。

suspend または suspendtransfers コマンドで停止したサービスを再アクティブ化するには、resume または resumetransfers コマンドをそれぞれ使用します。

管理アプライアンスの現在のステータス（オンラインまたは一時停止）を特定するには、Web インターフェイスで [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）] を選択します。

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」。

CLI の例：suspend および suspendtransfers コマンド

```
sma.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.
sma.example.com>
```

```
sma.example.com> suspendtransfers

Transfers suspended.
sma.example.com>
```

一時停止状態からの再開

resume コマンドは、suspend または suspenddel コマンドの使用後にアプライアンスを通常の動作状態に戻します。

resumetransfers コマンドは、suspendtransfers コマンドの使用後にアプライアンスを通常の動作状態に戻します。

CLI の例：resume および resumetransfers コマンド

```
sma.example.com> resume

Receiving resumed.
Mail delivery resumed.
sma.example.com>


sma.example.com> resumetransfers

Receiving resumed.
Transfers resumed.
sma.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 • 隔離されたメッセージを保持	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. アプライアンスのサービスを一時停止します。 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> suspend

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有効化

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。

アプライアンスの電源をリモートでリセットする場合は、このセクションで説明されている手順を使用して、この機能を事前に有効にし、設定しておく必要があります。

はじめる前に

- 専用リモート電源管理ポートをセキュア ネットワークに直接、ケーブル接続します。詳細については、ハードウェア インストレーション ガイドを参照してください。
- ファイアウォールを通過するために必要なポートを開くなど、アプライアンスがリモートアクセス可能であることを確認します。
- この機能では、専用のリモート電源管理インターフェイス用に一意の IPv4 アドレスが必要です。このインターフェイスは、このセクションで説明されている手順でのみ設定可能です。`ipconfig` コマンドを使用して設定することはできません。
- アプライアンスの電源を再投入するには、Intelligent Platform Management Interface（IPMI）バージョン 2.0 をサポートするデバイスを管理できるサードパーティ製ツールが必要です。このようなツールを使用できるように準備されていることを確認します。
- コマンドライン インターフェイスへのアクセスに関する詳細については、CLI のリファレンス 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　管理者権限を持つアカウントを使用してログインします。

ステップ 3　次のコマンドを入力します。

