Cisco IronPort AsyncOS 7.9 for Security Management ユーザ ガイド

2012 年 4 月 2 日

Text Part Number: 該当なし

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

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

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

Cisco IronPort AsyncOS 7.9 for Security Management ユーザ ガイド

CONTENTS

CHAPTER 1

セキュリティ管理アプライアンスをご使用の前に

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

今回のリリースでの変更点

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

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

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

また、http://www.cisco.com/en/US/products/ps10154/prod_release_notes_list.html にある『Release Notes for Cisco IronPort AsyncOS 7.6 for Email Security』の「New Features」リストも参照してください。

表 1-1　AsyncOS 7.9 for Security Management の新機能

機能	説明
新機能：	
新規の電子メール セキュリティ機能に対するレポーティングおよびメッセージ トラッキングのサポート	AsyncOS 7.6 for Email Security の次の新機能が、[Centralized Reporting] または [Centralized Message Tracking]、あるいはその両方でサポートされています。 • レポーティング、トラッキング、および Cisco IronPort Spam Quarantine での IPv6 経由で送品されたメッセージに対するサポート。 （今回のリリースでは、セキュリティ管理アプライアンスのすべてのインターフェイスで引き続き IPv4 が使用されます）。 • 送信者ごとのレート制限に対するレポーティングおよびメッセージ トラッキングのサポート。 これには、新規の中央集中型レート制限レポートが含まれます。このレポートでは、組織で受信された大量の電子メール メッセージの上位送信者を識別できます。 • メッセージ トラッキングにおける、新規の [Quarantine a copy and deliver] 機能で処理されるメッセージの識別。これにより、メッセージに対する措置を取ることなく、データ消失防止違反をモニタできます。 これらのレポートの基礎をなす機能の一般的な情報については、『Release Notes for Cisco IronPort AsyncOS 7.6 for Email Security』を参照してください。 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章の検索およびインタラクティブ電子メール レポート ページと [Rate Limits] ページ、および電子メール メッセージのトラッキングの章の電子メール メッセージの検索も参照してください。
アップグレードとサービス アップデートに対する異なるサーバ設定	イメージ サーバとリスト サーバの両方について、アップグレードとアップデートで別個のダウンロード サーバ設定を指定できるようになりました。 たとえば、AsyncOS のアップグレード用にローカル サーバ、サービス アップデート用に Cisco IronPort アップデート サーバをそれぞれ指定できます。これにより、サービス アップデートを即時利用できるようにしながら、アップグレードのタイミングを制御することが可能になります。 詳細については、一般的な管理タスクの章のアップグレードおよびサービス アップデートの設定を参照してください。
ルート ログインを防止する機能	現在、ルート レベルの SSH アクセスはデフォルトでディセーブルになりますが、Cisco IronPort サポート担当者がアクセスできるよう、必要に応じてイネーブルにすることができます。
拡張機能：	
拡張対象： DLP トラッキング権限に対するきめ細かな制御	メッセージ トラッキングにおける機密のデータ消失防止情報に対するユーザの役割でのアクセスを制限できるようになりました。 詳細については、管理タスクの分散の章のメッセージ トラッキングでの DLP 機密情報へのアクセスの制御を参照してください。

表 1-1　AsyncOS 7.9 for Security Management の新機能（続き）

機能	説明
拡張対象： SNMP	SNMP で、キャパシティの高いインターフェイスに対する 64 ビット カウンタがサポートされるようになりました。 現在、ifXTable（COUNTER64）、SNMP MIB OID を使用してアプライアンス ステータスを取得できます。
拡張対象： Windows 7 でのブラウザ サポート	AsyncOS for Security Management では現在、Windows 7 で動作する Internet Explorer 8 をサポートしています。

はじめる前に

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

このマニュアルは、参考資料として使用することもできます。ネットワークやファイアウォールの設定など、アプライアンスの存続期間を通して参照できる重要な情報が含まれています。

このマニュアルを読む前に、アプライアンスの『*Quick Start Guide*』と、製品の最新のリリース ノートを参照してください。このマニュアルは、アプライアンスが開梱されてラックに設置され、電源がオンされていることを前提としています。

（注）　すでにアプライアンスをネットワークに配線済みの場合は、IronPort アプライアンスのデフォルト IP アドレスが、ネットワーク上の他の IP アドレスと競合していないことを確認します。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。

詳細情報の入手先

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

- 「ドキュメント セット」（P.1-4）
- 「トレーニングと認定試験」（P.1-4）
- 「ナレッジ ベース」（P.1-4）
- 「シスコ サポート コミュニティ」（P.1-5）
- 「シスコのテクニカル サポート」（P.1-5）
- 「サード パーティ コントリビュータ」（P.1-6）

ドキュメント セット

マニュアルは、PDF ファイルおよび HTML ファイルとして配布されます。このマニュアルの電子バージョンは、Cisco IronPort カスタマー サポート サイトで入手できます。また、右上の [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。

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

- すべての製品のリリース ノート
- セキュリティ管理アプライアンス の『*Quick Start Guide*』
- 『*Cisco IronPort AsyncOS for Security Management ユーザ ガイド*』（本書）
- 『*Cisco IronPort AsyncOS for Web Security User Guide*』
- Cisco IronPort AsyncOS for Email Security のユーザ ガイド：
  - 『*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 IronPort AsyncOS CLI Reference Guide*』

このドキュメントおよびその他のドキュメントは、次の場所にあります。

Cisco IronPort 製品に関するドキュメント：	入手場所
セキュリティ管理アプライアンス	http://www.cisco.com/en/US/products/ps10155/tsd_products_support_series_home.html
電子メール セキュリティ アプライアンスおよび CLI リファレンス ガイド	http://www.cisco.com/en/US/products/ps10154/tsd_products_support_series_home.html
Web セキュリティ アプライアンス	http://www.cisco.com/en/US/products/ps10164/tsd_products_support_series_home.html
Cisco IronPort 暗号化	http://www.cisco.com/en/US/partner/products/ps10602/tsd_products_support_series_home.html

トレーニングと認定試験

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

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

ナレッジ ベース

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

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

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

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

一般に、項目は次のカテゴリのいずれかに分類されています。

- **手順**：手順の項目では、Cisco IronPort 製品を使用して何かを実行する方法について説明します。たとえば、アプライアンスのデータベースをバックアップおよび復元する手順を示します。
- **問題と解決策**：問題と解決策の項目では、Cisco IronPort 製品の使用時に発生する可能性があるエラーや問題に対処します。たとえば、製品の新バージョンにアップグレードしたときにエラー メッセージが表示された場合の対処方法を示します。
- **参考資料**：参考資料の項目では、特定のハードウェアに関連するエラー コードなどの情報を一覧表示します。
- **トラブルシューティング**：トラブルシューティングの項目では、Cisco IronPort 製品に関連する一般的な問題を分析し、解決する方法について説明します。たとえば、DNS で問題が発生した場合に実行する手順を示します。

シスコ サポート コミュニティ

シスコ サポート コミュニティは、シスコのお客様、パートナー、および従業員のオンライン フォーラムです。電子メールおよび Web セキュリティ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。フォーラムにトピックを投稿して質問したり、他のシスコ ユーザや Cisco IronPort ユーザと情報を共有したりできます。

シスコ サポート コミュニティには次の URL からアクセスできます。

https://supportforums.cisco.com

シスコのテクニカル サポート

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

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

以下を含むさまざまな作業にこの Web サイトが役立ちます。

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

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

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

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

サード パーティ コントリビュータ

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

契約の全文については、次の URL を参照してください。

https://support.ironport.com/3rdparty/AsyncOS_User_Guide-1-1.html

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

このマニュアルの一部は、Dell Computer Corporation の許可を受けて複製されています。このマニュアルの一部は、McAfee, Inc. の許可を受けて複製されています。このマニュアルの一部は、Sophos Plc の許可を受けて複製されています。

マニュアルに関するフィードバック

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

セキュリティ管理アプライアンスの概要

絶えず複雑化していくセキュリティ導入において、小規模な組織であっても、オンプレミス システム、管理対象サービス、リモート ワーカー、および提携する外部パートナーからなるその組織インフラストラクチャは複雑です。分散化された企業で結合力のあるセキュリティおよび企業コンプライアンスを確保するには、適切なコンポーネントを適所に配置するだけでは足りません。この複雑性をすべて考慮に入れた管理システムが必要となります。

柔軟なポリシー設定、包括的なモニタリング、洞察力に富むレポート、および効率的なトラブルシューティングが必要です。

セキュリティ管理アプライアンスは、電子メールおよび Web セキュリティを管理し、トラブルシューティングを実行し、さらに数ヵ月あるいは数年に及ぶデータ保存用のスペースを維持する統合管理プラットフォームです。

企業ポリシーの設定および監査情報をモニタするように設計された Cisco IronPort セキュリティ管理アプライアンスは、Cisco IronPort 電子メール セキュリティ アプライアンス（ESA）および Web セキュリティ アプライアンス（WSA）に対応するハードウェア、オペレーティング システム（AsyncOS）、およびサービスのサポートを兼ね備えています。

セキュリティ管理アプライアンスは、重要なポリシーとランタイム データを集中化および統合して、管理者およびエンド ユーザに対し、Web セキュリティ アプライアンスと電子メール セキュリティ アプライアンスのレポーティングおよび監査情報を管理するための 1 つのインターフェイスを提供します。また、最大 150 台の Web セキュリティ アプライアンスに対するポリシー定義とポリシー導入を集中的に管理できます。

セキュリティ管理アプライアンスは、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 アプライアンスから最大のパフォーマンスを確保し、導入の柔軟性を高めることによって企業ネットワークの整合性を保護します。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。

セキュリティ管理アプライアンスによって、安定性、拡張性、および敏速性が備わります。セキュリティ管理アプライアンスは、Web セキュリティ アプライアンスおよび電子メール セキュリティ アプライアンス用の単一の管理プラットフォームであり、システム上のアプライアンスに対する洞察力、制御力、および柔軟性を電子メールおよび Web セキュリティ管理者にもたらします。

（注）　セキュリティ管理アプライアンスは、中央集中型のトラッキング、レポーティング、および隔離管理に対応する堅牢なアプライアンスですが、中央集中型電子メール管理、つまり「クラスタリング」にセキュリティ管理アプライアンスを使用することは推奨されません。

セキュリティ管理アプライアンスでサポートされるサービス

セキュリティ管理アプライアンスは、次のサービスをサポートしています。

- 電子メール セキュリティ管理
- Web セキュリティ管理
- 追加機能

電子メール セキュリティ管理

電子メール管理者にとって、ネットワークの洞察は電子メール管理に不可欠であり、これはレポーティングによって実現されます。電子メール レポートは、電子メール管理者にとって次の 2 つの重要な機能を果たします。

- ネットワーク上の電子メール トラッキングの全体図を示す。
- アンチウイルス、スパム、および着信または発信メールの使用カウンタなど、複数のセキュリティ サービスからのデータを相互に関連させる、直感的なレポートを数量化する。

レポートには、ブロックされたスパムの統計情報や、電子メールに伴う脅威も表示されます。その他のレポートでは、内部ユーザの動作を洞察できるので、企業ポリシーへの準拠を維持するのに役立ちます。これらのレポートは、ボタンをクリックすることで PDF に変換できます。または、簡単に電子メール配信できるようにレポートをスケジュールしたり、電子メールをさらに処理するために CVS にエクスポートしたりすることができます。

セキュリティ管理アプライアンスは、ほぼリアルタイムで複数の電子メール セキュリティ アプライアンスからデータを収集することによって、包括的な洞察を可能にします。レポーティングで洞察が停止することはありません。詳細なメッセージ トラッキングは、準拠の維持や、「1 時間前に送信した電子メールはどうなったか」などの質問に答えるのに役立ちます。

セキュリティ管理アプライアンスは、直感的なユーザ インターフェイス、迅速な検索結果、および検索のインタラクティブな絞り込みを実現するので、電子メール管理者は日常的な検索作業に費やす時間を短縮できます。

セキュリティ管理アプライアンスにおける電子メール セキュリティ アプライアンスの制御は、中央集中型管理機能を介して提供されます。電子メール セキュリティ アプライアンスで使用できるこの機能によって、一貫性と結合性のあるポリシーを一元的に管理できます。管理者は、ユーザ、LDAP グループ メンバーシップ、またはドメイン メンバーシップに応じて、固有のポリシーを設定することを必要とするため、現在、このレベルのポリシー割り当てが可能になりました。役割ベースのアクセスによって、モニタリング タスクを振り分けることができます。

セキュリティ管理アプライアンスが中央集中型スパム隔離を備えていることから、エンド ユーザは独自の隔離を管理できます。

Web セキュリティ管理

Web セキュリティ管理者にとって、ネットワーク上のマルウェア プログラムや疑わしい Web サイトは大きな頭痛の種です。Web セキュリティ アプライアンスは、企業のセキュリティを脅かし、知的財産権を侵害する Web ベースのマルウェアおよびスパイウェア プログラムから企業ネットワークを保護する、堅牢性、安全性、および効率性に優れたデバイスです。Web セキュリティ アプライアンスは、HTTP、HTTPS、および FTP などの標準の通信プロトコルに対する保護が含まれるように、Cisco IronPort の SMTP セキュリティ アプライアンスを拡張します。

悪意のあるプログラムや Web サイトに関する情報にアクセスするには、セキュリティ管理アプライアンスでレポーティングを使用できます。これにより、システム管理者がマルウェアの脅威を確認するための、包括的なセキュリティ レポートが提供されます。さらに、コンプライアンス レポートにより、アクセスが許可されない URL カテゴリに従業員がアクセスしたかどうかを確認できます。これらのレポートおよび他のレポートを Web セキュリティ アプライアンス上で管理することは、セキュリティ管理アプライアンスの非常に重要な機能です。

Web 管理者は、一貫した許容可能な使用ポリシーおよびセキュリティ ポリシーを、組織全体にわたって適用したいと望んでいます。ポリシーは、セキュリティ管理アプライアンスから、複数の AsyncOS バージョンが動作する複数のセキュリティ アプリケーションにプッシュできます。これにより、段階的なネットワーク アップグレードの間も、一貫したポリシー アプリケーションを提供できます。組織内のさまざまな従業員間に責任を配布する機能により、ローカルな優先事項を設定して全体のポリシー制御を行うことができます。ロール ベースのアクセス制御および委任管理により、Web 管理者は、柔軟できめ細かな保護を行うことができます。

さらに、Web 管理者は、ポリシーの変更を監査し、履歴ポリシーをバックアップできます。

追加機能

AsyncOS for Security Management には、次の機能も組み込まれています。

- **外部 Cisco IronPort 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。
- **中央集中型レポーティング：**複数の電子メールおよび Web セキュリティ アプライアンスから集約したデータに対してレポートを実行します。
- **中央集中型トラッキング：**複数の電子メールおよび Web セキュリティ アプライアンスを通過する電子メールおよび Web メッセージを追跡します。

Cisco IronPort Centralized Configuration Manager : 複数の電子メールおよび Web セキュリティ アプライアンスに対するポリシー定義とポリシー導入を管理します。

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

集中管理型の Cisco IronPort ソリューションを設定するには、次の手順に従ってください。

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。「SMA 互換性マトリクス」（P.2-2）を参照してください。

ステップ 2 **すべてのアプライアンス。**必要に応じて、アプライアンスをアップグレードします。

ステップ 3 **電子メール セキュリティ アプライアンス。**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 IronPort AsyncOS for Email Security*』マニュアルを参照してください。

ステップ 4 **Web セキュリティ アプライアンス。**中央集中型サービスを環境に取り入れる前に、必要なセキュリティ機能が提供されるように少なくとも 1 つの Web セキュリティ アプライアンスを設定し、すべての機能が予期したとおりに動作することを確認します。『*Cisco IronPort AsyncOS for Web Security User Guide*』を参照してください。

ステップ 5 **セキュリティ管理アプライアンス。**アプライアンスを設定し、システム セットアップ ウィザードを実行します。「設置計画」（P.2-4）、「セットアップの準備」（P.2-6）、および「システム セットアップ ウィザードの実行」（P.2-10）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。**導入する各中央集中型サービスを設定します。「セキュリティ管理アプライアンスでのサービスの設定」（P.2-17）から開始します。

SMA 互換性マトリクス

ここでは、今回リリースの AsyncOS for Security Management と、電子メール セキュリティ アプライアンスおよび Web セキュリティ アプライアンスに対応する各 AsyncOS リリースとの互換性について説明します。さらに、サポートされるコンフィギュレーション ファイルの表も示してあります。

（注）　（Web セキュリティ アプライアンスのある導入環境の場合）Web セキュリティ アプライアンスは、前の 2 つのメジャー バージョンまで、そのコンフィギュレーション データの後方互換性を維持します。ソースおよびターゲット アプライアンスでのソフトウェアのバージョンによっては、アップグレードが セキュリティ管理アプライアンスの機能に影響を与える可能性があることに注意してください。

表 2-1　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 アプライアンスの互換性

バージョン	レポート	トラッキング	セーフリスト/ブロックリスト	ISQ
ESA 6.3	サポートなし	サポートなし	サポートなし	サポート
ESA 6.4	サポート	サポート	サポート	サポート
ESA 6.5	サポート	サポート	サポート	サポート
ESA 7.0	サポート	サポート	サポート	サポート
ESA 7.1	サポート	サポート	サポート	サポート
ESA 7.3	サポート	サポート	サポート	サポート
ESA 7.5	サポート	サポート	サポート	サポート
ESA 7.6	サポート	サポート	サポート	サポート

表 2-2　セキュリティ管理アプライアンスと Web セキュリティ アプライアンスの互換性

バージョン	中央集中レポーティングおよびトラッキング	ICCM 公開[a]	Web セキュリティ アプライアンス への拡張ファイル公開
WSA 5.7	機能は使用不可	サポートなし	コンフィギュレーション ファイルのバージョンは、ターゲットの WSA バージョンと一致している必要があります。
WSA 6.0	機能は使用不可	サポートなし	サポートなし
WSA 6.3	機能は使用不可	6.3 の Configuration Master でサポート	コンフィギュレーション ファイルのバージョンは、ターゲットの WSA バージョンと一致している必要があります。
WSA 7.0	機能は使用不可	6.3 の Configuration Master でサポート	コンフィギュレーション ファイルのバージョンは、ターゲットの WSA バージョンと一致している必要があります。
WSA 7.1	サポート	6.3 と 7.1 の Configuration Master でサポート	コンフィギュレーション ファイルのバージョンは、ターゲットの WSA バージョンと一致している必要があります。
WSA 7.5	サポート	6.3、7.1、および 7.5 の Configuration Master でサポート Configuration Master 7.5 を強く推奨します。	コンフィギュレーション ファイルのバージョンは、ターゲットの WSA バージョンと一致している必要があります。

a. 表内の ICCM 公開行と拡張ファイル公開行の公開先は Web セキュリティ アプライアンスです。

表 2-3　（WSA のある導入のみ）Configuration Master の互換性

ターゲット Configuration Master のバージョン：	ソース Configuration Master のバージョン：	ソース コンフィギュレーション ファイルが存在する Web セキュリティ アプライアンスのバージョン：
6.3	N/A	Web セキュリティ アプライアンス 6.3
7.1	Configuration Master 6.3	Web セキュリティ アプライアンス 7.1
7.5	Configuration Master 6.3 または 7.1	Web セキュリティ アプライアンス 7.5

設置計画

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

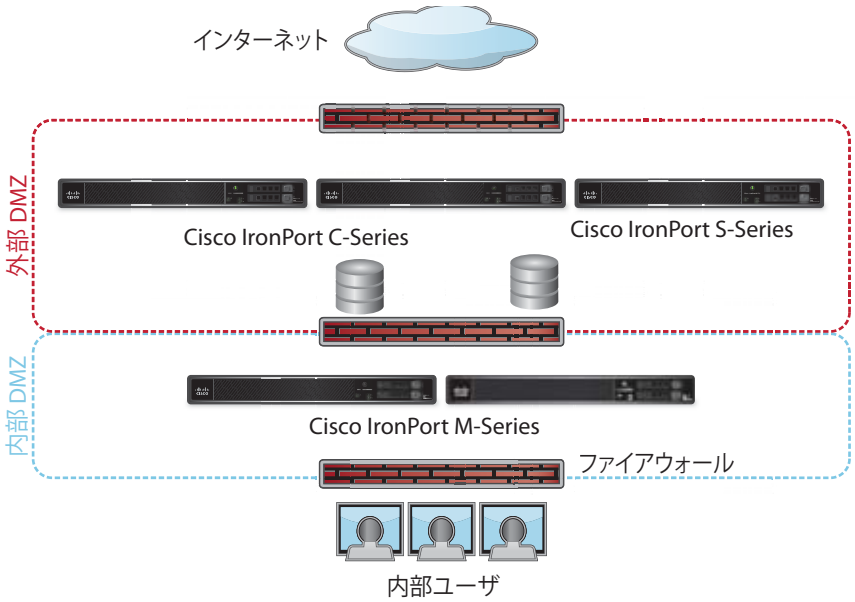


図 2-1 に、セキュリティ管理アプライアンスと複数の DMZ を含む一般的なネットワーク設定を示します。内部ネットワークで、DMZ の外側に セキュリティ管理アプライアンスを導入します。管理対象電子メール セキュリティ アプライアンス（Cisco IronPort C-Series）および管理対象 Web セキュリティ アプライアンス（Cisco IronPort S-Series）へのすべての接続は、セキュリティ管理アプライアンス（Cisco IronPort M-Series）によって開始されます。

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

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の物理的寸法

Cisco IronPort M1000/1050 および M600/650 セキュリティ管理アプライアンスには、次の物理的寸法が適用されます。

- 高さ：8.656 cm（3.40 インチ）
- 幅：レールを取り付けて 48.26 cm（19.0 インチ）（レールを取り付けない場合は 17.5 インチ）
- 奥行：75.68 cm（29.79 インチ）
- 重量：最大 26.76 kg（59 ポンド）

Cisco IronPort M1070 および 670 セキュリティ管理アプライアンスには、次の物理的寸法が適用されます。

- 高さ：8.64 cm（3.40 インチ）
- 幅：レールの取り付け有無によらず 48.24 cm（18.99 インチ）
- 奥行：72.06 cm（28.40 インチ）
- 重量：最大 26.76 kg（59 ポンド）

Cisco IronPort M170 セキュリティ管理アプライアンスには、次の物理的寸法が適用されます。

- 高さ：4.1 cm（1.625 インチ）
- 幅：レールの取り付け有無によらず 48.26 cm（19.0 インチ）
- 奥行：39.7 cm（15.625 インチ）
- 重量：6.53 kg（14.40 ポンド）

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、『*Cisco IronPort AsyncOS for Email Security Configuration Guide*』の「Cisco IronPort M-Series Security Management Appliance」の章を参照してください。（「M シリーズ アプライアンス」はセキュリティ管理アプライアンスの別の表現です）。

中央集中型管理とセキュリティ管理アプライアンス

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

セットアップの準備

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

ステップ 1　セキュリティ ソリューションのコンポーネントに互換性があることを確認します。「SMA 互換性マトリクス」（P.2-2）を参照してください。

ステップ 2　この導入に対応できるネットワークと物理的空間の準備があることを確認します。「設置計画」（P.2-4）を参照してください。

ステップ 3　セキュリティ管理アプライアンスを物理的に設定し、接続します。「アプライアンスの物理的なセットアップと接続」（P.2-6）を参照してください。

ステップ 4　ネットワーク アドレスと IP アドレスの割り当てを決定します。「ネットワーク アドレスと IP アドレスの割り当ての決定」（P.2-6）を参照してください。

ステップ 5　システム セットアップに関する情報を収集します。「セットアップ情報の収集」（P.2-7）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

この章の手順を実行する前に、アプライアンスに付属の『*Cisco IronPort M-Series Quickstart Guide*』に記載された手順を実行してください。

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

出荷時に割り当てられた管理ポートの 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 [Management Appliance] > [Network] > [IP Interfaces] ページに移動し、セキュリティ管理アプライアンスが使用するインターフェイスを変更します。

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

- IP アドレス
- ネットマスク

さらに、ネットワーク全体に関する次の情報も必要になります。

- ネットワークのデフォルト ルータ（ゲートウェイ）の IP アドレス
- DNS サーバの IP アドレスおよびホスト名（インターネット ルート サーバを使用する場合は不要）
- NTP サーバのホスト名または IP アドレス（システム時刻を手動で設定する場合は不要）

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

（注）　インターネットと Cisco IronPort 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、Cisco IronPort アプライアンスを正常に機能させるために、特定のポートを開ける必要がある場合があります。ファイアウォールの詳細については、付録 C「ファイアウォール情報」を参照してください。

（注）　電子メール セキュリティ アプライアンスとの間で電子メール メッセージを送受信するには、常にセキュリティ管理アプライアンスで同じ IP アドレスを使用してください。詳細については、『*Cisco IronPort AsyncOS for Email Security Configuration Guide*』の「Mail Flow and the IronPort M-Series Appliance」を参照してください。

セットアップ情報の収集

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

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

表 2-4　システム セットアップ ワークシート

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

セキュリティ管理アプライアンスへのアクセス

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

グラフィカル ユーザ インターフェイスへのアクセス

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　工場で割り当てられた次のユーザ名とパスワードを対応するテキスト フィールドに入力します。

- ユーザ名：**admin**
- パスワード：**ironport**

（注）　デフォルトでは、30 分以上アイドル状態になっている場合、またはログアウトせずにブラウザを閉じた場合は、セッションがタイムアウトします。この場合、ユーザ名とパスワードを再入力する必要があります。システム セットアップ ウィザードを実行中にセッションがタイムアウトした場合は、最初からやり直す必要があります。タイムアウト制限を変更するには、「Web UI セッション タイムアウトの設定」（P.12-22）を参照してください。

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

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

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。サポートされるブラウザには、次のものが含まれます。

- Internet Explorer 9.0（Windows 7 のみ）、8.0、および 7.0
- Safari 4.0 以降
- Firefox 4.x および 3.6x
- Google Chrome

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。

（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。

サポートされる言語

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

- 英語
- フランス語
- スペイン語
- ドイツ語
- イタリア語

- 韓国語
- 日本語
- ポルトガル語（ブラジル）
- 中国語（繁体字および簡体字）
- ロシア語

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

- 言語を設定します。「プリファレンスの 設定」（P.13-60）を参照してください。
- GUI ウィンドウの右上にある [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）。

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

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

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

システム セットアップ ウィザードの実行

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

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

はじめる前に

「セットアップの準備」（P.2-6）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」（P.12-22）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

ステップ 1　エンド ユーザ ライセンス契約書の確認

ステップ 2　次に示すシステム設定の実行：

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

ステップ 3　次に示すネットワーク設定の実行：

- アプライアンスのホスト名
- アプライアンスの IP アドレス、ネットワーク マスク、およびゲートウェイ
- デフォルト ルータと DNS 設定

ステップ 4　設定の確認

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

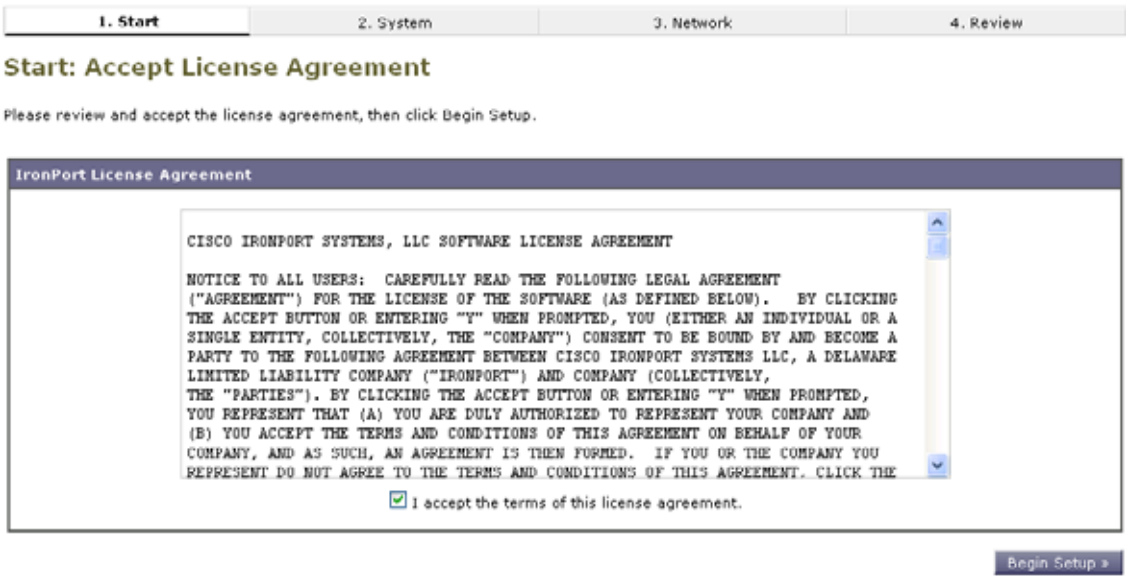
システム セットアップ ウィザードの起動

ウィザードを起動するには、「グラフィカル ユーザ インターフェイスへのアクセス」（P.2-8）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、[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（[Management Appliance] > [System Administration] > [System Setup Wizard]）。

エンド ユーザ ライセンス契約書を確認します。

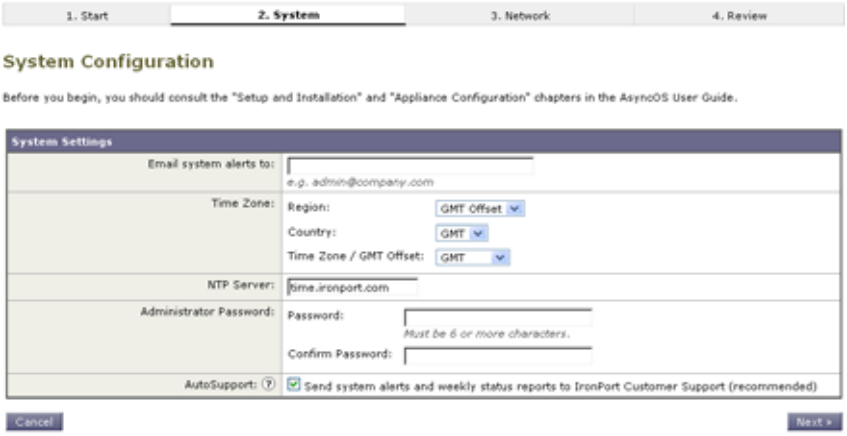
ライセンス契約書の参照から開始します。ライセンス契約書を参照し、同意する場合は、同意することを示すチェックボックスをオンにし、[Begin Setup] をクリックして続行します。

図 2-2　ライセンス契約書の確認



システムの設定

図 2-3　[System Configuration] ページでのシステム設定の実行



システム アラート用の電子メール アドレスの入力

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

システム アラート用の電子メール アドレスを 1 つ以上追加する必要があります。複数のアドレスを指定する場合は、カンマで区切ります。入力した電子メール アドレスでは、当初、すべてのレベルのすべてのタイプのアラートが受信されます。アラート設定は、後からカスタマイズできます。詳細については、「アラートの管理」（P.13-34）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）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 IronPort Systems のタイム サーバ（time.IronPort.com）が、セキュリティ管理アプライアンス上で時刻を同期する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、[Add Entry] をクリックして追加の NTP サーバを設定します。詳細については、「システム時刻の設定」（P.13-47）を参照してください。

（注）　レポートのデータを収集すると、セキュリティ管理アプライアンスによってデータにタイム スタンプが適用されます。タイム スタンプは、「システム時刻の設定」（P.13-47）の手順で実装された設定を使用して適用されます。
セキュリティ管理アプライアンスがデータを収集する方法の詳細については、「セキュリティ アプライアンスによるレポート用データの収集方法」（P.3-2）を参照してください。

パスワードの設定

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

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

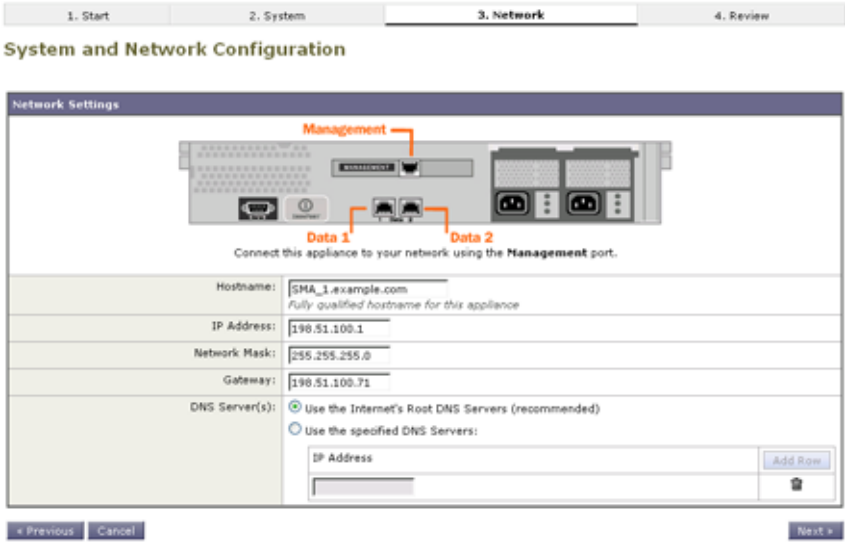
AutoSupport のイネーブル化

Cisco IronPort AutoSupport 機能（デフォルトでイネーブル）で、セキュリティ管理アプライアンスに関する問題を Cisco IronPort カスタマー サポートに通知することにより、最適なサポートを提供できます。詳細については、「Cisco IronPort AutoSupport」（P.13-36）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。

図 2-4　ネットワーク設定の実行



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

ネットワーク設定

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

セキュリティ管理アプライアンスの IP アドレスを入力します。

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

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

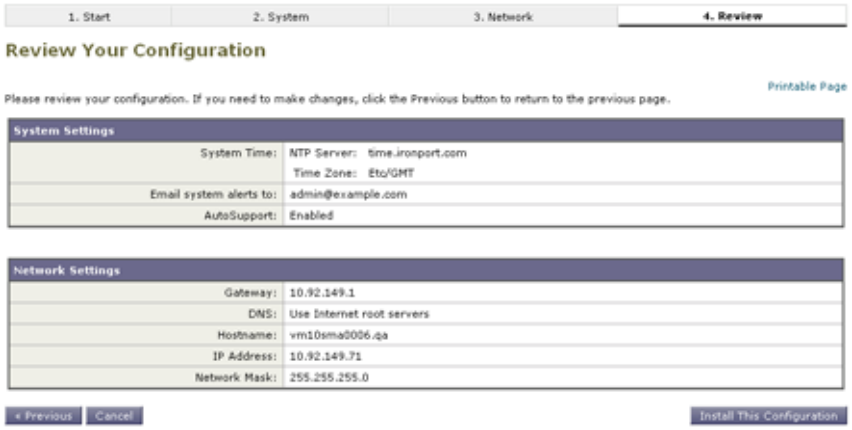
（注）　指定した DNS サーバの初期プライオリティは 0 です。詳細については、「ドメイン ネーム システム設定値の設定」（P.13-43）を参照してください。

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

設定の確認

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

図 2-5　　設定の確認

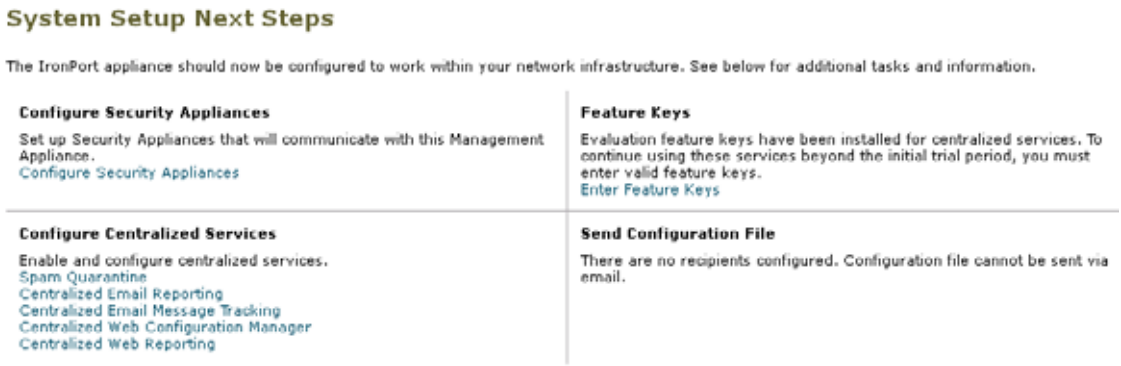


情報を確認した後、[Install This Configuration] をクリックします。次に、表示される確認ダイアログ ボックスで [Install] をクリックします。

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、[System Setup Next Steps] ページが表示されます。

図 2-6　　システム セットアップ：次の手順



[System Setup Next Steps] ページのいずれかのリンクをクリックして、Cisco IronPort アプライアンスの設定を続行します。

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

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

管理対象アプライアンスの追加について

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

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

リモート アプライアンスを追加すると、セキュリティ管理アプライアンスによって、リモート アプライアンスの製品名と追加するアプライアンスのタイプが比較されます。たとえば、[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。

[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。[Connection Established?] カラムは、モニタリング サービスの接続が適切に設定されているかどうかを示します。

管理対象アプライアンスの追加方法は、次の手順に含まれています。

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

管理対象アプライアンスの編集と削除

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後、設定の編集または削除が必要になることがあります。

管理対象アプライアンスの設定の編集

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

ステップ 2　[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　[Submit] をクリックして、ページ上の変更を送信し、[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

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

ステップ 2　[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 [Delete] をクリックします。

ステップ 4　[Submit] をクリックし、[Commit Changes] をクリックして変更を保存します。

セキュリティ管理アプライアンスでのサービスの設定

セキュリティ管理アプライアンスで 1 つまたは複数のセキュリティ サービスを設定し、使用するには、次の情報を参照してください。

電子メール セキュリティ サービス：

- 第 4 章「中央集中型電子メール セキュリティ レポーティングの使用」
- 第 6 章「電子メール メッセージのトラッキング」
- 第 7 章「Cisco IronPort スパム隔離の管理」

Web セキュリティ サービス：

- 第 5 章「中央集中型 Web レポーティングの使用方法」
- 第 8 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

セキュリティ管理アプライアンス GUI で設定を変更する場合、[Commit Changes] ボタンをクリックして、その変更を明示的に確定する必要があります。変更を行わなかった場合、[Commit Changes] の代わりに [No Changes] が表示されます。

図 2-7　[Commit Changes] ボタン

[Commit Changes] をクリックすると、コメントの追加と変更の確定、最新の確定以降に行ったすべての変更の破棄、またはキャンセルを行うことができるページが表示されます。変更が送信されると、[Commit Changes] の色がオレンジに変化します。

変更の破棄

変更をコミットせずにキャンセルするには、[Commit Changes] ボタンをクリックしてから、[Abandon Changes] をクリックします。

CHAPTER 3

レポートでの作業

レポーティングに関する次のトピックは、電子メール レポートと Web レポートの両方に共通します。

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
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	• 「インタラクティブ レポート ページのビューのカスタマイズ」（P.3-3） • 第 4 章「中央集中型電子メール セキュリティ レポーティングの使用」 • 第 5 章「中央集中型 Web レポーティングの使用方法」
反復するレポートを自動的に生成する	• 「電子メール レポートのスケジュール設定」（P.4-55） • 「Web レポートのスケジュール設定」（P.5-63）
レポートをオンデマンドで生成する	• 「オンデマンドでの電子メール レポートの生成」（P.4-56） • 「オンデマンドでの Web レポートの生成」（P.5-67）

表 3-1　レポーティング データを表示する方法（続き）

目的	参照先
raw データを CSV（カンマ区切り）ファイルとしてエクスポートする	• 「レポート データの印刷とエクスポート」（P.3-7） • 「カンマ区切り（CSV）ファイルとしてのレポート データのエクスポート」（P.3-8）
レポート データの PDF を生成する	「レポート データの印刷とエクスポート」（P.3-7）
レポート情報を自分自身や他のユーザに電子メールで送信する	• 「オンデマンドでの電子メール レポートの生成」（P.4-56） • 「電子メール レポートのスケジュール設定」（P.4-55） • 「オンデマンドでの Web レポートの生成」（P.5-67） • 「Web レポートのスケジュール設定」（P.5-63）
スケジュールされたレポートまたはオンデマンド レポートのアーカイブ済みのコピーを、システムから削除されるまで表示する	「アーカイブされた Web レポートの表示と管理」（P.5-69）
特定のトランザクションに関する情報を検索する	「[Web Tracking] ページ」（P.5-51）

（注）　ロギングとレポーティングの違いについては、「ロギングとレポーティング」（P.14-1）を参照してください。

セキュリティ アプライアンスによるレポート用データの収集方法

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

（注）　セキュリティ管理アプライアンスは、レポートのデータを収集する際に、セキュリティ管理アプライアンス上で時間設定を行った際に設定した情報からタイム スタンプを適用します。セキュリティ管理アプライアンス上の時間設定の詳細については、「システム時刻の設定」（P.13-47）を参照してください。

レポーティング データの保存方法

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

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

	毎分	毎時	毎日	毎週	毎月	毎年
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		•	•	•	•	•

インタラクティブ レポート ページのビューのカスタマイズ

インタラクティブ レポート ページを表示する場合は、次のことを行ってビューをカスタマイズできます。

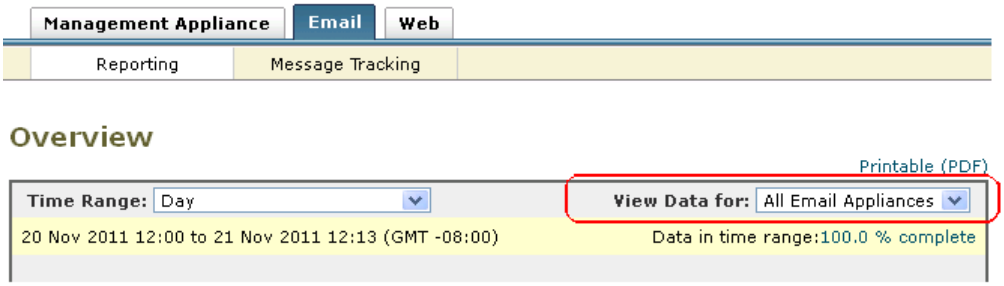
- **アプライアンスごとに、特定のレポートのみのデータを表示する**。詳細については、「アプライアンスによるレポーティング データの制約」（P.3-3）を参照してください。
- **時間範囲を指定する**。詳細については、「インタラクティブ レポートの時間範囲の選択」（P.3-4）を参照してください。
- **（Web レポートの場合）チャート化するデータを選択する**。「（Web レポートのみ）チャート化するデータの選択」（P.3-5）を参照してください。
- **テーブルをカスタマイズする**。「レポート ページのテーブルのカスタマイズ」（P.3-5）を参照してください。
- **表示する特定の情報またはデータのサブセットを検索する**。電子メール レポートについては、「検索およびインタラクティブ電子メール レポート ページ」（P.4-6）を参照してください。Web レポートについては、ほとんどのテーブルの下方にある [Find] オプションまたは [Filter] オプションを探してください。

（注）　すべてのレポートにすべてのインタラクティブな機能を使用できるわけではありません。

アプライアンスによるレポーティング データの制約

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

ビューを指定するには、サポートされるページの [View Data for] リストからアプライアンスを選択します。



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、[Management Appliance] > [Centralized Services] > [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）。

インタラクティブ レポートの時間範囲の選択

ほとんどのインタラクティブ 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、[Time Range] メニューで異なる値を選択するまで、すべてのレポート ページを通して使用されます。

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
Hour	過去 60 分間と最大 5 分間の延長時間		•		•
Day	過去 24 時間	•	•	•	•
Week	当日の経過時間を含む、過去 7 日間	•	•	•	•
30 days	当日の経過時間を含む、過去 30 日間	•	•	•	•
90 days	当日の経過時間を含む、過去 90 日間	•	•	•	
Year	過去 12 ヵ月と現在月の経過日数	•			
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）	•	•	•	•
Previous Calendar Month	月の第 1 日目の 00:00 からその月の最終日の 23:59 まで	•	•	•	
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）　インタラクティブ 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。

ヒント　ログインするたびに常に表示する、デフォルトの時間範囲を指定できます。詳細については、「プリファレンスの 設定」（P.13-60）を参照してください。

（Web レポートのみ）チャート化するデータの選択

各 Web レポーティング ページのデフォルト チャートには、一般に参照されるデータが表示されますが、代わりに異なるデータをチャート化するように選択できます。ページに複数のチャートがある場合は、チャートごとに変更できます。

通常、チャートのオプションは、レポート内のテーブルのカラムと同じです。ただし、チャート化できないカラムもあります。カラムの見出しについては、「Web レポーティング ページのテーブル カラムの説明」（P.5-10）を参照してください。

チャートには、関連付けられたテーブルに表示するように選択した項目（行）数に関係なく、テーブル カラムの使用可能なすべてのデータが反映されます。

ステップ 1　チャートの下の [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　[Done] をクリックします。

レポート ページのテーブルのカスタマイズ

表 3-4　Web レポート ページのテーブルのカスタマイズ

目的	操作内容	追加情報
• 追加のカラムを表示する • 表示可能なカラムを非表示にする • テーブルに使用可能なカラムを判断する	テーブルの下の [Columns] リンクをクリックし、表示するカラムを選択して、[Done] をクリックします。	ほとんどのテーブルでは、デフォルトで一部のカラムが非表示になります。 レポート ページごとに、異なるカラムが提供されます。 カラムの詳細については、次の項を参照してください。 • 「電子メール レポーティング ページのテーブル カラムの説明」（P.4-9） • 「Web レポーティング ページのテーブル カラムの説明」（P.5-10）
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。	—

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	追加情報
選択した見出しでテーブルをソートする	カラムの見出しをクリックします。	—
表示するデータの行数を加減する	テーブルの右上にある [Items Displayed] ドロップダウン リストから、表示する行数を選択します。	Web レポートの場合、デフォルトの表示行数を設定することもできます。「プリファレンスの 設定」（P.13-60）を参照してください。
可能な場合は、テーブル エントリの詳細を表示する	テーブル内の青色のエントリをクリックします。	—
データのプールを特定のサブセットに絞り込む	可能な場合は、テーブルの下のフィルタ設定で値を選択するか、入力します。	Web レポートの使用可能なフィルタについては、各レポート ページの説明に記載されています。「Web レポーティング ページについて」（P.5-7）を参照してください。

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（[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 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 [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

- [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 [Last Year] レポートに影響を与えます。

  - Internal Users
  - Internal User Details
  - IP Addresses for Outgoing Senders
  - Content Filters

- [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 [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。

レポート データの印刷とエクスポート

表 3-5　レポート データの印刷とエクスポート

取得対象	PDF	CSV	操作内容	コメント
インタラクティブ レポート ページの PDF	•		インタラクティブ レポート ページの右上にある [Printable (PDF)] リンクをクリックします。	PDF には、現在表示しているカスタマイゼーションが反映されます。 PDF は、プリンタ対応の形式に設定されます。
レポート データの PDF	•		スケジュール設定されたレポートまたはオンデマンドのレポートを作成します。次の各項を参照してください。 • 「オンデマンドでの電子メール レポートの生成」（P.4-56） • 「電子メール レポートのスケジュール設定」（P.4-55） • 「オンデマンドでの Web レポートの生成」（P.5-67） • 「Web レポートのスケジュール設定」（P.5-63）	—

表 3-5　レポート データの印刷とエクスポート（続き）

取得対象	PDF	CSV	操作内容	コメント
raw データ		•	チャートまたはテーブルの下にある [Export] リンクをクリックします。	CSV ファイルには、チャートまたはテーブルに表示できるデータだけではなく、適用可能な最大限のデータがすべて含まれます。
「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」（P.3-8）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。次の各項を参照してください。 • 「オンデマンドでの電子メール レポートの生成」（P.4-56） • 「電子メール レポートのスケジュール設定」（P.4-55） • 「オンデマンドでの Web レポートの生成」（P.5-67） • 「Web レポートのスケジュール設定」（P.5-63）	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、または韓国語で PDF を生成するには、該当するフォント パックを Adobe.com からダウンロードして、ローカル コンピュータにインストールする必要があります。
（Web セキュリティ）レポート データのカスタム サブセット（特定のユーザ用のデータなど）。	•	•	[Web Tracking] で検索を実行し、[Web Tracking] ページの [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、最大 1,000 件のトランザクションが含まれます。 CSV ファイルには、検索条件に一致するすべての raw データが含まれます。
（電子メール セキュリティ）データのカスタム サブセット（特定のユーザ用のデータなど）。		•	[Message Tracking] で検索を実行し、結果の上にある [Export] リンクをクリックします。	メッセージ トラッキング検索結果および CSV ファイルには最大 250 件の結果が含まれます。

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

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、「レポート データの印刷とエクスポート」（P.3-7）を参照してください。

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	アドウェア	マルウェア カテゴリの名前。
Transactions Monitored	525	モニタリングされたトランザクション数。
Transactions Blocked	2100	ブロックされたトランザクション数。
Transactions Detected	2625	トランザクションの合計数： 検出されたトランザクション数 + ブロックされたトランザクション数。

（注） カテゴリ ヘッダーは、レポートのタイプごとに異なります。

ローカライズされた CSV データをエクスポートすると、ブラウザによっては見出しが正しく表示されない場合があります。これは、ブラウザによっては、ローカライズされたテキストに対して適切な文字セットが使用されない場合があることから発生します。この問題の回避策としては、ローカル マシンにファイルを保存し、[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におけるサブドメインとセカンドレベル ドメインの比較

レポーティングおよびトラッキングの検索では、セカンドレベルのドメイン（http://george.surbl.org/two-level-tlds に表示されている地域ドメイン）は、ドメイン タイプがサブドメインと同じように見えますが、サブドメインとは別の方法で処理されます。次に例を示します。

- レポートには、co.uk などの 2 レベルのドメインの結果は含まれませんが、foo.co.uk の結果は含まれます。レポートには、cisco.com などの主要な企業ドメインの下にサブドメインが含まれます。
- 地域ドメイン co.uk に対するトラッキング検索結果には、foo.co.uk などのドメインは含まれませんが、cisco.com に対する検索結果には subdomain.cisco.com などのサブドメインが含まれます。

電子メール レポートおよび Web レポート

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

Web レポートに固有の情報については、第 5 章「中央集中型 Web レポーティングの使用方法」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

電子メール レポーティング機能は、電子メール 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、個々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情報を集約します。リアルタイムでレポートを実行して、特定の期間のシステム アクティビティをインタラクティブに表示することも、レポートをスケジュール設定して、定期的に実行することもできます。また、レポーティング機能を使用して、raw データをファイルにエクスポートすることもできます。

中央集中型電子メール レポーティング機能は、概要レポートを生成してネットワークで起きていることを把握できるだけでなく、特定のドメイン、ユーザ、またはカテゴリのトラフィックの詳細を、ドリルダウンして確認できます。

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

（注） 電子メール セキュリティ アプライアンスでデータが保存されるのは、ローカル レポーティングが使用される場合だけです。中央集中型レポーティングを電子メール セキュリティ アプライアンスに対してイネーブルにした場合、電子メール セキュリティ アプライアンスでは、システム キャパシティおよびシステム ステータス以外のレポーティング データは保持されません。中央集中型電子メール レポーティングがイネーブルでない場合、生成されるレポートはシステム ステータスとシステム キャパシティだけです。詳細については、『*Cisco IronPort AsyncOS for Email Security Configuration Guide*』の「Centralized Reporting Mode」を参照してください。

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、『*Cisco IronPort AsyncOS for Email Security Configuration Guide*』の「Centralized Reporting Mode」を参照してください。

中央集中型電子メール レポーティングの設定

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

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

「電子メール レポーティング グループの作成」（P.4-4）も参照してください。

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

セキュリティ管理アプライアンスに電子メール レポーティングを集中化するには、このサービスをイネーブルにする必要があります。

（注）　次の手順は、電子メール セキュリティ アプライアンスをすでにセキュリティ管理アプライアンスに追加していることを前提としています。詳細については、「管理対象アプライアンスの追加について」（P.2-16）を参照してください。

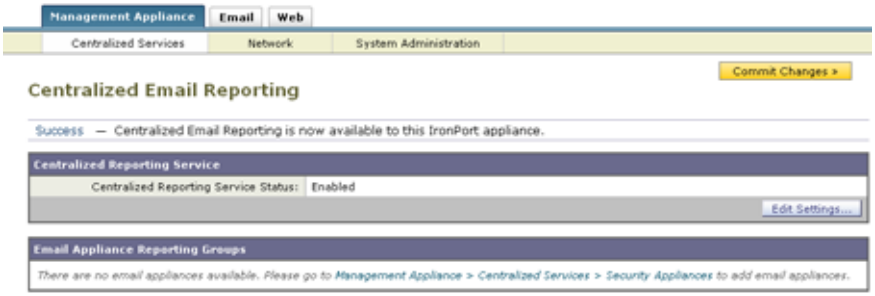
（注）　中央集中型電子メール レポーティングをイネーブルにする前に、十分なディスク領域がサービスに割り当てられていることを確認します。「ディスク使用量の管理」（P.13-58）を参照してください。

ステップ 1　セキュリティ管理アプライアンスで、[Management Appliance] > [Centralized Services] > [Email] > [Centralized Reporting] を選択します。

ステップ 2　[Enable] をクリックします。

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

セキュリティ管理アプライアンスで中央集中型レポーティングが正常にイネーブルになったことを知らせる、次のウィンドウが表示されます。



ステップ 3　[Submit] をクリックして、ページ上の変更を送信し、[Commit Changes] をクリックして変更を保存します。

（注）　アプライアンスで電子メール レポーティングがイネーブルになっていて、この処理にディスク領域が割り当てられていない場合、ディスク領域が割り当てられるまで、中央集中型電子メール レポーティングが機能しません。電子メール レポーティングおよびトラッキングに設定するクォータが、現在使用しているディスク領域よりも大きい場合、レポーティングおよびトラッキングのデータは失われません。詳細については、「ディスク使用量の管理」（P.13-58）を参照してください。

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

中央集中型レポーティングをイネーブルにする前に、すべての電子メール 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。

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

手順については、『*Cisco IronPort AsyncOS for Email Security Configuration Guide*』の「Configuring an Email Security Appliance to Use Centralized Reporting」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。

ステップ 1　セキュリティ管理アプライアンスで、[Management Appliance] > [Centralized Services] > [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.　[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. [Add Email Appliance] をクリックします。

b. [Appliance Name and IP Address] テキスト フィールドに、Cisco IronPort アプライアンスの管理インターフェイスのアプライアンス名と IP アドレスを入力します。

（注） [IP Address] テキスト フィールドに DNS 名を入力した場合でも、[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. [Centralized Reporting] サービスが事前に選択されています。

d. [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、[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. [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. [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　[Submit] をクリックします。

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

ステップ 6　変更を保存します。

電子メール レポーティング 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。

電子メール レポーティング グループの追加

ステップ 1　セキュリティ管理アプライアンスで、[Management Appliance] > [Centralized Services] > [Centralized Reporting] を選択します。

ステップ 2　[Add Group] をクリックします。

ステップ 3　グループの一意の名前を入力します。

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

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

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

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

ステップ 5　[Submit] をクリックして、ページ上の変更を送信し、[Commit Changes] をクリックして変更を保存します。

（注）　アプライアンスを、複数のグループに含めることができます。

電子メール レポーティング グループの編集と削除

ステップ 1　[Management Appliance] > [Centralized Services] > [Centralized Reporting] を選択します。

ステップ 2　グループを削除するには、削除するグループの横にある対応するゴミ箱アイコンをクリックします。

または

グループを編集するには、編集するグループの名前をクリックしてから編集します。

ステップ 3　変更を送信し、保存します。

インタラクティブ電子メール レポーティング ページでの作業

- レポート データのアクセスおよび表示に関するオプションついては、「レポーティング データを表示する方法」（P.3-1）を参照してください。
- 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には、「インタラクティブ レポート ページのビューのカスタマイズ」（P.3-3）を参照してください。
- データ内の特定の情報を検索するには、「検索およびインタラクティブ電子メール レポート ページ」（P.4-6）を参照してください。
- レポート情報を印刷またはエクスポートするには、「レポート データの印刷とエクスポート」（P.3-7）を参照してください。
- さまざまなインタラクティブ レポート ページを理解するには、「電子メール レポーティング ページの概要」（P.4-7）を参照してください。
- レポートをオンデマンドで生成するには、「オンデマンドでの電子メール レポートの生成」（P.4-56）を参照してください。
- 指定した間隔および時刻に自動的に実行されるようにレポートをスケジュール設定するには、「電子メール レポートのスケジュール設定」（P.4-55）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、「[Archived Email Reports] の表示と管理」（P.4-58）を参照してください。

- バックグラウンド情報については、「セキュリティ アプライアンスによるレポート用データの収集方法」（P.3-2）を参照してください。
- 大量のデータを処理するときにパフォーマンスを向上させるには、「電子メール レポートのパフォーマンスの向上」（P.3-6）を参照してください。

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

多数のインタラクティブ電子メール レポーティング ページには、[Search For:] ドロップダウン メニューがあります。

次の図に、[Search For] ドロップダウン メニューを示します。

ドロップダウン メニューから、次のような数種類の条件で検索できます。

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

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

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

IPv6 検索の場合、次の例の形式を使用して、アドレスを入力できます。

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

電子メール レポーティング ページの概要

表 4-1　[Email Reporting] タブのオプション

[Email Reporting] メニュー	アクション
電子メール レポーティングの [Overview] ページ	[Overview] ページには、Cisco IronPort 電子メール アプライアンスでのアクティビティの概要が表示されます。これには、着信および発信メッセージに関するグラフやサマリー テーブルが含まれます。 詳細については、「電子メール レポーティングの [Overview] ページ」（P.4-11）を参照してください。
[Incoming Mail] ページ	[Incoming Mail] ページには、管理対象の 電子メール セキュリティ アプライアンスに接続されているすべてのリモート ホストのリアルタイム情報の、インタラクティブなレポートが表示されます。システムに電子メールを送信している IP アドレス、ドメイン、およびネットワーク オーナー（組織）の情報を収集できます。 詳細については、「[Incoming Mail] ページ」（P.4-15）を参照してください。
[Outgoing Destinations] ページ	[Outgoing Destinations] ページに、組織が電子メールを送信する宛先のドメインについての情報が表示されます。ページの上部には、発信脅威メッセージごとの上位の宛先、および発信クリーン メッセージ別の上位の宛先を示すグラフが表示されます。ページの下部には、総受信者数別にソートされた（デフォルト設定）カラムを示す表が表示されます。 詳細については、「[Outgoing Destinations] ページ」（P.4-25）を参照してください。
[Outgoing Senders] ページ	[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、「[Outgoing Senders] ページ」（P.4-27）を参照してください。
[Internal Users] ページ	[Internal Users] には、*電子メール アドレスごと* に内部ユーザによって送受信された電子メールについての情報が表示されます。1 人のユーザが複数の電子メール アドレスを持っている場合があります。レポートでは、電子メール アドレスがまとめられません。 詳細については、「[Internal Users] ページ」（P.4-28）を参照してください。
[DLP Incident Summary] ページ	[DLP Incident Summary] ページには、送信メールで発生した Data Loss Prevention（DLP）ポリシー違反インシデントに関する情報が示されます。 詳細については、「[DLP Incident Summary] ページ」（P.4-31）を参照してください。

表 4-1　[Email Reporting] タブのオプション （続き）

[Email Reporting] メニュー	アクション
[Content Filters] ページ	[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。[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、「[Content Filters] ページ」（P.4-33）を参照してください。
[Virus Types] ページ	[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。[Virus Types] ページには、電子メール セキュリティ アプライアンスで稼働し、セキュリティ管理アプライアンスに表示されるウイルス スキャン エンジンによって検出されたウイルスが表示されます。このレポートを使用して、特定のウイルスに対して処置を行います。 詳細については、「[Virus Types] ページ」（P.4-35）を参照してください。
[TLS Connections] ページ	[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 Connections] ページ」（P.4-37）を参照してください。
[Rate Limits] ページ	[Rate Limits] ページには、送信者ごとのメッセージ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、「[Rate Limits] ページ」（P.4-40）を参照してください。
[Outbreak Filters] ページ	[Outbreak Filters] ページには、ウイルス感染フィルタによって隔離された最近のアウトブレイクやメッセージに関する情報が示されます。このページを使用して、ウイルス攻撃に対する防御をモニタします。 詳細については、「[Outbreak Filters] ページ」（P.4-41）を参照してください。
[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、「[System Capacity] ページ」（P.4-43）を参照してください。
[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、「[Reporting Data Availability] ページ」（P.4-48）を参照してください。

表 4-1　[Email Reporting] タブのオプション （続き）

[Email Reporting] メニュー	アクション
電子メール レポートのスケジュール設定	指定した時間範囲のレポートのスケジュールを設定できます。詳細については、「電子メール レポートのスケジュール設定」（P.4-55）を参照してください。
[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、「[Archived Email Reports] の表示と管理」（P.4-58）を参照してください。 また、オンデマンド レポートを生成することもできます。「オンデマンドでの電子メール レポートの生成」（P.4-56）を参照してください。

電子メール レポーティング ページのテーブル カラムの説明

表 4-2　電子メール レポーティング ページのテーブル カラムの説明

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

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

カラム名	説明
Stopped by Reputation Filtering	[Stopped by Reputation Filtering] の値は、次の複数の要素に基づいて算出されます。 • この送信者からの「調整された」メッセージの数 • 拒否された、または TCP 拒否の接続数（部分的に集計されます） • 接続ごとのメッセージ数に対する控えめな乗数 アプライアンスに重い負荷がかけられている場合、拒否された接続の正確な数を送信者別に維持できません。代わりに、拒否された接続数は、インターバルごとの最大送信者だけに対して維持されます。この場合、表示される値は「下限」、つまり少なくともこの数のメッセージが阻止されたと解釈できます。 （注）　[Overview] ページの [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。
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。
Spam Detected	検出されたすべてのスパム。
Virus Detected	検出されたすべてのウイルス。
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。
Total Threat	脅威メッセージ（評価により阻止されたもの、無効な受信者、スパム、およびウイルスとして阻止されたもの）の総数
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。
Clean	すべてのクリーン メッセージ。
User Mail Flow Details（[Internal Users] ページ）	
Incoming Spam Detected	検出されたすべての着信スパム。
Incoming Virus Detected	検出された着信ウイルス。
Incoming Content Filter Matches	検出された着信コンテンツ フィルタの一致。
Incoming Stopped by Content Filter	設定されていたコンテンツ フィルタのために阻止された着信メッセージ。
Incoming Clean	すべての着信クリーン メッセージ。
Outgoing Spam Detected	検出された発信スパム。
Outgoing Virus Detected	検出された発信ウイルス。
Outgoing Content Filter Matches	検出された発信コンテンツ フィルタの一致。
Outgoing Stopped by Content Filter	設定されていたコンテンツ フィルタのため阻止された発信メッセージ。
Outgoing Clean	すべての発信クリーン メッセージ。
Incoming and Outgoing TLS Connections（[TLS Connections] ページ）	
Required TLS: Failed	失敗した、必要なすべての TLS 接続。

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

カラム名	説明
Required TLS: Successful	成功した、必要なすべての TLS 接続。
Preferred TLS: Failed	失敗した、優先するすべての TLS 接続。
Preferred TLS: Successful	成功した、優先するすべての TLS 接続。
Total Connections	TLS 接続の合計数。
Total Messages	TLS メッセージの総数。
Outbreak Filters	
Outbreak Name	アウトブレイクの名前。
Outbreak ID	アウトブレイク ID。
First Seen Globally	ウイルスが最初にグローバルに発見された時刻。
Protection Time	ウイルスから保護されていた時間。
Quarantined Messages	隔離に関するメッセージ。

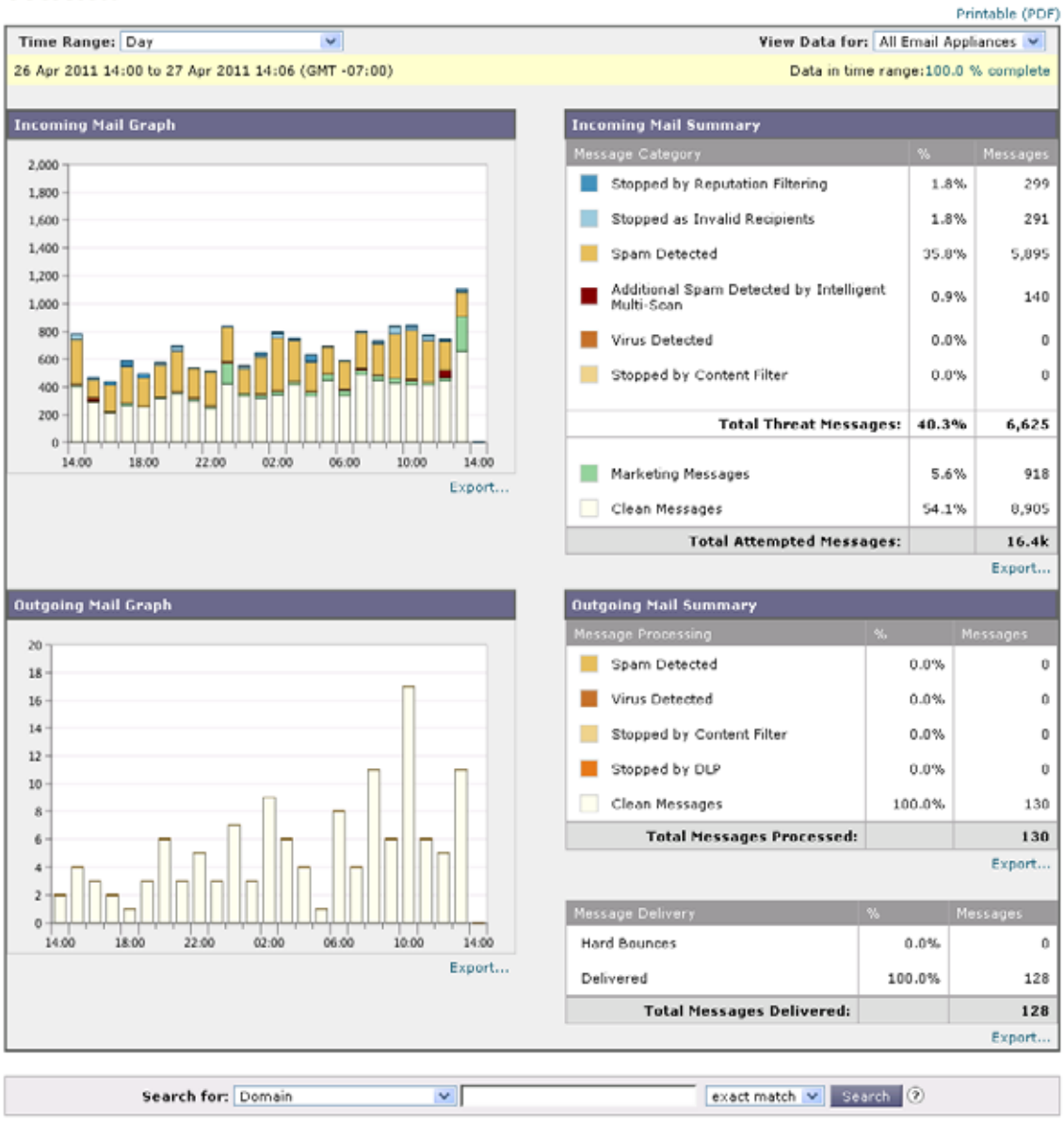
電子メール レポーティングの [Overview] ページ

セキュリティ管理アプライアンスの [Email] > [Reporting] > [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。[Overview] ページには、グラフや、着信および発信メッセージの要約テーブルが表示されます。

ステップ 1　セキュリティ管理アプライアンスで、[Management Appliance] > [Email] > [Reporting] > [Overview] を選択します。

図 4-1 に、[Overview] ページを示します。

図 4-1　[Email] > [Reporting] > [Overview] ページ



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

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

（注）　[Domain-Based Executive Summary] レポートおよび [Executive Summary] レポートが電子メール レポーティングの [Overview] ページに基づいていることに注意してください。[Domain-Based Executive Summary] レポートは、指定されたドメインのグループに制限されます。レポートのスケジュール設定については、「電子メール レポートのスケジュール設定」（P.4-55）を参照してください。

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

表 4-3　[Email] > [Reporting] > [Overview] ページの詳細

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

着信メール メッセージのカウント方法

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

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

アプライアンスによる電子メール メッセージの分類方法

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

これらの優先ルールに続いて、次のようなさまざまな判定が行われます。

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

- ウイルス陽性
- コンテンツ フィルタとの一致

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

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

[Overview] ページでの電子メール メッセージの分類

[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　[Overview] ページの電子メールのカテゴリ

カテゴリ	説明
Stopped by Reputation Filtering	HAT ポリシーによってブロックされたすべての接続数に、固定乗数（「着信メール メッセージのカウント方法」（P.4-13）を参照）を掛けたものに、受信者のスロットリングによってブロックされたすべての受信者数を加えた値。 [Overview] ページの [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。
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。
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。
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。
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。

表 4-4　[Overview] ページの電子メールのカテゴリ（続き）

カテゴリ	説明
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。
Clean Messages Accepted	このカテゴリは、受け入れられ、ウイルスでもスパムでもないと見なされたメールです。 受信者単位のスキャン アクション（個々のメール ポリシーで処理される分裂したメッセージなど）を考慮したときに受信されたクリーン メッセージを最も正確に表したものです。 ただし、スパム陽性またはウイルス陽性というマークを付けられたが、それでも配信されるメッセージはカウントされないため、配信される実際のメッセージ数はクリーン メッセージ数とは異なる可能性があります。 メッセージが*メッセージ フィルタ*と一致し、フィルタによってドロップされたり、バウンスされたりしていない場合は、クリーンなメッセージとして扱われます。メッセージ フィルタによってドロップされたか、バウンスされたメッセージは、総数に含まれません。

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

[Incoming Mail] ページ

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

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

[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。[Incoming Mail] ページまたは他の [Sender Profile] ページの上部にある対応するリンクをクリックすると、IP アドレス、ドメイン、またはネットワーク オーナーの [Sender Profile] ページにアクセスできます。

[Incoming Mail] ページでは、次の操作を実行できます。

- セキュリティ管理アプライアンスに電子メールを送信したメール送信者の IP アドレス、ドメイン、またはネットワーク オーナー（組織）に関する検索を実行する。「検索およびインタラクティブ電子メール レポート ページ」（P.4-6）を参照してください。

- 送信者グループ レポートを表示して、特定の送信者グループおよびメール フロー ポリシー アクションに従って接続をモニタする。詳細については、「[Sender Groups] レポート ページ」（P.4-24）を参照してください。
- 電子メールをアプライアンスに送信した送信者の詳細な統計情報を表示する。統計情報には、セキュリティ サービス（評価フィルタリング、アンチスパム、アンチウイルスなど）によってブロックされたメッセージの数が含まれます。
- アンチスパムまたはアンチウイルス セキュリティサービスによって測定される、大量のスパムまたはウイルス電子メールを送信した送信者別にソートする。
- Cisco IronPort SenderBase レピュテーション サービスを使用して特定の IP アドレス、ドメイン、および組織の間の関係の分析を行い、送信者に関する情報を取得する。
- 送信者の SenderBase レピュテーション スコア、ドメインが直近に一致した送信者グループなど Cisco IronPort SenderBase レピュテーション サービスから送信者に関する詳細を取得する。送信者を送信者グループに追加する。
- アンチスパムまたはアンチウイルス セキュリティ サービスによって測定される、大量のスパムまたはウイルス電子メールを送信した特定の送信者についての詳細情報を取得する。

[Incoming Mail] ページ内のビュー

[Incoming Mail] ページには、次の 3 つのビューがあります。

- IP アドレス
- ドメイン
- ネットワーク オーナー

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

さらに、[Incoming Mail] ページの [Incoming Mail Details] セクションでは、[Sender’s IP Address]、[Domain name]、または [Network Owner Information] をクリックすると、特定の [Sender Profile Information] を取得できます。[Sender Profile] の情報の詳細については、「[Sender Profile] ページ」（P.4-20）を参照してください。

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

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

IP アドレス、ドメイン、またはネットワーク オーナーをクリックすると、[Sender Profile] ページの送信者の詳細にアクセスできます。[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 [Incoming Mail] ページです。

[Incoming Mail] ページの下部にある [Sender Groups Report] リンクをクリックすると、送信者グループ別のメール フロー情報にアクセスできます。

[Incoming Mail] ページでの電子メール メッセージの分類

[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　[Incoming Mail] ページの電子メールのカテゴリ

カテゴリ	説明
Stopped by Reputation Filtering	HAT ポリシーによってブロックされたすべての接続数に、固定乗数（「着信メール メッセージのカウント方法」（P.4-13）を参照）を掛けたものに、受信者のスロットリングによってブロックされたすべての受信者数を加えた値。 [Stopped by Reputation Filtering] の値は、次の複数の要素に基づいて算出されます。 • この送信者からの「調整された」メッセージの数 • 拒否された、または TCP 拒否の接続数（部分的に集計されます） • 接続ごとのメッセージ数に対する控えめな乗数 アプライアンスに重い負荷がかけられている場合、拒否された接続の正確な数を送信者別に維持できません。代わりに、拒否された接続数は、インターバルごとの最大送信者だけに対して維持されます。この場合、表示される値は「下限」、つまり少なくともこの数のメッセージが阻止されたと解釈できます。
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。
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。
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。
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。
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。
Clean Messages Accepted	受け入れられ、ウイルスでもスパムでもないと見なされたメール。受信者単位のスキャン アクション（個々のメール ポリシーで処理される分裂したメッセージなど）を考慮したときに受信されたクリーン メッセージを最も正確に表したものです。ただし、スパム陽性またはウイルス陽性というマークを付けられたが、それでも配信されるメッセージはカウントされないため、配信される実際のメッセージ数はクリーン メッセージ数とは異なる可能性があります。

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

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

場合によっては、いくつかのレポート ページに、トップレベルのページからアクセスできる独自のサブレポートが複数含まれることがあります。たとえば、セキュリティ管理アプライアンスの [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 [Incoming Mail] レポート ページからアクセスできるサブページです。

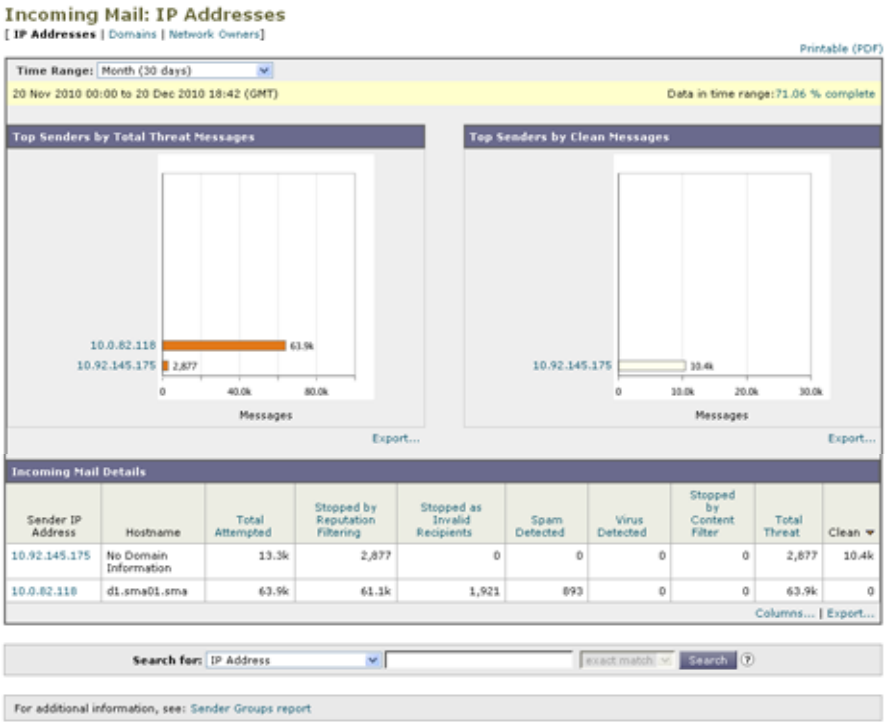
トップレベル ページ（この場合には [Incoming Mail] レポート ページ）の右上にある [Printable PDF] リンクをクリックすると、これらの各サブレポート ページの結果を、1 つの統合レポートに生成できます。「電子メール レポーティング ページの概要」（P.4-7）の重要な情報を参照してください。

[Incoming Mail] ページを表示するには、次の手順を実行します。

ステップ 1　セキュリティ管理アプライアンスで、[Email] > [Reporting] > [Incoming Mail] を選択します。

ステップ 2　ビューをクリックします（[IP Addresses]、[Domains]、または [Network Owners]）。

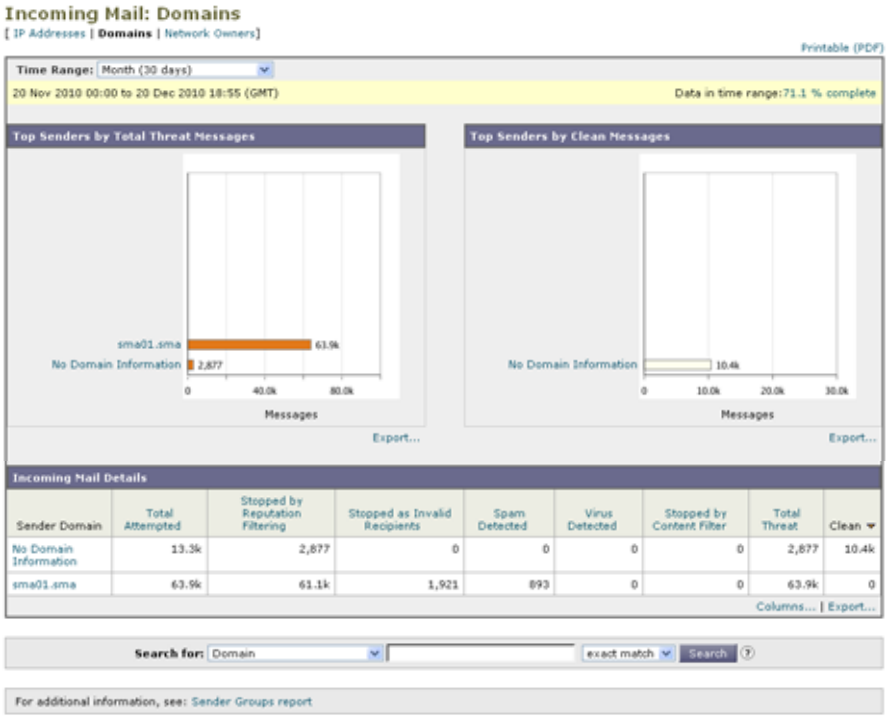
図 4-2　　[Incoming Mail] ページ：[IP Address] ビュー



[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、「[Incoming Mail Details] テーブル」（P.4-20）を参照してください。

この例では、[Domain] ビューが選択されています。

図 4-3　[Incoming Mail] ページ：[Domain] ビュー



[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、「電子メール レポーティング ページの概要」（P.4-7）を参照してください。

（注）　[Incoming Mail] レポート ページのスケジュール設定されたレポートを生成できます。「電子メール レポートのスケジュール設定」（P.4-55）を参照してください。

[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 [No Domain Information] に自動的に分類されます。これらの種類の検証されないホストを、送信者の検証によってどのように管理するかを制御できます。送信者検証の詳細については、『*Cisco IronPort AsyncOS for Email Security Configuration Guide*』を参照してください。

[Items Displayed] メニューを使用して、リストに表示する送信者の数を選択できます。

メール トレンド グラフにおける時間範囲

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

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

[Incoming Mail Details] テーブル

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

*ダブル DNS ルックアップ*を実行することで、システムはリモート ホストの IP アドレスの正当性を確保および検証します。ダブル DNS ルックアップと送信者検証の詳細については、『*Cisco IronPort AsyncOS for Email Security Configuration Guide*』を参照してください。

[Incoming Mail Details] テーブルの最初のカラム、または [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、[Sender] または [No Domain Information] リンクをクリックすると、送信者の詳細情報が表示されます。結果は、[Sender Profile] ページに表示され、IronPort SenderBase レピュテーション サービスからのリアルタイム情報が含まれます。送信者プロファイル ページからは、特定の IP アドレスまたはネットワーク オーナーに関する詳細を表示できます。詳細については、「[Sender Profile] ページ」（P.4-20）を参照してください。

[Incoming Mail] ページの下部にある [Sender Groups Report] をクリックして、[Sender Groups] レポートを表示することもできます。[Sender Groups] レポート ページの詳細については、「[Sender Groups] レポート ページ」（P.4-24）を参照してください。

[Sender Profile] ページ

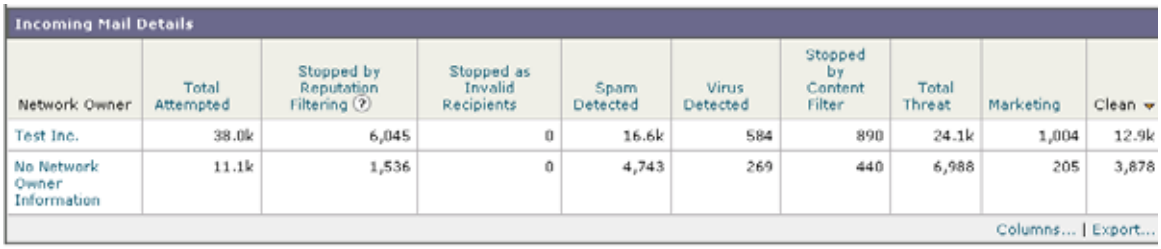
[Incoming Mail] ページで [Incoming Mail Details] インタラクティブ テーブルの送信者をクリックすると、[Sender Profile] ページが表示されます。ここには、特定の IP アドレス、ドメイン、またはネットワーク オーナー（組織）の詳細情報が表示されます。[Incoming Mail] ページまたは他の [Sender Profile] ページにある対応するリンクをクリックすると、IP アドレス、ドメイン、またはネットワーク オーナーの [Sender Profile] ページにアクセスできます。

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

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

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

図 4-4　ネットワーク オーナーのドメイン リスト



Incoming Mail Details

Network Owner	Total Attempted	Stopped by Reputation Filtering	Stopped as Invalid Recipients	Spam Detected	Virus Detected	Stopped by Content Filter	Total Threat	Marketing	Clean
Test Inc.	38.0k	6,045	0	16.6k	584	890	24.1k	1,004	12.9k
No Network Owner Information	11.1k	1,536	0	4,743	269	440	6,988	205	3,878

Columns... | Export...