```
remotepower
setup
```

ステップ 4　プロンプトに従って、次の情報を指定します。

- この機能専用の IP アドレスと、ネットマスクおよびゲートウェイ。
- 電源の再投入コマンドを実行するために必要なユーザ名とパスワード。

これらのクレデンシャルは、アプライアンスへのアクセスに使用する他のクレデンシャルに依存しません。

ステップ 5　commit を入力して変更を保存します。

ステップ 6　設定をテストして、アプライアンスの電源をリモートで管理できることを確認します。

ステップ 7　入力したクレデンシャルが、将来、いつでも使用できることを確認します。たとえば、この情報を安全な場所に保管し、このタスクを実行する必要がある管理者が、必要なクレデンシャルにアクセスできるようにします。

関連項目

- アプライアンスの電源のリモート リセット（16-8 ページ）

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

バックアップの対象として、すべてのデータまたは次のデータの任意の組み合わせを選択できます。

- 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
- 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

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（14-14 ページ）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	ソースおよびターゲット セキュリティ管理アプライアンスの AsyncOS バージョンは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。
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。
ターゲット アプライアンスを停止する必要があります。	プライマリ アプライアンスのみが、管理対象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データを取得する必要があります。確実に実行するために、ターゲット アプライアンスによる管理対象アプライアンスからのデータの直接取得の防止（14-11 ページ）を参照してください。 また、バックアップ アプライアンスでスケジュール設定されている設定公開ジョブをキャンセルしてください。

制約事項	要件
アプライアンス キャパシティ	ターゲット アプライアンスのディスク領域キャパシティが、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 アプライアンスで各データ タイプ（レポーティング、トラッキング、隔離など）に割り当てるディスク領域は、ソース アプライアンスの対応する割り当てより少なくすることはできません。 各データ タイプの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 アプライアンス上にあれば、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。ソース アプライアンスがターゲット アプライアンスよりも大きい場合、ターゲット アプライアンスで使用可能な領域に合わせて、ソース アプライアンスで割り当てられている領域を削減します。 ディスク領域の割り当てとキャパシティを表示および管理するには、ディスク領域の管理（14-53 ページ）を参照してください。 仮想アプライアンスのディスク容量については、『*Cisco Content Security Virtual Appliance Installation Guide*』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以降、ソース アプライアンスとターゲット アプライアンス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、ソース アプライアンスとターゲット アプライアンスの両方で、サービスがバックアップ開始時の状態に戻ります。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 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（unresolved）」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。このウィンドウでは、ページの上部に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。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。

ターゲット アプライアンスによる管理対象アプライアンスからのデータの直接取得の防止

ステップ 1　ターゲット アプライアンスのコマンドライン インターフェイスにアクセスします。この説明については、コマンドライン インターフェイスへのアクセス（2-8 ページ）を参照してください。

ステップ 2　`suspendtransfers` コマンドを実行します。

ステップ 3　プロンプトが再表示されるまで待ちます。

ステップ 4　`suspend` コマンドを実行します。

ステップ 5　プロンプトが再表示されるまで待ちます。

ステップ 6　ターゲット アプライアンスのコマンドライン インターフェイスを終了します。

バックアップ ステータスに関するアラートの受信

バックアップの完了時に問題を通知するアラートを受信するには、タイプが [システム（System）] で重大度が [情報（Info）] のアラートを送信するようにアプライアンスを設定します。アラートの管理（14-34 ページ）を参照してください。

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

- バックアップの制約事項および要件（14-9 ページ）の項目に対処します。

（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　ソース アプライアンスのコマンドライン インターフェイスに、管理者としてログインします。

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　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。

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、`Schedule a single backup` に **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. 繰り返しバックアップ スケジュールを設定するため、**1** を入力して Enter を押します。

b. 定期バックアップの頻度を選択し、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（14-14 ページ）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

- バックアップの制約事項および要件（14-9 ページ）のすべての要件を満たします。

（注）　ターゲット マシンでバックアップが実行中の場合、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　ソース アプライアンスのコマンドライン インターフェイスに、管理者としてログインします。

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　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。

ステップ 9　単一バックアップをすぐに開始するため、**3** を入力して 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されます。

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（14-14 ページ）も参照してください。

バックアップ ステータスの確認

ステップ 1　プライマリ アプライアンスのコマンドライン インターフェイスに、管理者としてログインします。

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。

ステータスの確認対象	操作内容
スケジュール設定されたバックアップ	`View` 操作を選択します。
進行中のバックアップ	`Status` 操作を選択します。 アラートを設定している場合は、電子メールを確認するか、最新アラートの表示（14-35 ページ）を参照してください。

関連項目

- ログ ファイルのバックアップ情報（14-14 ページ）

ログ ファイルのバックアップ情報

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。

関連項目

- バックアップ ステータスの確認（14-13 ページ）

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（14-47 ページ）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。
- Configuration Master の設定に使用した、Web セキュリティ アプライアンスのコンフィギュレーション ファイルをすべて保存します。
- 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（15-22 ページ）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（15-24 ページ）を参照してください。

バックアップ アプライアンスのプライマリ アプライアンスとしての使用

アプライアンス ハードウェアをアップグレードする場合、またはその他の理由でアプライアンスを切り替える場合は、次の手順を使用します。

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（14-8 ページ）の情報を確認してください。

手順

ステップ 1　旧/プライマリ/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、新しい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（14-47 ページ）を参照してください。

ステップ 2　新規/バックアップ/ターゲット 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 3　バックアップの制約事項および要件（14-9 ページ）の要件を満たします。

ステップ 4　旧/プライマリ/ソース アプライアンスからバックアップを実行します。即時バックアップの開始（14-13 ページ）の手順を参照してください。

ステップ 5　バックアップが完了するまで待ちます。

ステップ 6　旧/プライマリ/ソース アプライアンスで `suspendtransfers` および `suspend` コマンドを実行します。

ステップ 7　2 番目のバックアップを実行して、旧/プライマリ/ソース アプライアンスから新規/バックアップ/ターゲット アプライアンスに直前のデータを転送します。

ステップ 8　コンフィギュレーション ファイルを新規/バックアップ/ターゲット アプライアンスにインポートします。

ステップ 9　新規/バックアップ/ターゲット アプライアンスで `resumetransfers` および `resume` コマンドを実行します。

旧/元プライマリ/ソース アプライアンスでこのコマンドを実行しないでください。

ステップ 10　新規/バックアップ/ターゲット アプライアンスと管理対象の電子メールおよび Web セキュリティ アプライアンスの間の接続を確立します。

a. [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。
b. アプライアンス名をクリックします。
c. [接続の確立（Establish Connection）] ボタンをクリックします。
d. [接続のテスト（Test Connection）] をクリックします。
e. アプライアンスのリストに戻ります。
f. 管理対象の各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 11　新規/ターゲット アプライアンスがプライマリ アプライアンスとして機能していることを確認します。

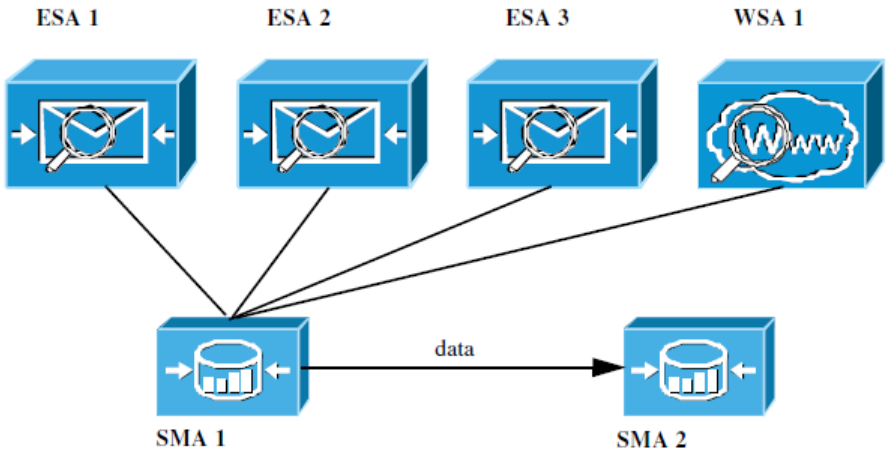
[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [システムステータス（System Status）] を選択し、データ転送のステータスを確認します。

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（14-8 ページ）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。

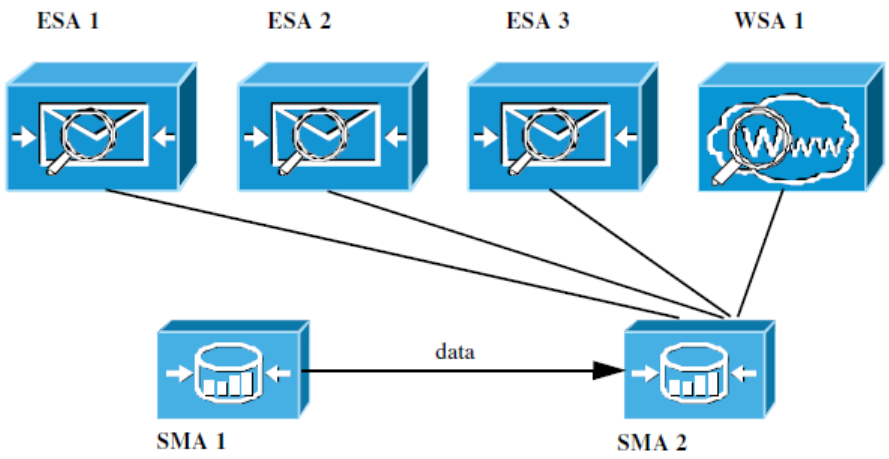
SMA 2 を新しいプライマリ セキュリティ管理アプライアンスとして設定し、サービスを復元するには、次の手順を実行します。

手順	操作内容	詳細情報
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（14-48 ページ）を参照してください。

手順	操作内容	詳細情報
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（A-2 ページ）を参照してください。
ステップ 4	変更を送信し、保存します。	—
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有効にします。	セキュリティ管理アプライアンスでのサービスの設定（2-14 ページ）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有効となり、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（2-12 ページ）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で隔離の移行を設定し、その後該当する各電子メール セキュリティ アプライアンスで移行を有効にして設定します。	一元化されたポリシー、ウイルス、アウトブレイク隔離（8-3 ページ）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（14-14 ページ）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

バックアップ アプライアンスのプライマリ アプライアンスとしての使用（14-14 ページ）を参照してください。

AsyncOS のアップグレード

アップグレード用のバッチ 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、AsyncOS for Email の CLI リファレンス ガイド（http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-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

シスコ コンテンツ セキュリティ アプライアンスのアップデート サーバは、ダイナミック IP アドレスを使用します。ファイアウォール ポリシーを厳しく設定している場合、AsyncOS アップグレードに対して静的な参照先を設定する必要がある場合があります。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の選択：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。

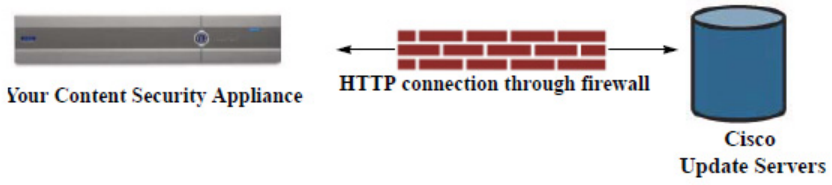
- ストリーミング アップグレード：各アプライアンスはシスコ コンテンツ セキュリティ アップグレード サーバから HTTP を介して AsyncOS アップグレードを直接ダウンロードします。
- リモート アップグレード：シスコからアップグレード イメージを 1 回だけダウンロードし、アプライアンスに保存します。次に、アプライアンスは、ネットワーク内のサーバから AsyncOS アップグレードをダウンロードします。

アップグレードおよびサービス アップデートの設定（14-22 ページ）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 の **updateconfig** コマンドを使用することもできます。

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、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シスコ コンテンツ セキュリティ アップデート サーバに接続し、アップグレードを検索してダウンロードします。

図 14-3　　ストリーミング アップデートの方法

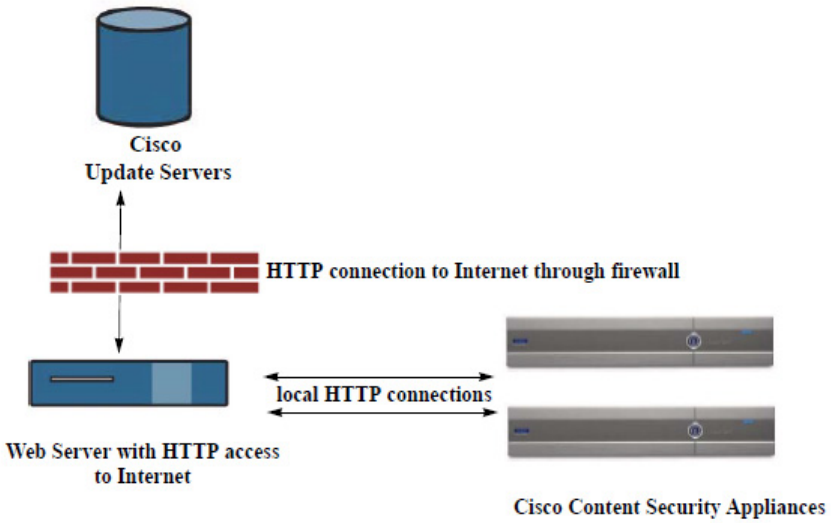


この方式では、アプライアンスがシスコ コンテンツ セキュリティ アップデート サーバにネットワークから直接接続する必要があります。

リモート アップグレードの概要

また、Cisco 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する（リモート アップグレード）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 14-4　　リモート アップデートの方法



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（14-21 ページ）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（14-21 ページ）の情報をお読みください。

ステップ 2　アップグレード ファイルを取得および供給するようにローカル サーバを設定します。

ステップ 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（14-18 ページ）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 ファイルの*ダウンロード*では、次の要件を備えた内部ネットワークにシステムを構築する必要があります。

- シスコ コンテンツ セキュリティ アプライアンスのアップデート 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 ファイルの*ホスティング*では、次の要件を備えた内部ネットワークにサーバを構築する必要があります。

- 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 文字を超えるディレクトリまたはファイル名の表示をサポートしていること
  - ディレクトリの参照ができること
  - 匿名認証（認証不要）または基本（「シンプル」）認証用に設定されていること
  - 各 AsyncOS アップデート イメージ用に最低 350 MB 以上の空きディスク領域が存在すること

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。この場合でも、シスコ コンテンツ セキュリティ アプライアンスはシスコ 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 ベースの記事（TechNotes）（E-3 ページ）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、イメージを利用できる場所にシスコ サーバまたはローカル サーバのどちらから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を選択したり、アップデート間隔を設定したり、自動アップデートを無効にしたりすることができます。

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。

アップグレード通知を設定することもできます。

アップグレードと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))	シスコ サーバまたはローカル Web サーバのどちらから、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を選択します。デフォルトでは、アップグレードおよびアップデートの両方でシスコ サーバが選択されます。 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(14-24 ページ)を参照してください。 • 適宜、アプライアンスに 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 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の選択:リモートまたはストリーミング(14-19 ページ)およびリモート アップグレードの概要(14-20 ページ)を参照してください。
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、シスコ サーバとローカル 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。 アップグレードおよびアップデートの両方で、デフォルトはシスコ 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(14-24 ページ)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の選択:リモートまたはストリーミング(14-19 ページ)およびリモート アップグレードの概要(14-20 ページ)を参照してください。
自動更新(Automatic Updates)	時間帯ルールの自動更新を有効にするかどうかを選択します。有効にする場合は、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。

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
インターフェイス（Interface）	時間帯ルールおよび AsyncOS アップグレードをアップデート サーバに問い合わせるときに使用するネットワーク インターフェイスを選択します。利用可能なプロキシ データ インターフェイスが表示されます。デフォルトでは、アプライアンスは使用するインターフェイスを選択します。
HTTP プロキシ サーバ（HTTP Proxy Server）	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。 このプロキシ サーバは、クラウドからファイル分析レポートの詳細を取得するためにも使用されます。ファイル分析レポートの詳細の要件（5-25 ページ）（Web レポート）、またはファイル分析レポートの詳細の要件（4-31 ページ）（電子メール レポート）も参照してください。
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。 このプロキシ サーバは、クラウドからファイル分析レポートの詳細を取得するためにも使用されます。ファイル分析レポートの詳細の要件（5-25 ページ）（Web レポート）、またはファイル分析レポートの詳細の要件（4-31 ページ）（電子メール レポート）も参照してください。

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 14-5　[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

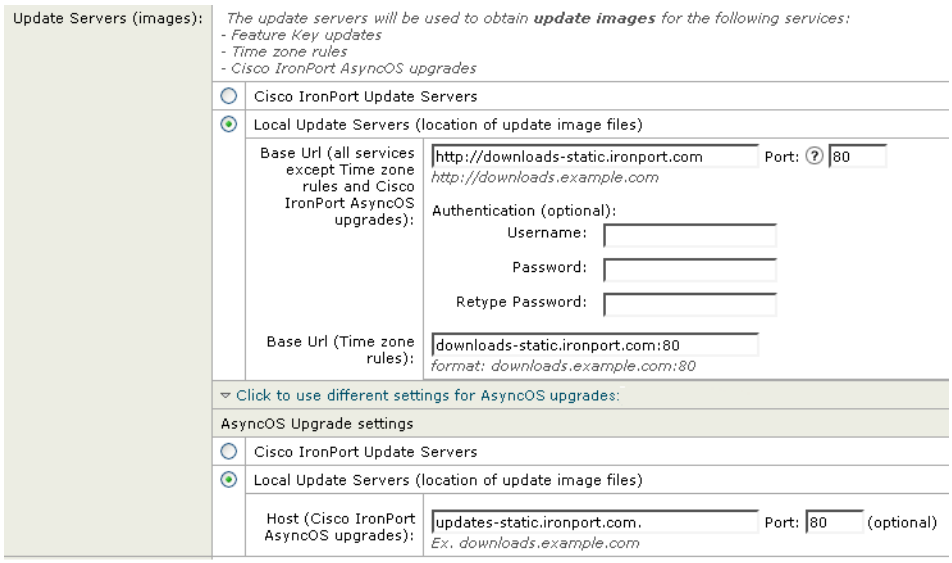


図 14-6　[アップデート サーバ(リスト)(Update Servers (list))] 設定のスタティック URL

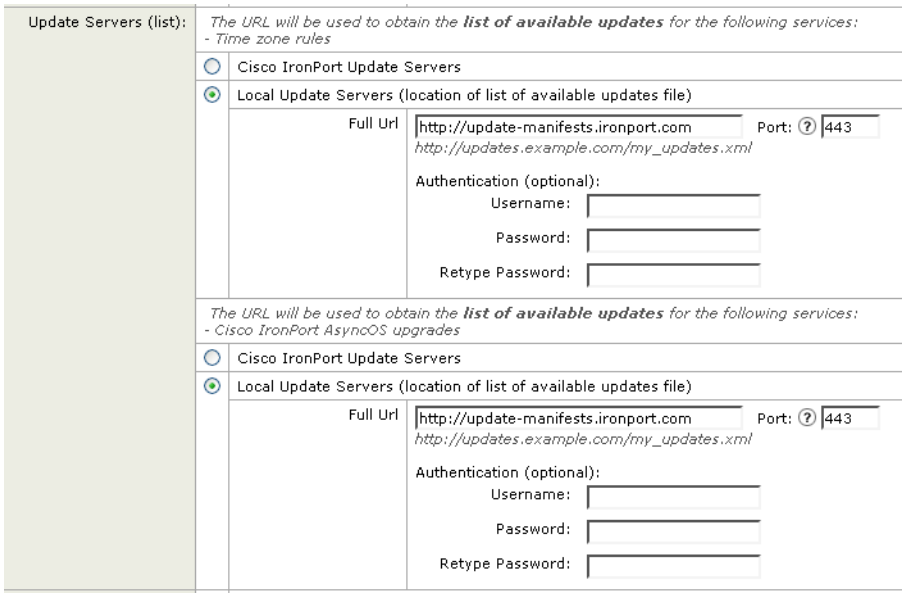


表 14-2　厳格なファイアウォール ポリシーを適用している環境のスタティック アドレス

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)）	ベースURL（タイムゾーンルールおよびAsyncOSアップグレード以外のすべてのサービス）（Base URL (all services except Time zone rules and AsyncOS upgrades)）	http://downloads-static.ironport.com 204.15.82.8 Port 80
	ベースURL（タイムゾーンルール）（Base URL (Time zone rules)）	downloads-static.ironport.com 204.15.82.8 Port 80
	ホスト（AsyncOSアップグレード）（Host (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):）	物理ハードウェア アプライアンスでのアップデート用: フルURL（Full URL）	update-manifests.ironport.com 208.90.58.5 Port 443
	仮想アプライアンスでのアップデート用: フルURL（Full URL）	update-manifests.sco.cisco.com Port 443
	アップグレード用:フルURL（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　[更新設定を編集（Edit Update Settings）] をクリックします。

アップグレードとアップデートの設定（14-23 ページ） 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。

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。

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。

アップグレードの通知

デフォルトでは、AsyncOS アップグレードがアプライアンスで使用可能な場合、管理者および技術者の権限を持つユーザには、Web インターフェイスの上部に通知が表示されます。

目的	操作内容
最新のアップグレードの詳細情報を表示する	アップグレード通知にカーソルを合わせます。
使用できるすべてのアップグレードのリストを表示する	通知の下向き矢印をクリックします。
現在の通知を閉じる 新しいアップグレードが入手可能になるまで、アプライアンスは別の通知を表示しません。	下向き矢印をクリックして [通知を消去（Clear the notification）] を選択してから、[閉じる（Close）] をクリックします。
今後の通知を中止する（管理者権限を持つユーザのみ）	[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）] に移動します。

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（14-19 ページ）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（14-55 ページ）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（14-48 ページ）で説明する警告を参照してください。

何らかの理由でアップグレード前のリリースに戻す場合は、このファイルが必要です。

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。

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 からのアップグレードを実行する場合は、リスナーの停止が自動的に実行されます。

ステップ 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（14-22 ページ）を参照してください。

AsyncOS のアップグレード

1 回の操作でダウンロードとインストールを行うか、またはバックグラウンドでダウンロードして後でインストールできます。

（注）　シスコ サーバからではなくローカル サーバから 1 回の操作で AsyncOS をダウンロードおよびアップグレードすると、*ダウンロード中*に即座にアップグレードが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

- シスコから直接アップグレードをダウンロードするか、またはネットワーク上のサーバからアップグレード イメージをホストするかを選択します。次に、選択した方式をサポートするようにネットワークをセット アップします。そして、選択した入手先からアップグレードを入手するためにアプライアンスを設定します。アップグレード方式の選択：リモートまたはストリーミング（14-19 ページ）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（14-22 ページ）を参照してください。
- アップグレードをインストールする前に、アップグレードする前に：重要な手順（14-27 ページ）の手順を実行してください。

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）] > [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
1 回の操作でアップグレードのダウンロードとインストールを実行する	[ダウンロードしてインストール（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たことがある場合、既存のダウンロードを上書きするよう求められます。
アップグレード インストーラをダウンロードします。	[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たことがある場合、既存のダウンロードを上書きするよう求められます。 インストーラはサービスを中断することなく、バックグラウンドでダウンロードします。