各 [Sender Profile] ページには、ページの下部の現在の情報テーブルに次のデータが含まれます。

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

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

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

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

  Cisco IronPort 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、[More from SenderBase] をクリックします。
- このネットワーク オーナーによって管理されるドメインおよび IP アドレスに関する詳細は、ネットワーク オーナー プロファイル ページに表示されます。ドメイン内の IP アドレスに関する詳細は、ドメイン ページに表示されます。

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

図 4-5　ネットワーク オーナーの現在の情報

図 4-6　ドメイン プロファイル ページ

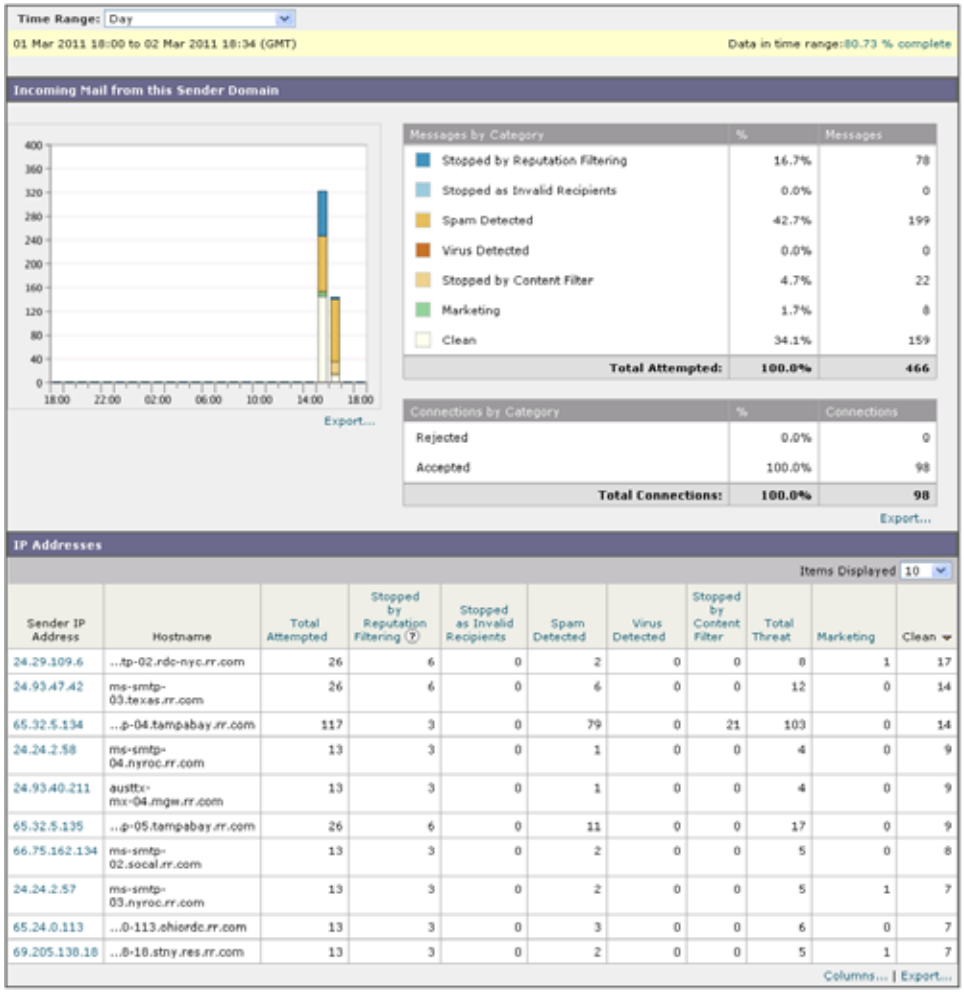


図 4-7　ネットワーク オーナー プロファイル ページ

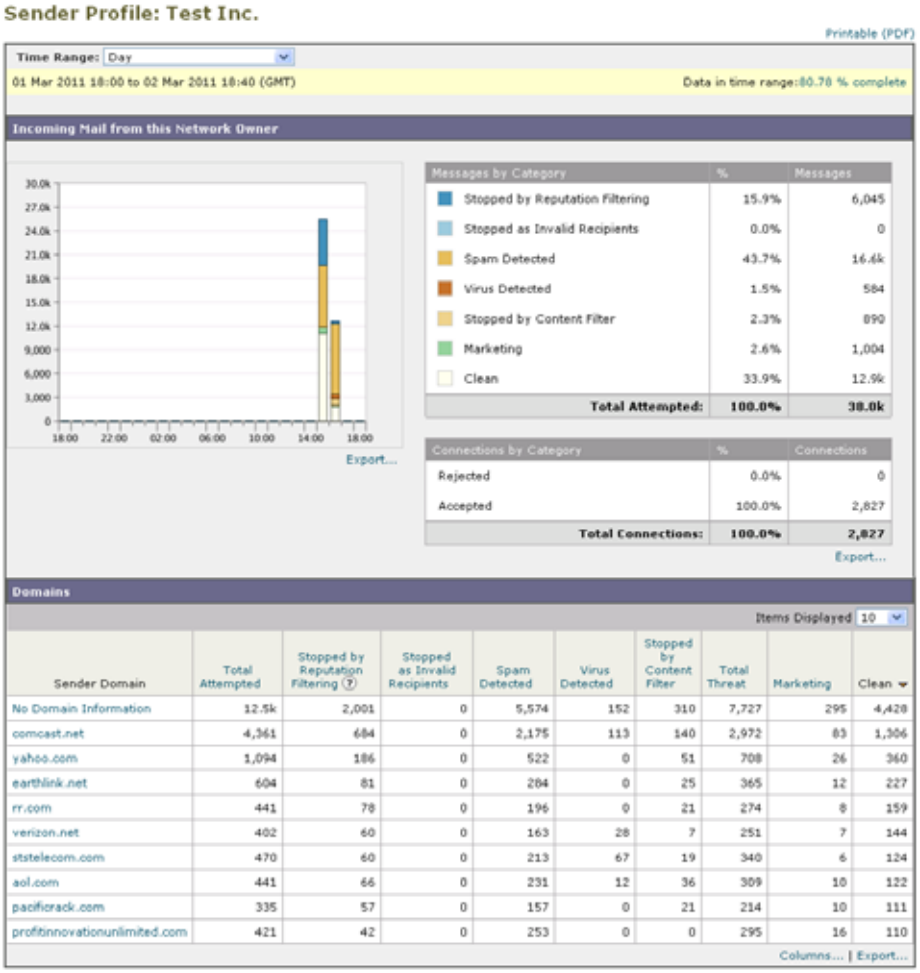
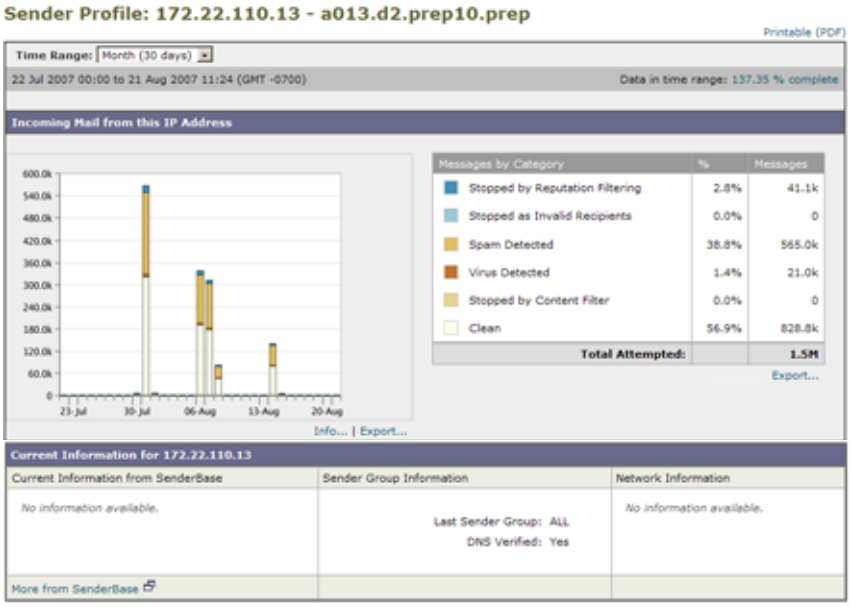


図 4-8　IP アドレス プロファイル ページ

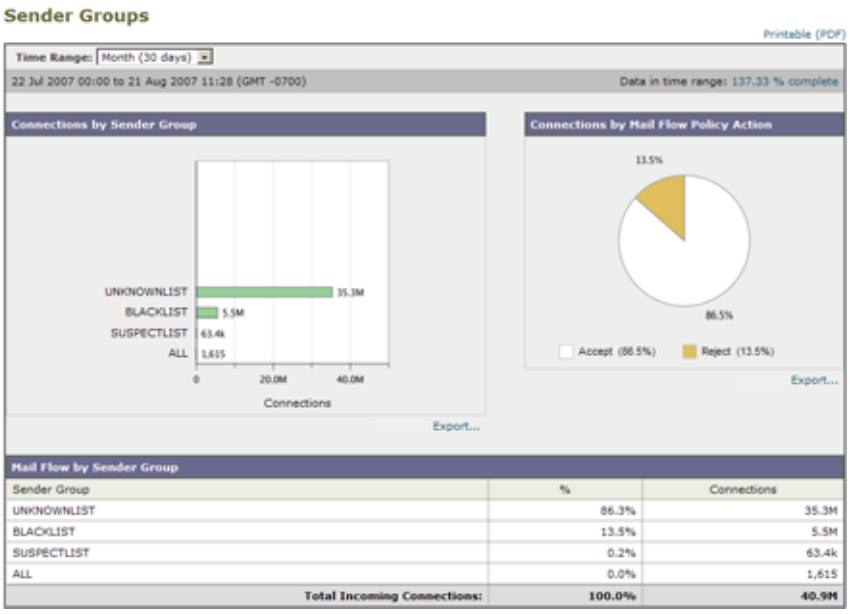


[Sender Groups] レポート ページ

[Sender Groups] レポート ページは、送信者グループ別およびメール フロー ポリシー アクション別の接続のサマリーを提供し、SMTP 接続およびメール フロー ポリシーのトレンドを確認できるようにします。[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。[Connections by Mail Flow Policy Action] グラフは、各メール フローポリシー アクションの接続の割合を示します。このページには、Host Access Table（HAT; ホスト アクセス テーブル）ポリシーの有効性の概要が示されます。HAT の詳細については、『*Cisco IronPort AsyncOS for Email Security Configuration Guide*』を参照してください。

[Sender Groups] レポート ページを表示するには、[Incoming Mail] レポート ページの下部にある [Sender Groups report] リンクをクリックします。

図 4-9　[Sender Groups] レポート ページ



[Sender Group] 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、「電子メール レポーティング ページの概要」（P.4-7）を参照してください。

（注）　[Sender Group] レポート ページのスケジュール設定されたレポートを生成できます。「電子メール レポートのスケジュール設定」（P.4-55）を参照してください。

[Outgoing Destinations] ページ

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

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

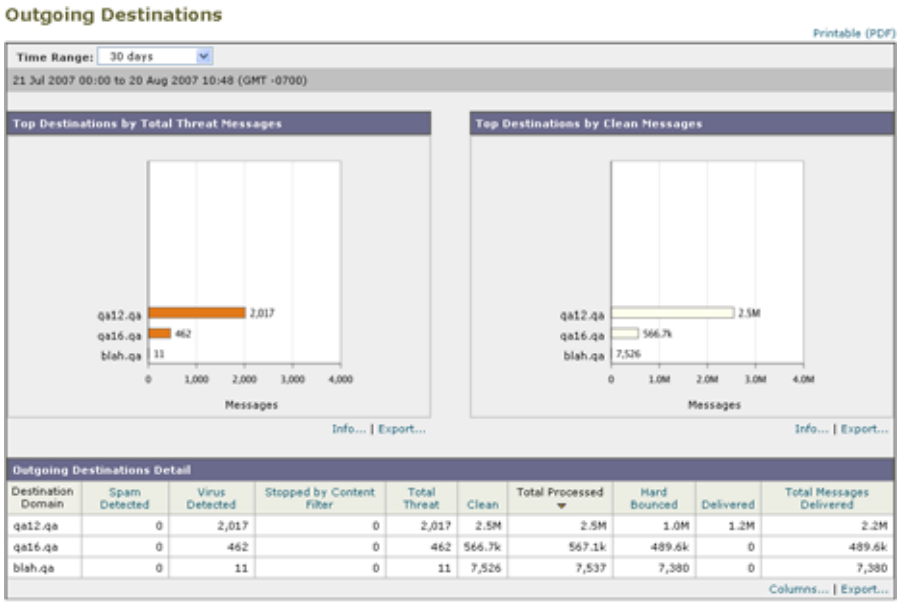
- 電子メール セキュリティ アプライアンスが電子メールを送信する宛先ドメイン。
- 各ドメインに送信される電子メールの量。
- クリーン、スパム陽性、またはコンテンツ フィルタによる阻止のメールの割合。
- 配信されたメッセージおよび宛先サーバによってハードバウンスされたメッセージの数。

[Outgoing Destinations] ページを表示するには、次の手順を実行します。

ステップ 1　セキュリティ管理アプライアンスで、[Email] > [Reporting] > [Outgoing Destinations] を選択します。

[Outgoing Destinations] ページが表示されます。

図 4-10　[Email] > [Reporting] > [Outgoing Destinations] ページ



次のリストでは、[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　[Email] > [Reporting] > [Outgoing Destinations] ページの詳細

セクション	説明
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、「インタラクティブ レポートの時間範囲の選択」（P.3-4）を参照してください。
Top Destination by Total Threat	組織によって送信された発信脅威メッセージ（スパム、アンチウイルスなど）の上位の宛先ドメイン。コンテンツ フィルタをトリガーしたスパム陽性またはウイルス陽性の脅威メッセージを含む、脅威メッセージの総数。
Top Destination by Clean Messages	組織によって送信されたクリーンな発信脅威メッセージの上位の宛先ドメイン。
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。

[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、「電子メール レポーティング ページの概要」（P.4-7）を参照してください。

（注）　[Outgoing Destinations] ページのスケジュール設定されたレポートを生成できます。「電子メール レポートのスケジュール設定」（P.4-55）を参照してください。

[Outgoing Senders] ページ

[Email] > [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。

[Outgoing Senders] ページを使用して、次の情報を入手できます。

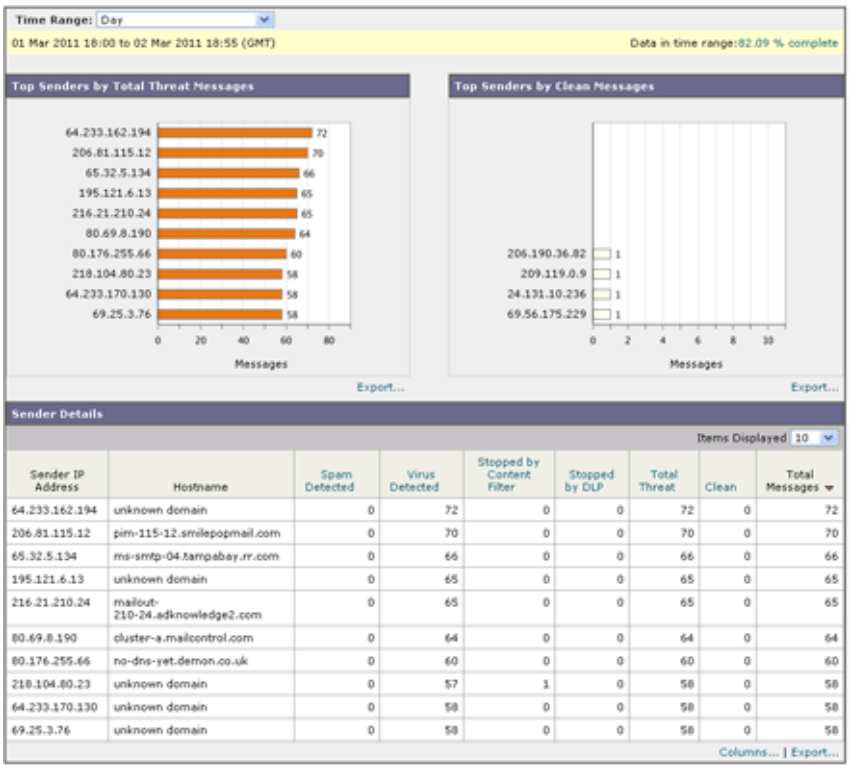
- 最も多くのウイルスまたはスパム陽性の電子メールを送信した IP アドレス
- 最も頻繁にコンテンツ フィルタをトリガーした IP アドレス。
- 最も多くのメールを送信するドメイン
- 配信が試行された場所で処理された受信者の総数。

[Outgoing Sender] ページを表示するには、次の手順を実行します。

ステップ 1　セキュリティ管理アプライアンスで、[Email] > [Reporting] > [Outgoing Sender] を選択します。

[Outgoing Sender] ページが表示されます。

図 4-11　[Email] > [Reporting] > [Outgoing Senders] ページ（IP アドレスを表示中）



[Outgoing Senders] の結果は次の 2 種類のビューで表示できます。

- [Domain]：このビューでは、各ドメインから送信された電子メールの量を表示できます。
- [IP 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、[Outgoing Destinations] ページの両方のビューのさまざまなセクションについて説明します。

表 4-7　[Email] > [Reporting] > [Outgoing Sender] ページの詳細

セクション	説明
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、「インタラクティブ レポートの時間範囲の選択」（P.3-4）を参照してください。
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）。
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）。
Sender Details	組織内によって送信されたすべての発信メッセージの送信者のすべての詳細情報（IP アドレス別またはドメイン別）。詳細情報には検出されたスパム、ウイルス、クリーンメッセージなどが含まれます。

（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、[Monitor]> [Delivery Status] を選択します。

[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、「電子メール レポーティング ページの概要」（P.4-7）を参照してください。

（注） [Outgoing Senders] レポート ページのスケジュール設定されたレポートを生成できます。「電子メール レポートのスケジュール設定」（P.4-55）を参照してください。

[Internal Users] ページ

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

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

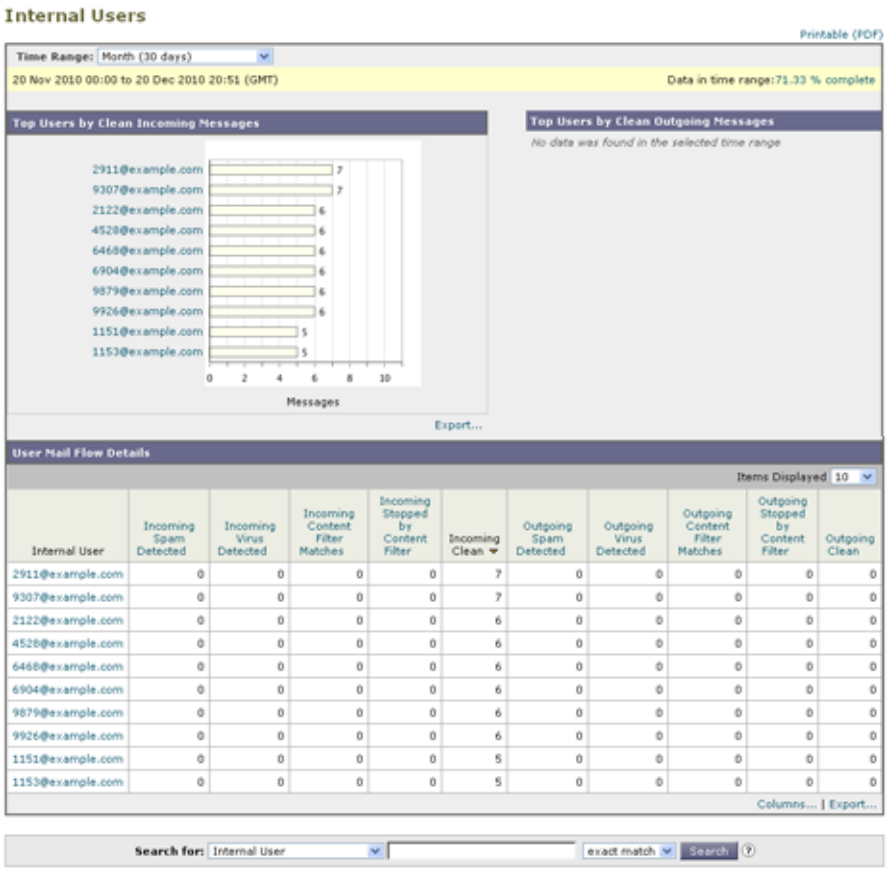
- 最も多くの外部メールを送信したユーザ。
- 最も多くのクリーン電子メールを受信したユーザ
- 最も多くのスパムを受信したユーザ
- 特定のコンテンツ フィルタをトリガーしたユーザ。
- 特定のユーザからの電子メールを阻止したコンテンツ フィルタ。

[Internal Users] ページを表示するには、次の手順を実行します。

ステップ 1　セキュリティ管理アプライアンスで、[Email] > [Reporting] > [Internal Users] を選択します。

[Internal Users] ページが表示されます。

図 4-12　[Email] > [Reporting] > [Internal Users] ページ



次のリストでは、[Internal Users] 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 4-8　[Email] > [Reporting] > [Internal Users] ページの詳細

セクション	説明
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、「インタラクティブ レポートの時間範囲の選択」（P.3-4）を参照してください。
Top Users by Clean Incoming Messages	組織内で送信されたクリーンな着信メッセージの上位ユーザ（IP アドレス別またはドメイン別）。

表 4-8　[Email] > [Reporting] > [Internal Users] ページの詳細（続き）

セクション	説明
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）。
User Mail Flow Details	[User Mail Flow Details] インタラクティブ セクションでは、各電子メール アドレスで送受信した電子メールが [Clean]、[Spam Detected]（受信のみ）、[Virus Detected]、[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。 内部ユーザの [Internal User Detail] ページを表示するには、[Internal User] カラムの内部ユーザをクリックします。[Internal Users Details] ページの詳細については、「[Internal User Details] ページ」（P.4-30）を参照してください。

[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、「電子メール レポーティング ページの概要」（P.4-7）を参照してください。

（注）　[Internal Users] ページのスケジュール設定されたレポートを生成できます。「電子メール レポートのスケジュール設定」（P.4-55）を参照してください。

[Internal User Details] ページ

[Internal User Details] ページでは、各カテゴリ（[Spam Detected]、[Virus Detected]、[Sopped By Content Filter]、および [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。

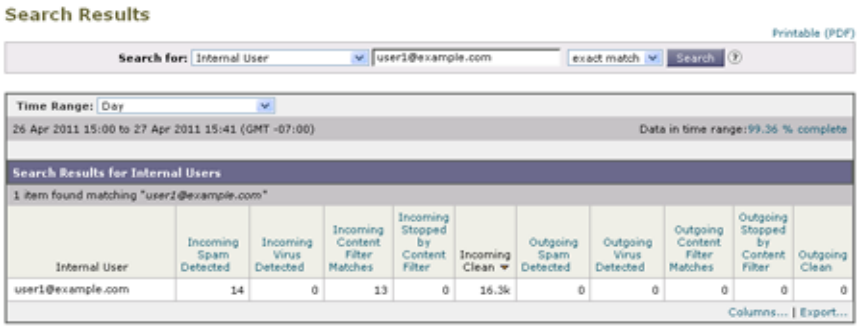
コンテンツ フィルタの詳細情報を対応するコンテンツ フィルタ情報ページに表示するには、そのコンテンツ フィルタ名をクリックします（「[Content Filters] ページ」（P.4-33）を参照）。この方法を使用すると、特定のコンテンツ フィルタに一致したメールを送受信したすべてのユーザのリストも表示できます。

（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

[Internal Users] ページおよび [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。

図 4-13　内部ユーザ検索の結果



[DLP Incident Summary] ページ

[DLP Incident Summary] ページには、送信メールで発生した Data Loss Prevention（DLP）ポリシー違反インシデントに関する情報が示されます。Cisco IronPort アプライアンスでは、[Outgoing Mail Policies] テーブルでイネーブルにした DLP 電子メール ポリシーを使用して、ユーザが送信した機密データを検出します。DLP ポリシーに違反する送信メッセージが発生するたびに、インシデントとして報告されます。

[DLP 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。

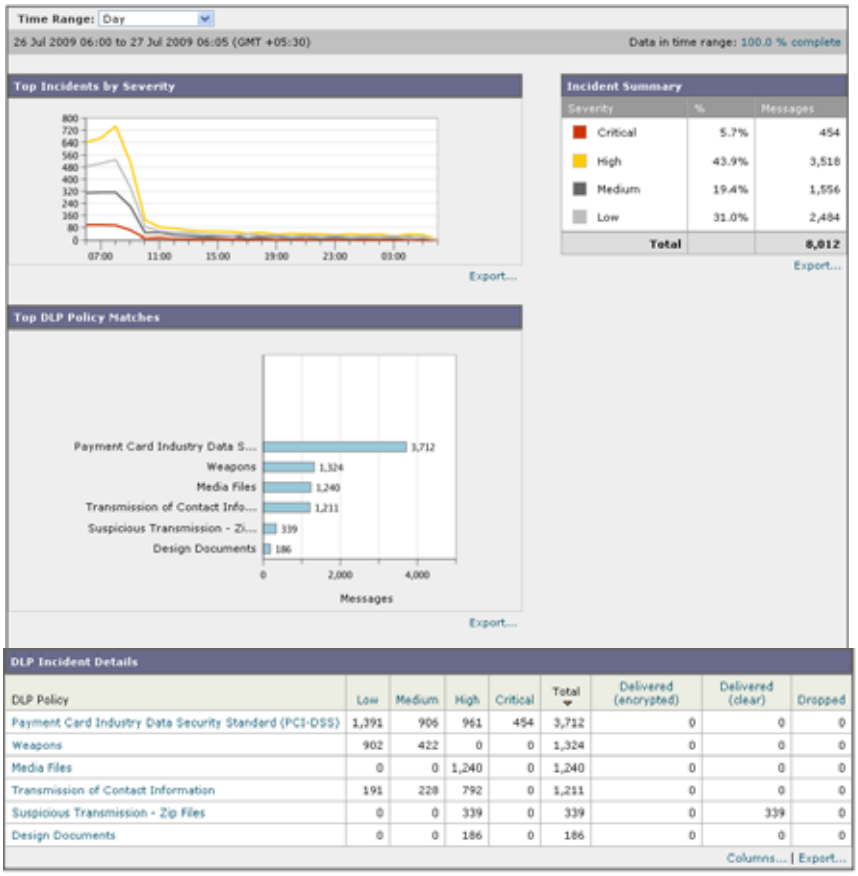
- ユーザが送信した機密データの種類
- これらの DLP インシデントの重大度
- これらのメッセージのうち、配信されたメッセージの数
- これらのメッセージのうち、ドロップされたメッセージの数
- これらのメッセージの送信者

[DLP Summary] ページを表示するには、次の手順を実行します。

ステップ 1　セキュリティ管理アプライアンスで、[Email] > [Reporting] > [DLP Summary] を選択します。

[DLP Summary] ページが表示されます。

図 4-14　[Email] > [Reporting] > [DLP Summary] ページ



[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（[Low]、[Medium]、[High]、[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 Incident Details] リスト

次のリストでは、[DLP Incident Summary] ページのさまざまなセクションについて説明します。

表 4-9　[Email] > [Reporting] > [DLP Incident Summary] ページの詳細

セクション	説明
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、「インタラクティブ レポートの時間範囲の選択」（P.3-4）を参照してください。
Top Incidents by Severity	重大度別の上位 DLP インシデント。
Incident Summary	各電子メール アプライアンスの送信メール ポリシーで現在イネーブルになっている DLP ポリシーは、[DLP Incident Summary] ページの下部にある [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　[Email] > [Reporting] > [DLP Incident Summary] ページの詳細（続き）

セクション	説明
Top DLP Policy Matches	一致している上位 DLP ポリシー。
DLP Incident Details	[DLP Incident Details] テーブルには、ポリシーごとの DLP インシデントの数に加えて、重大度レベル別の内訳、メッセージのいずれかがクリアに配信されたか、暗号化されて配信されたか、ドロップされたかが示されます。 詳細情報を表示するには、DLP ポリシーの名前をクリックします。[DLP Incidents Details] ページの詳細については、「[DLP Incidents Details] テーブル」（P.4-33）を参照してください。

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

[DLP Incidents Details] テーブル

[DLP Incident Details] テーブルは、ポリシーごとの DLP インシデントの数に加えて、重大度レベル別の内訳、メッセージのいずれかがクリアに配信されたか、暗号化されて配信されたか、ドロップされたかが表示されるインタラクティブ テーブルです。データをソートするには、カラム見出しをクリックします。このインタラクティブ テーブルに表示される DLP ポリシーの詳細情報を検索するには、DLP ポリシー名をクリックすると、その DLP ポリシーのページが表示されます。詳細については、「[DLP Policy Detail] ページ」（P.4-33）を参照してください。

[DLP Policy Detail] ページ

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

このページには、DLP ポリシーに違反したメッセージを送信した各内部ユーザを表示する、ページ下部にある [Incidents by Sender] テーブルも含まれます。このテーブルには、このポリシーに関するユーザごとの DLP インシデントの総数に加えて、重大度レベル別の内訳、メッセージのいずれかがクリアに配信されたか、暗号化されて配信されたか、ドロップされたかが示されます。[Incidents by Sender] テーブルを使用すると、組織の機密データをネットワーク外のユーザに送信した可能性のあるユーザを検索できます。

送信者名をクリックすると、[Internal Users] ページが開きます。詳細については、「[Internal Users] ページ」（P.4-28）を参照してください。

[Content Filters] ページ

[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。[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。

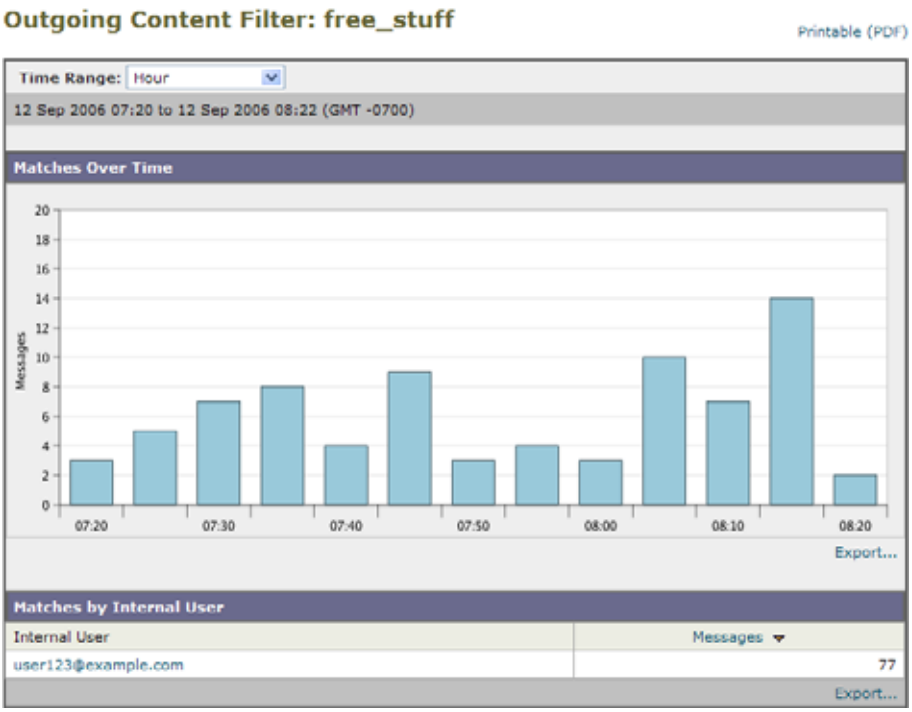
- 受信メールまたは送信メールによってトリガーされた回数の最も多いコンテンツ フィルタ。
- 特定のコンテンツ フィルタをトリガーしたメールを送受信した上位ユーザ。

[Content Filter] ページを表示するには、次の手順を実行します。

ステップ 1　セキュリティ管理アプライアンスで、[Email] > [Reporting] > [Content Filter] を選択します。

[Content Filter] ページが表示されます。

図 4-15　[Email] > [Reporting] > [Content Filter] ページ



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。[Content Filter Details] ページが表示されます。[Content Filter Details] ページの詳細については、「[Content Filter Details] ページ」（P.4-34）を参照してください。

[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、「電子メール レポーティング ページの概要」（P.4-7）を参照してください。

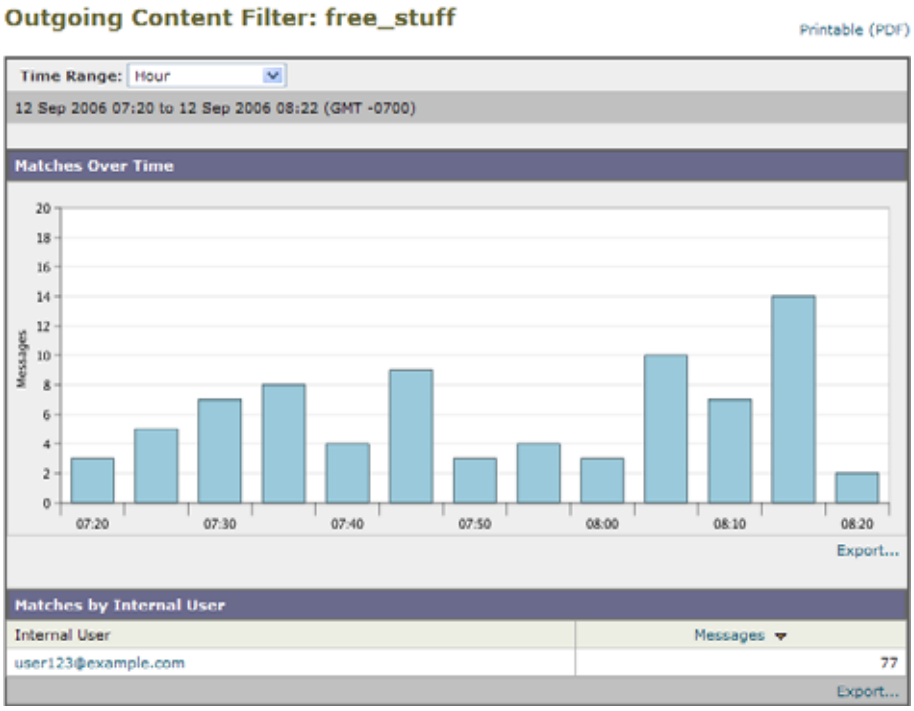
（注）　[Content Filter] ページのスケジュール設定されたレポートを生成できます。「電子メール レポートのスケジュール設定」（P.4-55）を参照してください。

[Content Filter Details] ページ

[Content Filter Detail] 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。

[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、「[Internal User Details] ページ」（P.4-30）を参照してください。

図 4-16　[Content Filters Details] ページ



[Virus Types] ページ

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

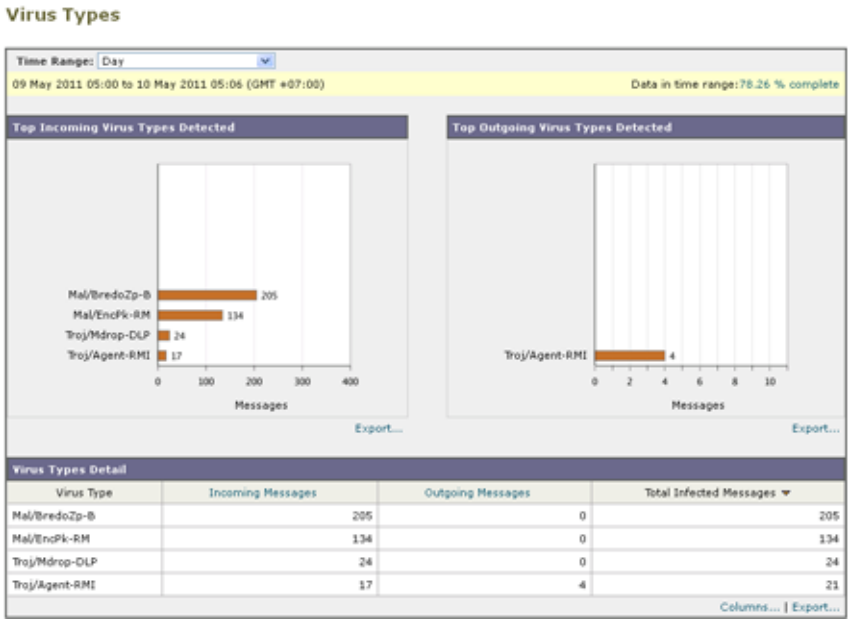
（注）　ウイルス感染フィルタでは、ユーザが介入することなく、これらの種類のウイルスに感染したメッセージを隔離することができます。

[Virus Types] ページを表示するには、次の手順を実行します。

ステップ 1　セキュリティ管理アプライアンスで、[Email] > [Reporting] > [Virus Types] を選択します。

[Virus Types] ページが表示されます。

図 4-17　[Email] > [Reporting] > [Virus Types] ページ



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

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

表 4-10　[Email] > [Reporting] > [Virus Types] ページの詳細

セクション	説明
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、「インタラクティブ レポートの時間範囲の選択」（P.3-4）を参照してください。
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。
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。
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、[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、[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。

[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、「電子メール レポーティング ページの概要」（P.4-7）を参照してください。

（注）　[Virus Types] ページのスケジュール設定されたレポートを生成できます。「電子メール レポートのスケジュール設定」（P.4-55）を参照してください。

[TLS Connections] ページ

[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 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。

[TLS Connections] ページを表示するには、次の手順を実行します。

ステップ 1　セキュリティ管理アプライアンスで、[Email] > [Reporting] > [TLS Connections] を選択します。

[TLS Connections Report] ページが表示されます。

[TLS Connections Report] ページは、2 つのセクションに分かれています。

- 「[TLS Connections Report] ページ：[Incoming Connections]」
- 「[TLS Connections Report] ページ：[Outgoing Connections]」

図 4-18　[TLS Connections Report] ページ : [Incoming Connections]

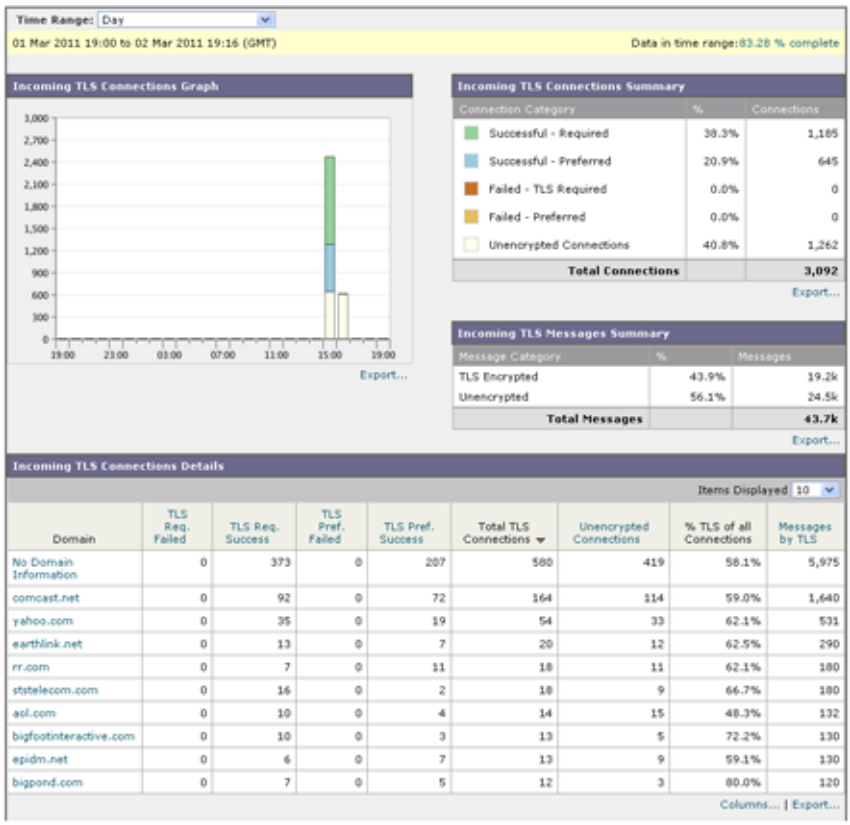
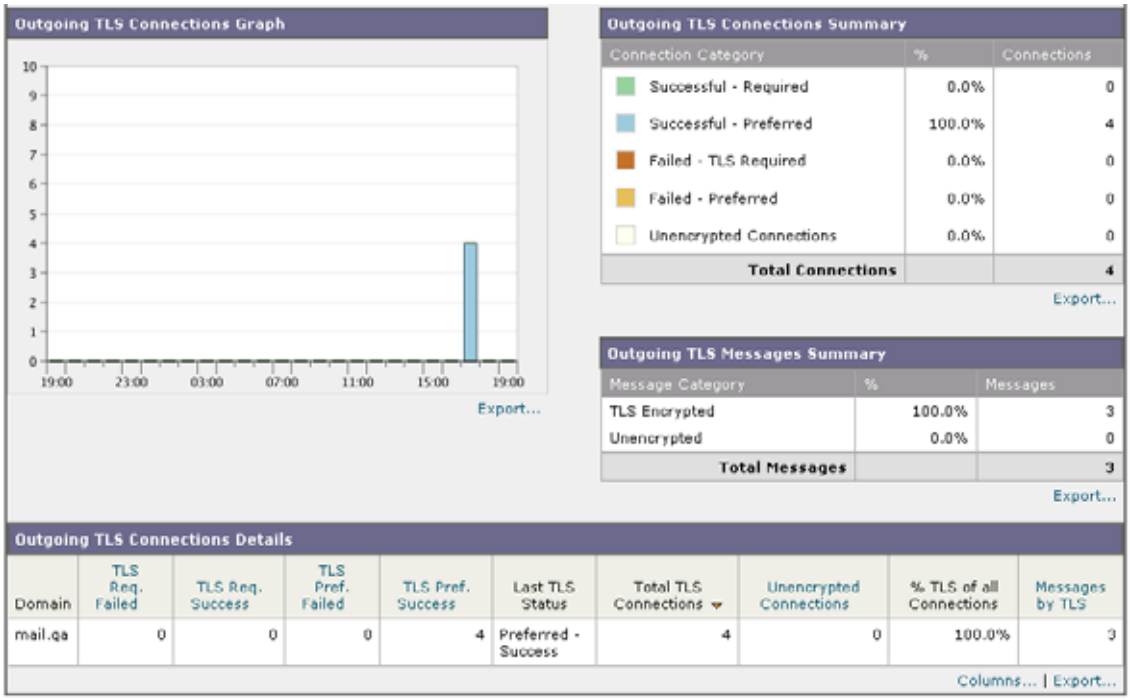


図 4-19　[TLS Connections Report] ページ : [Outgoing Connections]



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

表 4-11　[Email] > [Reporting] > [TLS Connections] ページの詳細

セクション	説明
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、「インタラクティブ レポートの時間範囲の選択」（P.3-4）を参照してください。
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。
Incoming TLS Connections Summary	この表には、着信メッセージの総量、暗号化された / 暗号化されないメッセージの量、成功 / 失敗した受信 TLS 暗号化メッセージの量が表示されます。
Incoming TLS Message Summary	この表には、着信メッセージの総量の概要が表示されます。
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。
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。
Outgoing TLS Connections Summary	この表には、発信メッセージの総量、暗号化された / 暗号化されないメッセージの量、成功 / 失敗した送信 TLS 暗号化メッセージの量が表示されます。

表 4-11　[Email] > [Reporting] > [TLS Connections] ページの詳細（続き）

セクション	説明
Outgoing TLS Message Summary	この表には、発信メッセージの総量が表示されます。
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。

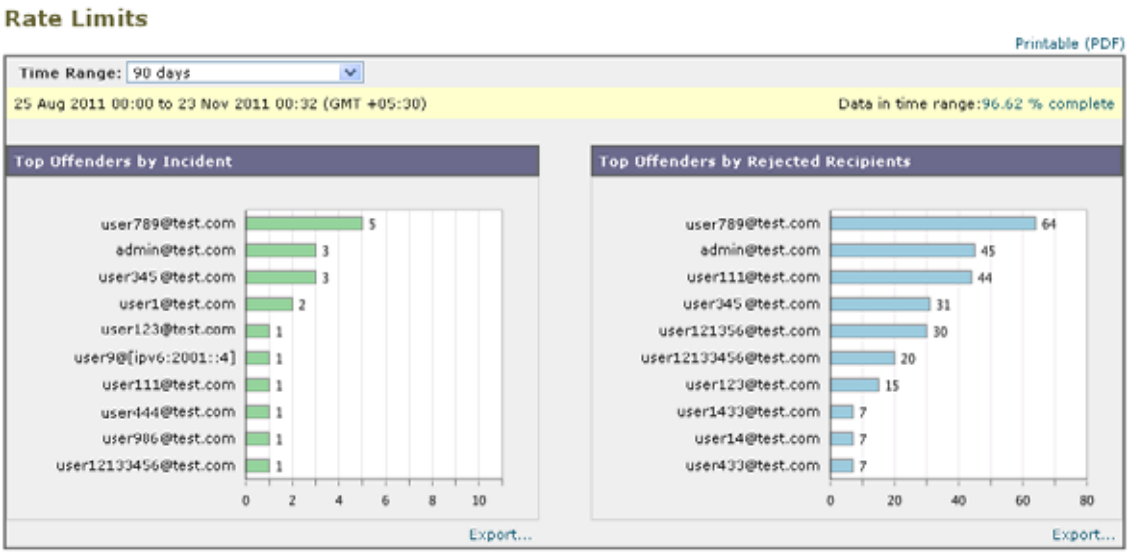
[Rate Limits] ページ

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 メッセージ数を制限できます。[Rate Limits] レポートを利用すると、多数のメッセージから個々の送信者をすばやく識別できます。このレポートは、次の場合に役立ちます。

- ユーザの資格情報が危険にさらされている場合や、アカウントがスパムの一括送信に使用されている場合など、内部ユーザ アカウントからのスパムを制御する。
- 危険にさらされているユーザ アカウントを識別する。
- 通知、アラート、自動設定などに関する電子メールを使用する、制御できないアプリケーションを制限する。
- 組織のオンライン レピュテーションに対する被害と、その状況に付随する混乱を回避する。

[Rate Limit for Envelope Senders] 設定を含む [Rate Limiting] 設定は、電子メール セキュリティ アプライアンス の [Mail Policies] > [Mail Flow Policies settings] で行います。

図 4-20　[Rate Limits] ページ



[Outbreak Filters] ページ

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

[Outbreak Filters] ページを使用して、次の情報を入手できます。

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

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

[Past Year Outbreak Summary] には、前年のグローバルな発生およびローカルでの発生が表示されるので、ローカル ネットワーク トレンドとグローバル トレンドを比較できます。グローバル発生リストは、ウイルス性と非ウイルス性の両方のすべての発生の上位集合です。これに対して、ローカル発生は、お使いの Cisco IronPort アプライアンスに影響を与えたウイルス感染発生に限定されています。ローカル発生データには非ウイルス性の脅威は含まれません。グローバル感染発生データは、アウトブレイク隔離で現在設定されているしきい値を超えた、Cisco IronPort Threat Operations Center によって検出されたすべての感染を表します。ローカル感染発生データは、アウトブレイク隔離で現在設定されているしきい値を超えた、このアプライアンスで検出されたすべてのウイルス感染を表します。[Total Local Protection Time] は、Cisco IronPort Threat Operations Center による各ウイルス感染の検出と、主要ベンダーによるアンチウイルス シグニチャの解放との時間差に常に基づいています。必ずしもすべてのグローバル発生が、お使いの Cisco IronPort 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。

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

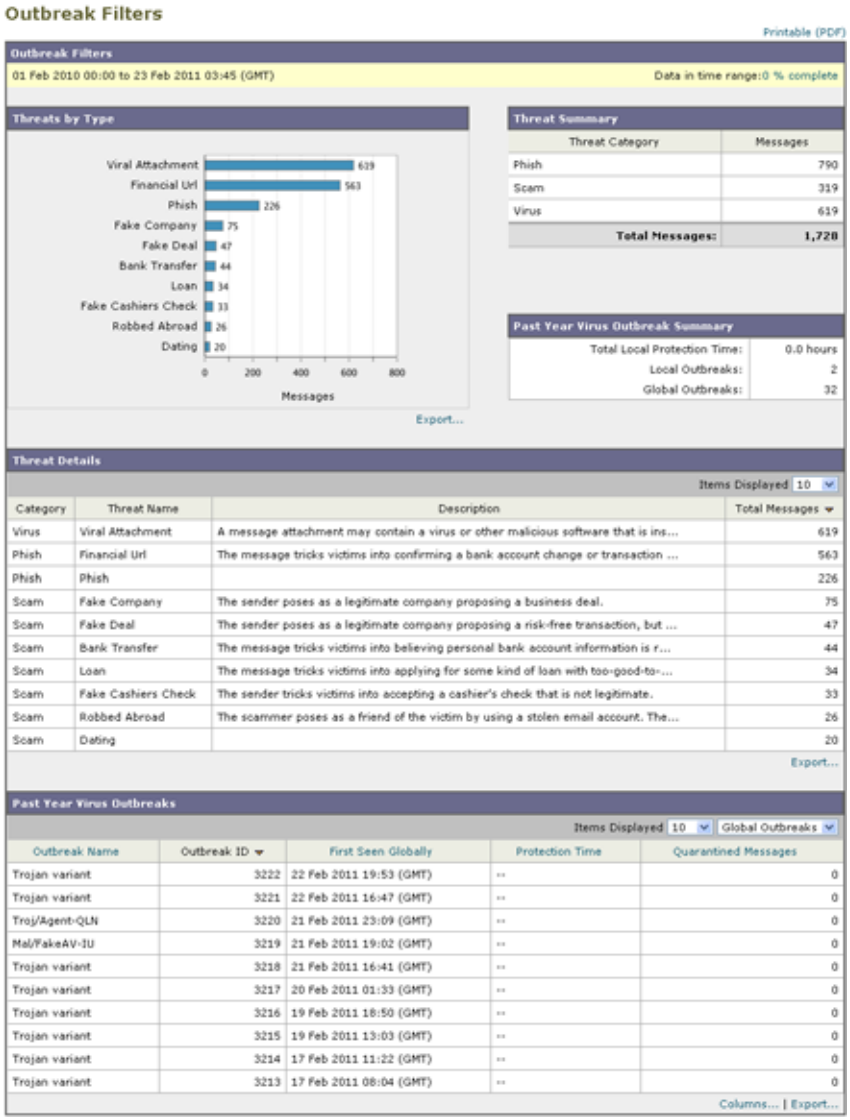
[Threat Details] リストには、脅威のカテゴリ（ウイルス、詐欺、またはフィッシング）、脅威名、脅威の説明、識別されたメッセージ数など、特定の発生についての情報が表示されます。ウイルス感染発生の場合、[Past Year Virus Outbreaks] に感染名、および ID、ウイルス感染が最初にグローバルに発見された時刻と日付、感染フィルタによって保護された時刻、および隔離されたメッセージ数が含まれます。左側のメニューを使用して、グローバル発生またはローカル発生のいずれか、および表示するメッセージの数を選択できます。カラム ヘッダーをクリックすることにより、表示をソートできます。

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

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

[Outbreak Filters] ページを表示するには、[Email] > [Reporting] > [Outbreak Filters] を選択します。図 4-21 に、[Outbreak Filters] ページの表示例を示します。

図 4-21　[Outbreaks] ページ



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

[System Capacity] ページ

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

[System Capacity] ページを使用すると、次の情報を確認できます。

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

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

- **量**：「正常」なメッセージ量と環境内での「通常」のスパイクを把握することが重要です。経時的にこのデータを追跡して、量の増加を測定します。[Incoming Mail] ページおよび [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、「[System Capacity] : [Incoming Mail]」（P.4-45）および「[System Capacity] : [Outgoing Mail]」（P.4-46）を参照してください。
- **作業キュー**：作業キューは、スパム攻撃の吸収とフィルタリングを行い、非スパム メッセージの異常な増加を処理する、「緩衝装置」として設計されています。ただし、作業キューは負荷のかかっているシステムを示す指標でもあります。長く、頻繁な作業キューのバックアップは、キャパシティの問題を示している可能性があります。[System Capacity] : [Workqueue] ページを使用すると、作業キュー内のアクティビティを追跡できます。詳細については、「[System Capacity] : [Workqueue]」（P.4-44）を参照してください。
- **リソース節約モード**：Cisco IronPort 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 Cisco IronPort 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、[System Capacity] ページでは追跡できません。

[System Capacity] ページに表示されるデータの解釈方法

[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。

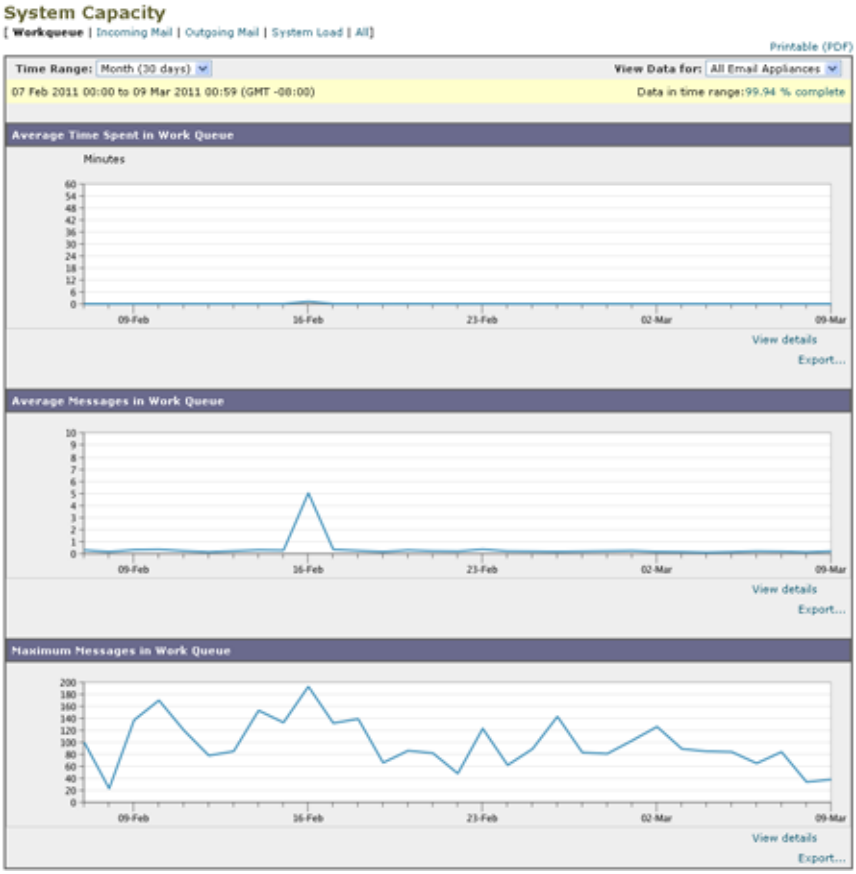
[System Capacity] ページの [Maximum] 値インジケータは、指定された期間の最大値を示します。[Average] 値は指定された期間のすべての値の平均です。集計期間は、レポートに対して選択された間隔に応じて異なります。たとえば、月単位のチャートの場合は、日付ごとの [Average] 値と [Maximum] 値を表示することができます。

特定のグラフの [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。

[System Capacity] : [Workqueue]

[System Capacity] : [Workqueue] ページには、指定された期間の作業キュー内のメッセージ量が表示されます。また、同じ期間の作業キュー内の最大メッセージも表示されます。日、週、月、または年のデータを表示することもできます。[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、作業キュー バックアップの頻度を測定し、10,000 メッセージを超える作業キュー バックアップに注意することが推奨されます。

図 4-22　[System Capacity] : [Workqueue]

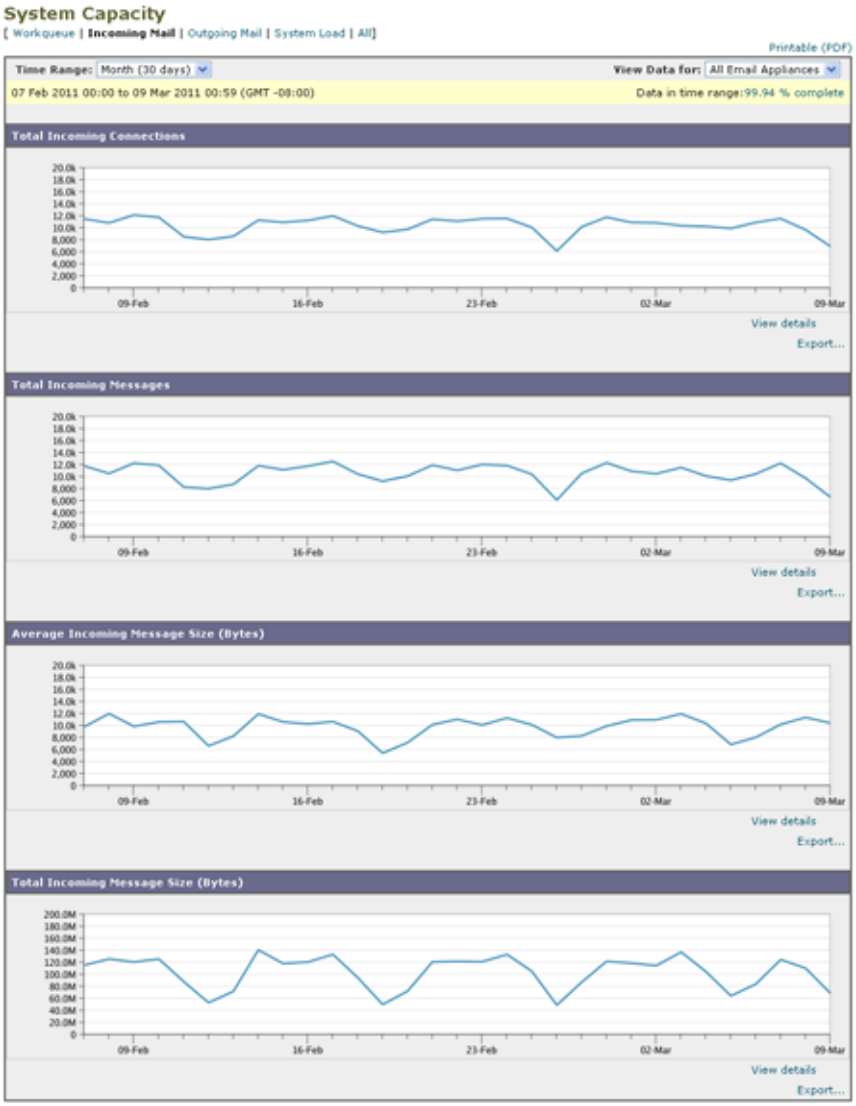


[System Capacity] : [Incoming Mail]

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

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

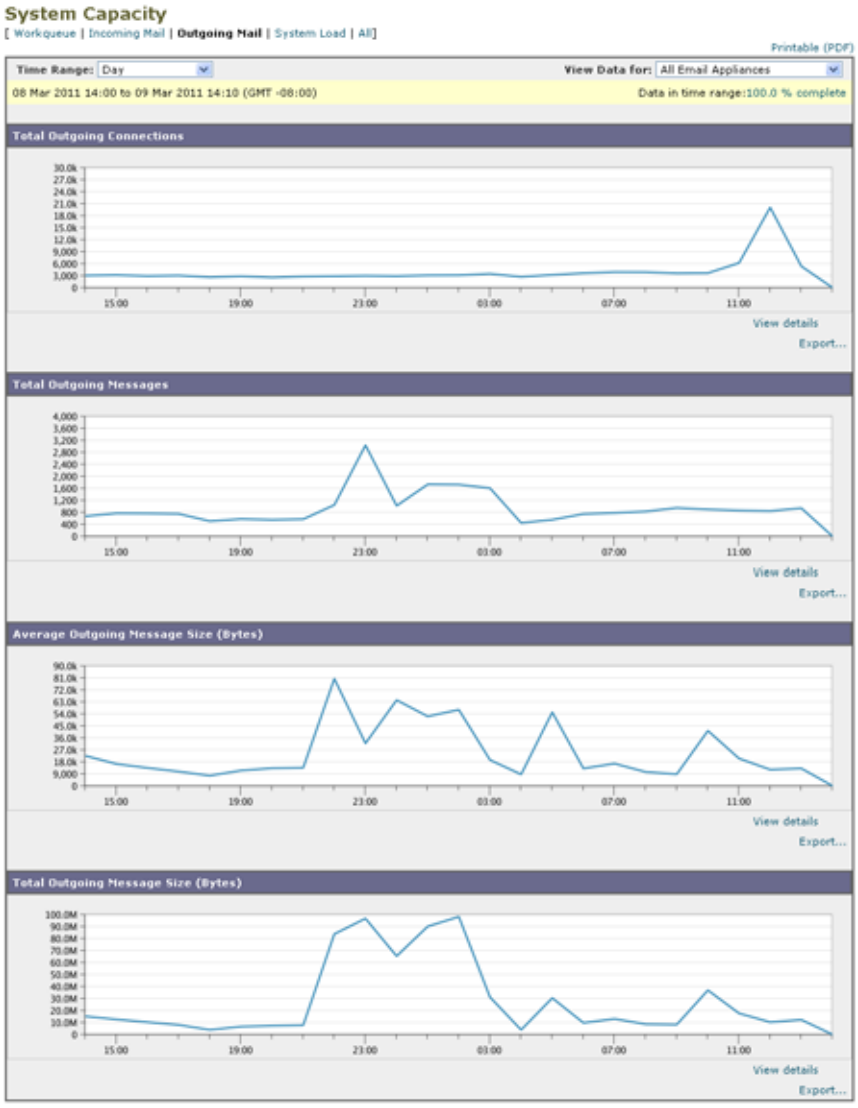
図 4-23　[System Capacity] : [Incoming Mail]



[System Capacity]：[Outgoing Mail]

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

図 4-24　[System Capacity]：[Outgoing Mail]



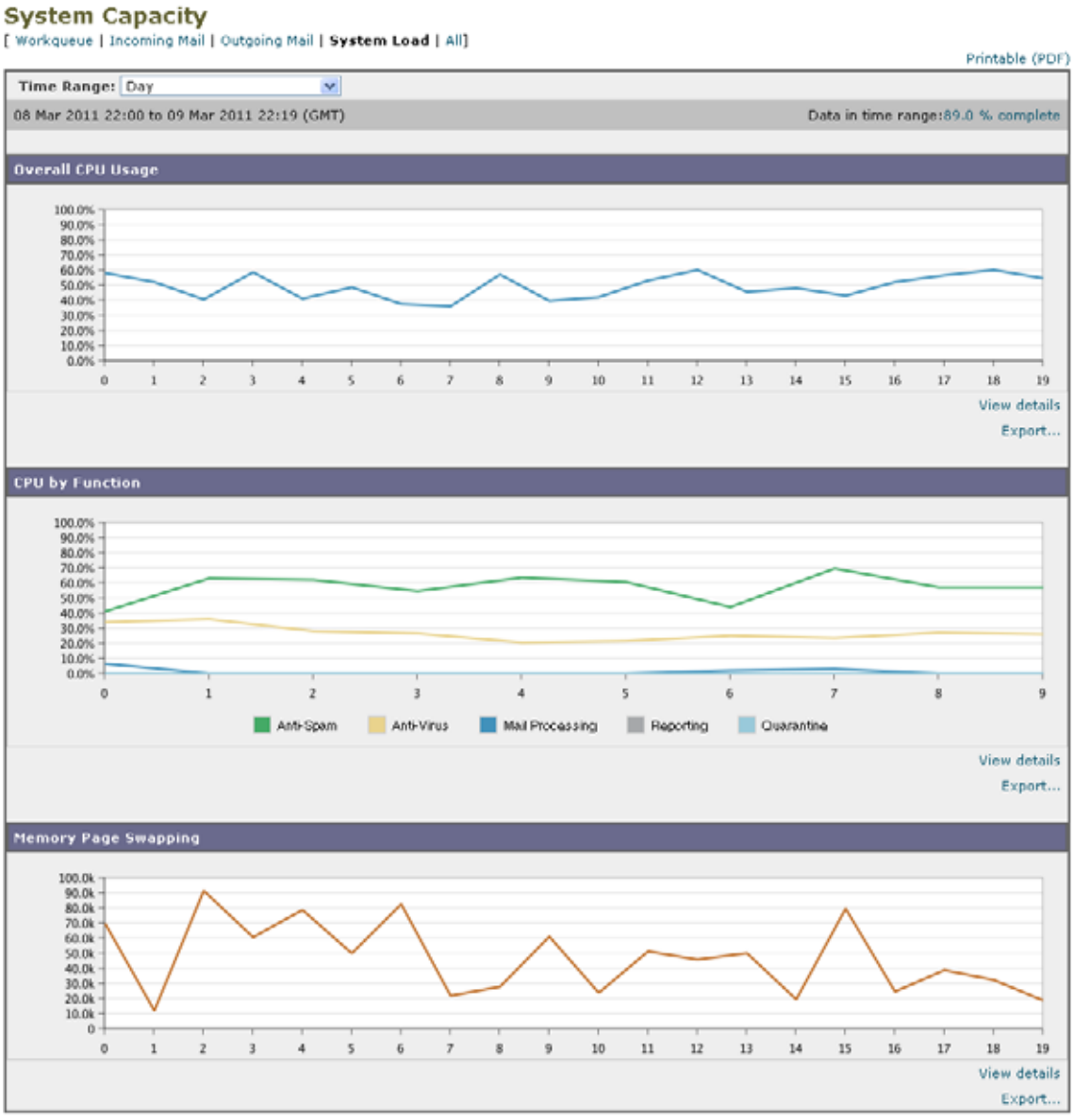
[System Capacity]：[System Load]

システム負荷レポートには、電子メール セキュリティ アプライアンスでの総 CPU 使用率が示されます。AsyncOS は、アイドル状態の CPU リソースを使用してメッセージ スループットを向上させるように最適化されています。CPU 使用率が高くても、必ずしもシステム キャパシティの問題を示すわけ

ではありません。CPU 使用率が高く、かつ高ボリュームのメモリ ページ スワッピングが発生する場合、キャパシティの問題の可能性があります。このページでは、メール処理、スパムおよびウイルス エンジン、レポート、および隔離などさまざまな機能によって使用される CPU の量を表示するグラフも示されます。機能別 CPU のグラフは、システム上で最も多くのリソース使用する製品の領域を示す指標です。アプライアンスの最適化が必要な場合、このグラフは、調整やディセーブル化の必要な機能を判断するのに役立ちます。

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

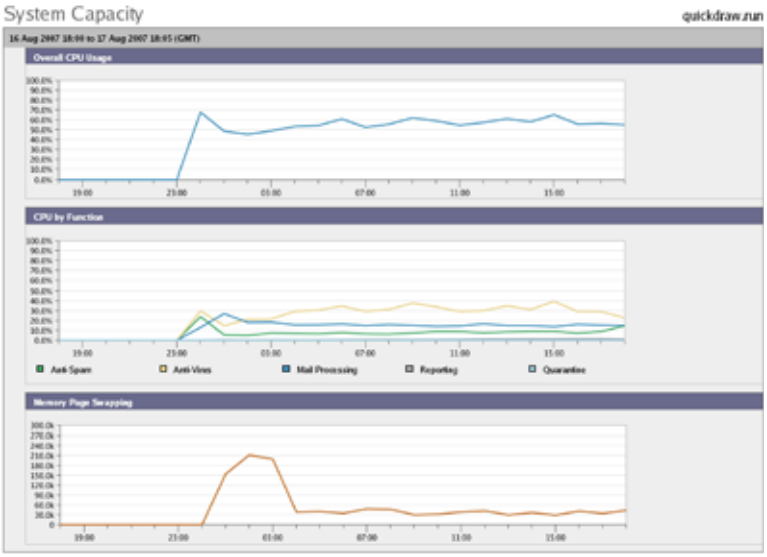
図 4-25　[System Capacity] : [System Load]



メモリ ページ スワッピングに関する注意事項

システムは、定期的にメモリをスワップするように設計されているので、一部のメモリ スワッピングは起こり得るものであり、アプライアンスの問題を示すものではありません。システムが*常に*高ボリュームのメモリ スワッピングを行う場合以外は、メモリ スワッピングは正常であり、起こり得る挙動です（特に C150 アプライアンスの場合）。たとえば、図 4-26 に、高ボリュームのメモリ スワッピングを常に行うシステムを示します。パフォーマンスを向上させるには、ネットワークに Cisco IronPort アプライアンスを追加するか、設定を調整して、最大のスループットを確保することが必要な場合もあります。

図 4-26　[System Capacity] : [System Load]（高負荷時のシステム）



[System Capacity] : [All]

[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。

[Reporting Data Availability] ページ

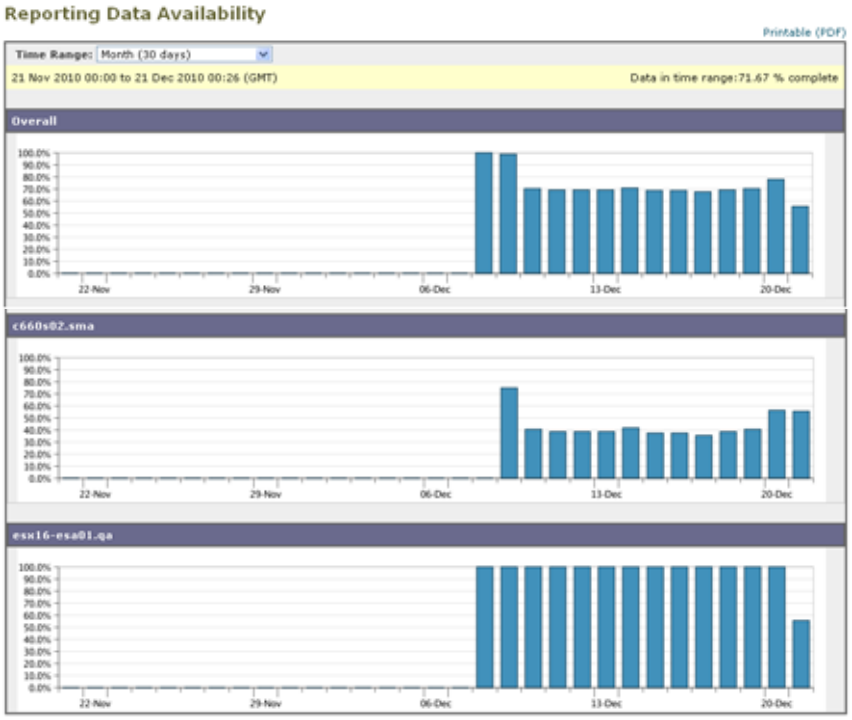
[Email] > [Reporting] > [Reporting Data Availability] ページでは、リソース使用率および電子メール トラフィックの障害のある場所がリアルタイムに表示されるようにデータを表示、更新およびソートできます。

[Reporting Data Availability] ページを表示するには、次の手順を実行します。

ステップ 1　セキュリティ管理アプライアンスのページで、[Email] > [Reporting] > [Reporting Data Availability] を選択します。

[Reporting Data Availability] ページが表示されます。

図 4-27　[Email Reporting Data Availability] ページ



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

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

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

使用可能なレポートの種類

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

- [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、「[Content Filters] ページ」（P.4-33）を参照してください。
- [DLP Incident Summary]：このページに表示される情報については、「[DLP Incident Summary] ページ」（P.4-31）を参照してください。
- [Delivery Status]：このレポート ページには、特定の受信者ドメインまた仮想ゲートウェイ アドレスへの配信の問題についての情報が表示されます。また、このページには、直近 3 時間以内にシステムによって配信されたメッセージの上位 20、50、または 100 の受信者ドメインのリストが表示されます。各統計情報のカラム見出しのリンクをクリックすることによって、最新のホスト ステータス、アクティブな受信者（デフォルト）、切断した接続、配信された受信者、ソフト バウン

ス イベント、およびハード バウンス受信者別にソートできます。電子メール セキュリティ アプライアンスの [Delivery Status] の詳細については、『*Cisco IronPort AsyncOS for Email Security Daily Management Guide*』を参照してください。

- [Domain-Based Executive Summary]：このレポートは 電子メール レポーティングの [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、「[Domain-Based Executive Summary] レポート」（P.4-51）を参照してください。
- [Executive Summary]：このレポートは 電子メール レポーティングの [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、「[Domain-Based Executive Summary] レポート」（P.4-51）を参照してください。
- [Incoming Mail Summary]：このページに表示される情報については、「[Incoming Mail] ページ」（P.4-15）を参照してください。
- [Internal Users Summary]：このページに表示される情報については、「[Internal Users] ページ」（P.4-28）を参照してください。
- [Outbreak Filters]：このページに表示される情報については、「[Outbreak Filters] ページ」（P.4-41）を参照してください。
- [Outgoing Destinations]：このページに表示される情報については、「[Outgoing Destinations] ページ」（P.4-25）を参照してください。
- [Outgoing Mail Summary]：このページに表示される情報については、「[Outgoing Senders] ページ」（P.4-27）を参照してください。
- [Outgoing Senders]：このページに表示される情報については、「[Outgoing Senders] ページ」（P.4-27）を参照してください。
- [Sender Groups]：このページに表示される情報については、「[Sender Groups] レポート ページ」（P.4-24）を参照してください。
- [System Capacity]：このページに表示される情報については、「[System Capacity] ページ」（P.4-43）を参照してください。
- [TLS Connections]：このページに表示される情報については、「[TLS Connections] ページ」（P.4-37）を参照してください。
- [Virus Types]：このページに表示される情報については、「[Virus Types] ページ」（P.4-35）を参照してください。

時間範囲

各レポートは、前日、過去 7 日間、前月、過去の日（最大 250 日）、または過去の月（最大 12 ヵ月）のデータを含めるように設定できます。また、指定した日数（2 ～ 100 日）または指定した月数（2 ～ 12 ヵ月）のデータを含めることもできます。

レポートの実行時間にかかわらず、直前の時間間隔（過去 1 時間、1 日、1 週間、または 1 ヵ月）のデータのみが含まれます。たとえば、日次レポートを午前 1 時に実行するようにスケジュールを設定した場合、レポートには前日の 00:00 から 23:59 までのデータが含まれます。

言語とロケール

（注） 個々のレポートに特定のロケールを使用して、PDF レポートをスケジュール設定したり、raw データを CSV ファイルとしてエクスポートしたりすることができます。[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。「レポート データの印刷とエクスポート」（P.3-7）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、「[Archived Email Reports] の表示と管理」（P.4-58）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 [Email] > [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。

- [Domain-Based Executive Summary] レポート
- [Executive Summary] レポート

[Domain-Based Executive Summary] レポート

[Domain-Based Executive Summary] レポートには、ネットワーク内の 1 つまたは複数のドメインの着信および発信メッセージの概要が表示されます。これは [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。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。その他のスケジュール設定されたレポートとは異なり、[Domain-Based Executive Summary] レポートはアーカイブされません。

レピュテーション フィルタリングによってブロックされたメッセージは作業キューに入らないため、AsyncOS はこれらのメッセージに対して、宛先ドメインを判定するための処理は行いません。アルゴリズムによって、ドメインごとに拒否されたメッセージ数が推定されます。ドメインごとのブロックされたメッセージの正確な数を知るには、メッセージ受信者レベル（RCPT TO）に達するまで Cisco IronPort セキュリティ管理アプライアンスで HAT 拒否を遅延します。そうすることで、AsyncOS が着信メッセージから受信者データを収集できるようになります。Cisco IronPort 電子メール セキュリティ アプライアンスで **listenerconfig -> setup** コマンドを使用すると、拒否を遅延できます。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。HAT 遅延拒否の詳細については、『Cisco IronPort AsyncOS for Email Security』関連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 [Domain-Based Executive Summary] レポートの [Stopped by Reputation Filtering] の結果を表示するには、電子メール セキュリティ アプライアンスと セキュリティ管理アプライアンスの両方で **hat_reject_info** をイネーブルにする必要があります。

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

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。

[Domain-Based Executive Summary] レポートを作成するには、次の手順を実行します。

ステップ 1　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. [Email] > [Reporting] > [Scheduled Reports] を選択します。

b. [Add Scheduled Report] をクリックします。

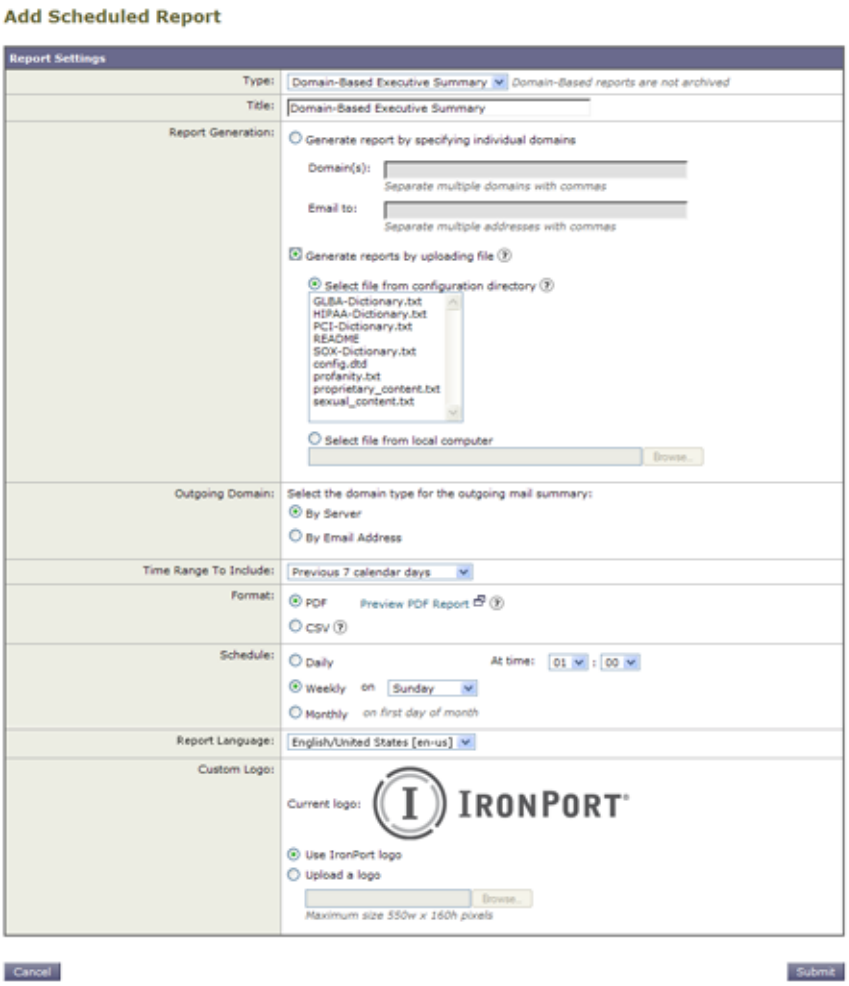
オンデマンド レポートを作成するには、次の手順を実行します。

a. [Email] > [Reporting] > [Archived Reports] を選択します。

b. [Generate Report Now] をクリックします。

ステップ 2　[Report Type] ドロップダウン リストから、[Domain-Based Executive Summary] レポート タイプを選択します。

図 4-28　[Domain-Based Executive Summary] レポートの追加



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

- [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。

- [Generate reports by uploading file]。レポートのドメイン、および受信者の電子メール アドレスのリストが含まれるコンフィギュレーション ファイルをインポートします。アプライアンスのコンフィギュレーション ディレクトリからコンフィギュレーション ファイルを選択することも、ローカル コンピュータからアップロードすることもできます。頻繁に変更される多数のドメインのレポートを作成する場合は、コンフィギュレーション ファイルの使用を推奨します。ドメインベースのレポートのコンフィギュレーション ファイルの詳細については、「[Domain-Based Executive Summary] レポートのコンフィギュレーション ファイル」（P.4-54）を参照してください。

（注）　外部アカウント（Yahoo! Mail や Gmail など）にレポートを送信する場合、レポーティング返信アドレスを外部アカウントのホワイトリストに追加して、レポート メッセージが誤ってスパムとして分類されないようにします。

ステップ 4　[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　[Outgoing Domain] セクションで、発信メール サマリーのドメイン タイプを選択します。選択肢は [By Server] または [By Email Address] です。

ステップ 6　[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　[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。[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　[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 [Daily]、[Weekly]（曜日のドロップダウン リストがあります）または [monthly] です。

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

- このロゴは、最大で 550 x 50 ピクセルの .jpg、.gif、または .png ファイルにする必要があります。
- ロゴ ファイルをアップロードしなかった場合、デフォルトの Cisco IronPort 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、「レポート データの印刷とエクスポート」（P.3-7）の重要な情報を参照してください。

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

[Domain-Based Executive Summary] レポートのコンフィギュレーション ファイル

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

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

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

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

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

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

[Executive Summary] レポート

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

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

[Scheduled Reports] ページ

- 電子メール レポートのスケジュール設定
- Web レポートのスケジュール設定

電子メール レポートのスケジュール設定

「スケジュール設定された電子メール レポートとオンデマンドの電子メール レポートについて」（P.4-49）に示されているすべてのレポートをスケジュール設定できます。

レポートのスケジュール設定の管理方法については、次を参照してください。

- 「スケジュール設定されたレポートの追加」（P.4-55）
- 「スケジュール設定されたレポートの編集」（P.4-56）
- 「スケジュール設定されたレポートの中止」（P.4-56）

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。

ステップ 1　セキュリティ管理アプライアンスのウィンドウで、[Email] > [Reporting] > [Scheduled Reports] を選択します。

ステップ 2　[Add Scheduled Report] をクリックします。

ステップ 3　レポート タイプを選択します。

レポート タイプの説明については、「スケジュール設定された電子メール レポートとオンデマンドの電子メール レポートについて」（P.4-49）を参照してください。

（注）　[Domain-Based Executive Summary] レポートの設定の詳細については、「[Domain-Based Executive Summary] レポート」（P.4-51）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　[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　[Time Range to Include] ドロップダウン メニューからレポートの時間範囲を選択します。

ステップ 6　生成されるレポートの**形式**を選択します。

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

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

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

ステップ 9　[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　[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、「レポート データの印刷とエクスポート」（P.3-7）の重要な情報を参照してください。

ステップ 12　[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

ステップ 1　セキュリティ管理アプライアンスのウィンドウで、[Email] > [Reporting] > [Scheduled Reports] を選択します。

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

ステップ 3　レポート設定値を変更します。

ステップ 4　変更を送信し、保存します。

スケジュール設定されたレポートの中止

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

ステップ 1　セキュリティ管理アプライアンスのウィンドウで、[Email] > [Reporting] > [Scheduled Reports] を選択します。

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

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」（P.4-59）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

「電子メール レポーティング ページの概要」（P.4-7）で説明したインタラクティブ レポート ページを使用して表示（および PDF を生成）できるレポートに加えて、「スケジュール設定された電子メール レポートとオンデマンドの電子メール レポートについて」（P.4-49）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。

ステップ 1　セキュリティ管理アプライアンスで、[Email] > [Reporting] > [Archived Reports] を選択します。

ステップ 2　[Generate Report Now] をクリックします。

ステップ 3　レポート タイプを選択します。

レポート タイプの説明については、「スケジュール設定された電子メール レポートとオンデマンドの電子メール レポートについて」（P.4-49）を参照してください。

ステップ 4　[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）　[Domain-Based Executive Summary] レポートの設定の詳細については、「[Domain-Based Executive Summary] レポート」（P.4-51）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　[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　[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。[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 raw データを含む 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　[Delivery Option] セクションから、次のオプションを選択します。

- [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 [Archived Reports] ページに表示されます。

  （注）　[Domain-Based Executive Summary] レポートはアーカイブできません。

- [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、「レポート データの印刷とエクスポート」（P.3-7）の重要な情報を参照してください。

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

[Archived Email Reports] ページ

[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 12 のインスタンスで、生成された最新のレポートをすべてのレポートに対して、合計 1000 バージョンまで保持します。12 インスタンスという制限は、同じ名前と時間範囲のスケジュール設定された各レポートに適用されます。

アーカイブ済みのレポートは自動的に削除されます。新しいレポートが追加されると、古いレポートが削除され、常に 1000 という数が維持されます。

アーカイブ済みのレポートは、アプライアンスの `/periodic_reports` ディレクトリに保管されます。（詳細については、付録 A「IP インターフェイスおよびアプライアンスへのアクセス」を参照してください）。

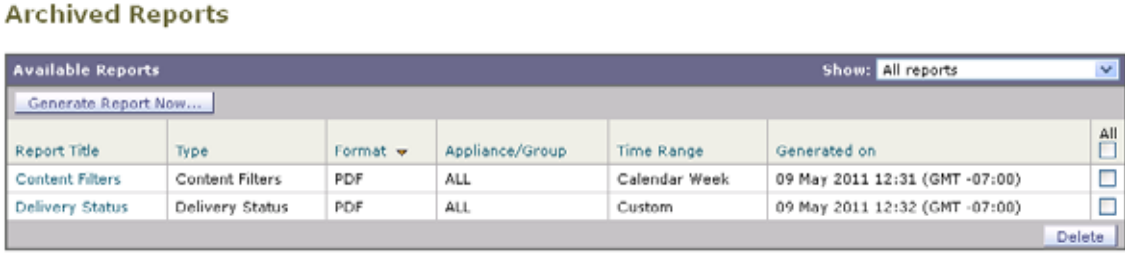
アーカイブ済みのレポートへのアクセス

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

ステップ 1　[Email] > [Reporting] > [Archived Reports] を選択します。

[Archived Reports] のリストが表示されます。

図 4-29　Archived Reports



ステップ 2　リストが長い場合に特定のレポートを見つけるには、[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　[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

「[Archived Email Reports] の表示と管理」（P.4-58）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。

ステップ 1　セキュリティ管理アプライアンスで、[Email] > [Reporting] > [Archived Reports] を選択します。

選択可能なアーカイブ済みのレポートが表示されます。

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

ステップ 3　[Delete] をクリックします。

ステップ 4　スケジュール設定されたレポートで、今後のインスタンスが生成されないようにするには、「スケジュール設定されたレポートの中止」（P.4-56）を参照してください。

CHAPTER 5

中央集中型 Web レポーティングの使用方法

中央集中型 Web レポーティングの概要

Web レポーティング機能は、個々のセキュリティ機能から情報を収集し、Web トラフィック パターンやセキュリティ リスクのモニタに使用できるデータを記録します。レポートをリアルタイムで実行して所定の期間内のシステム アクティビティをインタラクティブに表示したり、スケジュールを作成してレポートを定期的に実行したりできます。また、レポーティング機能を使用して、raw データをファイルにエクスポートすることもできます。

中央集中型 Web レポーティング機能を使用すると、管理者は概要レポートを作成してネットワークの現状を把握できるだけでなく、特定のドメイン、ユーザ、またはカテゴリのトラフィックの詳細を、ドリルダウンして確認できます。

ドメイン情報

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

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

ユーザ

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

- ユーザ「Jamie」がアクセスした上位ドメインのリスト

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

カテゴリ

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

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

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

一般

ロギング ページとレポーティング ページの詳細については、「ロギングとレポーティング」（P.14-1）を参照してください。

（注）　アクセスされた特定の URL だけでなく、ユーザが利用するすべてのドメイン情報を取得することができます。ユーザがアクセスしている特定の URL、その URL にアクセスした時刻、その URL が許可されているかどうかなどの情報を入手するには、[Web Tracking] ページの [Proxy Services] タブを使用します。

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

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

- インタラクティブ レポート ページを表示する場合は、「Web レポーティング ページについて」（P.5-7）を参照してください。
- レポートをオンデマンドで生成するには、「オンデマンドでの Web レポートの生成」（P.5-67）を参照してください。
- レポートが定期的に繰り返し作成されるようにスケジュールを設定する場合は、「スケジュール設定されたレポートとオンデマンド Web レポートについて」（P.5-63）を参照してください。
- 以前に実行されたレポート（スケジュール設定されたレポートとオンデマンドで生成されたレポートの両方）のアーカイブ版を表示する方法については、「アーカイブされた Web レポートの表示と管理」（P.5-69）を参照してください。

中央集中型 Web レポーティングの設定

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

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

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

セキュリティ管理アプライアンスで Web レポーティングを使用する前に、セキュリティ管理アプライアンスで Web レポーティングをイネーブルにする必要があります。

ステップ 1　中央集中型 Web レポーティングをイネーブルにする前に、十分なディスク領域がサービスに割り当てられていることを確認します。「ディスク使用量の管理」（P.13-58）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、[Management Appliance] > [Centralized Services] > [Web] > [Centralized Reporting] を選択します。

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

a.　[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、[Accept] をクリックします。

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

a.　[Edit Settings] をクリックします。

b.　[Enable Centralized Web Report Services] チェックボックスを選択します。

c.　「Web レポートでのユーザ名の匿名化」（P.5-4）はここで実行することも、後で実行することもできます。

ステップ 5　変更を送信し、保存します。

（注）　アプライアンスで Web レポーティングがイネーブルになっていて、この処理にディスク領域が割り当てられていない場合、ディスク領域が割り当てられるまで、中央集中型 Web レポーティングが機能しません。Web レポーティングおよびトラッキングに設定するクォータが、現在使用しているディスク領域よりも大きい場合、Web レポーティングおよびトラッキングのデータは失われません。詳細については、「ディスク使用量の管理」（P.13-58）を参照してください。

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

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

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

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

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

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

ステップ 1　セキュリティ管理アプライアンスで、[Management Appliance] > [Centralized Services] > [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. [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. [Add Web Appliance] をクリックします。

b. [Appliance Name and IP Address] テキスト フィールドに、Cisco IronPort アプライアンスの管理インターフェイスのアプライアンス名と IP アドレスを入力します。

（注） [IP Address] テキスト フィールドに DNS 名を入力した場合でも、[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. [Centralized Reporting] サービスが事前に選択されています。

d. [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、[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. [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. [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　[Submit] をクリックします。

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

ステップ 6　変更を保存します。

Web レポートでのユーザ名の匿名化

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

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

図 5-1　ユーザ名が表示されたレポーティング ページ

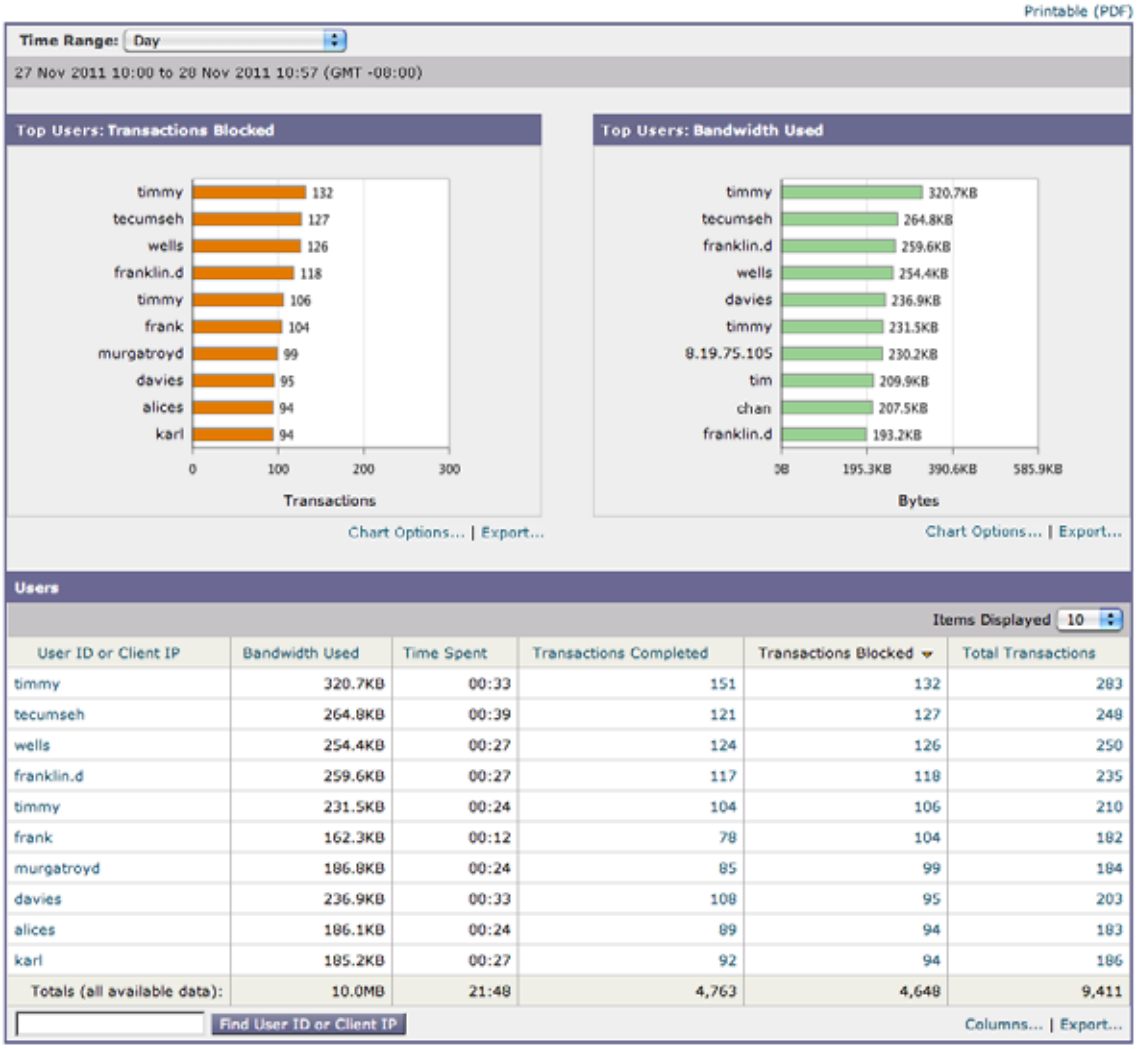
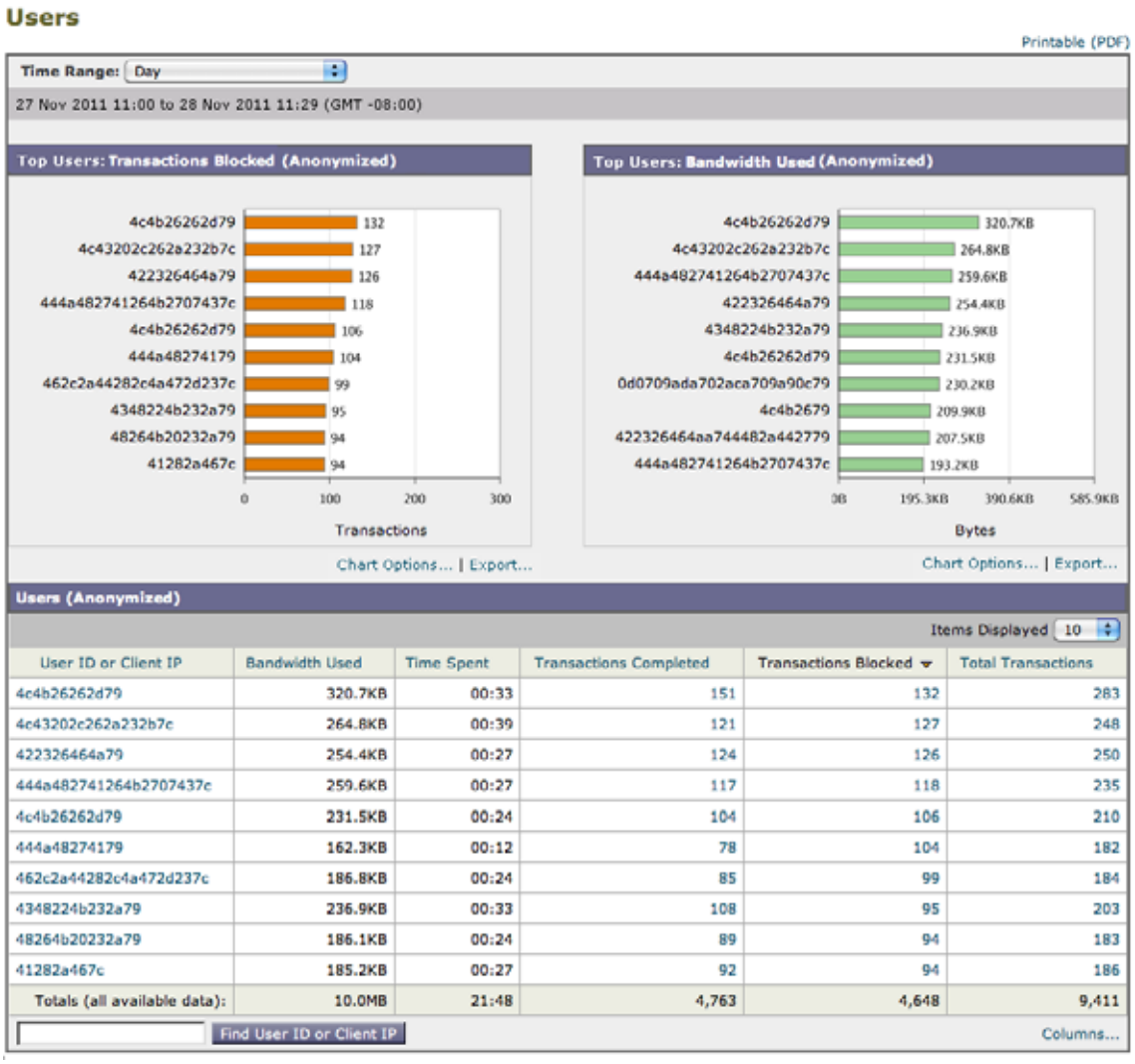


図 5-2　ユーザを匿名にしたレポーティング ページ



レポートでユーザ名を識別できないようにするには、次の手順を実行します。

ステップ 1　[Management Appliance] > [Centralized Services] > [Web] > [Centralized Reporting] を選択します。

ステップ 2　[Edit Settings] をクリックします。

ステップ 3　[Anonymize usernames in reports] チェックボックスをオンにします。

ステップ 4　変更を送信し、保存します。

インタラクティブ Web レポーティング ページの操作

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

これらのページの操作については、次の項目を参照してください。

表 5-1　インタラクティブ Web レポーティング ページの操作

目的	参照先
レポート データのアクセスおよび表示オプションを確認する	「レポーティング データを表示する方法」（P.3-1）
テーブル内のデータの意味を理解する	「Web レポーティング ページのテーブル カラムの説明」（P.5-10）
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	「インタラクティブ レポート ページのビューのカスタマイズ」（P.3-3）
データ内の情報を検索する	「[Web Tracking] ページ」（P.5-51）
レポート情報を印刷またはエクスポートする	「レポート データの印刷とエクスポート」（P.3-7）
さまざまなインタラクティブ レポート ページについて理解する	「Web レポーティング ページについて」（P.5-7）
レポートをオンデマンドで生成する	「スケジュール設定されたレポートとオンデマンド Web レポートについて」（P.5-63）
レポートが指定した間隔で所定の時刻に自動的に実行されるようスケジュールを設定する	「スケジュール設定されたレポートとオンデマンド Web レポートについて」（P.5-63）
アーカイブ済みのオンデマンド レポートとスケジュールされたレポートを表示する	「アーカイブされた Web レポートの表示と管理」（P.5-69）
データの収集方法を理解する	「セキュリティ アプライアンスによるレポート用データの収集方法」（P.3-2）

Web レポーティング ページについて

[Web] > [Reporting] タブには、レポート データを表示するためのオプションがいくつかあります。ここでは、このタブに表示される各レポーティング ページ、および各レポーティング ページに表示される情報について説明します。

（注）　[Web Reporting] タブのどのオプションをオンデマンドまたはスケジュール済みレポートとして使用できるかについては、「スケジュール設定されたレポートとオンデマンド Web レポートについて」（P.5-63）を参照してください。

表 5-2　[Web Reporting] タブの詳細

[Web Reporting] メニュー	アクション
Web レポーティングの [Overview] ページ	[Overview] ページには、お使いの Cisco IronPort アプライアンスでのアクティビティの概要が表示されます。これには、着信および発信トランザクションに関するグラフやサマリー テーブルも含まれます。詳細については、「Web レポーティングの [Overview] ページ」（P.5-13）を参照してください。
[Users] ページ	[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。 [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。 [Users] ページのインタラクティブな [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 [User Details] ページに表示されます。 [User Details] ページでは、[Web] > [Reporting] > [Users] ページのインタラクティブな [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、「[Users] ページ」（P.5-17）を参照してください。システムにおける各ユーザの情報については、「[User Details] ページ」（P.5-20）を参照してください。
[Web Sites] ページ	[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 Sites] ページ」（P.5-24）を参照してください。
[URL Categories] ページ	[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 Categories] ページ」（P.5-26）を参照してください。

表 5-2　[Web Reporting] タブの詳細（続き）

[Web Reporting] メニュー	アクション
[Application Visibility] ページ	[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、「[Application Visibility] ページ」（P.5-30）を参照してください。
Security	
[Anti-Malware] ページ	[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、「[Anti-Malware] ページ」（P.5-33）を参照してください。
[Client Malware Risk] ページ	[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、「[Client Malware Risk] ページ」（P.5-39）を参照してください。
[Web Reputation Filters] ページ	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 Reputation Filters] ページ」（P.5-41）を参照してください。
[L4 Traffic Monitor] ページ	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 Traffic Monitor] ページ」（P.5-44）を参照してください。
[Reports by User Location] ページ	[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、「[Reports by User Location] ページ」（P.5-49）を参照してください。
Reporting	

表 5-2　[Web Reporting] タブの詳細（続き）

[Web Reporting] メニュー	アクション
[Web Tracking] ページ	[Web Tracking] ページでは、次の 2 種類の情報を検索できます。 • [Proxy Services] タブでは、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 Traffic Monitor] タブでは、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。 詳細については、「[Web Tracking] ページ」（P.5-51）を参照してください。
[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、「[System Capacity] ページ」（P.5-57）を参照してください。
[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、「[Data Availability] ページ」（P.5-62）を参照してください。
Scheduled Reports	指定した時間範囲のレポートのスケジュールを設定できます。詳細については、「スケジュール設定されたレポートとオンデマンド Web レポートについて」（P.5-63）を参照してください。
Archived Reports	指定した時間範囲のレポートをアーカイブできます。詳細については、「アーカイブされた Web レポートの表示と管理」（P.5-69）を参照してください。

（注）　ほとんどの Web レポーティング カテゴリでレポートをスケジュール設定できます。これには、拡張された上位 URL カテゴリおよび上位アプリケーション タイプに関する追加のレポートが含まれます。レポートのスケジュール設定の詳細については、「スケジュール設定されたレポートとオンデマンド Web レポートについて」（P.5-63）を参照してください。

Web レポーティング ページのテーブル カラムの説明

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

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

レポートでのテーブルの操作の詳細については、「レポート ページのテーブルのカスタマイズ」（P.3-5）を参照してください。

表 5-3　Web レポーティング ページのテーブル カラムの説明

カラム名	説明
Domain or Realm	テキスト形式で表示されるユーザのドメインまたはレルム。
UserID or Client IP	テキスト形式で表示されるユーザのユーザ ID またはクライアント IP。
Bandwidth Used	特定のユーザまたはアクションによって使用される帯域幅の量。帯域幅の単位は、バイトまたは % で表示されます。
Bandwidth Saved by Blocking	特定のトランザクションのブロックのため節約された帯域幅の量。帯域幅単位はバイトで表示されます。

表 5-3　Web レポーティング ページのテーブル カラムの説明（続き）

カラム名	説明
Time Spent	Web ページに費やされた時間。各 URL カテゴリでユーザが費やした時間。ユーザを調査する目的で使用されます。URL のトラッキング時には、その特定の URL に各ユーザが費やした時間。 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、[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。
Allowed URL Category	許可されたカテゴリの数とタイプ。単位はトランザクション タイプで表示されます。
Monitored URL Category	モニタリングされているカテゴリの数とタイプ。単位はトランザクション タイプで表示されます。
Warned URL Category	警告が発行されたカテゴリの数とタイプ。単位はトランザクション タイプで表示されます。
Blocked by URL Category	URL カテゴリが原因でブロックされたトランザクション。単位はトランザクション タイプで表示されます。
Blocked by Application or Application Type	アプリケーション タイプが原因でブロックされたアプリケーション。単位はトランザクション タイプで表示されます。
Blocked by Web Reputation	Web レピュテーションのためブロックされたトランザクション。単位はトランザクション タイプで表示されます。
Blocked by Anti-Malware	Anti-Malware によってブロックされたトランザクション。単位はトランザクション タイプで表示されます。

表 5-3　Web レポーティング ページのテーブル カラムの説明（続き）

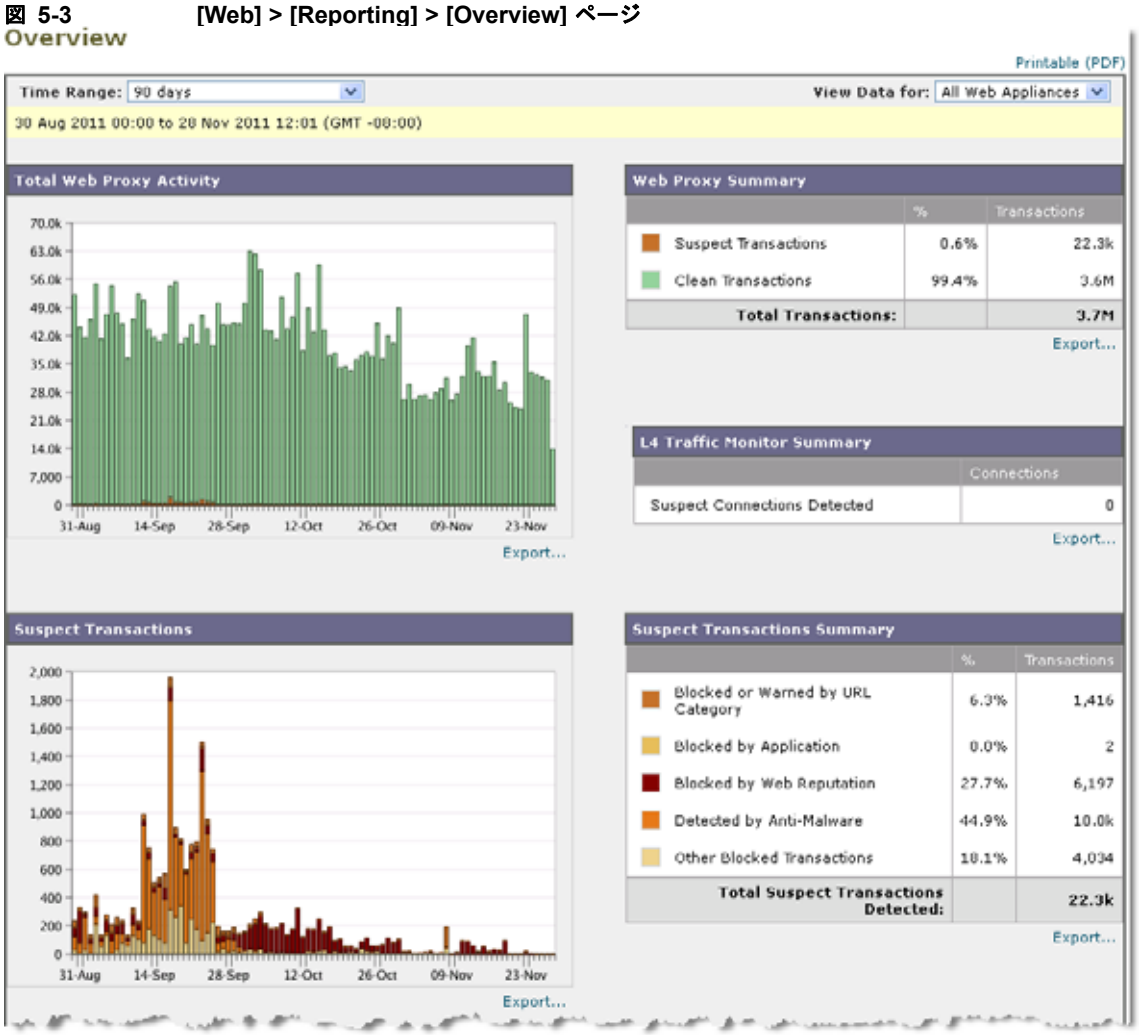
カラム名	説明
Other Blocked Transactions	ブロックされた他のすべてのトランザクション。単位はトランザクション タイプで表示されます。
Transactions with Bandwidth Limit	帯域幅の制限があるトランザクションの数。
Transactions without Bandwidth Limit	帯域幅の制限がないトランザクションの数。
Transactions Blocked by Application	特定のアプリケーション タイプによってブロックされたトランザクションの数。
Warned Transactions	ユーザに警告が発せられたすべてのトランザクション。単位はトランザクション タイプで表示されます。
Transactions Completed	ユーザが完了したトランザクション。単位はトランザクション タイプで表示されます。
Transactions Blocked	ブロックされたすべてのトランザクション。単位はトランザクション タイプで表示されます。
Total Transactions	発生したトランザクションの合計数。

Web レポーティングの [Overview] ページ

[Web] > [Reporting] > [Overview] ページでは、お使いの Cisco IronPort アプライアンスでのアクティビティの概要が表示されます。これには、着信および発信トランザクションに関するグラフやサマリーテーブルも含まれます。

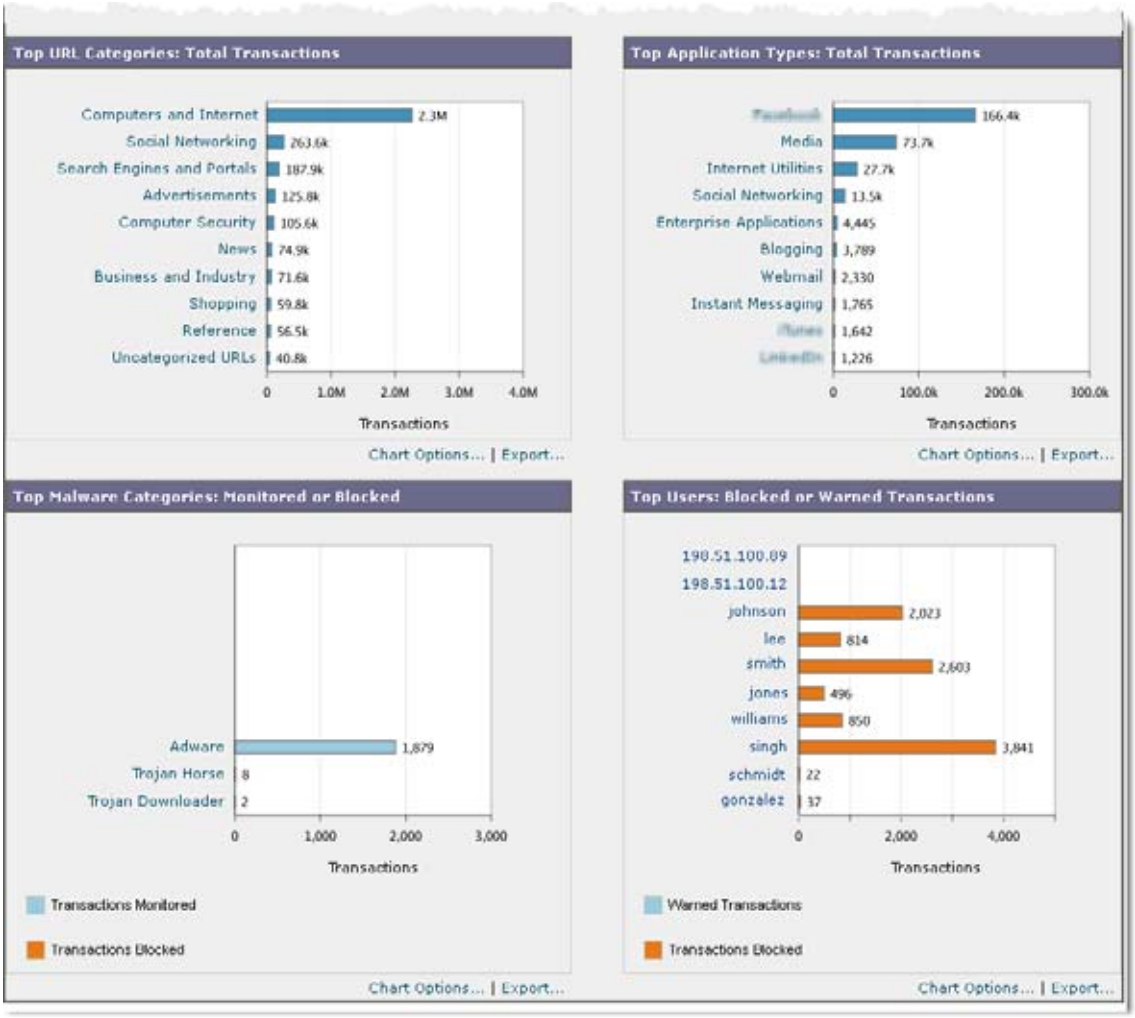
図 5-3 に、[Overview] ページを示します。

図 5-3　[Web] > [Reporting] > [Overview] ページ



（次のページに続く）

（前ページからの続き）



[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。

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

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

表 5-4　[Web] > [Reporting] > [Overview] ページの詳細

セクション	説明
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、「インタラクティブ レポートの時間範囲の選択」（P.3-4）を参照してください。
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、[All Web Appliances] を選択します。 「アプライアンスによるレポーティング データの制約」（P.3-3）も参照してください。
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 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 Traffic Monitor Summary	このセクションには、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レイヤ 4 トラフィックが表示されます。
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。
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。
Top URL Categories by Total Transactions	このセクションには、ブロックされている上位 10 の URL カテゴリが表示されます。URL カテゴリのタイプ（縦の目盛り）、特定タイプのカテゴリが実際にブロックされた回数（横の目盛り）などがあります。 すでに定義されている一連の URL カテゴリは更新されることがあります。こうした更新によるレポート結果への影響については、「URL カテゴリ セットの更新とレポート」（P.5-28）を参照してください。
Top Application Types by Total Transactions	このセクションには、ブロックされている上位アプリケーション タイプが表示されます。これには、実際のアプリケーション タイプ名（縦の目盛り）、特定のアプリケーションがブロックされた回数（横の目盛り）が含まれます。

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

セクション	説明
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。
Top Users Blocked or Warned Transactions	このセクションには、ブロックされたトランザクションまたは警告が発行されたトランザクションを生成している実際のユーザが表示されます。ユーザは IP アドレスまたはユーザ名で表示できます。ユーザ名を識別できないようにするには、「Web レポートでのユーザ名の匿名化」（P.5-4）を参照してください。

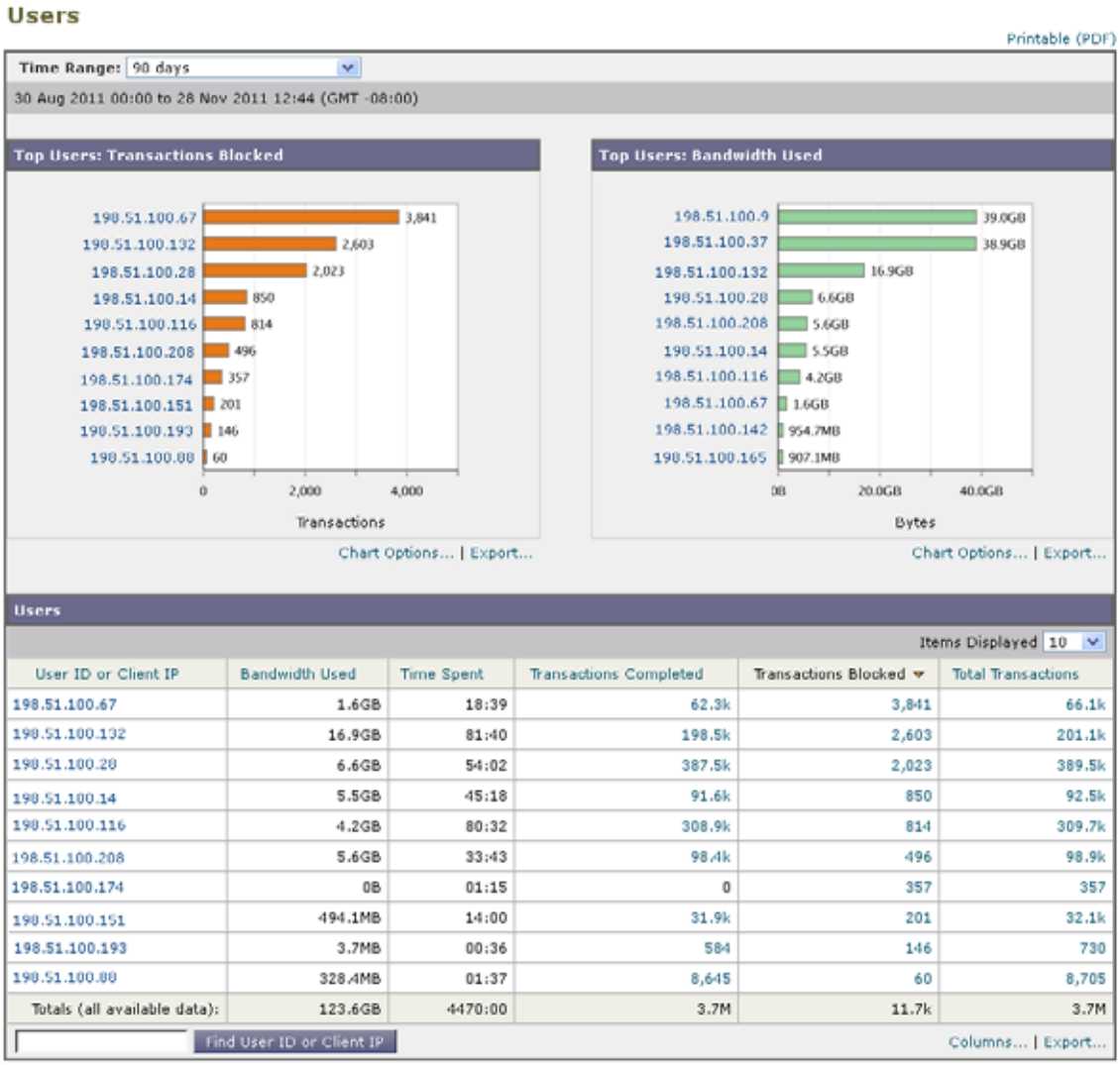
[Users] ページ

[Web] > [Reporting] > [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。

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

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

図 5-4　[Web] > [Reporting] > [Users] ページ



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

表 5-5　[Web] > [Reporting] > [Users] ページの詳細

セクション	説明
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、「インタラクティブ レポートの時間範囲の選択」（P.3-4）を参照してください。
Top Users by Transactions Blocked	このセクションには、IP アドレスまたはユーザ名で示された上位ユーザ（縦の目盛り）、そのユーザがブロックされたトランザクションの数（横の目盛り）が表示されます。レポーティングを目的として、ユーザ名または IP アドレスを認識できないようにすることができます。このページまたはスケジュール設定されたレポートでユーザ名を認識不可能にする方法の詳細については、「セキュリティ管理アプライアンスでの中央集中型 Web レポーティングのイネーブル化」（P.5-3）を参照してください。デフォルト設定では、すべてのユーザ名が表示されます。ユーザ名を非表示にするには、「Web レポートでのユーザ名の匿名化」（P.5-4）を参照してください。
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。
[Users] テーブル	このテーブルのデータの詳細については、「Web レポーティング ページのテーブル カラムの説明」（P.5-10）を参照してください。 さらに、特定のユーザ ID またはクライアント IP アドレスを検索できます。[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、[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。 [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、[User Details] ページに表示されます。[User Details] ページの詳細については、「[User Details] ページ」（P.5-20）を参照してください。

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

ヒント このレポートのビューをカスタマイズするには、「インタラクティブ Web レポーティング ページの操作」（P.5-6）を参照してください。

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

（注）　[Users] ページについて、レポートを生成またはスケジュールすることができます。詳細については、「スケジュール設定されたレポートとオンデマンド Web レポートについて」（P.5-63）を参照してください。

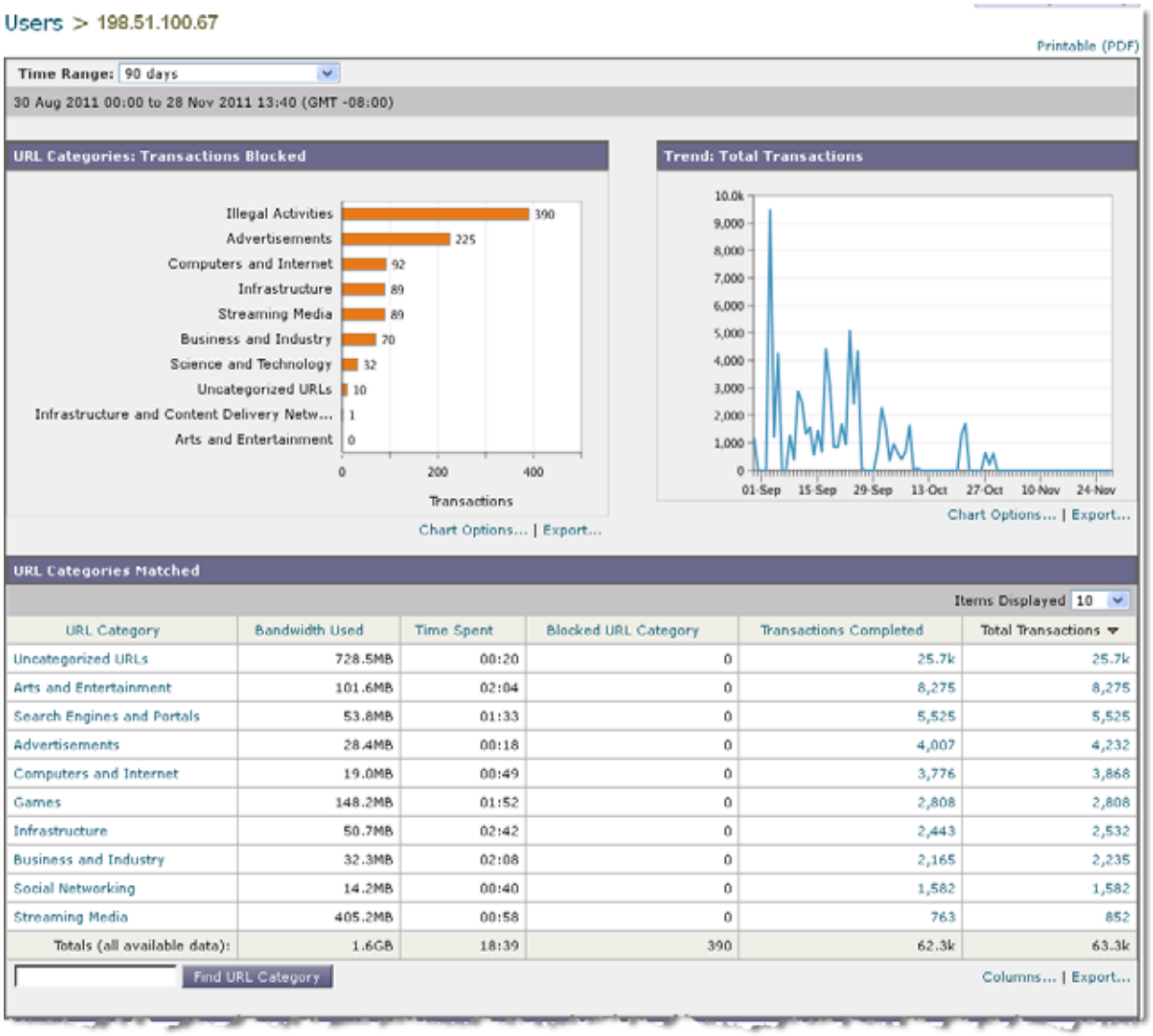
[User Details] ページ

[User Details] ページでは、[Web] > [Reporting] > [Users] ページのインタラクティブな [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。

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

図 5-5　[User Details] ページ



（次のページに続く）

（前ページからの続き）

Domains Matched

Items Displayed 10

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

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

Applications Matched

Items Displayed 10

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

Find Application　　Columns... | Export...

Malware Threats Detected

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

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

Policies Matched

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

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

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

表 5-6　[Web] > [Reporting] > [User] > [User Details] ページの詳細

セクション	説明
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、「インタラクティブ レポートの時間範囲の選択」（P.3-4）を参照してください。
URL Categories by Total Transactions	このセクションには、特定のユーザが使用している特定の URL カテゴリのリストが表示されます。 すでに定義されている一連の URL カテゴリは更新されることがあります。こうした更新によるレポート結果への影響については、「URL カテゴリ セットの更新とレポート」（P.5-28）を参照してください。
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。[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。
URL Categories Matched	[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、[Find URL Category] をクリックします。カテゴリは正確に一致している必要はありません。 すでに定義されている一連の URL カテゴリは更新されることがあります。こうした更新によるレポート結果への影響については、「URL カテゴリ セットの更新とレポート」（P.5-28）を参照してください。
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、[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。
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、[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、[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。

表 5-6　[Web] > [Reporting] > [User] > [User Details] ページの詳細（続き）

セクション	説明
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 [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、[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。
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、[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。

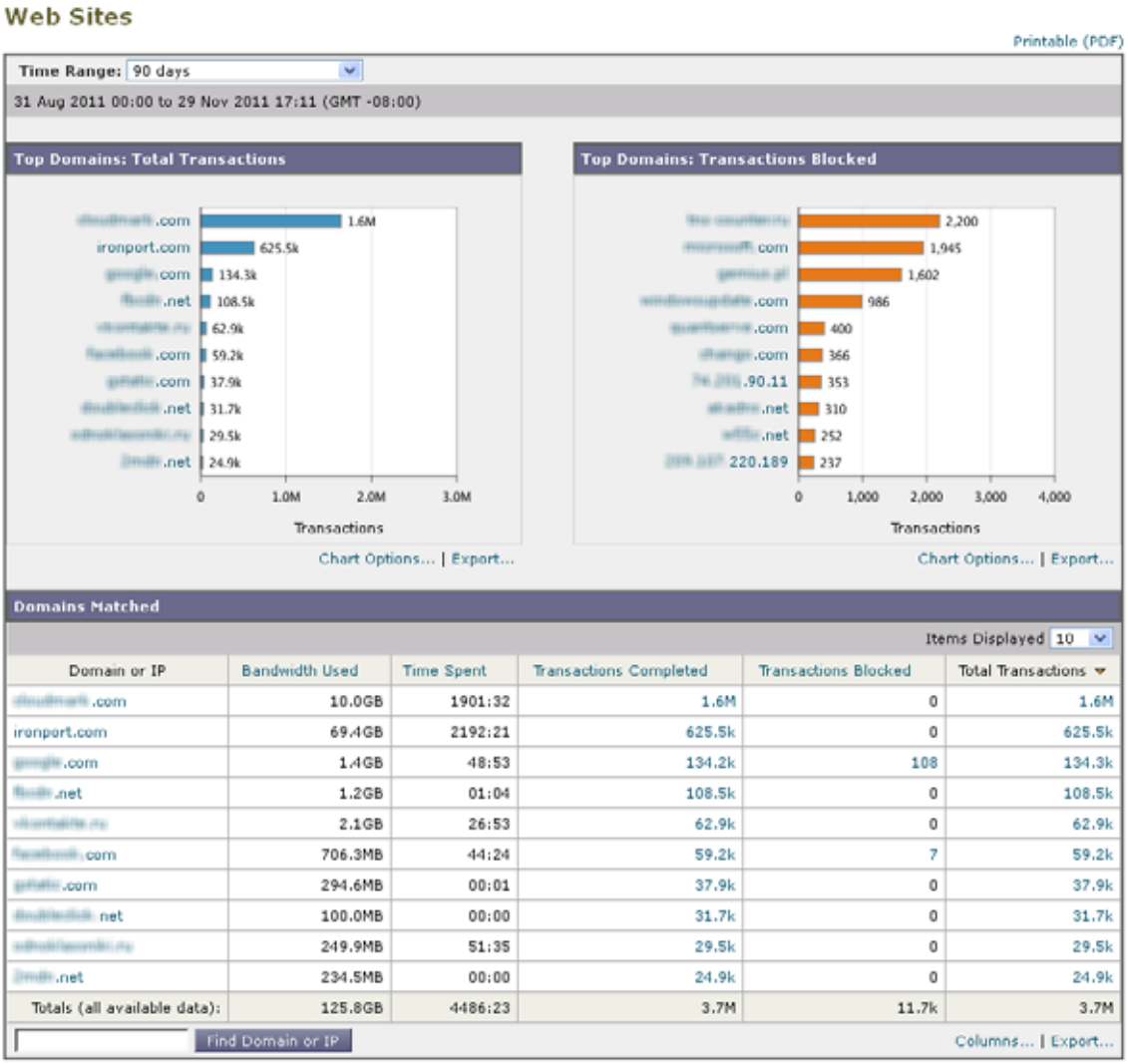
（注）　[Client Malware Risk Details] テーブルのクライアント レポートでは、ユーザ名の末尾にアスタリスク（*）が付いていることがあります。たとえば、クライアント レポートに「jsmith」と「jsmith*」の両方のエントリが表示される場合があります。アスタリスク（*）が付いているユーザ名は、ユーザの指定したユーザ名が認証サーバで確認されていないことを示しています。この状況は、認証サーバがその時点で使用できず、かつ認証サービスを使用できないときもトラフィックを許可するようにアプライアンスが設定されている場合に発生します。

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

[Web Sites] ページ

[Web] > [Reporting] > [Web Sites] ページでは、管理対象のアプライアンスで発生しているアクティビティ全体を集約したものです。このページでは、特定の時間範囲内にアクセスされたリスクの高い Web サイトをモニタできます。

図 5-6　[Web Sites] ページ



[Web Sites] ページには次の情報が表示されます。

表 5-7　[Web] > [Reporting] > [Web Sites] ページの詳細

セクション	説明
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、「インタラクティブ レポートの時間範囲の選択」（P.3-4）を参照してください。
Top Domains by Total Transactions	このセクションには、サイト上でアクセスされた上位ドメインがグラフ形式で表示されます。

表 5-7　[Web] > [Reporting] > [Web Sites] ページの詳細（続き）

セクション	説明
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。
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 Tracking] ページに [Proxy Services] タブが表示され、トラッキング情報と、特定のドメインがブロックされた理由を確認できます。 このテーブルのデータの詳細については、「Web レポーティング ページのテーブル カラムの説明」（P.5-10）を参照してください。 特定のドメインをクリックすると、そのドメインの上位ユーザ、そのドメインでの上位トランザクション、一致した URL カテゴリ、および検出されたマルウェアの脅威が表示されます。 Web トラッキングの使用例については、「例 2：URL のトラッキング」（P.D-5）を参照してください。

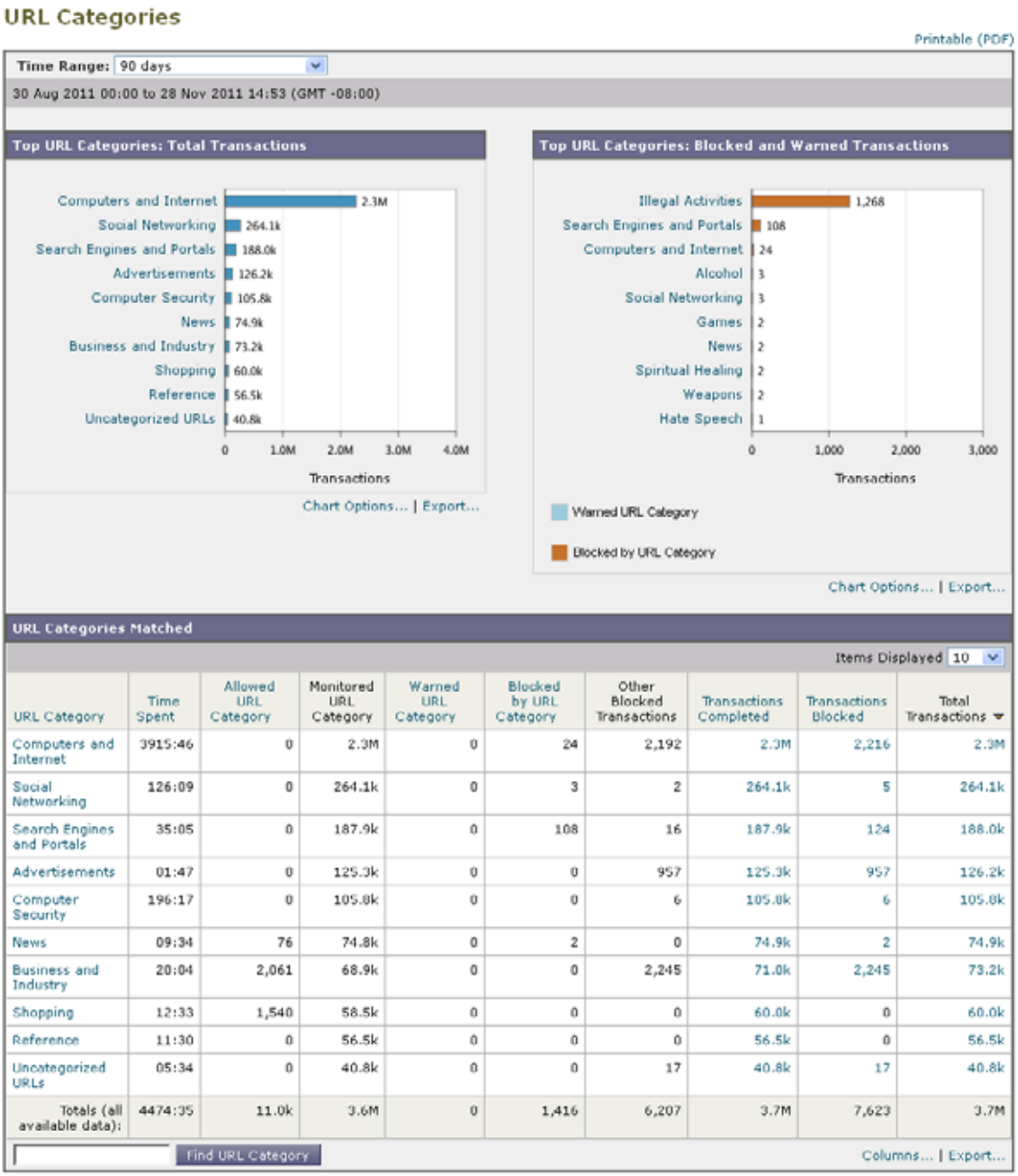
ヒント　このレポートのビューをカスタマイズするには、「インタラクティブ Web レポーティング ページの操作」（P.5-6）を参照してください。

（注）　[Web Sites] ページの情報について、レポートを生成またはスケジュールすることができます。詳細については、「スケジュール設定されたレポートとオンデマンド Web レポートについて」（P.5-63）を参照してください。

[URL Categories] ページ

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

図 5-7　[URL Categories] ページ



[URL Categories] ページには次の情報が表示されます。

表 5-8　[Web] > [Reporting] > [URL Categories] ページの詳細

セクション	説明
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、「インタラクティブ レポートの時間範囲の選択」（P.3-4）を参照してください。
Top URL Categories by Total Transactions	このセクションには、サイト上でアクセスされた上位 URL カテゴリがグラフ形式で表示されます。

表 5-8　[Web] > [Reporting] > [URL Categories] ページの詳細（続き）

セクション	説明
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。
URL Categories Matched	[URL Categories Matched] セクションには、指定した時間範囲内における URL カテゴリ別のトランザクションの処理、使用された帯域幅、各カテゴリで費やされた時間が表示されます。 未分類の URL の比率が 15 ～ 20 % を上回る場合は、次のオプションを検討してください。 • 特定のローカライズされた URL の場合は、カスタム URL カテゴリを作成し、特定のユーザまたはグループ ポリシーに適用できます。詳細については、『*Cisco IronPort AsyncOS for Web Security User Guide*』の「Custom URL Categories」を参照してください。 • 既存またはその他のカテゴリに含めるべきサイトについては、「誤って分類された URL と未分類の URL のレポート」（P.5-29）を参照してください。

ヒント　このレポートのビューをカスタマイズするには、「インタラクティブ Web レポーティング ページの操作」（P.5-6）を参照してください。

（注）
- このページよりもさらに詳細なレポートを生成するには、「Top URL Categories — Extended」（P.5-65）を参照してください。
- URL カテゴリに関するスケジュール設定されたレポート内でデータ アベイラビリティが使用されている場合に、いずれかのアプライアンスでデータに欠落があると、ページの下部に「`Some data in this time range was unavailable.`」というメッセージが表示されます。欠落がない場合は何も表示されません。

URL カテゴリ セットの更新とレポート

「URL カテゴリ セットの更新と中央集中型コンフィギュレーション管理」（P.8-23）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 Categories] ページとその他のレポーティング ページの併用

[URL Categories] ページと [Application Visibility] ページおよび [Users] ページを併用すると、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 Categories] ページで、サイトからアクセスされたすべての URL カテゴリの詳細を表示する、人事部門向けの概要レポートを生成できます。同じページの [URL 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。[Streaming Media] カテゴリ リンクをクリックすると、特定の [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（[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（[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、[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 [User Details] ページが表示され、そのユーザのトレンドを確認し、そのユーザの Web での行動を正確に把握できます。

さらに詳しい情報が必要な場合は、インタラクティブ テーブルで [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 Tracking] ページに [Proxy Services] タブが表示され、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 Categories] ページの他の使用例については、「例 3：アクセス数の多い URL カテゴリの調査」（P.D-6）を参照してください。

誤って分類された URL と未分類の URL のレポート

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

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

送信内容は評価され、今後のルール更新に活用されます。

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

[Application Visibility] ページ

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

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

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

- 回避アプリケーション（アノニマイザや暗号化トンネルなど）。
- コラボレーション アプリケーション（Cisco WebEx、Facebook、インスタント メッセージングなど）。
- リソースを大量消費するアプリケーション（ストリーミング メディアなど）。

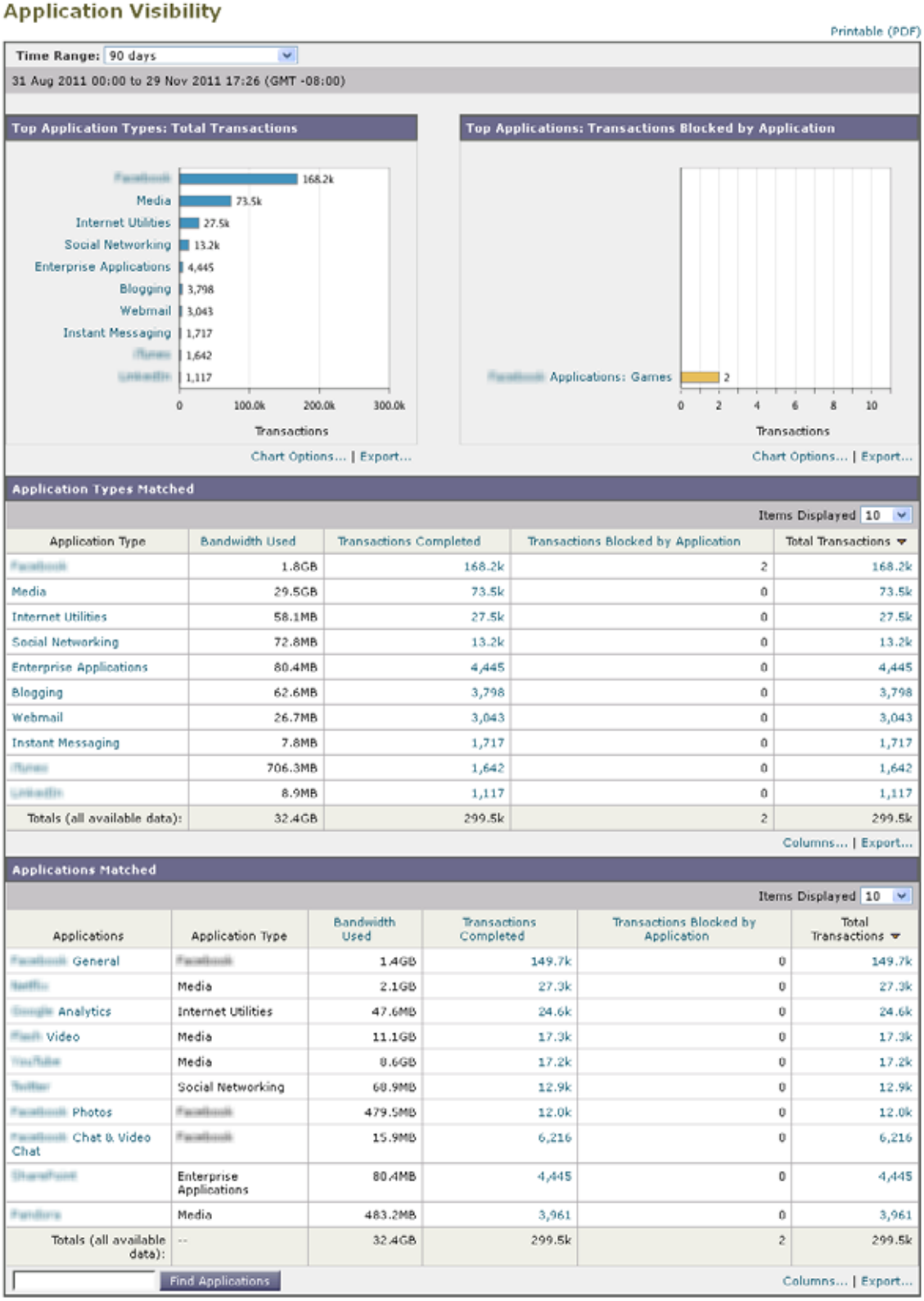
アプリケーションとアプリケーション タイプの違いについて

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

- **アプリケーション タイプ。**1 つまたは複数のアプリケーションを含むカテゴリです。たとえば**検索エンジン**は、Google Search や Craigslist などの検索エンジンを含むアプリケーション タイプです。インスタント メッセージングは、Yahoo Instant Messenger や Cisco WebEx などを含む別のアプリケーション タイプです。Facebook もアプリケーション タイプです。
- **アプリケーション。**アプリケーション タイプに属している特定のアプリケーションです。たとえば、YouTube はメディア アプリケーション タイプに含まれるアプリケーションです。
- **アプリケーション動作。**アプリケーション内でユーザが実行できる特定のアクションまたは動作です。たとえば、ユーザは Yahoo Messenger などのアプリケーションの使用中にファイルを転送できます。すべてのアプリケーションに、設定可能なアプリケーション動作が含まれているわけではありません。

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

図 5-8　[Application Visibility] ページ



[Application Visibility] ページには次の情報が表示されます。

表 5-9　[Web] > [Reporting] > [Application Visibility] ページの詳細

セクション	説明
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、「インタラクティブ レポートの時間範囲の選択」（P.3-4）を参照してください。
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。
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。
Application Types Matched	[Application Types Matched] インタラクティブ テーブルでは、[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。[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。
Applications Matched	[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。 [Applications Matched] セクションに表示するカラムを設定することができます。このセクションのカラムの設定については、「インタラクティブ Web レポーティング ページの操作」（P.5-6）を参照してください。 [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 [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、[Application 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、[Find Application] をクリックします。

ヒント　このレポートのビューをカスタマイズするには、「インタラクティブ Web レポーティング ページの操作」（P.5-6）を参照してください。

（注）　[Application Visibility] ページの情報に関して、スケジュール設定されたレポートを生成することができます。レポートのスケジュール設定については、「スケジュール設定されたレポートとオンデマンド Web レポートについて」（P.5-63）を参照してください。

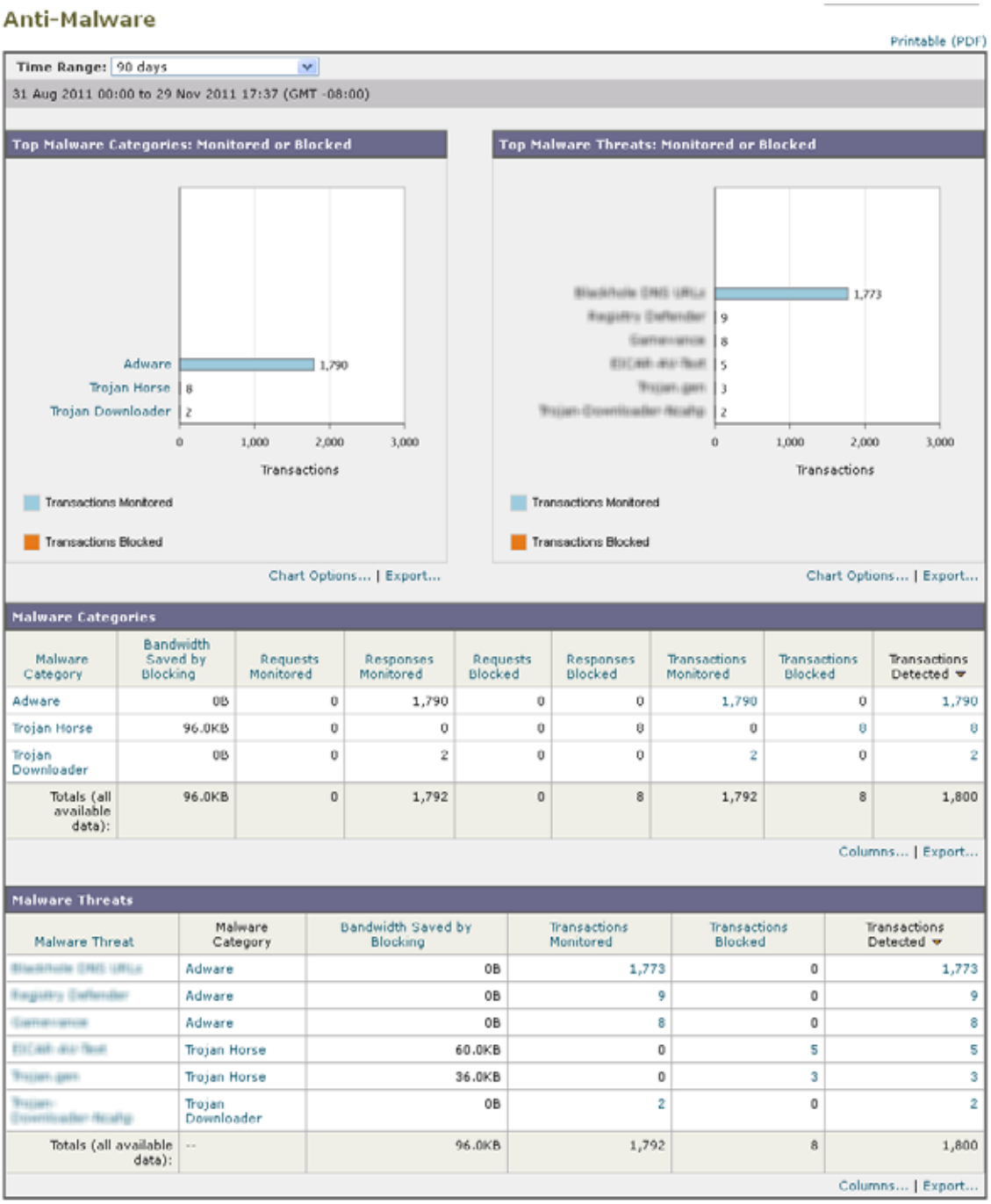
[Anti-Malware] ページ

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

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

（注）　L4 トラフィック モニタリングで検出されたマルウェアのデータを表示するには、「[L4 Traffic Monitor] ページ」（P.5-44）を参照してください。

図 5-9　[Anti-Malware] ページ



[Anti-Malware] ページには次の情報が表示されます。

表 5-10　[Web] > [Reporting] > [Anti-Malware] ページの詳細

セクション	説明
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、「インタラクティブ レポートの時間範囲の選択」（P.3-4）を参照してください。
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、表 5-10（P.5-38）を参照してください。
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。
Malware Categories	[Malware Categories] インタラクティブ テーブルには、[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。 [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 [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、表 5-10（P.5-38）を参照してください。
Malware Threats	[Malware Threats] インタラクティブ テーブルには、[Top Malware Threats] セクションに表示されている個々のマルウェアの脅威に関する詳細情報が表示されます。 「Outbreak」のラベルと番号が付いている脅威は、他のスキャン エンジンとは別に、Adaptive Scanning 機能によって特定された脅威です。 **（注）** [Malware Threat] でテーブルを昇順にソートすると、リストの最上部に [Unnamed Malware] が表示されます。

ヒント　このレポートのビューをカスタマイズするには、「インタラクティブ Web レポーティング ページの操作」（P.5-6）を参照してください。

[Malware Category] レポート ページ

[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。

[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。

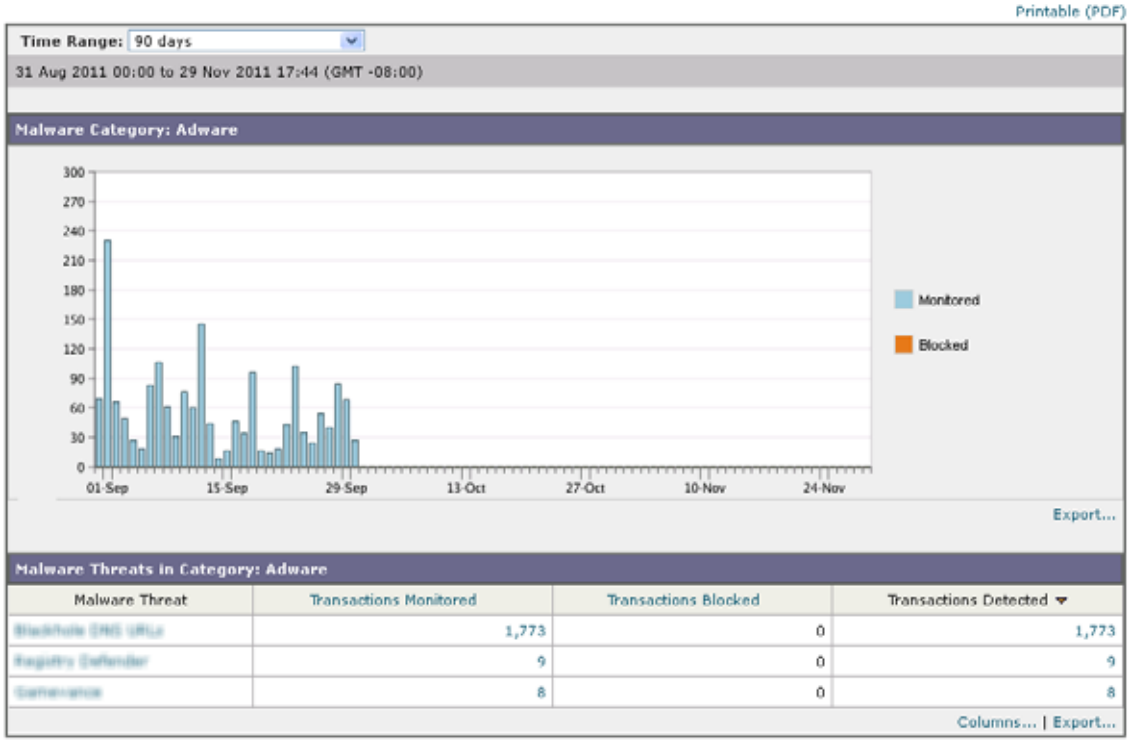
ステップ 1　セキュリティ管理アプライアンスのウィンドウで、[Web] > [Reporting] > [Anti-Malware] を選択します。

[Anti-Malware] ページが表示されます。

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

[Malware Category] レポート ページが表示されます。

図 5-10　[Malware Category] レポート ページ



ステップ 3　このレポートのビューをカスタマイズするには、「インタラクティブ Web レポーティング ページの操作」（P.5-6）を参照してください。

[Malware Threat] レポート ページ

[Malware Threat] レポート ページには、特定の脅威にさらされているクライアント、および感染した可能性があるクライアントのリストが表示され、[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。

[Malware Threat] レポート ページにアクセスするには、次の手順を実行します。

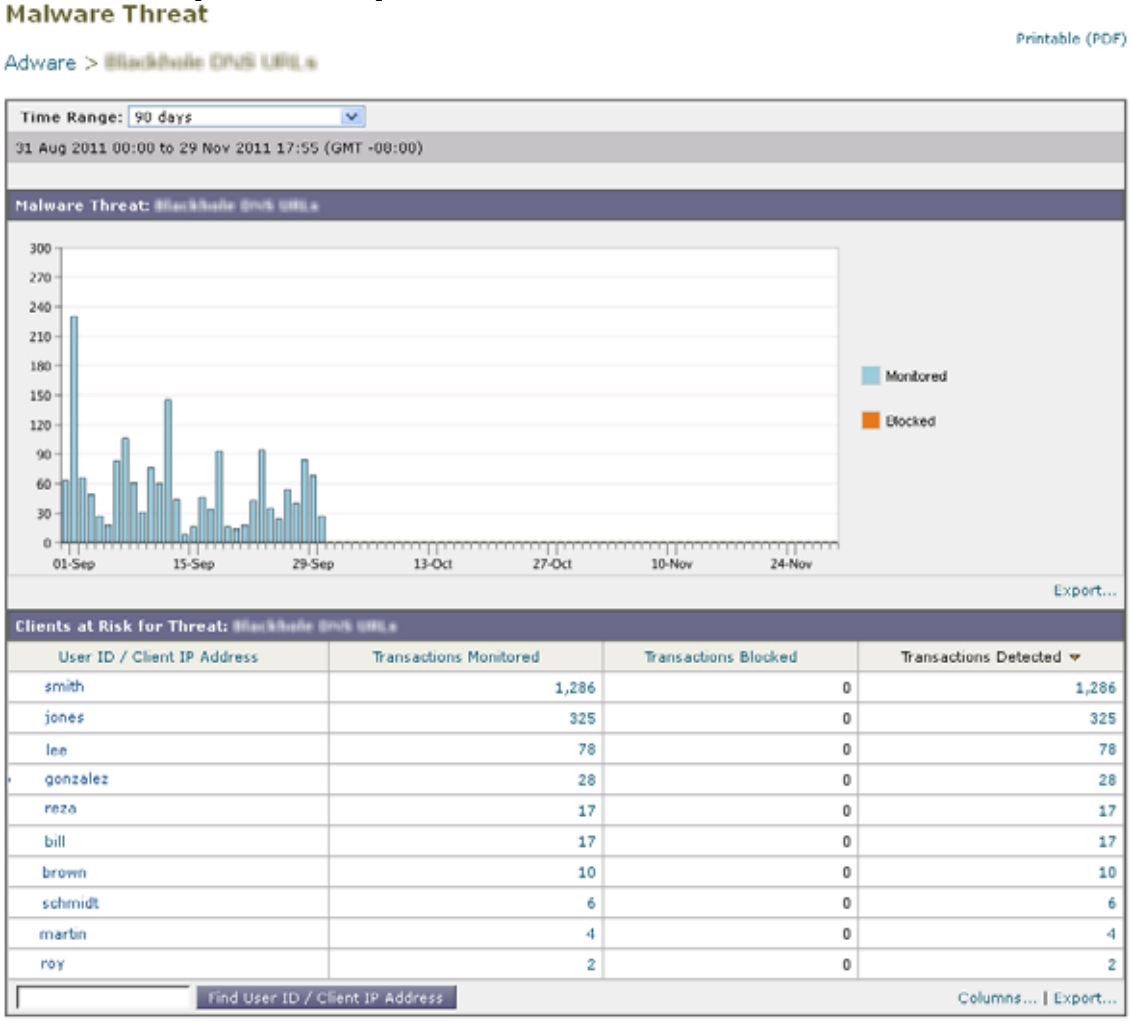
ステップ 1　セキュリティ管理アプライアンスのウィンドウで、[Web] > [Reporting] > [Anti-Malware] を選択します。

[Anti-Malware] ページが表示されます。

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

[Malware Threat] レポート ページが表示されます。

図 5-11　[Malware Threat] レポート ページ



ステップ 3　このレポートのビューをカスタマイズするには、「インタラクティブ Web レポーティング ページの操作」（P.5-6）を参照してください。

ステップ 4　詳細については、テーブルの下の [Support Portal Malware Details] リンクをクリックしてください。

（注）　[Anti-Malware] ページの [Top Malware Categories Detected] および [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、[Malware Categories] および [Malware Threats] レポート ページから生成されるレポートを、スケジュール設定することはできません。レポートのスケジュール設定については、「スケジュール設定されたレポートとオンデマンド Web レポートについて」（P.5-63）を参照してください。

マルウェアのカテゴリについて

次の表に、Web セキュリティ アプライアンスでブロックできるさまざまなマルウェアのカテゴリを示します

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。アドウェア アプリケーションの中には、別々のプロセスを同時に実行して互いをモニタさせて、変更を永続化するものがあります。変異型の中には、マシンが起動されるたびに自らが実行されるようにするものがあります。また、これらのプログラムによってセキュリティ設定が変更されて、ユーザがブラウザ検索オプション、デスクトップ、およびその他のシステム設定を変更できなくなる場合もあります。
ブラウザ ヘルパー オブジェクト	ブラウザ ヘルパー オブジェクトは、広告の表示やユーザ設定の乗っ取りに関連するさまざまな機能を実行するおそれがあるブラウザ プラグインです。
商用システム モニタ	商用システム モニタは、正当な手段によって正規のライセンスで取得できる、システム モニタの特性を備えたソフトウェアです。
ダイヤラ	ダイヤラは、モデムあるいは別のタイプのインターネット アクセスを利用して、ユーザの完全で有効な承諾なしに、長距離通話料のかかる電話回線またはサイトにユーザを接続するプログラムです。
一般的なスパイウェア	スパイウェアはコンピュータにインストールされるタイプのマルウェアで、ユーザに知られることなくその詳細情報を収集します。
ハイジャッカー	ハイジャッカーは、ユーザの完全で有効な承諾なしにユーザを Web サイトに誘導したりプログラムを実行したりできるように、システム設定を変更したり、ユーザのシステムに不要な変更を加えたりします。
その他のマルウェア	このカテゴリは、定義済みのどのカテゴリにも当てはまらないマルウェアと疑わしい動作に使用されます。
アウトブレイク ヒューリスティック	このカテゴリは、他のアンチマルウェア エンジンとは別に、Adaptive Scanning によって検出されたマルウェアを示しています。
フィッシング URL	フィッシング URL は、ブラウザのアドレス バーに表示されます。場合によっては、正当なドメインを模倣したドメイン名が使用されます。フィッシングは、ソーシャル エンジニアリングと技術的欺瞞の両方を使用して個人データや金融口座の認証情報を盗み出す、オンライン ID 盗難の一種です。
PUA	望ましくないアプリケーションのこと。PUA は、悪質ではないが好ましくないと見なされるアプリケーションです。
システム モニタ	システム モニタには、次のいずれかのアクションを実行するソフトウェアが含まれます。 公然と、または密かに、システム プロセスやユーザ アクションを記録する。 これらの記録を後で取得して確認できるようにする。
トロイのダウンローダ	トロイのダウンローダは、インストール後にリモート ホスト/サイトにアクセスして、リモート ホストからパッケージやアフィリエイトをインストールするトロイの木馬です。これらのインストールは、通常はユーザに気付かれることなく行われます。また、トロイのダウンローダはリモート ホストまたはサイトからダウンロード命令を取得するので、インストールごとにペイロードが異なる場合があります。
トロイの木馬	トロイの木馬は、安全なアプリケーションを装う有害なプログラムです。ウイルスとは異なり、トロイの木馬は自己複製しません。

マルウェアのカテゴリについて（続き）

マルウェアのタイプ	説明
トロイのフィッシャ	トロイのフィッシャは、感染したコンピュータに潜んで特定の Web ページがアクセスされるのを待つか、または感染したマシンをスキャンして銀行サイト、オークション サイト、あるいはオンライン支払サイトに関係するユーザ名とパスワードを探します。
ウイルス	ウイルスは、ユーザが気付かない間にコンピュータにロードされ、ユーザの意思に反して実行されるプログラムまたはコードです。
ワーム	ワームは、コンピュータ ネットワーク上で自己を複製し、通常は悪質なアクションを実行するプログラムまたはアルゴリズムです。

[Client Malware Risk] ページ

[Web] > [Reporting] > [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。

[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 [Client Malware Risk] ページには、L4 トラフィック モニタ（L4TM）によって特定された、頻度の高いマルウェア接続に関与しているクライアント IP アドレスが表示されます。マルウェア サイトに頻繁に接続するコンピュータは、マルウェアに感染している可能性があります。これらのマルウェアは中央のコマンド/コントロール サーバに接続しようとするので、除去しなければなりません。

図 5-12 に [Client Malware Risk] ページを示します。

図 5-12　[Client Malware Risk] ページ

Client Malware Risk

Printable (PDF)

Time Range: 90 days

31 Aug 2011 00:00 to 29 Nov 2011 18:15 (GMT -08:00)

Web Proxy - Top Clients: Monitored or Blocked

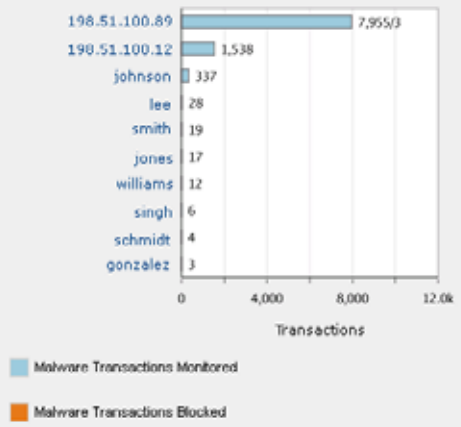


Chart Options... | Export...

L4 Traffic Monitor: Malware Connections Detected

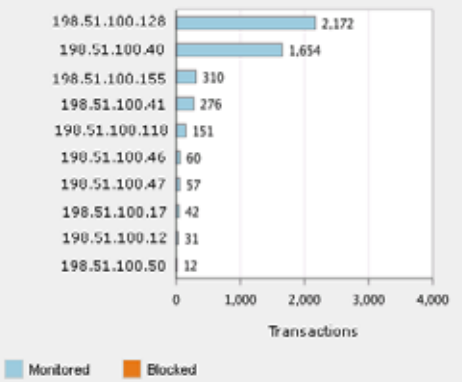


Chart Options... | Export...

Web Proxy - Client Malware Risk

Items Displayed 10

User ID / Client IP Address	Malware Transactions Monitored	Malware Transactions Blocked	Total Malware Transactions Detected
198.51.100.89	7,955	3	7,958
198.51.100.12	1,538	0	1,538
johnson	337	0	337
lee	28	0	28
smith	19	0	19
jones	17	0	17
williams	12	0	12
singh	6	0	6
schmidt	4	0	4
gonzalez	0	3	3
Totals (all available data):	9,918	8	9,926

Find User ID / Client IP Address

Columns... | Export...

L4 Traffic Monitor - Clients by Malware Risk

Items Displayed 10

Client IP	Malware Connections Monitored	Malware Connections Blocked	Total Malware Connections Detected
198.51.100.128	2,172	0	2,172
198.51.100.40	1,654	0	1,654
198.51.100.155	310	0	310
198.51.100.41	276	0	276
198.51.100.110	151	0	151
198.51.100.46	60	0	60
198.51.100.47	57	0	57
198.51.100.17	42	0	42
198.51.100.12	31	0	31
198.51.100.50	12	0	12
Totals (all available data):	4,795	0	4,795

Filter by Port

Columns... | Export...