ダウンロードしたアップグレード インストーラのインストール	[Install（インストール）] 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ている場合にのみ表示されます。 インストールする AsyncOS のバージョンは、[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　インストール中の場合、次に従います。

a. 現在の設定をアプライアンス上の `configuration` ディレクトリに保存するかどうかを選択します。

b. 設定ファイルでパスワードをマスクするかどうかを選択します。

（注）　マスクされたパスワードが記載された設定ファイルは、GUI の [設定ファイル（Configuration File）] ページや CLI の `loadconfig` コマンドからロードできません。

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] をクリックします。

ステップ 7　インストール中の場合、次に従います。

a. プロセス中のプロンプトに答える準備をしてください。

応答するまでプロセスは中断されます。

ページの上部の近くに、経過表示バーが表示されます。

b. プロンプトで、[今すぐ再起動（Reboot Now）] をクリックします。

（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切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てログインします。

次の作業

- プロセスが中断された場合、プロセスを再開する必要があります。
- アップグレードをダウンロードしてインストールしなかった場合は次のとおりです。

  アップグレードをインストールする準備ができたら、「始める前に」の項の前提条件も含め次の手順を最初から実行しますが、[インストール（Install）] オプションを選択します。
- 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（14-30 ページ）を参照してください。

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 ステータスの表示	ページの真ん中を確認してください。 進行中のダウンロードおよびダウンロードが完了してインストールされるのを待っているものがない場合は、ダウンロードのステータス情報は表示されません。 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。
ダウンロードのキャンセル	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、ダウンロード進行中にのみ表示されます。
ダウンロードされたインストーラの削除	ページの中央にある、[ファイルを削除（Delete 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ている場合にのみ表示されます。

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）リスナーを再度有効にします。
- （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。中央集中型で Webセキュリティ アプライアンスを管理する Configuration Master の設定（9-2 ページ）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（14-47 ページ）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。

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。

復元の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既存の設定および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。

復元によってライセンス キーまたは仮想アプライアンス ライセンスの有効期限日に影響が及ぶことはありません。

AsyncOS の復元

はじめる前に

- 保持する必要があるデータをアプライアンス以外の場所にバックアップまたは保存します。
- 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。設定ファイルに下位互換性は*ありません*。
- このコマンドはすべての設定を破壊するため、復元を実行する場合は、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。
- お使いの電子メール セキュリティ アプライアンスで隔離が有効になっている場合は、それらのアプライアンスでローカルに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。設定ファイルに下位互換性はありません。

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。設定ファイルを取得するには、ファイルを電子メールでユーザ自身に送信するか、ファイルを FTP で取得します。簡単に行うには、`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）　このコピーは、バージョンを戻した後にロードする設定ファイルではありません。

ステップ 3　セーフリスト/ブロックリスト機能を使用する場合は、セーフリスト/ブロックリスト データベースを別のマシンにエクスポートします。

ステップ 4　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` コマンドの実行時には、いくつかの警告プロンプトが発行されます。これらの警告プロンプトに同意すると、すぐにバージョンを戻す動作が開始します。このため、復元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 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 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 回再起動するまで待ちます。

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　少なくとも 1 つの Web セキュリティ アプライアンスを追加し、URL カテゴリ アップデートがそのアプライアンスからダウンロードされるまで数分待ちます。

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有効にします。

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（14-22 ページ）を参照してください。

関連項目

- 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（14-33 ページ）
- アップグレードおよびサービス アップデートの設定（14-22 ページ）

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 セットの更新の準備および管理（9-22 ページ）
- URL カテゴリ セットの更新とレポート（5-18 ページ）

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

アプライアンスから、アプライアンスで発生しているイベントに関する電子メール アラートが送信されます。

目的	操作内容
タイプの異なるアラートが別の管理ユーザに送信されるようにする	[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。 システムのセットアップ時に AutoSupport を有効にした場合、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。 複数のアドレスを指定する場合は、カンマで区切ります。
次のようなアラートのグローバル設定を行う • アラート送信者（FROM:）アドレス • 重複したアラートの制御 • AutoSupport 設定	[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。 重複したアラートについて（14-36 ページ）を参照してください Cisco AutoSupport（14-36 ページ）を参照してください
最近のアラートのリストを表示 このリストの設定を管理する	最新アラートの表示（14-35 ページ）を参照してください
アラートのリストと説明を表示する	参照先: ハードウェア アラートの説明（14-36 ページ）。 システム アラートの説明（14-37 ページ）
アラートの配信メカニズムを理解する	アラートの配信（14-35 ページ）を参照してください

アラート タイプおよび重大度

アラート タイプは次のとおりです。

- ハードウェア アラート。ハードウェア アラートの説明（14-36 ページ）を参照してください。
- システム アラート。システム アラートの説明（14-37 ページ）を参照してください。
- アップデータ アラート。

アラートの重大度は次のとおりです。

- 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。
  - 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。
- 展開に電子メール セキュリティ アプライアンスが含まれる場合：
  - 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。

重複したアラートについて

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。[重複するアラート メッセージを送信する前に待機する最大の秒数（Maximum Number of Seconds to Wait Before Sending a Duplicate Alert）] フィールドを使用して、待機間隔の秒数に制限を設けることができます。たとえば、初期値を 5 秒に設定し、最大値を 60 秒に設定すると、アラートは 5 秒後、15 秒後、35 秒後、60 秒後、120 秒後といった間隔で送信されます。

Cisco AutoSupport

十分なサポートと今後のシステム変更の設計を可能にするため、システムで生成されたすべてのアラート メッセージをシスコに送信するようにシスコ 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。「AutoSupport」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、AutoSupport はシステムの稼働時間、**status** コマンドの出力、および使用されている AsyncOS バージョンを通知するレポートを毎週送信します。

デフォルトでは、アラート タイプが System で重大度レベルが Information のアラートを受信するように設定されているアラート受信者は、シスコに送信される各メッセージのコピーを受信します。内部にアラート メッセージを毎週送信しない場合は、この設定を無効にできます。この機能を有効または無効にするには、[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、[設定を編集（Edit Settings）] をクリックします。

AutoSupport が有効の場合、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、デフォルトで毎週 AutoSupport レポートが送信されます。

ハードウェア アラートの説明

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。	警告
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。	警告
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。	クリティカル（Critical）
SYSTEM.RAID_EVENT_ ALERT	重大な RAID-event が発生した場合に送信されます。	警告
SYSTEM.RAID_EVENT_ ALERT_INFO	RAID-event が発生した場合に送信されます。	情報

システム アラートの説明

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。	クリティカル（Critical）
COMMON.KEY_EXPIRED_ALERT	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。	警告
COMMON.KEY_EXPIRING_ALERT	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。	警告
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。	警告
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。	警告
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。	警告
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。	情報
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。	クリティカル（Critical）
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。	クリティカル（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。	情報
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。	情報
COMMON.INVALID_FILTER	無効なフィルタが存在する場合に送信されます。	警告

アラート名	説明	重大度
IPBLOCKD.HOST_ADDED_TO_WHITELIST **IPBLOCKD.HOST_ADDED_TO_BLACKLIST** **IPBLOCKD.HOST_REMOVED_FROM_BLACKLIST**	アラート メッセージ: • <IP address>のホストがSSH DoS攻撃のためブラックリストに追加されました。(The host at <IP address> has been added to the blacklist because of an SSH DOS attack.) • <IP address>のホストがSSHホワイトリストに追加されました。(The host at <IP address> has been permanently added to the ssh whitelist.) • <IP address>のホストがブラックリストから削除されました(The host at <IP address> has been removed from the blacklist) SSH を介してアプライアンスへの接続を試みているが、有効なクレデンシャルを提示しない IP アドレスは、2 分以内に 10 回以上試行に失敗した場合、SSH のブラックリストに追加されます。 同じ IP アドレスからのユーザ ログインが成功した場合、その IP アドレスはホワイトリストに追加されます。 ホワイトリストのアドレスは、ブラックリストにも登録されていてもアクセスが許可されます。	警告
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。	クリティカル (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。	クリティカル (Critical)
LOG.ERROR.*	さまざまなロギング エラー。	クリティカル (Critical)
MAIL.PERRCPT.LDAP_GROUP_QUERY_FAILED	受信者ごとのスキャン中に LDAP グループ クエリーが失敗した場合に送信されます。	クリティカル (Critical)
MAIL.QUEUE.ERROR.*	メール キューのさまざまなハード エラー。	クリティカル (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。	クリティカル (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 リソース節約が有効になった場合に送信されます。	クリティカル (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。	クリティカル (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。	クリティカル (Critical)
MAIL.RES_CON_START_ALERT	アプライアンスが「リソース節約」モードになった場合に送信されます。	クリティカル (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。	クリティカル (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。	クリティカル (Critical)

アラート名	説明	重大度
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。	クリティカル（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。	警告
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。	クリティカル（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。	クリティカル（Critical）
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。	クリティカル（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。	クリティカル（Critical）
REPORTD.AGGREGATION_D ISABLED_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 は集約を無効にし、アラートを送信します。	警告
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。	警告
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。	クリティカル（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。	情報
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。	クリティカル（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。	クリティカル（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。	クリティカル（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。	情報
SMAD.ICCM.ALERT_PUSH_ FAILED	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。	警告
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。	警告
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。	警告
SMTPAUTH.LDAP_QUERY_F AILED	LDAP クエリーが失敗した場合に送信されます。	警告

アラート名	説明	重大度
SYSTEM.HERMES_SHUTDOWN_FAILURE.REBOOT	再起動中のシステムをシャットダウンしている際に問題が発生した場合に送信されます。	警告
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。	警告
SYSTEM.RCPTVALIDATION.UPDATE_FAILED	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。	クリティカル（Critical）
SYSTEM.SERVICE_TUNNEL.DISABLED	シスコ サポート サービス用に作成されたトンネルが無効の場合に送信されます。	情報
SYSTEM.SERVICE_TUNNEL.ENABLED	シスコ サポート サービス用に作成されたトンネルが有効の場合に送信されます。	情報

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（2-8 ページ）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（Password）]

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 サーバのどちらを使用するか、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」を設定する場合は、in-addr.arpa（PTR）エントリも同様に設定する必要があります。このため、たとえば「.eng」クエリーをネームサーバ 1.2.3.4 にリダイレクトする際に、すべての .eng エントリが 172.16 ネットワークにある場合、スプリット DNS 設定に「eng,16.172.in-addr.arpa」を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 14-3　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「ダブル 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（14-41 ページ）で説明されている一般的な DNS タイムアウトには適用されません。

デフォルト値は 20 秒です。秒数に「0」を入力することで、すべてのリスナーに対してグローバルに逆引き DNS ルックアップのタイムアウトを無効にできます。値を 0 秒に設定した場合、逆引き DNS ルックアップは試行されず、代わりに標準のタイムアウト応答がすぐに返されます。

DNS アラート

アプライアンスの再起動時に、まれにメッセージ「DNSキャッシュのブートストラップに失敗しました（Failed to bootstrap the DNS cache）」が付与されたアラートが生成される場合があります。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 [キャッシュを消去（Clear Cache）] ボタン、または `dnsflush` コマンドを使用して、DNS キャッシュのすべての情報をクリアします（`dnsflush` コマンドの詳細については、マニュアル（E-1 ページ）に指定された場所で入手可能な『*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内部 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（14-41 ページ）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（14-44 ページ）
- デフォルト ゲートウェイの変更（GUI）（14-44 ページ）

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。

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。

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）（14-44 ページ）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

（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」セクション（3-2 ページ）を参照してください。

コマンドライン インターフェイスを使用して時間に関連する設定を行うには、`ntpconfig`、`settime`、および `settz` コマンドを使用します。

目的	操作内容
システム時刻を設定する	[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。 ネットワーク タイム プロトコル（NTP）サーバの使用（14-45 ページ）も参照してください。
時間帯を設定する	[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。 関連項目： • GMT オフセットの選択（14-45 ページ） • 時間帯ファイルの更新（14-46 ページ）

ネットワーク タイム プロトコル（NTP）サーバの使用

ネットワーク タイム プロトコル（NTP）サーバを使用して、セキュリティ管理アプライアンス システム クロックをネットワークまたはインターネット上の他のコンピュータと同期できます。

デフォルトの NTP サーバは `time.sco.cisco.com` です。

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

関連項目

- システム時刻の設定（14-45 ページ）

GMT オフセットの選択

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　[設定の編集（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。

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。

時間帯ファイルの更新

いずれかの国の時間帯ルールに変更があった場合は必ず、アプライアンス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（14-46 ページ）
- 時間帯ファイルの手動更新（14-46 ページ）

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　変更を送信し、保存します。

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。

[設定ファイル（Configuration File）] ページ

次のセクションの詳細について	参照先
現在の設定の保存	コンフィギュレーション設定の保存とインポート（14-47 ページ）
保存されている設定のロード	コンフィギュレーション設定の保存とインポート（14-47 ページ）
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）	セーフリスト/ブロックリストのバックアップと復元（7-14 ページ）
設定のリセット	出荷時の初期状態への設定のリセット

コンフィギュレーション設定の保存とインポート

（注）　ここで説明す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を設定するために使用します。第 9 章「Web セキュリティ アプライアンスの管理」で説明し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 アプライアンスを設定するために使用します。

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。

このファイルは次の複数の方法で使用できます。

- 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。
- 設定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を間違えた場合、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。
- 既存の設定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簡単に確認できます（新しいブラウザの多くに、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）。現在の設定にマイナー エラー（誤植など）があった場合、この機能がトラブルシューティングに役立つことがあります。
- 既存の設定ファイルをダウンロードし、変更を行い、そのファイルを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 設定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 設定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）。
- コンフィギュレーション ファイルを使用して、別のアプライアンス（クローン作成された仮想アプライアンスなど）を迅速に設定できます。

コンフィギュレーション ファイルの管理

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。

パスワードがマスクされた設定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。設定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、設定ファイルを検証できます。

いずれのインポート方法でも、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（上記の宣言タグを含み、`<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。

注意　設定ファイルまたは設定ファイルのサブセクションをアップロードまたは解析する場合は、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

設定ファイルのセクションをアップロードまたは解析する場合は注意が必要です。タグを含めないと、設定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>
```