表 5-11 で [Client Malware Risk] ページの情報について説明します。

表 5-11　[Client Malware Risk] レポート ページの内容

セクション	説明
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、「インタラクティブ レポートの時間範囲の選択」（P.3-4）を参照してください。
Web 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 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 Traffic Monitor] ページ」（P.5-44）の [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 Proxy: Client Malware Risk	[Web Proxy: Client Malware Risk] テーブルには、[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 [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、「[User Details] ページ」（P.5-20）を参照してください。 テーブルで任意のリンクをクリックすると、個々のユーザと、マルウェアのリスクをトリガーしているそのユーザのアクティビティをさらに詳しく表示できます。たとえば [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 [User] ページに移動します。
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 Traffic Monitor] ページ」（P.5-44）の [Client Source IPs] テーブルと同じです。テーブルの操作についてはこの項を参照してください。

ヒント　このレポートのビューをカスタマイズするには、「インタラクティブ Web レポーティング ページの操作」（P.5-6）を参照してください。

[Web Reputation Filters] ページ

[Web] > [Reporting] > [Web Reputation Filters] は、指定した時間範囲内のトランザクションに対する Web レピュテーション フィルタ（ユーザが設定）の結果を表示する、セキュリティ関連のレポーティング ページです。

Web レピュテーション フィルタとは

Web レピュテーション フィルタは、Web サーバの動作を分析し、URL ベースのマルウェアが含まれている可能性を判断するためのレピュテーション スコアを URL に割り当てます。この機能は、エンドユーザのプライバシーや企業の機密情報を危険にさらす URL ベースのマルウェアを防ぐために役立ち

ます。Web セキュリティ アプライアンスは、URL レピュテーション スコアを使用して、疑わしいアクティビティを特定するとともに、マルウェア攻撃を未然に防ぎます。Web レピュテーション フィルタは、アクセス ポリシーと復号化ポリシーの両方と組み合わせて使用できます。

Web レピュテーション フィルタでは、統計的に有意なデータを使用してインターネット ドメインの信頼性が評価され、URL のレピュテーションにスコアが付けられます。特定のドメインが登録されていた期間、Web サイトがホストされている場所、Web サーバがダイナミック IP アドレスを使用しているかどうかなどのデータを使用して、特定の URL の信頼性が判定されます。

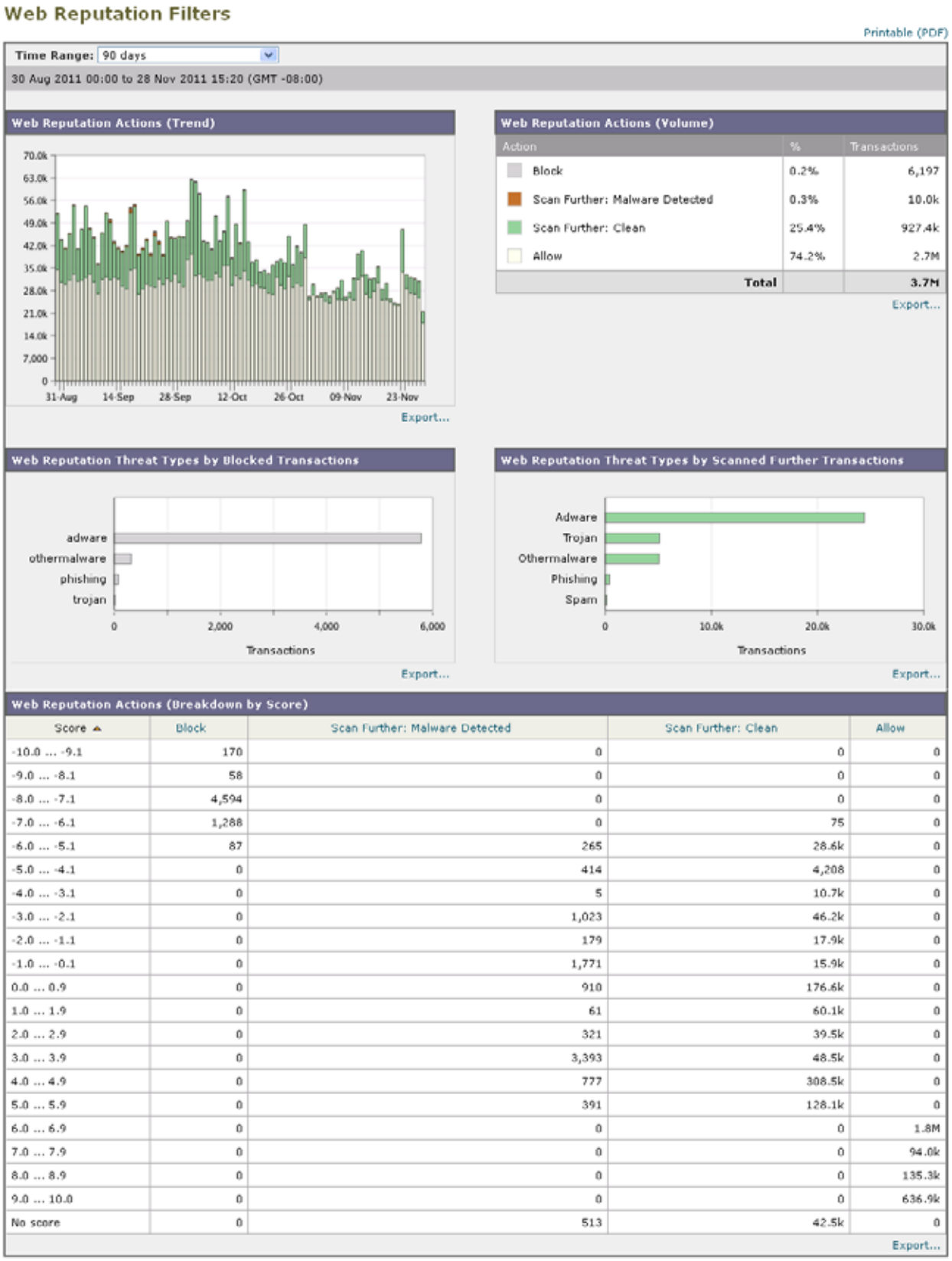
Web レピュテーションの計算では、URL をネットワーク パラメータに関連付けて、マルウェアが存在する可能性が判定されます。マルウェアが存在する可能性の累計が、-10 ～ +10 の Web レピュテーション スコアにマッピングされます（+10 がマルウェアを含む可能性が最も低い）。

パラメータには、たとえば次のものがあります。

- URL 分類データ
- ダウンロード可能なコードの存在
- 長く不明瞭なエンドユーザ ライセンス契約書（EULA）の存在
- グローバルなボリュームとボリュームの変更
- ネットワーク オーナー情報
- URL の履歴
- URL の経過時間
- ブロック リストに存在
- 許可リストに存在
- 人気のあるドメインの URL タイプミス
- ドメインのレジストラ情報
- IP アドレス情報

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

図 5-13　[Web Reputation Filters] ページ



[Web Reputation Filters] ページには次の情報が表示されます。

表 5-12　[Web] > [Reporting] > [Web Reputation Filters] ページの詳細

セクション	説明
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、「インタラクティブ レポートの時間範囲の選択」（P.3-4）を参照してください。
Web 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 Reputation Actions (Volume)	このセクションには、Web レピュテーション アクションのボリュームがトランザクション数の比率で表示されます。
Web Reputation Threat Types by Blocked Transactions	このセクションには、ブロックされた Web レピュテーション タイプが表示されます。
Web Reputation Threat Types by Scanned Further Transactions	Adaptive Scanning がイネーブルの場合、このセクションには脅威の可能性が検出されたトランザクションの数が表示されます。 Adaptive Scanning がイネーブルでない場合、このセクションにはブロックされたためにさらにスキャンを必要とする Web レピュテーション タイプが表示されます。Web レピュテーション フィルタリングの結果が「Scan Further」の場合、トランザクションはアンチマルウェア ツールに渡されて追加のスキャンが行われます。
Web Reputation Actions (Breakdown by Score)	Adaptive Scanning がイネーブルでない場合、このインタラクティブ テーブルには各アクションの Web レピュテーション スコアの内訳が表示されます。

ヒント　このレポートのビューをカスタマイズするには、「インタラクティブ Web レポーティング ページの操作」（P.5-6）を参照してください。

Web レピュテーション設定の調整

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

[L4 Traffic Monitor] ページ

[Web] > [Reporting] > [L4 Traffic Monitor] ページはセキュリティ関連のレポーティング ページであり、指定した時間範囲内に L4 トラフィック モニタによって 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。

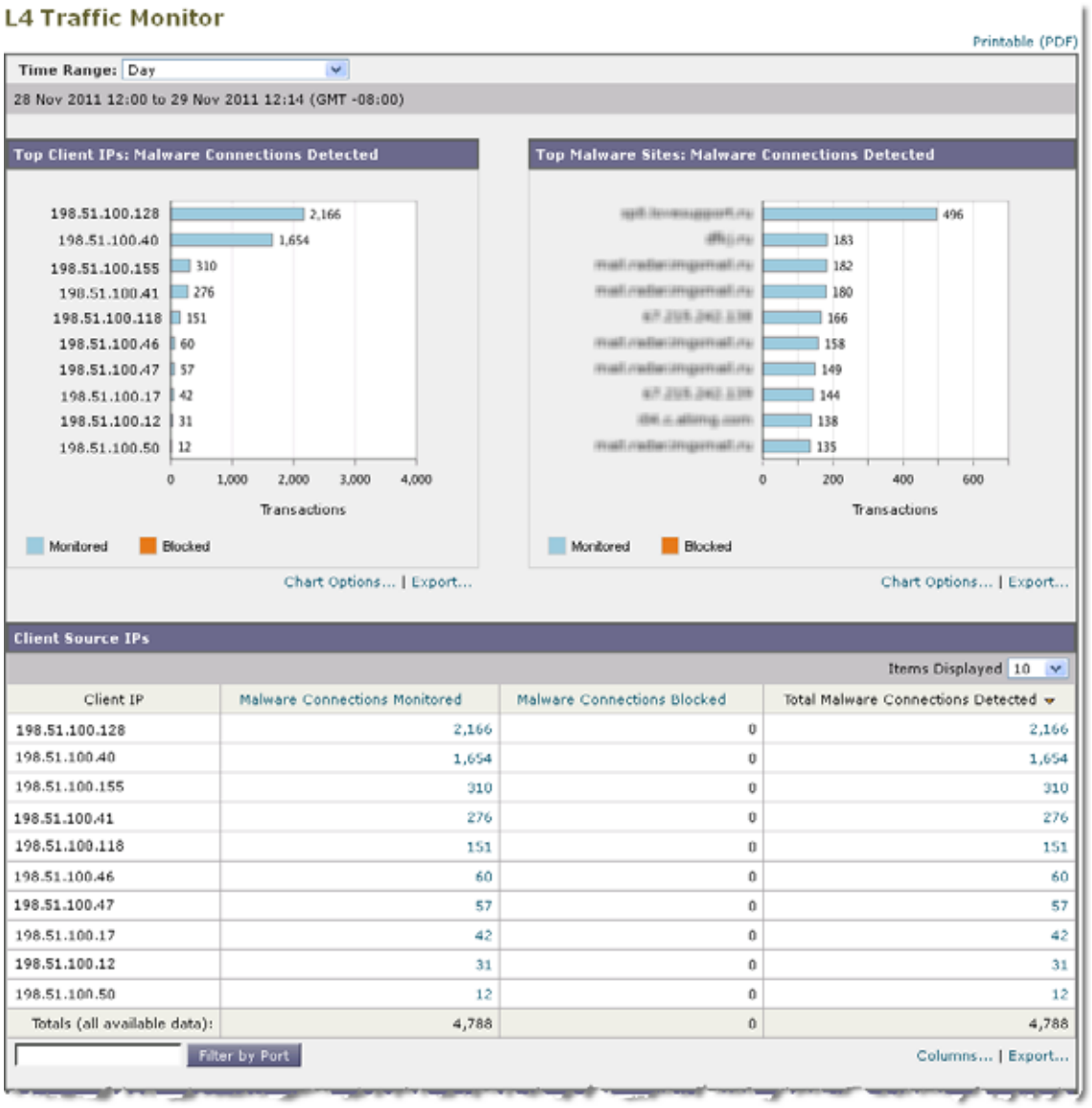
L4 トラフィック モニタは、各 Web セキュリティ アプライアンスのすべてのポートに着信するネットワーク トラフィックをリッスンし、ドメイン名と IP アドレスを独自のデータベース テーブルのエントリと照合して、着信トラフィックと発信トラフィックを許可するかどうかを決定します。

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。

図 5-14 に [L4 Traffic Monitor] ページを示します。

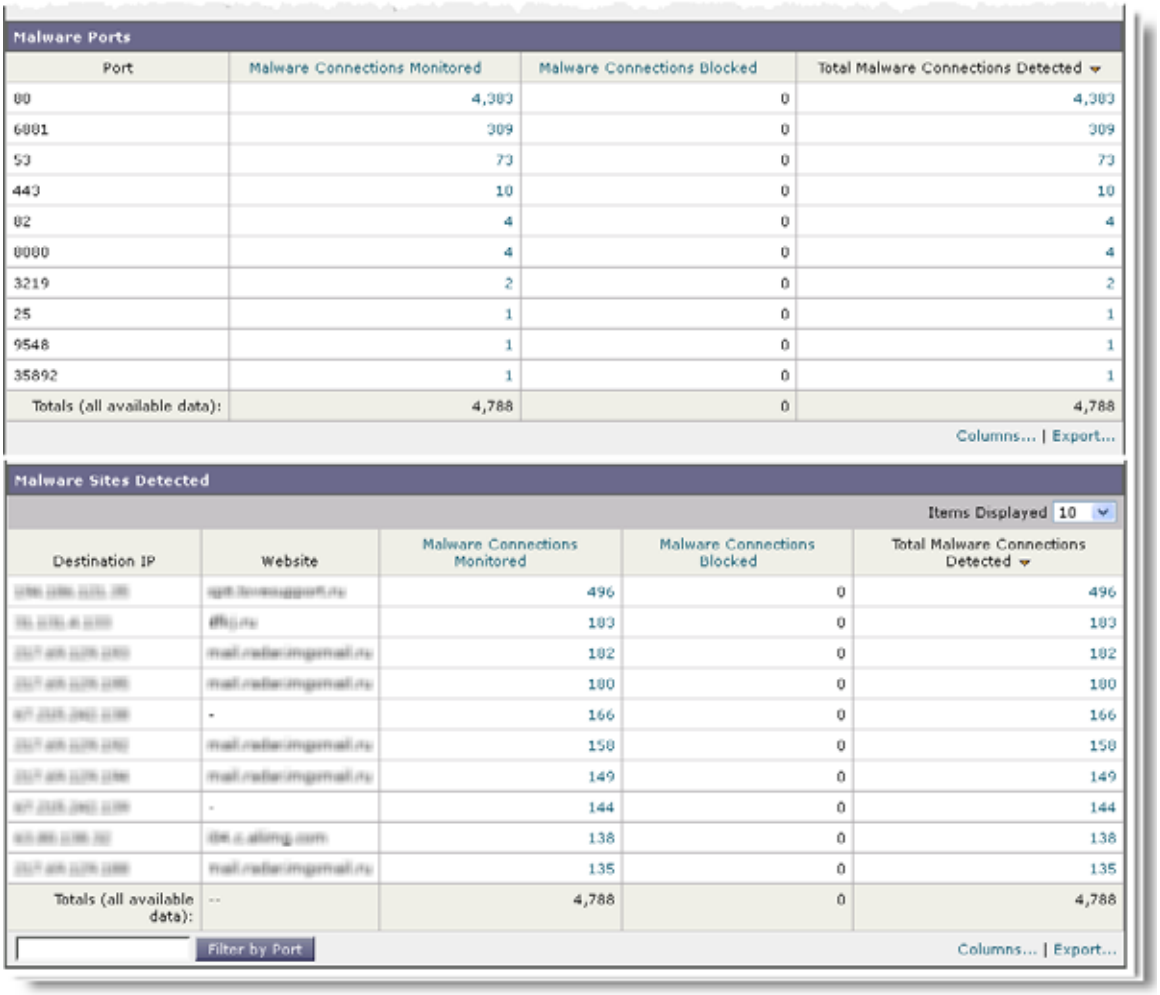
ヒント　このレポートのビューをカスタマイズするには、「インタラクティブ Web レポーティング ページの操作」（P.5-6）を参照してください。

図 5-14　[L4 Traffic Monitor] ページ



（次のページに続く）

（前ページからの続き）



Malware Ports

Port	Malware Connections Monitored	Malware Connections Blocked	Total Malware Connections Detected
80	4,383	0	4,383
6881	309	0	309
53	73	0	73
443	10	0	10
82	4	0	4
8080	4	0	4
3219	2	0	2
25	1	0	1
9548	1	0	1
35892	1	0	1
Totals (all available data):	4,788	0	4,788

Columns... | Export...

Malware Sites Detected

Items Displayed 10

Destination IP	Website	Malware Connections Monitored	Malware Connections Blocked	Total Malware Connections Detected
[redacted]	[redacted]	496	0	496
[redacted]	[redacted]	183	0	183
[redacted]	[redacted]	182	0	182
[redacted]	[redacted]	180	0	180
[redacted]	-	166	0	166
[redacted]	[redacted]	150	0	150
[redacted]	[redacted]	149	0	149
[redacted]	-	144	0	144
[redacted]	[redacted]	138	0	138
[redacted]	[redacted]	135	0	135
Totals (all available data):	--	4,788	0	4,788

Filter by Port

Columns... | Export...

表 5-13 で [L4 Traffic Monitor] ページに表示される情報を説明します。

表 5-13　[L4 Traffic Monitor] レポート ページの内容

セクション	説明
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、「インタラクティブ レポートの時間範囲の選択」（P.3-4）を参照してください。
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 [Chart Options] リンクをクリックすると、表示を総合的な [Malware Connections Detected] から [Malware Connections Monitored] または [Malware Connections Blocked] に変更できます。 このチャートは、「[Client Malware Risk] ページ」（P.5-39）の [L4 Traffic Monitor: Malware Connections Detected] と同じです。

表 5-13　[L4 Traffic Monitor] レポート ページの内容（続き）

セクション	説明
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 [Chart Options] リンクをクリックすると、表示を総合的な [Malware Connections Detected] から [Malware Connections Monitored] または [Malware Connections Blocked] に変更できます。
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、[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 [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] > [Reporting] > [Web Tracking] ページの [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 Traffic Monitor] タブ」（P.5-56）を参照してください。 このテーブルは、「[Client Malware Risk] ページ」（P.5-39）の [L4 Traffic Monitor: Clients by Malware Risk] テーブルと同じです。
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、[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] > [Reporting] > [Web Tracking] ページの [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 Traffic Monitor] タブ」（P.5-56）を参照してください。
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、[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、[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] > [Reporting] > [Web Tracking] ページの [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 Traffic Monitor] タブ」（P.5-56）を参照してください。

ヒント　このレポートのビューをカスタマイズするには、「インタラクティブ Web レポーティング ページの操作」（P.5-6）を参照してください。

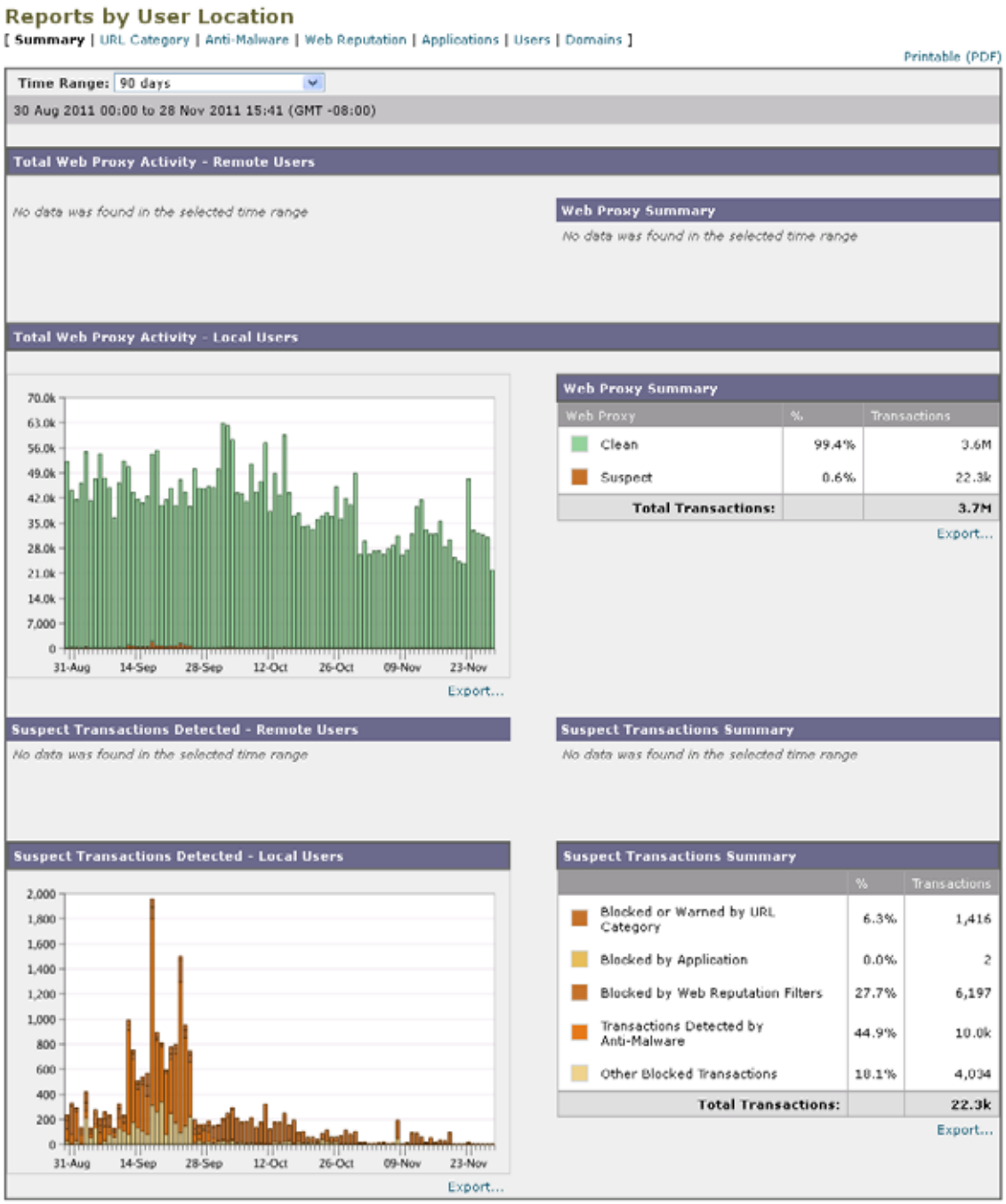
[Reports by User Location] ページ

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

対象となるアクティビティは次のとおりです。

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

図 5-15　[Reports by User Location] ページ



[Reports by User Location] ページには次の情報が表示されます。

表 5-14　[Web] > [Reporting] > [Reports by User Location] ページの詳細

セクション	説明
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、「インタラクティブ レポートの時間範囲の選択」（P.3-4）を参照してください。
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 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。

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

ヒント　このレポートのビューをカスタマイズするには、「インタラクティブ Web レポーティング ページの操作」（P.5-6）を参照してください。

（注）　[Reports by User Location] ページの情報について、スケジュール設定されたレポートを生成することができます。レポートのスケジュール設定については、「スケジュール設定されたレポートとオンデマンド Web レポートについて」（P.5-63）を参照してください。

[Web Tracking] ページ

[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。目的に応じて、次のタブのいずれかまたは両方で検索を行います。

- 「[Proxy Services] タブ」（P.5-52）
- 「[L4 Traffic Monitor] タブ」（P.5-56）

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

[Proxy Services] タブ

[Web] > [Reporting] > [Web Tracking] ページの [Proxy Services] タブを使用して、個々のセキュリティ コンポーネント、およびアクセプタブル ユース適用コンポーネントから収集された Web トラッキング データを検索します。このデータに L4 トラフィック モニタリング データは含まれません。

このデータを使用して、次の役割を補助することができます。

- **人事または法律マネージャ。**所定の期間内の従業員に関するレポートを調査します。

  たとえば、[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。

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

[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 Categories] ページとその他のレポーティング ページの併用」（P.5-29）を参照してください。

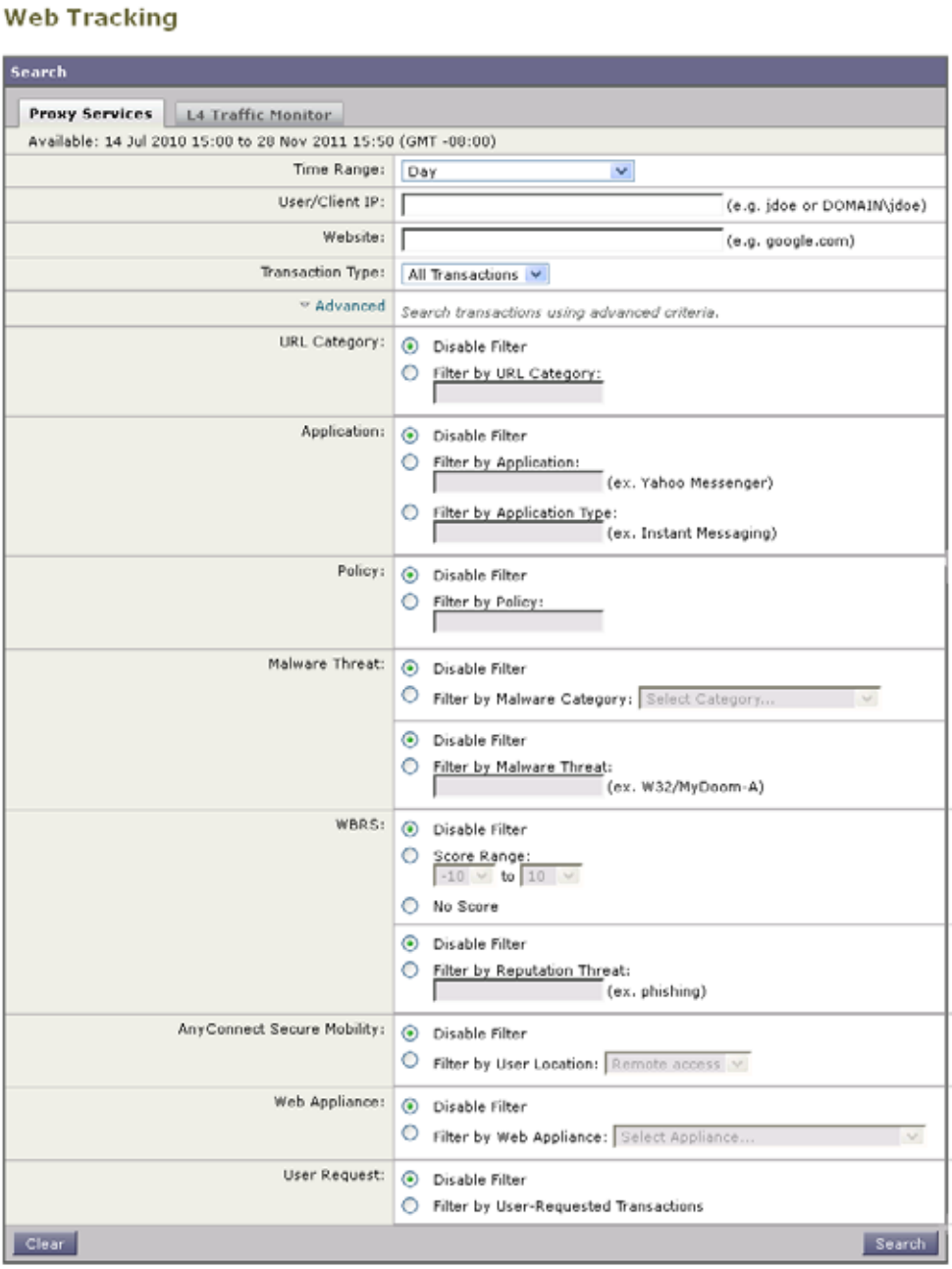
関心のある Web アクティビティのインスタンスを検索するには、次の手順を実行します。

ステップ 1　セキュリティ管理アプライアンスのウィンドウで、[Web] > [Reporting] > [Web Tracking] を選択します。

ステップ 2　[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、[Advanced] をクリックします。

図 5-16　[Web Tracking] ページの [Proxy Services] タブ



ステップ 4　検索条件を入力します。

表 5-15　[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	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、「インタラクティブ レポートの時間範囲の選択」（P.3-4）を参照してください。

表 5-15　[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
ユーザ/クライアント IP	レポートに表示される認証ユーザ名、または追跡対象のクライアント IP アドレスを任意で入力します。IP 範囲を 172.16.0.0/16 のような CIDR 形式で入力することもできます。 このフィールドを空にしておくと、すべてのユーザに関する検索結果が返されます。
Web サイト	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	追跡対象のトランザクションのタイプを [All Transactions]、[Completed]、[Blocked]、[Monitored]、または [Warned] から選択します。
高度な検索条件	
URL カテゴリ	URL カテゴリでフィルタリングするには、[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。 カスタム URL カテゴリの名前が定義済みカテゴリと同じ場合、または、システムの URL フィルタリング エンジンが変更されている場合、そのカテゴリに関連付けられた URL フィルタリング エンジン名は想定と異なる場合があります。ただし検索結果は、関連付けられたエンジンではなくカテゴリ名のみに基づきます。 一連の URL カテゴリが更新されると、一部のカテゴリに「Deprecated」のラベルが付けられる場合があります。これらのカテゴリは、少なくとも 1 つの管理対象 Web セキュリティ アプライアンスでの新しいトランザクションでは使用できなくなります。ただし、そのカテゴリが有効な間に発生した最近のトランザクションについては、引き続き検索を実行できます。URL カテゴリ セットの更新については、「URL カテゴリ セットの更新とレポート」（P.5-28）を参照してください。 お使いの Web セキュリティ アプライアンスで、現在の URL フィルタリング エンジンとは別のエンジンを使用したことがある場合、非アクティブなエンジンのみに関連付けられたカテゴリに、それを示すラベルが付けられます。 ドロップダウン リストに表示されるエンジン名またはカテゴリ ステータスに関係なく、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	アプリケーションでフィルタリングするには、[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、[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。

表 5-15　[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
ポリシー	ポリシー グループでフィルタリングするには、[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。
マルウェアの脅威	特定のマルウェアの脅威でフィルタリングするには、[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、[Filter by Malware Category] を選択し、フィルタリングに使用するマルウェア カテゴリを選択します。
WBRS	[WBRS] セクションでは、Web ベースのレピュテーション スコアによるフィルタリングと、特定の Web レピュテーションの脅威によるフィルタリングが可能です。 • Web レピュテーション スコアでフィルタリングするには、[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、[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、[Filter by Reputation Threat] を選択し、フィルタリングに使用する Web レピュテーションの脅威を入力します。 WBRS スコアの詳細については、『*Cisco IronPort AsyncOS for Web Security User Guide*』を参照してください。
AnyConnect セキュア モビリティ	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、[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、[Disable Filter] を選択します （旧リリースでは、このオプションは Mobile User Security と呼ばれていました。
ユーザ要求	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、[Filter by User-Requested Transactions] を選択します。 **（注）** このフィルタをイネーブルにすると、検索結果には「最良の推測」トランザクションが含まれます。
Web アプライアンス	特定の Web アプライアンスでフィルタリングするには、[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。 [Disable Filter] を選択すると、検索にはセキュリティ管理アプライアンスに関連付けられたすべての Web セキュリティ アプライアンスが含まれます。

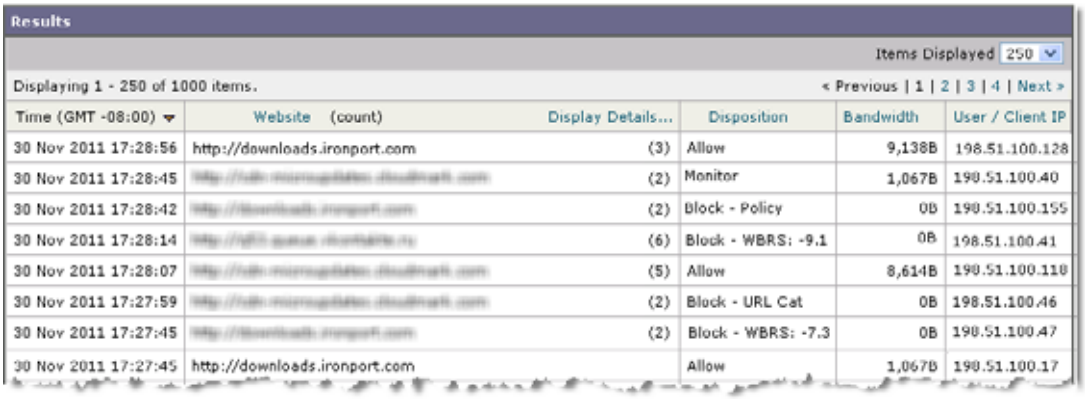
ステップ 5　[Search] をクリックします。

Web トラッキングの検索結果が表示されます。

Web トラッキング結果について

デフォルトでは、結果はタイム スタンプでソートされ、最新の結果が最上部に表示されます。

図 5-17　Web トラッキング検索結果（[Proxy Services] タブ）



[Results] ウィンドウには次の情報が表示されます。

- URL がアクセスされた時刻
- トランザクションに関係した Web サイト
- ロードされたイメージ、実行された JavaScript、アクセスされたセカンダリ サイトなど、ユーザが開始したトランザクションによって発生した関連トランザクションの数。この数値は、カラム見出しの [Display Details] リンクの下にカッコで囲まれて表示されます。
- 処理（トランザクションの結果。該当する場合、トランザクションがブロックまたはモニタされた理由、あるいは警告が発行された理由が表示されます）。
- トランザクションの帯域幅
- ユーザ ID/ クライアント IP アドレス

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

（注）　1000 件を超える結果を表示する必要がある場合は、[Printable Download] リンクをクリックすると、関連するトランザクションの詳細を除く raw データ一式が含まれた CSV ファイルを取得できます。

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

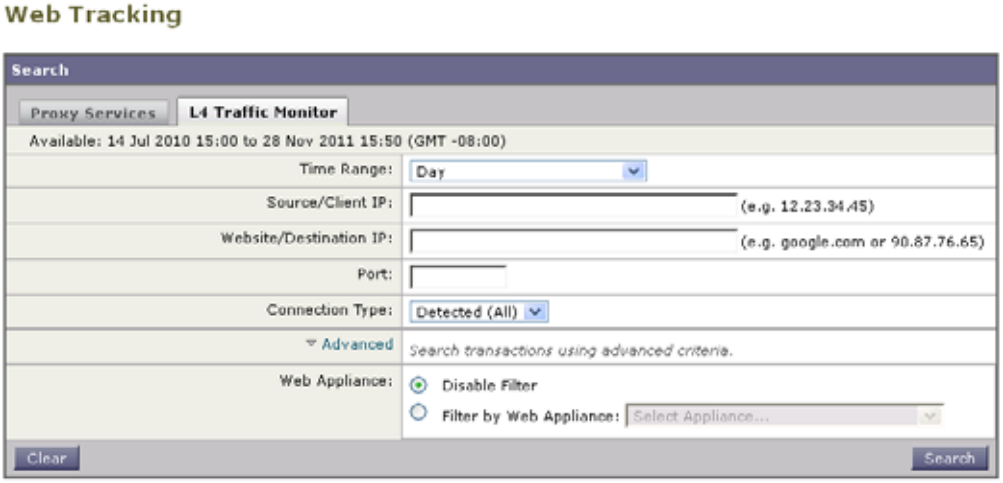
500 件までの関連トランザクションの詳細を表示するには、[Related Transactions] リンクをクリックします。

[L4 Traffic Monitor] タブ

[Web] > [Reporting] > [Web Tracking] ページの [L4 Traffic Monitor] タブには、マルウェア サイトおよびポートへの接続に関する詳細情報が表示されます。マルウェア サイトへの接続は、次のタイプの情報によって検索できます。

- 時間範囲
- サイト、使用された IP アドレスまたはドメイン
- ポート
- 組織内のコンピュータに関連付けられた IP アドレス
- 接続タイプ
- 接続を処理した Web セキュリティ アプライアンス

図 5-18　[Web Tracking] ページの [L4 Traffic Monitor] タブ



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、[Destination IP Address] カラム見出しの [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 Traffic Monitor] ページ」（P.5-44）を参照してください。

[System Capacity] ページ

[Web] > [Reporting] > [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、[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。

[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。

[System Capacity] ページに表示されるデータの解釈方法

[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。

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

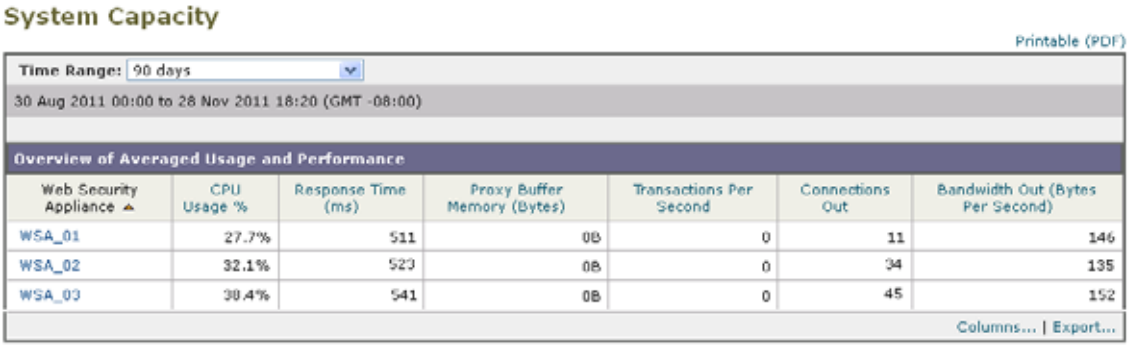
（注） 他のレポートで時間範囲に [Year] を選択した場合は、最大の時間範囲である 90 日を選択することを推奨します。

[System Capacity] ページにアクセスするには、次の手順を実行します。

ステップ 1　セキュリティ管理アプライアンスのウィンドウで、[Web] > [Reporting] > [System Capacity] を選択します。

[System Capacity] ページが表示されます。

図 5-19　[System Capacity] ページ



ステップ 2　他のタイプのデータを表示するには、[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、[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 [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。

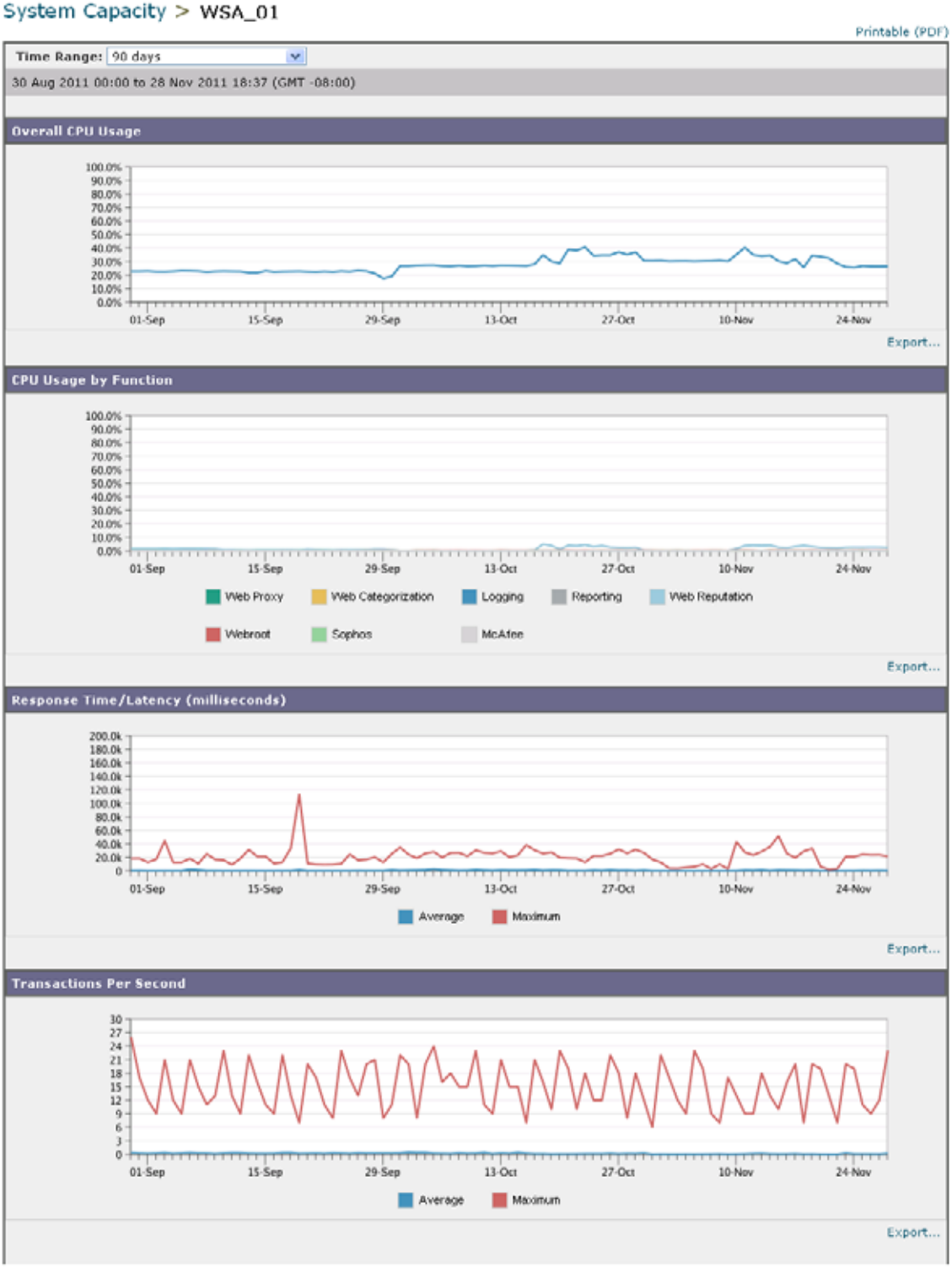
- [System Capacity]：[System Load]
- 「[System Capacity]：[Network Load]」

[System Capacity]：[System Load]

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

また、応答時間 / 遅延のグラフと 1 秒あたりのトランザクションのグラフには、全体的な応答時間（ミリ秒単位）、および [Time Range] ドロップダウン メニューで指定した日付範囲での 1 秒あたりのトランザクション数が示されます。

図 5-20　[System Capacity] : [System Load]



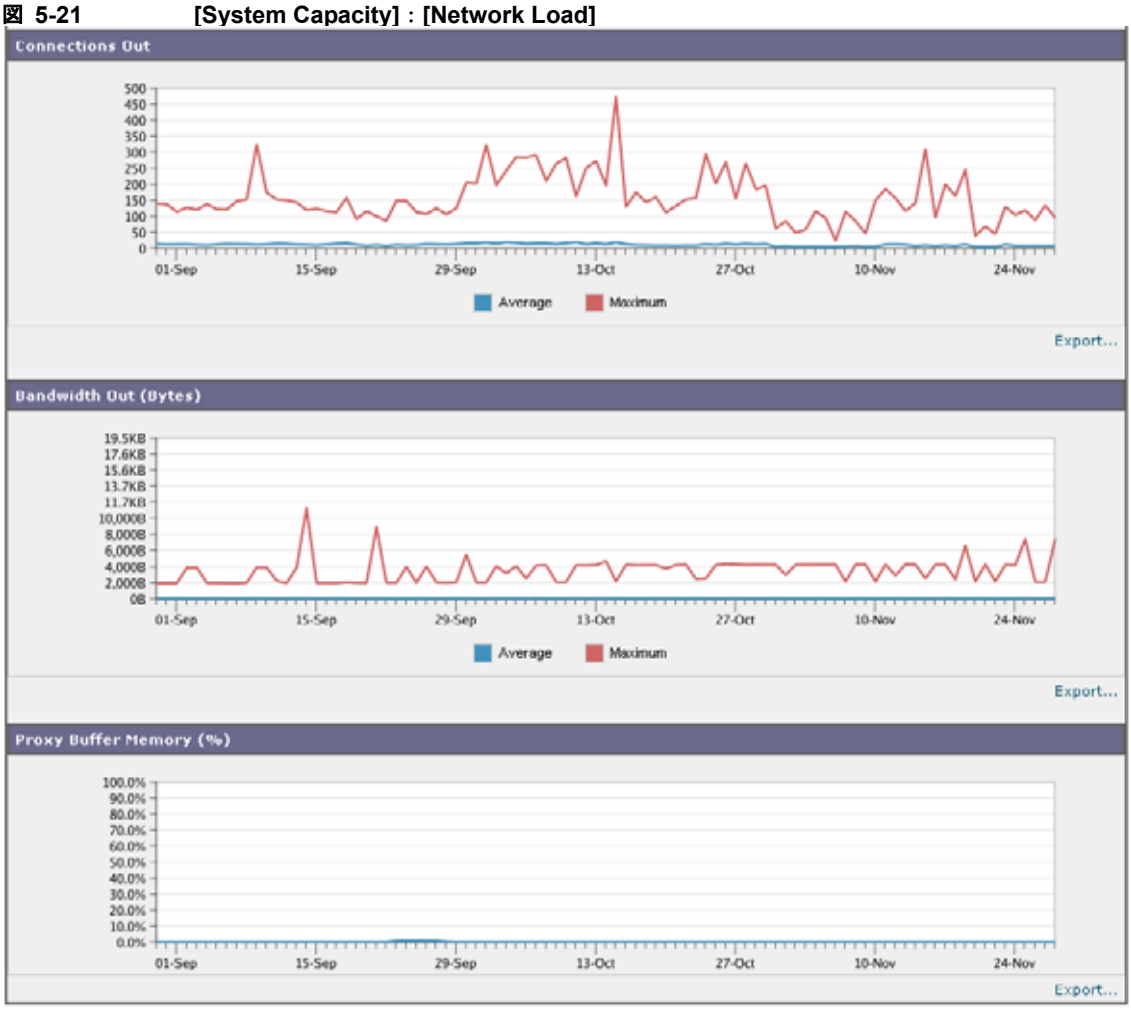
[System Capacity]：[Network Load]

[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。

[Proxy Buffer Memory] は、通常動作時におけるネットワーク トラフィックの急増を示している場合もありますが、グラフが最大値まで徐々に上昇している場合は、アプライアンスがのキャパシティが最大値に達しており、キャパシティの追加を検討すべきである可能性もあります。

次のチャートは、「[System Capacity]：[System Load]」、図 5-20 と同じページでこれらのチャートの下に表示されます。

図 5-21　[System Capacity]：[Network Load]



プロキシ バッファ メモリ スワッピングに関する注意事項

システムは、定期的にプロキシ バッファ メモリをスワップするように設計されているので、一部のプロキシ バッファ メモリ スワッピングは起こり得るものであり、アプライアンスの問題を示すものではありません。システムが*継続的に*高ボリュームのプロキシ バッファ メモリをスワップする場合を除き、プロキシ バッファ メモリのスワッピングは正常かつ通常の動作です。システムが極端に大量の処理を

行い、大量であるためにプロキシ バッファ メモリを絶えずスワップする場合は、ネットワークに Cisco IronPort 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。

[Data Availability] ページ

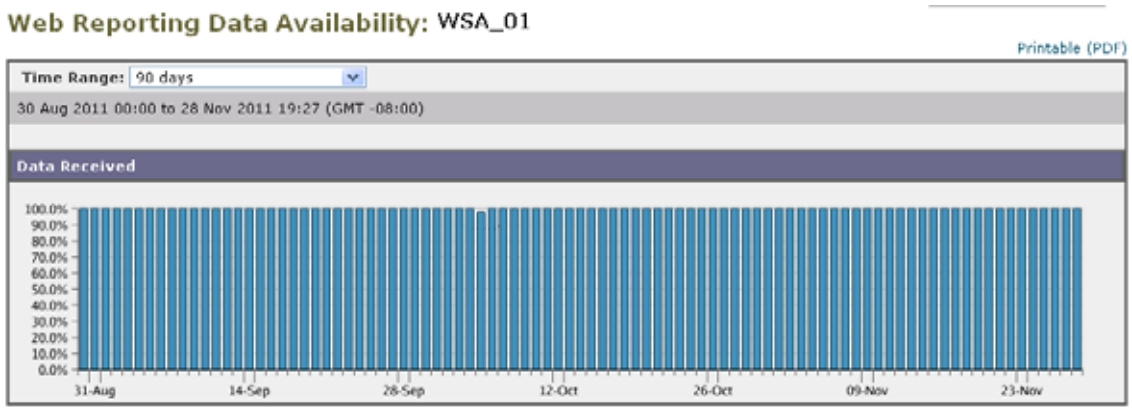
[Web] > [Reporting] > [Data Availability] ページには、管理対象の各 Web セキュリティ アプライアンスに対応するセキュリティ管理アプライアンスでレポーティングおよび Web トラッキング データを使用できる日付範囲の概要が表示されます。

図 5-22　[Web Reporting Data Availability] ページ

（注）　Web レポーティングがディセーブルになると、セキュリティ管理アプライアンスは Web セキュリティ アプライアンスから新しいデータを取得しなくなりますが、以前に取得したデータは セキュリティ管理アプライアンスに残っています。ディスク使用率の管理方法については、「ディスク使用量の管理」（P.13-58）を参照してください。

[Web Reporting] の [From] カラムと [To] カラム、および [Web Reporting and Tracking] の [From] カラムと [To] カラムでステータスが異なる場合は、[Status] カラムに最も深刻な結果が示されます。

特定のアプライアンスのデータ アベイラビリティをグラフ形式で表示するには、[Web セキュリティ アプライアンス] カラムでアプライアンスをクリックします。



（注）　URL カテゴリに関するスケジュール済みレポートでデータ アベイラビリティが使用されている場合、いずれかのアプライアンスのデータにギャップがあると、ページの下部に「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 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 [Overview] ページ」（P.5-13）を参照してください。
- [Users]：このページに表示される情報については、「[Users] ページ」（P.5-17）を参照してください。
- [Web Sites]：このページに表示される情報については、「[Web Sites] ページ」（P.5-24）を参照してください。
- [URL Categories]：このページに表示される情報については、「[URL Categories] ページ」（P.5-26）を参照してください。
- [Top URL Categories — Extended]：[Top URL Categories — Extended] のレポートを生成する方法については、「Top URL Categories — Extended」（P.5-65）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。
- [Application Visibility]：このページに表示される情報については、「[Application Visibility] ページ」（P.5-30）を参照してください。
- [Top Application Types — Extended]：[Top URL Categories — Extended] のレポートを生成する方法については、「Top Application Types — Extended」（P.5-66）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。
- [Anti-Malware]：このページに表示される情報については、「[Anti-Malware] ページ」（P.5-33）を参照してください。
- [Client Malware Risk]：このページに表示される情報については、「[Client Malware Risk] ページ」（P.5-39）を参照してください。
- [Web Reputation Filters]：このページに表示される情報については、「[Web Reputation Filters] ページ」（P.5-41）を参照してください。
- [L4 Traffic Monitor]：このページに表示される情報については、「[L4 Traffic Monitor] ページ」（P.5-44）を参照してください。
- [Mobile Secure Solution]：このページに表示される情報については、「[Reports by User Location] ページ」（P.5-49）を参照してください。
- [System Capacity]：このページに表示される情報については、「[System Capacity] ページ」（P.5-57）を参照してください。

Web レポートのスケジュール設定

ここでは、次の内容について説明します。

（注）　すべてのレポートで、ユーザ名を認識できないようにすることができます。詳細については、「Web レポートでのユーザ名の匿名化」（P.5-4）を参照してください。

日単位、週単位、または月単位で実行されるようにレポートをスケジュール設定することができます。スケジュール設定されたレポートは、前日、過去 7 日間、前月、過去の日（最大 250 日）、過去の月（最大 12 ヵ月）のデータを含めるように設定できます。また、指定した日数（2 ～ 100 日）または指定した月数（2 ～ 12 ヵ月）のデータを含めることもできます。

レポートの実行時間にかかわらず、直前の時間間隔（過去 1 時間、1 日、1 週間、または 1 ヵ月）のデータのみが含まれます。たとえば、日次レポートを午前 1 時に実行するようにスケジュールを設定した場合、レポートには前日の 00:00 から 23:59 までのデータが含まれます。

セキュリティ管理アプライアンスは、生成した最新のレポートを保持します（すべてのレポートに対して、最大で 1000 バージョン）。必要に応じた数（ゼロも含む）のレポート受信者を定義できます。電子メール受信者を指定しない場合でも、レポートはアーカイブされます。レポートを多数のアドレスに送信する必要がある場合、個別に受信者を設定するよりも、メーリング リストを作成するほうが容易です。

デフォルトでは、スケジュール設定された各レポートのうち、直近の 12 のレポートがアーカイブされます。レポートは、アプライアンスの **/periodic_reports** ディレクトリに保管されます。（詳細については、付録 A「IP インターフェイスおよびアプライアンスへのアクセス」を参照してください）。

スケジュール設定されたレポートの追加

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

ステップ 1　セキュリティ管理アプライアンスのウィンドウで、[Web] > [Reporting] > [Scheduled Reports] を選択します。

ステップ 2　[Add Scheduled Report] をクリックします。

ステップ 3　[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　[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　[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　[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　[Charts] では、[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　[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　[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　[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　[Submit] をクリックします。

スケジュール設定されたレポートの編集

レポートを編集するには、[Web] > [Reporting] > [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、[Submit] をクリックしてページでの変更を送信し、[Commit Changes] ボタンをクリックしてアプライアンスへの変更を確定します。

スケジュール設定されたレポートの削除

レポートを削除するには、[Web] > [Reporting] > [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、[All] チェックボックスを選択し、**削除**を実行して変更を**確定**します。削除されたレポートのアーカイブ版は削除されません。

追加の拡張レポート

さらに 2 種類のレポートを、スケジュール設定されたレポートとしてのみセキュリティ管理アプライアンスで使用することができます。

- Top URL Categories — Extended
- Top Application Types — Extended

Top URL Categories — Extended

[Top URL Categories — Extended] レポートは、管理者が [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 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、[Top URL Categories —Extended] レポートを使用します。

（注）

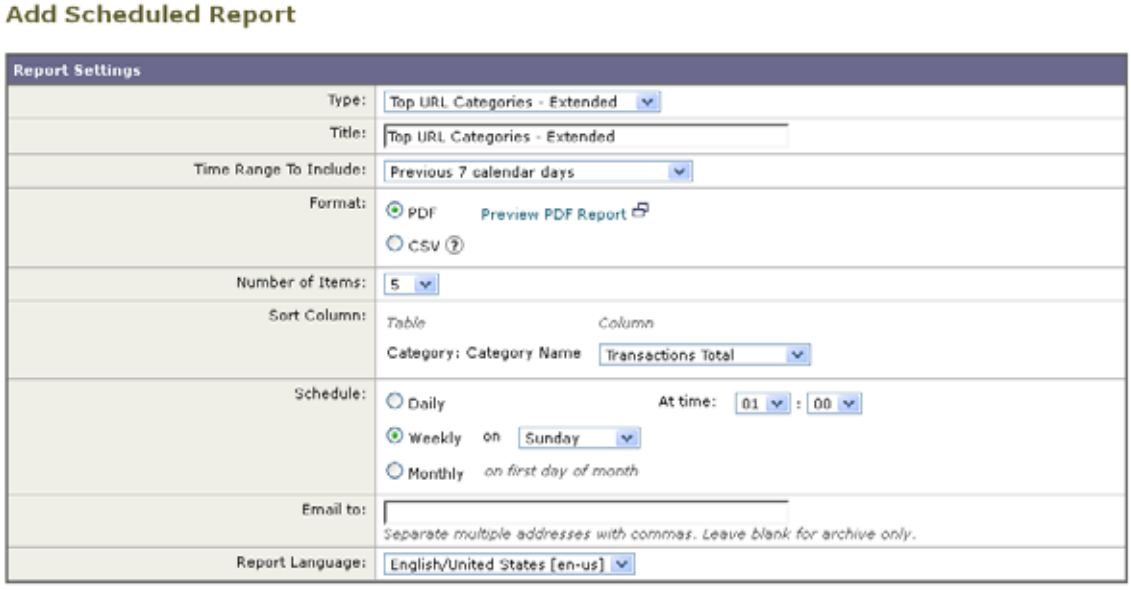
- このタイプのレポートで生成できる最大レポート数は 20 です。
- 定義済みの URL カテゴリ リストは更新されることがあります。こうした更新によるレポート結果への影響については、「URL カテゴリ セットの更新とレポート」（P.5-28）を参照してください。

[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。

ステップ 1　セキュリティ管理アプライアンスのウィンドウで、[Web] > [Reporting] > [Scheduled Reports] を選択します。

ステップ 2　[Add Scheduled Report] をクリックします。

ステップ 3　[Type] の横のドロップダウン メニューから、[Top URL categories — Extended] を選択します。



ステップ 4　[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　[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　[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　[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　[Charts] では、[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　[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　[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　[Submit] をクリックします。

Top Application Types — Extended

[Top Application Type — Extended] レポートを生成するには、次の手順を実行します。

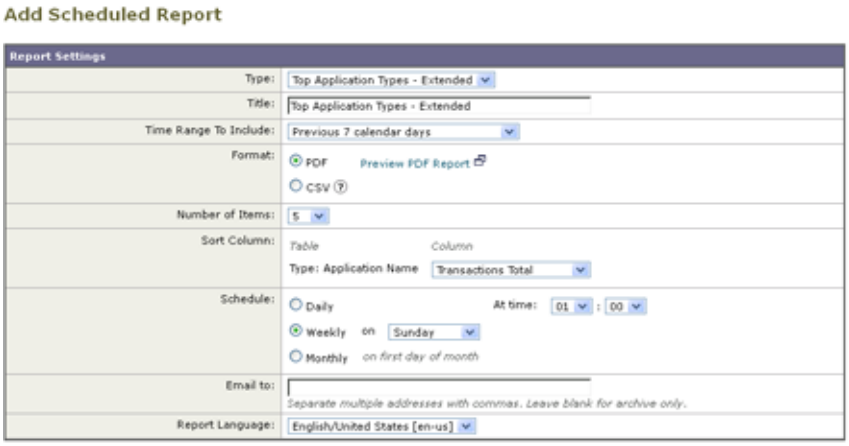
ステップ 1　セキュリティ管理アプライアンスのウィンドウで、[Web] > [Reporting] > [Scheduled Reports] を選択します。

ステップ 2　[Add Scheduled Report] をクリックします。

[Add Scheduled Report] ウィンドウが表示されます。

ステップ 3　[Type] の横のドロップダウン メニューから、[Top Application Types — Extended] を選択します。

このページのデフォルト オプションは変更される場合があります。



ステップ 4　[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　[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　[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　[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、[Transactions Completed]、[Transactions Blocked]、[Transaction Totals] です。

ステップ 9　[Charts] では、[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　[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　[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　[Submit] をクリックします。

オンデマンドでの Web レポートの生成

スケジュールを設定できるレポートのほとんどは、オンデマンドでの作成も可能です。

（注）　一部のレポートは、オンデマンドではなくスケジュール設定されたレポートとしてのみ使用できます。「追加の拡張レポート」（P.5-65）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。

ステップ 1　セキュリティ管理アプライアンスのウィンドウで、[Web] > [Reporting] > [Archived Reports] を選択します。

ステップ 2　[Generate Report Now] をクリックします。

ステップ 3　[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　[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　[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　[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。[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。

- [Number of rows]：テーブルに表示するデータの行数。
- [Charts]：レポートのチャートに表示するデータ。

  [Data to display] の下のデフォルト オプションを選択します。
- [Sort Column]：各テーブルのソート基準となるカラム。

ステップ 8　[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 [Archived Reports] ページに表示するには、[Archive Report] チェックボックスを選択します。

（注）　[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、[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　[Deliver This Report] をクリックして、レポートを生成します。

[Archived Web Reports] ページ

アーカイブされた Web レポートの表示と管理

[Web] > [Reporting] > [Archived Reports] ページには次の内容が表示されます。

- 「スケジュール設定されたレポートの追加」（P.5-64）の手順を使用してスケジュールを設定したレポート
- 「オンデマンドでの Web レポートの生成」（P.5-67）の手順を使用して作成したレポート

レポートを表示するには、[Report Title] カラムでレポート名をクリックします。[Show] ドロップダウン メニューでは、[Archived Reports] ページに表示されるレポートのタイプをフィルタリングできます。

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

アプライアンスでは、スケジュール設定されたレポートごとに最大 12 のインスタンスが保存されます（最大 1000 レポート）。アーカイブ済みのレポートは、アプライアンスの `/periodic_reports` ディレクトリに保管されます。アーカイブ済みのレポートは自動的に削除されます。新しいレポートが追加されると、古いレポートが削除され、常に 1000 という数が維持されます。12 インスタンスという制限は、同じ名前と時間範囲のスケジュール設定された各レポートに適用されます。

CHAPTER 6

電子メール メッセージのトラッキング

トラッキング サービスの概要

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 アプライアンスと補完関係にあります。セキュリティ管理アプライアンスによって、電子メール管理者はすべての電子メール セキュリティ アプライアンスを通過するメッセージのステータスを 1 箇所から追跡できます。

セキュリティ管理アプライアンスを使用すると、電子メール セキュリティ アプライアンスで処理されるメッセージのステータスを容易に検出できます。電子メール管理者は、メッセージの正確な場所を判断することで、ヘルプ デスク コールを迅速に解決できます。管理者はセキュリティ管理アプライアンスを使用して、特定のメッセージについて、配信されたか、ウイルス感染が検出されたか、スパム隔離に入れられたか、あるいはメール ストリーム以外の場所にあるのかを判断できます。

grep や同様のツールを使用してログ ファイルを検索する代わりに、セキュリティ管理アプライアンスの柔軟なトラッキング インターフェイスを使用してメッセージの場所を特定できます。さまざまな検索パラメータを組み合わせて使用できます。

トラッキング クエリーには次の項目を含めることができます。

- **エンベロープ情報：**照合するテキスト文字列を入力し、特定のエンベロープ送信者または受信者からのメッセージを検索します。
- **件名ヘッダー：**件名行のテキスト文字列を照合します。警告：規制によりそのようなトラッキングが禁止されている環境では、このタイプの検索を使用しないでください。
- **タイム フレーム：**指定された日数と時間内に送信されたメッセージを検索します。
- **送信元 IP アドレスまたは拒否された接続：**特定の IP アドレスからのメッセージを検索します。または、検索結果内の拒否された接続を表示します。
- **添付ファイル名**：メッセージを添付ファイル名で検索できます。照会した名前の添付ファイルが少なくとも 1 つ含まれているメッセージが検索結果に表示されます。

  パフォーマンス上の理由から、OLE オブジェクトなどの添付ファイルや .ZIP ファイルなどのアーカイブに含まれるファイル名は追跡されません。

添付ファイルの中には追跡されないものもあります。パフォーマンス上の理由から、添付ファイル名のスキャンは他のスキャン動作の一環としてのみ実行されます。たとえば、メッセージまたはコンテンツ フィルタリング、DLP、免責事項スタンプなどです。添付ファイル名は、ファイルがまだ添付されている間に本文スキャンを通過するメッセージでのみ使用できます。添付ファイル名が表示されない例を次に示します（ただしこれらに限られるわけではありません）。

  - システムがコンテンツ フィルタのみを使用しており、アンチスパムまたはアンチウイルス フィルタによってメッセージがドロップされたか、その添付ファイルが除去された場合
  - 本文スキャンの実行前に、メッセージ分裂ポリシーによって一部のメッセージから添付ファイルが除去された場合

- **イベント：**ウイルス陽性、スパム陽性、またはスパムの疑いのフラグが設定されたメッセージや、配信された、ハード バウンスされた、ソフト バウンスされた、またはウイルス アウトブレイク隔離に送信されたメッセージなど、指定されたイベントに一致するメッセージを検索します。
- **メッセージ ID：**SMTP「Message-ID:」ヘッダー、または Cisco IronPort メッセージ ID（MID）を識別してメッセージを検索します。
- **電子メール セキュリティ アプライアンス（ホスト）：**検索条件を特定の電子メール セキュリティ アプライアンスに絞り込むか、すべての管理対象アプライアンスを検索します。

中央集中型メッセージ トラッキングの設定

中央集中型メッセージ トラッキングを設定するには、次の手順を順序どおりに実行します。

- 「セキュリティ管理アプライアンスでの中央集中型電子メール トラッキングのイネーブル化」（P.6-2）
- 「電子メール セキュリティ アプライアンスでの中央集中型メッセージ トラッキングの設定」（P.6-3）
- 「管理対象の各電子メール セキュリティ アプライアンスへの中央集中型メッセージ トラッキング サービスの追加」（P.6-3）

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

ステップ 1　セキュリティ管理アプライアンスの場合：

a. [Management Appliance] > [Centralized Services] > [Email] > [Centralized Message Tracking] を選択します。

b. [Message Tracking Service] セクションで [Enable] をクリックします。

c. システム セットアップ ウィザードを実行してから初めて中央集中型電子メッセージ トラッキングをイネーブルにする場合は、エンドユーザ ライセンス契約書を確認し、[Accept] をクリックします。

[Centralized Message Tracking] ページが表示されます。中央集中型電子メール トラッキングをイネーブルにすると、[Message Tracking Service] ボックスの右側のカラムに [Enable] と表示されます。

d. セキュリティ管理アプライアンスでの変更を**送信**し、確定します。

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

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　[Security Services] > [Message Tracking] に移動します。

ステップ 3　[Edit Settings] をクリックします。

ステップ 4　[Centralized Tracking] を選択します。

ステップ 5　[Submit] をクリックします。

ステップ 6　電子メールの添付ファイル名を検索および記録できるようにする場合は、次の点に注意してください。

少なくとも 1 つの受信コンテンツ フィルタまたは本文スキャン機能が 電子メール セキュリティ アプライアンスで設定され、イネーブルになっていることを確認します。コンテンツ フィルタおよび本文スキャンの詳細については、『*Cisco IronPort AsyncOS for Email Security Advanced Configuration Guide*』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。

ステップ 1　セキュリティ管理アプライアンスで、[Management Appliance] > [Centralized Services] > [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.　[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.　[Add Email Appliance] をクリックします。

b.　[Appliance Name and IP Address] テキスト フィールドに、Cisco IronPort アプライアンスの管理インターフェイスのアプライアンス名と IP アドレスを入力します。

（注）　[IP Address] テキスト フィールドに DNS 名を入力した場合でも、[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.　[Centralized Message Tracking] サービスがすでに選択されています。

d.　[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、[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. [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. [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　[Submit] をクリックします。

ステップ 5　中央集中型メッセージ トラッキングをイネーブルにする各電子メール セキュリティ アプライアンスに対し、この手順を繰り返します。

ステップ 6　変更を保存します。

機密情報へのアクセスの管理

管理タスクを数人で分配する場合、データ消失防止（DLP）ポリシーに違反するメッセージに表示される機密情報へのアクセスを制限するには、「メッセージ トラッキングでの DLP 機密情報へのアクセスの制御」（P.12-23）を参照してください。

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。

指定した条件に一致する個々の電子メール メッセージまたはメッセージのグループを検索するには、次の手順を実行します。

ステップ 1　[Security Management appliance] ウィンドウで [Email] > [Message Tracking] > [Message Tracking] を選択します。

ステップ 2　（任意）[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。

- [Envelope Sender] : [Begins With]、[Is]、または [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]*.
- [Envelope Recipient] : [Begins With]、[Is]、または [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。
- [Subject] : [Begins With]、[Is]、[Contains]、または [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。

（注）　国際文字セットは、件名ヘッダーでサポートされません。

- [Message Received] : [Last Day]、[Last 7 Days]、または [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 [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 [Last 7 Days] オプションと当日の経過時間を使用します。

  日付を指定しなければ、クエリーは、すべての日付に対するデータを返します。時間範囲だけを指定すると、クエリーは、すべての利用可能な日付にわたってその時間範囲内のデータを返します。終了日と終了時刻に現在の日付と 23:59 を指定すると、クエリーは現在の日付に関するすべてのデータを返します。

  日付と時間は、データベースに保管される際に GMT 形式に変換されます。アプライアンス上で日付と時刻を表示する場合は、そのアプライアンスの現地時間で表示されます。

  メッセージの検索結果は、それらメッセージが電子メール セキュリティ アプライアンスのログに記録され、セキュリティ管理アプライアンスが取得した後でのみ表示されます。ログのサイズとポーリングの頻度によっては、電子メール メッセージが送信された時間と、それがトラッキングとレポーティングの結果に実際に表示される時間との間にわずかな差が生じることがあります。
- [Sender IP Address] : 送信者の IP アドレスを入力し、メッセージを検索するか、あるいは拒否された接続だけを検索するかを選択します。
  - IPv4 アドレスは、ピリオドで区切られた 4 つの数値であり、それぞれの数値は 0 ～ 255 でなければなりません（例 : *203.0.113.15*）。
  - IPv6 アドレスでは、8 つの 16 ビットの 16 進数値がコロンで区切られて構成されます。いずれか 1 箇所で、*2001:db8:80:1::5* のようにゼロ圧縮を使用できます。

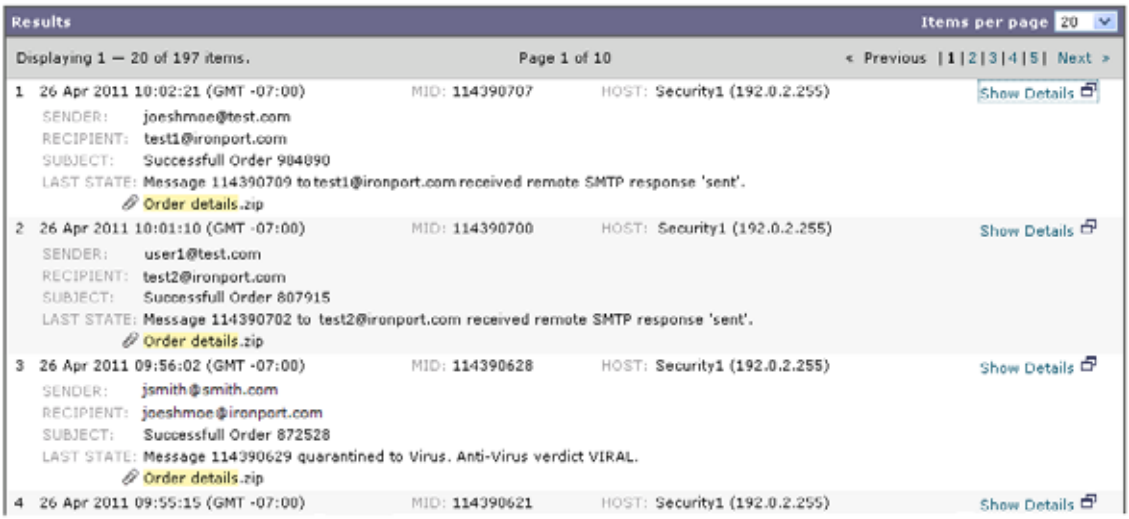
- [Message Event]：追跡対象のイベントを選択します。オプションは、[Virus Positive]、[Spam Positive]、[Suspect Spam]、[Delivered]、[DLP Violations]（DLP ポリシーの名前を入力し、違反の重大度を選択できます）、[Hard Bounced]、[Soft Bounced]、[Currently in Outbreak Quarantine]、[Quarantined as Spam] です。トラッキング クエリーに追加する多くの条件と違い、イベントは「OR」演算子を使用して追加します。複数のイベントを選択すると、検索結果は拡大します。
- [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。
- [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 minute]、[2 minutes]、[5 minutes]、[10 minutes]、[No time limit] です。クエリーから返される結果の最大数（最大 1000）も選択します。
- [Attachment name]：[Begins With]、[Is]、または [Contains] を選択し、検索する添付ファイル名の ASCII または Unicode テキスト文字列を入力します。入力したテキストの先頭および末尾のスペースは除去されません。

すべてのフィールドに入力する必要はありません。[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　[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 [Items per page] フィールドで指定した値よりも大きい場合、結果は複数のページに表示されます。ページ間を移動するには、リストの上部または下部にあるページ番号をクリックします。

必要に応じて、新しい検索条件を入力して検索精度を高め、再びクエリーを実行します。あるいは、次の項で説明するように、結果セットを絞り込んで検索精度を高めることもできます。

結果セットの絞り込み

クエリーを実行すると、結果セットに必要以上の情報が含まれていることがあります。新しいクエリーを作成するのではなく、結果リストの行内の値をクリックし、結果セットを絞り込みます。値をクリックすると、そのパラメータ値が検索の条件として追加されます。たとえば、クエリー結果に複数の日付のメッセージが含まれている場合、行内の特定の日付をクリックすると、その日付に受信されたメッセージだけが表示されます。

ステップ 1　条件として追加する値の上にカーソルを移動します。値が黄色で強調表示されます。

次のパラメータ値を使用して、検索を精密化します。

- Date and time
- Message ID（MID）
- Host（電子メール セキュリティ アプライアンス）
- Sender
- Recipient
- メッセージの件名行、または件名の先頭語

ステップ 2　値をクリックして、検索を精密化します。

[Results] セクションに、元のクエリー パラメータおよび追加した新しい条件に一致するメッセージが表示されます。

ステップ 3　必要に応じて、結果内の他の値をクリックして、検索をさらに精密化します。

（注）　クエリー条件を削除するには、[Clear] をクリックし、新しいトラッキング クエリーを実行します。

トラッキング クエリー結果について

トラッキング クエリー結果には、トラッキング クエリーで指定した条件に一致するすべてのメッセージがリストされます。[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。

（注）　50 名以上の受信者がいるメッセージは、トラッキング クエリー結果に表示されません。この問題は、AsyncOS の今後のリリースで解決される予定です。

各メッセージについて、日付/時刻、送信者、受信者、件名、最終状態、メッセージに含まれていた添付ファイル、Cisco IronPort メッセージ ID（MID）、および Cisco IronPort ホスト（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。メッセージの詳細情報を表示するには、各メッセージの [Show Details] リンクをクリックします。詳細については、「メッセージの詳細」（P.6-8）を参照してください。

（注）　セキュリティ管理アプライアンスからは、最初の 10,000 行までのデータが返されます。その他のレコードにアクセスするにはクエリー パラメータを調整し、新しいクエリーを実行します。

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 [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。

- 「Envelope and Header Summary」（P.6-8）
- 「Sending Host Summary」（P.6-8）
- 「Processing Details」（P.6-9）

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。収集する情報は次のとおりです。

[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。

[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「(No Subject)」という値になることがあります。

[Envelope Sender]：SMTP エンベロープ内の送信者のアドレス。

[Envelope Recipients]：SMTP エンベロープ内の受信者のアドレス。

[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 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 User ID]：送信者が SMTP 認証を使用して電子メールを送信した場合は、送信者の SMTP 認証ユーザ名。それ以外の場合、この値は「N/A」となります。

[Attachments]：メッセージに添付されたファイルの名前。

Sending Host Summary

[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 Address]：送信側ホストの IP アドレス。

[SBRS Score]：(SenderBase レピュテーション スコア)。範囲は、10（最も信頼できる送信者）～-10（明らかなスパム送信者）です。スコアが「None」の場合、そのメッセージが処理された時点において、このホストに関する情報が存在しなかったことを意味します。

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 Matched Content

このセクションには、データ消失防止（DLP）ポリシーに違反するコンテンツが表示されます。

通常、このコンテンツには機密情報、たとえば企業秘密や、クレジット カード番号、健康診断の結果などの個人情報が含まれるため、セキュリティ管理アプライアンスへのアクセス権はあるが管理者レベルの権限を所持していないユーザに対し、このコンテンツへのアクセスをディセーブルにする必要が生じることがあります。「メッセージ トラッキングでの DLP 機密情報へのアクセスの制御」（P.12-23）を参照してください。

CHAPTER 7

Cisco IronPort スパム隔離の管理

Cisco IronPort スパム隔離について

Cisco IronPort スパム隔離では、組織内の電子メール ユーザに対するスパム メッセージやスパムであると疑われるメッセージを捕捉します。スパム隔離は、「誤検出」（正規の電子メールがスパムとして検出または削除されること）が問題とされる組織でのセーフガード メカニズムとなります。この機能により、エンド ユーザおよび管理者は、スパムとフラグ付けされたメッセージを確認してから最終的な決定を下すことができるようになります。さらに、セーフリスト/ブロックリスト機能をイネーブルにすると、どのようなメッセージをスパムとしてマークするかをエンド ユーザ（電子メール ユーザ）が制御できるようになります。

（注） *システム隔離*はスパム隔離とは別の機能です。電子メール セキュリティ アプライアンスに常駐し、コンテンツ フィルタリング、スキャニング、感染フィルタの適用など、AsyncOS が実行するさまざまなアクションに基づいてメッセージを隔離して捕捉します。

ローカルの Cisco IronPort スパム隔離は、電子メール セキュリティ ゲートウェイ アプライアンスに常駐します。メッセージを、別の Cisco IronPort アプライアンス（通常は セキュリティ管理アプライアンス）に常駐している*外部の* Cisco IronPort スパム隔離に送信することもできます。

（注） Cisco IronPort スパム隔離へのエンド ユーザのアクセスは、指定したユーザまたはユーザ グループに対してのみ実装できます。また、最初にエンド ユーザ アクセスを実装した後で、エンド ユーザが隔離内のメッセージを表示および解放することがほとんどない場合は、アクセスをディセーブルにできます。

また、スパムおよびその疑いのあるメッセージが隔離されたことをエンド ユーザに電子メールで通知するように、AsyncOS を設定することもできます。通知には、そのユーザ向けに現在 Cisco IronPort スパム隔離で捕捉されているメッセージの要約が記述されています。ユーザはこのメッセージを確認して、電子メールの受信ボックスに配信するか、削除するかを判断できます。また、ユーザはその隔離さ

れたメッセージ全体を検索することができます。スパム隔離には通知メッセージからアクセスすることも、Web ブラウザを使用して直接アクセスすることもできます（スパム隔離にエンド ユーザが直接アクセスするには、認証が必要です）。詳細については、「エンド ユーザ隔離へのアクセスの設定」（P.7-9）を参照してください）。

デフォルトでは、Cisco IronPort スパム隔離は自己メンテナンス型になっています。古いメッセージによって隔離領域がすべて消費されることを避けるために、AsyncOS は Cisco IronPort スパム隔離から定期的にメールを削除します。

管理者レベルのすべてのユーザ（デフォルトの admin ユーザなど）は、Cisco IronPort スパム隔離にアクセスし、変更を行うことができます。AsyncOS オペレータ ユーザ、およびカスタム ロールによってスパム隔離へのアクセス権が割り当てられているユーザは、隔離コンテンツの表示および管理ができますが、隔離設定の変更はできません。Cisco IronPort スパム隔離へのエンド ユーザ アクセスがイネーブルになっている場合、メールのエンド ユーザは、隔離領域にある自分のメッセージにアクセスできます。

[Edit Spam Quarantine] ページ

中央集中型スパム隔離の設定

スパム隔離を中央集中型にする前に、使用している電子メール セキュリティ アプライアンスでローカルのスパム隔離を設定し、動作をテストする必要があります。

アクティブなスパム隔離を電子メール セキュリティ アプライアンスからセキュリティ管理アプライアンスへ移行するには、次の作業を順番に行ってください。

必要な IP アドレスの特定

「セキュリティ管理アプライアンスでの発信 IP インターフェイスの設定」（P.7-4）の手順で使用する IP アドレスを入手または特定します。通常、これはセキュリティ管理アプライアンスの Data 2 インターフェイスのものになります。ネットワーク要件の詳細については、付録 B「ネットワークと IP アドレスの割り当て」を参照してください。

セキュリティ管理アプライアンスでの Cisco IronPort スパム隔離の設定

ステップ 1　セキュリティ管理アプライアンスのウィンドウで、[Management Appliance] > [Centralized Services] > [Spam Quarantine] を選択します。

ステップ 2　システム セットアップ ウィザードの実行後、Cisco IronPort スパム隔離を初めてイネーブルにする場合は、次の手順を実行します。

a.　[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、[Accept] をクリックします。

ステップ 3　既存の設定を編集する場合は、[Cisco IronPort Spam Quarantine Settings] セクションで [Edit Settings] をクリックします。

ステップ 4　[Quarantine IP Interface] セクションで、ドロップダウン リストからスパム隔離用の適切な IP インターフェイスとポートを指定します。

デフォルトでは、スパム隔離では管理インターフェイスとポート 6025 を使用します。IP インターフェイスは、着信メールをリッスンするように設定されている セキュリティ管理アプライアンスのインターフェイスです。隔離ポートは、送信アプライアンスが外部隔離設定で使用しているポート番号です。

ステップ 5　[Deliver Messages Via] セクションで、対応するテキスト フィールドに、メールを配送するためのプライマリ ルートと代替用ルートを入力します。

セキュリティ管理アプライアンスからメッセージを直接送信することはしないため、発信する隔離関係の電子メール（スパム隔離から送信されるスパム通知やメッセージなど）は、メッセージ送信が設定されている他のアプライアンスまたはサーバを経由して配送する必要があります。

これらのメッセージは、SMTP またはグループウェア サーバを使用して送信できます。また、電子メール セキュリティ アプライアンスの発信リスナー インターフェイス（通常は Data2 インターフェイス）を指定することもできます。

代替用アドレスは、ロードバランシングとフェールオーバーに使用します。

電子メール セキュリティ アプライアンスが複数台ある場合は、管理対象の任意の電子メール セキュリティ アプライアンスの発信リスナー インターフェイスをプライマリ アドレスまたは代替用アドレスとして使用できます。これらはいずれも同じインターフェイス（Data 1 または Data 2）を発信リスナーとして使用する必要があります。

これらのアドレスについての他の注意事項を画面で確認してください。

ステップ 6　[Schedule Delete After] セクションで、メッセージを削除する前に保持する日数を指定します。

または、[Do not schedule a delete] オプション ボタンを選択して、スケジュールされた削除をディセーブルにします。削除をスケジュールするよう、隔離を設定することを推奨します。隔離によってキャパシティがいっぱいになると、最も古いメッセージから削除されます。

ステップ 7　[Default Language] セクションで、デフォルト言語を指定します。

これは、エンド ユーザが Cisco IronPort スパム隔離にアクセスしたときに表示される言語です。

ステップ 8　（任意）[Notify Cisco IronPort upon Message Release] で、解放されたメッセージのコピーを分析のために Cisco IronPort に送信する機能のチェックボックスをオンにします。

解放されたメッセージを分析のために送信するよう、隔離を設定することを推奨します。

ステップ 9　（任意）[Spam Quarantine Appearance] セクションで、エンド ユーザが隔離結果を表示するときに表示されるページをカスタマイズします。

次のオプションがあります。

- Use Current logo

- Use Cisco IronPort Spam Quarantine logo
- Upload Custom logo

[Upload Custom logo] を選択すると、隔離されたメッセージを表示するためにユーザがログインしたときに、[Cisco IronPort Spam Quarantine] ページの上部にロゴが表示されます。このロゴは、最大で 550 x 50 ピクセルの .jpg、.gif、または .png ファイルにする必要があります。ロゴ ファイルがない場合、デフォルトの Cisco IronPort スパム隔離のロゴが使用されます。

ステップ 10　（任意）[Login Page Message] テキスト フィールドに、ログイン ページのメッセージを入力します。このメッセージは、エンド ユーザに対して隔離へのログイン プロンプトを表示するときに表示されます。

ステップ 11　オプションで、Cisco IronPort スパム隔離を表示する権限を持つユーザのリストを変更します。詳細については、「Cisco IronPort スパム隔離への管理者ユーザ アクセスの設定」（P.7-8）を参照してください。

ステップ 12　オプションで、エンド ユーザのアクセス、およびスパム通知を設定します。詳細については、「エンド ユーザのためのスパム管理機能の設定」（P.7-8）を参照してください。

ステップ 13　変更を送信し、保存します。

セキュリティ管理アプライアンスでのインターフェイスの設定

セキュリティ管理アプライアンスでの発信 IP インターフェイスの設定

セキュリティ管理アプライアンスで、隔離に関係するメッセージ（通知や解放された電子メールなど）を 電子メール セキュリティ アプライアンスに送信するインターフェイスを設定します。

ステップ 1　この手順は、「IP インターフェイスの設定」（P.A-2）の説明と併せて実行してください。

ステップ 2　セキュリティ管理アプライアンスで、[Management Appliance] > [Network] > [IP Interfaces] を選択します。

ステップ 3　[Add IP Interface] をクリックします。

ステップ 4　次の設定値を入力します。

- 名前
- イーサネット ポート

  通常は Data 2 になります。具体的には、この設定は [Management Appliance] > [Centralized Services] > [Spam Quarantine] の [Spam Quarantine Settings] ページにおいて、[Deliver Messages Via] セクションでプライマリ サーバに指定した電子メール セキュリティ アプライアンスのデータ インターフェイスと同じである必要があります。
- IP アドレス

  上で指定したインターフェイスの IP アドレス。
- ネットマスク
- ホスト名

  たとえば、Data 2 インターフェイスの場合は、`data2.sma.example.com` を使用します。

このインターフェイスの [Spam Quarantine] セクションには入力しないでください。

ステップ 5　変更を送信し、保存します。

スパム隔離にアクセスするための IP アドレスの設定

管理者またはエンド ユーザがスパム隔離にアクセスするときには、専用のブラウザ ウィンドウが開きます。

ステップ 1　セキュリティ管理アプライアンスで、[Management Appliance] > [Network] > [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　[Spam Quarantine] セクションで、スパム隔離にアクセスするための設定を行います。

- [HTTP] または [HTTPS]、あるいはその両方を選択し、ポートを指定します。
- 通知とスパム隔離のブラウザ ウィンドウに記載される URL を指定します。

  たとえば、使用しているセキュリティ管理アプライアンスのホスト名を表示したくない場合には、代わりのホスト名を指定できます。

  ここに入力した URL や IP アドレスが、使用している DNS サーバで解決できることを確認してください。

ステップ 4　変更を送信し、保存します。

中央集中型スパム隔離のための電子メール セキュリティ アプライアンスの設定

セキュリティ管理アプライアンスで中央集中型の Cisco IronPort スパム隔離サービスを使用するには、電子メール セキュリティ アプライアンスでスパム隔離の設定を一部変更する必要があります。

操作内容	参照先
電子メール セキュリティ アプライアンスでスパム隔離が正しく動作していることを確認します。 何らかの問題がある場合は、スパム隔離を中央集中型にする前に解決します。	—
セキュリティ管理アプライアンスを外部スパム隔離として使用するよう、電子メール セキュリティ アプライアンスをイネーブル化および設定します。	「中央集中型スパム隔離のための電子メール セキュリティ アプライアンスの設定」（P.7-6）

操作内容	参照先
電子メール セキュリティ アプライアンス でローカルのスパム隔離をディセーブルにします。	『*Cisco IronPort AsyncOS for Email Security Daily Management Guide*』の「Disabling the Local IronPort Spam Quarantine」 この変更によって生じたメール ポリシーを調整するための警告は無視します。メール ポリシーで外部スパム隔離を使用するようになります。
電子メール セキュリティ アプライアンスで既存のローカルのスパム隔離メッセージを管理する方法を確認します。	『*Cisco IronPort AsyncOS for Email Security Daily Management Guide*』の「Migrating from a Local IronPort Spam Quarantine to an External Quarantine」

中央集中型スパム隔離のための電子メール セキュリティ アプライアンスの設定

電子メール セキュリティ アプライアンスでセキュリティ管理アプライアンスの Cisco IronPort スパム隔離を使用するには、電子メール セキュリティ アプライアンスの外部隔離を設定する必要があります。

（注）　これまで、電子メール セキュリティ アプライアンスに別の外部スパム隔離を設定していた場合は、まず、その外部スパム隔離設定をディセーブルにする必要があります。

外部隔離を設定するには、次の手順を**すべての** 電子メール セキュリティ アプライアンスで実行する必要があります。

ステップ 1　電子メール セキュリティ アプライアンスで、[Security Services] > [External Spam Quarantine] を選択します。

ステップ 2　[Configure] をクリックします。

ステップ 3　チェックボックスを選択して、外部スパム隔離をイネーブルにします。

ステップ 4　Cisco IronPort スパム隔離の名前を入力します。隔離領域があるセキュリティ管理アプライアンスの名前を入力することもできます。

ステップ 5　セキュリティ管理アプライアンスの正しいインターフェイスの IP アドレスを入力します。

通常は管理インターフェイスのアドレスになります。具体的には、[Management Appliance] > [Centralized Services] > [Spam Quarantine] の [Spam Quarantine Settings] ページにある [Quarantine IP Interface] 設定で、セキュリティ管理アプライアンスに指定したインターフェイスに割り当てた IP アドレスです。

指定したインターフェイスの IP アドレスを表示するには、セキュリティ管理アプライアンスで、[Management Appliance] > [Network] > [IP Interfaces] を選択して、インターフェイス名をクリックしてください。

ステップ 6　スパムおよびその疑いのあるメッセージの配信に使用するポート番号を入力します。デフォルトは 6025 です。このポート番号は、[Management Appliance] > [Centralized Services] > [Spam Quarantine] の [Spam Quarantine Settings] ページで入力した隔離ポート番号と同じである必要があります。

ステップ 7　簡単にするために、セーフリスト/ブロックリスト機能は後で設定します。全体の説明と詳細については、「エンド ユーザのセーフリスト/ブロックリスト機能の設定と管理」（P.7-11）を参照してください。

ステップ 8　変更を送信し、保存します。

ステップ 9　ローカルのスパム隔離をディセーブルにします。『*Cisco IronPort AsyncOS for Email Security Daily Management Guide*』の「Disabling the Local IronPort Spam Quarantine」を参照してください。

この変更によって生じたメール ポリシーを調整するための警告は無視します。メール ポリシーで外部スパム隔離を使用するようになります。

ステップ 10　管理対象の電子メール セキュリティ アプライアンスに対して、この手順を繰り返します。

管理対象の各電子メール セキュリティ アプライアンスへの中央集中型スパム隔離サービスの追加

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

ステップ 1　セキュリティ管理アプライアンスで、[Management Appliance] > [Centralized Services] > [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.　[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.　[Add Email Appliance] をクリックします。

b.　[Appliance Name and IP Address] テキスト フィールドに、Cisco IronPort アプライアンスの管理インターフェイスのアプライアンス名と IP アドレスを入力します。

（注）　[IP Address] テキスト フィールドに DNS 名を入力した場合でも、[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.　[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、[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.　[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.　[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　[Submit] をクリックします。

ステップ 5　スパム隔離をイネーブルにする電子メール セキュリティ アプライアンスごとに、この手順を繰り返します。

ステップ 6　変更を保存します。

Cisco IronPort スパム隔離への管理者ユーザ アクセスの設定

この項の手順を実行すると、Operator、Read-Only Operator、Help Desk のロール、または Guest ロール、およびスパム隔離にアクセスできるカスタム ユーザ ロールを持つ管理者ユーザが、Cisco IronPort スパム隔離でメッセージを管理できるようになります。

デフォルトの admin ユーザ、Email Administrator ユーザを含む Administrator レベルのユーザは、常にスパム隔離にアクセスできるので、この手順を使用してスパム隔離機能に関連付ける必要はありません。

（注）　管理者レベル以外のユーザはスパム隔離のメッセージにアクセスできますが、隔離の設定を編集することはできません。管理者レベルのユーザは、メッセージにアクセスし、設定を編集することができます。

完全な管理者権限を持っていない管理者ユーザがスパム隔離のメッセージを管理できるようにするには、次の手順を実行してください。

ステップ 1　ユーザを作成し、そのユーザにスパム隔離へのアクセス権があるユーザ ロールを割り当てる必要があります。詳細については、「管理タスクの分散について」（P.12-1）を参照してください。

ステップ 2　セキュリティ管理アプライアンスで、[Management Appliance] > [Centralized Services] > [Spam Quarantine] を選択します。

ステップ 3　[Spam Quarantine Settings] セクションで、[Enable] または [Edit Settings] をクリックします。

ステップ 4　[Spam Quarantine Settings] セクションの [Administrative Users] 領域で、[Local Users]、[Externally Authenticated Users]、または [Custom User Roles] の選択リンクをクリックします。

ステップ 5　スパム隔離のメッセージを表示および管理できるアクセス権を付与するユーザを選択します。

ステップ 6　[OK] をクリックします。

ステップ 7　必要な場合、このセクションの [Administrative Users] にリストされているその他のタイプ（[Local Users]、[Externally Authenticated Users]、または [Custom User Roles]）について繰り返します。

ステップ 8　変更を送信し、保存します。

エンドユーザのためのスパム管理機能の設定

- 「エンド ユーザ隔離へのアクセスの設定」（P.7-9）
- 「エンドユーザのためのスパム通知の設定」（P.7-10）
- 「エンド ユーザのセーフリスト / ブロックリスト機能の設定と管理」（P.7-11）

（注）　追加設定はいずれか 1 つだけ設定でき、それ以外は設定できません。たとえば、常に要求に基づいて、または指定されたユーザにのみアクセスを許可する場合、エンド ユーザ アクセスを設定できますが、スパム通知は設定できません。

エンド ユーザ隔離へのアクセスの設定

電子メール ユーザが、Cisco IronPort スパム隔離で自身のメッセージを管理できるようにします。

ステップ 1　セキュリティ管理アプライアンスで、[Management Appliance] > [Centralized Services] > [Spam Quarantine] を選択します。

ステップ 2　[Cisco IronPort Spam Quarantine Settings] セクションで [Edit Settings] をクリックします。

ステップ 3　[End-User Quarantine Access] セクションまでスクロールします。

ステップ 4　[Enable End-User Quarantine Access] チェックボックスをオンにします。

ステップ 5　エンド ユーザが隔離されたメッセージを表示しようとしたときに、エンド ユーザを認証する方式を指定します。メールボックス認証、LDAP 認証、または「なし」を指定できます。

- **メールボックス認証**：認証用の LDAP ディレクトリがないサイトの場合、スパム隔離では、ユーザのメールボックスを保有している標準の IMAP サーバまたは POP サーバにユーザの電子メール アドレスとパスワードを照合することができます。Web UI にログインするとき、ユーザは自身の完全な電子メール アドレスとメールボックスのパスワードを入力します。隔離はこの情報を使用し、そのユーザとしてメールボックス サーバにログインします。ログインに成功すると、そのユーザは認証され、スパム隔離はユーザの受信箱を変更せずにメールボックス サーバからログアウトします。LDAP ディレクトリを使用しないサイトには、メールボックス認証が推奨されます。ただし、メールボックス認証では、複数の電子メール エイリアスに送信された隔離済みメッセージを表示できません。

  メールボックス サーバのタイプ（IMAP または POP）を選択します。サーバ名と、安全な接続に SSL を使用するかどうかを指定します。サーバのポート番号を入力します。未修飾のユーザ名の後ろに追加するドメイン（company.com など）を入力します。

  POP サーバがバナーに APOP サポートをアドバタイズする場合は、セキュリティの理由から（すなわち、パスワードがクリアな状態で送信されないように）、アプライアンスでは APOP だけを使用します。一部のユーザで APOP がサポートされていない場合は、APOP をアドバタイズしないように POP サーバを再設定する必要があります。

- LDAP：LDAP サーバまたはアクティブなエンド ユーザ認証クエリーが設定されていない場合は、[Management Appliance] > [System Administration] > [LDAP] リンクを選択して、LDAP サーバ設定とエンド ユーザ認証クエリー ストリングを設定します。LDAP 認証の設定の詳細については、「LDAP サーバ プロファイルの作成」（P.10-2）を参照してください。

- [None]：認証をイネーブルにしなくても、Cisco IronPort スパム隔離へのエンド ユーザのアクセスを許可できます。この場合、ユーザは通知メッセージのリンクをクリックして隔離にアクセスでき、システムはメールボックス認証または LDAP 認証を行いません。

ステップ 6　隔離からメッセージが解放される前に、メッセージ本文を表示するかどうかを指定します。このチェックボックスが選択されていると、[Cisco IronPort Spam Quarantine] ページでメッセージ本文を表示できなくなります。代わりとして、隔離されたメッセージを表示するには、そのメッセージを解放してから、ユーザのメール アプリケーション（Microsoft Outlook など）で表示する必要があります。この機能は、ポリシーおよび規制（表示したすべての電子メールをアーカイブすることが要求されている場合など）へのコンプライアンスの目的で使用できます。

ステップ 7　変更を送信し、保存します。

エンドユーザのためのスパム通知の設定

スパム通知とは、Cisco IronPort スパム隔離内にメッセージが捕捉されているときに、電子メール ユーザに送信される電子メール メッセージのことです。通知には、そのユーザ宛の隔離されたスパムまたはその疑いのあるメッセージのリストが含まれます。さらに、各ユーザがそれぞれの隔離されたメッセージを表示できるリンクも含まれます。イネーブルにすると、指定したスケジュールに従って通知が送信されます。

スパム通知を使用すると、エンド ユーザが LDAP 認証またはメールボックス認証を使用しないでスパム隔離にログインできるようになります。ユーザは、受信した電子メール通知を介して隔離にアクセスします（その隔離に対して通知がイネーブルになっている場合）。メッセージの件名をクリックすると、ユーザは隔離の Web UI にログインします。

（注）　このログイン方式では、そのエンド ユーザが持っている可能性のある他のエイリアス宛の隔離済みメッセージは表示されません。また、アプライアンスで処理した後に展開される配布リストに通知が送信された場合、複数の受信者がそのリストの同じ隔離にアクセスできます。

アプライアンスがスパム通知を生成する方法でそのようになっているため、ユーザは、自分の電子メール エイリアス宛の複数のスパム通知を受信することがあります。また、複数の電子メール アドレスを使用しているユーザも、複数のスパム通知を受信することがあります。複数の通知は、エイリアス統合機能を使用して一部の発生を防ぐことができます。LDAP サーバまたはアクティブなエイリアス統合クエリーが設定されていない場合は、[Management Appliance] > [System Administration] > [LDAP] を選択して、LDAP サーバ設定とエイリアス統合クエリー ストリングを設定します。詳細については、「エンドユーザのためのスパム管理機能の設定」（P.7-8）を参照してください。

ステップ 1　セキュリティ管理アプライアンスで、[Management Appliance] > [Centralized Services] > [Spam Quarantine] を選択します。

ステップ 2　[Cisco IronPort Spam Quarantine Settings] セクションで [Edit Settings] をクリックします。

ステップ 3　[Enable Spam Notification] チェックボックスをオンにして、スパム通知をイネーブルにします。

ステップ 4　通知の [From Address] を入力します。このアドレスを、ユーザの電子メール クライアントでサポートされている「ホワイトリスト」に追加することもできます。

ステップ 5　通知の [Subject] を入力します。

ステップ 6　カスタマイズする通知の [Title] を入力します。

ステップ 7　[Default Language] を選択します。

ステップ 8　メッセージ本文をカスタマイズします。AsyncOS では、メッセージ本文に挿入されると、個々のエンド ユーザに対応した実際の値に展開されるいくつかのメッセージ変数がサポートされています。たとえば、**%username%** は、そのユーザへの通知が生成されるときに、実際のユーザ名に展開されます。サポートされるメッセージ変数には、次のものがあります。

- [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。
- [Total Message Count]（**%total_message_count%**）：エンド ユーザ隔離内にあるこのユーザ宛のメッセージの数
- [Days Until Message Expires]（**%days_until_expire%**）

- [Quarantine URL]（**%quarantine_url%**）：スパム隔離にログインし、メッセージを表示するための URL。
- [Username]（**%username%**）
- [New Message Table]（**%new_quarantine_messages%**）：隔離領域内にあるこのユーザ宛の新しいメッセージのリスト

これらのメッセージ変数は、[Message Body] フィールドのテキスト内に直接入力して、メッセージ本文に挿入できます。あるいは、変数を挿入する場所にカーソルを配置してから、右側の [Message Variables] リスト内にある変数の名前をクリックすることもできます。

ステップ 9　メッセージ形式（HTML、テキスト、または HTML/テキスト）を選択します。

ステップ 10　バウンス アドレスを指定します。バウンスされた通知は、このアドレスに送信されます。

ステップ 11　必要に応じて、異なるアドレスで同じ LDAP ユーザに送信されたメッセージを統合できます。

ステップ 12　通知スケジュールを設定します。通知を月に一度、週に一度、または毎日（平日のみ、または週末も含めて）の指定した時間に送信するように設定できます。

ステップ 13　変更を送信し、保存します。

エンド ユーザのセーフリスト/ブロックリスト機能の設定と管理

エンド ユーザによるセーフリストとブロックリストの作成を許可して、スパムとして処理する電子メール メッセージをより適切に制御できます。セーフリストによって、指定されたユーザおよびドメインからのメールがスパムとして処理されないようにできます。ブロックリストでは、他のユーザおよびドメインからのメールが常にスパムとして処理されるようにします。セーフリスト/ブロックリスト機能がイネーブルにされると、各エンド ユーザは、自分の電子メール アカウントに対してセーフリストとブロックリストを維持できるようになります。

（注）　セーフリストやブロックリストを設定しても、メッセージに対するウイルスのスキャンや、内容に関連したメール ポリシーの基準をメッセージが満たすかどうかの判定は、電子メール セキュリティ アプライアンスで実行されます。セーフリストのメンバーから送信されたメッセージの場合、他のスキャン設定に従って配信されない場合があります。

ユーザがセーフリストまたはブロックリストにエントリを追加すると、そのエントリは セキュリティ管理アプライアンス上のデータベースに保管され、関連するすべての 電子メール セキュリティ アプライアンスで、定期的に更新および同期されます。同期の詳細については、「セーフリストとブロックリストの設定とデータベースの同期」（P.7-13）を参照してください。データベースのバックアップの詳細については、「セーフリスト/ブロックリスト データベースのバックアップと復元」（P.7-14）を参照してください。

セーフリストとブロックリストは、エンド ユーザによって作成およびメンテナンスされます。ただし、この機能をイネーブルにし、ブロックリスト内のエントリに一致する電子メール メッセージの配信設定を設定するのは管理者です。セーフリストとブロックリストは Cisco IronPort スパム隔離に関連するため、配信の動作は、他のアンチスパム設定にも左右されます。電子メール パイプラインでメッセージが電子メール セキュリティ マネージャに到達する前に発生する処理に基づいて、メッセージがアンチスパム スキャンをスキップすることがあります。メッセージ処理の詳細については、『*Cisco IronPort AsyncOS for Email Security Configuration Guide*』の「Understanding the Email Pipeline」を参照してください。

たとえば、アンチスパム スキャンをスキップするように HAT で「Accept」メール フロー ポリシーを設定すると、そのリスナー上でメールを受信するユーザでは、自分のセーフリストとブロックリストの設定をそのリスナー上で受信されたメールに適用しないようになります。同様に、一部のメッセージ受信者についてアンチスパム スキャンをスキップするメールフロー ポリシーを作成すると、それらの受信者は、自分のセーフリストとブロックリストの設定が適用されなくなります。

セーフリスト/ブロックリスト メッセージの配信の詳細については、「セーフリストとブロックリストのメッセージ配信」（P.7-13）を参照してください。

セキュリティ管理アプライアンスでのセーフリスト/ブロックリストのイネーブル化と設定

セーフリスト/ブロックリスト機能をイネーブル化する前に、アプライアンスで Cisco IronPort スパム隔離をイネーブル化する必要があります。Cisco IronPort スパム隔離のイネーブル化の詳細については、「中央集中型スパム隔離の設定」（P.7-2）を参照してください。

ステップ 1　セキュリティ管理アプライアンスで、[Management Appliance] > [Centralized Services] > [Spam Quarantine] を選択します。

ステップ 2　[End-User Safelist/Blocklist] セクションで [Enable] をクリックします。

ステップ 3　[End-User Safelist/Blocklist] セクションで [Edit Settings] をクリックします。

ステップ 4　[Enable End User Safelist/Blocklist Feature] チェックボックスがオンになっていることを確認します。

ステップ 5　ユーザごとの最大リスト項目数を指定します。この値は、ユーザがそれぞれのセーフリスト/ブロックリストに含めることのできるアドレスとドメインの最大数です。デフォルトは 100 です。

（注）　ユーザごとのリスト エントリ数を大きくすると、システムのパフォーマンスに悪影響を与えることがあります。

ステップ 6　更新頻度を選択します。この値によって、AsyncOS がシステムにある 電子メール セキュリティ アプライアンスのセーフリスト/ブロックリスト データベースを更新する頻度が決まります。M10、M600、および M650 アプライアンスのデフォルトは、2 時間ごとです。M1000 および M1050 アプライアンスのデフォルトは、4 時間ごとです。

ステップ 7　変更を送信し、保存します。

ステップ 8　この機能の中央集中化をサポートするよう、電子メール セキュリティ アプライアンスを設定します。「電子メール セキュリティ アプライアンスでのセーフリスト/ブロックリストの設定」（P.7-12）を参照してください。

電子メール セキュリティ アプライアンスでのセーフリスト/ブロックリストの設定

管理対象の電子メール セキュリティ アプライアンスでセーフリスト/ブロックリストの設定を行うには、**それぞれの**電子メール セキュリティ アプライアンスで次の手順を実行してください。

ステップ 1　電子メール セキュリティ アプライアンスで、[Security Services] > [External Spam Quarantine] を選択します。

ステップ 2　[Edit Settings] ボタンをクリックします。

ステップ 3　セーフリスト/ブロックリスト機能をイネーブルにするチェックボックスを選択します。

ステップ 4　ブロックリストに含まれる送信者からのメッセージを隔離するか、削除するかを選択します。

ステップ 5　変更を送信し、保存します。

ステップ 6　管理対象の電子メール セキュリティ アプライアンスに対して、この手順を繰り返します。

セーフリストとブロックリストの設定とデータベースの同期

セキュリティ管理アプライアンスを使用すると、簡単に、すべての管理対象アプライアンスでセーフリスト/ブロックリスト データベースを同期することができます。

（注）　セーフリスト/ブロックリスト データベースを同期する前に、セーフリスト/ブロックリスト機能をイネーブル化して、少なくとも 1 台の管理対象アプライアンスを セキュリティ管理アプライアンスに追加する必要があります。管理対象アプライアンスを追加する方法の詳細については、「管理対象アプライアンスの追加について」（P.2-16）を参照してください。

セーフリスト/ブロックリスト データベースを同期するには、[Management Appliance] > [Centralized Services] > [Spam Quarantine] ページで [Synchronize All Appliances] ボタンをクリックします。

集中管理機能を使用して複数のアプライアンスを設定する場合は、集中管理を使用して管理者設定を設定できます。集中管理を使用しない場合は、マシン間で設定が整合していることを手動で確認できます。

FTP を使用してアプライアンスにアクセスする方法の詳細については、付録 A「IP インターフェイスおよびアプライアンスへのアクセス」（P.1）を参照してください。

セーフリストとブロックリストのメッセージ配信

セーフリストとブロックリストをイネーブルにすると、電子メール セキュリティ アプライアンスは、アンチスパム スキャンの直前にセーフリスト/ブロックリスト データベースと照合してメッセージをスキャンします。アプライアンスがエンド ユーザのセーフリスト/ブロックリスト設定に一致する送信者またはドメインを検出したとき、セーフリスト/ブロックリスト設定が異なる受信者が複数存在すると、そのメッセージは分割されます。たとえば、送信者 X が受信者 A と受信者 B の両方にメッセージを送信したとします。受信者 A のセーフリストには送信者 X のエントリがありますが、受信者 B のセーフリストにもブロックリストにも、この送信者のエントリがありません。この場合、メッセージは 2 つのメッセージ ID で 2 つのメッセージに分割されます。受信者 A に送信されたメッセージには、*X-SLBL-Result-Safelist* ヘッダーによって、セーフリストに登録されているというマークが付けられます。これにより、アンチスパム スキャンがスキップされます。受信者 B に宛てられたメッセージは、アンチスパム スキャン エンジンでスキャンされます。その後、どちらのメッセージもパイプライン（アンチウイルス スキャン、コンテンツ ポリシーなど）を続行し、設定されているすべての設定に従います。

メッセージの送信者またはドメインがブロックリストに含まれる場合、配信の動作は、ブロックリスト アクション設定によって決まります。セーフリストの配信の場合と同様に、セーフリスト/ブロックリスト設定の異なる複数の受信者が存在すると、そのメッセージは分裂します。分裂したメッセージのうちブロックリストに含まれるものは、ブロックリスト アクション設定に応じて隔離されるかドロップされます。

（注）　ブロックリスト アクションは、電子メール セキュリティ アプライアンスの外部スパム隔離設定で指定します。詳細については、「中央集中型スパム隔離のための電子メール セキュリティ アプライアンスの設定」（P.7-6）を参照してください。

メッセージを隔離するようにブロックリスト アクションを設定した場合、メッセージはスキャンされ、最終的に隔離されます。メッセージを削除するようにブロックリスト アクションを設定した場合、セーフリスト/ブロックリスト スキャンの直後にメッセージは削除されます。

セーフリスト/ブロックリスト データベースのバックアップと復元

セーフリスト/ブロックリスト データベースのバックアップを維持できるように、セキュリティ管理アプライアンスでデータベースを .csv ファイルとして保存できます。.csv ファイルは、アプライアンスの設定が格納される XML コンフィギュレーション ファイルとは別に保管されます。アプライアンスをアップグレードする場合、またはシステム セットアップ ウィザードを実行する場合、まず、セーフリスト/ブロックリスト データベースを .csv ファイルにバックアップする必要があります。

（注）　.csv ファイルを編集してからアップロードすると、個別のエンド ユーザのセーフリストおよびブロックリストを変更できます。

データベースをバックアップすると、アプライアンスによって、.csv ファイルが次の命名規則に従って `/configuration` ディレクトリに保存されます。

slbl-<serial number>-<timestamp>.csv

セキュリティ管理アプライアンスをバックアップするときには、セーフリストおよびブロックリストのデータベースを対象に含めるかどうかを選択できます 「セキュリティ管理アプライアンスのバックアップ」（P.13-6）を参照してください。

ステップ 1　セキュリティ管理アプライアンスで、[Management Appliance] > [System Administration] > [Configuration File] を選択します。

ステップ 2　[End-User Safelist/Blocklist Database (Spam Quarantine)] セクションまでスクロールします。

ステップ 3　データベースを .csv ファイルにバックアップするには、[Backup Now] をクリックします。

ステップ 4　[Select File to Restore] をクリックして、データベースを復元します。

アプライアンスにより、`/configuration` ディレクトリに保管されているバックアップ ファイルのリストが表示されます。

ステップ 5　復元するセーフリスト/ブロックリスト バックアップ ファイルを選択し、[Restore] をクリックします。

セーフリストとブロックリストのトラブルシューティング

エンド ユーザは、自分のセーフリストとブロックリストを管理します。管理者が、エンド ユーザ アカウントにそのユーザのログイン名とパスワードでログインすると、エンド ユーザのセーフリストまたはブロックリストにアクセスできます。または、管理者はセーフリスト/ブロックリスト データベースのバックアップ バージョンをダウンロードして、個別のユーザのリストを編集できます。

セーフリストとブロックリストに関する問題をトラブルシューティングするために、ログ ファイルまたはシステム アラートを表示できます。

電子メール メッセージがセーフリスト/ブロックリスト設定によってブロックされると、そのアクションが ISQ_logs またはアンチスパム ログ ファイルにロギングされます。

アラートは、データベースが作成または更新されたり、データベースの変更またはセーフリスト/ブロックリスト プロセスの実行においてエラーが発生したりすると送信されます。

アラートの詳細については、「アラートの管理」（P.13-34）を参照してください。

ログ ファイルの詳細については、第 14 章「ロギング」を参照してください。

エンド ユーザのセーフリストおよびブロックリストの使用

エンド ユーザは、指定した送信者からのメッセージをスパムの判定から除外するために、セーフリストを作成できます。また、指定した送信者からのメッセージを常にスパムとして扱うために、ブロックリストを使用できます。たとえば、エンド ユーザは、受信したくない電子メールをメーリング リストから受信する場合があります。この送信者をブロックリストに追加すると、この送信者からの電子メール メッセージが配信されないようになります。一方、エンド ユーザは、正当な送信者からの電子メール メッセージが Cisco IronPort スパム隔離に送信されていることに気づき、この電子メール メッセージがスパムとして処理されないようにしたいと考えることがあります。その送信者からのメールが隔離されないようにするには、ユーザのセーフリストに送信者を追加します。

（注）　セーフリスト/ブロックリスト設定は、システム管理者が設定する他の設定の影響を受けます。たとえば、セーフリストに登録されているメッセージが、ウイルス陽性と判断された場合、または管理者によって内容が企業の電子メール ポリシーに準拠していないと判断された場合、このメッセージは配信されません。

セーフリストとブロックリストへのアクセス

LDAP 認証またはメールボックス（IMAP または POP）認証を使用してアカウントが認証されるエンド ユーザは、セーフリストとブロックリストにアクセスするために、Cisco IronPort スパム隔離の自分のアカウントにログインする必要があります。これらのエンド ユーザは、通常はスパム通知経由でメッセージにアクセスしているとしても（この場合は一般に LDAP 認証またはメールボックス認証を必要としません）、自分のアカウントにログインしなければなりません。エンド ユーザ認証が [None] に設定されている場合、エンド ユーザは、セーフリスト/ブロックリスト設定にアクセスする際に自分のアカウントにログインする必要はありません。

セーフリストおよびブロックリストへのエントリの追加

エントリ（IPv6 アドレスを使用するものを含む）をセーフリスト/ブロックリストに追加するときには、次の形式を使用できます。

- user@domain.com

  user@[203.0.113.15]

  user@[ipv6:2001:db8:80:1::5]
- server.domain.com
- domain.com

  [203.0.113.15]

  [ipv6:2001:db8:80:1::5]

エンド ユーザは、同じ送信者またはドメインをセーフリストとブロックリストの両方に同時には追加できません。ただし、あるドメインをセーフリストに追加し、そのドメインに所属するユーザをブロックリストに追加した場合、両方のルールが適用されます（逆の場合も同様です）。たとえば、エンド

ユーザが *example.com* をセーフリストに追加し、*george@example.com* をブロックリストに追加すると、アプライアンスは、example.com からのすべてのメールをスパムかどうかスキャンせずに配信しますが、*george@example.com* からのメールはスパムとして処理します。

エンド ユーザは、.domain.com のような構文を使用して、サブドメインの範囲を許可したり、ブロックしたりはできません。ただし、エンド ユーザは、server.domain.com のような構文を使用して、特定のドメインを明示的にブロックすることはできます。

セーフリストの操作

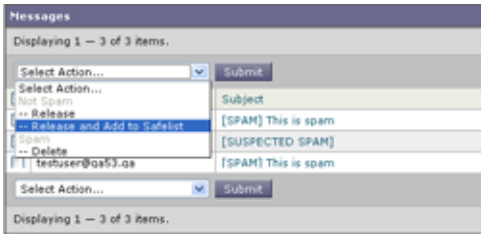
エンド ユーザは、次の 2 つの方法で送信者をセーフリストに追加できます。Cisco IronPort スパム隔離から、グラフィカル ユーザ インターフェイスの右上にある [Options] メニューをクリックし、[Safelist] を選択して、手動で送信者をセーフリストに追加できます。

図 7-1　　エンド ユーザ隔離のセーフリスト

電子メール アドレスまたはドメインをリストに追加し、[Add to List] をクリックします。

エンド ユーザは、メッセージが Cisco IronPort スパム隔離に送信されていても、その送信者をセーフリストに追加できます。特定の送信者からのメッセージが Cisco IronPort スパム隔離に捕捉されている場合、エンド ユーザはそのメッセージの横にあるチェックボックスをオンにして、ドロップダウン メニューから [Release and Add to Safelist] を選択できます。

図 7-2　　エンド ユーザ隔離のセーフリスト



指定したメールのエンベロープ送信者と差出人ヘッダーが両方ともセーフリストに追加されます。解放されたメッセージは、それ以降の電子メール パイプライン内の作業キューの処理をスキップして、宛先キューへ直接進みます。

（注） エンド ユーザは、スパム通知メッセージを使用してメッセージを解放することもできます。[Not Spam] リンクをクリックして、特定のメッセージを解放します。送信者をエンド ユーザのセーフリストに追加するオプションもあります。

ブロックリストの操作

エンド ユーザは、ブロックリストを使用して、指定した送信者からのメールが配信されないようにできます。送信者をブロックリストに追加するには、エンド ユーザ隔離から [Options] > [Blocklist] を選択します。

図 7-3　　ブロックリストへの送信者の追加

エンド ユーザ隔離から、フィールドに電子メール アドレスまたはドメインを入力し、[Add to List] をクリックします。

電子メール セキュリティ アプライアンスは、ブロックリスト内のエントリと一致する電子メール アドレスまたはドメインからのメールを受信すると、そのメールをスパムとして処理します。ブロックリスト アクション設定に応じて、そのメールは削除または隔離されます。

Cisco IronPort スパム隔離内のメッセージの管理

ここでは、管理者が Cisco IronPort スパム隔離内のメッセージを管理する方法について説明します。管理者が隔離を表示する場合、その隔離領域に含まれるすべてのメッセージを利用できます。

（注） メッセージを表示および管理するグラフィカル ユーザ インターフェイスは、Cisco IronPort スパム隔離にアクセスするエンド ユーザ用のものとは少し異なります。エンド ユーザ用のグラフィカル ユーザ インターフェイスについては、エンド ユーザとして Cisco IronPort スパム隔離にアクセスし、オンライン ヘルプを参照してください。

管理者として、Cisco IronPort スパム隔離内のメッセージに対して次のアクションを実行できます。

- メッセージの表示
- メッセージの配信
- メッセージの削除
- メッセージの検索

Cisco IronPort スパム隔離内でのメッセージの検索

ステップ 1　セキュリティ管理アプライアンスで、[Email] > [Message Quarantine] > [Spam Quarantine] を選択します。

ステップ 2　[Spam Quarantine] リンクを選択します。

ステップ 3　検索フォームで、検索する日付を入力します。現在の日、または過去の週からメッセージを検索できます。または、カレンダー アイコンをクリックして、日付範囲を選択できます。

ステップ 4　オプションで、差出人アドレス、受取人アドレス、メッセージ件名のテキスト文字列を指定します。入力した値が検索結果に含まれる、含まれない、全体と一致、先頭と一致、末尾と一致のいずれかを選択します。

ステップ 5　オプションで、エンベロープ受信者を指定します。入力した値が検索結果に含まれる、含まれない、全体と一致、先頭と一致、末尾と一致のいずれかを選択します。

エンベロープ受信者とは、「RCPT TO」SMTP コマンドで定義されている電子メール メッセージ受信者のアドレスです。エンベロープ受信者は、「Recipient To」アドレスまたは「Envelope To」アドレスと呼ばれることもあります。

ステップ 6　[Search] をクリックします。

検索条件に一致するメッセージがページの [Search] セクションの下に表示されます。

大量メッセージの検索

Cisco IronPort スパム隔離内に大量のメッセージが保存されており、検索条件が狭く定義されていない場合、検索結果の表示に時間がかかることや、クエリーがタイムアウトすることがあります。

その場合、検索を再実行するかどうか確認されます。

（注）　大量の検索を同時に複数実行すると、アプライアンスのパフォーマンスに悪影響を与えることがあります。

Cisco IronPort スパム隔離内のメッセージの表示

メッセージのリストにより、Cisco IronPort スパム隔離内のメッセージが表示されます。1 ページに表示されるメッセージの数を選択できます。カラム見出しをクリックすることにより、表示をソートできます。再度カラム見出しをクリックすると、ソートの順を反転できます。

メッセージの件名をクリックしてメッセージを表示します。これには、本文とヘッダーが含まれます。[Message Details] ページには、メッセージの先頭 20K が表示されます。メッセージがそれよりも長い場合は、20K に切り詰められます。ページの下部にあるリンクをクリックすると、メッセージの残りの部分が表示されます。

[Message Details] ページから、[Delete] を選択してメッセージを削除したり、[Release] を選択してメッセージを隔離から解放したりできます。メッセージを解放すると、そのメッセージは配信されます。

HTML メッセージの表示

Cisco IronPort スパム隔離では、HTML ベースのメッセージは近似で表示されます。イメージは表示されません。

符号化されたメッセージの表示

Base64 で符号化されたメッセージは、復号化されてから表示されます。

Cisco IronPort スパム隔離内のメッセージの配信

メッセージを配信のために解放するには、メッセージの隣にあるチェックボックスを選択して、[Release] をクリックします。

ページに表示されているすべてのメッセージを選択するには、見出し行にあるチェックボックスをオンにします。

解放されたメッセージは、それ以降の電子メール パイプライン内の作業キューの処理をスキップして、宛先キューへ直接進みます。

Cisco IronPort スパム隔離からのメッセージの削除

Cisco IronPort スパム隔離では、指定された時間後にメッセージが自動で削除されるように設定できます。Cisco IronPort スパム隔離からメッセージを手動で削除することも可能です。

個別のメッセージを削除するには、削除するメッセージの横にあるチェックボックスをオンにして、[Delete] をクリックします。ページに表示されているすべてのメッセージを選択するには、見出し行にあるチェックボックスをオンにします。

Cisco IronPort スパム隔離内のすべてのメッセージを削除するには、[Management Appliance] > [Centralized Services] > [Spam Quarantine] ページから隔離をディセーブルにして、表示される [Delete All] をクリックします。

CHAPTER 8

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、セキュリティ管理アプライアンスから関連する Web セキュリティ アプライアンスに設定を公開できるようになり、次のような利点が得られます。

- Web セキュリティ ポリシーの設定や設定の更新を個々の Web セキュリティ アプライアンスではなくセキュリティ管理アプライアンスで一度行うだけで済み、管理を簡便化および迅速化できます。
- 展開されているネットワーク全体で、ポリシーを均一に適用できます。

Web セキュリティ アプライアンスには、次の 2 種類のコンフィギュレーション ファイルを公開できます。

- Configuration Master
- コンフィギュレーション ファイル（拡張ファイル公開を使用）

適切な設定公開方式の決定

セキュリティ管理アプライアンスから設定を公開するには異なる 2 つの方法があり、それぞれ異なる設定を公開します。設定の中には中央集中型で管理できないものもあります。

一般的には次のようになります。

- 次の設定に対しては、Configuration Master を使用します。

  Web セキュリティ アプライアンスの [Web Security Manager] メニューに表示される機能。ポリシーやカスタム URL のカテゴリなど。

例外：L4 トラフィック モニタの（L4TM）の設定は、Configuration Master の対象に含まれません。

サポートの対象となる機能は、Configuration Master のバージョンによって変わります。このバージョンは AsyncOS for Web Security のバージョンに対応します。

- 次の設定に対しては、コンフィギュレーション ファイル（拡張ファイル公開）を使用します。

  アプライアンスの管理に関係する機能。たとえば、ログ サブスクリプションやアラートの設定、または管理責任の分散など。

  例外：

  ネットワークやインターフェイスの設定、DNS、Web Cache Communication Protocol（WCCP）、アップストリーム プロキシ グループ、証明書、プロキシ モード、SNTP などの時間設定、レベル 4 トラフィック モニタ（L4TM）の設定、認証リダイレクト ホスト名。

  これらの設定は、管理対象の Web セキュリティ アプライアンスで直接設定する必要があります。『*Cisco IronPort AsyncOS for Web Security User Guide*』を参照してください。

Configuration Master を使用するための設定

Configuration Master を使用して中央集中型コンフィギュレーション管理を設定するには、「Configuration Master を使用するための設定の概要」（P.8-2）で説明する手順を順序に従って実行してください。

拡張ファイル公開だけを使用するように準備するには、「拡張ファイル公開を使用するための設定」（P.8-14）を参照してください。

Configuration Master を使用するための設定の概要

Web セキュリティ アプライアンスを中央集中方式で管理するようにシステムを設定するには、次の手順に従ってください。

ステップ 1　**（任意）Web セキュリティ アプライアンス。**すべての Web セキュリティ アプライアンスの設定モデルとして動作している Web セキュリティ アプライアンスがすでにある場合は、その Web セキュリティ アプライアンスからコンフィギュレーション ファイルをダウンロードします。このファイルを使用すると、セキュリティ管理アプライアンスでの Configuration Master の設定を迅速に行うことができます。方法については、『*Cisco IronPort AsyncOS for Web Security User Guide*』の「Saving and Loading the Appliance Configuration」を参照してください。

コンフィギュレーション ファイルと Configuration Master のバージョンの互換性については、「表 2-3（WSA のある導入のみ）Configuration Master の互換性」（P.2-3）を参照してください。

ステップ 2　設定のための一般的な要件や注意事項を確認します。「Configuration Master を使用するための重要な注意事項」（P.8-3）を参照してください。

ステップ 3　各 Web セキュリティ アプライアンスに使用する Configuration Master のバージョンを確認します。「使用する Configuration Master のバージョンの確認」（P.8-3）を参照してください。

ステップ 4　**セキュリティ管理アプライアンス。**Cisco IronPort 中央集中型コンフィギュレーション マネージャをイネーブルにして設定します。「セキュリティ管理アプライアンスでの中央集中型コンフィギュレーション管理のイネーブル化」（P.8-4）を参照してください。

ステップ 5　**セキュリティ管理アプライアンス。**Configuration Master を初期化します。「Configuration Master の初期化」（P.8-4）を参照してください。

ステップ 6　**セキュリティ管理アプライアンス。**Web セキュリティ アプライアンスを Configuration Master に関連付けます。「Web セキュリティ アプライアンスと Configuration Master の関連付けについて」（P.8-5）を参照してください。

ステップ 7　**セキュリティ管理アプライアンス。**ポリシー、カスタム URL カテゴリ、および Web プロキシ バイパス リストを Configuration Master にインポートするか、手動で設定します。「公開のための設定」（P.8-6）を参照してください。

ステップ 8　**セキュリティ管理アプライアンス。**それぞれの Web セキュリティ アプライアンスでイネーブルにされている機能が、そのアプライアンスに関連付けられている Configuration Master でイネーブルにされている機能と一致していることを確認します。「機能が常にイネーブルにされていることの確認」（P.8-10）を参照してください。

ステップ 9　**セキュリティ管理アプライアンス。**必要とする Configuration Master を設定し、必要な機能をイネーブルにしたら、Web セキュリティ アプライアンスに設定を公開します。「Configuration Master の公開」（P.8-14）を参照してください。

Configuration Master を使用するための重要な注意事項

（注）　中央集中型で管理する Web セキュリティ アプライアンスのそれぞれについて、同名のレルムに対する設定が同一である場合を除いて、[Network] > [Authentication] ですべての [Realm Names] がアプライアンス全体で一意になっていることを確認します。

使用する Configuration Master のバージョンの確認

AsyncOS for Security Management には複数の Configuration Master があるため、複数の Web セキュリティ アプライアンスで異なる機能をサポートする異なるバージョンの AsyncOS for Web Security が実行されているという、異機種混在環境でも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。

使用している AsyncOS for Web Security のバージョンで使用できる Configuration Master を判断するには、「SMA 互換性マトリクス」（P.2-2）を参照してください。

（注）　最善の結果を得るには、Configuration Master のバージョンが、Web セキュリティ アプライアンスの AsyncOS のバージョンと同じである必要があります。古いバージョンの Configuration Master から新しいバージョンの Web セキュリティ アプライアンスに対して公開を行うと、Web セキュリティ アプライアンスの設定が Configuration Master の設定と一致していない場合には、処理に失敗するおそれがあります。この問題は、[Web Appliance Status Details] ページに不一致が見られない場合でも発生することがあります。この場合は、各アプライアンスでの設定を手動で比較する必要があります。

セキュリティ管理アプライアンスでの中央集中型コンフィギュレーション管理のイネーブル化

ステップ 1　セキュリティ管理アプライアンスで、[Management Appliance] > [Centralized Services] > [Web] > [Centralized Configuration Manager] を選択します。

ステップ 2　[Centralized Configuration Manager] ページで [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 Cisco IronPort 中央集中型コンフィギュレーション マネージャをイネーブルにする場合は、エンドユーザ ライセンス契約書を確認し、[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 初期化とインポート

Configuration Master の初期化

（注）　Configuration Master 7.1 を Configuration Master 7.5 にコピーまたはインポートする前に、「Configuration Master 7.5 を設定する前の注意事項」（P.8-24）を参照してください。

ステップ 1　メイン セキュリティ管理アプライアンスで、[Web] > [Utilities] > [Configuration Masters] を選択します。

ステップ 2　[Options] カラムの [Initialize] をクリックします。

ステップ 3　[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、[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、[Use default settings] を選択します。

ステップ 4　[Initialize] をクリックします。

これで Configuration Master が使用可能な状態になります。

ステップ 5　それぞれの Configuration Master のバージョンに対して初期化作業を繰り返します。

（注）　Configuration Master を初期化すると、[Initialize] オプションは使用できなくなります。その代わりに、「公開のための設定」（P.8-6）で説明されている方法のいずれかを使用して Configuration Master を設定します。

Web セキュリティ アプライアンスと Configuration Master の関連付けについて

中央集中型で管理する Web セキュリティ アプライアンスのそれぞれにおいて、そのアプライアンスの AsyncOS バージョンと一致する Configuration Master にポリシー設定を関連付ける必要があります。たとえば、Web セキュリティ アプライアンスで AsyncOS 6.3 for Web を実行中の場合は、Configuration Master 6.3 に関連付ける必要があります。

このための最も単純な方法は、状況によって異なります。

条件	参照する手順
まだ Web セキュリティ アプライアンスをセキュリティ管理アプライアンス に追加していない	「Web セキュリティ アプライアンスの追加と Configuration Master のバージョンとの関連付け」（P.8-5）
すでに Web セキュリティ アプライアンスを追加済みである	「Configuration Master のバージョンと Web セキュリティ アプライアンスとの関連付け」（P.8-6）

Web セキュリティ アプライアンスの追加と Configuration Master のバージョンとの関連付け

まだ Web セキュリティ アプライアンスを中央集中管理の対象に追加していない場合は、この手順を実行してください。

ステップ 1　使用している Web セキュリティ アプライアンスと、この AsyncOS for Security Management のリリースで使用できる Configuration Master のバージョンとの互換性を確認します。「SMA 互換性マトリクス」（P.2-2）を参照してください。

ステップ 2　セキュリティ管理アプライアンスで、[Management Appliance] > [Centralized Services] > [Security Appliances] を選択します。

ステップ 3　[Add Web Appliance] をクリックします。

ステップ 4　[Appliance Name and IP Address] テキスト フィールドに、Cisco IronPort アプライアンスの管理インターフェイスのアプライアンス名と IP アドレスを入力します。

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

ステップ 5　Centralized Configuration Manager サービスが事前に選択されています。

ステップ 6　[Establish Connection] をクリックします。

ステップ 7　管理対象となるアプライアンスの管理者アカウントのユーザ名とパスワードを入力し、[Establish Connection] をクリックします。

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

ステップ 8　[Success] メッセージがページのテーブルの上に表示されるまで待機します。

ステップ 9　アプライアンスに関連付ける Configuration Master のバージョンを選択します。

ステップ 10　変更を送信し、保存します。

ステップ 11　中央集中型コンフィギュレーション管理をイネーブルにする Web セキュリティ アプライアンスごとに、この手順を繰り返します。

Configuration Master のバージョンと Web セキュリティ アプライアンスとの関連付け

Web セキュリティ アプライアンスをセキュリティ管理アプライアンスに追加済みの場合は、次の手順を使用して、Web セキュリティ アプライアンスを Configuration Master のバージョンに素早く関連付けることができます。

ステップ 1　使用している Web セキュリティ アプライアンスと、この AsyncOS for Security Management のリリースで使用できる Configuration Master のバージョンとの互換性を確認します。「SMA 互換性マトリクス」（P.2-2）を参照してください。

ステップ 2　セキュリティ管理アプライアンスで、[Web] > [Utilities] > [Configuration Masters] を選択します。

（注）　Configuration Master が [Disabled] と表示されている場合にイネーブルにするには、[Web] > [Utilities] > [Security Services Display] の順にクリックし、次に [Edit Display Settings] をクリックします。対象とする Configuration Master のチェックボックスを選択して、イネーブルにします。詳細については、「公開する機能のイネーブル化」（P.8-11）を参照してください。

ステップ 3　[Edit Appliance Assignment List] をクリックします。

ステップ 4　関連付けるアプライアンスの行でクリックし、[Masters] カラムにチェックマークを入れます。

ステップ 5　変更を送信し、保存します。

公開のための設定

公開する設定を Configuration Master に設定します。

Configuration Master の設定には、いくつかの方法があります。

- AsyncOS for Security Management の以前のリリースからアップグレードする場合 : 以前の既存の Configuration Master をコピーして新しい Configuration Master のバージョンを初期化していない場合は、古いバージョンをインポートすることができます。「既存の Configuration Master からのインポート」（P.8-7）を参照してください。

- Web セキュリティ アプライアンスを設定済みで、複数の Web セキュリティ アプライアンスで同じ設定を使用したい場合：保存されているコンフィギュレーション ファイルをアプライアンスから Configuration Master にインポートします（「Configuration Master を使用するための設定」（P.8-2）でコンフィギュレーション ファイルを保存した場合）。

  インポートの手順については、「Web セキュリティ アプライアンスからの設定のインポート」（P.8-7）を参照してください。
- インポートした設定を変更する場合は、「Configuration Master での Web セキュリティ機能の直接設定」（P.8-8）を参照してください。
- Web セキュリティ アプライアンスでポリシー、URL カテゴリ、バイパス設定をまだ設定していない場合は、セキュリティ管理アプライアンスでこれらの設定を対応する Configuration Master に設定します。

  詳細については、「Configuration Master での Web セキュリティ機能の直接設定」（P.8-8）を参照してください。

既存の Configuration Master からのインポート

既存の Configuration Master を新しい Configuration Master のバージョンにアップグレードすることができます。たとえば、Configuration Master 7.1 の設定を、新しい Configuration Master 7.5 にインポートすることができます。

（注）　Configuration Master 7.5 にコピーまたはインポートする前に、「Configuration Master 7.5 を設定する前の注意事項」（P.8-24）を参照してください。

ステップ 1　セキュリティ管理アプライアンスで、[Web] > [Utilities] > [Configuration Masters] を選択します。

ステップ 2　[Options] カラムで、[Import Configuration] をクリックします。

ステップ 3　[Select Configuration Source] で、リストから [Configuration Master] を選択します。

ステップ 4　この設定に、既存のカスタム ユーザ ロールを取り込むかどうかを選択します。

カスタム ユーザ ロールの詳細については、「Custom Web User ロールについて」（P.12-9）を参照してください。

ステップ 5　[Import] をクリックします。

Web セキュリティ アプライアンスからの設定のインポート

使用中の Web セキュリティ アプライアンスで機能している既存の設定を使用する場合は、そのコンフィギュレーション ファイルをセキュリティ管理アプライアンスにインポートして、Configuration Master 用のデフォルトのポリシー設定を作成できます。

コンフィギュレーション ファイルと Configuration Master のバージョンの互換性については、「表 2-3（WSA のある導入のみ）Configuration Master の互換性」（P.2-3）を参照してください。

警告　管理対象の Web セキュリティ アプライアンスに設定をすでに公開してある場合でも、互換性のある Web コンフィギュレーション ファイルを何回でもインポートすることができます。ただし、コンフィギュレーション ファイルを Configuration Master にインポートすると、選択した

Configuration Master に関連付けられている設定が上書きされることに注意してください。また、[Security Services Display] ページのセキュリティ サービスの設定は、インポートしたファイルと一致するよう設定されます。

Configuration Master に Web コンフィギュレーション ファイルを取り込むには、次の手順を実行します。

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] > [Utilities] > [Configuration Masters] を選択します。

ステップ 3　[Options] カラムで、[Import Configuration] をクリックします。

ステップ 4　[Select Configuration] ドロップダウン リストから、[Web Configuration File] を選択します。

ステップ 5　[New Master Defaults] セクションで、[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　[Import File] をクリックします。

ステップ 7　[Import] をクリックします。

Configuration Master での Web セキュリティ機能の直接設定

Configuration Master では、バージョンに応じて次の機能を設定することができます。

Configuration Master 6.3	Configuration Master 7.1	Configuration Master 7.5
• ID • 復号ポリシー • ルーティング ポリシー • アクセス ポリシー • プロキシ バイパス • IronPort データ セキュリティ ポリシー • 外部 DLP ポリシー • カスタム URL カテゴリ • 時間範囲	• ID • SaaS ポリシー • 復号ポリシー • ルーティング ポリシー • アクセス ポリシー • 全体の帯域幅の制限 • IronPort データ セキュリティ • 外部データ消失防止 • Outbound Malware Scanning • カスタム URL カテゴリ • 定義済みの時間範囲 • バイパス設定	• ID • SaaS ポリシー • 復号ポリシー • ルーティング ポリシー • アクセス ポリシー • 全体の帯域幅の制限 • IronPort データ セキュリティ • 外部データ消失防止 • Outbound Malware Scanning • カスタム URL カテゴリ • 定義済みの時間範囲 • バイパス設定

Configuration Master で各機能を直接設定するには、[Web] > [Configuration Master <*version*>] > <*feature*> を選択します。

「Configuration Master で機能を設定する場合の SMA 特有の違い」（P.8-9）で説明する一部の項目を除いて、Configuration Master で機能を設定する方法は、Web セキュリティ アプライアンスで同じ機能を設定する場合と同じです。各説明については、Configuration Master のバージョンに対応する AsyncOS のバージョンの『*Cisco IronPort AsyncOS for Web Security User Guide*』を参照してくださ

い。必要な場合は、「使用する Configuration Master のバージョンの確認」（P.8-3）を参照して、使用している Web セキュリティ アプライアンスに対応する正しい Configuration Master を判別してください。

Web セキュリティ ユーザ ガイドは、http://www.cisco.com/en/US/products/ps10164/products_user_guide_list.html ですべてのバージョンを入手できます。

Configuration Master で機能を設定する場合の SMA 特有の違い

Configuration Master で機能を設定するときには、以下で説明する Web セキュリティ アプライアンスで同じ機能を直接設定する場合との違いに注意してください。

表 8-1　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] > [Utilities] > [Security Services Display] にある機能をイネーブルにする必要があります。詳細については、「機能が常にイネーブルにされていることの確認」（P.8-10）を参照してください。
[Identities] > [Add or Edit Identity]	[Identify Users Transparently] オプションは、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ときに有効になります。 この機能は、Configuration Master 7.5 で導入されました。
ID	「Configuration Master で ID を使用する場合のヒント」（P.8-9）を参照してください。
SaaS ポリシー	認証オプションの [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。
[Access Policies] > [Edit Group]	[Policy Member Definition] セクションで [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。 [Edit Group] ページでグループを検索した場合、検索結果の最初の 500 項目しか表示されません。対象とするグループが見つからない場合は、そのグループを「Authorized Groups」に追加することができます。これを行うには、[Directory] 検索フィールドにこのグループを入力して、[Add] ボタンをクリックします。
[Access Policies] > [Web Reputation and Anti-Malware Settings]	このページで指定できるオプションは、関連する Configuration Master に対して Adaptive Scanning がイネーブルにされているかどうかによって変わります。[Web] > [Utilities] > [Security Services Display] でこの設定を確認してください。 この機能は、Configuration Master 7.5 で導入されました。

Configuration Master で ID を使用する場合のヒント

セキュリティ管理アプライアンスで ID を作成する際には、特定のアプライアンスのみに適用されるオプションがあります。たとえば、セキュリティ管理アプライアンスを購入し、Web セキュリティ アプライアンスごとに作成された既存の Web セキュリティ アプライアンス コンフィギュレーションとポリシーを保持する場合は、1 つのファイルをマシンにロードし、次に他のマシンから手動でポリシーを追加する必要があります。

これを実行するための方法の 1 つとして、各アプライアンスに一連の ID を作成し、これらの ID を参照するポリシーを設定する方法があります。セキュリティ管理アプライアンスが設定を公開すると、これらの ID と、ID を参照するポリシーは自動的に削除され、ディセーブルになります。この方法を使用すると、手動で何も設定する必要がありません。これは基本的に「アプライアンスごと」の ID です。

この方法の唯一の問題は、デフォルトのポリシーまたは ID が、サイト間で異なる場合です。たとえば、あるサイトではポリシーを「default allow with auth」に設定し、別のサイトでは「default deny」に設定している場合です。この場合、アプライアンスごとの ID とポリシーをデフォルトのすぐ上に作成する必要があります。基本的には独自の「デフォルト」ポリシーを作成します。

機能が常にイネーブルにされていることの確認

Configuration Master を公開する前に、それが公開されることと、公開後に目的の機能がイネーブルになり、意図するように設定されていることを確認します。

このためには、次の両方を実行してください。

- 「イネーブルにされている機能の比較」（P.8-10）
- 「公開する機能のイネーブル化」（P.8-11）

（注）　異なる機能がイネーブルになっている複数の Web セキュリティ アプライアンスが同じ Configuration Master に割り当てられている場合は、各アプライアンスを別個に公開するようにし、公開前にこれらの手順を実行する必要があります。

イネーブルにされている機能の比較

それぞれの Web セキュリティ アプライアンスでイネーブルにされている機能が、そのアプライアンスに関連付けられている Configuration Master でイネーブルにされている機能と一致していることを確認します。

（注）　異なる機能を持つ複数の Web セキュリティ アプライアンスが同じ Configuration Master に割り当てられている場合は、各アプライアンスを別個に公開するようにし、公開前にこのチェックを実行する必要があります。

Web セキュリティ アプライアンスでイネーブルにされている機能を確認するには、次の手順を実行します。

ステップ 1　セキュリティ管理アプライアンスで、[Web] > [Utilities] > [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　[Security Services] テーブルまでスクロールします。

ステップ 4　イネーブルにされているすべての機能の機能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　[Services] カラムの設定を比較します。

[Web Appliance Service] カラムと、[Is Service Displayed on Management Appliance?] カラムが同じである必要があります。

[Enabled] = [Yes]

[Disabled] および [Not Configured] = [No] または [Disabled]

[N/A] は適用外であることを意味します。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、機能キーのステータスを確認することができます。

コンフィギュレーションが不一致の場合は、文字が赤色で表示されます。

ステップ 6　ある機能についてのイネーブルおよびディセーブルの設定が一致していない場合は、次のいずれかを実行します。

- Configuration Master の対応する設定を変更します。「公開する機能のイネーブル化」（P.8-11）を参照してください。
- Web セキュリティ アプライアンスの当該の機能をイネーブルまたはディセーブルにします。変更内容によっては、複数の機能に影響する場合があります。関連する機能については、『*Cisco IronPort AsyncOS for Web Security User Guide*』を参照してください。

公開する機能のイネーブル化

Configuration Master を使用して設定を公開する機能をイネーブルにします。

（注）　Configuration Master に対して機能をイネーブルにしても、その機能が Web セキュリティ アプライアンスでイネーブルになるわけではありません。

各 Configuration Master に対してイネーブルにした機能は、[Security Services Display] ページに要約されます。「N/A」と表示されている場合は、その機能がその Configuration Master のバージョンで使用できないことを表します。

図 8-1　[Security Services Display] ページ

Security Services Display

Configuration Master Settings for Display of Security Services

Features	Configuration Masters		
	6.3	7.1	7.5
Transparent mode	Yes	Yes	Yes
FTP Proxy	Yes	Yes	Yes
HTTPS Proxy	Yes	Yes	Yes
Upstream Proxy Groups	Yes	Yes	Yes
Acceptable Use Controls	Cisco IronPort Web Usage Controls	Cisco IronPort Web Usage Controls (with Application Visibility and Control)	Cisco IronPort Web Usage Controls (with Application Visibility and Control)
AnyConnect Secure Mobility	N/A	IP Range	IP Range
Web Reputation Filters	Yes	Yes	Yes (Adaptive Scanning: Yes)
Webroot Anti-Malware	Yes	Yes	Yes
McAfee Anti-Malware	Yes	Yes	Yes
Sophos Anti-Malware	N/A	Yes	Yes
End-User Acknowledgement	Yes	Yes	Yes
Cisco IronPort Data Security Filters	Yes	Yes	Yes
External DLP Servers	Yes	Yes	Yes
Credential Encryption	N/A	No	No
Identity Provider for SaaS	N/A	Yes	Yes

Edit Display Settings...

公開する機能をイネーブルにするには、次の手順を実行してください。

ステップ 1　イネーブルにする機能とディセーブルにする機能を確認します。「イネーブルにされている機能の比較」（P.8-10）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] > [Utilities] > [Security Services Display] を選択します。

ステップ 3　[Edit Settings] をクリックします。

[Edit Security Services Display] ページに、各 Configuration Master に表示される機能が一覧されます。

（注）　Web プロキシは機能として一覧されていません。これは、Web プロキシは Web セキュリティ アプライアンスで管理されているプロキシ タイプのいずれかを実行するためにイネーブルになっていると見なされているためです。Web プロキシをディセーブルにすると、Web セキュリティ アプライアンスに公開されたすべてのポリシーが無視されます。

ステップ 4　（任意）使用しない Configuration Master は非表示にします。意図しない影響が生じるのを避けるため、「使用しない Configuration Master のディセーブル化」（P.8-12）の「注」を参照してください。

ステップ 5　使用する各 Configuration Master について、イネーブルにする各機能に対する [Yes] チェックボックスを選択または選択解除します。

一部の機能について、次のような特別な注意事項があります（Configuration Master による）。

- トランスペアレント モード。フォワード モードを使用した場合、プロキシ バイパス機能は使用できなくなります。
- HTTPS プロキシ。HTTPS プロキシは、復号ポリシーを実行するためにイネーブルにする必要があります。
- アップストリーム プロキシ グループ。ルーティング ポリシーを使用する場合は、Web セキュリティ アプライアンスでアップストリーム プロキシ グループが使用できるようになっている必要があります。
- 許容範囲内の使用制御。使用するサービス（[Cisco IronPort URL Filters] または [Cisco IronPort Web Usage Controls]）を選択し、[Application Visibility and Control] をイネーブルにするかどうかを選択します。
- AnyConnect セキュア モビリティ。[IP Range] または [Cisco ASA] を選択します。
- Web レピュテーション フィルタリング。Adaptive Scanning をイネーブルにするかどうかを指定します。

ステップ 6　使用する各 Configuration Master に対して変更を加えます。

ステップ 7　[Submit] をクリックします。セキュリティ サービスの設定に加えた変更が、Web セキュリティ アプライアンスで設定されたポリシーに影響する場合、GUI に特定の警告メッセージが表示されます。変更を送信することが確実な場合は、[Continue] をクリックします。

ステップ 8　[Security Services Display] ページで、選択した各オプションの横に [Yes] と表示されることを確認します。

ステップ 9　変更を保存します。

ステップ 10　公開先のアプライアンスに対して、すべての機能が正しくイネーブルまたはディセーブルになっていることを確認します。「イネーブルにされている機能の比較」（P.8-10）を参照してください。

使用しない Configuration Master のディセーブル化

使用しない Configuration Master を表示しないようにすることができます。

たとえば、一部の Configuration Master をディセーブルにしたとき、[Configuration Master] タブと [Security Services Display] ページは次のように表示されます。

Security Services Display

Configuration Master Settings for Display of Security Services

Features	Configuration Masters		
	6.3 (disabled)	7.1 (disabled)	7.5
Transparent mode	Yes	Yes	Yes
FTP Proxy	Yes	Yes	Yes
HTTPS Proxy	Yes	Yes	Yes
Upstream Proxy Groups	Yes	Yes	Yes
Acceptable Use Controls	Cisco IronPort Web Usage Controls	Cisco IronPort Web Usage Controls (with Application Visibility and Control)	Cisco IronPort Web Usage Controls (with Application Visibility and Control)
AnyConnect Secure Mobility	N/A	IP Range	IP Range
Web Reputation Filters	Yes	Yes	Yes (Adaptive Scanning: Yes)
Webroot Anti-Malware	Yes	Yes	Yes
McAfee Anti-Malware	Yes	Yes	Yes
Sophos Anti-Malware	N/A	Yes	Yes
End-User Acknowledgement	Yes	Yes	Yes
Cisco IronPort Data Security Filters	Yes	Yes	Yes
External DLP Servers	Yes	Yes	Yes
Credential Encryption	N/A	No	No
Identity Provider for SaaS	N/A	Yes	Yes

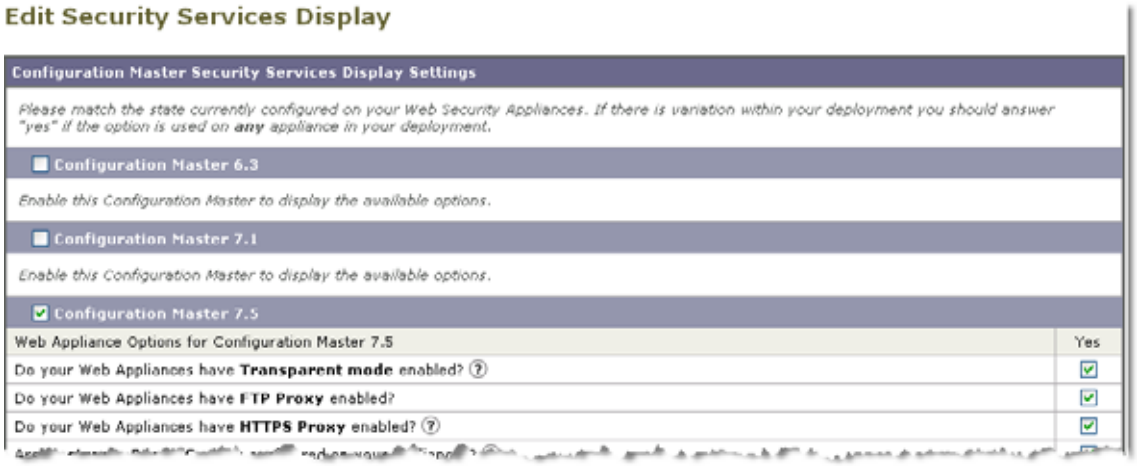
Edit Display Settings...

（注） Configuration Master をディセーブルにすると、それに対するすべての参照が、対応する [Configuration Master] タブを含めて GUI から削除されます。その Configuration Master を使用する保留中の公開ジョブは削除され、非表示の Configuration Master に割り当てられていたすべての Web セキュリティ アプライアンスが、割り当てられていないものとして再分類されます。少なくとも 1 つの Configuration Master をイネーブルにする必要があります。

ステップ 1　セキュリティ管理アプライアンスで、[Web] > [Utilities] > [Security Services Display] を選択します。

ステップ 2　[Edit Settings] をクリックします。

ステップ 3　使用しない Configuration Master に対するチェックボックスを選択解除します。



ステップ 4　変更を送信し、保存します。

拡張ファイル公開を使用するための設定

システムで Configuration Master を使用するよう設定されている場合は、拡張ファイル公開に対する設定も行われています。

そうでない場合は、次の項で説明する手順を実行してください。これらは、拡張ファイル公開だけでなく、Configuration Master の公開にも適用されます。

- 「セキュリティ管理アプライアンスでの中央集中型コンフィギュレーション管理のイネーブル化」（P.8-4）
- 「Configuration Master の初期化」（P.8-4）
- 「Web セキュリティ アプライアンスと Configuration Master の関連付けについて」（P.8-5）

Web セキュリティ アプライアンスへの設定の公開

- 「Configuration Master の公開」（P.8-14）
- 「拡張ファイル公開による設定の公開」（P.8-18）

Configuration Master の公開

Configuration Master で設定を編集またはインポートした後、その設定を、Configuration Master に関連付けられている Web セキュリティ アプライアンスへ公開できます。

- 「Configuration Master を公開する前に」（P.8-15）
- 「Configuration Master の公開」（P.8-16）
- 「Configuration Master を後日公開」（P.8-16）
- 「コマンドライン インターフェイスによる Configuration Master の公開」（P.8-17）

Configuration Master を公開する前に

Configuration Master を公開すると、その Configuration Master に関連付けられている Web セキュリティ アプライアンスの既存のポリシー情報が上書きされます。

Configuration Master を使用して設定できる設定の詳細については、「適切な設定公開方式の決定」（P.8-1）を参照してください。

Configuration Master を公開する前に、次のことを確認します。

- 対象となる Web セキュリティ アプライアンスの AsyncOS のバージョンが、Configuration Master のバージョンと同じかそれより新しいものである必要があります。具体的な要件については、「SMA 互換性マトリクス」（P.2-2）を参照してください。AsyncOS 7.5 を実行している Web セキュリティ アプライアンスに対して公開するには、Configuration Master 7.5 を使用することを強く推奨します。
- （初回のみ）「Configuration Master を使用するための設定」（P.8-2）で説明する手順に従います。
- 対象とする各 Web セキュリティ アプライアンスからコンフィギュレーション ファイルを保存して、公開された設定によって問題が生じた場合に既存の設定を復元できるようにします。詳細については、『*Cisco IronPort AsyncOS for Web Security User Guide*』を参照してください。
- Configuration Master が公開を実施し、公開後に意図する機能がイネーブルになるようにするには、各 Web セキュリティ アプライアンスと、これに対応する Configuration Master の機能を確認し、必要に応じて変更を加えます。「イネーブルにされている機能の比較」（P.8-10）、および必要に応じて「公開する機能のイネーブル化」（P.8-11）を参照してください。

  同じ Configuration Master に割り当てられている複数の Web セキュリティ アプライアンスで異なる機能がイネーブルになっている場合は、各アプライアンスを別個に公開するようにし、それぞれの公開前に機能がイネーブルになっていることを確認する必要があります。
- 対象の Web セキュリティ アプライアンスで AsyncOS を復元した場合は、そのアプライアンスを異なる Configuration Master と関連付けなければならない場合があります。
- Configuration Master を、トランスペアレント ユーザ ID がイネーブルになったレルムを持たない Web セキュリティ アプライアンスに公開したものの、[Identity] または [SaaS Policy] で [Transparent User Identification] を選択していると、次のようになります。
  - [Identity] の場合、[Transparent User Identification] はディセーブルになり、代わりに [Require Authentication] オプションが選択されます。
  - [SaaS Policy] の場合、[Transparent User Identification] オプションはディセーブルになり、代わりにデフォルトのオプション（SaaS ユーザに対して常にプロキシ認証を要求）が選択されます。
- Web セキュリティ アプライアンスでコミットしたときに Web プロキシの再起動が必要になる変更内容は、それを セキュリティ管理アプライアンスから公開したときにもプロキシの再起動が必要になります。この場合は、警告が発生します。

  プロキシの再起動が必要な変更を Web セキュリティ アプライアンスで行うと、公開時にもプロキシの再起動が発生することがあります。たとえば、Web セキュリティ アプライアンスで新しいグループをアクセス ポリシーのグループ認証設定に追加すると、次に Configuration Master が公開されるときに Web プロキシが再起動します。このような場合は、プロキシの再起動に関する警告は発生しません。

  Web プロキシの再起動により、Web セキュリティ サービスは一時的に中断されます。Web プロキシの再起動による影響の詳細については、『*Cisco IronPort AsyncOS 7.5 for Web Security User Guide*』の「Checking for Web Proxy Restart on Commit」を参照してください。
- ID に対する変更を公開すると、すべてのエンド ユーザが再認証を受ける必要が生じます。

（注）　セキュリティ管理アプライアンスから、RSA サーバ用に設定されていない複数の Web セキュリティ アプライアンスに、外部 DLP ポリシーを公開しても問題ありません。公開しようとすると、セキュリティ管理アプライアンスから、次の公開ステータス警告が送信されます。「**The Security Services display settings configured for Configuration Master 7.1 do not currently reflect the state of one or more Security Services on Web Appliances associated with this publish request.The affected appliances are: "[***WSA Appliance Name***]".This may indicate a misconfiguration of the Security Services display settings for this particular Configuration Master.Go to the Web Appliance Status page for each appliance provides a detailed view to troubleshooting this issue.Do you want to continue publishing the configuration now?**」
公開を続行した場合、RSA サーバ用に設定されていない Web セキュリティ アプライアンスは、外部 DLP ポリシーを受信しますが、これらのポリシーはディセーブルにされます。外部 DLP サーバが設定されていない場合、Web セキュリティ アプライアンスの [External DLP] ページには公開されたポリシーが表示されません。

Configuration Master の公開

ステップ 1　「Configuration Master を公開する前に」（P.8-15）の重要な要件と情報を参照してください。

ステップ 2　セキュリティ管理アプライアンスで、[Web] > [Utilities] > [Publish to Web Appliances] を選択します。

ステップ 3　[Publish Configuration Now] をクリックします。

ステップ 4　デフォルトでは [System-generated job name] が選択されています。あるいは、ユーザ定義のジョブ名（80 文字以下）を入力します。

ステップ 5　公開する Configuration Master を選択します。

ステップ 6　Configuration Master の公開先となる Web セキュリティ アプライアンスを選択します。Configuration Master に割り当てられているすべてのアプライアンスに設定を公開するには、[All assigned appliances] を選択します。

または

[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　[Publish] をクリックします。

[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] > [Utilities] > [Publish to Web Appliances] ページにも表示されます。[Publish in Progress] にアクセスするには、[Check Progress] をクリックします。

ステップ 8　公開が正しく完了したことを確認します。「公開履歴の表示」（P.8-19）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

ステップ 1　「Configuration Master を公開する前に」（P.8-15）の重要な要件と情報を参照してください。

ステップ 2　セキュリティ管理アプライアンスで、[Web] > [Utilities] > [Publish to Web Appliances] を選択します。

ステップ 3　[Schedule a Job] をクリックします。

ステップ 4　デフォルトでは [System-generated job name] が選択されています。あるいは、ユーザ定義のジョブ名（80 文字以下）を入力します。

ステップ 5　Configuration Master を公開する日時を入力します。

ステップ 6　公開する Configuration Master を選択します。

ステップ 7　Configuration Master の公開先となる Web セキュリティ アプライアンスを選択します。Configuration Master に割り当てられているすべてのアプライアンスに設定を公開するには、[All assigned appliances] を選択します。

または

[Select appliances in list] を選択して、Configuration Master に割り当てられているアプライアンスの一覧を表示します。設定の公開先となるアプライアンスを選択します。

ステップ 8　[Submit] をクリックします。

ステップ 9　スケジュールされているジョブのリストは、[Web] > [Utilities] > [Publish to Web Appliances] ページに表示されます。スケジュールされているジョブを編集するには、そのジョブの名前をクリックします。保留中のジョブをキャンセルするには、対応するごみ箱アイコンをクリックして、ジョブの削除を確認します。

ステップ 10　公開が正しく完了したことを確認するために、自分自身に対する覚え書きを（カレンダーなどに）作成することもできます。「公開履歴の表示」（P.8-19）を参照してください。完全に公開されなかった項目が表示されます。

（注）　スケジュールされた公開ジョブが発生する前に、アプライアンスをリブートまたはアップグレードした場合は、ジョブを再度スケジュールする必要があります。

コマンドライン インターフェイスによる Configuration Master の公開

（注）　「Configuration Master を公開する前に」（P.8-15）の重要な要件と情報を参照してください。

セキュリティ管理アプライアンスでは、次の CLI コマンドを使用して Configuration Master から変更を公開できます。

publishconfig config_master [*--job_name*] [*--host_list* | *host_ip*]

ここで、**config_master** は 6.3、7.1、または 7.5 になります。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] > [Utilities] > [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] > [Utilities] > [Publish] > [Publish History] により、[Publish History] ページに進むことができます。

拡張ファイル公開による設定の公開

拡張ファイル公開を使用して、互換性のある XML コンフィギュレーション ファイルを、ローカル ファイル システムから管理対象の Web セキュリティ アプライアンスにプッシュします。

拡張ファイル公開を使用して設定できる設定の詳細については、「適切な設定公開方式の決定」（P.8-1）を参照してください。

（注） Web セキュリティ アプライアンスでコミットしたときに Web プロキシの再起動が必要になる変更内容は、それを セキュリティ管理アプライアンスから公開したときにもプロキシの再起動が必要になります。拡張ファイル公開を使用するときには、プロキシの再起動に関する警告が発生します。

Web プロキシの再起動により、Web セキュリティ サービスは一時的に中断されます。Web プロキシの再起動による影響の詳細については、『*Cisco IronPort AsyncOS 7.5 for Web Security User Guide*』の「Checking for Web Proxy Restart on Commit」を参照してください。

拡張ファイル公開を実行するには、次のいずれかを選択します。

- 「拡張ファイル公開：[Publish Configuration Now]」（P.8-18）
- 「拡張ファイル公開：[Publish Later]」（P.8-18）

拡張ファイル公開：[Publish Configuration Now]

ステップ 1　元となる Web セキュリティ アプライアンスから、コンフィギュレーション ファイルを保存します。

ファイルの互換性については、「SMA 互換性マトリクス」（P.2-2）を参照してください。

Web セキュリティ アプライアンスからコンフィギュレーション ファイルを保存する方法については、『*Cisco IronPort AsyncOS for Web Security User Guide*』を参照してください。

ステップ 2　各宛先の Web セキュリティ アプライアンスにおいて、Web セキュリティ アプライアンスの既存の設定をコンフィギュレーション ファイルに保存します。詳細については、『*Cisco IronPort AsyncOS for Web Security User Guide*』を参照してください。

ステップ 3　セキュリティ管理アプライアンスのメイン ウィンドウで、[Web] > [Utilities] > [Publish to Web Appliances] を選択します。

ステップ 4　[Publish Configuration Now] をクリックします。

ステップ 5　デフォルトでは [System-generated job name] が選択されています。あるいはジョブ名（80 文字まで）を入力します。

ステップ 6　[Configuration Master to Publish] で、[Advanced file options] を選択します。

ステップ 7　[Browse] をクリックして、ステップ 1 で保存したファイルを選択します。

ステップ 8　[Web Appliances] ドロップダウン リストから、[Select appliances in list] または [All assigned to Master] を選択して、コンフィギュレーション ファイルの公開先となるアプライアンスを選択します。

ステップ 9　[Publish] をクリックします。

拡張ファイル公開：[Publish Later]

ステップ 1　元となる Web セキュリティ アプライアンスから、コンフィギュレーション ファイルを保存します。

ファイルの互換性については、「SMA 互換性マトリクス」（P.2-2）を参照してください。

Web セキュリティ アプライアンスからコンフィギュレーション ファイルを保存する方法については、『*Cisco IronPort AsyncOS for Web Security User Guide*』を参照してください。

ステップ 2　各宛先の Web セキュリティ アプライアンスにおいて、Web セキュリティ アプライアンスの既存の設定をコンフィギュレーション ファイルに保存します。詳細については、『*Cisco IronPort AsyncOS for Web Security User Guide*』を参照してください。

ステップ 3　セキュリティ管理アプライアンスのメイン ウィンドウで、[Web] > [Utilities] > [Publish to Web Appliances] を選択します。

ステップ 4　[Schedule a Job] をクリックします。

ステップ 5　デフォルトでは [System-generated job name] が選択されています。あるいはジョブ名（80 文字まで）を入力します。

ステップ 6　設定を公開する日時を入力します。

ステップ 7　[Configuration Master to Publish] で、[Advanced file options] を選択し、次に [Browse] をクリックして、ステップ 1 で保存したコンフィギュレーション ファイルを選択します。

ステップ 8　[Web Appliances] ドロップダウン リストから、[Select appliances in list] または [All assigned to Master] を選択して、コンフィギュレーション ファイルの公開先となるアプライアンスを選択します。

ステップ 9　[Publish] をクリックします。

公開ジョブのステータスと履歴の表示

スケジュール設定された公開ジョブの表示

スケジュール設定されているものの、まだ実行されていない公開ジョブの一覧を確認するには、[Web] > [Utilities] > [Publish to Web Appliances] を選択して、[Pending Jobs] セクションを確認します。

現在の公開ジョブのステータスの表示

現在進行中の公開ジョブのステータスを確認するには、[Web] > [Utilities] > [Publish to Web Appliances] を選択して、[Publishing Progress] セクションを確認します。

公開履歴の表示

公開履歴を表示すると、公開中に発生した可能性のあるエラーのチェックに役立ちます。

ステップ 1　セキュリティ管理アプライアンスで、[Web] > [Utilities] > [Publish History] を選択します。

[Publish History] ページには、試行された最近のすべての公開ジョブがリストされます。カラム情報には、ジョブ名、ジョブ完了時刻、使用された Configuration Master（または、拡張ファイル公開を実行した場合は XML コンフィギュレーション ファイルの名前）、ジョブの公開先にしたアプライアンスの数、およびステータス（[Success] または [Failure]）があります。

ステップ 2　特定のジョブに関してさらに詳細を表示するには、[Job Name] カラムで特定のジョブ名のハイパーテキスト リンクをクリックします。

ステップ 3　[Publish History: Job Details] ページでは、アプライアンス名をクリックすることにより、[Web] > [Utilities] > [Web Appliance Status] ページを表示して、ジョブの特定のアプライアンスに関する追加の詳細を表示できます。ジョブの特定のアプライアンスに関するステータスの詳細を表示することもでき、対応する [Details] リンクをクリックして [Web Appliance Publish Details] ページに詳細を表示します。

[Web Appliance Status] ページの [Web Appliance Service] カラムのステータスと、[Is Service Displayed on Management Appliance?] カラムのステータスに不一致があると、公開処理が失敗します。両方のカラムで、機能がイネーブルになっているものの、対応する機能キーがアクティブになっていない場合（期限切れなど）にも、公開処理が失敗します。

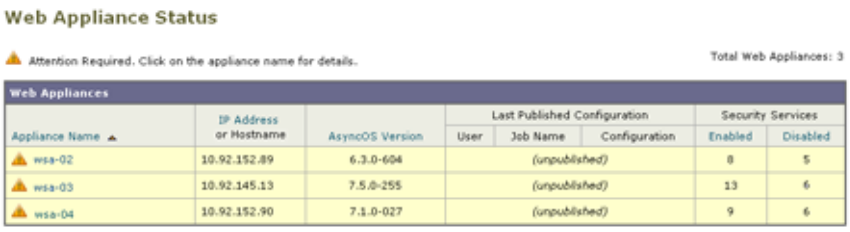
Web セキュリティ アプライアンスのステータスの表示

AsyncOS には、2 つの Web セキュリティ アプライアンス ステータス レポートがあります。1 つは セキュリティ管理アプライアンスに接続された Web セキュリティ アプライアンスの概略サマリーを示すもので、もう 1 つは接続された各 Web セキュリティ アプライアンスのステータスの詳細ビューです。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、機能キーのステータスなどがあります。