注意　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。管理ポートで別のプロトコル、シリアル インターフェイス、または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無効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設定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（14-5 ページ）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、データ損失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（14-5 ページ）を参照）

- publishconfig
- backupconfig（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（14-8 ページ）を参照）

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（14-50 ページ）を参照してください。

（注）　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に、パスワードを含めることを選択すると（「Do you want to include passwords?」に「yes」と回答した場合）、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ない PEM 形式で含められます。

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: 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 形式の設定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（14-48 ページ）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（14-50 ページ）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　設定ファイル全体または設定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設定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、新しい設定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+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（詳細については、システム セットアップ ウィザードの実行（2-8 ページ）を参照してください）。最後に、変更を確定します。

```
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
```

ディスク領域の管理

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。

（仮想アプライアンスのみ）使用可能なディスク領域の拡大

ESXi 5.5 および VMFS 5 を実行する仮想アプライアンスの場合、2 TB を超えるディスク領域を割り当てることができます。ESXi 5.1 を実行するアプライアンスの場合は 2 TB に制限されます。

（注）　ESXi でのディスク領域の削減はサポートされません。詳細については、VMware のマニュアルを参照してください。

仮想アプライアンス インスタンスにディスク領域を追加するには、次の手順を実行します。

はじめる前に

必要な追加ディスク領域を慎重に検討します。

手順

ステップ 1　Cisco コンテンツ セキュリティ管理アプライアンス インスタンスを停止します。

ステップ 2　VMware が提供するユーティリティまたは管理ツールを使用してディスク領域を増やします。

VMware のマニュアルで仮想ディスク設定の変更に関する情報を参照してください。

ESXi 5.5 の情報は http://pubs.vmware.com/vsphere-55/index.jsp?topic=%2Fcom.vmware.vsphere.hostclient.doc%2FGUID-81629CAB-72FA-42F0-9F86-F8FD0DE39E57.html で入手できます。

ステップ 3　[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）] に移動して、変更が反映されていることを確認します。

ディスク クォータおよび使用状況の表示

目的	操作内容
セキュリティ管理アプライアンスのモニタリング サービスごとに、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量を表示する	[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	[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、[集約管理サービス（Centralized Services）] セクションで確認します。

最大ディスク領域と割り当て

表 14-4　使用可能な最大ディスク領域（GB 単位）（ハードウェア）

	ハードウェア モデル							
	M160	M170	M380	M660	M670	M680	M1060	M1070
すべてのデータ タイプに対して使用可能な合計	165	165	968	681	681	1805	1039	1407

- 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有効にすると、すべての領域が有効にした機能専用になります。両方を有効にした場合、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 レポーティングを有効にしているが、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。
- その他のクォータを現在の使用量より少なくする前に、不要なデータを削除する必要があります。その他のクォータのディスク領域の管理（14-55 ページ）を参照してください。
- ポリシー、ウイルス、およびアウトブレイク隔離のディスク領域を管理する方法については、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（8-10 ページ）および隔離内のメッセージの保存期間（8-10 ページ）を参照してください。
- 他のすべてのデータ タイプでは、既存の割り当て量を現在の使用量より少なくした場合、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。

ディスク領域に関するアラートの受信の確認

その他のディスク使用量がクォータの 75% に達すると、警告レベルのシステム アラートを受信します。これらのアラートを受信した場合は、対処する必要があります。

確実にアラートが届くようにするには、アラートの管理（14-34 ページ）を参照してください。

その他のクォータのディスク領域の管理

その他のクォータにはシステム データとユーザ データが含まれます。システム データは削除できません。管理できるユーザ データには次のファイル タイプがあります。

管理対象	操作内容
ログ ファイル	[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ログサブスクリプション（Log Subscriptions）] に移動して、以下を実行します。 • [サイズ（Size）] カラム見出しをクリックして、最も多くのディスク領域を消費しているログを確認します。 • 生成されるすべてのログ サブスクリプションが必要であることを確認します。 • 必要以上に詳細なログ レベルになっていないかを確認します。 • 可能な場合は、ロールオーバー ファイル サイズを小さくします。
パケット キャプチャ	[ヘルプとサポート（Help and Support）]（画面上部の右側付近）> [パケットキャプチャ（Packet Capture）] に移動します。不要なキャプチャを削除します。
コンフィギュレーション ファイル （これらのファイルが多くのディスク領域を消費する可能性は低いと考えられます）。	アプライアンスの `/data/pub` ディレクトリに FTP でアクセスします。 アプライアンスへの FTP アクセスを設定するには、FTP 経由でのアプライアンスへのアクセス（A-3 ページ）を参照してください。

ディスク領域量の再割り当て

使用しない機能にディスク領域が割り当てられている場合、またはアプライアンスで特定の機能のディスク領域が頻繁に不足し、その他の機能に余分な領域がある場合は、ディスク領域を再割り当てすることができます。

すべての機能にさらに領域が必要な場合は、ハードウェアのアップグレード、または仮想アプライアンスへの追加ディスク領域の割り当てを検討してください。（仮想アプライアンスのみ）使用可能なディスク領域の拡大（14-54 ページ）を参照してください。

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（14-55 ページ）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のみ）よく利用するページのクイック アクセス 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する	追加するページに移動し、ウィンドウの右上部付近にある [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。 お気に入りへの変更は確定操作は必要ありません。
お気に入りの順序を変更する	[お気に入り（My Favorites）] > [お気に入りをすべて表示（View All My Favorites）] を選択し、適切な順序にお気に入りをドラッグします。
お気に入りページ、名前、または説明を編集する	[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、編集するお気に入りの名前をクリックします。
お気に入りを削除する	[お気に入り（My Favorites）] > [お気に入りをすべて表示（View All My Favorites）] を選択し、お気に入りを削除します。
お気に入りページに移動する	ウィンドウの右上部付近にある [お気に入り（My Favorites）] からページを選択します。
カスタム レポート ページを表示または作成する	カスタム レポート（3-7 ページ）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 ページに使用できる時間範囲のサブセットです）
- 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。

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、通常の動作が記録されます。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）、コンプライアンス アーカイブ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 GUI 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、Cisco 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、スパム隔離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。このデータは ESA からプッシュされます。

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、GUI でログ 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（File size）

- 時刻（Time）
  - 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 時間半などの複合間隔を入力するには、例の 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。たとえば午後 11 時は 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

デフォルトで有効になるログ

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	スパム隔離ログ	FTP ポーリング
euqgui_logs	スパム隔離 GUI 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
gui_logs	HTTP ログ	FTP ポーリング
mail_logs	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
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（15-23 ページ）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（15-22 ページ）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（15-22 ページ）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 ログにはバックアップ プロセスが開始から終了まで記録されます。 バックアップ スケジューリングに関する情報は、SMA ログに含まれます。
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有効になっている 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有効になっている 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 GUI 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（6-1 ページ）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
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（14-45 ページ）を参照してください。
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るレポーティング 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。中央集中型レポーティング、中央集中型トラッキング、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	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、スパム隔離 GUI に関連付けられたアクションが記録されます。
スパム隔離ログ	スパム隔離ログには、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

						次の文字列を含む					
	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。ユーザが変更を保存するたびに、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。

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: 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。

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。

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。

例

次の HTTP ログの例は、admin ユーザによる GUI 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
```

スパム隔離ログの使用

表 15-8 に、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　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。

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
```

スパム隔離 GUI ログの使用

表 15-9 に、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　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。

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　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
```

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（6-1 ページ）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	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、1 つのメッセージも数千のメッセージも送信できます。
DCID	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 接続 ID。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、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。

テキスト メール ログのサンプル

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、番号は*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。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）

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するときのプロンプトは次のとおりです。