（注）　セキュリティ管理アプライアンスに追加するすべての Web アプライアンスは、[Web] > [Utilities] > [Web Appliance Status] ページにエントリが表示されます。ただし、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。管理がサポートされているバージョンは、AsyncOS 6.0 を除く、AsyncOS 5.7 以降のすべてのバージョンの Web セキュリティ アプライアンスです。したがって、AsyncOS 5.7、6.3、7.1、7.5 を実行しているすべてのアプライアンスに表示するデータがあることになります。

ステップ 1　セキュリティ管理アプライアンスで、[Web] > [Utilities] > [Web Appliances Status] を選択します。

図 8-2　[Web Appliances Status] ページ



（注）　Web セキュリティ アプライアンスの Acceptable Use Control Engine の各種バージョンが、セキュリティ管理アプライアンスのバージョンと一致しない場合は、警告メッセージが表示されます。そのサービスが Web セキュリティ アプライアンスでディセーブルになっているか、そこに存在しない場合は、[N/A] と表示されます。

[Web Appliance Status] ページには、接続されている Web セキュリティ アプライアンスのリストが、アプライアンス名、IP アドレス、AsyncOS バージョン、最後に公開された設定情報（ユーザ、ジョブ名、コンフィギュレーション バージョン）、使用可能または使用不可にされているセキュリティ サービスの数、および接続しているアプライアンスの総数（最大 150）とともに表示されます。警告アイコンは、接続されたアプライアンスの 1 つに注意が必要なことを示しています。

（注） Web セキュリティ アプライアンスで発生した最新の設定変更が [Web Appliance Status] ページに反映されるまでに、数分かかることがあります。データをすぐに更新するには、[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。

ステップ 2　アプライアンスの名前をクリックします。

そのアプライアンスの [Appliance Status] ページが表示されます。このページには、次のセクションがあります。

- 「[Web Appliance Status Details] ページ：システム ステータス、設定の公開履歴、および中央集中型レポーティングのステータス」
- 「[Web Appliance Status Details] ページ：セキュリティ サービス セクション」
- 「[Web Appliance Status Details] ページ：AnyConnect セキュア モビリティ、プロキシ、および認証の設定」

図 8-3　[Web Appliance Status Details] ページ：システム ステータス、設定の公開履歴、および中央集中型レポーティングのステータス

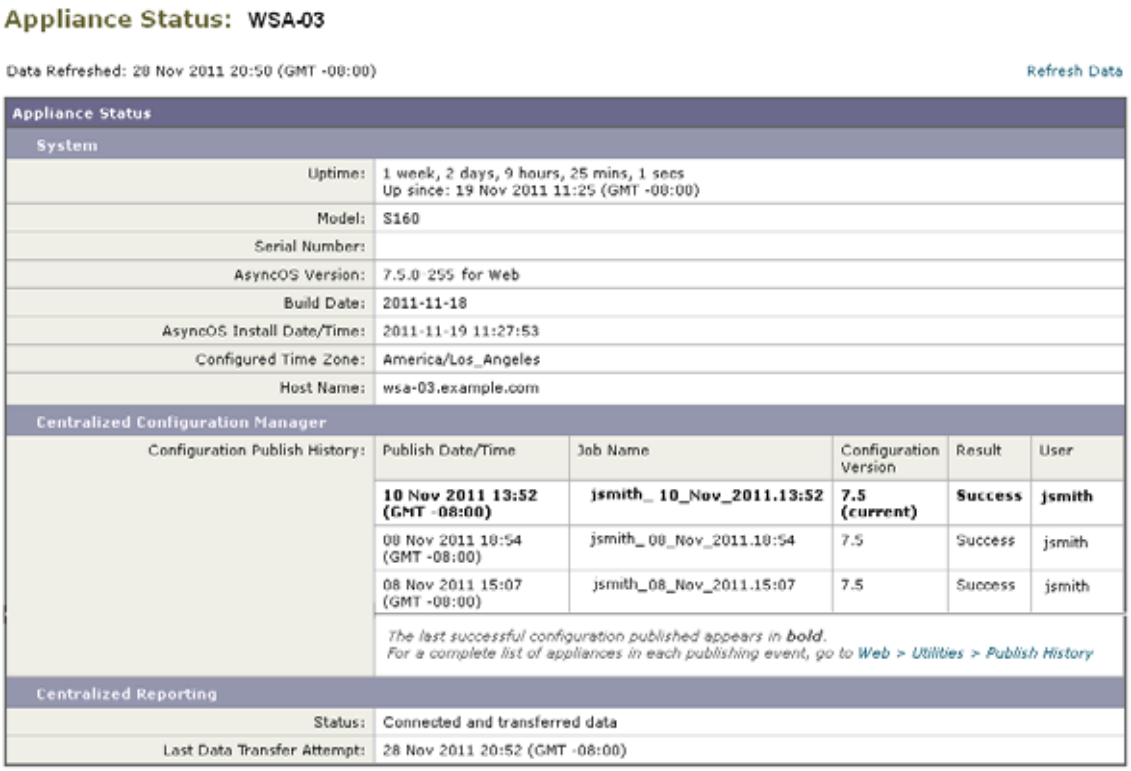


図 8-4　[Web Appliance Status Details] ページ：セキュリティ サービス セクション

Security Services

Description	Services		Feature Keys		
	Web Appliance Service	Is Service Displayed on Management Appliance?	Status	Time Remaining	Expiration Date
Cisco IronPort Web Proxy & DVS(TM) Engine	Enabled	Yes	Active	30 days	Thu 29 Dec 2011
Cisco IronPort L4 Traffic Monitor	N/A	N/A	N/A	N/A	N/A
Proxy Mode	Forward	No (Bypass Proxy)			
FTP Proxy	Enabled	Yes			
Cisco IronPort HTTPS Proxy	Enabled	Yes	Active	30 days	Thu 29 Dec 2011
Upstream Proxy Groups	Not Configured	No (Routing Policies)			
AnyConnect Secure Mobility	Cisco ASA	Yes (Cisco ASA)	Active	30 days	Thu 29 Dec 2011
Cisco IronPort URL Filtering	Disabled	No	Active	30 days	Thu 29 Dec 2011
Cisco IronPort Web Usage Controls	Enabled	Yes	Active	30 days	Thu 29 Dec 2011
Application Visibility and Control	Enabled	Yes			
Cisco IronPort Centralized Web Reporting	Enabled	Yes			
Cisco IronPort Web Reputation Filters	Enabled	Yes	Active	30 days	Thu 29 Dec 2011
Adaptive Scanning	Disabled	No			
Webroot Anti-Malware	Enabled	Yes	Active	30 days	Thu 29 Dec 2011
McAfee Anti-Malware	Enabled	Yes	Active	30 days	Thu 29 Dec 2011
Sophos Antivirus	Enabled	Yes	Active	30 days	Thu 29 Dec 2011
End-User Acknowledgement	Enabled	Yes			
Cisco IronPort Data Security Filters	Enabled	Yes			
External DLP Servers	Not Configured	No			
Credential Encryption	Disabled	No			
Identity Provider for SaaS	Not Configured	No			

Acceptable Use Controls Engine Updates

Update Type	Web Appliance Version	Management Appliance Version
Web Categorization Categories List	1320090990	N/A
Application Visibility and Control Data	1319743829	N/A

図 8-5　[Web Appliance Status Details] ページ：
AnyConnect セキュア モビリティ、プロキシ、および認証の設定

AnyConnect Secure Mobility Settings

Cisco ASA:	[IP address and port go here]

Proxy Settings

Upstream Proxies:	*No upstream proxies configured.*
HTTP Ports to Proxy:	[Port goes here]

Authentication Service

Authentication Realms:	Name	Protocol	Servers	Support Transparent User Identification
	NTLM AUTH	NTLM	ad.example.com	No
	LDAP AUTH	LDAP	ad.example.com	No
Authentication Sequences:	Name		Order of Realms	
	All Realms		NTLMSSP: NTLM AUTH Basic: NTLM AUTH, LDAP AUTH	
Unreachable Authentication Service Action:	Block all traffic if authentication fails			

詳細には次の情報が含まれます。

- セキュリティ ステータス情報（稼働時間、アプライアンス モデル、シリアル番号、AsyncOS のバージョン、ビルド日、AsyncOS のインストール日時、ホスト名）
- 設定公開履歴（公開日時、ジョブ名、コンフィギュレーション バージョン、公開の結果、ユーザ）

- 直近に試行されたデータ転送の時刻など、中央集中型レポーティングのステータス
- Web セキュリティ機能のステータス（機能説明、設定のサマリー、セキュリティ サービスの設定、機能キーのステータス）

  この情報は、使用するアプライアンスに中央集中型管理を設定する場合に使用します。
- 管理対象および管理側のアプライアンスの Acceptable Use Controls Engine のバージョン
- AnyConnect セキュア モビリティの設定
- プロキシ設定（アップストリーム プロキシとプロキシの HTTP ポート）
- 認証サービス（名前、プロトコル、認証レルムのサーバ、認証手順におけるレルムの名前と順序、トランスペアレント ユーザ ID のサポートの有無、認証に失敗した場合のトラフィックのブロックまたは許可）

ステップ 3　Web セキュリティ アプライアンスに変更を加えたときや、アプライアンスに対する情報を表示できないというメッセージが表示された場合に詳細をリフレッシュするには、[Refresh Data] リンクをクリックします。ページのタイム スタンプは、データが最後にリフレッシュされた時刻を示しています。

URL カテゴリ セットの更新と中央集中型コンフィギュレーション管理

URL カテゴリ セットの更新は、Configuration Master 7.5 に対してのみ適用されます。

システムで Web の使用率を管理するために事前定義されている URL カテゴリを最新の状態に維持するためには、Cisco IronPort Web Usage Controls（WUC）の URL カテゴリ セットを時折更新します。デフォルトでは、Web セキュリティ アプライアンスが URL カテゴリ セットを Cisco IronPort 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。更新された URL カテゴリ セットは、Configuration Master 7.5 の ID とアプライアンス ポリシーにただちに表示されます。

以下のことを実施してください。

- 「URL カテゴリ セットの更新による影響の理解」（P.8-23）
- 「URL カテゴリ セットの更新に関するアラートを受信」（P.8-24）
- 「Configuration Master 7.5 を設定する前の注意事項」（P.8-24）
- 「新規または変更されたカテゴリのデフォルト設定の指定」（P.8-24）
- 「URL カテゴリ セットの更新時にポリシーと ID の設定を確認」（P.8-24）

URL カテゴリ セットの更新による影響の理解

URL カテゴリ セットの更新の前後に実行する手順の重要な説明については、「ドキュメント セット」（P.1-4）のリンクに掲載されている、『*Cisco IronPort AsyncOS for Web Security User Guide*』の「Managing Updates to the Set of URL Categories」の章を参照してください。カテゴリについては、同じ章の「URL Category Descriptions」で説明されています。

URL カテゴリ セットの更新に関するアラートを受信

Configuration Master のポリシー設定に影響を及ぼす URL カテゴリ セットの更新について、アラートを受信するようにするには、[Management Appliance] > [System Administration] > [Alerts] を選択し、[System] カテゴリで警告レベルのアラートを受信するよう設定します。アラートについての詳細は、「アラートの管理」（P.13-34）を参照してください。

Configuration Master 7.5 を設定する前の注意事項

Configuration Master 7.1 の設定を Configuration Master 7.5 にコピーまたはインポートすると、URL カテゴリを参照するすべての ID およびポリシーが Configuration Master 7.5 で変更されます。この代わりとして、正しく設定された Web セキュリティ アプライアンスからコンフィギュレーション ファイルをインポートすることができます。また、コピーまたはインポートする前に Configuration Master 7.1 の各ポリシーについて未分類の URL 設定を評価することもできます。

新規または変更されたカテゴリのデフォルト設定の指定

将来、URL カテゴリ セットが更新されると、既存の Configuration Master 7.5 のポリシーの動作が変化する可能性があります。URL カテゴリ セットを更新する前に、URL フィルタリングを行うポリシーの新規カテゴリやマージされたカテゴリにデフォルトの動作を指定するか、これらがすでに設定されている Web セキュリティ アプライアンスから設定をインポートする必要があります。

詳細については、『*User Guide for Cisco IronPort AsyncOS for Web Security*』の「URL Filters」の章にある「Choosing Default Settings for New and Changed Categories」項、または Web セキュリティ アプライアンスのオンライン ヘルプを参照してください。

URL カテゴリ セットの更新時にポリシーと ID の設定を確認

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

- カテゴリの変更についてのアラート
- カテゴリの変更によって変更された、またはディセーブルにされたポリシーについてのアラート

URL カテゴリ セットの変更に関するアラートを受信した場合は、Configuration Master 7.5 で既存の URL カテゴリに基づくポリシーと ID を確認して、それらが引き続きポリシーの目的を満たしていることを確認してください。

注意が必要な変更の詳細については、「ドキュメント セット」（P.1-4）のリンクに掲載されている、『*Cisco IronPort AsyncOS 7.5 for Web Security User Guide*』の「Responding to Alerts about URL Category Set Updates」を参照してください。

CHAPTER 9

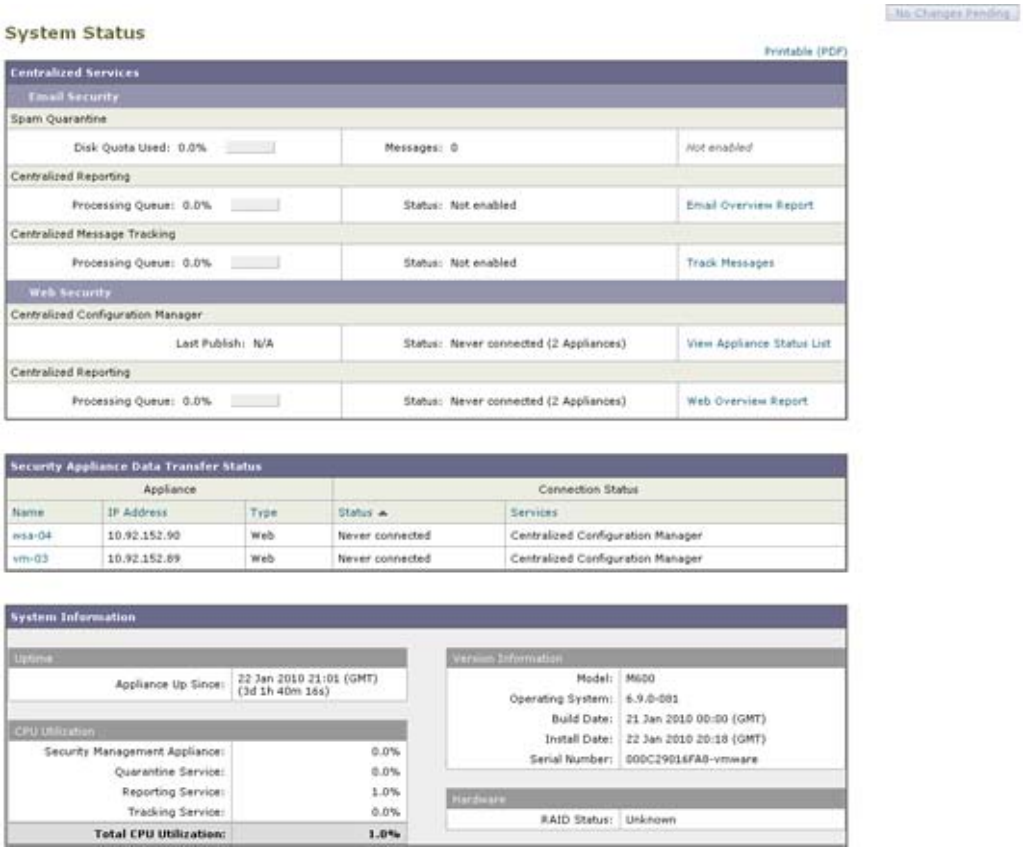
システム ステータスのモニタリング

セキュリティ管理アプライアンスのモニタリング

デフォルトで、[System Status] ページは、セキュリティ管理アプライアンスの GUI にアクセスするときに表示される最初のページです。（ランディング ページを変更するには、「プリファレンスの 設定」（P.13-60）を参照してください）

GUI から [System Status] ページにアクセスするには、[Management Appliance] > [Centralized Services] > [System Status] を選択します。

図 9-1　[System Status] ページ



サービスのモニタリングをイネーブルにして、管理対象アプライアンスを追加するまでは、[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、サービスのモニタリングをイネーブルにして、管理対象アプライアンスを追加すると、[Services] セクションおよび [Security Appliance Data Transfer Status] セクションにデータが表示されます。管理対象アプライアンスの追加、サービスのイネーブル化、および両方のステータスの表示の詳細については、「管理対象アプライアンスの追加について」（P.2-16）、「セキュリティ管理アプライアンスでのサービスの設定」（P.2-17）、および「管理対象アプライアンスのステータスの表示」（P.9-6）を参照してください。

一般に、[System Status] ページには、次のようなセキュリティ管理アプライアンスの詳細なステータス情報が表示されます。

- **システム ステータス：**サービスの概要（Cisco IronPort スパム隔離、中央集中型レポーティング、中央集中型トラッキング、および中央集中型コンフィギュレーション マネージャ）
- **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 バージョン、インストール日、およびシリアル番号

Centralized Services

[Centralized Services] セクションには、セキュリティ管理アプライアンスのサービスの概要が表示されます。

メインのセキュリティ管理アプライアンスで、[Management Appliance] > [Centralized Services] > [System Status] を選択して、管理対象 電子メール セキュリティ アプライアンス、Web セキュリティ アプライアンス、およびセキュリティ管理アプライアンスの間で行われるレポーティング データの転送に関する概要情報を表示します。

[Centralized Services] > [System Status] の下に、2 つのセクションがあります。

- Email Security
- Web Security

Email Security

[Email Security] セクションは、電子メール セキュリティ アプライアンスの情報にのみ関連しています。[Email Security] セクションには、次の情報が表示されます。

- [Spam Quarantine] : このセクションには、Cisco IronPort スパム隔離で保持されているメッセージの数、および隔離が使用しているディスク クォータの割合が表示されます。[Spam Quarantine View] リンクをクリックすると、[Spam Quarantine] ページにアクセスできます。Cisco IronPort スパム隔離の詳細については、第 7 章「Cisco IronPort スパム隔離の管理」を参照してください。
- [Centralized Reporting] : このセクションには、処理キューの情報が表示され、レポーティング データによって使用されている処理キューの割合が表示されます。

  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 電子メール セキュリティ 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。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。

（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。

  [Email Overview Report] リンクをクリックすると、[Overview interactive report] ページにアクセスできます。[Overview report] ページの詳細については、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」の電子メール レポーティングの [Overview] ページを参照してください。
- [Centralized Message Tracking] : このセクションには、管理対象 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行われるトラッキング データの転送に関する概要情報が表示されます。[Processing Queue] フィールドに、トラッキング データによって利用される処理キューの割合が表示されます。[Track Messages] リンクをクリックすると、[Message Tracking query] ページにアクセスできます。トラッキング メッセージの詳細については、第 6 章「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。

Web Security

[Web Security] セクションは、Web セキュリティ アプライアンスの情報にのみ関連しています。[Web Security] セクションには、次の情報が表示されます。

- [Centralized Reporting] : このセクションには、処理キューの情報が表示され、レポーティング データによって使用されている処理キューの割合が表示されます。

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 Web セキュリティ 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。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。

（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。

[Web Overview Report] リンクをクリックすると、[Overview interactive report] ページにアクセスできます。[Overview report] ページの詳細については、第 5 章「中央集中型 Web レポーティングの使用方法」の Web レポーティング ページについてを参照してください。

- [Centralized Configuration Manager] : このセクションには、最後に成功した Web セキュリティ アプライアンスの設定更新に関する概要情報が表示されます。インタラクティブ リンクをクリックして、システムで正常に公開された最新アップデートに移動できます。[View Appliance Status List] をクリックして、セキュリティ管理アプライアンス上の個々のアプライアンスのステータスを表示します。システム上のアプライアンスの現在のステータスの詳細については、「管理対象アプライアンスのステータスの表示」（P.9-6）を参照してください。

Security Appliance Data Transfer Status

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。[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、[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、[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）　[System Status] ページの [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。[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。

[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。詳細については、アプライアンス名をクリックして、そのアプライアンスの [Data Transfer Status] ページを表示します。

図 9-2　[Data Transfer Status: <Appliance_Name>] ページ

Data Transfer Status: esa01

Printable (PDF)

Security Appliance Data Transfer Status		
	Last Data Transfer Attempt	
Service	Status	Time
Configuration Manager	Not enabled	N/A
Reporting	Never connected	N/A
Tracking	Never connected	N/A
ISQ Safelist/Blocklist	Never connected	N/A

[Data Transfer Status: *Appliance_Name*] 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。

- [Not enabled] : モニタリング サービスが 電子メール セキュリティ アプライアンスでイネーブルになっていません。
- [Never connected] : モニタリング サービスは 電子メール セキュリティ アプライアンスでイネーブルになっていますが、電子メール セキュリティ アプライアンスと セキュリティ管理アプライアンスの間で接続が確立されていません。
- [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。
- [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。
- [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。

- [Not enabled] : 中央集中型コンフィギュレーション マネージャは、Web セキュリティ アプライアンスでイネーブルになっていません。
- [Never connected] : 中央集中型コンフィギュレーション マネージャは Web セキュリティ アプライアンスでイネーブルになっていますが、Web セキュリティ アプライアンスと セキュリティ管理アプライアンスの間で接続が確立されていません。
- [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。
- [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。
- [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。
- [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。
- [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 [Never connected] および [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 [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。

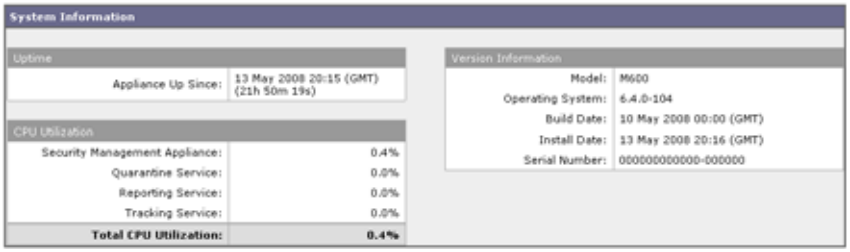
アプライアンスに [File transfer failure] ステータスが表示された場合は、そのアプライアンスをモニタして、その失敗がネットワークの問題によるものなのか、アプライアンスの設定の問題によるものなのかを判断します。データを転送できない理由がネットワークの問題ではなく、ステータスが [Connected and transferred data] に変化しない場合、データ転送ができるようにアプライアンスの設定を変更する必要があります。

System Information

[System Status] ページの [System Information] セクションには、セキュリティ管理アプライアンスのオペレーティング システムおよびパフォーマンスに関する情報が表示されます。[Uptime] フィールドには、アプライアンスが最後に起動された時刻と、実行を継続している時間が表示されます。[Version Information] 領域には、モデル番号、AsyncOS のバージョン、オペレーティング システムのビルドおよびインストール日付、アプライアンスのシリアル番号がリスト表示されます。

（注）　Cisco IronPort カスタマー サポートにトラブルシューティングを依頼するときに、アプライアンスのシリアル番号が必要になることがあります。

図 9-3　　[System Status] ページの [System Information] セクション



[CPU Utilization] の割合は、セキュリティ管理アプライアンスのモニタリング サービスそれぞれに使われる CPU 処理の割合を示します。割合は、主要な 3 つのサービスによって使用されている現在の CPU 量を示します。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 [Security Management appliance] の下にまとめられます。

CPU 使用率の割合は、常に変化します。最新のデータを表示するには、ブラウザを更新します。

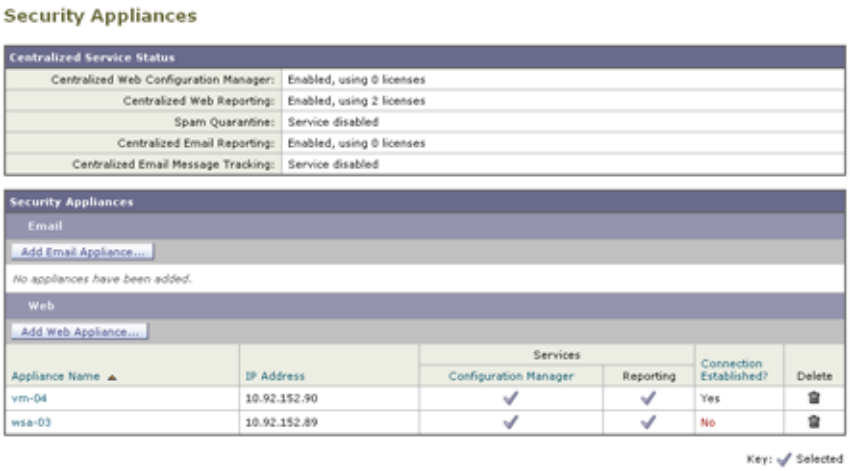
管理対象アプライアンスのステータスの表示

[Security Appliances] ページに、管理対象アプライアンスのステータスに関する情報が表示されます。

[Security Appliances] ページにアクセスするには、次の手順を実行します。

セキュリティ管理アプライアンスで、[Management Appliance] > [Centralized Services] > [Security Appliances] を選択します。

図 9-4　[Security Appliances] ページ



[Centralized Service Status] セクションに、イネーブル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。[Security Appliances] セクションには、追加したアプライアンスがリスト表示されます。チェック マークは、イネーブルになっているサービスを示し、[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。アプライアンスを追加または削除することもできます。詳細については、「管理対象アプライアンスの追加について」（P.2-16）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 アプライアンスのデータ アベイラビリティのモニタリング」（P.9-7）
- 「Web セキュリティ アプライアンスのデータ アベイラビリティのモニタリング」（P.9-8）

電子メール セキュリティ アプライアンスのデータ アベイラビリティのモニタリング

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 セキュリティ管理アプライアンスでモニタするには、次の手順を実行します。

ステップ 1　セキュリティ管理アプライアンスで、[Email] > [Reporting] > [Reporting Data Availability] を選択します。

図 9-5　[Reporting Data Availability] ページ

[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。

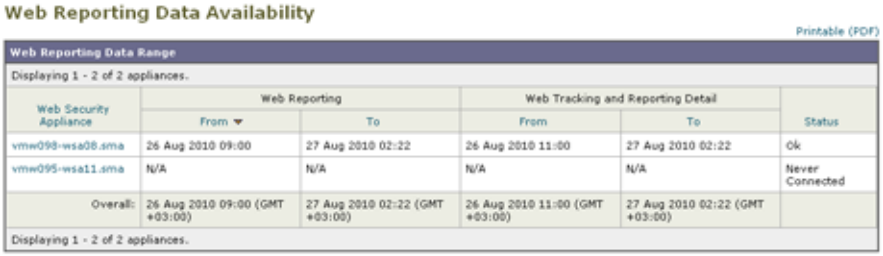
（注）　ハードウェア障害または他の理由で、電子メール セキュリティ アプライアンスの交換が必要になった場合、置き換えられた電子メール セキュリティ アプライアンスからのデータは失われませんが、そのデータはセキュリティ管理アプライアンスで正常に表示されません。

Web セキュリティ アプライアンスのデータ アベイラビリティのモニタリング

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 セキュリティ管理アプライアンスでモニタするには、次の手順を実行します。

ステップ 1　セキュリティ管理アプライアンスで、[Web] > [Reporting] > [Data Availability] を選択します。

[Data Availability] ページからデータの更新およびソートができ、リソース使用率および Web トラフィックの問題箇所をリアルタイムに表示できます。


Web Reporting Data Availability

Printable (PDF)

Web Reporting Data Range

Displaying 1 - 2 of 2 appliances.

Web Security Appliance	Web Reporting		Web Tracking and Reporting Detail		Status
	From	To	From	To	
vmw098-wsa08.sma	26 Aug 2010 09:00	27 Aug 2010 02:22	26 Aug 2010 11:00	27 Aug 2010 02:22	Ok
vmw095-wsa11.sma	N/A	N/A	N/A	N/A	Never Connected
Overall:	26 Aug 2010 09:00 (GMT +03:00)	27 Aug 2010 02:22 (GMT +03:00)	26 Aug 2010 11:00 (GMT +03:00)	27 Aug 2010 02:22 (GMT +03:00)	

Displaying 1 - 2 of 2 appliances.

（注）　[Web Reporting Data Availability] ウィンドウでは、Web Reporting と Email Reporting の**両方が**ディセーブルの場合にのみ、Web Reporting がディセーブルであると表示されます。

このページから、すべてのデータ リソース使用率および Web トラフィックの問題箇所を表示できます。リスト表示されている Web セキュリティ アプライアンス リンクのいずれかをクリックすると、そのアプライアンスのレポーティング データ アベイラビリティを表示できます。

レポーティング データ アベイラビリティは、前の日、週、年についてモニタできます。セキュリティ管理アプライアンスが Web セキュリティ アプライアンスから受信したレポーティング データが 100% 未満の場合は、データが不完全なことがすぐにわかります。データ アベイラビリティ情報を使用して、レポーティング データの検証およびシステムの問題のトラブルシューティングができます。

URL カテゴリに関するスケジュール設定されたレポート内でデータ アベイラビリティが使用されている場合に、いずれかのアプライアンスでデータに欠落があると、ページの下部に「Some data in this time range was unavailable.」というメッセージが表示されます。欠落がない場合は何も表示されません。

Web セキュリティ アプライアンスの [Data Availability] ページの詳細については、「[Data Availability] ページ」を参照してください。

トラッキング データ 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で、任意のアプライアンスからのデータをモニタし、トラッキングできます。

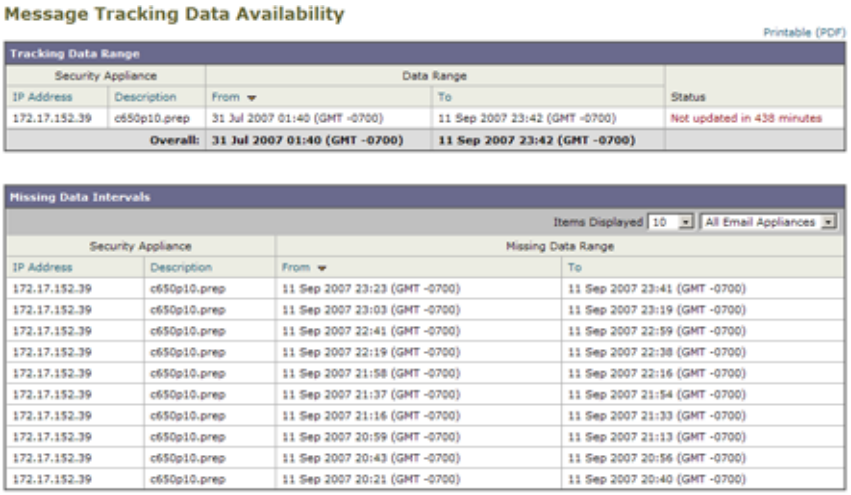
- 「電子メール トラッキング データ ステータスのモニタリング」（P.9-9）
- 「Web トラッキング データ ステータス」（P.9-10）

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

（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。

ステップ 1　メインのセキュリティ管理アプライアンスで、[Email] > [Message Tracking] > [Message Tracking Data Availability] を選択します。

図 9-6　[Message Tracking Data Availability] ページ



Message Tracking Data Availability

Printable (PDF)

Tracking Data Range

Security Appliance		Data Range		
IP Address	Description	From	To	Status
172.17.152.39	c650p10.prep	31 Jul 2007 01:40 (GMT -0700)	11 Sep 2007 23:42 (GMT -0700)	Not updated in 438 minutes
	Overall:	31 Jul 2007 01:40 (GMT -0700)	11 Sep 2007 23:42 (GMT -0700)	

Missing Data Intervals

Items Displayed 10 | All Email Appliances

Security Appliance		Missing Data Range	
IP Address	Description	From	To
172.17.152.39	c650p10.prep	11 Sep 2007 23:23 (GMT -0700)	11 Sep 2007 23:41 (GMT -0700)
172.17.152.39	c650p10.prep	11 Sep 2007 23:03 (GMT -0700)	11 Sep 2007 23:19 (GMT -0700)
172.17.152.39	c650p10.prep	11 Sep 2007 22:41 (GMT -0700)	11 Sep 2007 22:59 (GMT -0700)
172.17.152.39	c650p10.prep	11 Sep 2007 22:19 (GMT -0700)	11 Sep 2007 22:38 (GMT -0700)
172.17.152.39	c650p10.prep	11 Sep 2007 21:58 (GMT -0700)	11 Sep 2007 22:16 (GMT -0700)
172.17.152.39	c650p10.prep	11 Sep 2007 21:37 (GMT -0700)	11 Sep 2007 21:54 (GMT -0700)
172.17.152.39	c650p10.prep	11 Sep 2007 21:16 (GMT -0700)	11 Sep 2007 21:33 (GMT -0700)
172.17.152.39	c650p10.prep	11 Sep 2007 20:59 (GMT -0700)	11 Sep 2007 21:13 (GMT -0700)
172.17.152.39	c650p10.prep	11 Sep 2007 20:43 (GMT -0700)	11 Sep 2007 20:56 (GMT -0700)
172.17.152.39	c650p10.prep	11 Sep 2007 20:21 (GMT -0700)	11 Sep 2007 20:40 (GMT -0700)

[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。

Web トラッキング データ ステータス

ステップ 1　セキュリティ管理アプライアンスで、[Web] > [Reporting] > [Web Tracking] を選択します。

ステップ 2　[Time Range] ドロップダウン リストから、情報を表示する時間範囲を選択します。

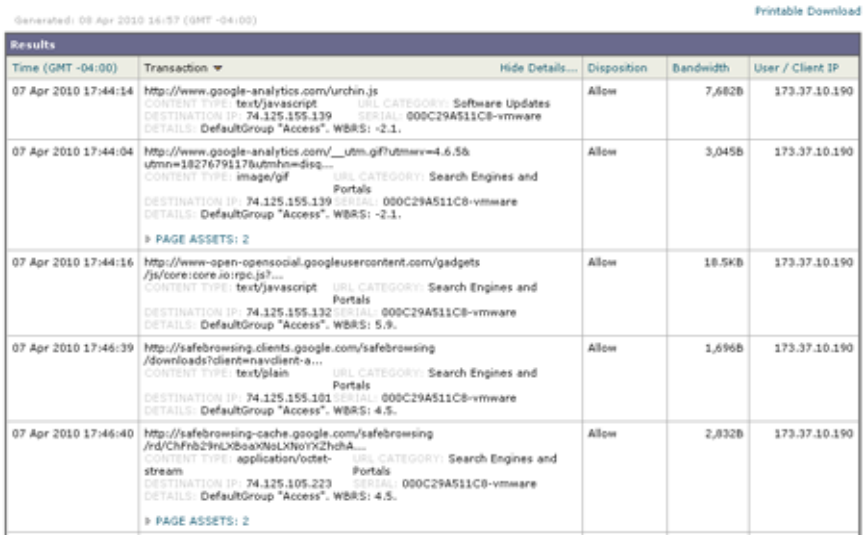
ステップ 3　[User/Client IP] または [Website] テキスト フィールドに、値を入力します。

ステップ 4　[Transaction Type] ドロップダウン リストから、トランザクションの種類を選択します。

選択肢としては、[All Transactions]、[Completed]、[Blocked]、[Monitored]、[Warned] などがあります。

次に、[Website] テキスト フィールドに「google.com」と入力した場合の結果の例を示します。

図 9-7　[Web Tracking Data Status] ページ



Web トラッキングの詳細については、「[Web Tracking] ページ」（P.5-51）を参照してください。

CHAPTER 10

LDAP との統合

概要

企業の LDAP ディレクトリ（例：Microsoft Active Directory、SunONE Directory Server、または OpenLDAP ディレクトリなど）のエンド ユーザのパスワードおよび電子メール エイリアスを管理する場合、LDAP ディレクトリを使用して次のユーザを認証することができます。

- Cisco IronPort スパム隔離にアクセスするエンド ユーザおよび管理ユーザ。

  ユーザが Cisco IronPort スパム隔離の Web UI にログインする場合、LDAP サーバはログイン名とパスワードを検証し、AsyncOS は対応する電子メール エイリアスのリストを取得します。そのユーザの電子メール エイリアスのいずれかに送信された隔離メッセージは、アプライアンスが書き換えない限り Cisco IronPort スパム隔離で表示できます。

  「Cisco IronPort スパム隔離と連携させるための LDAP の設定」（P.10-1）を参照してください。

- 外部認証がイネーブルに設定されている場合、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」（P.10-13）を参照してください。

Cisco IronPort スパム隔離と連携させるための LDAP の設定

Cisco IronPort 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。

ステップ 1　**LDAP サーバ プロファイルを設定します。**

サーバ プロファイルの内容は、AsyncOS から LDAP サーバに接続するための、次のような情報です。

- サーバ名およびポート
- ベース DN
- サーバをバインディングするための認証要件

サーバ プロファイルの設定方法の詳細については、「LDAP サーバ プロファイルの作成」（P.10-2）を参照してください。

LDAP サーバ プロファイルを作成するときに、AsyncOS からの接続先となる LDAP サーバを複数設定できます。詳細については、「AsyncOS を複数の LDAP サーバと連携させるための設定」（P.10-11）を参照してください。

ステップ 2　**LDAP クエリーを設定します。**

LDAP サーバ プロファイル用に生成されたデフォルトのスパム隔離クエリーを使用するか、または実際に使用する LDAP の実装とスキーマに合わせて自分のクエリーを作成することができます。次に、スパム通知、および隔離へのエンドユーザ アクセス検証に使用するアクティブ クエリーを指定します。

クエリーの詳細については、「LDAP クエリーの設定」（P.10-4）を参照してください。

ステップ 3　**Cisco IronPort スパム隔離に対して、LDAP エンドユーザ アクセスおよびスパム通知をイネーブルにします。**

Cisco IronPort スパム隔離に対するエンドユーザ アクセスをイネーブルにして、エンドユーザが隔離メッセージを表示したり管理したりできるようにします。ユーザが複数の通知を受信しないように、スパム通知のエイリアス統合をイネーブルにすることもできます。

詳細については、「中央集中型スパム隔離の設定」（P.7-2）を参照してください。

LDAP サーバ プロファイルの作成

LDAP ディレクトリを使用するように AsyncOS を設定した場合は、LDAP サーバに関する情報を保存するために LDAP サーバ プロファイルを作成します。

ステップ 1　メインのセキュリティ管理アプライアンスで、[Management Appliance] > [System Administration] > [LDAP] を選択します。

ステップ 2　[Add LDAP Server Profile] をクリックします。

ステップ 3　[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　[Host Name(s)] テキスト フィールドに、LDAP サーバのホスト名を入力します。

複数のホスト名を入力すると、LDAP サーバのフェールオーバーやロード バランシングができるようになります。複数のエントリを指定する場合は、カンマで区切ります。詳細については、「AsyncOS を複数の LDAP サーバと連携させるための設定」（P.10-11）を参照してください。

ステップ 5　認証方式を選択します。匿名認証を使用することも、ユーザ名とパスワードを指定することもできます。

（注）　レポート上のクライアント IP アドレスではなくクライアント ユーザ ID を表示するには、LDAP 認証を設定する必要があります。LDAP 認証を使用しない場合、システムでは IP アドレスによるユーザの参照のみができます。[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。[Internal Users Summary] ページにユーザ名が表示されます。

ステップ 6　LDAP サーバ タイプを、[Active Directory]、[OpenLDAP]、または [Unknown or Other] から選択します。

ステップ 7　ポート番号を入力します。

デフォルト ポートは 3268 です。これは、複数台のサーバ環境でグローバル カタログへのアクセスをイネーブルにする Active Directory 用のデフォルト ポートです。

ステップ 8　LDAP サーバのベース DN（識別名）を入力します。

ユーザ名とパスワードで認証を行う場合、ユーザ名にはパスワードが含まれているエントリの完全 DN が含まれている必要があります。たとえば、電子メール アドレスが joe@example.com というユーザがマーケティング グループのユーザだとします。このユーザ用のエントリは、次のエントリのようになります。

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

ステップ 9　[Advanced] で、LDAP サーバとの通信に SSL を使用するかどうかを選択します。

ステップ 10　キャッシュ存続可能時間を入力します。この値は、キャッシュを保持する時間の長さです。

ステップ 11　保持するキャッシュ エントリの最大数を入力します。

ステップ 12　同時接続の最大数を入力します。

ロード バランシングのために LDAP サーバ プロファイルを設定する場合、これらの接続はリストで指定された LDAP サーバ間で配分されます。たとえば、同時接続数を 10 と設定し、3 台のサーバを使用して接続のロード バランシングを行う場合は、AsyncOS によってサーバへの接続が 10 ずつ作成され、接続の総数は 30 となります。詳細については、「ロード バランシング」（P.10-12）を参照してください。

（注）　同時接続の最大数には、LDAP クエリーに使用される LDAP 接続が含まれます。ただし、Cisco IronPort スパム隔離のための LDAP 認証をイネーブルにする場合、アプライアンスはエンド ユーザ隔離に対して 20 の追加接続を許可し、接続の総数は 30 となります。

ステップ 13　サーバへの接続をテストするために、[Test Server(s)] ボタンをクリックします。複数の LDAP サーバを指定した場合は、すべてのサーバのテストが実行されます。テストの結果が [Connection Status] フィールドに表示されます。詳細については、「LDAP サーバのテスト」（P.10-4）を参照してください。

ステップ 14　スパム隔離クエリーを作成します。該当するチェックボックスをオンにして、フィールドに入力します。

ユーザがエンドユーザ隔離にログインするときにそのユーザを検証する、隔離エンドユーザ認証クエリーを設定できます。エンドユーザが電子メール エイリアスごとに隔離通知を受け取らないように、エイリアス統合クエリーを設定できます。これらのクエリーを使用するには、[Designate as the active query] チェックボックスをオンにします。詳細については、「LDAP クエリーの設定」（P.10-4）を参照してください。

ステップ 15　[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 [Run Test] をクリックします。テストの結果が [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、[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

[Add/Edit LDAP Server Profile] ページの [Test Server(s)] ボタン（または CLI の `ldapconfig` コマンドの `test` サブコマンド）を使用して、LDAP サーバへの接続をテストします。サーバ ポートへの接続に成功したか失敗したかを示すメッセージが表示されます。複数の LDAP サーバを設定した場合は、AsyncOS によって各サーバがテストされ、結果が個別に表示されます。

LDAP クエリーの設定

次のセクションで、Cisco IronPort スパム隔離クエリーのタイプごとに、デフォルトのクエリー文字列と設定の詳細を示します。

- **スパム隔離へのエンドユーザ認証のクエリー。**詳細については、「スパム隔離へのエンドユーザ認証のクエリー」（P.10-5）を参照してください。
- **スパム隔離のエイリアス統合のクエリー。**詳細については、「スパム隔離のエイリアス統合クエリー」（P.10-6）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、[Designate as the active query] チェックボックスをオンにします。隔離アクセスを制御するエンドユーザ認証クエリーを 1 つと、スパム通知用のエイリアス統合クエリーを 1 つ指定できます。既存のアクティブ クエリーはすべてディセーブルになります。セキュリティ管理アプライアンスで、[Management Appliance] > [System Administration] > [LDAP] ページを選択します。アスタリスク（*）がアクティブ クエリーの横に表示されます。

ドメインベースのクエリーまたはチェーン クエリーも、アクティブなエンドユーザ アクセス クエリーまたはスパム通知クエリーとして指定できます。詳細については、「ドメインベース クエリー」（P.10-8）および「チェーン クエリー」（P.10-9）を参照してください。

（注）　[LDAP] ページの [Test Query] ボタン（または **ldaptest** コマンド）を使用して、クエリーから返される結果が期待したとおりであることを確認します。

LDAP クエリーの構文

LDAP パス内でスペースを使用できます。引用符で囲む必要はありません。CN と DC の構文では、大文字と小文字は区別されません。

Cn=First Last,oU=user,dc=domain,DC=COM

クエリーに入力する変数名では、大文字と小文字が区別されます。また、正しく動作するためには、LDAP 実装と一致している必要があります。たとえば、プロンプトで **mailLocalAddress** と入力したときに実行されるクエリーは、**maillocaladdress** と入力したときとは異なります。

トークン

次のトークンを LDAP クエリー内で使用できます。

- {a} ユーザ名 @ ドメイン名
- {d} ドメイン
- {dn} 識別名
- {g} グループ名
- {u} ユーザ名
- {f} MAILFROM: アドレス

（注）　{f} トークンを使用できるのは、受け入れクエリーのみです。

たとえば、メールを受け入れるための Active Directory LDAP サーバに対するクエリーは、**(|(mail={a})(proxyAddresses=smtp:{a}))** になります。

（注）　作成したクエリーは、[LDAP] ページの [Test] 機能（または **ldapconfig** コマンドの **test** サブコマンド）を使用してテストすることを強く推奨します。期待したとおりの結果が返されることを確認してから、リスナーに対して LDAP 機能をイネーブルにしてください。詳細については、「LDAP クエリーのテスト」（P.10-7）を参照してください。

スパム隔離へのエンドユーザ認証のクエリー

エンドユーザ認証のクエリーとは、ユーザが Cisco IronPort スパム隔離にログインするときにユーザを検証するためのクエリーです。トークン {u} は、ユーザを示します（ユーザのログイン名を表します）。トークン {a} は、ユーザの電子メール アドレスを示します。LDAP クエリーによって「SMTP:」が電子メール アドレスから除去されることはありません。ただし、AsyncOS はこの部分をアドレスから除去します。

サーバ タイプに基づいて、次のデフォルト クエリー文字列がエンドユーザ認証クエリーに使用されます。

- **Active Directory :** `(sAMAccountName={u})`
- **OpenLDAP :** `(uid={u})`
- **Unknown** または **Other :**（ブランク）

デフォルトでは、プライマリ メール属性は **mail** です。独自のクエリーとメール属性を入力できます。クエリーを CLI で作成するには、**ldapconfig** コマンドの `isqauth` サブコマンドを使用します。

（注）　ユーザのログイン時に各自の電子メール アドレス全体を入力させる場合は、`(mail=smtp:{a})` というクエリー文字列を使用します。

Active Directory エンドユーザ認証の設定の例

ここでは、Active Directory サーバとエンドユーザ認証クエリーの設定の例を示します。この例では、Active Directory サーバのパスワード認証、Active Directory サーバのためのエンドユーザ認証のデフォルト クエリー文字列、mail および proxyAddresses メール属性を使用します。

表 10-1　LDAP サーバとスパム隔離へのエンドユーザ認証の設定例：Active Directory

認証方式	パスワードを使用 （検索用にバインドするための低特権のユーザを作成するか、匿名検索を設定する必要があります）
サーバ タイプ	Active Directory
ポート	3268
ベース DN	（ブランク）
接続プロトコル	（ブランク）
クエリー文字列	(sAMAccountName={u})
メール属性	mail,proxyAddresses

OpenLDAP エンドユーザ認証の設定の例

ここでは、OpenLDAP サーバとエンドユーザ認証クエリーの設定の例を示します。この例では、OpenLDAP サーバの匿名認証、OpenLDAP サーバのためのエンドユーザ認証のデフォルト クエリー文字列、mail および mailLocalAddress メール属性を使用します。

表 10-2　LDAP サーバとスパム隔離へのエンドユーザ認証の設定例：OpenLDAP

認証方式	匿名
サーバ タイプ	OpenLDAP
ポート	389
ベース DN	（ブランク）（古いスキーマでは具体的なベース DN の使用が要求されることがあります）
接続プロトコル	（ブランク）
クエリー文字列	(uid={u})
メール属性	mail,mailLocalAddress

スパム隔離のエイリアス統合クエリー

スパム通知を使用する場合は、スパム隔離のエイリアス統合クエリーを使用して電子メール エイリアスを 1 つにまとめると、受信者がエイリアスごとに隔離通知を受け取ることはなくなります。たとえば、ある受信者がメール アドレス john@example.com、jsmith@example.com、および john.smith@example.com のメールを受け取るとします。エイリアス統合を使用すると、受信者が受け取るスパム通知は 1 通だけとなります。送信先は、このユーザのエイリアスすべてに送信されるメッセージのプライマリ メール アドレスとして選択されたアドレスです。

メッセージを統合してプライマリ メール アドレスに送信するには、受信者の代替の電子メール エイリアスを検索するためのクエリーを作成してから、受信者のプライマリ メール アドレスを [Email Attribute] フィールドに入力します。

Active Directory サーバの場合は、デフォルトのクエリー文字列は (|(proxyAddresses={a})(proxyAddresses=smtp:{a})) で、デフォルトのメール属性は mail です。OpenLDAP サーバの場合は、デフォルトのクエリー文字列は (mail={a}) で、デフォルトのメール属性は mail です。独自のクエリーとメール属性を定義することもできます。属性が複数の場合は、カンマで区切ります。入力するメール属性が複数ある場合は、Cisco IronPort では最初のメール属性として、変動する可能性のある値を複数持つ属性（たとえば proxyAddresses）ではなく、値を 1 つだけ使用する一意の属性（たとえば mail）を入力することを推奨します。

クエリーを CLI で作成するには、ldapconfig コマンドの isqalias サブコマンドを使用します。

Active Directory エイリアス統合の設定の例

ここでは、Active Directory サーバとエイリアス統合クエリーの設定の例を示します。この例では、Active Directory サーバに対して匿名認証を使用し、Active Directory サーバに対するエイリアス統合用のクエリー文字列を指定し、メール属性は mail を使用します。

表 10-3　LDAP サーバとスパム隔離のエイリアス統合の設定例：Active Directory

認証方式	匿名
サーバ タイプ	Active Directory
ポート	3268
ベース DN	（ブランク）
接続プロトコル	Use SSL
クエリー文字列	(|(mail={a})(mail=smtp:{a}))
メール属性	mail

OpenLDAP エイリアス統合の設定の例

ここでは、OpenLDAP サーバとエイリアス統合クエリーの設定の例を示します。この例では、OpenLDAP サーバに対して匿名認証を使用し、OpenLDAP サーバに対するエイリアス統合用のクエリー文字列を指定し、メール属性は mail を使用します。

表 10-4　LDAP サーバとスパム隔離のエイリアス統合の設定例：OpenLDAP

認証方式	匿名
サーバ タイプ	OpenLDAP
ポート	389
ベース DN	（ブランク）（古いスキーマでは具体的なベース DN の使用が要求されることがあります）
接続プロトコル	Use SSL
クエリー文字列	(mail={a}))
メール属性	mail

LDAP クエリーのテスト

[Add/Edit LDAP Server Profile] ページの [Test Query] ボタン（または CLI の ldaptest コマンド）を使用して、クエリーをテストします。AsyncOS に、クエリー接続テストの各ステージの詳細が表示されます。たとえば、最初のステージの SMTP 認証に成功したか失敗したか、バインド照合の返された結果が true か false か、などです。

`ldaptest` コマンドは、次の例のようにバッチ コマンドとして使用できます。

```
ldaptest LDAP.isqalias foo@cisco.com
```

クエリーに入力する変数名では、*大文字と小文字が区別されます*。また、正しく動作するためには、LDAP 実装と一致している必要があります。たとえば、メール属性に `mailLocalAddress` と入力すると、`maillocaladdress` と入力する場合とは異なるクエリーを実行します。

クエリーをテストするには、テスト パラメータを入力して、[Run Test] をクリックします。[Test Connection] フィールドに結果が表示されます。エンドユーザ認証クエリーが成功した場合、「Success: Action: match positive」という結果が表示されます。エイリアス統合クエリーの場合は、統合されたスパム通知の電子メール アドレスと共に、「Success: Action: alias consolidation」という結果が表示されます。クエリーが失敗すると、一致する LDAP レコードが見つからない、一致したレコードにメール属性が含まれていないなど、失敗の原因が表示されます。複数の LDAP サーバを使用している場合、Cisco IronPort アプライアンスは、LDAP サーバごとにクエリーをテストします。

ドメインベース クエリー

ドメインベース クエリーとは、LDAP クエリーをタイプ別にグループ化し、ドメインに関連付けたものです。複数の別の LDAP サーバが異なるドメインに関連付けられているが、エンドユーザ隔離アクセスに対し、すべての LDAP サーバでクエリーを実行する必要がある場合、ドメインベース クエリーの使用を推奨します。たとえば、Bigfish という名前の会社が Bigfish.com、Redfish.com、および Bluefish.com というドメインを所持していて、それぞれのドメインに関連する従業員用に別の LDAP サーバを管理するとします。Bigfish は、ドメインベース クエリーを使用して、3 つのドメインすべての LDAP ディレクトリに対してエンドユーザを認証することができます。

ドメインベース クエリーを使用してエンドユーザ アクセスまたは Cisco IronPort スパム隔離の通知を制御するには、次の手順を実行します。

ステップ 1　ドメインベース クエリーで使用する各ドメインについて LDAP サーバ プロファイルを作成します。各サーバ プロファイルでは、ドメインベース クエリーで使用するクエリーを設定します。詳細については、「LDAP サーバ プロファイルの作成」（P.10-2）を参照してください。

ステップ 2　ドメインベース クエリーを作成します。ドメインベース クエリーを作成するときに、各サーバ プロファイルからクエリーを選択し、ドメインベース クエリーを Cisco IronPort スパム隔離のアクティブ クエリーとして指定します。クエリーの作成方法の詳細については、「ドメインベース クエリーの作成」（P.10-8）を参照してください。

ステップ 3　Cisco IronPort スパム隔離に対して、エンドユーザ アクセスまたはスパム通知をイネーブルにします。詳細については、「中央集中型スパム隔離の設定」（P.7-2）を参照してください。

ドメインベース クエリーの作成

ステップ 1　セキュリティ管理アプライアンスで、[Management Appliance] > [System Administration] > [LDAP] を選択します。

ステップ 2　[LDAP] ページで、[Advanced] をクリックします。

ステップ 3　ドメインベース クエリーの名前を入力します。

ステップ 4　クエリーのタイプを選択します。

（注）　ドメインベース クエリーを作成するときは、シングル クエリー タイプを指定します。クエリーのタイプを選択すると、該当するクエリーが LDAP サーバ プロファイルからクエリー フィールド ドロップダウン リストに含まれるようになります。

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

ステップ 6　このドメインに関連付けるクエリーを選択します。

ステップ 7　行を追加して、ドメインベース クエリーのドメインごとにクエリーを選択します。

ステップ 8　どのクエリーにも一致しないときに実行する、デフォルトのクエリーを入力します。デフォルトのクエリーを入力しない場合は、[None] を選択します。

図 10-1　　ドメインベース クエリーの例

ステップ 9　[Test Query] ボタンをクリックし、[Test Parameters] フィールドにテストするユーザのログインとパスワード、または電子メール アドレスを入力して、クエリーをテストします。[Connection Status] フィールドに結果が表示されます。

ステップ 10　Cisco IronPort スパム隔離でドメインベース クエリーを使用するには、[Designate as the active query] チェックボックスをオンにします。

（注）　ドメインベース クエリーが、指定されたクエリー タイプのアクティブ LDAP クエリーになります。たとえば、ドメインベース クエリーがエンドユーザ認証に使用されている場合は、Cisco IronPort スパム隔離のアクティブ エンドユーザ認証クエリーになります。

ステップ 11　[Submit] をクリックし、[Commit] をクリックして変更を保存します。

（注）　同じ設定をコマンドライン インターフェイスで行うには、コマンド ライン プロンプトで、`ldapconfig` コマンドの `advanced` サブコマンドを入力します。

チェーン クエリー

チェーン クエリーは、AsyncOS が連続して実行する一連の LDAP クエリーです。AsyncOS は LDAP サーバから肯定的なレスポンスが返されると、または最後のクエリーで否定的なレスポンスが返されるか失敗するまで、シリーズ内の各クエリー、「チェーン」内の各クエリーを実行します。チェーン クエリーが役立つのは、LDAP ディレクトリ内のエントリにおいて、さまざまな属性に類似の（または同一の）値が格納されている場合です。たとえば、組織の各部門が、異なるタイプの LDAP ディレクト

リを使用していることがあります。IT 部門が OpenLDAP を使用し、営業部門が Active Directory を使用しているとします。クエリーが両方のタイプの LDAP ディレクトリに対して実行されていることを確認するために、チェーン クエリーを使用できます。

チェーン クエリーを使用してエンドユーザ アクセスまたは Cisco IronPort スパム隔離の通知を制御するには、次の手順を実行します。

ステップ 1　チェーン クエリーで使用するクエリーごとに 1 つずつ、LDAP サーバ プロファイルを作成します。このサーバ プロファイルのそれぞれについて、チェーン クエリーに使用するクエリーを設定します。詳細については、「LDAP サーバ プロファイルの作成」（P.10-2）を参照してください。

ステップ 2　チェーン クエリーを作成し、Cisco IronPort スパム隔離のアクティブ クエリーとして指定します。詳細については、「チェーン クエリーの作成」（P.10-10）を参照してください。

ステップ 3　Cisco IronPort スパム隔離に対して、LDAP エンドユーザ アクセスまたはスパム通知をイネーブルにします。スパム隔離の詳細については、「中央集中型スパム隔離の設定」（P.7-2）を参照してください。

チェーン クエリーの作成

ヒント　CLI から、`ldapconfig` コマンドの `advanced` サブコマンドも使用できます。

ステップ 1　セキュリティ管理アプライアンスで、[Management Appliance] > [System Administration] > [LDAP] > [LDAP Server] を選択します。

ステップ 2　[LDAP Server Profiles] ページの [Advanced] をクリックします。

ステップ 3　[Add Chained Query] をクリックします。

ステップ 4　チェーン クエリーの名前を入力します。

ステップ 5　クエリーのタイプを選択します。

チェーン クエリーを作成するときは、そのコンポーネントのクエリーすべてを同じクエリー タイプにします。クエリーのタイプを選択すると、該当するクエリーが LDAP からクエリー フィールド ドロップダウン リストに表示されます。

ステップ 6　チェーンの最初のクエリーを選択します。

Cisco IronPort 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 10-2　チェーン クエリーの例

ステップ 7　[Test Query] ボタンをクリックし、[Test Parameters] フィールドにユーザのログインとパスワード、または電子メール アドレスを入力して、クエリーをテストします。[Connection Status] フィールドに結果が表示されます。

ステップ 8　Cisco IronPort スパム隔離でドメイン クエリーを使用するには、[Designate as the active query] チェックボックスをオンにします。

（注）　チェーン クエリーが、指定されたクエリー タイプのアクティブ LDAP クエリーになります。たとえば、チェーン クエリーがエンドユーザ認証に使用されている場合は、Cisco IronPort スパム隔離のアクティブ エンドユーザ認証クエリーになります。

ステップ 9　変更を送信し、保存します。

（注）　同じ設定をコマンドライン インターフェイスで行うには、コマンド ライン プロンプトで、`ldapconfig` コマンドの `advanced` サブコマンドを入力します。

AsyncOS を複数の LDAP サーバと連携させるための設定

LDAP サーバ プロファイルを設定するときに、Cisco IronPort 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 Cisco IronPort アプライアンスを設定します。

- **フェールオーバー**。Cisco IronPort 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**。Cisco IronPort 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、[Management Appliance] > [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

[Add（または Edit）LDAP Server Profile] ページの [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。

Cisco IronPort 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。Cisco IronPort アプライアンスが確実にプライマリ LDAP サーバにデフォルトで接続するようにするには、そのサーバが LDAP サーバ リストの先頭に入力されていることを確認してください。

Cisco IronPort アプライアンスが 2 番目の、または後続の LDAP サーバに接続する場合、そのサーバへの接続は所定の時間が経過するまで維持されます。この時間が経過すると、アプライアンスはリスト内の最初のサーバに対して再接続を試行します。

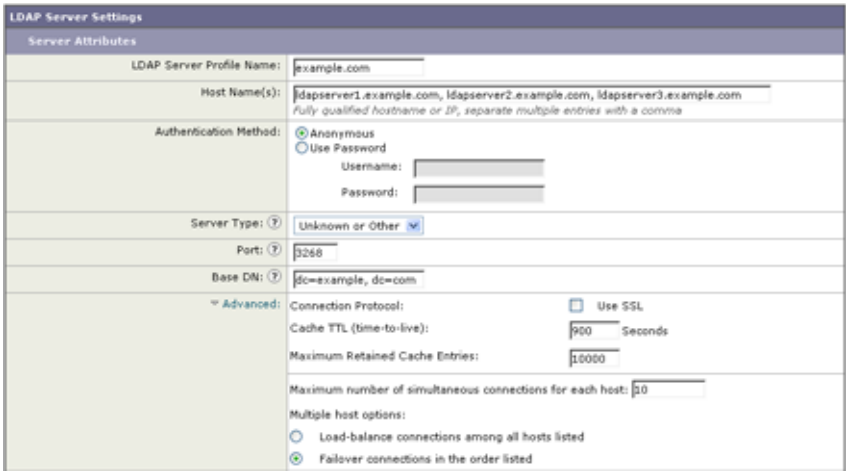
LDAP フェールオーバーのための Cisco IronPort アプライアンスの設定

ステップ 1　セキュリティ管理アプライアンスで、[Management Appliance] > [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 10-3　　LDAP フェールオーバー コンフィギュレーションの例



ステップ 3　[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　[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　[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、Cisco IronPort 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、Cisco IronPort 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。Cisco IronPort 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、Cisco IronPort 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。

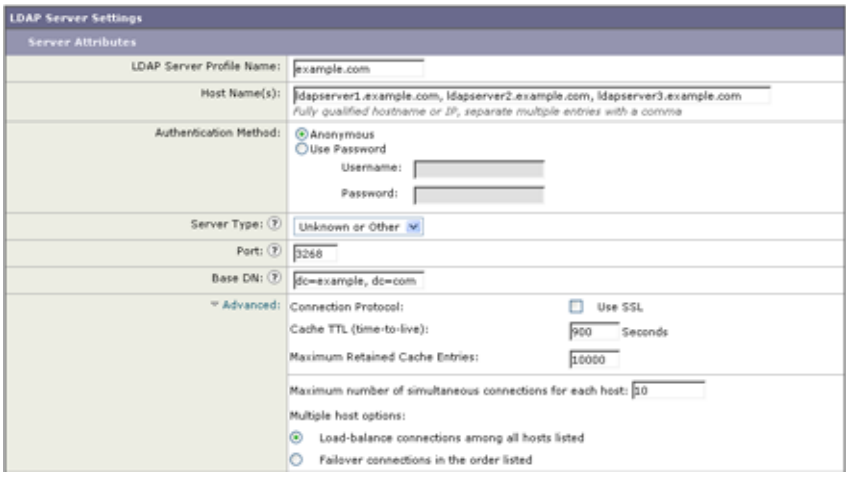
ロード バランシングのための Cisco IronPort アプライアンスの設定

ステップ 1　セキュリティ管理アプライアンスで、[Management Appliance] > [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 10-4　　ロード バランシング コンフィギュレーションの例



ステップ 3　[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　[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　[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 Cisco IronPort 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、セキュリティ管理アプライアンスにログインできるようになります。

ステップ 1　**LDAP サーバ プロファイルを設定します。**「LDAP サーバ プロファイルの作成」（P.10-2）を参照してください。

ステップ 2　**ユーザ アカウントを見つけるためのクエリーを作成します。**LDAP サーバ プロファイルの、[External Authentication Queries] セクションで、クエリーを作成して LDAP ディレクトリ内のユーザ アカウントを検索します。「管理ユーザの認証のためのユーザ アカウント クエリー」（P.10-14）を参照してください。

ステップ 3　**グループ メンバーシップ クエリーを作成します。**あるユーザがディレクトリ グループのメンバーであるかどうかを判断するクエリーを作成し、あるグループのすべてのメンバーを検索する別のクエリーを作成します。詳細については、「管理ユーザの認証のためのグループ メンバーシップ クエリー」（P.10-15）および『*Cisco IronPort AsyncOS for Email Security Advanced User Guide*』を参照してください。

（注）　そのページの [External Authentication Queries] セクションにある [Test Queries] ボタン（または `ldaptest` コマンド）を使用して、クエリーから返される結果が期待したとおりであることを確認します。関連情報については、「LDAP クエリーのテスト」（P.10-7）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イネーブル化」（P.10-16）および『*Cisco IronPort AsyncOS for Email Security Advanced User Guide*』の「Adding Users」を参照してください。

管理ユーザの認証のためのユーザ アカウント クエリー

外部ユーザを認証するために、AsyncOS はクエリーを使用してそのユーザのレコードを LDAP ディレクトリ内で検出し、ユーザのフル ネームが格納されている属性を見つけます。管理者が選択したサーバ タイプに応じて、AsyncOS によってデフォルトのクエリーとデフォルトの属性が入力されます。アカウントが失効しているユーザは拒否するようにアプライアンスを設定することもできます。それには、RFC 2307 で規定されている属性が LDAP ユーザ レコード内で定義されている必要があります（**shadowLastChange**、**shadowMax**、および **shadowExpire**）。ユーザのレコードがあるドメイン レベルのベース DN が必要です。

表 10-5 に、AsyncOS がユーザ アカウントを Active Directory サーバ上で検索するときに使用されるデフォルトのクエリー文字列とユーザのフル ネーム属性を示します。

表 10-5　Active Directory サーバのデフォルト クエリー文字列

サーバ タイプ	Active Directory
ベース DN	（ブランク）（ユーザ レコードを見つけるには具体的なベース DN を使用する必要があります）
クエリー文字列	`(&(objectClass=user)(sAMAccountName={u}))`
ユーザのフル ネームが格納されている属性	`displayName`

表 10-6 に、AsyncOS がユーザ アカウントを OpenLDAP サーバ上で検索するときに使用されるデフォルトのクエリー文字列とユーザのフル ネーム属性を示します。

表 10-6　Open LDAP サーバのデフォルト クエリー文字列

サーバ タイプ	OpenLDAP
ベース DN	（ブランク）（ユーザ レコードを見つけるには具体的なベース DN を使用する必要があります）
クエリー文字列	`(&(objectClass=posixAccount)(uid={u}))`
ユーザのフル ネームが格納されている属性	`gecos`

管理ユーザの認証のためのグループ メンバーシップ クエリー

LDAP グループをアプライアンスにアクセスするためのユーザ ロールと関連付けることができます。

AsyncOS は、あるユーザがディレクトリ グループのメンバーであるかどうかを判断するクエリーや、あるグループのすべてのメンバーを検索する別のクエリーを使用することもできます。ディレクトリ グループ メンバーシップ内のメンバーシップによって、そのユーザのシステム内のアクセス許可が決まります。GUI の [Management Appliance] > [System Administration] > [Users] ページ（または CLI の `userconfig`）で外部認証をイネーブルにするときに、ユーザ ロールを LDAP ディレクトリ内のグループに割り当てます。ユーザ ロールによって、そのユーザがシステム内で持つアクセス許可が決まります。外部認証されたユーザの場合は、ロールは個々のユーザではなくディレクトリ グループに割り当てられます。たとえば、IT というディレクトリ グループ内のユーザに「Administrator」というロールを割り当て、「Support」というディレクトリ グループのユーザに「Help Desk User」というロールを割り当てます。

ユーザが異なるユーザ ロールを持つ複数の LDAP グループに属する場合は、AsyncOS がユーザに最も制限されたロールの権限を割り当てます。たとえば、ユーザが Operator 権限を持つグループと Help Desk User 権限を持つグループに属する場合、AsyncOS はユーザに Help Desk User ロールの権限を割り当てます。

グループ メンバーシップを問い合わせるための LDAP プロファイルを設定するときに、グループ レコードが格納されているディレクトリ レベルのベース DN を入力し、グループ メンバーのユーザ名が格納されている属性と、グループ名が格納されている属性を入力します。LDAP サーバ プロファイルに対して選択されたサーバ タイプに基づいて、ユーザ名とグループ名の属性のデフォルト値とデフォルト クエリー文字列が AsyncOS によって入力されます。

（注）　Active Directory サーバの場合は、ユーザが特定のグループのメンバーかどうかを判断するためのデフォルトのクエリー文字列は (&(objectClass=group)(member={u})) です。ただし、使用する LDAP スキーマにおいて、「memberof」のリストでユーザ名ではなく識別名が使用されている場合は、{dn} を {u} の代わりに使用できます。

表 10-7 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 10-7　Active Directory サーバのデフォルト クエリー文字列および属性

クエリー文字列	Active Directory
ベース DN	（ブランク）（グループ レコードを見つけるには具体的なベース DN を使用する必要があります）
ユーザが特定のグループのメンバーかどうかを判断するためのクエリー文字列	`(&(objectClass=group)(member={u}))` （注）　使用する LDAP スキーマにおいてメンバーのリストの中でユーザ名ではなく識別名が使用されている場合は、`{u}` の代わりに `{dn}` を使用できます。
グループのすべてのメンバーを判別するクエリー文字列	`(&(objectClass=group)(cn={g}))`
各メンバーのユーザ名（またはそのユーザのレコードの DN）が格納されている属性	`member`
グループ名が格納されている属性	`cn`

表 10-8 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 10-8　Open LDAP サーバのデフォルト クエリー文字列および属性

クエリー文字列	OpenLDAP
ベース DN	（ブランク）（グループ レコードを見つけるには具体的なベース DN を使用する必要があります）
ユーザが特定のグループのメンバーかどうかを判断するためのクエリー文字列	`(&(objectClass=posixGroup)(memberUid={u}))`
グループのすべてのメンバーを判別するクエリー文字列	`(&(objectClass=posixGroup)(cn={g}))`
各メンバーのユーザ名（またはそのユーザのレコードの DN）が格納されている属性	`memberUid`
グループ名が格納されている属性	`cn`

管理ユーザの外部認証のイネーブル化

LDAP サーバ プロファイルおよびクエリーを設定した後で、LDAP を使用する外部認証をイネーブルにすることができます。

ステップ 1　セキュリティ管理アプライアンスで、[Management Appliance] > [System Administration] > [Users] ページを選択します。

ステップ 2　[Enable] をクリックします。

ステップ 3　[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、[Add Row] をクリックして別のディレクトリ グループを追加することもできます。アプライアンスが認証する各ディレクトリ グループに対して、ステップ 7 とステップ 8 を繰り返します。

ステップ 9　変更を送信し、保存します。

CHAPTER 11

SMTP ルーティングの設定

この章では、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 Routes] ページと **smtproutes** コマンドの使用について説明します。

ローカル ドメインの電子メールのルーティング

セキュリティ管理アプライアンスは、次のメールをルーティングします。

- ISQ によりリリースされた、SMTP ルーティングを無視するメッセージ
- アラート
- 指定した宛先にメールできるコンフィギュレーション ファイル
- 定義された受信者にも送信できるサポート要求メッセージ

  最後の 2 種類のメッセージは、宛先への配信に SMTP ルートが使用されます。

電子メール セキュリティ アプライアンスでは、メールをローカル ドメイン経由で、[Management Appliance] > [Network] > [SMTP Routes] ページ（または **smtproutes** コマンド）を使用して指定されたホストにルーティングします。この機能は、sendmail の **mailertable** 機能に似ています。（[SMTP Routes] ページと **smtproutes** コマンドは、AsyncOS 2.0 ドメイン リダイレクト機能を拡張したものです）。

（注） GUI のシステム設定ウィザードを完了し、変更を保存した場合、その時点で入力した各 RAT エントリに対してアプライアンス上の最初の SMTP ルート エントリを定義します。

SMTP ルートの概要

SMTP ルートでは、異なる Mail Exchange（MX）ホストへ特定のドメインのすべての電子メールをリダイレクトできます。たとえば、`example.com` から `groupware.example.com` へのマッピングを行うことができます。このマッピングによって、[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。Cisco IronPort AsyncOS 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 Cisco IronPort アプライアンスに設定できます。（「SMTP ルートの制限」（P.11-3）を参照）。

この機能では、ホストを「ひとかたまりにする」ことも可能です。example.com などの部分ドメインを指定すると、example.com で終わるすべてのドメインがエントリと一致します。たとえば、fred@foo.example.com と wilma@bar.example.com は、両方ともマッピングに一致します。

SMTP ルート テーブルにホストがない場合は、DNS を使用して MX ルックアップが実行されます。結果は、SMTP ルート テーブルに対して再チェックされません。foo.domain の DNS MX エントリが bar.domain の場合、foo.domain に送信されるすべての電子メールが bar.domain に配信されます。bar.domain から他のホストへのマッピングを作成した場合、foo.domain へ送信される電子メールは影響を受けません。

つまり、再帰的なエントリは続きません。a.domain から b.domain にリダイレクトされるエントリがあり、b.domain から a.domain にリダイレクトされるエントリがその後にある場合、メールのループは作成*されません*。この場合、a.domain に送信される電子メールは、b.domain で指定された MX ホストに配信されます。反対に、b.domain に送信される電子メールは、a.domain で指定された MX ホストに配信されます。

すべての電子メール配信で、SMTP ルート テーブルは、上から順に読み取られます。マッピングと一致する最も具体的なエントリが選択されます。たとえば、SMTP ルート テーブルに host1.example.com と example.com の両方のマッピングがある場合は、host1.example.com の方が具体的なエントリになっているため、こちらが使用されます。具体的でない方の example.com エントリが先にあっても、同じ結果になります。そうでない場合は、エンベロープ受信者のドメインで通常の MX ルックアップが実行されます。

デフォルトの SMTP ルート

特殊なキーワード ALL を使用して、デフォルトの SMTP ルートも定義できます。ドメインが SMTP ルート リストの以前のマッピングと一致しない場合、デフォルトでは、それが ALL エントリで指定される MX ホストにリダイレクトされます。

SMTP ルート エントリを印刷する場合、デフォルトの SMTP ルートは ALL: として一覧表示されます。デフォルトの SMTP ルートは削除できません。入力した値をクリアすることのみ可能です。

[Management Appliance] > [Network] > [SMTP Routes] ページを使用するか、または **smtproutes** コマンドを使用して、デフォルトの SMTP ルートを設定します。

SMTP ルートの定義

電子メール セキュリティ アプライアンスはローカル ドメイン宛てのメールを、[Management Appliance] > [Network] > [SMTP Routes] ページ（または **smtproutes** コマンド）を使用して指定されたホストにルーティングします。この機能は、sendmail の mailer table 機能に似ています。（[SMTP 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）。

[Management Appliance] > [Network] > [SMTP Routes] ページ（または **smtproutes** コマンド）を使用してルートを作成します。新しいルートを作成するには、まず、永続的なルートを作成するドメインまたはドメインの一部を指定する必要があります。次に、宛先ホストを指定します。宛先ホストは、完全修飾ホスト名として入力することも、IP アドレスとして入力することもできます。エントリと一致するメッセージをドロップするために、特殊な宛先ホスト /dev/null を指定することもできます。（実際に /dev/null をデフォルト ルートに指定すると、アプライアンスが受信したメールは配信されなくなります）。

複数の宛先ホスト エントリに、完全修飾ホスト名と IP アドレスの両方を含めることができます。複数のエントリを指定する場合は、カンマで区切ります。

1 つまたは複数のホストが応答しない場合、メッセージは到達可能なホストの 1 つに配信されます。設定されたすべてのホストが応答しない場合、メールはそのホストのキューに格納されます（MX レコードの使用にフェールオーバーしません）。

SMTP ルートの制限

最大 10,000 ルートまで定義できます。最後のデフォルト ルート ALL は、この制限内のルートとしてカウントされます。したがって、定義できるのは最大 9,999 のカスタム ルートと、特殊キーワード ALL を使用する 1 つのルートです。

SMTP ルートと DNS

MX ルックアップを実行して、特定のドメインに対するネクスト ホップを決定するようアプライアンスに指示するには、特殊キーワード USEDNS を使用します。これは、サブドメインのメールを特定のホストにルーティングする必要がある場合に役立ちます。たとえば、example.com へのメールが企業の Exchange サーバに送信されることになっている場合、次のような SMTP ルートになっていることがあります。

```
example.com exchange.example.com
```

ただし、さまざまなサブドメイン（foo.example.com）宛のメールの場合は、次のような SMTP ルートを追加します。

```
.example.com USEDNS
```

SMTP ルート、メール配信、およびメッセージ分裂

着信：1 つのメッセージに 10 人の受信者がいて、全員が同じ Exchange サーバに属する場合、AsyncOS では TCP 接続を 1 つ開き、メール ストアには 10 の別々のメッセージではなく、メッセージを 1 つのみ配置します。

発信：同様に機能しますが、1 つのメッセージが 10 の異なるドメインの 10 人の受信者に送られる場合、AsyncOS では 10 の MTA に対する 10 の接続を開き、それぞれに 1 つずつ電子メール配信を行います。

分裂：1 つの着信メッセージに 10 人の受信者がいて、それぞれが別々の Incoming Policy グループ（10 グループ）に属する場合、10 人全員の受信者が同じ Exchange サーバを使用していても、メッセージは分裂します。つまり、10 の別々の電子メールが 1 つの TCP 接続で配信されます。

SMTP ルートと発信 SMTP 認証

発信 SMTP 認証プロファイルが作成されたら、SMTP ルートに適用できます。これにより、ネットワークのエッジにあるメール リレー サーバの背後に Cisco IronPort アプライアンスが位置する場合に、発信メールの認証が可能になります。

セキュリティ管理アプライアンスでの SMTP ルートの管理

ステップ 1　セキュリティ管理アプライアンスで、[Management Appliance] > [Network] > [SMTP Routes] を選択します。

このページを使用して、Cisco IronPort アプライアンスで SMTP ルートを管理します。このページから、テーブルのマッピングの追加、変更、および削除を行うことができます。SMTP ルート エントリをエクスポートまたはインポートすることができます。

SMTP ルートの追加

ステップ 1　セキュリティ管理アプライアンスで、[Management Appliance] > [Network] > [SMTP Routes] を選択します。

ステップ 2　[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、[Add Row] をクリックし、新しい行に次の宛先ホストを入力します。

ステップ 4　ポート番号を指定するには、宛先ホストに「:<*port number*>」を追加します（例：`example.com:25`）。

ステップ 5　変更を送信し、保存します。

SMTP ルートの編集

ステップ 1　セキュリティ管理アプライアンスで、[Management Appliance] > [Network] > [SMTP Routes] を選択します。

ステップ 2　SMTP ルートのリストで、既存の SMTP ルートの名前をクリックします。

ステップ 3　ルートを編集します。

ステップ 4　変更を送信し、保存します。

SMTP ルートの削除

ステップ 1　セキュリティ管理アプライアンスで、[Management Appliance] > [Network] > [SMTP Routes] を選択します。

ステップ 2　削除する SMTP ルートの右側にあるチェックボックスを選択します。

ステップ 3　[Delete] をクリックします。

すべての SMTP ルートを削除するには、[All] というラベルの付いたチェックボックスを選択して [Delete] をクリックします。

SMTP ルートのエクスポート

ホスト アクセス テーブル（HAT）および受信者アクセス テーブル（RAT）の場合と同様に、ファイルをエクスポートおよびインポートして SMTP ルート マッピングを変更することもできます。

ステップ 1　[SMTP Routes] ページの [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、[Submit] をクリックします。

SMTP ルートのインポート

Host Access Table（HAT）および Recipient Access Table（RAT）の場合と同様に、ファイルをエクスポートおよびインポートして SMTP ルート マッピングを変更することもできます。

ステップ 1　[SMTP Routes] ページの [Import SMTP Routes] をクリックします。

ステップ 2　エクスポートされた SMTP ルートが含まれているファイルを選択します。

ステップ 3　[Submit] をクリックします。インポートにより、既存の SMTP ルートがすべて置き換えられることが警告されます。テキスト ファイルにあるすべての SMTP ルートがインポートされます。

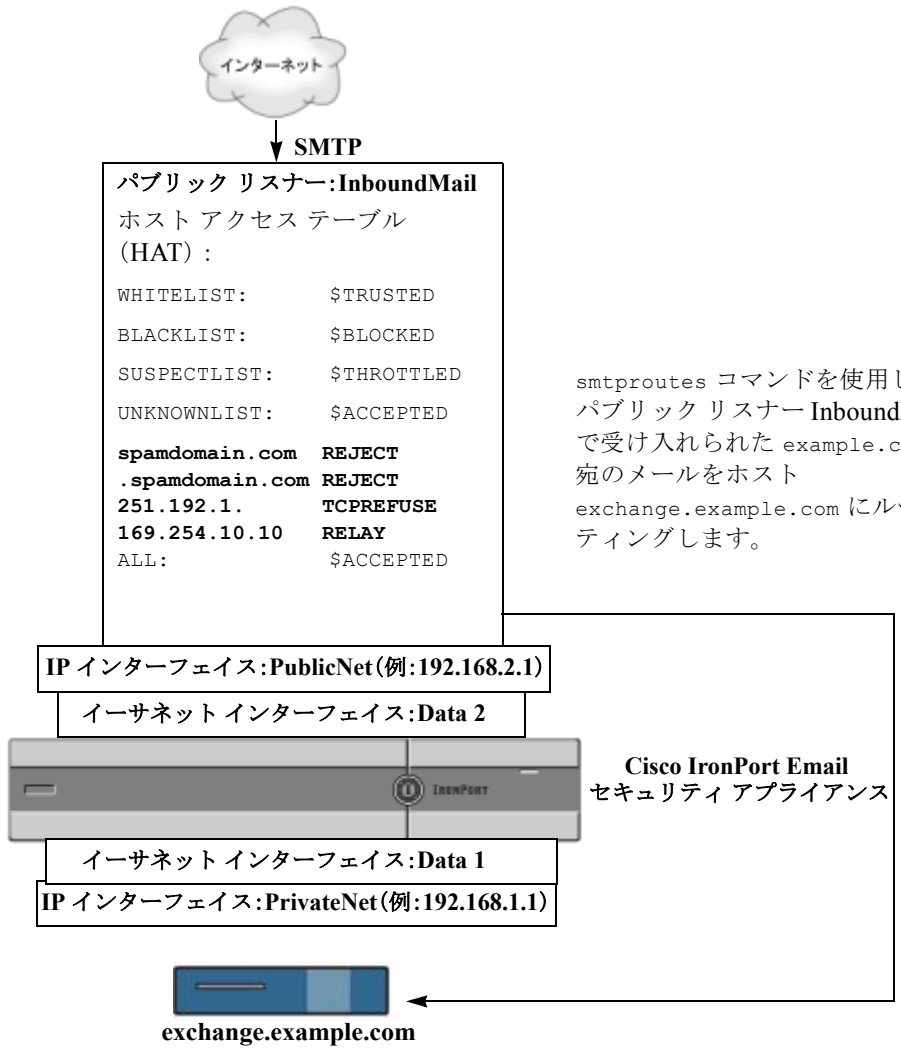
ステップ 4　[Import] をクリックします。

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

```
# this is a comment, but the next line is not
ALL:
```