```
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
```

添付ファイルを含むメッセージ

この例では、添付ファイル名の識別を有効にするように、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。

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、スパムとしてタグが付けられたメッセージが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 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。

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 7:36:39 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 8:44:59 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。

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。

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。

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。

例

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 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。

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。

表 15-19　ステータス ログの統計情報（続き）

統計	説明
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	グローバルでの配信停止のヒット数。
ActvRcp	アクティブ受信者。
UnatmptRcp	未試行受信者。
AtmptRcp	試行受信者。
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	ワーク 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集計されます）。
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。

表 15-19　ステータス ログの統計情報（続き）

統計	説明
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量。
EuQ	スパム隔離内のメッセージ数。
EuqRls	スパム隔離解放キュー内のメッセージ数。

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。

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: XXXXXXXXXXX-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

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 アプライアンスに保存されるか、リモートで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
ログ タイプ（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（15-5 ページ）を参照してください。
名前（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。
ログファイル名（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。
ファイルサイズ別ロールオーバー（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。
時刻によりロールオーバー（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（15-2 ページ）のオプションを参照してください。

表 15-21　ログ ファイルの属性（続き）

属性	説明
ログ レベル（Log Level）	各ログ サブスクリプションの詳細レベル。
取得方法（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 サブスクリプション（Log Subscriptions）] ページ（または CLI の `logconfig` コマンド）を使用して、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（15-5 ページ）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*の選択も要求されます。

（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）] > [ログサブスクリプション（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
クリティカル（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。
警告（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。
情報（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。

表 15-22　ログ レベル（続き）

ログ レベル	説明
デバッグ（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。
トレース（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 サブスクリプション（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（15-2 ページ）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　[ログサブスクリプション（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。

ロギングのグローバル設定

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。[ログサブスクリプション（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。

- システムがメトリックを記録する間隔（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
- 元のメッセージの件名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

シスコ コンテンツ セキュリティ アプライアンスのすべてのログには、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 カンバセーション配信時の 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）]: このオプションを有効にすると、各メッセージの元の件名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た場合、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 [ログサブスクリプション（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 メトリックの頻度、メール ログにメッセージ ID ヘッダーを記録するかどうか、リモート応答を記録するかどうか、および各メッセージの元の件名ヘッダーを記録す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、ロギングのグローバル設定（15-25 ページ）を参照してください。

ステップ 3 ログに記録するその他のヘッダーを入力します。各エントリを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 はログ ファイルのロールオーバー時に次を実行します。

- ロールオーバーのタイムスタンプで新規ログ ファイルを作成し、文字「`c`」の拡張子によって現在のファイルとして指定します。

- 現在のログ ファイルの名前を、保存済みを示す文字「s」の拡張子付きに変更します。
- 新たに保存されたログ ファイルをリモート ホストに転送します（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 ファイルを転送します（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を削除します（ポーリングベースの場合）。

関連項目

- ログ サブスクリプション内のログのロールオーバー（15-27 ページ）
- GUI を使用したログの即時ロールオーバー（15-27 ページ）
- CLI を使用したログの即時ロールオーバー（15-27 ページ）

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（15-2 ページ）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	[ログサブスクリプション（Log Subscriptions）] ページで、ロールオーバーするログ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 を使用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。

GUI での最新のログ エントリの表示

GUI を使用してログ ファイルを表示するには、[ログサブスクリプション（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。GUI でログを表示するには、管理インターフェイスで FTP サービスを有効にしておく必要があります。

最新のログ エントリの表示（tail コマンド）

AsyncOS 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 コマンドを実行して現在設定されているログの番号を選択すると、そのログが表示されます。tail コマンドを終了するには、Ctrl+C を押します。

（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

次の例では、tail コマンドを使用してシステム ログを表示します。tail コマンドでは、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 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: " Spam Quarantine Logs" Retrieval: FTP Poll
3. "euqgui_logs" Type: "Spam Quarantine GUI Logs" Retrieval: FTP Poll
4. "gui_logs" Type: "HTTP Logs" Retrieval: FTP Poll
5. "mail_logs" Type: "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
新規作成（New）	新しいキーを追加します。
編集（Edit）	既存のキーを変更します。
削除（Delete）	既存のキーを削除します。
スキャン（Scan）	ホスト キーを自動的にダウンロードします。
印刷（Print）	キーを表示します。
ホスト（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。
フィンガープリント（Fingerprint）	システム ホスト キーのフィンガープリントを表示します。
ユーザ（User）	リモート マシンにログをプッシュするシステム アカウントの公開キーを表示します。これは、SCP プッシュ サブスクリプションを設定するときに表示されるキーと同じです。これは、リモート システムの「authorized_keys」ファイルに配置される値です。

例

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。

機能の設定に関する問題のトラブルシューティング

機能を設定できない問題が発生した場合は、各機能で実行する必要があるタスクの概要を参照してください。概要には、それぞれの具体的な情報へのリンクが記載されています。

- 中央集中型 Web レポーティングおよびトラッキングの設定（5-3 ページ）
- 中央集中型電子メール レポーティングの設定（4-2 ページ）
- 中央集中型メッセージ トラッキングの設定（6-2 ページ）
- 中央集中型スパム隔離の設定（7-2 ページ）
- 一元化されたポリシー、ウイルス、アウトブレイク隔離（8-3 ページ）
- 中央集中型で Webセキュリティ アプライアンスを管理する Configuration Master の設定（9-2 ページ）

一般的なトラブルシューティング リソース

一般的なトラブルシューティング リソースは次のとおりです。

- 最新アラート。最新アラートの表示（14-35 ページ）を参照してください。
- ログ ファイル。第 15 章「ロギング」を参照してください
- 「マニュアルの更新」セクションを含むリリース ノート。マニュアル（E-1 ページ）を参照してください。
- Cisco Bug Search Tool（アクセスの手順はリリース ノートを参照してください）
- ナレッジ ベースの記事（TechNotes）（E-3 ページ）
- シスコ サポート コミュニティ（E-3 ページ）

管理対象アプライアンスのパフォーマンスに関する問題のトラブルシューティング

パフォーマンスに関する問題が発生した場合にシステムが最もリソースを使用している部分を特定するため、すべての管理対象アプライアンス（電子メールまたは Web セキュリティ）と、各管理対象アプライアンスのシステム キャパシティ レポートを参照できます。電子メール セキュリティ アプライアンスについては、[システム容量（System Capacity）] ページ（4-37 ページ）を参照してください。Web セキュリティ アプライアンスについては、[システム容量（System Capacity）] ページ（5-35 ページ）を参照してください。

特定の機能で発生する問題のトラブルシューティング

機能の設定に関する問題のトラブルシューティング（16-1 ページ）も参照してください。

Web セキュリティ関連の問題

- すべてのレポートのトラブルシューティング（3-13 ページ）
- Web レポーティングおよびトラッキングのトラブルシューティング（5-52 ページ）
- コンフィギュレーション管理上の問題のトラブルシューティング（9-24 ページ）
- Web セキュリティ アプライアンスの設定が原因で機能関連の問題が発生する場合もあります。マニュアル（E-1 ページ）に示された場所でお使いのリリースのリリース ノートおよびオンライン ヘルプまたはユーザ ガイドを参照してください。

電子メール セキュリティ関連の問題

- すべてのレポートのトラブルシューティング（3-13 ページ）
- 電子メール レポートのトラブルシューティング（4-50 ページ）
- メッセージ トラッキングのトラブルシューティング（6-11 ページ）
- スパム隔離機能のトラブルシューティング（7-26 ページ）
- 集約ポリシー隔離のトラブルシューティング（8-25 ページ）
- 電子メール セキュリティ アプライアンスの設定が原因で機能関連の問題が発生する場合もあります。マニュアル（E-1 ページ）に示された場所でお使いのリリースのリリース ノートおよびオンライン ヘルプまたはユーザ ガイドを参照してください。

一般的な問題

- アップグレードを最近実行し、オンライン ヘルプの表示が古い場合や、新しい機能に関する情報が見つからない場合は、ブラウザのキャッシュをクリアしてからブラウザ ウィンドウを再度開きます。
- 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いる場合、Web インターフェイスを使用して設定を行うと、予期しない動作が発生することがあります。
- 管理ユーザ アクセスのトラブルシューティング（13-28 ページ）。

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

この方法を使用して Cisco TAC または独自のサポート サービスに連絡することができます。

はじめる前に

Cisco TAC に連絡する場合：

- 緊急の問題の場合、この方法は使用しないでください。この場合は、カスタマー サポート（E-4 ページ）に記載されているその他の方法のいずれかを使用してサポートに連絡してください。
- ヘルプに関しては別の選択肢を検討してみてください。
  - ナレッジ ベースの記事（TechNotes）（E-3 ページ）
  - シスコ サポート コミュニティ（E-3 ページ）
- この手順を使用してサポート事例を開くと、アプライアンスの設定ファイルがシスコ 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たくない場合、別の方法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。
- アプライアンスがインターネットに接続され電子メールを送信できる必要があります。
- 既存の事例に関する情報を送信する場合は、ケース番号を確認してください。

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設定します。

要求を Cisco TAC に送信する	[Ciscoテクニカルサポート（Cisco Technical Support）] チェックボックスをオンにします。
内部サポート デスクにだけ要求を送信する	• [Ciscoテクニカルサポート（Cisco Technical Support）] チェックボックスをオフにします。 • 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。

仮想アプライアンスのサポートの取得

Cisco Content Security 仮想アプライアンスのサポート ケースを報告する場合は、契約番号と製品 ID コード（PID）を提供する必要があります。

発注書を参照するか次の表を使用すると、仮想アプライアンスで動作中のソフトウェア ライセンスに基づく PID を特定できます。

機能	PID	説明
すべての中央集中型 Web セキュリティ機能	SMA-WMGT-LIC=	—
すべての中央集中型電子メール セキュリティ機能	SMA-EMGT-LIC=	

シスコのテクニカル サポート担当者のリモート アクセスの有効化

シスコのカスタマー アシスタンスのみ、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されたアプライアンスへのリモート アクセスのイネーブル化（16-4 ページ）
- インターネットに直接接続されていないアプライアンスへのリモート アクセスのイネーブル化（16-5 ページ）
- テクニカル サポートのトンネルのディセーブル化（16-6 ページ）
- リモート アクセスの無効化（16-6 ページ）
- サポートの接続状態の確認（16-6 ページ）

インターネット接続されたアプライアンスへのリモート アクセスのイネーブル化

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。デフォルトでは、ポート 25 です。このポートは大部分の環境で機能します。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 ウィンドウの右上にある、[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。

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ディセーブル化（16-6 ページ）を参照してください。

インターネットに直接接続されていないアプライアンスへのリモート アクセスのイネーブル化

インターネットに直接接続されていないアプライアンスの場合、インターネットに接続されている第 2 のアプライアンスを介してアクセスされます。

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第 2 のアプライアンスにポート 22 で接続する必要があります。
- インターネットに接続されているアプライアンスで該当のアプライアンスへのサポート トンネルを作成するには、インターネット接続されたアプライアンスへのリモート アクセスのイネーブル化（16-4 ページ）の手順を実行します。

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` と入力します。

ステップ 3　プロンプトに従います。

次の作業

サポート担当者のリモート アクセスが不要になった場合は、次を参照してください。

- リモート アクセスの無効化（16-6 ページ）
- テクニカル サポートのトンネルのディセーブル化（16-6 ページ）

テクニカル サポートのトンネルのディセーブル化

イネーブルにした techsupport トンネルは、upgrades.ironport.com に 7 日間接続されたままになります。その後、確立された接続は切断されませんが、いったん切断されるとトンネルに再接続できません。

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 ウィンドウの右上にある、[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　[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 と入力します。

ステップ 3　disable と入力します。

サポートの接続状態の確認

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 と入力します。

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 TCP/IP データおよびその他にアプライアンスから出入りするパケットを表示できるようにします。これはネットワーク設定をデバッグしたり、どのようなネットワーク トラフィックがアプライアンスに到達または送出されているかを検出することができます。

手順

ステップ 1　[ヘルプとサポート（Help and Support）] > [パケット キャプチャ（Packet Capture）] を選択します。

ステップ 2　パケット キャプチャ設定の指定

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。

サポート担当者が、これらの設定の方法を説明する場合があります。

時間の単位を指定しないでキャプチャ期間を入力すると、AsyncOS はデフォルトで秒を使用します。

[フィルタ（Filters）] セクションで次を実行します。

- 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。パケット キャプチが終了する前にパケット 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 で実行したキャプチャは、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するようにします。またはキャプチャを無期限に実行する場合、[キャプチャを停止（Stop Capture）] をクリックして停止します。

ステップ 5　パケット キャプチャ ファイルへアクセスします。

- [パケット キャプチャ ファイルの管理（Manage Packet Capture Files）] リストでファイルをクリックして、[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には、FTP または SCP を使用します。

次の作業

サポートで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 アクセスを許可した場合、Technician 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 サポート担当者のリモート アクセスの有効化（16-4 ページ）を参照してください。
- 電子メールでファイルをサポートに送信します。

アプライアンスの電源のリモート リセット

アプライアンスのハード リセットが必要な場合は、サードパーティの Platform Management（IPMI）ツールを使用してアプライアンス シャーシをリモートからリブートできます。

制約事項

- リモート電源管理は、特定のハードウェアでのみ使用できます。

  詳細については、リモート電源管理の有効化（14-7 ページ）を参照してください。
- この機能を使用可能にするには、事前に有効にする必要があります。

  詳しくは、リモート電源管理の有効化（14-7 ページ）を参照してください。
- 次の IPMI コマンドのみがサポートされています。

  `status`、`on`、`off`、`cycle`、`reset`、`diag`、`soft`

  サポートされていないコマンドを発行すると、「権限不足」エラーが発生します。

はじめる前に

- IPMI バージョン 2.0 を使用してデバイスを管理できるユーティリティを取得し、設定します。
- サポートされている IPMI コマンドの使用方法を理解します。IPMI ツールのマニュアルを参照してください。

手順

ステップ 1　IPMI を使用して、必要なクレデンシャルとともに、先に設定したリモート電源管理ポートに割り当てられた IP アドレスに、サポートされている電源の再投入コマンドを発行します。

たとえば、IPMI をサポートする UNIX タイプのマシンからは、次のようなコマンドを発行します。

```
ipmitool -I lan -H 192.0.2.1 -U remoteresetuser -P password chassis power reset
```

ここで、`192.0.2.1` は、リモート電源管理ポートに割り当てられた IP アドレスで、`remoteresetuser` および `password` は、この機能を有効にしたときに入力したクレデンシャルです。

ステップ 2　アプライアンスが再起動されるまで、少なくとも 5 分間待ちます。

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有効または無効に設定されています。

表 A-1　IP インターフェイスに対してデフォルトで有効になるサービス

		デフォルトで有効かどうか	
サービス	**デフォルト ポート**	**管理インターフェイス**	**新規作成された IP インターフェイス**
FTP	21	いいえ	いいえ
Telnet	23	はい	いいえ
SSH	22	はい	いいえ
HTTP	80	はい	いいえ
HTTPS	443	はい	いいえ

IP インターフェイス

IP インターフェイスには、ネットワークへの個別の接続に必要なネットワーク設定データが含まれています。1 つの物理イーサネット インターフェイスに対して複数の IP インターフェイスを設定できます。IP インターフェイス経由での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では、各 IP インターフェイスが特定の 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 アドレスとして動作します。インターフェイスを独立したグループに（CLI を使用して）「参加」させることもできます。システムは、電子メールの配信時にこれらのグループを順番に使用します。仮想ゲートウェイへの参加またはグループ化は、複数のインターフェイス間で大規模な電子メール キャンペーンをロードバランシングするのに役立ちます。VLAN を作成し、他のインターフェイスと同様に（CLI を使用して）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 ガイドまたはオンライン ヘルプの「Advanced Networking」の章を参照してください。

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ること、および逆引き 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、スパム隔離、HTTP、および HTTPS はインターフェイス上で有効または無効にできます。サービスごとにポートを設定できます。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、変更を保存した場合は、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ます。

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有効にする各サービスの横にあるチェックボックスをオンにします。必要に応じて、対応するポートを変更します。

ステップ 8　アプライアンス管理用にインターフェイスで HTTP から HTTPS へのリダイレクトを有効にするかどうかを選択します。

ステップ 9　スパム隔離を使用している場合は、HTTP、HTTPS、またはその両方を選択し、それぞれにポート番号を指定できます。HTTP 要求を HTTPS にリダイレクトするかどうかも選択できます。最後に、IP インターフェイスをスパム隔離のデフォルト インターフェイスにするかどうか、ホスト名を URL として使用するかどうか、およびカスタム URL を指定するかどうかを指定できます。

ステップ 10　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無効にすることにより、アプライアンスへの接続方法に応じて、GUI または CLI から接続を解除できます。管理ポートで別のプロトコル、シリアル インターフェイス、または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 アクセスを有効にします。

（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、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)] > [ログサブスクリプション(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」の章の「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記述した 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別のマシンにコピーしたり、ファイルをデータベースにロードして独自の分析アプリケーションを作成したり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　FTP プログラムを使用して、適切なディレクトリに対するファイルのアップロードおよびダウンロードを行います。

secure copy（scp）アクセス

クライアント オペレーティング システムで secure copy（scp）コマンドがサポートされている場合は、表 A-3（A-4 ページ）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。この例は参考用です。オペレーティング システムの secure copy の実装方法によって異なる場合があります。

```
% scp /tmp/test.txt admin@mail3.example.com:configuration
The authenticity of host 'mail3.example.com (192.168.42.42)' can't be established.
DSA key fingerprint is 69:02:01:1d:9b:eb:eb:80:0c:a1:f5:a6:61:da:c8:db.
Are you sure you want to continue connecting (yes/no)? Yes
Warning: Permanently added 'mail3.example.com ' (DSA) to the list of known hosts.
admin@mail3.example.com's password: (type the password)
test.txt             100% |***************************|  1007       00:00
%
```

この例では、同じファイルがアプライアンスからクライアント マシンにコピーされます。

```
% scp admin@mail3.example.com:configuration/text.txt .
admin@mail3.example.com's password: (type the password)
test.txt             100% |***************************|  1007       00:00
```

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 secure copy（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（14-31 ページ）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-1 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-1　　シリアル ポートのピン番号

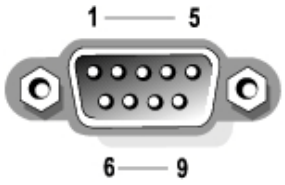


表 A-4　　シリアル ポートのピン割り当て

ピン留め	信号	I/O	定義
1	DCD	I	データ キャリア検出
2	SIN	I	シリアル入力
3	SOUT	O	シリアル出力
4	DTR	O	データ ターミナル レディ
5	GND	適用対象外	信号アース
6	DSR	I	データ セット レディ
7	RTS	I	送信要求
8	CTS	O	送信可
9	RI	I	リング インジケータ
シェル	適用対象外	適用対象外	シャーシ アース

ネットワーク アドレスと IP アドレスの割り当て

この付録では、ネットワーク アドレスと IP アドレスの割り当てに関する一般的なルールについて説明し、ネットワークにシスコ 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 コンテンツ セキュリティ アプライアンスには、構成（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）に応じて、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。これらには次のようなラベルが付けられています。

- 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 アプライアンスが発信パケットの送信に一意のインターフェイスを選択できる必要があります。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。ここでの規則により、単一のネットワークに配置できるインターフェイスは（ネットマスクをインターフェイスの IP アドレスに適用する関係上）1 つに限られています。

IP アドレスは、特定のネットワーク上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。イーサネット インターフェイスが複数の IP アドレスを持つ場合は、パケットの送信元アドレスとして任意の IP アドレスを 1 つ使用することで、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、Virtual Gateway 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、Classless Inter-Domain Routing（CIDR）形式で表現されることがあります。すなわち、ビット数（1 ～ 32）の先頭にスラッシュが付きます。

この方法では、単純にバイナリ表記で 1 を数えることでネットマスクを表現できます。したがって `255.255.255.0` は「`/24`」となり、`255.255.240.0` は「`/20`」となります。

インターフェイスの設定例

ここでは、いくつかの代表的なネットワークに基づいたインターフェイスの設定例を示します。この例では、Int1 と Int2 の 2 つのインターフェイスを使用します。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:

インターフェイスはそれぞれ、別々のネットワークに配置する必要があります。

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 で送出されます。`192.168.0.X` にアドレス指定されたデータは、Int2 で送出されます。この形式ではない他のアドレス（WAN またはインターネット上である可能性が高い）宛てのパケットは、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いずれか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`

この場合、2 つの異なるイーサネット インターフェイスが同じネットワーク アドレスを持つという矛盾した状態になっています。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べきかを特定できません。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ます。その場合は、そのパケットの送信先を見つけることができません。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、次のように 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ことが想定されます。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。
- 同じネットワーク スイッチに接続されている 2 つのイーサネット インターフェイスが、最終的に別のホスト ダウンストリーム上の単一のインターフェイスと通信する場合、またはすべてのデータがすべてのポートにエコーされるネットワーク ハブに接続されている場合、2 つのインターフェイスを使用しても得られる利点はありません。
- 1000Base-T で動作するインターフェイスを介した SMTP カンバセーションは、100Base-T で動作する同じインターフェイスを介した場合より若干速くなりますが、これは理想的な条件下でのみです。
- 配信ネットワークのその他の部分にボトルネックがある場合、ネットワークへの接続を最適化しても意味がありません。ボトルネックは、インターネットへの接続や、接続プロバイダーによるアップストリームへの接続で最も頻繁に発生します。

接続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。ご使用のネットワーク トポロジやデータのボリュームから判断して不要であれば、複数のインターフェイスに接続する必要はありません。また、最初は単純な接続にしておき、ゲートウェイに慣れてきたら、ボリュームやネットワーク トポロジでの必要に応じて接続を増やすこともできます。

ファイアウォール情報

次の表に示すポートは、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く必要がある場合があります(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	入力または出力	AsyncOS IP、FTP サーバ	ログ ファイルのアグリゲーション用 FTP。 データ ポート TCP 1024 以上は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 ベースの記事（TechNotes）（E-3 ページ）を参照してください。
22	SSH	発信（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 プッシュ。 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	発信（Out）	SCP サーバ	ログ サーバへの SCP プッシュ。
23	Telnet	In	AsyncOS IP	CLI への Telnet アクセス。
23	Telnet	発信（Out）	Telnet サーバ	Telnet アップグレード。
25	TCP	発信（Out）	任意（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	発信（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	発信（Out）	updates.cisco.com	AsyncOS アップグレード。

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
82	HTTP	In	AsyncOS IP	スパム隔離の表示に使用されます。
83	HTTPS	In	AsyncOS IP	スパム隔離の表示に使用されます。
53	UDP/TCP	発信（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	発信（Out）	POP サーバ	スパム隔離のためのエンド ユーザの POP 認証。
123	UDP	発信（Out）	NTP サーバ	タイム サーバがファイアウォールの外側にある場合の NTP。
143	TCP	発信（Out）	IMAP サーバ	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	発信（Out）	管理ステーション	SNMP トラップ。
389 3268	LDAP	発信（Out）	LDAP サーバ	LDAP ディレクトリ サーバがファイアウォールの外側にある場合の LDAP。スパム隔離のための LDAP 認証。
636 3269	LDAPS	発信（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 へのセキュア HTTP（`https`）アクセス。
443	TCP	発信（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	発信（Out）	update-manifests.ironport.com	アップデート サーバから最新のファイルのリストを取得します（物理ハードウェア アプライアンスの場合）。
443	TCP	発信（Out）	update-manifests.sco.cisco.com	アップデート サーバから最新のファイルのリストを取得します（仮想アプライアンスの場合）。
443	TCP	発信（Out）	phonehome.senderbase.org	アウトブレイク フィルタの受信/送信。

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
443	TCP	発信（Out）	Web セキュリティ アプライアンスの [セキュリティ サービス（Security Services）] > [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] ページの [詳細設定（Advanced）] セクションで設定されているファイル分析サーバ URL。 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 サービス（Security Services）] > [ファイルレピュテーションと分析（File Reputation and Analysis）] ページの [詳細設定（Advanced）] セクションで設定されているファイル分析サーバ URL。	ファイル分析サーバに詳細なファイル分析結果を表示します。 関連項目： • 電子メール セキュリティ レポート：ファイル分析レポートの詳細の要件（4-31 ページ） • Web セキュリティ レポート：ファイル分析レポートの詳細の要件（5-25 ページ）
514	UDP/TCP	発信（Out）	Syslog サーバ	Syslog ロギング。
1024 以上	—	—	—	ポート 21（FTP）に関する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	外部スパム隔離が有効の場合、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します。
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 アプライアンスとセキュリティ管理アプライアンスの間でポリシー、ウイルス、およびアウトブレイク隔離データの受け渡しを行います。

Web セキュリティ管理の例

この付録では、シスコ コンテンツ セキュリティ管理アプライアンスの機能を導入するいくつかの一般的な方法について説明します。内容は次のとおりです。

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 レポーティングと Web トラッキングが有効になっ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 レポーティングを有効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

ここでは、システム管理者がどのように社内の特定ユーザを調査するかについて例を挙げます。

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。これを調査するには、システム管理者は 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 アクティビティをトラッキングすると、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。

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)] > [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** または**クライアント IP アドレス**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 の情報について調査します。

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（User Details）] ページが表示されます。

[ユーザの詳細（User Details）] ページから、総トランザクション数別 URL カテゴリ、総トランザクション数別傾向、一致した URL カテゴリ、一致したドメイン、一致したアプリケーション、検出されたマルウェア脅威、および一致したポリシーを確認できます。

これらのカテゴリによって、たとえば 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かどうかがわかります。

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）] をクリックすると、ユーザがアクセスしようとしたドメインおよび URL のリスト全体が表示されます。

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留意してください。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 の完全な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）（5-12 ページ）
[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）（5-13 ページ）
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（3-10 ページ）
[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（5-44 ページ）

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、自社で先週のアクセス数が多かった上位 5 つのサイトを知りたいと考えています。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。

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）] セクションまでスクロールすると、アクセスされたドメインまたは Web サイトが表示されます。

アクセス数が上位 25 位までの Web サイトが、[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（5-15 ページ）

例 3: アクセス数上位の URL カテゴリの調査

このシナリオでは、人事部マネージャが、最近 30 日間に従業員がアクセスしている上位 3 つの URL カテゴリを知りたいと考えています。さらに、ネットワーク管理者が、同様の情報を使って帯域幅の使用状況をモニタし、最も帯域幅を使用している URL がどれかを知りたいと考えています。

以下の例は、複数の人の関心事に対応するデータを 1 つのレポートで提供する方法を示します。

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）] > [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、インスタント メッセージ、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し、このファイルを人事部マネージャに送信できます。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　[使用帯域幅（Bandwidth Used）] カラムを表示するには、[一致したURLカテゴリ（URL Categories Matched）] テーブルまでスクロールします。

[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 マネージャに送信します。さらに詳しく調べる場合は、[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。

このページで、ネットワーク マネージャはインスタント メッセージ サイトの上位 10 人の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 のユーザがインスタント メッセージ 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　上位 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（URL Categories）] レポート（5-16 ページ）
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（3-10 ページ）

関連リソース

Cisco 通知サービス

セキュリティ アドバイザリ、フィールド ノーティス、販売終了とサポート終了の通知、およびソフトウェア アップデートと既知の問題に関する情報などの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（E-4 ページ）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。

Cisco Content Security 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/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html
Web セキュリティ アプライアンス	http://www.cisco.com/c/en/us/support/security/web-security-appliance/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/c/en/us/support/security/email-security-appliance/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/c/en/us/support/security/email-security-appliance/products-command-reference-list.html
Cisco IronPort 暗号化	http://www.cisco.com/c/en/us/support/security/email-encryption/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 9.0 for Cisco Content Security Management Appliances ユーザ ガイド*』ご使用のリリース用(このマニュアル)
- ご使用の Web セキュリティ アプライアンスのマニュアル

  Web セキュリティ リリース 8.0 以降:
  - ご使用のリリースの『*Cisco AsyncOS for Web User Guide*』

  Web セキュリティ リリース 8.0 より前:
  - ご使用のリリースの『*Cisco IronPort AsyncOS for Web User Guide*』
- Cisco AsyncOS for Email Security のドキュメント:

  Email Security リリース 8.0 以降:
  - ご使用のリリースの『*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*』(一部のコマンドはすべての Cisco Content Security 製品に適用されます)

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/c/en/us/support/security/content-security-management-appliance/products-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

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/learning/le31/email_sec/index.html
- http://www.cisco.com/web/learning/training-index.html

または、stbu-trg@cisco.com にお問い合わせください。

ナレッジ ベースの記事（TechNotes）

ステップ 1　メイン製品ページにアクセスします（http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html）

ステップ 2　名前に **TechNotes** が付くリンクを探します。

シスコ サポート コミュニティ

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 コミュニティへのアクセス先:

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

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

カスタマー サポート

サポートを受けるには、次の方法を使用してください。

米国外:http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

サポート サイト: http://www.cisco.com/web/services/acquisitions/ironport.html

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

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(16-3 ページ)も参照してください。

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(E-1 ページ)
- ナレッジ ベースの記事(TechNotes)(E-3 ページ)

マニュアルに関するフィードバック

テクニカル マニュアル チームは、製品マニュアルの改善に努めています。お客様からのご意見をお待ちしています。次の電子メール アドレス宛にお送りください。

contentsecuritydocs@cisco.com

メッセージの件名行に、このマニュアルのタイトルとタイトル ページに記載されている発行日をご記入ください。

End User License Agreement

Cisco Systems End User License Agreement

IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. IT IS VERY IMPORTANT THAT YOU CHECK THAT YOU ARE PURCHASING CISCO SOFTWARE OR EQUIPMENT FROM AN APPROVED SOURCE AND THAT YOU, OR THE ENTITY YOU REPRESENT (COLLECTIVELY, THE "CUSTOMER") HAVE BEEN REGISTERED AS THE END USER FOR THE PURPOSES OF THIS CISCO END USER LICENSE AGREEMENT. IF YOU ARE NOT REGISTERED AS THE END USER YOU HAVE NO LICENSE TO USE THE SOFTWARE AND THE LIMITED WARRANTY IN THIS END USER LICENSE AGREEMENT DOES NOT APPLY. ASSUMING YOU HAVE PURCHASED FROM AN APPROVED SOURCE, DOWNLOADING, INSTALLING OR USING CISCO OR CISCO-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.

CISCO SYSTEMS, INC. OR ITS SUBSIDIARY LICENSING THE SOFTWARE INSTEAD OF CISCO SYSTEMS, INC. ("CISCO") IS WILLING TO LICENSE THIS SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU PURCHASED THE SOFTWARE FROM AN APPROVED SOURCE AND THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS END USER LICENSE AGREEMENT PLUS ANY ADDITIONAL LIMITATIONS ON THE LICENSE SET FORTH IN A SUPPLEMENTAL LICENSE AGREEMENT ACCOMPANYING THE PRODUCT OR AVAILABLE AT THE TIME OF YOUR ORDER (COLLECTIVELY THE "AGREEMENT"). TO THE EXTENT OF ANY CONFLICT BETWEEN THE TERMS OF THIS END USER LICENSE AGREEMENT AND ANY SUPPLEMENTAL LICENSE AGREEMENT, THE SUPPLEMENTAL LICENSE AGREEMENT SHALL APPLY. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU ARE REPRESENTING THAT YOU PURCHASED THE SOFTWARE FROM AN APPROVED SOURCE AND BINDING YOURSELF TO THE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED CD PACKAGE AND ANY WRITTEN MATERIALS) FOR A FULL REFUND, OR, IF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM AN APPROVED SOURCE, AND APPLIES ONLY IF YOU ARE THE ORIGINAL AND REGISTERED END USER PURCHASER. FOR THE PURPOSES OF THIS END USER LICENSE AGREEMENT, AN "APPROVED SOURCE" MEANS (A) CISCO; OR (B) A DISTRIBUTOR OR SYSTEMS INTEGRATOR AUTHORIZED BY CISCO TO DISTRIBUTE /

SELL CISCO EQUIPMENT, SOFTWARE AND SERVICES WITHIN YOUR TERRITORY TO END USERS; OR (C) A RESELLER AUTHORIZED BY ANY SUCH DISTRIBUTOR OR SYSTEMS INTEGRATOR IN ACCORDANCE WITH THE TERMS OF THE DISTRIBUTOR'S AGREEMENT WITH CISCO TO DISTRIBUTE / SELL THE CISCO EQUIPMENT, SOFTWARE AND SERVICES WITHIN YOUR TERRITORY TO END USERS.

THE FOLLOWING TERMS OF THE AGREEMENT GOVERN CUSTOMER'S USE OF THE SOFTWARE (DEFINED BELOW), EXCEPT TO THE EXTENT: (A) THERE IS A SEPARATE SIGNED CONTRACT BETWEEN CUSTOMER AND CISCO GOVERNING CUSTOMER'S USE OF THE SOFTWARE, OR (B) THE SOFTWARE INCLUDES A SEPARATE "CLICK-ACCEPT" LICENSE AGREEMENT OR THIRD PARTY LICENSE AGREEMENT AS PART OF THE INSTALLATION OR DOWNLOAD PROCESS GOVERNING CUSTOMER'S USE OF THE SOFTWARE. TO THE EXTENT OF A CONFLICT BETWEEN THE PROVISIONS OF THE FOREGOING DOCUMENTS, THE ORDER OF PRECEDENCE SHALL BE (1)THE SIGNED CONTRACT, (2) THE CLICK-ACCEPT AGREEMENT OR THIRD PARTY LICENSE AGREEMENT, AND (3) THE AGREEMENT. FOR PURPOSES OF THE AGREEMENT, "SOFTWARE" SHALL MEAN COMPUTER PROGRAMS, INCLUDING FIRMWARE AND COMPUTER PROGRAMS EMBEDDED IN CISCO EQUIPMENT, AS PROVIDED TO CUSTOMER BY AN APPROVED SOURCE, AND ANY UPGRADES, UPDATES, BUG FIXES OR MODIFIED VERSIONS THERETO (COLLECTIVELY, "UPGRADES"), ANY OF THE SAME WHICH HAS BEEN RELICENSED UNDER THE CISCO SOFTWARE TRANSFER AND RE-LICENSING POLICY (AS MAY BE AMENDED BY CISCO FROM TIME TO TIME) OR BACKUP COPIES OF ANY OF THE FOREGOING.