この時点で、電子メール ゲートウェイの設定は次のようになります。

図 11-1　パブリック リスナー用に定義された SMTP ルート



CHAPTER 12

管理タスクの分散

セキュリティ管理アプライアンスを管理する管理タスクを分散させ、さまざまな方法でアプライアンスへのアクセスを制御することができます。

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、他のユーザにセキュリティ管理アプライアンスの管理タスクを分散できます。

管理タスクが分散されるように設定するには、事前定義されたユーザ ロールがニーズを満たしているかどうかを判断して、必要なカスタム ユーザ ロールを作成します。次に、セキュリティ アプライアンスでローカルに管理ユーザの認証を行う、および（または）独自の中央集中型の LDAP や RADIUS システムを使用して外部で管理ユーザの認証を行うようにアプライアンスを設定します。

さらに、アプライアンスおよびアプライアンス上の特定の情報へのアクセスに追加の制御を指定できます。

ユーザ ロールの割り当て

セキュリティ管理アプライアンスには、電子メールと Web セキュリティ アプライアンスのモニタリングおよび管理を行うための、事前定義ユーザ ロールとカスタム ユーザ ロールの両方が用意されています。

事前定義ユーザ ロール

特記のない限り、次の表で説明されている権限を持つ事前設定ユーザ ロール、またはカスタム ユーザ ロールを各ユーザに割り当てることができます。

表 12-1　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/スケジュール設定されたレポート機能
admin	**admin** ユーザはシステムのデフォルト ユーザ アカウントであり、すべての管理権限を持っています。便宜上、admin ユーザ アカウントをここに記載しましたが、これはユーザ ロールを使用して割り当てることはできず、パスワードの変更以外、編集や削除もできません。 **resetconfig** コマンドと **revert** コマンドを発行できるのは、**admin** ユーザだけです。	あり / あり
Administrator	Administrator ロールを持つユーザ アカウントはシステムのすべての設定に対する完全なアクセス権を持っています。	あり / あり
Operator	Operator ロールを持つユーザ アカウントは次のことができません。 • ユーザ アカウントの作成または編集 • `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 • LDAP が外部認証用にイネーブルになっている場合の、ユーザ名とパスワードを除く LDAP サーバ プロファイル設定の変更 これら以外は、Administrator ロールと同じ権限を持ちます。	あり / あり
Technician	Technician ロールを持つユーザ アカウントは、アップグレードおよびリブート、アプライアンスからのコンフィギュレーション ファイルの保存、機能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。	[Email] タブに表示されるシステム キャパシティ レポートへのアクセス
Read-Only Operator	Read-Only Operator ロールを持つユーザは、設定情報を参照するアクセス権を持っています。Read-Only Operator ロールを持つユーザは、機能の設定方法を確認するために大部分の変更を行って送信できますが、保存できません。または保存を必要としない変更を行うことができます。また、このロールを持つユーザは Cisco IronPort スパム隔離でメッセージを管理できます（アクセスがイネーブルな場合）。このロールを持つユーザは、ファイル システム、FTP、または SCP にアクセスできません。	あり / なし

表 12-1　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 / スケジュール設定されたレポート機能
Guest	Guest ロールを持つユーザ アカウントはステータス情報だけを参照できます。また、Guest ロールを持つユーザは Cisco IronPort スパム隔離でメッセージを管理することもできます（アクセスがイネーブルな場合）。Guest ロールを持つユーザはメッセージ トラッキングにアクセスできません。	あり / なし
Web Administrator	Web Administrator ロールを持つユーザ アカウントは、[Web] タブに表示されるすべての設定に対するアクセス権を持ちます。	あり / あり
Web Policy Administrator	Web Policy Administrator ロールを持つユーザ アカウントは、[Web Appliance Status] ページと、Configuration Master のすべてのページにアクセスできます。Web ポリシー管理者は、ID、アクセス ポリシー、暗号化ポリシー、ルーティング ポリシー、プロキシ バイパス、カスタム URL カテゴリ、および時間範囲を設定できます。Web ポリシー管理者は、設定を公開できません。	なし / なし
URL Filtering Administrator	URL Filtering Administrator ロールを持つユーザ アカウントは、URL フィルタリングだけを設定できます。	なし / なし
Email Administrator	Email Administrator ロールを持つユーザ アカウントは、Cisco IronPort スパム隔離など、[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 12-1　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 / スケジュール設定されたレポート機能
Help Desk User	Help Desk User ロールを持つユーザがアクセスできるのは次のものに制限されます。 • メッセージ トラッキング • Cisco IronPort スパム隔離の管理 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。このロールを持つユーザが Cisco IronPort スパム隔離の管理を行うには、そのスパム隔離へのアクセス権をイネーブルに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、[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、[Management Appliance] > [System Administration] > [User Roles] に移動して、ユーザ名をクリックします。 **（注）** Custom Email User ロールに割り当てられているユーザは、CLI にアクセスできません。 詳細については、「カスタム ユーザ ロール」（P.12-4）を参照してください。	なし / なし

一部のロール（Administrator、Operator、Guest、Technician、および Read-Only Operator）は、GUI と CLI の両方にアクセスできます。他のロール（Help Desk User、Email Administrator、Web Administrator、Web Policy Administrator、URL Filtering Administrator、およびカスタム ユーザ）は GUI だけにアクセスできます。

ユーザを認証するために LDAP ディレクトリを使用する場合は、ユーザ ロールに個々のユーザではなくディレクトリ グループを割り当てます。ユーザ ロールにディレクトリ グループを割り当てると、そのグループの各ユーザはそのユーザ ロールで定義された権限を受け取ります。詳細については、「外部ユーザ認証の使用方法」（P.12-18）を参照してください。

ユーザがスパム隔離にアクセスできるようにするには、そのアクセス権をイネーブルにする必要があります。「Cisco IronPort スパム隔離への管理者ユーザ アクセスの設定」（P.7-8）を参照してください。

カスタム ユーザ ロール

Administration 権限を持つユーザは、セキュリティ管理アプライアンスを使用してカスタム ロールに管理権限を委任できます。カスタム ロールは、事前定義されたユーザ ロールよりも、ユーザのアクセス権に対して柔軟な制御を行えます。

カスタム ユーザ ロールを割り当てたユーザは、アプライアンス、機能、またはエンド ユーザのサブセットに関して、ポリシーの管理またはレポートへのアクセスを行えます。たとえば、別の国にある組織の支社では、許容可能な使用ポリシーが組織の本社とは異なっている場合に、Web サービスに関して委任を受けた管理者に、支社のポリシーの管理を許可できます。カスタム ユーザ ロールを作成して、それらのロールにアクセス権を割り当てることで、管理を委任します。委任された管理者が表示および編集できるポリシー、機能、レポート、カスタム URL カテゴリなどを決定します。

詳細については、以下を参照してください。

- 「Custom Email User ロールについて」（P.12-5）
- 「Custom Web User ロールについて」（P.12-9）

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
- スパム隔離

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、[Management Appliance] タブ > [Centralized Services] メニューを使用して、[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）　カスタム ユーザ ロールは各 電子メール セキュリティ アプライアンスから直接作成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カスタム ユーザ ロールが使用できない機能への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、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Common Administration」の章にある「Managing Custom User Roles for Delegated Administration」を参照してください。

電子メール レポーティング

次のセクションで説明するように、電子メール レポートへのアクセス権をカスタム ユーザ ロールに付与できます。

セキュリティ管理アプライアンスの [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 [Email Security Monitor] ページを表示できます。

- Overview
- Incoming Mail
- Outgoing Destinations

- Outgoing Senders
- Internal Users
- DLP Incidents
- Content Filters
- Virus Types
- TLS Connections
- Outbreak Filters
- System Capacity
- Reporting Data Availability
- Scheduled Reports
- Archived Reports

メール ポリシー レポート

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 [Email Security Monitor] ページを表示できます。

- Overview
- Incoming Mail
- Outgoing Destinations
- Outgoing Senders
- Internal Users
- Content Filters
- Virus Types
- Outbreak Filters
- Reporting Data Availability
- Archived Reports

DLP レポート

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 [Email Security Monitor] ページを表示できます。

- DLP Incidents
- Reporting Data Availability
- Archived Reports

メッセージ トラッキング

カスタム ロールにメッセージ トラッキングへのアクセス権を付与すると、このロールを割り当てられたユーザは、セキュリティ管理アプライアンスによってトラッキングされたすべてのメッセージのステータスを表示できます。

DLP ポリシーに違反するメッセージ内の機密情報へのアクセスを制御するには、「メッセージ トラッキングでの DLP 機密情報へのアクセスの制御」（P.12-23）を参照してください。

セキュリティ管理アプライアンスでメッセージ トラッキングへのアクセスをイネーブルにするためのアプライアンスの設定方法など、メッセージ トラッキングの詳細については、「電子メール メッセージのトラッキング」を参照してください。

隔離

カスタム ロールに隔離へのアクセス権を付与すると、このロールを割り当てられたユーザは、この セキュリティ管理アプライアンスのスパム隔離メッセージを検索、表示、配信、または削除できます。

ユーザがスパム隔離にアクセスできるようにするには、そのアクセス権をイネーブルにする必要があります。「Cisco IronPort スパム隔離への管理者ユーザ アクセスの設定」（P.7-8）を参照してください。

セキュリティ管理アプライアンスからこの隔離へのアクセスをイネーブルにするためのアプライアンスの設定方法など、スパム隔離の詳細については、「Cisco IronPort スパム隔離の管理」の章を参照してください。

Custom Email User ロールの作成

電子メール レポーティング、メッセージ トラッキング、およびスパム隔離へのアクセスに対して、Custom Email User 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。

ステップ 1　[Management Appliance] > [System Administration] > [User Roles] を選択します。

ステップ 2　[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 [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。

（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。先頭をダッシュまたは数字にすることはできません。

ステップ 4　このロールに対してイネーブルにするアクセス権限を選択します。

ステップ 5　[Submit] をクリックして [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 [Email Reporting] カラムにある [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　このロールにスパム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イネーブルにします。「Cisco IronPort スパム隔離への管理者ユーザ アクセスの設定」（P.7-8）を参照してください。

Custom Email User ロールの編集

ステップ 1　[User Roles] ページでロール名をクリックし、[Edit Email User Role] ページを表示します。

ステップ 2　設定を編集します。

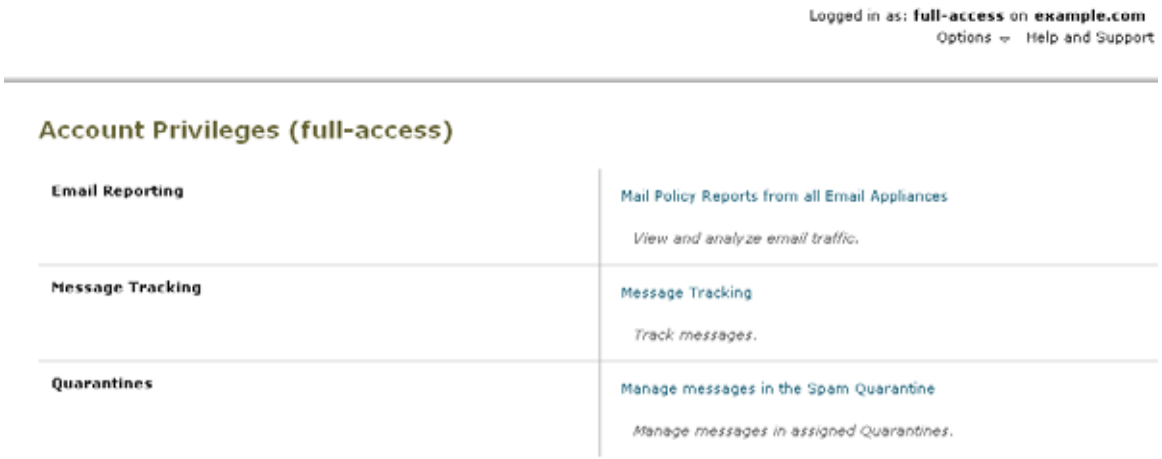
ステップ 3　変更を送信し、保存します。

ステップ 4　このロールにスパム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イネーブルにします。「Cisco IronPort スパム隔離への管理者ユーザ アクセスの設定」（P.7-8）を参照してください。

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、[Options] メニューで [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 12-1　Custom Email User ロールが割り当てられている委任管理者の [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] > [Configuration Master] > [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] > [Utilities] > [Publish Configuration Now] ページに移動して、可能な設定を表示することもできます。

（注） 公開権限を持つカスタム ロールを作成した場合、ユーザがログインすると、使用可能なメニューが表示されないことに注意してください。URL やポリシー タブが機能を持たないため、このようなユーザには公開メニューが表示されず、編集不可の固定画面が表示されます。つまり、どのカテゴリまたはポリシーも公開または管理できないユーザを作ってしまうことになります。

この問題の回避策としては、ユーザが公開はできるが、どのカテゴリまたはポリシーも管理できないようにする場合、どのポリシーでも使用されていないカスタム カテゴリを作成し、そのユーザに、そのカスタム カテゴリを管理する権限と公開する権限を付与する**必要があります**。このようにすると、ユーザがそのカテゴリで URL を追加または削除しても、他に影響が及びません。

カスタム ユーザ ロールを作成および編集して、Web 管理を委任できます。

- Custom Web User ロールの作成
- Custom Web User ロールの編集

Custom Web User ロールの作成

ステップ 1　[Management Appliance] > [System Administration] > [User Roles] を選択します。

ステップ 2　[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 [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　[Submit] をクリックして [User Roles] ページに戻ると、新しいユーザ ロールが表示されます。

（注）　Web レポーティングで匿名機能をイネーブルにしていた場合、Web レポーティングへのアクセス権を持つすべてのユーザ ロールには、インタラクティブなレポート ページで認識できないユーザ名とロールが表示されるようになります。第 5 章「中央集中型 Web レポーティングの使用方法」の Web レポートのスケジュール設定のセクションを参照してください。Administrator ロールの場合は例外的に、スケジュール設定されたレポートで実際のユーザ名を確認できます。匿名機能がイネーブルになっている場合、オペレータおよび Web 管理者によって作成されたスケジュール設定されたレポートは匿名になります。

（注）　[Web] > [Utilities] > [Security Services Display] > [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、[User Roles] ページでも対応する [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

ステップ 1　[User Roles] ページでロール名をクリックし、[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　[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。

[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、[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。[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。[Submit] をクリックして、[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。[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。[Submit] をクリックして、[User Roles] ページに戻ります。

[Users] ページ

次のセクションの詳細について	参照先
ユーザ	管理タスクの分散について Locally-Defined 管理ユーザの管理
[Reset Passwords] ボタン	ユーザに対する次回ログイン時のパスワード変更の義務付け
ローカル ユーザ アカウントとパスワードの設定	制限ユーザ アカウントとパスワードの設定
外部認証	外部ユーザ認証の使用方法
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

管理ユーザの認証の管理

認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。

- 「Locally-Defined 管理ユーザの管理」（P.12-11）
- 「外部ユーザ認証の使用方法」（P.12-18）

Locally-Defined 管理ユーザの管理

- 「Locally-Defined ユーザの追加」（P.12-11）
- 「Locally-Defined ユーザの編集」（P.12-12）
- 「Locally-Defined ユーザの削除」（P.12-12）
- 「ローカルに定義されたユーザのリストの表示」（P.12-12）
- 「パスワードの設定と変更」（P.12-13）
- 「制限ユーザ アカウントとパスワードの設定」（P.12-14）
- 「ユーザに対する次回ログイン時のパスワード変更の義務付け」（P.12-16）
- 「ローカル ユーザ アカウントのロックおよびロック解除」（P.12-17）

Locally-Defined ユーザの追加

外部認証を使用していない場合は、次の手順に従って、ユーザを セキュリティ管理アプライアンスに直接追加します。または、CLI で **userconfig** コマンドを使用します。

（注）　外部認証もイネーブルである場合は、ローカル ユーザ名が外部認証されたユーザ名と重複しないことを確認してください。

アプライアンスに作成できるユーザ アカウントの数に制限はありません。

ステップ 1　カスタム ユーザ ロールを割り当てる場合は、そのロールを先に定義しておくことを推奨します。「カスタム ユーザ ロール」（P.12-4）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、[Management Appliance] > [System Administration] > [Users] を選択します。

ステップ 3　[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 12-1 を参照してください。

新しい Email ロールまたは Web ロールをここに追加する場合は、ロールの名前を入力します。命名上の制限については、「Custom Email User ロールの作成」（P.12-7）または「Custom Web User ロールの作成」（P.12-9）を参照してください。

ステップ 7　パスワードを入力し、パスワードを再入力します。パスワードは、6 文字以上にする必要があります。

ステップ 8　変更を送信し、保存します。

ステップ 9　このページにカスタム ユーザ ロールを追加する場合は、この時点でそのロールに権限を割り当てます。「カスタム ユーザ ロール」（P.12-4）を参照してください。

Locally-Defined ユーザの編集

たとえば、パスワードを変更するには、次の手順を実行します。

ステップ 1　[Users] 一覧でユーザの名前をクリックします。

ステップ 2　ユーザに対して変更を行います。

ステップ 3　変更を送信し、保存します。

Locally-Defined ユーザの削除

ステップ 1　[Users] 一覧でユーザの名前に対応するゴミ箱のアイコンをクリックします。

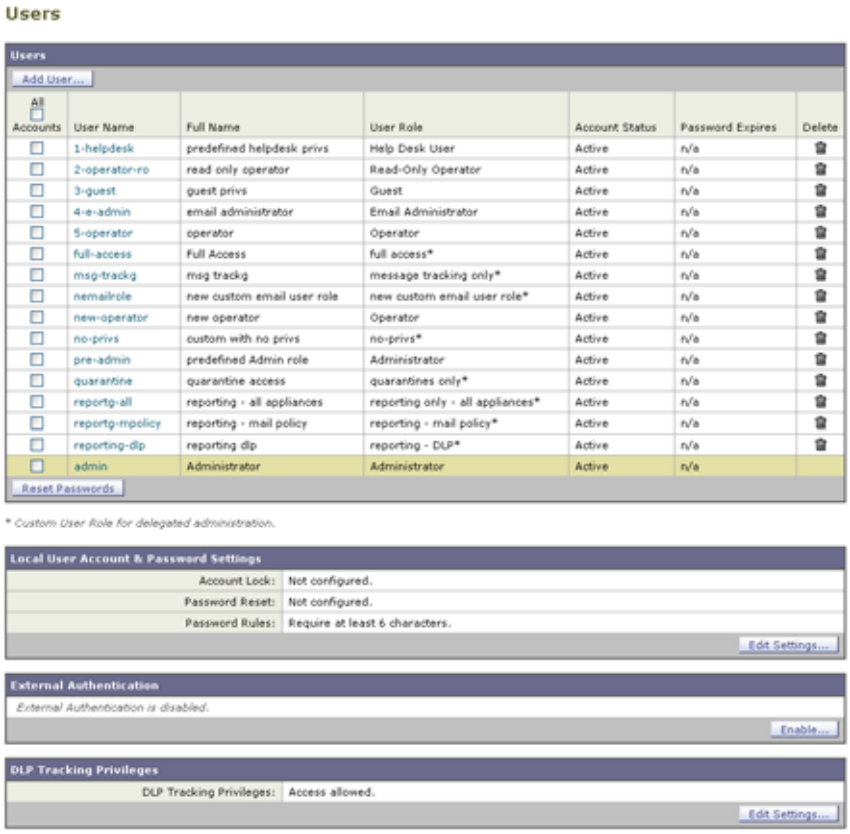
ステップ 2　表示される警告ダイアログで [Delete] をクリックして削除を確認します。

ステップ 3　[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

ステップ 1　セキュリティ管理アプライアンスで、[Management Appliance] > [System Administration] > [Users] を選択します。

図 12-2　[Users] ページの例



（注）　アスタリスクは、委任された管理に応じてユーザに割り当てられたカスタム ユーザ ロールを示します。ユーザのカスタム ロールが削除された場合は、[Unassigned] と赤く表示されます。カスタム ユーザ ロールの詳細については、「カスタム ユーザ ロール」（P.12-4）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 [Edit User] ページを使用します（詳細は、「Locally-Defined ユーザの編集」（P.12-12）を参照してください）。
- システムのデフォルト admin ユーザ アカウントのパスワードを変更するには、GUI の [Edit User] ページを使用するか（詳細は、「Locally-Defined ユーザの編集」（P.12-12）を参照してください）、CLI で `password` または `passwd` コマンドを使用します。admin ユーザ アカウントのパスワードを忘れた場合は、カスタマー サポート プロバイダーに問い合わせて、パスワードをリセットしてください。
- ユーザにパスワードの変更を強制するには、「ユーザに対する次回ログイン時のパスワード変更の義務付け」（P.12-16）を参照してください。
- GUI 右側上部の [Options] メニューをクリックして、[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。

[Change Password] ページで、古いパスワードを入力してから、新しいパスワードを入力し、確認のため、その新しいパスワードを再入力します。[Submit] をクリックして、ログアウトします。ログイン画面が表示されます。

制限ユーザ アカウントとパスワードの設定

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、Cisco IronPort アプライアンスに定義されたローカル ユーザに適用されます。次の設定値を設定できます。

- **ユーザ アカウントのロック。**ユーザがアカウントからロックアウトされるまでの、ログイン試行の失敗回数を定義できます。
- **パスワード期限の規則。**ログイン後にユーザがパスワードの変更を要求されるまでの、パスワードの使用期間を定義できます。
- **パスワードの規則。**どの文字が任意で、どの文字が必須かなど、ユーザが選択できるパスワードの種類を定義できます。

ステップ 1　[Management Appliance] > [System Administration] > [Users] を選択します。

ステップ 2　[Local User Account and Password Settings] セクションまでページを下にスクロールします。

ステップ 3　[Edit Settings] をクリックします。

ステップ 4　表 12-2 に示す設定値を設定します。

表 12-2　ローカル ユーザ アカウントとパスワードの設定

設定	説明
User Account Lock	ユーザが正常にログインできない場合に、ユーザ アカウントをロックするかどうかを決定します。アカウントがロックされるまでの、ログイン失敗回数を指定します。1 ～ 60 の範囲で任意の数字を入力できます。デフォルト値は 5 です。 アカウントのロックを設定する場合は、ログインしようとしているユーザに表示されるメッセージを入力します。7 ビットの ASCII 文字を使用して、テキストを入力します。このメッセージは、ユーザがロックされたアカウントに正しいパスワードを入力した場合だけ表示されます。 ユーザ アカウントがロックされた場合は、管理者が GUI の [Edit User] ページか、`userconfig` CLI コマンドを使用して、ロック解除できます。 ユーザが接続に使用したマシン、または接続の種類（SSH または HTTP）に関係なく、失敗したログイン試行はユーザごとに追跡されます。ユーザが正常にログインすると、失敗したログイン試行回数はゼロ（0）にリセットされます。 失敗したログイン試行の最大数に達したためにユーザ アカウントがロックアウトされた場合、アラートが管理者に送信されます。このアラートは「Info」重大度レベルに設定されます。 **（注）**　個々のユーザ アカウントを手動でロックすることもできます。「手動によるユーザ アカウントのロック」（P.12-17）を参照してください。

表 12-2　ローカル ユーザ アカウントとパスワードの設定（続き）

設定	説明
Password Reset	管理者がユーザのパスワードを変更後、ユーザにパスワードの変更を強制するかどうかを決定します。 また、パスワードの有効期限が切れた後に、ユーザにパスワードの変更を強制するかどうかを決定することもできます。ユーザによるパスワードの変更が必要になるまでの、パスワードの有効日数を入力します。1 ～ 366 の範囲で任意の数字を入力できます。デフォルトは 90 です。スケジュール外の時間に、ユーザにパスワードの変更を強制するには、「ユーザに対する次回ログイン時のパスワード変更の義務付け」（P.12-16）を参照してください。 パスワードの期限が切れた後、ユーザにパスワードの変更を強制する場合は、次回のパスワード期限切れについての通知を表示できます。期限切れの何日前に通知が行われるかを選択します。 パスワードが期限切れになると、ユーザは次回のログイン時にアカウント パスワードの変更を強制されます。 **（注）** ユーザ アカウントがパスワード チャレンジではなく SSH キーを使用している場合も、パスワードのリセット規則は適用されます。SSH キーを持つユーザ アカウントが期限切れになると、そのユーザは古いパスワードを入力するか、管理者に依頼して、パスワードを手動で変更し、アカウントに関連付けられたキーを変更してもらう必要があります。
Password Rules: Require at <number> least characters.	パスワードに含める最小文字数を入力します。 6 ～ 128 の範囲で任意の数字を入力できます。デフォルトは 6 です。
Password Rules: Require at least one number (0-9).	パスワードに 1 文字以上の数字を含める必要があるかどうかを決定します。

Password Rules:
 	
Require at least one special character.
	パスワードに 1 文字以上の特殊文字を含める必要があるかどうかを決定します。パスワードには、次の特殊文字を使用できます。
	
	`~ ?!@ # $ % ^ & * - _ + =`
	
	`¥ | / [ ] ( ) < > { } ` ' " ; : , .`

表 12-2　ローカル ユーザ アカウントとパスワードの設定（続き）

設定	説明
Password Rules: 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」
Password Rules: Ban reuse of the last <number> passwords.	ユーザにパスワードの変更を強制する場合に、最近使用したパスワードを選択できるかどうかを決定します。最近のパスワードの再利用を禁止した場合、再利用を禁止する最近のパスワードの個数を入力します。 1 ～ 15 の範囲で任意の数字を入力できます。デフォルトは 3 です。

ステップ 5　変更を送信し、保存します。

ユーザに対する次回ログイン時のパスワード変更の義務付け

すべての、または選択したユーザに、次回セキュリティ管理アプライアンスにアクセスしたときにパスワードを変更するように要求するには、次の手順を実行します。

ステップ 1　[Management Appliance] > [System Administration] > [Users] を選択します。

ステップ 2　[Users] セクションで、次回のログインでパスワードの変更が必要なユーザの横のチェックボックスを選択します。

ステップ 3　[Reset Passwords] をクリックします。

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、「制限ユーザ アカウントとパスワードの設定」（P.12-14）で説明されている [Password Reset] オプションを使用します。

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。「制限ユーザ アカウントとパスワードの設定」（P.12-14）を参照してください。
- 管理者はユーザ アカウントを手動でロックできます。「手動によるユーザ アカウントのロック」（P.12-17）を参照してください。

[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

ステップ 1　初回のみ：アプライアンスを設定して、ユーザ アカウントのロックをイネーブルにします。

a. [Management Appliance] > [System Administration] > [Users] に移動します。

b. [Local User Account & Password Settings] セクションで、[Edit Settings] をクリックします。

c. [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　[Management Appliance] > [System Administration] > [Users] に移動して、ユーザ名をクリックします。

（注）　admin アカウントをロックする前に、ロック解除できることを確認してください。「ユーザ アカウントのロック解除」（P.12-17）の（注）を参照してください。

ステップ 3　[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、[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、[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 ポートを使用したアプライアンスへのアクセスの詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Setup and Installation」の章を参照してください。

外部ユーザ認証の使用方法

ユーザ情報をネットワーク上の LDAP または RADIUS ディレクトリに保存した場合、セキュリティ管理アプライアンスにログインするユーザの認証に外部ディレクトリを使用するように Cisco IronPort アプライアンスを設定できます。

（注）　導入における、ローカル認証と外部認証の両方の使用については、次のとおりです。

- セキュリティ管理アプライアンスにローカル ユーザ ディレクトリも追加する場合は、ローカル ユーザ名が外部認証されたユーザ名と重複していないことを確認してください。
- 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。

認証に外部ディレクトリを使用するようにアプライアンスをセットアップするには、次の手順を実行します。

- Web インターフェイスを使用するには、以下を参照してください。
  - 「LDAP 認証の設定」（P.12-18）
  - 「RADIUS 認証のイネーブル化」（P.12-18）
- コマンドライン インターフェイス（CLI）を使用するには、コマンドライン プロンプトで **userconfig** コマンドおよび **external** サブコマンドを使用します。

LDAP 認証の設定

LDAP 認証を設定するには、「LDAP を使用した管理ユーザの外部認証の設定」（P.10-13）を参照してください。

RADIUS 認証のイネーブル化

ユーザの認証に RADIUS ディレクトリを使用し、ユーザのグループを Cisco IronPort ロールに割り当てることもできます。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 Cisco IronPort ユーザ ロールに割り当てるために CLASS 属性を使用します）。AsyncOS は、RADIUS サーバと通信するために Password Authentication Protocol（PAP; パスワード認証プロトコル）と Challenge Handshake Authentication Protocol（CHAP; チャレンジ ハンドシェイク認証プロトコル）の 2 つの認証プロトコルをサポートします。

RADIUS ユーザを Cisco IronPort ユーザ ロールに割り当てるには、最初に RADIUS サーバで `<radius-group>` という文字列値を使用して CLASS 属性を設定します（これは Cisco IronPort ユーザ ロールにマップされます）。CLASS 属性には文字、数字、およびダッシュを含めることができますが、先頭にダッシュを使用することはできません。AsyncOS は CLASS 属性で複数の値をサポートしません。CLASS 属性またはマップされていない CLASS 属性がないグループに属する RADIUS ユーザはアプライアンスにログインできません。

アプライアンスが RADIUS サーバと通信できない場合、ユーザはアプライアンスのローカル ユーザ アカウントでログインできます。

（注）　外部ユーザが RADIUS グループのユーザ ロールを変更する場合、外部ユーザはアプライアンスからログアウトし、再びログインする必要があります。このユーザは新しいロールの権限を持ちます。

ステップ 1　[Management Appliance] > [System Administration] > [Users] ページで、[Enable] をクリックします。

ステップ 2　[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 サーバの共有秘密パスワードを入力します。

（注）　Cisco IronPort アプライアンスのクラスタに対して外部認証をイネーブルにするには、クラスタ内のすべてのアプライアンスで同じ共有秘密パスワードを入力します。

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　RADIUS 認証として PAP を使用するか、CHAP を使用するかを選択します。

ステップ 9　また、[Add Row] をクリックして別の RADIUS サーバを追加することもできます。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。

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。

ステップ 11　RADIUS ユーザのグループを Cisco IronPort ロールにマップするかどうか、またはすべての RADIUS ユーザに Administrator ロールを割り当てるかどうかを選択します。RADIUS グループを Cisco IronPort ロールにマップすることを推奨します。

ステップ 12　RADIUS グループを Cisco IronPort ロールにマップすることを選択した場合は、グループの RADIUS CLASS 属性を入力し、その CLASS 属性を持つユーザのロールを選択します。

ステップ 13　また、[Add Row] をクリックして別の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ユーザの各グループに対してステップ 11 とステップ 12 を繰り返します。

ステップ 14　変更を送信し、保存します。

セキュリティ管理アプライアンスへのアクセスに対する追加の制御

IP ベースのネットワーク アクセスの設定

組織がリモート ユーザに逆プロキシを使用する場合、アプライアンスに直接接続するユーザ、および逆プロキシを介して接続するユーザのためのアクセス リストを作成することで、ユーザがどの IP アドレスからセキュリティ管理アプライアンスにアクセスするのかを制御できます。

直接接続

セキュリティ管理アプライアンスに接続できるマシンの IP アドレス、サブネット、または CIDR アドレスを指定できます。ユーザは、アクセス リストの IP アドレスを持つすべてのマシンから、アプライアンスにアクセスできます。リストに含まれていないアドレスからアプライアンスに接続しようとするユーザは、アクセスを拒否されます。

プロキシ経由の接続

組織のネットワークで、リモート ユーザのマシンとセキュリティ管理アプライアンスの間で逆プロキシが使用されている場合、AsyncOS では、アプライアンスに接続できるプロキシの IP アドレスのアクセス リストを作成できます。

逆プロキシを使用している場合でも、AsyncOS は、ユーザ接続が許可されている IP アドレスのリストと照合して、リモート ユーザのマシンの IP アドレスを検証します。リモート ユーザの IP アドレスを電子メール セキュリティ アプライアンスに送信するには、プロキシで `x-forwarded-for` HTTP ヘッダーをアプライアンスへの接続要求に含める必要があります。

`x-forwarded-for` ヘッダーは非 RFC 標準 HTTP ヘッダーであり、形式は次のとおりです。

```
x-forwarded-for: client-ip, proxy1, proxy2,... CRLF.
```

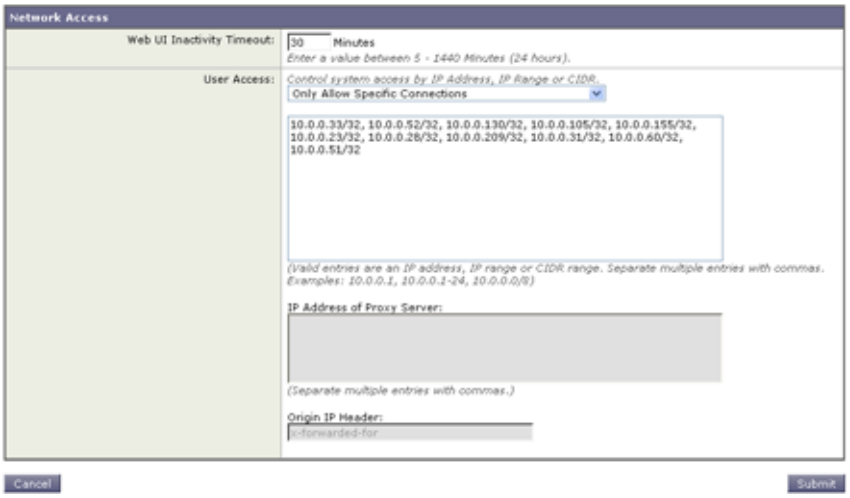
このヘッダーの値はカンマ区切りの IP アドレスのリストであり、左端のアドレスがリモート ユーザ マシンのアドレスで、その後に、接続要求を転送した一連の各プロキシのアドレスが続きます。（ヘッダー名は設定可能です）。セキュリティ管理アプライアンスは、ヘッダーから取得したリモート ユーザの IP アドレスおよび接続プロキシの IP アドレスを、アクセス リスト内の許可されたユーザ IP アドレスおよびプロキシ IP アドレスと照合します。

（注）　AsyncOS は、`x-forwarded-for` ヘッダーで IPv4 アドレスだけをサポートします。

アクセス リストの作成

GUI の [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 12-3 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 [Network Access] ページを示しています。

図 12-3　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。

- **[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。
- **[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]。**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、[Proxy Server] フィールドのアクセス リストの IP アドレスに含まれている。
  - プロキシで、接続要求に `x-forwarded-header` HTTP ヘッダーが含まれている。
  - `x-forwarded-header` の値が空ではない。
  - リモート ユーザの IP アドレスが `x-forwarded-header` に含まれ、それがアクセス リスト内の IP アドレス、IP 範囲、または CIDR 範囲と一致する。
- **[Only Allow Specific Connections Directly or Through Proxy]。**このモードは、ユーザの IP アドレスが、アクセス リストに含まれている IP アドレス、IP 範囲、または CIDR 範囲と一致する場合に、ユーザの逆プロキシを介した、あるいは直接的なアプライアンスへの接続を許可します。プロキシを介した接続の条件は、[Only Allow Specific Connections Through Proxy] モードの場合と同じです。

次のいずれかの条件に該当する場合、変更をサブミットおよびコミットした後に、アプライアンスにアクセスできなくなる可能性があります。

- [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。
- [Only Allow Specific Connections] を選択し、アプライアンスに現在接続されているプロキシの IP アドレスがプロキシ リストになく、元の IP ヘッダーの値が許可された IP アドレスのリストにない場合。
- [Only Allow Specific Connections Directly or Through Proxy] を選択し、次が当てはまる場合。
  - 元の IP ヘッダーの値が許可される IP アドレスのリストにない

    または

- 元の IP ヘッダーの値が許可される IP アドレスのリストになく、アプライアンスに接続されているプロキシの IP アドレスが許可されるプロキシのリストにない。

アクセス リストを修正せずに続行した場合、ユーザが変更を確定すると、AsyncOS はアプライアンスからユーザのマシンまたはプロキシを切断します。

ステップ 1　[System Administration] > [Network Access] を選択します。

ステップ 2　[Edit Settings] をクリックします。

ステップ 3　アクセス リストの制御モードを選択します。

ステップ 4　ユーザがアプライアンスへの接続が許可される IP アドレスを入力します。

IP アドレス、IP アドレス範囲または CIDR 範囲を入力できます。複数のエントリを区切るには、カンマを使用します。

ステップ 5　プロキシ経由の接続が許可されている場合は、次の情報を入力します。

- アプライアンスへの接続が許可されているプロキシの IP アドレス。複数のエントリを区切るには、カンマを使用します。
- プロキシがアプライアンスに送信する発信元の IP ヘッダーの名前。これには、リモート ユーザ マシンの IP アドレスと、要求を転送したプロキシ サーバの IP アドレスが含まれます。デフォルトでは、ヘッダーの名前が `x-forwarded-for` です。

ステップ 6　変更を送信し、保存します。

Web UI セッション タイムアウトの設定

セキュリティ管理アプライアンスの Web UI から AsyncOS が、非アクティブなユーザをログアウトするまでの時間を指定できます。この Web UI セッション タイムアウトは、admin を含めて、すべてのユーザに適用され、また HTTP セッションと HTTPS セッションの両方に使用されます。

AsyncOS によってユーザがログアウトされると、アプライアンスはユーザの Web ブラウザをログイン ページにリダイレクトします。

（注）　Web UI セッション タイムアウトは IronPort スパム隔離セッションには適用されません。このセッションには 30 分のタイムアウトが設定されており、変更できません。

ステップ 1　[System Administration] > [Network Access] ページを使用します。

ステップ 2　[Edit Settings] をクリックします。

ステップ 3　ユーザが非アクティブ状態になった後、何分経過後にログアウトされるかを入力します。タイムアウト時間には 5 ～ 1440 分を定義できます。

ステップ 4　変更を送信し、保存します。

メッセージ トラッキングでの DLP 機密情報へのアクセスの制御

データ消失防止（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 [Message Details] ページにある [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。

ステップ 1　[Management Appliance] > [System Administration] > [Users] ページに移動します。

ステップ 2　[DLP Tracking Privileges] セクションで、[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、[Management Appliance] > [Centralized Services] で中央集中型電子メール メッセージ トラッキング機能をイネーブルにする必要があります。

管理ユーザ アクティビティの表示

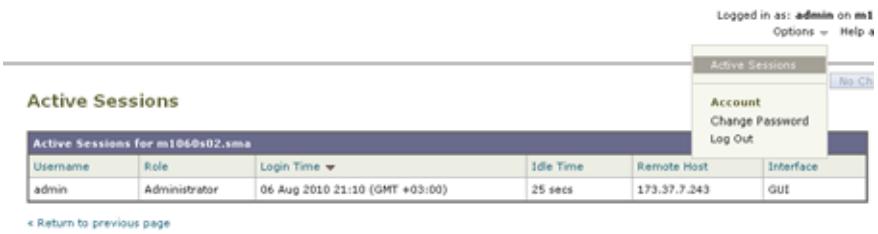
- 「Web を使用したアクティブなセッションの表示」（P.12-23）
- 「コマンドライン インターフェイスを介した管理ユーザ アクティビティの表示」（P.12-24）

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。

ステップ 1　ウィンドウの右上から、[Options] > [Active Sessions] を選択します。

図 12-4　[Active Sessions] メニュー



[Active Sessions] ページから、ユーザ名、ユーザが持っているロール、ユーザのログイン時間、アイドル時間、およびユーザがコマンドラインと GUI のどちらからログインしたかを表示できます。

コマンドライン インターフェイスを介した管理ユーザ アクティビティの表示

次に、アプライアンスへの複数ユーザ アクセスをサポートするコマンドを示します。

- **who** コマンドは、CLI からシステムにログインしたすべてのユーザ、ログイン時間、アイドル時間、およびユーザがログインしたリモート ホストを一覧表示します。

```
mail3.example.com> who

Username Login Time Idle Time Remote Host What
======== ========== ========= =========== ====
admin  03:27PM  0s   10.1.3.201 cli
```

- whoami コマンドは、現在ログインしているユーザのユーザ名および氏名と、ユーザが属しているグループを表示します。

```
mail3.example.com> whoami

Username: admin
Full Name: Administrator
Groups: admin, operators, config, log, guest
```

- last コマンドは、アプライアンスに最近ログインしたユーザを表示します。リモート ホストの IP アドレス、ログイン、ログアウト、および合計時間も表示されます。

```
mail3.example.com> last

Username Remote Host Login Time  Logout Time  Total Time
======== =========== ========== ========== ==========
admin  10.1.3.67 Sat May 15 23:42 still logged in 15m
admin  10.1.3.67 Sat May 15 22:52 Sat May 15 23:42 50m
admin  10.1.3.67 Sat May 15 11:02 Sat May 15 14:14 3h 12m
admin  10.1.3.67 Fri May 14 16:29 Fri May 14 17:43 1h 13m
shutdown         Fri May 14 16:22
shutdown         Fri May 14 16:15
admin  10.1.3.67 Fri May 14 16:05 Fri May 14 16:15 9m
admin  10.1.3.103 Fri May 14 16:12 Fri May 14 16:15 2m
admin  10.1.3.103 Thu May 13 09:31 Fri May 14 14:11 1d 4h 39m
admin  10.1.3.135 Fri May 14 10:57 Fri May 14 10:58 0m
admin  10.1.3.67 Thu May 13 17:00 Thu May 13 19:24 2h 24m
```

CHAPTER 13

一般的な管理タスク

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 [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 9 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、[Monitor] メニューでアプライアンスのステータス モニタリング機能を使用することができます。

（注） この章で説明する機能やコマンドの中には、ルーティングの優先順位に影響を及ぼすものがあります。詳細については、「IP アドレス、インターフェイス、およびルーティング」（P.B-3）を参照してください。

機能キーでの作業

メイン セキュリティ管理アプライアンスで、GUI を使用して [Management Appliance] > [System Administration] > [Feature Keys] を選択して（またはコマンド ライン プロンプトから **featurekey** コマンドで）キーを入力し、関連する機能をイネーブルにします。

キーは、アプライアンスのシリアル番号に固有のものであり、またイネーブルする機能にも固有です。1 つのシステムのキーを、別のシステムで再利用することはできません。キーを間違って入力した場合は、エラー メッセージが生成されます。

Cisco IronPort カスタマー サポートは、システム上で特定の機能をイネーブルにするキーを提供する場合があります。

[Feature Keys] ページと [Feature Key Settings] ページの 2 つのページで、機能キーの機能が提供されます。

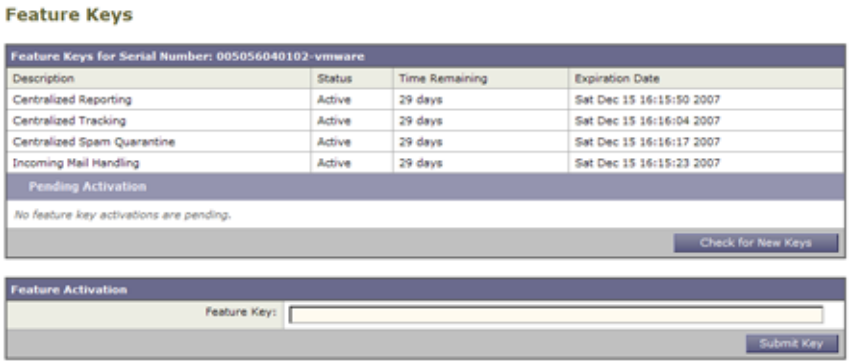
[Feature Keys] ページ

セキュリティ管理アプライアンスにログインし、[Management Appliance] > [System Administration] > [Feature Keys] を選択します。[Feature Keys] ページでは、次の作業を実行します。

- アプライアンスのアクティブな機能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機能キーを表示する。
- 発行された新しいキーを検索する。
- 機能キーをインストールする。

[Feature Keys for Serial Number: <*Serial Number*>] セクションには、アプライアンスに対してイネーブルとなっている機能の一覧が表示されます。[Pending Activation] セクションには、アプライアンスに対して発行され、まだアクティベートされていない機能キーの一覧が表示されます。デフォルトでは、アプライアンスは、新しいキーを定期的に確認します。アプライアンス設定を変更すると、この動作を変更できます。さらに、[Check for New Keys] ボタンをクリックして、保留中のキーの一覧をリフレッシュできます。

図 13-1　　[Feature Keys] ページ



新しい機能キーを手動で追加するには、[Feature Key] フィールドにキーを貼り付けるか、または入力し、[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、機能キーがリストに追加されます。

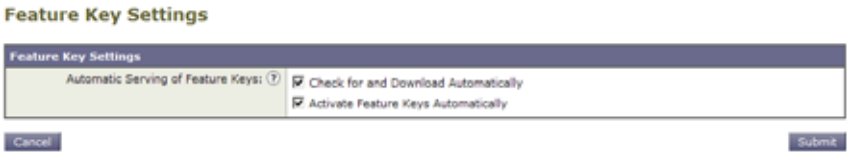
[Pending Activation] リストの新しい機能キーをアクティベートするには、そのキーを選択し（[Select] チェックボックスを選択）、[Activate Selected Keys] をクリックします。

新しいキーが発行されたときに、キーを自動的にダウンロードおよびインストールするように、アプライアンスを設定できます。この場合、[Pending Activation] リストは常に空白になります。

[Feature Key Settings] ページ

[Management Appliance] > [System Administration] > [Feature Key Settings] ページを使用して、アプライアンスが新しい機能キーがあるか確認し、ダウンロードするかどうか、またキーが自動的にアクティベートされるかどうかを制御します。

図 13-2　[Feature Key Settings] ページ



期限切れ機能キー

アクセスしようとしている機能の機能キーの有効期限が切れている場合は、シスコ担当者または他のカスタマー サポート組織までご連絡ください。

CLI コマンドを使用したメンテナンス作業の実行

ここで説明する操作とコマンドを利用すると、セキュリティ管理アプライアンス上でメンテナンスに関連する作業を実行できます。ここでは、次の操作とコマンドについて説明します。

- **shutdown**
- **reboot**
- **suspend**
- **offline**
- **resume**
- **resetconfig**
- **version**

セキュリティ管理アプライアンスのシャットダウン

セキュリティ管理アプライアンスをシャットダウンするには、[Management Appliance] > [System Administration] > [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 [System Administration] メニューで利用可能な [Shutdown/Reboot] ページを使用するか、CLI で reboot コマンドを使用します。

アプライアンスをリブートすると、AsyncOS が再起動されるため、アプライアンスの電源を安全にオフにし、アプライアンスをリブートできます。アプライアンスをシャットダウンする遅延値を入力する必要があります。デフォルト遅延値は 30 秒です。AsyncOS では、その遅延値の間はオープン中の接続を完了できます。その遅延値を超えると、オープン中の接続が強制的に閉じられます。アプライアンスを再起動しても、配信キューのメッセージは失われません。

セキュリティ管理アプライアンスをメンテナンス状態にする

システム メンテナンスを行う場合は、セキュリティ管理アプライアンスをオフライン状態にします。suspend および offline コマンドは、AsyncOS をオフライン状態にします。オフライン状態では、次のようになります。

- 着信電子メール接続は受け入れられません。
- 発信電子メール配信は停止されます。
- ログ転送は停止されます。
- CLI はアクセス可能のままになります。

オフライン状態にするアプライアンスの遅延値を入力する必要があります。デフォルト遅延値は 30 秒です。AsyncOS では、その遅延値の間はオープン中の接続を完了できます。その遅延値を超えると、オープン中の接続が強制的に閉じられます。オープン中の接続がない場合は、すぐにオフライン状態になります。

（注）　**suspend** コマンドと **offline** コマンドの相違点は、**suspend** コマンドはマシンがリブートされた後でもその状態を保つことです。**suspend** コマンドを発行してからアプライアンスをリブートする場合は、**resume** コマンドを使用してシステムをオンライン状態に戻す必要があります。

関連項目：

- 『*Cisco IronPort AsyncOS for Email Security Advanced User Guide*』の「Suspending Email Delivery」、「Resuming Email Delivery」、「Suspending Receiving」、および「Resuming Receiving」

suspend および offline コマンド

```
mail3.example.com> suspend

Enter the number of seconds to wait before abruptly closing connections.
[30]> 45

Waiting for listeners to exit...
Receiving suspended.
Waiting for outgoing deliveries to finish...
Mail delivery suspended.

mail3.example.com> offline

Enter the number of seconds to wait before abruptly closing connections.
[30]> 45
```

```
Waiting for listeners to exit...
Receiving suspended.
Waiting for outgoing deliveries to finish...
Mail delivery suspended.
```

オフライン状態からの再開

resume コマンドは、**suspenddel** コマンドまたは **suspend** コマンドを使用した後に、AsyncOS を通常の動作状態に戻します。

resume コマンド

```
mail3.example.com> resume

Receiving resumed.
Mail delivery resumed.
mail3.example.com>
```

出荷時の初期状態へのリセット

アプライアンスを物理的に移動する際、出荷時の初期状態で始めなければならない場合があります。[Management Appliance] > [System Administration] > [Configuration File] ページの [Reset Configuration] セクションの [Reset] ボタンか、**resetconfig** コマンドを使用すると、すべての AsyncOS 設定値が出荷時の初期状態にリセットされます。このコマンドは非常に破壊的であるため、ユニットを移動する場合や、設定の問題を解決する最後の手段としてのみ使用してください。設定のリセット後は、システム セットアップ ウィザードを実行することを推奨します。

（注） resetconfig コマンドは、アプライアンスがオフライン状態であるときにのみ機能します。**resetconfig** コマンドが完了すると、アプライアンスは自動的にオンライン状態に戻ります。**resetconfig** コマンドを実行する前に電子メールの送信が中断された場合は、**resetconfig** コマンドが完了したときに電子メールの送信が再試行されます。

警告 **resetconfig コマンドを実行すると、すべてのネットワーク設定が出荷時デフォルト値に戻ります。場合によっては、CLI から切断され、アプライアンスに接続するために使用したサービス（FTP、Telnet、SSH、HTTP、HTTPS）がディセーブルにされ、userconfig コマンドで作成した追加のユーザ アカウントが削除されます。このコマンドは、シリアル インターフェイスを使用するか、またはデフォルトの Admin ユーザ アカウントから管理ポート上のデフォルト設定を使用して CLI に再接続できない場合は使用しないでください。**

resetconfig コマンド

```
mail3.example.com> offline

Delay (seconds, minimum 30):
[30]> 45
```

```
Waiting for listeners to exit...
Receiving suspended.
Waiting for outgoing deliveries to finish...
Mail delivery suspended.

mail3.example.com> resetconfig

Are you sure you want to reset all configuration values? [N]> Y

All settings have been restored to the factory default.
```

AsyncOS のバージョン情報の表示

ステップ 1　セキュリティ管理アプライアンスで、[Management Appliances] > [Centralized Services] > [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、[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。

セキュリティ管理アプライアンスのバックアップ

データのバックアップについて

バックアップ データには、Web トラッキングおよびトレンド レポーティング、電子メール レポーティング、メッセージ トラッキング、Cisco IronPort スパム隔離、および Safelist/Blocklist データが含まれます。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。

セキュリティ管理アプライアンスでは、アクティブなデータ セットを「ソース」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コピーし、元の「ソース」セキュリティ管理アプライアンスの中断を最小限に抑えることができます。セキュリティ管理アプライアンスは、マシンを「プライマリ」または「バックアップ」アプライアンスではなく、「ソース」アプライアンスと「ターゲット」アプライアンスと見なします。つまり、データを送信するマシンが「ソース」であり、スケジュール設定されたバックアップの一部として、別のセキュリティ管理アプライアンスからデータを受信するアプライアンスが「ターゲット」です。

データの転送が完了すると、2 台のボックス上のデータが同一になります。バックアップ機能では **backupconfig** コマンドを使用して、セキュリティ管理アプライアンスの GUI を使用せずにデータ ファイルをバックアップできます。また、スケジュール設定されたバックアップと実行中のバックアップの表示またはキャンセル、バックアップ ステータスの確認、またはバックアップをリモート マシンにスケジュール設定できるかどうかの確認を行うこともできます。

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	セキュリティ管理データ用のこのリリースの AsyncOS は、セキュリティ管理用の同じリリースの AsyncOS を実行している別のセキュリティ管理アプライアンスに対してのみバックアップできます。バージョンが一致しない場合は、バックアップのスケジュールを設定する前に、ターゲット セキュリティ管理アプライアンスをアップグレードしてください。
ネットワーク上のターゲット アプライアンス	ターゲット アプライアンスがネットワーク上に設定されている必要があります。 ターゲット アプライアンスが新規の場合は、システム セットアップ ウィザードを実行して必要な情報を入力します。手順については、第 2 章「セットアップ、インストール、および基本設定」を参照してください。
アプライアンス間の通信	ソースおよびターゲット セキュリティ管理アプライアンスは、SSH を使用して通信できるようになっている必要があります。このため次のようになります。 • 両方のアプライアンスのポート 22 を開いておく必要があります。デフォルトでは、このポートはシステム セットアップ ウィザードを実行すると開きます。 • ドメイン ネーム サーバ（DNS）で、A レコードと PTR レコードの両方を使用して、両方のアプライアンスのホスト名を解決できる必要があります。

制約事項	要件
アプライアンス キャパシティ	ターゲット アプライアンスのキャパシティが、ソース アプライアンスのキャパシティと同等以上である必要があります。ターゲット アプライアンスのデータの各タイプに割り当てられているディスク領域は、ソース アプライアンスの対応する割り当て未満にできません。 **（注）** すべてのデータのバックアップに十分なスペースがターゲット上にあれば、大きいソースから小さいターゲット セキュリティ管理アプライアンスへのバックアップをスケジュール設定できます。たとえば、ソース アプライアンスが M1060 で、小さいほうの M650 がターゲットの場合、大きいほうの M1060 で割り当てられているスペースを削減して、小さいほうの M650 アプライアンスで使用可能なスペースと一致するようにしてください。ディスク領域の割り当てについては、「ディスク使用量の管理」（P.13-58）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。

完了したバックアップの所要時間

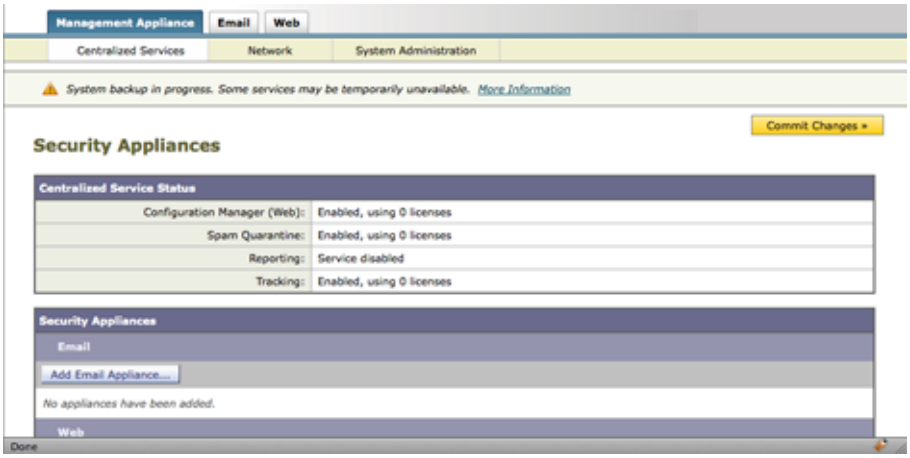
バックアップ中のサービスのアベイラビリティ

バックアップ プロセスのフェーズと、それらがサービスのアベイラビリティに及ぼす影響は次のとおりです。

- フェーズ 1：バックアップ プロセスのフェーズ 1 は、ソース アプライアンスとターゲット アプライアンス間のデータの転送で開始されます。データの転送中、ソース アプライアンスでのサービスは実行されたままになるため、データ収集をそのまま継続できます。ただし、ターゲット アプライアンスではサービスがシャットダウンされます。ソースからターゲット アプライアンスへのデータの転送が完了すると、フェーズ 2 が開始されます。
- フェーズ 2：フェーズ 2 が始まると、ソース アプライアンスでサービスがシャットダウンされます。最初のシャットダウンから、ソースおよびターゲット アプライアンスの間でのデータ転送中に収集された相違点がターゲット アプライアンスにコピーされ、サービスがソースとターゲットの両方のバックアップに戻されます。これにより、ソース アプライアンス上で最大の稼働時間を維持でき、いずれかのアプライアンスのデータが損失することがなくなります。

バックアップ中に、データのアベイラビリティ レポートが機能しなくなる場合があります。また、メッセージ トラッキング結果を表示すると、各メッセージのホスト名に「未解決」というラベルが付くことがあります。

レポートをスケジュール設定しようとしているときに、バックアップが進行中であることを忘れていた場合は、[Management Appliance] > [Centralized Services] を選択して、システムのステータスを確認できます。このウィンドウには、システムのバックアップが進行中であるという警告が表示されます。



バックアップ プロセスの中断

（注）　バックアップの実行中にソース アプライアンスの予期しないリブートがあっても、ターゲット アプライアンスはこの停止を認識しません。ターゲット アプライアンスでバックアップをキャンセルする必要があります。

バックアップ プロセスの中断があり、そのバックアップ プロセスが完了していない場合、バックアップを次に試行したときに、セキュリティ管理アプライアンスは停止した部分からバックアップ プロセスを開始できます。

進行中のバックアップをキャンセルすることは推奨されません。これは、既存のデータが不完全になり、エラーが発生した場合は、次のバックアップが完了するまで使用できないことがあります。進行中のバックアップのキャンセルが必要な場合は、できるだけ早く完全バックアップを実行し、常に使用可能な現在のバックアップを確保してください。

単一または定期バックアップのスケジュール設定

単一または定期バックアップを事前設定した時間に行うようにスケジュール設定できます。

（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。

ステップ 1　管理者として SSH セッションにログインします。

ステップ 2　コマンド プロンプトで **backupconfig** と入力し、Enter を押します。

実行する操作を選択します。

- [View]：スケジュール設定したバックアップを確認できます。
- [Verify]：バックアップをリモート マシンでスケジュール設定できるかどうかを確認します。
- [Schedule]：アプライアンスにバックアップをスケジュール設定します。
- [Cancel]：スケジュール設定されたバックアップをキャンセルします。
- [Status]：実行中のバックアップのステータスを表示します。
- [Setup]：バックアップ パラメータを設定します。

ステップ 3　ソース アプライアンスおよびターゲット アプライアンス間の接続が低速である場合は、データ圧縮をオンにします。

setup と入力して、Y を押します。

ステップ 4　**Schedule** と入力して、Enter を押します。

ステップ 5　ターゲットセキュリティ管理アプライアンスの IP アドレスを入力します。

ステップ 6　ターゲット アプライアンスを識別する有効な名前を入力します（最大 20 文字）。

ステップ 7　ターゲット アプライアンスの管理ユーザの名前およびパスワードを入力します。

ステップ 8　バックアップするデータに関するプロンプトに応答します。

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バックアップできます。

- スパム隔離
- 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

これで、セキュリティ管理アプライアンスはターゲット マシンの存在を確認し、ターゲット マシンにデータを受けるのに十分なスペースがあるかどうかを判別します。

ターゲット マシンのスペースが不十分な場合は、次のエラー メッセージが表示されます。「Backup cannot be scheduled.Reason: There is not enough space for Spam Quarantine, Email Tracking, Web Tracking, Reporting.Please increase disk allocation for these services on the target machine」。データは転送されません。

ターゲット マシンが検証されると、次の選択肢が表示されます。

1. [Setup Repeating Backup Schedule]：定期バックアップをスケジュール設定できます。
2. [Schedule a single backup]：単一バックアップをスケジュール設定できます。
3. [Start a Single Backup Now]：即時バックアップを開始できます。

ステップ 9　単一バックアップをスケジュール設定する場合は、2 を入力して、Enter を押します。

ステップ 10　定期バックアップをスケジュール設定する場合は、次の手順を実行します。

a. **1** を入力して、Enter を押します。

b. 次の選択肢が表示されます。`1.[Daily]、2.[Weekly]、3.[Monthly]。`

c. 定期バックアップの時間枠を選択し、Enter を押します。

ステップ 11　バックアップを開始する特定の日付または日および時間を入力して、Enter を押します。

ステップ 12　バックアップ プロセスの名前を入力します。

ステップ 13　バックアップが正常にスケジュール設定されたことを確認します。コマンド プロンプトで **View** または **Status** と入力して、Enter を押します。

ステップ 14　「その他の重要なバックアップ タスク」（P.13-13）も参照してください。

即時バックアップの開始

インスタント バックアップは、CLI で **backupconfig** コマンドを開始するとすぐに実行されます。

（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。

ステップ 1　管理者として SSH セッションにログインします。

ステップ 2　コマンド プロンプトで **backupconfig** と入力し、Enter を押します。

実行する操作を選択します。

- `[View]`：スケジュール設定したバックアップを確認できます。
- `[Verify]`：バックアップをリモート マシンでスケジュール設定できるかどうかを確認します。
- `[Schedule]`：アプライアンスにバックアップをスケジュール設定できます。
- `[Cancel]`：スケジュール設定されたバックアップをキャンセルします。
- `[Status]`：実行中のバックアップのステータスを確認できます。
- `[Setup]`：バックアップ パラメータを設定します。

ステップ 3　ソース アプライアンスおよびターゲット アプライアンス間の接続が低速である場合は、データ圧縮をオンにします。

setup と入力して、Y を押します。

ステップ 4　**Schedule** と入力して、Enter を押します。

ステップ 5　ターゲットセキュリティ管理アプライアンスの IP アドレスを入力します。

ステップ 6　ターゲット アプライアンスを識別する有効な名前を入力します（最大 20 文字）。

ステップ 7　ターゲット アプライアンスの管理ユーザの名前およびパスワードを入力します。

ステップ 8　バックアップするデータに関するプロンプトに応答します。

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バックアップできます。

- スパム隔離
- 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 データを含む）
- レポーティング（電子メール）

- セーフリスト / ブロックリスト

これで、セキュリティ管理アプライアンスはターゲット マシンの存在を確認し、ターゲット マシンにデータを受けるのに十分なスペースがあるかどうかを判別します。

ターゲット マシンのスペースが不十分な場合は、次のエラー メッセージが表示されます。「Backup cannot be scheduled.Reason: There is not enough space for Spam Quarantine, Email Tracking, Web Tracking, Reporting.Please increase disk allocation for these services on the target machine」。データは転送されません。

ターゲット マシンが検証されると、コンソールに次の選択肢が表示されます。

1. [Setup Reoccurring Backup]：定期バックアップをスケジュール設定できます。
2. [Schedule a Single backup]：単一バックアップをスケジュール設定できます。
3. [Start a Single Backup Now]：即時バックアップを開始できます。

ステップ 9　**3** と入力して、Enter を押します。

ステップ 10　バックアップ ジョブの有効な名前を入力します。

バックアップ プロセスが数分で開始し、ソース マシンからターゲット マシンへのデータの転送が開始されます。即時バックアップが開始されると、次のメッセージが表示されます。「Backup has been initiated and will begin in a few seconds」。

ステップ 11　（任意）バックアップの進捗状況を表示するには、コマンドライン プロンプトで **Status** と入力します。

ステップ 12　「その他の重要なバックアップ タスク」（P.13-13）も参照してください。

バックアップ ステータスの確認

ログ ファイルの確認

バックアップ ログはバックアップ プロセスを開始から終了まで記録します。

バックアップ スケジューリングに関する情報は、SMA ログ内にあります。

スケジュールされたバックアップの確認

ステップ 1　管理者として SSH セッションにログインします。

ステップ 2　コマンド プロンプトで **backupconfig** と入力し、Enter を押します。

ステップ 3　View 操作を選択します。

進行中のバックアップのステータスの確認

ステップ 1　管理者として SSH セッションにログインします。

ステップ 2　コマンド プロンプトで **backupconfig** と入力し、Enter を押します。

ステップ 3　Status 操作を選択します。

その他の重要なバックアップ タスク

ここで説明されているバックアップ プロセスではバックアップされない項目が失われることを防止するため、およびアプライアンスの障害が発生した場合にセキュリティ管理アプライアンスの交換を速めるため、次のことを検討してください。

- プライマリ セキュリティ管理アプライアンスから設定を保存するには、「コンフィギュレーション設定の保存とインポート」（P.13-50）を参照してください。プライマリ セキュリティ管理アプライアンスとは別の安全な場所にコンフィギュレーション ファイルを保存します。
- セキュリティ管理アプライアンスから別の場所にログ ファイルを保存する方法については、「ログ サブスクリプション」（P.14-22）を参照してください。

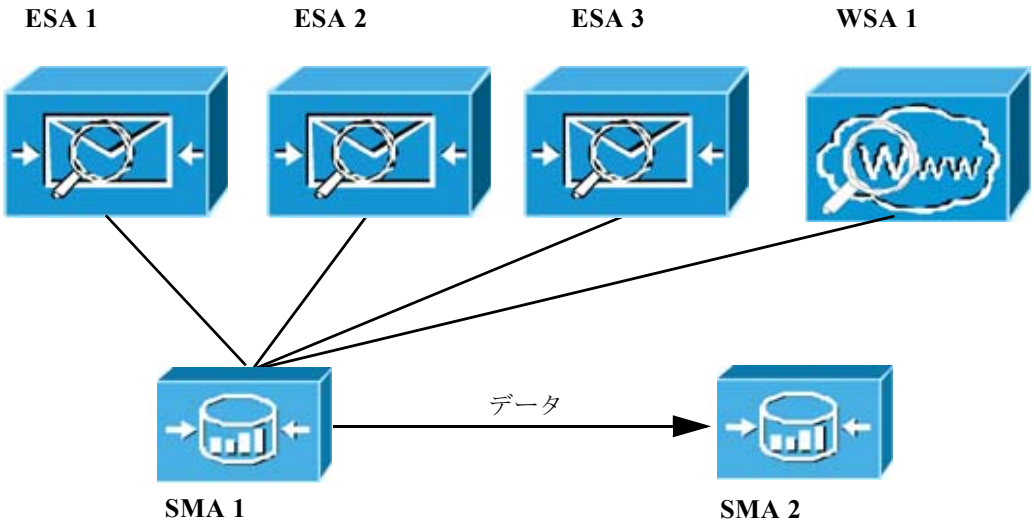
  さらに、バックアップ ログのログ サブスクリプションを設定できます。「GUI でのログ サブスクリプションの作成」（P.14-24）を参照してください。

セキュリティ管理アプライアンスでのディザスタ 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バックアップ」（P.13-6）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 13-3 のようになります。

図 13-3　　ディザスタ リカバリ：一般的な環境



この環境で、SMA 1 は ESA 1 ～ 3 および WSA 1 からデータを受信しているプライマリ セキュリティ管理アプライアンスです。SMA 2 は SMA1 からバックアップ データを受信しているバックアップ セキュリティ管理アプライアンスです。

失敗した場合は、SMA 2 がプライマリ セキュリティ管理アプライアンスになるように設定する必要があります。

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

ステップ 1　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。

詳細については、「コンフィギュレーション ファイルのロード」（P.13-52）を参照するか、`loadconfig` コマンドを使用します。

ステップ 2　次のようにして、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。

a.　SMA 2 で、[Network] > [IP Interfaces] > [Add IP Interfaces] を選択します。

b.　[Add IP Interfaces] ページで、障害が発生した SMA1 のすべての関連 IP 情報をテキスト フィールドに入力して、SMA 2 のインターフェイスを再作成します。

IP インターフェイスの追加の詳細については、「IP インターフェイスの設定」（P.A-2）を参照してください。

ステップ 3　[Submit] と [Commit] をクリックします。

ステップ 4　新しい セキュリティ管理アプライアンス（SMA 2）ですべてのサービスをイネーブルにします。

この場合、ESA 1 ～ 3 と WSA 1 のサービスも再度イネーブルにする必要があります。詳細については、「セキュリティ管理アプライアンスでのサービスの設定」（P.2-17）を参照してください。

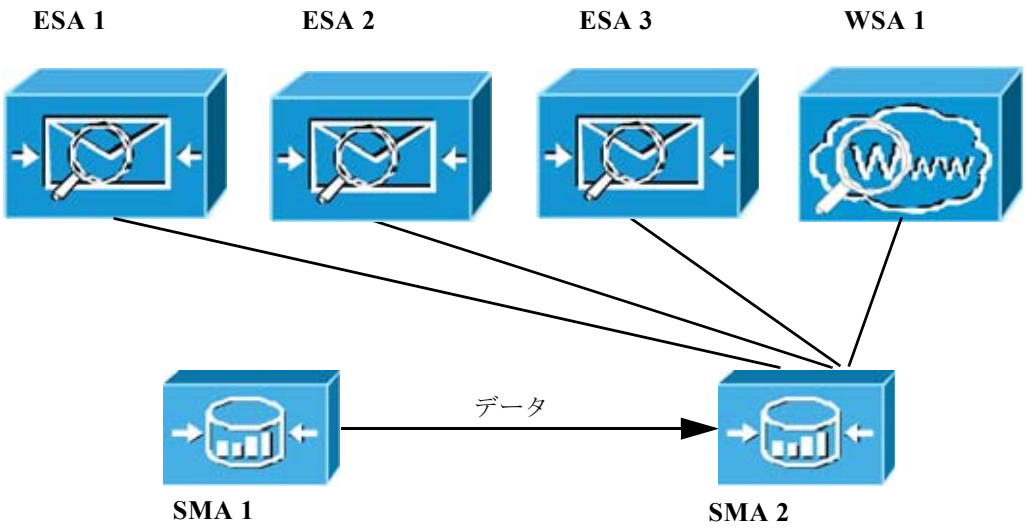
ステップ 5　すべてのアプライアンスを新しい セキュリティ管理アプライアンス（SMA 2）に追加します。

詳細については、「管理対象アプライアンスの追加について」（P.2-16）を参照してください。

ステップ 6　アプライアンスへの接続を確立し、その接続をテストすることで、各アプライアンスがイネーブルとなり、機能していることをテストして確認します。

これで、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した。これで、図 13-4 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 13-4　ディザスタ リカバリ：最終結果



その他のデータの復元

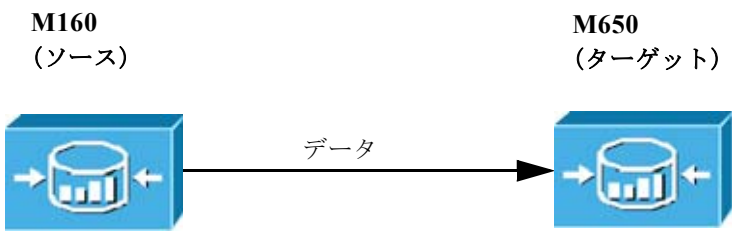
復元が必要な追加のデータについては、「その他の重要なバックアップ タスク」（P.13-13）を参照してください。

アプライアンス ハードウェアのアップグレード

古い セキュリティ管理アプライアンスから新しいモデルにアップグレードする場合（たとえば、M160 から M650 へのアップグレード）、次の手順を実行して、古いアプライアンスから新しいアプライアンスにデータを正しく転送します。

（注）　異なるサイズの セキュリティ管理アプライアンス間でデータを転送することはできますが、新しいアプライアンスには同等以上のサイズが割り当てられている必要があります。

図 13-5　新しいセキュリティ管理アプライアンス ハードウェアのアップグレード



（注）　以下に示すすべての説明は、コマンド プロンプトに入力する場合のものです。

ステップ 1　管理者として SSH セッションにログインします。

ステップ 2　コマンド プロンプトで **backupconfig** と入力し、Enter を押します。

実行する操作を選択します。

- [View]：スケジュール設定したバックアップを確認できます。
- [Verify]：バックアップをリモート マシンでスケジュール設定できるかどうかを確認します。
- [Schedule]：アプライアンスにバックアップをスケジュール設定できます。
- [Cancel]：スケジュール設定されたバックアップをキャンセルします。
- [Status]：実行中のバックアップのステータスを確認できます。

ステップ 3　**Schedule** と入力して、Enter を押します。

ステップ 4　ターゲット セキュリティ管理アプライアンスの IP アドレスと名前を入力します。

これで、セキュリティ管理アプライアンスはターゲット マシンが存在するかどうか、およびターゲット マシンにデータを受けるのに十分なスペースがあるかどうかを確認します。

異なるサイズの セキュリティ管理アプライアンス間でデータを転送することはできますが、新しいアプライアンスには同等以上のサイズが割り当てられている可能性があります。ターゲット マシンのスペースが不十分な場合は、次のエラー メッセージが表示されます。「**Backup cannot be scheduled.Reason: There is not enough space for isq, tracking, reporting, slbl.Please increase disk allocation for these services on the target machine**」。データは転送されません。

ターゲット マシンが検証されると、コンソールに次の選択肢が表示されます。

- 1. [Setup Reoccurring Backup]：定期バックアップをスケジュール設定できます。
- 2. [Schedule a Single backup]：単一バックアップをスケジュール設定できます。
- 3. [Start a Single Backup Now]：即時バックアップを開始できます。

ステップ 5　**3** と入力して、Enter を押します。

バックアップ プロセスが開始し、ソース マシンからターゲット マシンへのデータの転送がすぐに開始されます。即時バックアップが開始されると、次のメッセージが表示されます。「`Backup has been initiated and will begin in a few seconds`」。

ステップ 6　コマンドライン プロンプトに **suspendtransfers** コマンドを入力し、ソース アプライアンスと新しいターゲット アプライアンス間のすべてのデータ転送を一時停止します。

suspendtransfers コマンドによって、古いソース セキュリティ管理アプライアンスのデータ受信が停止されます。

ステップ 7　上記のステップ 2 から 5 を繰り返して、ソース マシンで新しいインスタント バックアップを実行します。

AsyncOS のアップグレード

ここでは、セキュリティ管理アプライアンスでのソフトウェア アップグレードおよびアップデートに関連する次の内容について説明します。

- 「クラスタ化されたシステムのアップグレードについて」（P.13-17）
- 「ネットワーク要件の決定」（P.13-17）
- 「アップグレード方式：リモートまたは ストリーミング」（P.13-17）
- 「アップグレードおよびサービス アップデートの設定」（P.13-20）
- 「アップグレードする前に：重要な手順」（P.13-28）

クラスタ化されたシステムのアップグレードについて

クラスタ化されたマシンをアップグレードする場合は、『*Cisco IronPort AsyncOS for Email Advanced User Guide*』の「Centralized Management」の章にある「Upgrading Machines in a Cluster」を参照してください。

ネットワーク要件の決定

Cisco IronPort Systems では分散アップグレード サーバ アーキテクチャを使用して、顧客がどこからでも AsyncOS アップグレードをすばやくダウンロードできます。この分散サーバ アーキテクチャのため、Cisco IronPort アップデート サーバではダイナミック IP アドレスが使用されます。厳格なファイアウォール ポリシーを適用している場合は、AsyncOS のアップグレード用に静的な場所の設定が必要になることがあります。アップグレードに関して、ファイアウォール設定にスタティック IP が必要であると判断した場合は、Cisco IronPort カスタマー サポートに連絡して、必要な URL アドレスを取得してください。

（注） 既存のファイアウォール ルールで `upgrades.cisco.com` ポート（22、25、80、4766 など）からのレガシー アップグレードのダウンロードが許可されている場合は、それらを削除するか、修正したファイアウォール ルールに置き換える必要があります。

アップグレード方式：リモートまたは ストリーミング

Cisco IronPort では、Cisco IronPort アプライアンスで AsyncOS をアップグレードするための 2 つの方式（または「ソース」）を使用できます。

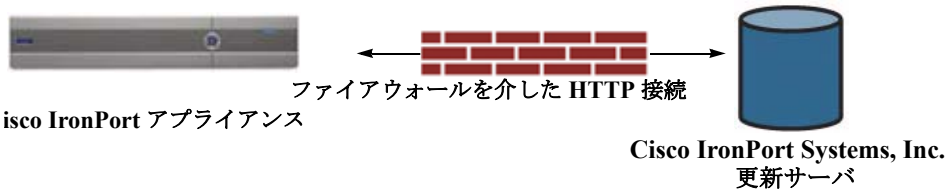
- ストリーミング アップグレード: 各 Cisco IronPort アプライアンスは Cisco IronPort アップグレード サーバから HTTP を介して AsyncOS アップグレードを直接ダウンロードします。
- リモート アップグレード : Cisco IronPort からアップグレード イメージを 1 回だけダウンロードし、Cisco IronPort アプライアンスに保存します。Cisco IronPort アプライアンスはネットワーク内のサーバから AsyncOS アップグレードをダウンロードします。

「アップグレードおよびサービス アップデートの設定」（P.13-20）にある、アップグレード方式を設定します。オプションで、CLI で **updateconfig** コマンドを使用します。

ストリーミング アップグレードの概要

ストリーミング アップグレードでは、各 Cisco IronPort アプライアンスが直接 Cisco IronPort アップデート サーバに接続して、アップグレードを検索してダウンロードします。

図 13-6　ストリーミング アップデート方式

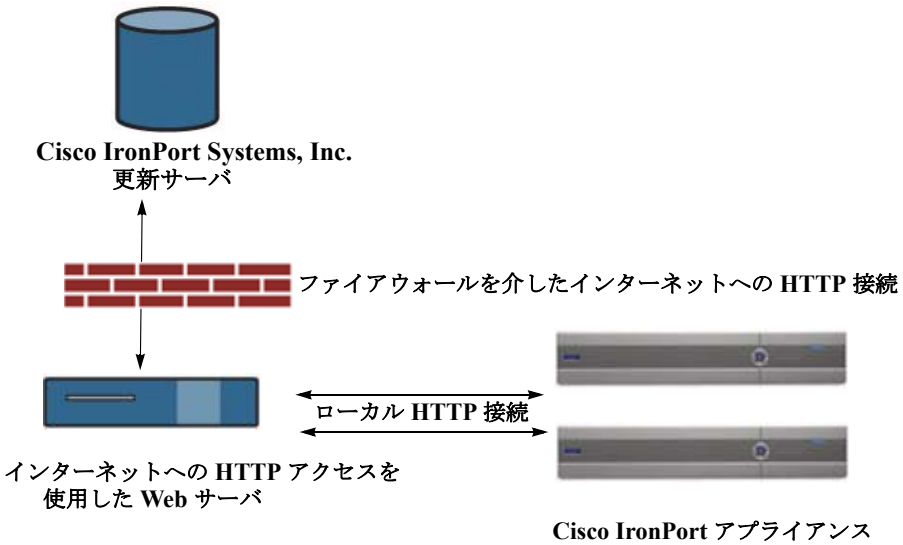


この方式では、Cisco IronPort アプライアンスが Cisco IronPort Systems アップデート サーバにネットワークから直接接続する必要があります。

リモート アップグレードの概要

また、Cisco IronPort のアップデート サーバから直接アップデートを取得する（ストリーミング アップグレード）のではなく、ネットワーク内からローカルで AsyncOS にアップデートをダウンロードおよびホスト（リモート アップグレード）することもできます。この機能を使用して、インターネットにアクセスできるネットワーク上のすべてのサーバに HTTP で暗号化されたアップデート イメージをダウンロードします。アップデート イメージをダウンロードする場合は、内部 HTTP サーバ（アップデート マネージャ）を設定し、Cisco IronPort 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 13-7　リモート アップデート方式



基本的なプロセスは、次のとおりです。

ステップ 1　「リモート アップグレードのハードウェア要件およびソフトウェア要件」（P.13-19）および「リモート アップグレード イメージのホスティング」（P.13-19）の情報をお読みください。

ステップ 2　アップグレード ファイルを取得して処理するように、ローカル サーバを設定します。

ステップ 3　アップグレード ファイルをダウンロードします。

ステップ 4　[Management Appliance] > [System Administration] > [Update SettingsChoose] 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　[Management Appliance] > [System Administration] > [System Upgrade] を選択します。

ステップ 6　[Available Upgrades] をクリックします。

（注）　コマンドライン プロンプトから、次を行うこともできます。
updateconfig コマンドを実行してから **upgrade** コマンドを実行する。

詳細については、「AsyncOS のアップグレード」（P.13-16）を参照してください。

リモート アップグレードのハードウェア要件およびソフトウェア要件

AsyncOS アップグレード ファイルを*ダウンロード*するには、内部ネットワークに次を持つシステムが必要です。

- Cisco IronPort Systems アップデート サーバへのインターネット アクセス。
- Web ブラウザ。

（注）　今回のリリースでアップデート サーバのアドレスへの HTTP アクセスを許可するファイアウォール設定値を設定する必要がある場合、特定の IP アドレスではなく DNS 名を使用する必要があります。

AsyncOS アップデート ファイルを*ホスティング*するには、内部ネットワークに次を持つサーバが必要です。

- Web サーバ。たとえば、次のような Microsoft IIS（Internet Information Services）または Apache オープン ソース サーバ。
  - 24 文字を超えた、ディレクトリまたはファイル名の表示をサポート
  - ディレクトリ参照に対応
  - 匿名（認証なし）または基本（「簡易」）認証用に設定されている
  - 各 AsyncOS アップデート イメージに対して少なくとも 350MB の空きディスク領域がある

リモート アップグレード イメージのホスティング

ローカル サーバの設定が完了したら、**http://updates.ironport.com/fetch_manifest.html** にアクセスしてアップグレード イメージの zip ファイルをダウンロードします。イメージをダウンロードするには、Cisco IronPort 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 [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 Cisco IronPort 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、Cisco IronPort アプライアンスは Cisco IronPort Systems アップデート サーバからアップグレードをダウンロードします。アップグレード リストをローカル サーバにホスティングする場合は、zip ファイルをダウンロードして、`asyncos/phoebe-my-upgrade.xml` ファイルをローカル サーバのルート ディレクトリに展開します。AsyncOS アップグレードのアップグレード リストを使用するには、XML ファイルの完全 URL を [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、Cisco IronPort ナレッジ ベースを参照するか、Cisco IronPort Support 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

セキュリティ管理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、ファイルをダウンロードするときに使用するネットワーク インターフェイスを選択したり、アップデート間隔を設定したり、自動アップデートをディセーブルにしたり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。

アップグレードおよびアップデートの設定

表 13-1 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 13-1　セキュリティ サービスのアップデート設定