License. Conditioned upon compliance with the terms and conditions of the Agreement, Cisco grants to Customer a nonexclusive and nontransferable license to use for Customer's internal business purposes the Software and the Documentation for which Customer has paid the required license fees to an Approved Source. "Documentation" means written information (whether contained in user or technical manuals, training materials, specifications or otherwise) pertaining to the Software and made available by an Approved Source with the Software in any manner (including on CD-Rom, or on-line). In order to use the Software, Customer may be required to input a registration number or product authorization key and register Customer's copy of the Software online at Cisco's website to obtain the necessary license key or license file.

Customer's license to use the Software shall be limited to, and Customer shall not use the Software in excess of, a single hardware chassis or card or such other limitations as are set forth in the applicable Supplemental License Agreement or in the applicable purchase order which has been accepted by an Approved Source and for which Customer has paid to an Approved Source the required license fee (the "Purchase Order").

Unless otherwise expressly provided in the Documentation or any applicable Supplemental License Agreement, Customer shall use the Software solely as embedded in, for execution on, or (where the applicable Documentation permits installation on non-Cisco equipment) for communication with Cisco equipment owned or leased by Customer and used for Customer's internal business purposes. No other licenses are granted by implication, estoppel or otherwise.

For evaluation or beta copies for which Cisco does not charge a license fee, the above requirement to pay license fees does not apply.

General Limitations. This is a license, not a transfer of title, to the Software and Documentation, and Cisco retains ownership of all copies of the Software and Documentation. Customer acknowledges that the Software and Documentation contain trade secrets of Cisco or its suppliers or licensors, including but not limited to the specific internal design and structure of individual programs and associated interface information. Except as otherwise expressly provided under the Agreement, Customer shall only use the Software in connection with the use of Cisco equipment purchased by the Customer from an Approved Source and Customer shall have no right, and Customer specifically agrees not to:

(i) transfer, assign or sublicense its license rights to any other person or entity (other than in compliance with any Cisco relicensing/transfer policy then in force), or use the Software on Cisco equipment not purchased by the Customer from an Approved Source or on secondhand Cisco equipment, and Customer acknowledges that any attempted transfer, assignment, sublicense or use shall be void;

(ii) make error corrections to or otherwise modify or adapt the Software or create derivative works based upon the Software, or permit third parties to do the same;

(iii) reverse engineer or decompile, decrypt, disassemble or otherwise reduce the Software to human-readable form, except to the extent otherwise expressly permitted under applicable law notwithstanding this restriction or except to the extent that Cisco is legally required to permit such specific activity pursuant to any applicable open source license;

(iv) publish any results of benchmark tests run on the Software;

(v) use or permit the Software to be used to perform services for third parties, whether on a service bureau or time sharing basis or otherwise, without the express written authorization of Cisco; or

(vi) disclose, provide, or otherwise make available trade secrets contained within the Software and Documentation in any form to any third party without the prior written consent of Cisco. Customer shall implement reasonable security measures to protect such trade secrets.

To the extent required by applicable law, and at Customer's written request, Cisco shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of Cisco's applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Cisco makes such information available.

Software, Upgrades and Additional Copies. NOTWITHSTANDING ANY OTHER PROVISION OF THE AGREEMENT: (1) CUSTOMER HAS NO LICENSE OR RIGHT TO MAKE OR USE ANY ADDITIONAL COPIES OR UPGRADES UNLESS CUSTOMER, AT THE TIME OF MAKING OR ACQUIRING SUCH COPY OR UPGRADE, ALREADY HOLDS A VALID LICENSE TO THE ORIGINAL SOFTWARE AND HAS PAID THE APPLICABLE FEE TO AN APPROVED SOURCE FOR THE UPGRADE OR ADDITIONAL COPIES; (2) USE OF UPGRADES IS LIMITED TO CISCO EQUIPMENT SUPPLIED BY AN APPROVED SOURCE FOR WHICH CUSTOMER IS THE ORIGINAL END USER PURCHASER OR LESSEE OR OTHERWISE HOLDS A VALID LICENSE TO USE THE SOFTWARE WHICH IS BEING UPGRADED; AND (3) THE MAKING AND USE OF ADDITIONAL COPIES IS LIMITED TO NECESSARY BACKUP PURPOSES ONLY.

Proprietary Notices. Customer agrees to maintain and reproduce all copyright, proprietary, and other notices on all copies, in any form, of the Software in the same form and manner that such copyright and other proprietary notices are included on the Software. Except as expressly authorized in the Agreement, Customer shall not make any copies or duplicates of any Software without the prior written permission of Cisco.

Term and Termination. The Agreement and the license granted herein shall remain effective until terminated. Customer may terminate the Agreement and the license at any time by destroying all copies of Software and any Documentation. Customer's rights under the Agreement will terminate immediately without notice from Cisco if Customer fails to comply with any provision of the Agreement. Upon termination, Customer shall destroy all copies of Software and Documentation in its possession or control. All confidentiality obligations of Customer, all restrictions and limitations imposed on the Customer under the section titled "General Limitations" and all limitations of liability and disclaimers and restrictions of warranty shall survive termination of this Agreement. In addition, the provisions of the sections titled "U.S. Government End User Purchasers" and "General Terms Applicable to the Limited Warranty Statement and End User License Agreement" shall survive termination of the Agreement.

Customer Records. Customer grants to Cisco and its independent accountants the right to examine Customer's books, records and accounts during Customer's normal business hours to verify compliance with this Agreement. In the event such audit discloses non-compliance with this Agreement, Customer shall promptly pay to Cisco the appropriate license fees, plus the reasonable cost of conducting the audit.

Export, Re-Export, Transfer and Use Controls. The Software, Documentation and technology or direct products thereof (hereafter referred to as Software and Technology), supplied by Cisco under the Agreement are subject to export controls under the laws and regulations of the United States (U.S.) and any other applicable countries' laws and regulations. Customer shall comply with such laws and regulations governing export, re-export, transfer and use of Cisco Software and Technology and will obtain all required U.S. and local authorizations, permits, or licenses. Cisco and Customer each agree to provide the other information, support documents, and assistance as may reasonably be required by the other in connection with securing authorizations or licenses. Information regarding compliance with export, re-export, transfer and use may be located at the following URL:

http://www.cisco.com/web/about/doing_business/legal/global_export_trade/general_export/contract_compliance.html.

U.S. Government End User Purchasers. The Software and Documentation qualify as "commercial items," as that term is defined at Federal Acquisition Regulation ("FAR") (48 C.F.R.) 2.101, consisting of "commercial computer software" and "commercial computer software documentation" as such terms are used in FAR 12.212. Consistent with FAR 12.212 and DoD FAR Supp. 227.7202-1 through 227.7202-4, and notwithstanding any other FAR or other contractual clause to the contrary in any agreement into which the Agreement may be incorporated, Customer may provide to Government end user or, if the Agreement is direct, Government end user will acquire, the Software and Documentation with only those rights set forth in the Agreement. Use of either the Software or Documentation or both constitutes agreement by the Government that the Software and Documentation are "commercial computer software" and "commercial computer software documentation," and constitutes acceptance of the rights and restrictions herein.

Identified Components; Additional Terms. The Software may contain or be delivered with one or more components, which may include third-party components, identified by Cisco in the Documentation, readme.txt file, third-party click-accept or elsewhere (e.g. on www.cisco.com) (the "Identified Component(s)") as being subject to different license agreement terms, disclaimers of warranties, limited warranties or other terms and conditions (collectively, "Additional Terms") than those set forth herein. You agree to the applicable Additional Terms for any such Identified Component(s)."

Limited Warranty

Subject to the limitations and conditions set forth herein, Cisco warrants that commencing from the date of shipment to Customer (but in case of resale by an Approved Source other than Cisco, commencing not more than ninety (90) days after original shipment by Cisco), and continuing for a period of the longer of (a) ninety (90) days or (b) the warranty period (if any) expressly set forth as applicable specifically to software in the warranty card accompanying the product of which the Software is a part (the "Product") (if any): (a) the media on which the Software is furnished will be free of defects in materials and workmanship under normal use; and (b) the Software substantially conforms to the Documentation. The date of shipment of a Product by Cisco is set forth on the packaging material in which the Product is shipped. Except for the foregoing, the Software is provided "AS IS". This limited warranty extends only to the Software purchased from an Approved Source by a Customer who is the first registered end user. Customer's sole and exclusive remedy and the entire liability of Cisco and its suppliers under this limited warranty will be (i) replacement of defective media and/or (ii) at Cisco's option, repair, replacement, or refund of the purchase price of the Software, in both cases subject to the condition that any error or defect constituting a breach of this limited warranty is reported to the Approved Source supplying the Software to Customer, within the warranty period. Cisco or the Approved Source supplying the Software to Customer may, at its option, require return of the Software and/or Documentation as a condition to the remedy. In no event does Cisco warrant that the Software is

error free or that Customer will be able to operate the Software without problems or interruptions. In addition, due to the continual development of new techniques for intruding upon and attacking networks, Cisco does not warrant that the Software or any equipment, system or network on which the Software is used will be free of vulnerability to intrusion or attack.

Restrictions. This warranty does not apply if the Software, Product or any other equipment upon which the Software is authorized to be used (a) has been altered, except by Cisco or its authorized representative, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Cisco, (c) has been subjected to abnormal physical or electrical stress, abnormal environmental conditions, misuse, negligence, or accident; or (d) is licensed for beta, evaluation, testing or demonstration purposes. The Software warranty also does not apply to (e) any temporary Software modules; (f) any Software not posted on Cisco's Software Center; (g) any Software that Cisco expressly provides on an "AS IS" basis on Cisco's Software Center; (h) any Software for which an Approved Source does not receive a license fee; and (i) Software supplied by any third party which is not an Approved Source.

DISCLAIMER OF WARRANTY

EXCEPT AS SPECIFIED IN THIS WARRANTY SECTION, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, SATISFACTORY QUALITY, NON-INTERFERENCE, ACCURACY OF INFORMATIONAL CONTENT, OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW AND ARE EXPRESSLY DISCLAIMED BY CISCO, ITS SUPPLIERS AND LICENSORS. TO THE EXTENT THAT ANY OF THE SAME CANNOT BE EXCLUDED, SUCH IMPLIED CONDITION, REPRESENTATION AND/OR WARRANTY IS LIMITED IN DURATION TO THE EXPRESS WARRANTY PERIOD REFERRED TO IN THE "LIMITED WARRANTY" SECTION ABOVE. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY IN SUCH STATES. THIS WARRANTY GIVES CUSTOMER SPECIFIC LEGAL RIGHTS, AND CUSTOMER MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. This disclaimer and exclusion shall apply even if the express warranty set forth above fails of its essential purpose.

Disclaimer of Liabilities - Limitation of Liability. IF YOU ACQUIRED THE SOFTWARE IN THE UNITED STATES, LATIN AMERICA, CANADA, JAPAN OR THE CARIBBEAN, NOTWITHSTANDING ANYTHING ELSE IN THE AGREEMENT TO THE CONTRARY, ALL LIABILITY OF CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS COLLECTIVELY, TO CUSTOMER, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), BREACH OF WARRANTY OR OTHERWISE, SHALL NOT EXCEED THE PRICE PAID BY CUSTOMER TO ANY APPROVED SOURCE FOR THE SOFTWARE THAT GAVE RISE TO THE CLAIM OR IF THE SOFTWARE IS PART OF ANOTHER PRODUCT, THE PRICE PAID FOR SUCH OTHER PRODUCT. THIS LIMITATION OF LIABILITY FOR SOFTWARE IS CUMULATIVE AND NOT PER INCIDENT (I.E. THE EXISTENCE OF TWO OR MORE CLAIMS WILL NOT ENLARGE THIS LIMIT).

IF YOU ACQUIRED THE SOFTWARE IN EUROPE, THE MIDDLE EAST, AFRICA, ASIA OR OCEANIA, NOTWITHSTANDING ANYTHING ELSE IN THE AGREEMENT TO THE CONTRARY, ALL LIABILITY OF CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS COLLECTIVELY, TO CUSTOMER, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), BREACH OF WARRANTY OR OTHERWISE, SHALL NOT EXCEED THE PRICE PAID BY CUSTOMER TO CISCO FOR THE SOFTWARE THAT GAVE RISE TO THE CLAIM OR IF THE SOFTWARE IS PART OF ANOTHER PRODUCT, THE PRICE PAID

FOR SUCH OTHER PRODUCT. THIS LIMITATION OF LIABILITY FOR SOFTWARE IS CUMULATIVE AND NOT PER INCIDENT (I.E. THE EXISTENCE OF TWO OR MORE CLAIMS WILL NOT ENLARGE THIS LIMIT). NOTHING IN THE AGREEMENT SHALL LIMIT (I) THE LIABILITY OF CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS TO CUSTOMER FOR PERSONAL INJURY OR DEATH CAUSED BY THEIR NEGLIGENCE, (II) CISCO'S LIABILITY FOR FRAUDULENT MISREPRESENTATION, OR (III) ANY LIABILITY OF CISCO WHICH CANNOT BE EXCLUDED UNDER APPLICABLE LAW.

Disclaimer of Liabilities - Waiver of Consequential Damages and Other Losses. IF YOU ACQUIRED THE SOFTWARE IN THE UNITED STATES, LATIN AMERICA, THE CARIBBEAN OR CANADA, REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE OR OTHERWISE, IN NO EVENT WILL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR LOST OR DAMAGED DATA, BUSINESS INTERRUPTION, LOSS OF CAPITAL, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY OR WHETHER ARISING OUT OF THE USE OF OR INABILITY TO USE SOFTWARE OR OTHERWISE AND EVEN IF CISCO OR ITS SUPPLIERS OR LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

IF YOU ACQUIRED THE SOFTWARE IN JAPAN, EXCEPT FOR LIABILITY ARISING OUT OF OR IN CONNECTION WITH DEATH OR PERSONAL INJURY, FRAUDULENT MISREPRESENTATION, AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE OR OTHERWISE, IN NO EVENT WILL CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR LOST OR DAMAGED DATA, BUSINESS INTERRUPTION, LOSS OF CAPITAL, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY OR WHETHER ARISING OUT OF THE USE OF OR INABILITY TO USE SOFTWARE OR OTHERWISE AND EVEN IF CISCO OR ANY APPROVED SOURCE OR THEIR SUPPLIERS OR LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IF YOU ACQUIRED THE SOFTWARE IN EUROPE, THE MIDDLE EAST, AFRICA, ASIA OR OCEANIA, IN NO EVENT WILL CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS, BE LIABLE FOR ANY LOST REVENUE, LOST PROFIT, OR LOST OR DAMAGED DATA, BUSINESS INTERRUPTION, LOSS OF CAPITAL, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES, HOWSOEVER ARISING, INCLUDING, WITHOUT LIMITATION, IN CONTRACT, TORT (INCLUDING NEGLIGENCE) OR WHETHER ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF, IN EACH CASE, CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS, HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT FULLY APPLY TO YOU. THE FOREGOING EXCLUSION SHALL NOT APPLY TO ANY LIABILITY ARISING OUT OF OR IN CONNECTION WITH: (I) DEATH OR PERSONAL INJURY, (II) FRAUDULENT MISREPRESENTATION, OR (III) CISCO'S LIABILITY IN CONNECTION WITH ANY TERMS THAT CANNOT BE EXCLUDED UNDER APPLICABLE LAW.

Customer acknowledges and agrees that Cisco has set its prices and entered into the Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the parties.

Controlling Law, Jurisdiction. If you acquired, by reference to the address on the purchase order accepted by the Approved Source, the Software in the United States, Latin America, or the Caribbean, the Agreement and warranties ("Warranties") are controlled by and construed under the laws of the State of California, United States of America, notwithstanding any conflicts of law provisions; and the state and federal courts of California shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties. If you acquired the Software in Canada, unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of the Province of Ontario, Canada, notwithstanding any conflicts of law provisions; and the courts of the Province of Ontario shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties. If you acquired the Software in Europe, the Middle East, Africa, Asia or Oceania (excluding Australia), unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of England, notwithstanding any conflicts of law provisions; and the English courts shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties. In addition, if the Agreement is controlled by the laws of England, no person who is not a party to the Agreement shall be entitled to enforce or take the benefit of any of its terms under the Contracts (Rights of Third Parties) Act 1999. If you acquired the Software in Japan, unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of Japan, notwithstanding any conflicts of law provisions; and the Tokyo District Court of Japan shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties. If you acquired the Software in Australia, unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of the State of New South Wales, Australia, notwithstanding any conflicts of law provisions; and the State and federal courts of New South Wales shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties. If you acquired the Software in any other country, unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of the State of California, United States of America, notwithstanding any conflicts of law provisions; and the state and federal courts of California shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties.

For all countries referred to above, the parties specifically disclaim the application of the UN Convention on Contracts for the International Sale of Goods. Notwithstanding the foregoing, either party may seek interim injunctive relief in any court of appropriate jurisdiction with respect to any alleged breach of such party's intellectual property or proprietary rights. If any portion hereof is found to be void or unenforceable, the remaining provisions of the Agreement and Warranties shall remain in full force and effect. Except as expressly provided herein, the Agreement constitutes the entire agreement between the parties with respect to the license of the Software and Documentation and supersedes any conflicting or additional terms contained in any Purchase Order or elsewhere, all of which terms are excluded. The Agreement has been written in the English language, and the parties agree that the English version will govern.

Product warranty terms and other information applicable to Cisco products are available at the following URL:

http://www.cisco.com/go/warranty

Supplemental End User License Agreement for Cisco Systems Content Security Software

IMPORTANT: READ CAREFULLY

This Supplemental End User License Agreement ("SEULA") contains additional terms and conditions for the Software product licensed under the End User License Agreement ("EULA") between You ("You" as used herein means You and the business entity you represent or "Company") and Cisco (collectively, the "Agreement"). Capitalized terms used in this SEULA but not defined will have the meanings assigned to them in the EULA. To the extent that there is a conflict between the terms and conditions of the EULA and this SEULA, the terms and conditions of this SEULA will take precedence.

In addition to the limitations set forth in the EULA on your access and use of the Software, you agree to comply at all times with the terms and conditions provided in this SEULA.

DOWNLOADING, INSTALLING, OR USING THE SOFTWARE CONSTITUTES ACCEPTANCE OF THE AGREEMENT, AND YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT TO THE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED CD PACKAGE AND ANY WRITTEN MATERIALS) FOR A FULL REFUND, OR, IF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM CISCO OR AN AUTHORIZED CISCO RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL END USER PURCHASER.

For purposes of this SEULA, the Product name and the Product description You have ordered is any of the following Cisco Systems Email Security Appliance ("ESA"), Cisco Systems Web Security Appliance ("WSA") and Cisco Systems Security Management Application ("SMA") (collectively, "Content Security") and their Virtual Appliance equivalent ("Software"):

Cisco AsyncOS for Email

Cisco AsyncOS for Web

Cisco AsyncOS for Management

Cisco Email Anti-Spam, Sophos Anti-Virus

Cisco Email Outbreak Filters

Cloudmark Anti-Spam

Cisco Image Analyzer

McAfee Anti-Virus

Cisco Intelligent Multi-Scan

Cisco RSA Data Loss Prevention

Cisco Email Encryption

Cisco Email Delivery Mode

Cisco Web Usage Controls

Cisco Web Reputation

Sophos Anti-Malware

Webroot Anti-Malware

McAfee Anti-Malware

Cisco Email Reporting

Cisco Email Message Tracking

Cisco Email Centralized Quarantine

Cisco Web Reporting

Cisco Web Policy and Configuration Management

Cisco Advanced Web Security Management with Splunk

Email Encryption for Encryption Appliances

Email Encryption for System Generated Bulk Email

Email Encryption and Public Key Encryption for Encryption Appliances

Large Attachment Handling for Encryption Appliances

Secure Mailbox License for Encryption Appliances

Definitions

For purposes of this SEULA, the following definitions apply:

"Company Service" means the Company's email, Internet, security management services provided to End Users for the purposes of conducting Company's internal business.

"End User" means: (1) for the WSA and SMA, the employee, contractor or other agent authorized by Company to access the Internet and the SMA via the Company Service; and (2) for the ESA, the email boxes of the employees, contractors, or other agent authorized by Company to access or use the email services via the Company Service.

"Ordering Document" means the purchase agreement, evaluation agreement, beta, pre-release agreement or similar agreement between the Company and Cisco or the Company and a Cisco reseller, or the valid terms of any purchase order accepted by Cisco in connection therewith, containing the purchase terms for the Software license granted by this Agreement.

"Personally Identifiable Information" means any information that can be used to identify an individual, including, but not limited to, an individual's name, user name, email address and any other personally identifiable information.

"Server" means a single physical computer or devices on a network that manages or provides network resources for multiple users.

"Services" means Cisco Software Subscription Services.

"Service Description" means the description of the Software Subscription Support Services at http://www.cisco.com/web/about/doing_business/legal/service_descriptions/index.html

"Telemetry Data" means samples of Company's email and web traffic, including data on email message and web request attributes and information on how different types of email messages and web requests were handled by Company's Cisco hardware products. Email message metadata and web requests included in Telemetry Data are anonymized and obfuscated to remove any Personally Identifiable Information.

"Term" means the length of the Software subscription You purchased, as indicated in your Ordering Document.

"Virtual Appliance" means the virtual version of Cisco's email security appliances, web security appliances, and security management appliances.

"Virtual Machine" means a software container that can run its own operating system and execute applications like a Server.

Additional License Terms and Conditions

LICENSE GRANTS AND CONSENT TO TERMS OF DATA COLLECTION

License of Software.

By using the Software and the Documentation, Company agrees to be bound by the terms of this Agreement, and so long as Company is in compliance with this Agreement, Cisco hereby grants to Company a nonexclusive, non-sublicensable, non-transferable, worldwide license during the Term to use the Software only on Cisco's hardware products, or in the case of the Virtual Appliances, on a Virtual Machine, solely in connection with the provision of the Company Service to End Users. The number of End Users licensed for the use of the Software is limited to the number of End Users specified in the Ordering Documents. In the event that the number of End Users in connection with the provision of the Company Service exceeds the number of End Users specified in the Ordering Documents, Company shall contact an Approved Source to purchase additional licenses for the Software. The duration and scope of this license(s) is further defined in the Ordering Document. The Ordering Document supersedes the EULA with respect to the term of the Software license. Except for the license rights granted herein, no right, title or interest in any Software is granted to the Company by Cisco, Cisco's resellers or their respective licensors. Your entitlement to Upgrades to the Software is subject to the Service Description. This Agreement and the Services are co-terminus.

Consent and License to Use Data.

Subject to the Cisco Privacy Statement at http://www.cisco.com/web/siteassets/legal/privacy.html, Company hereby consents and grants to Cisco a license to collect and use Telemetry Data from the Company. Cisco does not collect or use Personally Identifiable Information in the Telemetry Data. Cisco may share aggregated and anonymous Telemetry Data with third parties to assist us in improving your user experience and the Software and other Cisco security products and services. Company may terminate Cisco's right to collect Telemetry Data at any time by disabling SenderBase Network Participation in the Software. Instructions to enable or disable SenderBase Network Participation are available in the Software configuration guide.

Description of Other Rights and Obligations

Please refer to the Cisco Systems, Inc. End User License Agreement, Privacy Statement and Service Description of Software Subscription Support Services.

記号

A

C

D

F

G

H

I

L

M

N

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

と

ね

は

ひ

ふ

へ

ほ

ま

み

む

め

も

ゆ

ら

り

る

れ

ろ