設定	説明
Update Servers (images)	Cisco IronPort アップデート サーバまたはローカル Web サーバから、Cisco IronPort AsyncOS アップグレード イメージおよびサービス アップデート（時間帯ルールや機能キーのアップデートなど）をダウンロードするかどうかを決定します。デフォルトは、アップグレードおよびアップデートの両方で Cisco IronPort アップデート サーバです。 次のいずれかの場合、ローカル Web サーバを選択します。 • Cisco IronPort からアップグレードおよびアップデート イメージをダウンロードし、Cisco IronPort カスタマー サポートから提供されたスタティック アドレスを入力する必要がある場合。「厳格なファイアウォール ポリシーを適用している環境のスタティック アップグレードおよびアップデート サーバ設定」（P.13-22）を参照してください。 • 任意のタイミングで Cisco IronPort AsyncOS アップグレード イメージをダウンロードする場合。（この場合でも、Cisco Ironport アップデート サーバからサービス アップデート イメージを動的にダウンロードできます）。 ローカル アップデート サーバを選択した場合は、アップグレードとアップデートのダウンロードに使用するサーバの基本 URL とポート番号を入力します。サーバが認証を必要とする場合、有効なユーザ名とパスワードも入力します。 詳細については、「アップグレード方式：リモートまたは ストリーミング」（P.13-17）および「リモート アップグレードの概要」（P.13-18）を参照してください。
Update Servers (lists)	利用可能なアップグレードおよびサービス アップデートのリスト（マニフェスト XML ファイル）を、Cisco IronPort アップデート サーバまたはローカル Web サーバのどちらからダウンロードするかを選択します。 デフォルトは、アップグレードおよびアップデートの両方で Cisco IronPort アップデート サーバです。アップグレードとアップデートには、それぞれ異なる設定を選択できます。 該当する場合は、「厳格なファイアウォール ポリシーを適用している環境のスタティック アップグレードおよびアップデート サーバ設定」（P.13-22）を参照してください。 ローカル アップデート サーバを選択した場合、サーバのファイル名およびポート番号を含む、各リストのマニフェスト XML ファイルのフル パスを入力します。ポートのフィールドを空のままにした場合、AsyncOS はポート 80 を使用します。サーバが認証を必要とする場合、有効なユーザ名とパスワードも入力します。 詳細については、「アップグレード方式：リモートまたは ストリーミング」（P.13-17）および「リモート アップグレードの概要」（P.13-18）を参照してください。
Automatic Updates	時間帯ルールの自動アップデートをイネーブルにするかどうかを選択します。イネーブルにする場合は、アップデートを確認する間隔を入力します。分の場合は **m**、時間の場合は **h**、日の場合は **d** を末尾に追加します。

表 13-1　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
Interface	時間帯ルールや AsyncOS アップグレードなどをアップデート サーバに問い合わせるときに、どのネットワーク インターフェイスを使用するかを選択します。使用可能なプロキシ データ インターフェイスが表示されます。デフォルトでは、使用するインターフェイスがアプライアンスにより選択されます。
HTTP Proxy Server	アップストリームの HTTP プロキシ サーバが存在し、認証が必要な場合は、サーバ情報、ユーザ名、およびパスワードをここに入力します。 プロキシ サーバを指定すると、GUI にリストされているサービスへのアクセスおよびアップデートにそれが使用されます。
HTTPS Proxy Server	アップストリームの HTTPS プロキシ サーバが存在し、認証が必要な場合は、サーバ情報、ユーザ名、およびパスワードをここに入力します。 プロキシ サーバを指定すると、GUI にリストされているサービスへのアクセスおよびアップデートにそれが使用されます。

厳格なファイアウォール ポリシーを適用している環境のスタティック アップグレードおよびアップデート サーバ設定

Cisco IronPort 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、[Update Settings] ページで次の設定を使用します。

図 13-8　[Update Servers (images)] 設定のスタティック URL

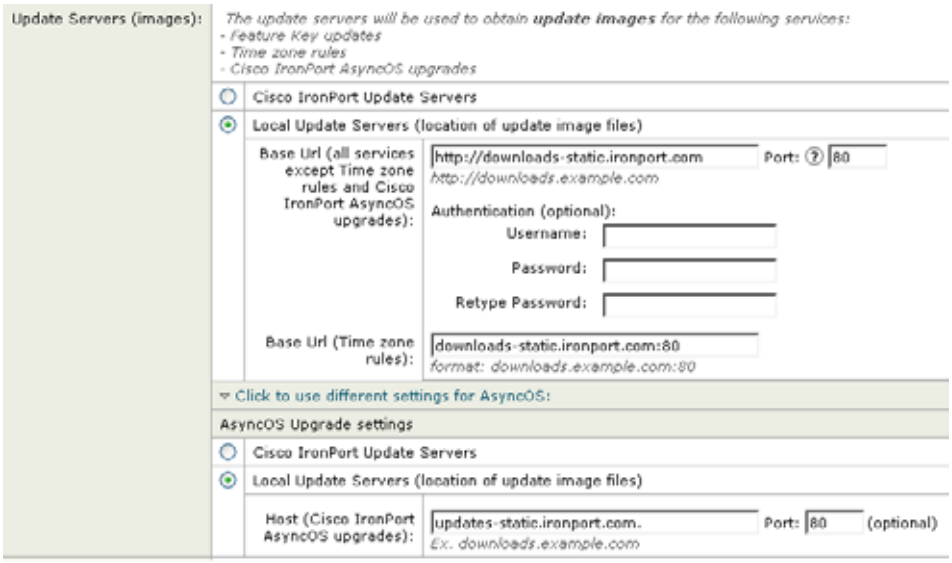


図 13-9　[Update Servers (list)] 設定のスタティック URL

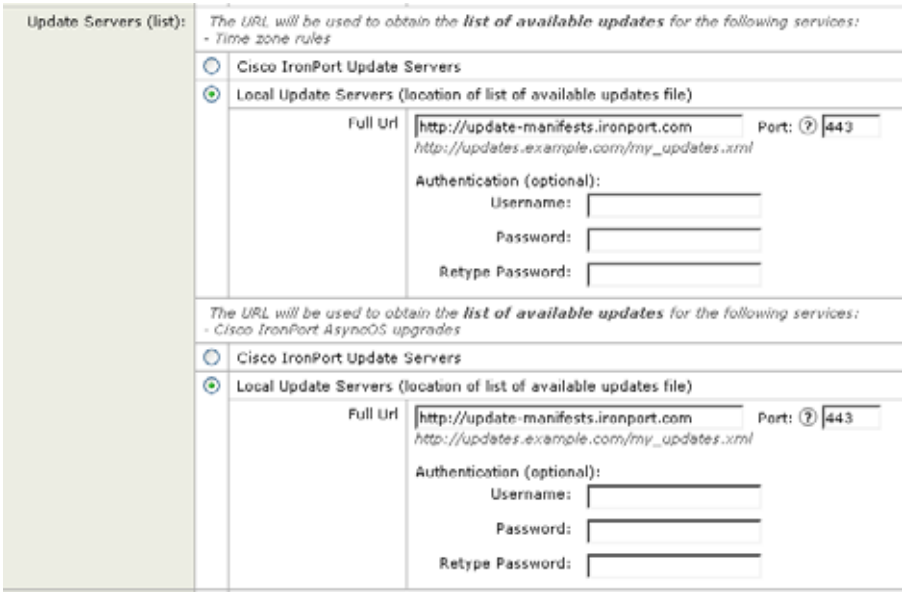


表 13-2　厳格なファイアウォール ポリシーを適用している環境のスタティック アドレス

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
Update Servers (images)	Base Url (all services except Time zone rules and Cisco IronPort AsyncOS upgrades)	http://downloads-static.ironport.com 204.15.82.8 Port 80
	Base Url (Time zone rules)	downloads-static.ironport.com 204.15.82.8 Port 80
	Host (Cisco IronPort AsyncOS upgrades)	updates-static.ironport.com 204.15.82.16 Port 80
Update Servers (list):	For updates: Full Url	update-manifests.ironport.com 204.15.82.17 Port 443
	For upgrades: Full Url	update-manifests.ironport.com 204.15.82.17 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

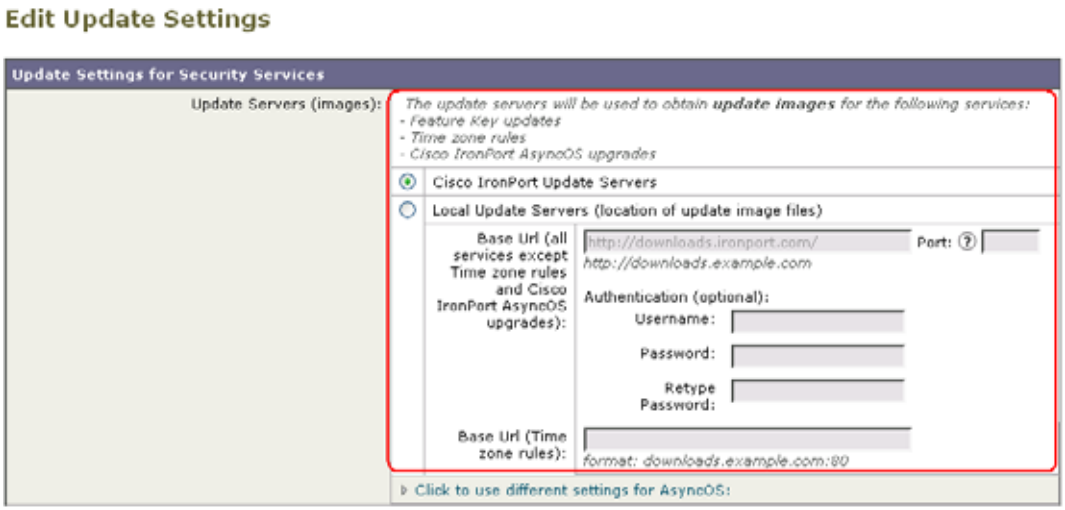
ステップ 1　[Management Appliance] > [System Administration] > [Update Settings] を選択します。

ステップ 2　[Edit Update Settings] をクリックします。

表 13-1（P.13-21）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　[Update Servers (images)] セクションで、アップデートのイメージのダウンロード元のサーバを指定します。

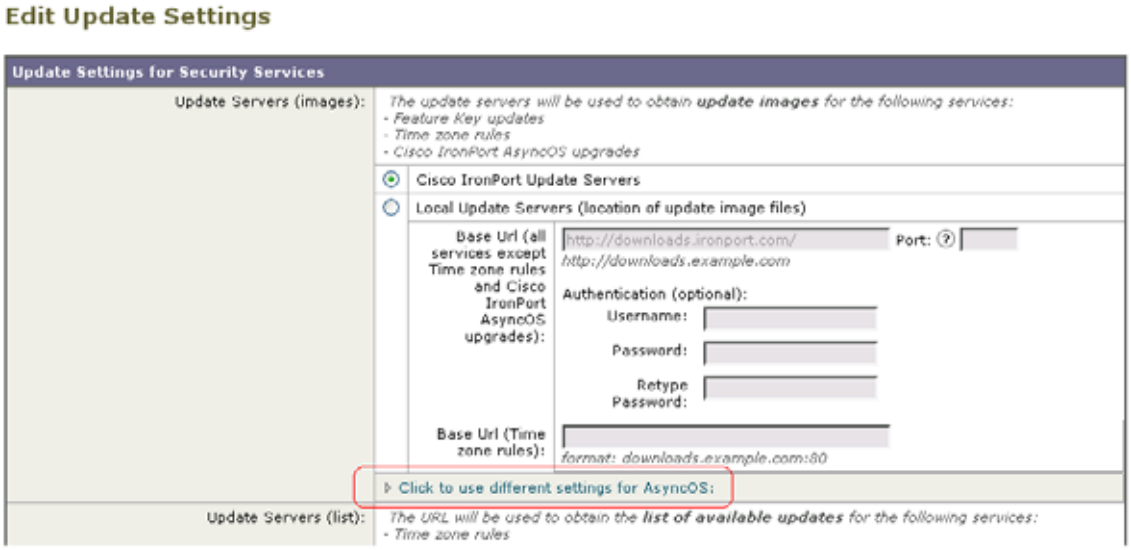
図 13-10　アップデート イメージのサーバ設定



ステップ 4　同じセクションの下部で、AsyncOS アップグレードのイメージのダウンロード元のサーバを指定します。

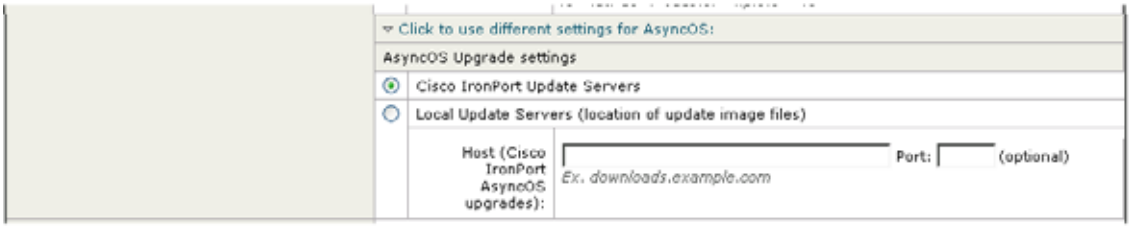
a.　[Click to use different settings for AsyncOS] リンクをクリックします。

図 13-11　アップグレード イメージのサーバ設定を指定するリンク



b. AsyncOS アップグレードのイメージのダウンロードのサーバ設定を指定します。

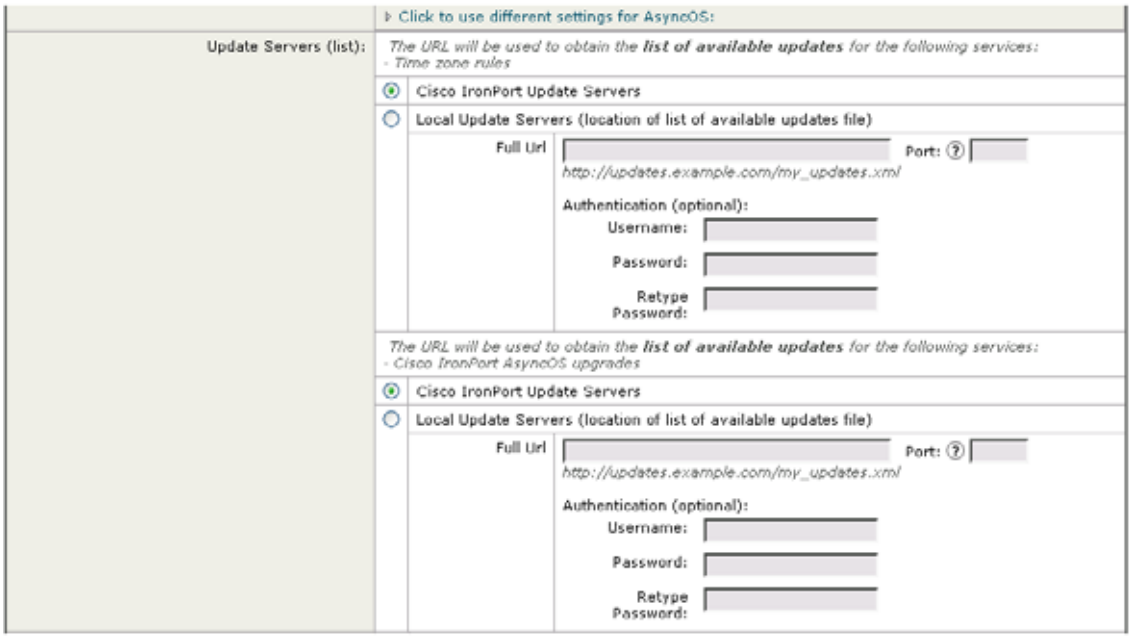
図 13-12　アップグレード イメージのサーバ設定



ステップ 5　[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の取得の設定を指定します。

上部のセクションはアップデートに適用されます。下部のセクションはアップグレードに適用されます。

図 13-13　利用可能なアップデートおよびアップグレードのリストのサーバ設定

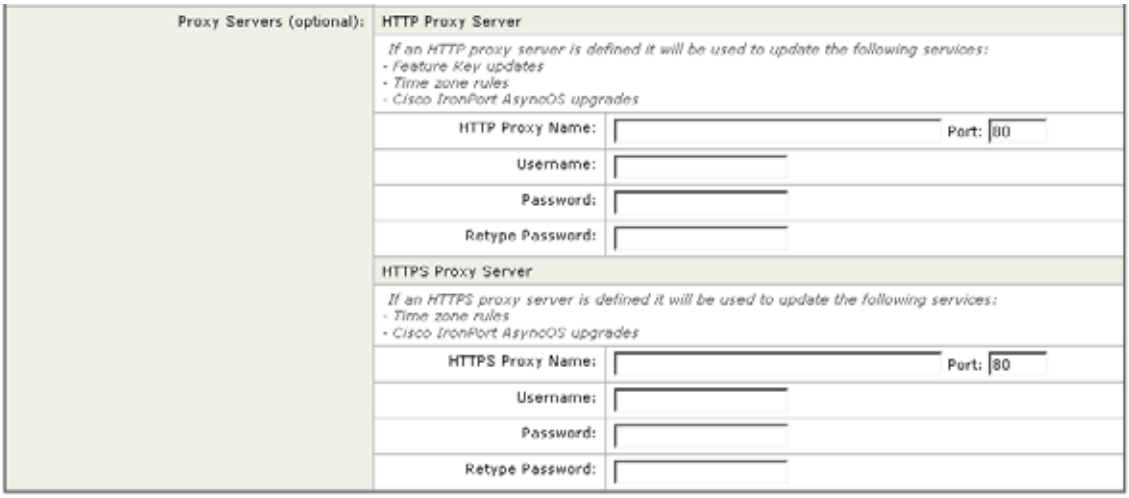


ステップ 6　時間帯ルールおよびインターフェイスの設定を指定します。

図 13-14　時間帯ルールおよびインターフェイスの設定

ステップ 7　（任意）プロキシ サーバの設定を指定します。

図 13-15　　プロキシ サーバの設定



ステップ 8　変更を送信し、保存します。

CLI からのアップデートおよびアップグレード設定値の設定

`updateconfig` コマンドを使用すると、Cisco IronPort アプライアンスにサービス アップデートおよび AsyncOS アップグレードを探す場所を指示できます。リモート アップグレードの場合、`updateconfig` コマンドを発行して、アプライアンスがその目的でローカル アップデート サーバを使用するように設定します。

```
sma.example.com> updateconfig

Service (images):                Update URL:
-------------------------------------------------------------------------------
Feature Key updates              http://downloads.ironport.com/asyncos
Timezone rules                   Cisco IronPort Servers
Cisco IronPort AsyncOS upgrades  Cisco IronPort Servers

Service (list):                  Update URL:
-------------------------------------------------------------------------------
Timezone rules                   Cisco IronPort Servers
Cisco IronPort AsyncOS upgrades  Cisco IronPort Servers

Update interval: 5m

Proxy server: not enabled

HTTPS Proxy server: not enabled

Choose the operation you want to perform:
- SETUP - Edit update configuration.
[]> setup


For the following services, please select where the system will download
updates from:
Service (images):                Update URL:
```

```
-------------------------------------------------------------------------------
Feature Key updates               http://downloads.ironport.com/asyncos

1. Use Cisco IronPort update servers (http://downloads.ironport.com)
2. Use own server
[1]>


For the following services, please select where the system will download
updates from (images):
Service (images):                 Update URL:
-------------------------------------------------------------------------------
Timezone rules                    Cisco IronPort Servers

1. Use Cisco IronPort update servers
2. Use own server
[1]>


For the following services, please select where the system will download
updates from (images):
Service (images):                 Update URL:
-------------------------------------------------------------------------------
Cisco IronPort AsyncOS upgrades   Cisco IronPort Servers

1. Use Cisco IronPort update servers
2. Use own server
[1]> 2


Enter the hostname and port of the HTTP server to download updates (images)
from, using the format (local.server:port). The server name may be an IP
address. The default port is 80; you do not need to specify the port unless
you wish to use a non-standard port.
[]>upgradeserver.example.com


For the following services, please select where the system will download the
list of available updates from:
Service (list):                   Update URL:
-------------------------------------------------------------------------------
Timezone rules                    Cisco IronPort Servers

1. Use Cisco IronPort update servers
2. Use own update list
[1]>


For the following services, please select where the system will download the
list of available updates from:
Service (list):                   Update URL:
-------------------------------------------------------------------------------
Cisco IronPort AsyncOS upgrades   Cisco IronPort Servers

1. Use Cisco IronPort update servers
2. Use own update list
[1]>


Enter the time interval between checks for new:
 - Timezone rules
Use a trailing 'm' for minutes or 'h' for hours. Enter '0' to disable automatic
updates (manual updates will still be available for individual services).
[5m]>
```

```
When initiating a connection to the update server the originating IP interface
is chosen automatically. If you want to choose a specific interface, please
specify it now.
1. Auto
2. Management (198.51.100.0/24: sma.example.com)
[1]>


Do you want to set up a proxy server for HTTP updates for ALL of the following
services:
 - Feature Key updates
 - Timezone rules
 - Cisco IronPort AsyncOS upgrades
[N]>


Do you want to set up an HTTPS proxy server for HTTPS updates for ALL of the
following
services:
 - Timezone rules
 - Cisco IronPort AsyncOS upgrades
[N]>


Service (images):                  Update URL:
-------------------------------------------------------------------------------
Feature Key updates                http://downloads.ironport.com/asyncos
Timezone rules                     Cisco IronPort Servers
Cisco IronPort AsyncOS upgrades    http://upgradeserver.example.com


Service (list):                    Update URL:
-------------------------------------------------------------------------------
Timezone rules                     Cisco IronPort Servers
Cisco IronPort AsyncOS upgrades    Cisco IronPort Servers

Update interval: 5m

Proxy server: not enabled

HTTPS Proxy server: not enabled

Choose the operation you want to perform:
- SETUP - Edit update configuration.
[]>
```

忘れずに変更を確定してください。

（注） ping コマンドを使用すると、アプライアンスがローカル サーバに接続できることを確認できます。また、telnet コマンドを使用してローカル サーバのポート 80 に Telnet 接続することで、ローカル サーバが該当のポートをリッスンしていることが確認できます。

アップグレードする前に：重要な手順

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。「使用可能な最大ディスク領域」（P.13-58）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。

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。

ステップ 4　CLI からアップグレードを実行している場合は、**suspendlistener** コマンドを使用してリスナーを停止します。GUI からアップグレードを実行した場合は、自動的にリスナーの一時停止が発生します。

ステップ 5　メール キューとデリバリ キューを解放します。

ステップ 6　アップグレード設定が希望どおりに設定されていることを確認します。「アップグレードおよびサービス アップデートの設定」（P.13-20）を参照してください。

GUI からの AsyncOS のアップグレード

ステップ 1　「アップグレードする前に：重要な手順」（P.13-28）に示された作業を完了したことを確認します。

ステップ 2　セキュリティ管理アプライアンスで、[Management Appliance] > [System Administration] > [System Upgrade] を選択します。

ステップ 3　[Available Upgrades] をクリックします。

ステップ 4　利用可能なアップグレードのリストから、アップグレードを選択します。

ステップ 5　アップグレード前に設定ディレクトリに現在の設定を保存する場合は、[Upgrade Preparation] セクションでチェックボックスをオンにします。この設定が推奨されます。また、テキスト フィールドにメール アドレスを入力することで、選択した電子メールにこのパスワード ファイルを送信できます。

このセクションでは、[Configuration File] チェックボックスの [Mask Passwords] をオンにすることで、コンフィギュレーション ファイルにパスワードが表示されないようにすることもできます。

ステップ 6　[Begin Upgrade] をクリックします。ページの上部に経過表示バーが表示されます。変更の確定や新しいライセンス契約書への合意を 1 回以上求められる場合があります。

ステップ 7　アップグレードを完了するには、[Continue] をクリックします。

ステップ 8　アップグレードが完了すると、アプライアンスをリブートするように求められます。

ステップ 9　[Reboot Now] をクリックします。

ステップ 10　他の推奨される作業については、「アップグレード後」（P.13-31）を参照してください。

CLI を使用したアップグレードの実行

AsyncOS アップグレードを取得する場所（ローカル サーバまたは Cisco IronPort サーバ）を指定するには、`updateconfig` コマンドを実行します。アップグレードをインストールするには、`upgrade` コマンドを実行します。デフォルトでは、`upgrade` コマンドを入力すると、アプライアンスは Cisco IronPort アップグレード サーバに最新のアップデートを問い合わせます。

（注）　6.5 以前のバージョンの AsyncOS では、AsyncOS のアップグレードの取得に upgradeconfig コマンドが使用されていました。このコマンドは、現在サポートされていません。

（注）　アップグレード中は、さまざまなプロンプトを一時停止のまま長時間放置しないでください。TCP セッションがダウンロード中にタイムアウトしてしまった場合、アップグレードが失敗する可能性があります。

アップグレードする前に、「アップグレードする前に：重要な手順」（P.13-28）の関連する手順を完了します。

upgrade コマンドを発行して、利用可能なアップグレードのリストを表示します。リストから目的のアップグレードを選択して、インストールします。メッセージを確認するか、ライセンス契約を読んで、同意するように求められる場合があります。

```
Welcome to the IronPort M650 Security Management(tm) Appliance

sma.example.com> upgrade

Would you like to save the current configuration to the configuration directory before
upgrading? [Y]> y

Would you like to email the current configuration before upgrading? [N]> y

Do you want to include passwords? Please be aware that a configuration without passwords
will fail when reloaded with loadconfig. [Y]> y

Enter email addresses. Separate multiple addresses with commas.
[]> email@example.com

Upgrades available:
1. AsyncOS test.test

[1]> 1

Performing an upgrade may require a reboot of the system after the upgrade is applied. You
may log in again after this is done. Do you wish to proceed with the upgrade? [Y]> y

Preserving configuration ...
Finished preserving configuration
Cisco IronPort Security Management Appliance(tm) Upgrade

Warning: The 5.7 configuration master will be deleted on upgrade.
All settings in that configuration master will be deleted and will not be recoverable.

Do you wish to proceed with the upgrade? [y]> y

Finding partitions... done.
Setting next boot partition to current partition as a precaution... done.
Erasing new boot partition... done.
Installing application... done.
Installing CASE... done.
Installing Sophos Anti-Virus... done.
Reinstalling AsyncOS... done.
Installing Scanners... done.
Installing Brightmail Anti-Spam... done.
Installing Tracking Tools... done.
Configuring AsyncOS disk partitions... done.
Configuring AsyncOS user passwords... done.
```

```
Configuring AsyncOS network interfaces... done.
Configuring AsyncOS timezone... done.
Moving new directories across partitions... done.
Syncing... done.
Reinstalling boot blocks... done.
Will now boot off new boot partition... done.

Upgrade complete. It will be in effect after this mandatory reboot.

Upgrade installation finished.
Enter the number of seconds to wait before forcibly closing connections.
[30]>
```

アップグレードが完了したら、「アップグレード後」（P.13-31）の作業を実行します。

アップグレード後

アップグレードが完了したら、次の手順を実行します。

- （関連する電子メール セキュリティ アプライアンスのある導入環境の場合）リスナーを再度イネーブルにします。
- システムが最新の Configuration Master をサポートするように設定します。「Configuration Master を使用するための設定の概要」（P.8-2）を参照してください。
- 設定を保存するかどうか判断します。詳細については、「コンフィギュレーション設定の保存とインポート」（P.13-50）を参照してください。

AsyncOS の以前のバージョンへの復元

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。

アップグレードによって主要なサブシステムの一方向の変換が行われるため、バージョンの復元プロセスは複雑であり、Cisco IronPort 品質保証チームの認定が必要です。復元できるのは、前の 2 つのバージョンの中の 1 つだけです。最初にこの機能がサポートされた AsyncOS バージョンは AsyncOS 6.5 です。これよりも前のバージョンの AsyncOS はサポートされていません。

アプライアンス上のすべてのデータをクリアし、新しい、クリーンな設定から始める場合は、現在実行中のビルドに戻すこともできます。

復元による影響に関する重要な注意事項

Cisco IronPort 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。このコマンドにより、すべての設定ログとデータベースが破壊されます。さらに、復元ではアプライアンスが再設定されるまでメール処理が中断されます。このコマンドはすべての設定を破壊するため、`revert` コマンドを発行する場合は、Cisco IronPort アプライアンスへの物理的なローカル アクセスを必ず用意するようにしてください。

警告　戻し先のバージョンのコンフィギュレーション ファイルが必要です。コンフィギュレーション ファイルには、後方互換性が*ありません*。

AsyncOS 復元の実行

ステップ 1　戻し先のバージョンのコンフィギュレーション ファイルがあることを確認してください。コンフィギュレーション ファイルには、後方互換性がありません。

ステップ 2　アプライアンスの現在の設定のバックアップ コピーを、（パスワードをマスクしない状態で）別のマシンに保存します。それには、電子メールで自分に送信したり、ファイルを FTP で転送します。簡単に行うには、`mailconfig` CLI コマンドを実行すると、アプライアンスの現在のコンフィギュレーション ファイルが指定したメール アドレスに送信されます。

（注）　復元後にロードするのは、このコンフィギュレーション ファイルではありません。

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

ステップ 4　電子メール セキュリティ アプライアンスで、すべてのリスナーを一時停止します。

ステップ 5　メール キューが空になるまで待ちます。

ステップ 6　バージョンを戻すアプライアンスの CLI にログインします。

`revert` コマンドを実行すると、いくつかの警告プロンプトが出されます。これらの警告プロンプトに同意すると、すぐにバージョンを戻す動作が開始します。このため、復元前の手順を完了するまで、復元プロセスを開始しないでください。

ステップ 7　コマンドライン プロンプトから **revert** コマンドを入力し、プロンプトに応答します。

次に、**revert** コマンドの例を示します。

```
m650p03.prep> revert

This command will revert the appliance to a previous version of AsyncOS.

WARNING: Reverting the appliance is extremely destructive.
The following data will be destroyed in the process:
- all configuration settings (including listeners)
- all log files
- all databases (including messages in Virus Outbreak and Policy
quarantines)
- all reporting data (including saved scheduled reports)
- all message tracking data
- all Cisco IronPort Spam Quarantine message and end-user safelist/blocklist data

Only the network settings will be preseved.

Before running this command, be sure you have:
- saved the configuration file of this appliance (with passwords
unmasked)
- exported the Cisco IronPort Spam Quarantine safelist/blocklist database
 to another machine (if applicable)
- waited for the mail queue to empty

Reverting the device causes an immediate reboot to take place.
After rebooting, the appliance reinitializes itself and reboots again to the desired
version.

Do you want to continue? yes

Are you sure you want to continue? yes

Available versions
```

```
==================
 1. 7.2.0-390
 2. 6.7.6-020

Please select an AsyncOS version: 1

You have selected "7.2.0-390".

Reverting to "testing" preconfigure install mode.

The system will now reboot to perform the revert operation.
```

ステップ 8　アプライアンスが 2 回リブートするまで待ちます。

ステップ 9　CLI を使用してアプライアンスにログインします。

ステップ 10　アプライアンスが AsyncOS 7.5 を実行する Web セキュリティ アプライアンスを管理する場合は、これらのアプライアンスの少なくとも 1 つを追加してから数分待機して、URL カテゴリ アップデートが Web セキュリティ アプライアンスからダウンロードされるようにします。

ステップ 11　URL カテゴリのアップデートが完了したら、戻し先のバージョンのコンフィギュレーション ファイルをロードします。

ステップ 12　セーフリスト/ブロックリスト機能を使用する場合は、セーフリスト/ブロックリスト データベースをインポートして復元します。

ステップ 13　電子メール セキュリティ アプライアンスで、すべてのリスナーを再びイネーブルにします。

ステップ 14　変更を保存します。

これで、復元が完了した Cisco IronPort 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、Cisco IronPort アプライアンスへのコンソール アクセスが再び利用可能になるまでには、15 ～ 20 分かかります。

アップデートについて

サービス アップデートは定期的にダウンロード可能にできます。これらのダウンロードの設定を指定するには、「アップグレードおよびサービス アップデートの設定」（P.13-20）を参照してください。

Cisco IronPort Web 使用率制御の URL カテゴリ セット アップデートについて

- 「URL カテゴリ セットの更新と中央集中型コンフィギュレーション管理」（P.8-23）
- 「URL カテゴリ セットの更新とレポート」（P.5-28）

生成されたメッセージの返信アドレスの設定

次の場合に対して、AsyncOS で生成されたメールのエンベロープ送信者を設定できます。

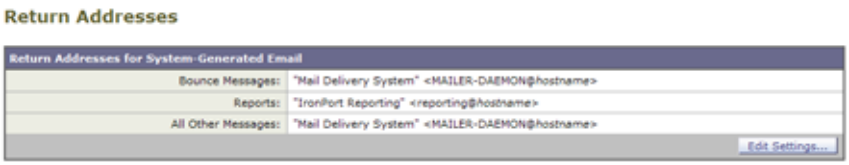
- バウンス メッセージ

- レポート

返信アドレスの表示、ユーザ、およびドメイン名を指定できます。ドメイン名に仮想ゲートウェイ ドメインの使用を選択することもできます。

GUI の [System Administration] メニューから利用できる [Return Addresses] ページを使用するか、CLI で **addressconfig** コマンドを使用します。

図 13-16　[Return Addresses] ページ



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、[Return Addresses] ページで [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 [Submit] をクリックし、変更を確定します。

アラートの管理

アラートとは、Cisco IronPort アプライアンスで発生しているイベントに関する情報が記載されている、電子メールによる通知のことです。これらのイベントにはマイナーからメジャーまでの重要度（または重大度）レベルがあり、一般的にアプライアンスの特定のコンポーネントまたは機能に関連しています。アラートは、Cisco IronPort アプライアンスで生成されます。どのアラート メッセージがどのユーザに送信され、イベントの重大度がどの程度である場合にアラートが送信されるかは、非常にきめ細かなレベルで指定できます。アラートの管理は、GUI の [Management Appliance] > [System Administration] > [Alerts] ページで行います（または、CLI で `alertconfig` コマンドを使用します）。

アラートの概要

次の機能によって、電子メール通知の動作が制御されます。

- **アラート：**電子メール通知を受け取るアラートを作成します。アラートは、アラートの受信者（受信アラートの電子メール アドレス）と、アラート通知（重大度とアラート タイプを含む）で構成されています。
- **アラート設定：**アラート機能の全般的な動作を指定します。たとえば、アラートの送信者（FROM:）のアドレス、重複アラートを送信する秒間隔、および AutoSupport をイネーブルにするかどうか（および、オプションで週次 AutoSupport レポートを送信するかどうか）などを指定します。

アラート：アラート受信者、アラート分類、および重要度

アラートとは、ハードウェア問題などの特定の機能についての情報が含まれている電子メール メッセージまたは通知であり、アラートの受信者に送信されます。アラート受信者とは、アラート通知が送信される電子メール アドレスのことです。通知に含まれる情報は、アラートの分類と重大度によって決まります。どのアラート分類を、どの重大度で、特定のアラート受信者に送信するかを指定できます。アラート エンジンを使用して、受信者に送信されるアラートを詳細に制御できます。たとえば、重大度レベルが Critical であり、アラート タイプが System の場合など、特定のタイプのアラートのみ

が受信者に送信されるようにシステムを設定できます。また、一般的な設定値も設定できます（「アラート設定値の設定」（P.13-38）を参照してください）。すべてのアラートのリストについては、「アラート リスト」（P.13-39）を参照してください。

アラートの分類

AsyncOS では、次のアラート分類を送信します。

- システム
- ハードウェア

重大度

アラートは、次の重大度に従って送信されます。

- Critical：すぐに対処が必要な問題
- Warning：今後モニタリングが必要な問題またはエラー。すぐに対処が必要な可能性もあります
- Info：このデバイスのルーティン機能で生成される情報

アラート設定

アラート設定では、アラートの全般的な動作と設定を制御します。設定には次のような項目があります。

- RFC 2822 Header From：アラートを送信するタイミング（アドレスを入力するか、デフォルトの「alert@<hostname>」を使用します）。また、`alertconfig -> from` コマンドを使用して、この値を CLI で設定することもできます。
- 重複したアラートを送信するまでに待機する秒数の初期値。
- 重複したアラートを送信するまでに待機する秒数の最大値。
- AutoSupport のステータス（イネーブルまたはディセーブル）。
- Information レベルのシステム アラートを受信するように設定されたアラート受信者への、AutoSupport の週次ステータス レポートの送信。

重複したアラートの送信

AsyncOS が重複したアラートを送信するまでに待機する秒数の初期値を指定できます。この値を 0 に設定した場合、重複したアラートのサマリーは送信されず、代わりにすべての重複したアラートがリアルタイムに送信されます（短時間に大量の電子メールを受信する可能性があります）。重複したアラートを送信するまでに待機する秒数は、アラートを送信するたびに増加します。この増加は、待機する秒数に、直前の間隔の 2 倍を加えたものになります。つまり、待機時間が 5 秒間の場合、アラートは 5 秒後、15 秒後、35 秒後、75 秒後、155 秒後、315 秒後といった間隔で送信されます。

最終的に、送信間隔は非常に長くなります。[Maximum Number of Seconds to Wait Before Sending a Duplicate Alert] フィールドを使用して、待機間隔の秒数に制限を設けることができます。たとえば、初期値を 5 秒に設定し、最大値を 60 秒に設定すると、アラートは 5 秒後、15 秒後、35 秒後、60 秒後、120 秒後といった間隔で送信されます。

アラートの配信

アラート メッセージは Cisco IronPort アプライアンス内の問題の通知に使用されるため、送信に AsyncOS の標準メール配信システムを使用しません。代わりに、アラート メッセージは AsyncOS で重大なシステム故障が発生しても動作するように設計された、個別に並行動作する電子メール システムで処理されます。

アラート メール システムは、AsyncOS と同一の設定を共有しません。このため、アラート メッセージは、次のように他のメール配信とは若干異なる動作をする可能性があります。

- アラート メッセージは、標準の DNS MX レコードおよび A レコードのルックアップを使用して配信されます。
  - 5.X よりも前の AsyncOS バージョンでは、アラート メッセージに SMTP ルートが使用されません。
  - アラート メッセージは DNS エントリを 30 分間キャッシュし、そのキャッシュは 30 分ごとにリフレッシュされます。このため、DNS 障害時にもアラートが出力されます。
- アラート メッセージはワーク キューを通過しないため、ウイルスまたはスパムのスキャン対象外です。メッセージ フィルタまたはコンテンツ フィルタの処理対象にも含まれません。
- アラート メッセージは配信キューを通過しないため、バウンスのプロファイルまたは送信先制御の制限には影響を受けません。

Cisco IronPort AutoSupport

Cisco IronPort による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 Cisco IronPort Systems に送信するように Cisco IronPort 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、Cisco IronPort 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、Cisco IronPort に送信される各メッセージのコピーを受信します。内部にアラート メッセージを毎週送信しない場合は、この設定をディセーブルにできます。この機能をイネーブルまたはディセーブルにするには、「アラート設定値の設定」（P.13-38）を参照してください。

アラート メッセージ

アラート メッセージは標準的な電子メール メッセージです。Header From: アドレスは設定できますが、メッセージのその他の部分は自動的に生成されます。

アラートの From アドレス

Header From: アドレスは、GUI で [Edit Settings] ボタンをクリックするか、CLI（『*Cisco IronPort AsyncOS CLI Reference Guide*』を参照）を使用して設定できます。

アラートの件名

アラート メッセージの件名は、次の形式になります。

```
Subject: [severity]-[hostname]: ([class]) short message
```

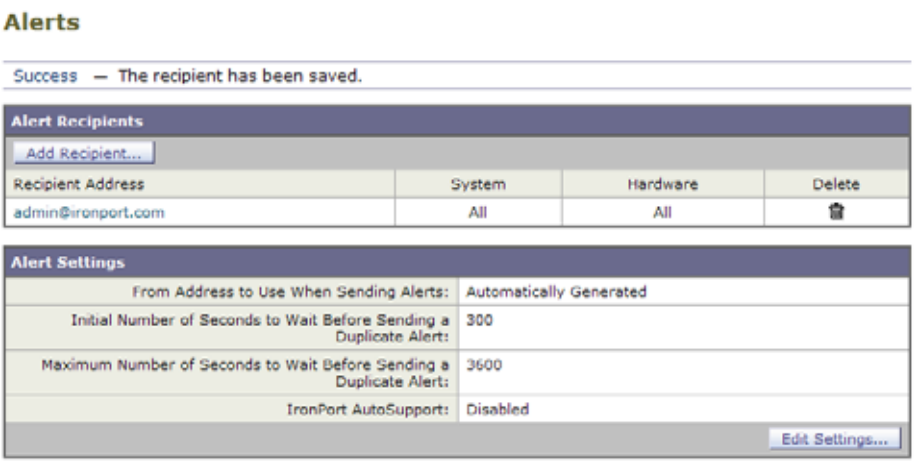
アラート メッセージの例

```
Date: 23 Mar 2007 21:10:19 +0000
To: joe@example.com
From: Cisco IronPort M650 Alert [alert@example.com]
Subject: Critical-example.com: (AntiVirus) update via http://newproxy.example.com failed

The Critical message is:

update via http://newproxy.example.com failed

Version: 6.0.0-419
Serial Number: XXXXXXXXXXX-XXXXXXX
Timestamp: Tue May 10 09:39:24 2007

For more information about this error, please see
 http://support.ironport.com
If you need further information, contact your support provider.
```

アラート受信者の管理

GUI にログインして、[System Administration] > [Alerts] を選択します。（GUI へのアクセス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へのアクセス」（P.2-8）を参照してください）。

図 13-17　[Alerts] ページ



（注）　システムのセットアップ時に AutoSupport をイネーブルにした場合、指定した電子メール アドレスはデフォルトで、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。

[Alerts] ページは、既存のアラート受信者およびアラート設定のリストを表示します。

[Alerts] ページからは、次の操作ができます。

- アラート受信者の追加、設定、または削除。
- アラート設定値の変更。

新規アラート受信者の追加

ステップ 1　[Alerts] ページで [Add Recipient] をクリックします。

ステップ 2　受信者の電子メール アドレスを入力します。複数のアドレスをカンマで区切って入力することもできます。

ステップ 3　アラート受信者が受信するアラート重大度を選択します。

ステップ 4　[Submit] をクリックして、アラート受信者を追加します。

ステップ 5　変更を保存します。

既存のアラート受信者の設定

ステップ 1　[Alert Recipients] のリストからアラート受信者をクリックします。

ステップ 2　アラート受信者の設定を変更します。

ステップ 3　変更を送信し、保存します。

アラート受信者の削除

ステップ 1　[Alert Recipient] のリストから、アラート受信者に対応するゴミ箱アイコンをクリックします。

ステップ 2　表示される警告ダイアログで [Delete] をクリックして削除を確認します。

ステップ 3　変更を保存します。

アラート設定値の設定

アラート設定は、セキュリティ管理アプライアンスが送信するすべてのアラートに適用されます。

アラート設定値の編集

ステップ 1　[Alerts] ページで [Edit Settings] をクリックします。

ステップ 2　アラートの送信に使用する Header From: アドレスを入力するか、[Automatically generated]（「alert@<hostname>」を自動生成）を選択します。

ステップ 3　重複したアラートを送信するまでに待機する秒数を指定する場合は、チェックボックスをオンにします。詳細については、「重複したアラートの送信」（P.13-35）を参照してください。

- 重複したアラートを送信するまでに待機する秒数の初期値を指定します。
- 重複したアラートを送信するまでに待機する秒数の最大値を指定します。

ステップ 4　必要に応じて、[Cisco IronPort AutoSupport] オプションを選択して、AutoSupport をイネーブルにします。AutoSupport の詳細については、「Cisco IronPort AutoSupport」（P.13-36）を参照してください。

– AutoSupport がイネーブルの場合、Information レベルのシステム アラートを受信するように設定されたアラート受信者に、週次 AutoSupport レポートが送信されます。チェックボックスを使用して、これをディセーブルにできます。

ステップ 5　変更を送信し、保存します。

アラート リスト

次の表に、アラート名、説明、および重大度など、アラートを分類別に示します。

ハードウェア アラート

表 13-3 には、アラートの説明やアラートの重大度など、AsyncOS によって生成される可能性のあるさまざまなハードウェア アラートを示してあります。

表 13-3　ハードウェア アラートのリスト

アラート名	説明	重大度
INTERFACE.ERRORS	インターフェイス エラーを検出した場合に送信されます。	Warning
MAIL.MEASUREMENTS_FILESYSTEM	ディスク パーティションが 75 % の使用率に近づいた場合に送信されます。	Warning
MAIL.MEASUREMENTS_FILESYSTEM.CRITICAL	ディスク パーティションが 90 % の使用率に達した場合（95 %、96 %、97 % など）に送信されます。	Critical
SYSTEM.RAID_EVENT_ALERT	重大な RAID-event が発生した場合に送信されます。	Warning
SYSTEM.RAID_EVENT_ALERT_INFO	RAID-event が発生した場合に送信されます。	Information

システム アラート

表 13-4 には、アラートの説明やアラートの重大度など、AsyncOS によって生成される可能性のあるさまざまなシステム アラートを示してあります。

表 13-4　システム アラートのリスト

アラート名	説明	重大度
COMMON.APP_FAILURE	不明なアプリケーション障害が発生した場合に送信されます。	Critical
COMMON.KEY_EXPIRED_ALERT	機能キーの有効期限が切れた場合に送信されます。	Warning
COMMON.KEY_EXPIRING_ALERT	機能キーの有効期限が切れる場合に送信されます。	Warning
COMMON.KEY_FINAL_EXPIRING_ALERT	機能キーの有効期限が切れる場合の最後の通知として送信されます。	Warning
DNS.BOOTSTRAP_FAILED	アプライアンスがルート DNS サーバに問い合わせることができない場合に送信されます。	Warning

表 13-4　システム アラートのリスト（続き）

アラート名	説明	重大度
INTERFACE.FAILOVER.FAILURE_BACKUP_DETECTED	バックアップ NIC ペアリング インターフェイスが故障した場合に送信されます。	Warning
INTERFACE.FAILOVER.FAILURE_BACKUP_RECOVERED	NIC ペアのフェールオーバーが復旧した場合に送信されます。	Information
INTERFACE.FAILOVER.FAILURE_DETECTED	インターフェイス故障により、NIC ペアリング フェールオーバーが検出された場合に送信されます。	Critical
INTERFACE.FAILOVER.FAILURE_DETECTED_NO_BACKUP	インターフェイス故障により NIC ペアリング フェールオーバーは検出されたけれども、バックアップ インターフェイスが利用できない場合に送信されます。	Critical
INTERFACE.FAILOVER.FAILURE_RECOVERED	NIC ペアのフェールオーバーが復旧した場合に送信されます。	Information
INTERFACE.FAILOVER.MANUAL	別の NIC ペアへの手動フェールオーバーが検出された場合に送信されます。	Information
COMMON.INVALID_FILTER	無効なフィルタが存在する場合に送信されます。	Warning
LDAP.GROUP_QUERY_FAILED_ALERT	LDAP グループ クエリーに失敗した場合に送信されます。	Critical
LDAP.HARD_ERROR	LDAP クエリーが（すべてのサーバで試行した後）完全に失敗した場合に送信されます。	Critical
LOG.ERROR.*	さまざまなロギング エラー。	Critical
MAIL.PERRCPT.LDAP_GROUP_QUERY_FAILED	各受信者のスキャン時に LDAP グループ クエリーに失敗した場合に送信されます。	Critical
MAIL.QUEUE.ERROR.*	メール キューのさまざまなハード エラー。	Critical
MAIL.RES_CON_START_ALERT.MEMORY	メモリ使用率がシステム リソース節約しきい値を超過した場合に送信されます。	Critical
MAIL.RES_CON_START_ALERT.QUEUE_SLOW	メール キューが過負荷となり、システム リソース節約がイネーブルになった場合に送信されます。	Critical
MAIL.RES_CON_START_ALERT.QUEUE	キュー使用率がシステム リソース節約しきい値を超過した場合に送信されます。	Critical
MAIL.RES_CON_START_ALERT.WORKQ	ワーク キューのサイズが大きすぎるため、リスナーが一時停止された場合に送信されます。	Critical
MAIL.RES_CON_START_ALERT	アプライアンスが「リソース節約」モードに入った場合に送信されます。	Critical
MAIL.RES_CON_STOP_ALERT	アプライアンスの「リソース節約」モードが解除された場合に送信されます。	Critical
MAIL.WORK_QUEUE_PAUSED_NATURAL	ワーク キューが中断された場合に送信されます。	Critical
MAIL.WORK_QUEUE_UNPAUSED_NATURAL	ワーク キューが再開された場合に送信されます。	Critical

表 13-4　システム アラートのリスト（続き）

アラート名	説明	重大度
NTP.NOT_ROOT	NTP が root として動作していないため、Cisco IronPort アプライアンスが時刻を調整できない場合に送信されます。	Warning
PERIODIC_REPORTS. DOMAIN_REPORT. DOMAIN_FILE_ERRORS	ドメイン指定ファイルでエラーが検出された場合に送信されます。	Critical
PERIODIC_REPORTS. DOMAIN_REPORT.FILE_ EMPTY	ドメイン指定ファイルが空の場合に送信されます。	Critical
PERIODIC_REPORTS. DOMAIN_REPORT.FILE_ MISSING	ドメイン指定ファイルが見つからない場合に送信されます。	Critical
REPORTD.DATABASE_ OPEN_FAILED_ALERT	レポート エンジンがデータベースを開けない場合に送信されます。	Critical
REPORTD.AGGREGATIO N_DISABLED_ALERT	システムのディスク領域が不足している場合に送信されます。ログ エントリに関するディスク使用率がログ使用率のしきい値を超過すると、reportd は集約をディセーブルにし、アラートを送信します。	Warning
REPORTING.CLIENT. UPDATE_FAILED_ALERT	レポート エンジンがレポート データを保存できなかった場合に送信されます。	Warning
REPORTING.CLIENT. JOURNAL.FULL	レポート エンジンが新規データを保存できない場合に送信されます。	Critical
REPORTING.CLIENT. JOURNAL.FREE	レポート エンジンが再び新規データを保存できるようになった場合に送信されます。	Information
PERIODIC_REPORTS. REPORT_TASK.BUILD_ FAILURE_ALERT	レポート エンジンがレポートを作成できない場合に送信されます。	Critical
PERIODIC_REPORTS. REPORT_TASK.EMAIL_ FAILURE_ALERT	レポートを電子メールで送信できなかった場合に送信されます。	Critical
PERIODIC_REPORTS. REPORT_TASK.ARCHIVE _FAILURE_ALERT	レポートをアーカイブできなかった場合に送信されます。	Critical
SENDERBASE.ERROR	SenderBase からの応答を処理中にエラーが発生した場合に送信されます。	Information
SMAD.ICCM.ALERT_PUS H_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。	Warning
SMAD.TRANSFER. TRANSFERS_STALLED	SMA ログがトラッキング データを 2 時間取得できなかった場合、またはレポーティング データを 6 時間取得できなかった場合に送信されます。	Warning
SMTPAUTH.FWD_SERVE R_FAILED_ALERT	SMTP 認証転送サーバが到達不能である場合に送信されます。	Warning
SMTPAUTH.LDAP_QUERY _FAILED	LDAP クエリーが失敗した場合に送信されます。	Warning

表 13-4　システム アラートのリスト（続き）

アラート名	説明	重大度
SYSTEM.HERMES_SHUTDOWN_FAILURE.REBOOT	リブート中のシステムをシャットダウンしている際に問題が発生した場合に送信されます。	Warning
SYSTEM.HERMES_SHUTDOWN_FAILURE.SHUTDOWN	システムをシャットダウンしている際に問題が発生した場合に送信されます。	Warning
SYSTEM.RCPTVALIDATION.UPDATE_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。	Critical
SYSTEM.SERVICE_TUNNEL.DISABLED	Cisco IronPort サポート サービス用に作成されたトンネルがディセーブルの場合に送信されます。	Information
SYSTEM.SERVICE_TUNNEL.ENABLED	Cisco IronPort サポート サービス用に作成されたトンネルがイネーブルの場合に送信されます。	Information

ネットワーク設定値の変更

このセクションでは、Cisco IronPort アプライアンスのネットワーク操作の設定に使用する機能について説明します。これらの機能では、「システム セットアップ ウィザードの実行」（P.2-10）でシステム セットアップ ウィザードを利用して設定したホスト名、DNS、およびルーティングの設定値に直接アクセスできます。

ここでは、次の機能について説明します。

- `sethostname`
- DNS 設定（GUI で設定。および CLI で `dnsconfig` コマンドを使用して設定）
- ルーティング設定（GUI で設定。および CLI で `routeconfig` コマンドと `setgateway` コマンドを使用して設定）
- `dnsflush`
- パスワード

システム ホスト名の変更

ホスト名は、CLI プロンプトでシステムを識別する際に使用されます。完全修飾ホスト名を入力する必要があります。`sethostname` コマンドは、Cisco IronPort 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 システム設定値の設定

Cisco IronPort アプライアンスのドメイン ネーム システム（DNS）は、GUI の [Management Appliance] > [Network] > [DNS] ページ、または dnsconfig コマンドを使用して設定できます。

次の設定値を設定できます。

- インターネットの DNS サーバまたはユーザ独自の DNS サーバを利用するか、および使用するサーバ
- DNS トラフィックに使用するインターフェイス
- 逆引き DNS ルックアップがタイムアウトするまで待機する秒数
- DNS キャッシュのクリア

DNS サーバの指定

AsyncOS では、インターネットのルート DNS サーバ、ユーザ独自の DNS サーバ、インターネットのルート DNS サーバ、または指定した権威 DNS サーバを使用できます。インターネットのルート サーバを使用するときは、特定のドメインに使用する代替サーバを指定することもできます。代替 DNS サーバは単一のドメインに適用されるため、該当ドメインに対する権威サーバ（最終的な DNS レコードを提供）になっている必要があります。

AsyncOS では、インターネットの DNS サーバを使用しない場合に「スプリット」DNS サーバをサポートしています。ユーザ独自の内部サーバを使用している場合は、例外のドメインおよび関連する DNS サーバを指定することもできます。

「スプリット」DNS を設定しているときは、in-addr.arpa（PTR）エントリも同様に設定する必要があります。このため、たとえば「.eng」クエリーをネームサーバ 1.2.3.4 にリダイレクトする際に、すべての .eng エントリが 172.16 ネットワークにある場合、スプリット DNS 設定に「eng,16.172.in-addr.arpa」をドメインとして指定する必要があります。

複数エントリとプライオリティ

入力する各 DNS サーバに、数値でプライオリティを指定できます。AsyncOS では、プライオリティが 0 に最も近い DNS サーバの使用を試みます。その DNS サーバが応答しない場合、AsyncOS は次のプライオリティを持つサーバの使用を試みます。同じプライオリティを持つ DNS サーバに複数のエントリを指定する場合、システムはクエリーを実行するたびに同じプライオリティを持つ DNS サーバをリストからランダムに選びます。次にシステムは最初のクエリーが期限切れになるか、「タイムアウト」になるまで短時間待機した後、さらにそれよりわずかに長い秒数待機するという動作を続けます。待機時間の長さは、DNS サーバの実際の総数と、設定されたプライオリティによって異なります。タイムアウトの長さはプライオリティに関係なく、すべての IP アドレスで同じです。最初のプライオリティには最も短いタイムアウトが設定されており、次のプライオリティにはより長いタイムアウトが設定されています。最終的なタイムアウト時間は約 60 秒です。1 つのプライオリティを設定している場合、

該当のプライオリティに対する各サーバのタイムアウトは 60 秒になります。2 つのプライオリティを設定している場合、最初のプライオリティに対する各サーバのタイムアウトは 15 秒になり、次のプライオリティに対する各サーバのタイムアウトは 45 秒になります。プライオリティが 3 つの場合、タイムアウトは 5 秒、10 秒、45 秒になります。

たとえば、4 つの DNS サーバを設定し、2 つにプライオリティ 0 を、1 つにプライオリティ 1 を、もう 1 つにプライオリティ 2 を設定したとします。

表 13-5　DNS サーバ、プライオリティ、およびタイムアウト間隔の例

プライオリティ	サーバ	タイムアウト（秒）
0	1.2.3.4、1.2.3.5	5、5
1	1.2.3.6	10
2	1.2.3.7	45

AsyncOS は、プライオリティ 0 に設定された 2 つのサーバをランダムに選択します。プライオリティ 0 のサーバの 1 つがダウンしている場合は、もう 1 つのサーバが使用されます。プライオリティ 0 のサーバが両方ダウンしている場合、プライオリティ 1 のサーバ（1.2.3.6）が使用され、最終的にプライオリティ 2（1.2.3.7）のサーバが使用されます。

タイムアウト時間はプライオリティ 0 のサーバは両方とも同じであり、プライオリティ 1 のサーバにはより長い時間が設定され、プライオリティ 2 のサーバにはさらに長い時間が設定されます。

インターネット ルート サーバの使用

AsyncOS DNS リゾルバは、高性能な電子メール配信に必要な大量の同時 DNS 接続を収容できるように設計されています。

（注） デフォルト DNS サーバにインターネット ルート サーバ以外を設定することを選択した場合、設定されたサーバは権威サーバとなっていないドメインのクエリーを再帰的に解決できる必要があります。

逆引き DNS ルックアップのタイムアウト

Cisco IronPort アプライアンスは電子メールの送受信の際に、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」（P.13-43）で説明されている一般的な DNS タイムアウトには適用されません。

デフォルト値は、20 秒です。秒数に「0」を入力することで、すべてのリスナーに対してグローバルに逆引き DNS ルックアップのタイムアウトをディセーブルにできます。値を 0 秒に設定した場合、逆引き DNS ルックアップは試行されず、代わりに標準のタイムアウト応答がすぐに返されます。

DNS アラート

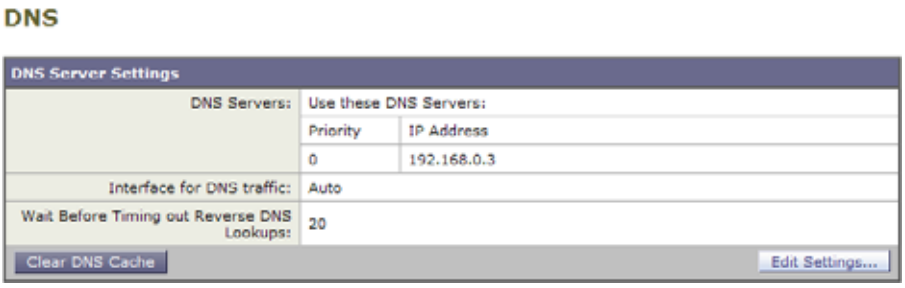
アプライアンスのリブート時に、メッセージ「Failed to bootstrap the DNS cache」が付与されたアラートが生成される場合がまれにあります。このメッセージは、システムによるプライマリ DNS サーバへの問い合わせができなかったことを示しています。この事象は、ネットワーク接続が確立される前に DNS サブシステムがオンラインになった場合、ブートのタイミングで発生します。このメッセージが別のタイミングで表示された場合、ネットワーク問題が発生しているか、または DNS 設定で有効なサーバが指定されていないことを示しています。

DNS キャッシュのクリア

GUI の [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、『*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

図 13-18　　[DNS] ページ



ステップ 1　[Management Appliance] > [Network] > [DNS] ページで、[Edit Settings] ボタンをクリックします。

ステップ 2　インターネットのルート DNS サーバまたはユーザ独自の DNS サーバのどちらを使用するかを選択して、権威 DNS サーバを指定します。

ステップ 3　ユーザ独自の DNS サーバを使用するか、権威 DNS サーバを指定する場合は、サーバ ID を入力し [Add Row] をクリックします。各サーバでこの作業を繰り返します。ユーザ独自の DNS サーバを入力する場合は、プライオリティも同時に指定します。詳細については、「DNS サーバの指定」（P.13-43）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、[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 [Management Appliance] > [Network] > [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

[Management Appliance] > [Network] > [Routing] ページを使用して、スタティック ルートの作成、編集、または削除を行えます。このページからデフォルト ゲートウェイの変更もできます。

スタティック ルートの追加

ステップ 1　[Management Appliance] > [Network] > [Routing] ページで、ルート リストの [Add Route] をクリックします。ルートの名前を入力します。

ステップ 2　宛先 IP アドレスを入力します。

ステップ 3　ゲートウェイの IP アドレスを入力します。

ステップ 4　変更を送信し、保存します。

スタティック ルートの削除

ステップ 1　[Static Routes] のリストから、スタティック ルート名に対応するゴミ箱アイコンをクリックします。

ステップ 2　表示される警告ダイアログで [Delete] をクリックして削除を確認します。

ステップ 3　変更を保存します。

スタティック ルートの編集

ステップ 1　[Static Routes] のリストでルートの名前をクリックします。

ステップ 2　ルートの設定を変更します。

ステップ 3　変更を送信し、保存します。

デフォルト ゲートウェイの変更（GUI）

ステップ 1　[Routing] ページのルート リストで [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 [Management Appliance] > [Network] > [Routing] ページ（「デフォルト ゲートウェイの変更（GUI）」（P.13-46）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。

admin ユーザのパスワード変更

admin ユーザのパスワードは GUI または CLI から変更できます。

GUI を使用してパスワードを変更するには、[Management Appliance] > [System Administration] > [Users] ページに移動します。詳細については、「パスワードの設定と変更」（P.12-13）を参照してください。

`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。パスワードは 6 文字以上である必要があります。`password` コマンドでは、セキュリティのために古いパスワードの入力が必要です。

（注）　パスワードの変更はすぐに有効になり、**commit** コマンドの実行は不要です。

システム時刻の設定

Cisco IronPort アプライアンスのシステム時刻を設定し、時間帯を指定できます。GUI の [Management Appliance] > [System Administration] > [Time Zone] ページと、[Management Appliance] > [System Administration] > [Time Settings] ページを使用します。または、CLI で `ntpconfig`、`settime`、および `settz` コマンドを使用します。

[Time Zone] ページ

[Time Zone] ページ（GUI の [System Administration] メニューから利用可能）では、Cisco IronPort アプライアンスの時間帯が表示されます。特定の時間帯または GMT オフセットを選択できます。

時間帯の選択

Cisco IronPort アプライアンスの時間帯を設定するには、次の手順を実行します。

ステップ 1　[Management Appliance] > [System Administration] > [Time Zone] を選択します。

ステップ 2　[Edit Settings] をクリックします。

ステップ 3　地域、国、および時間帯を選択します。

ステップ 4　変更を送信し、保存します。

GMT オフセットの選択

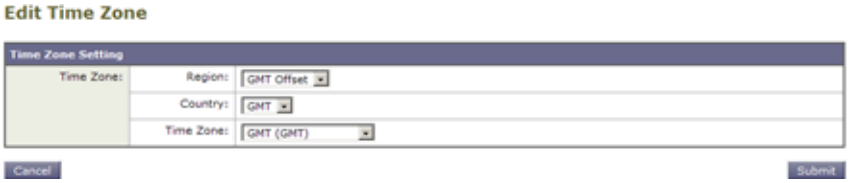
Cisco IronPort アプライアンスの GMT オフセットを設定するには、次の手順を実行します。

ステップ 1　[Management Appliance] > [System Administration] > [Time Zone] を選択します。

ステップ 2　[Edit Settings] をクリックします。

ステップ 3　地域のリストから [GMT Offset] を選択します。[Time Zone Setting] ページが更新され、[Time Zone] フィールドに GMT オフセットが含まれるようになります。

図 13-19　GMT オフセットの設定



ステップ 4　[Time Zone] フィールドでオフセットを選択します。オフセットとは、グリニッジ子午線のローカル時間であるグリニッジ標準時（GMT）に、加算または減算する時間のことです。時間の前にマイナス記号（「-」）が付いている場合、グリニッジ子午線の西側にあたります。プラス記号（「+」）の場合、グリニッジ子午線の東側にあたります。

ステップ 5　変更を送信し、保存します。

（注）　セキュリティ管理アプライアンスは、レポートのデータを収集する際に、セキュリティ管理アプライアンス上で時間設定を行った際に設定した情報からタイム スタンプを適用します。セキュリティ管理アプライアンスが情報を収集する方法の詳細については、「セキュリティ アプライアンスによるレポート用データの収集方法」（P.3-2）を参照してください。

時間帯ファイルの更新

いずれかの国の時間帯に変更があった場合は必ず、アプライアンスでこれらの時間帯ファイルを更新する必要があります。

時間帯ファイルの更新は、GUI で行うか、CLI の `tzupdate` コマンドを使用して行えます。

時間帯ファイルの自動更新

ステップ 1　[Management Appliance] > [System Administration] > [Update Settings] を選択します。

ステップ 2　[Enable automatic updates for Time zone rules] チェックボックスをオンにします。

ステップ 3　間隔を入力します。重要な情報については、ページ上の [?] ヘルプをクリックします。

ステップ 4　まだ実行していない場合は、このページの他の設定値を設定します。「アップグレードおよびサービス アップデートの設定」（P.13-20）を参照してください。

時間帯ファイルの手動更新

ステップ 1　[Management Appliance] > [System Administration] > [Time Settings] を選択します。

ステップ 2　[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、[Update Now] をクリックします。

時刻設定の編集

セキュリティ管理アプライアンスでシステム時刻を設定します。

ネットワーク タイム プロトコル（NTP）サーバを使用したシステム時刻の設定

NTP サーバを使用すると、セキュリティ管理アプライアンス システム クロックがネットワーク上の他のコンピュータと同期されます。

ステップ 1　[Management Appliance] > [System Administration] > [Time Settings] ページで、[Edit Settings] をクリックします。

ステップ 2　[Use Network Time Protocol] を選択します。

ステップ 3　NTP サーバのアドレスを入力します。

ステップ 4　（任意）[Add Row] をクリックして別の NTP サーバを追加します。

ステップ 5　NTP サーバをリストから削除するには、サーバのゴミ箱アイコンをクリックします。

ステップ 6　NTP クエリー用のインターフェイスを選択します。これは、NTP クエリーが発信される IP アドレスになります。

ステップ 7　変更を送信し、保存します。

システム時刻の手動設定

ステップ 1　[Management Appliance] > [System Administration] > [Time Settings] ページで、[Edit Settings] をクリックします。

ステップ 2　[Set Time Manually] を選択します。

ステップ 3　日付を MM/DD/YYYY 形式で入力するか、カレンダーのアイコンをクリックして日付を選択します。

ステップ 4　ローカル時刻を HH:MM:SS の形式で入力します。

ステップ 5　変更を送信し、保存します。

[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」（P.13-50）
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」（P.13-50）
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 データベースのバックアップと復元」（P.7-14）
設定のリセット	出荷時の初期状態へのリセット

コンフィギュレーション設定の保存とインポート

（注）　ここで説明されているコンフィギュレーション ファイルは、セキュリティ管理アプライアンスの設定に使用されます。第 8 章「Web セキュリティ アプライアンスの管理」で説明されているコンフィギュレーション ファイルおよび Configuration Master は、Web セキュリティ アプライアンスの設定に使用されます。

セキュリティ管理アプライアンスの大部分の設定は、1 つのコンフィギュレーション ファイルで管理できます。このファイルは Extensible Markup Language（XML）フォーマットで保持されます。

次のように、このファイルはさまざまな用途に使用できます。

- プライマリ セキュリティ管理アプライアンスで予期しない障害が発生した場合に、2 番目のセキュリティ管理アプライアンスをすばやく設定し、サービスを復元できます。
- コンフィギュレーション ファイルを別のシステムに保存し、重要な設定データをバックアップおよび保持できます。アプライアンスの設定中に間違いを犯した場合、保存した最新のコンフィギュレーション ファイルにロールバックできます。
- 既存のコンフィギュレーション ファイルをダウンロードし、アプライアンスの全体の設定を素早く確認できます（新しいブラウザの多くには XML ファイルを直接レンダリングする機能が含まれています）。これは、現在の設定にある可能性のあるマイナー エラー（誤植など）のトラブルシューティングに役立つ場合があります。
- 既存のコンフィギュレーション ファイルをダウンロードして、変更を行い、同じアプライアンスにアップロードできます。この場合は、実質的に設定の変更を行うために CLI と GUI の両方が「バイパス」されます。
- FTP を介してコンフィギュレーション ファイル全体をアップロードしたり、コンフィギュレーション ファイルの一部を CLI に直接貼り付けたりすることができます。
- このファイルは XML 形式になっているため、コンフィギュレーション ファイルのすべての XML エンティティが記述された、関連する文書型定義（DTD）も提供されます。XML コンフィギュレーション ファイルをアップロードする前にこの DTD をダウンロードして XML コンフィギュレーション ファイルを検証できます（XML 検証ツールはインターネットで簡単に入手できます）。

XML コンフィギュレーション ファイルを使用した複数のアプライアンスの管理

警告　ある セキュリティ管理アプライアンスから別の セキュリティ管理アプライアンスにコンフィギュレーション ファイルをインポートする場合は、次の点に注意してください。

元の設定内のすべて（IP アドレスを含む）が、コンフィギュレーション ファイルに含まれています。コンフィギュレーション ファイルを編集して IP アドレスを変更するか、元の セキュリティ管理アプライアンスがオフラインになっていることを確認します。

また、SSH 認証接続が終了することに注意してください。そうなった場合は、接続されたすべての Web セキュリティ アプライアンスおよび 電子メール セキュリティ アプライアンスとの接続を再確立する必要があります。

- ある Cisco IronPort アプライアンスから既存のコンフィギュレーション ファイルをダウンロードし、変更を行い、別のアプライアンスにアップロードできます。これにより、複数の Cisco IronPort アプライアンスのインストール済み環境の管理が容易になります。ただし、電子メール セキュリティ アプライアンスからセキュリティ管理アプライアンスに、コンフィギュレーション ファイルをロードすることはできません。
- あるアプライアンスからダウンロードされた既存のコンフィギュレーション ファイルを、複数のサブセクションに分割できます。（複数のアプライアンス環境の）すべてのアプライアンスで共通するこれらのセクションを変更し、サブセクションの更新時にこれらのセクションを他のアプライアンスにロードできます。

  たとえば、Global Unsubscribe コマンドをテストするためにテスト環境でアプライアンスを使用できます。グローバル配信停止リストを適切に設定した場合は、テスト アプライアンスのグローバル配信停止設定セクションをすべての実稼働アプライアンスにロードできます。

GUI を使用したコンフィギュレーション ファイルの管理

アプライアンスでコンフィギュレーション ファイルを管理するには、[Management Appliance] > [System Administration] > [Configuration File] を選択します。

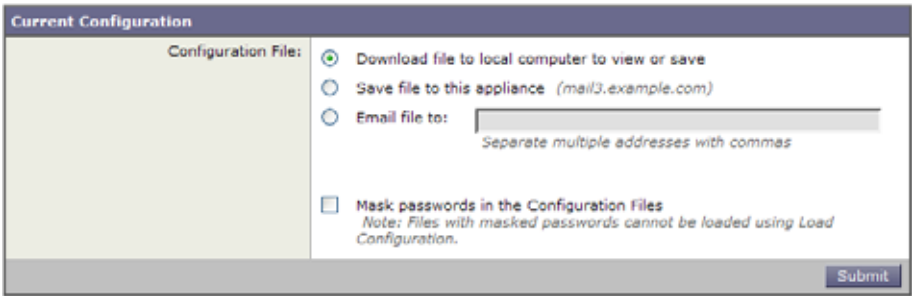
[Configuration File] ページには、次のセクションが含まれています。

- [Current Configuration]：現在のコンフィギュレーション ファイルを保存およびエクスポートするために使用します
- [Load Configuration]：コンフィギュレーション ファイルの全体または一部をロードするために使用します
- [End-User Safelist/Blocklist Database (Cisco IronPort Spam Quarantine)]：セーフリスト/ブロックリスト データベースの管理に使用します
- [Reset Configuration]：現在の設定を出荷時デフォルト値にリセットするために使用します（リセット前に設定を保存する必要があります）

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

[Management Appliance] > [System Administration] > [Configuration File] ページの [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。

図 13-20　現在のコンフィギュレーション ファイル



チェックボックスをオンすると、ユーザのパスワードをマスクできます。パスワードをマスクすると、元の暗号化されたパスワードが、エクスポートまたは保存されたファイルで「*****」に置き換えられます。

（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。

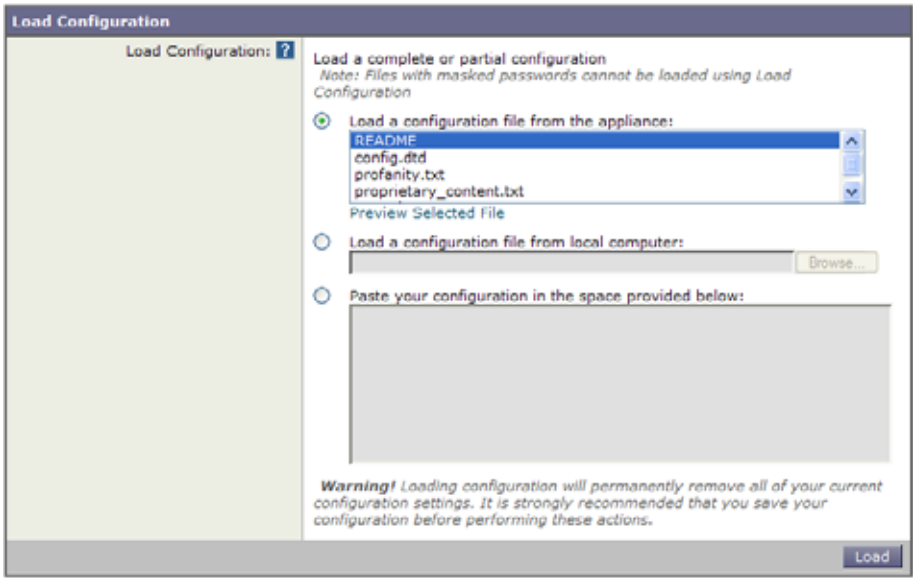
コンフィギュレーション ファイルのロード

[Management Appliance] > [System Administration] > [Configuration File] ページの [Load Configuration] セクションを使用して、新しい設定情報を Cisco IronPort アプライアンスにロードします。情報は次の 3 つのいずれかの方法でロードできます。

- `configuration` ディレクトリに情報を格納し、アップロードする
- コンフィギュレーション ファイルをローカル マシンから直接アップロードする
- GUI に設定情報を直接貼り付ける

パスワードがマスクされたコンフィギュレーション ファイルはロードできません。

図 13-21　コンフィギュレーション ファイルのロード



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、Cisco IronPort アプライアンスの configuration ディレクトリにある DTD を使用して解析および検証されます。DTD ファイルの名前は config.dtd です。loadconfig コマンドを使用したときにコマンド ラインで検証エラーが報告された場合、変更はロードされません。コンフィギュレーション ファイルをアップロードする前に、アプライアンスの外部で DTD をダウンロードし、コンフィギュレーション ファイルを検証できます。

いずれの方法の場合でも、コンフィギュレーション ファイル全体（最上位のタグである <config></config> 間で定義された情報）またはコンフィギュレーション ファイルの *complete* および *unique* サブセクション（上記の宣言タグが含まれ、<config></config> タグ内に存在する場合）をインポートできます。

「complete（完全）」とは、DTD で定義されたサブセクションの開始タグおよび終了タグ全体が含まれることを意味します。たとえば、次のコードをアップロードまたは貼り付けると、検証エラーが発生します。

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<config>
 <autosupport_enabled>0</autosu
</config>
```

しかし、次のコードをアップロードまたは貼り付けても、検証エラーは発生しません。

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<config>
 <autosupport_enabled>0</autosupport_enabled>
</config>
```

「unique（一意）」とは、アップロードまたは貼り付けられるコンフィギュレーション ファイルのサブセクションが、設定として多義的でないことを意味します。たとえば、システムは 1 つのホスト名しか持てないため、次のコード（宣言および <config></config> タグを含む）をアップロードすることは可能です。

```
<hostname>mail4.example.com</hostname>
```

しかし、システムにはそれぞれ異なる受信者アクセス テーブルが定義された複数のリスナーが定義されている可能性があるため、次のコードのみをアップロードすることは多義的であると見なされます。

```
     <rat>
        <rat_entry>
   <rat_address>ALL</rat_address>
   <access>RELAY</access>
  </rat_entry>
  </rat>
```

多義的であるため、「完全」な構文であっても許可されません。

警告　コンフィギュレーション ファイルまたはコンフィギュレーション ファイルのサブセクションをアップロードまたは貼り付ける場合は、待機中の可能性がある、保存されていない変更が破棄されることがあります。

空のタグと省略されたタグ

コンフィギュレーション ファイルのセクションをアップロードまたは貼り付ける場合は注意が必要です。タグを含めないと、コンフィギュレーション ファイルのアップロード時に設定の値が変更されません。ただし、空白タグを含めると、設定の問題が解消されます。

たとえば、次のコードをアップロードすると、システムからすべてのリスナーが削除されます。

```
<listeners></listeners>
```

警告　コンフィギュレーション ファイルのサブセクションをアップロードしたり、貼り付けたりした場合、GUI または CLI から切断され、大量の設定データが破壊されることがあります。別のプロトコル、シリアル インターフェイス、または管理ポートのデフォルト設定を使用してアプライアンスに再接続できない場合は、このコマンドでサービスをディセーブルにしないでください。また、DTD で定義された設定構文がよくわからない場合は、このコマンドを使用しないでください。新しいコンフィギュレーション ファイルをロードする前に、必ず設定データをバックアップしてください。

ログ サブスクリプションのパスワードのロードについての注意事項

パスワードが必要なログ サブスクリプションを含むコンフィギュレーション ファイルをロードしようとしても（たとえば、FTP プッシュを使用）、`loadconfig` コマンドは不明なパスワードについて警告しません。FTP プッシュが失敗し、`logconfig` コマンドを使用して正しいパスワードを設定するまで警告が生成されます。

文字セット エンコーディングについての注意事項

XML コンフィギュレーション ファイルの「encoding」属性は、ファイルをオフラインで操作するために使用している文字セットに関係なく、「`ISO-8859-1`」である必要があります。`showconfig` コマンド、`saveconfig` コマンド、または `mailconfig` コマンドを発行するたびに、エンコーディング属性がファイルで指定されます。

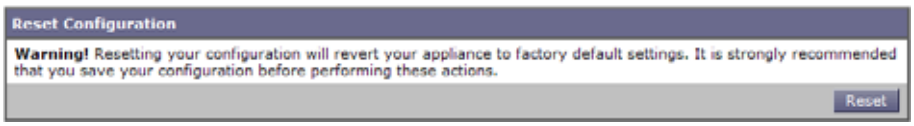
```
<?xml version="1.0" encoding="ISO-8859-1"?>
```

現時点では、このエンコーディングを持つコンフィギュレーション ファイルだけをロードできます。

現在の設定のリセット

現在の設定をリセットすると、Cisco IronPort アプライアンスが元の出荷時デフォルト値に戻ります。リセットする前に設定を保存してください。GUI の [Reset] ボタンを使用した設定のリセットは、クラスタリング環境ではサポートされていません。

図 13-22　コンフィギュレーション ファイルのリセット



「出荷時の初期状態へのリセット」（P.13-5）を参照してください。

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
- resetconfig（「出荷時の初期状態へのリセット」（P.13-5）を参照）
- publishconfig
- backupconfig

showconfig、mailconfig、および saveconfig コマンド

コンフィギュレーション コマンドの showconfig、mailconfig、および saveconfig の場合は、電子メールで送信されるファイルまたは表示されるファイルにパスワードを含めるかどうか選択することを求められます。パスワードを含めないことを選択すると、パスワード フィールドが空白のままになります。セキュリティの問題を心配する場合は、パスワードを含めないことを選択できます。ただし、loadconfig コマンドを使用してロードされた場合、パスワードがないコンフィギュレーション ファイルは失敗します。「ログ サブスクリプションのパスワードのロードについての注意事項」（P.13-54）を参照してください。

（注）　パスワードを含めることを選択した場合（「Do you want to include passwords?」に「yes」と回答します）にコンフィギュレーション ファイルを保存、表示、または電子メールで送信するとき、パスワードは暗号化されます。ただし、秘密キーと証明書は暗号化されていない PEM フォーマットで含まれます。

showconfig コマンドは現在の設定を画面に出力します。

```
mail3.example.com> showconfig

Do you want to include passwords? Please be aware that a configuration without passwords
will fail when reloaded with loadconfig.

<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">

<!--
 Product: Cisco IronPort model number Messaging Gateway Appliance(tm)
 Model Number: model number
 Version: version of AsyncOS installed
 Serial Number: serial number
 Current Time: current time and date
[The remainder of the configuration file is printed to the screen.]
```

mailconfig コマンドを使用して、現在の設定をユーザに電子メールで送信します。メッセージには config.xml という名前の XML 形式のコンフィギュレーション ファイルが添付されます。

```
mail3.example.com> mailconfig

Please enter the email address to which you want to send
```

```
the configuration file.
[]> administrator@example.com

Do you want to include passwords? Please be aware that a configuration without passwords
will fail when reloaded with loadconfig. [N]> y

The configuration file has been sent to administrator@example.com.
```

セキュリティ管理アプライアンスで saveconfig コマンドを使用すると、一意のファイル名を使用して、すべての Configuration Master 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

Cisco IronPort アプライアンスに新しい設定情報をロードするには、loadconfig コマンドを使用します。情報は次の 2 つのいずれかの方法でロードできます。

- configuration ディレクトリに情報を格納し、アップロードする
- CLI に設定情報を直接貼り付ける。

詳細については、「コンフィギュレーション ファイルのロード」（P.13-52）を参照してください。

publishconfig コマンド

変更を Configuration Master に公開するには、publishconfig コマンドを使用します。構文は次のとおりです。

publishconfig *config_master* [*job_name*] [*host_list* | *host_ip*

ここで、*config_master* は、「SMA 互換性マトリクス」（P.2-2）の表 2-3 に示すとおり、サポートされている Configuration Master です。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] > [Utilities] > [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] > [Utilities] > [Publish] > [Publish History] により、[Publish History] ページに進むことができます。

backupconfig コマンド

アクティブなデータセットを「ソース」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、元の「ソース」セキュリティ管理アプライアンスの中断を最小限に抑えてコピーするには、backupconfig コマンドを使用します。

このコマンドとその使用法、およびデータセットのバックアップの詳細については、「セキュリティ管理アプライアンスのバックアップ」（P.13-6）を参照してください。

CLI を使用した設定変更のアップロード

ステップ 1　CLI の外部で、アプライアンスの configuration ディレクトリにアクセスできることを確認します。詳細については、付録 A「IP インターフェイスおよびアプライアンスへのアクセス」を参照してください。

ステップ 2　コンフィギュレーション ファイル全体またはコンフィギュレーション ファイルのサブセクションをアプライアンスの configuration ディレクトリに格納するか、saveconfig コマンドで作成した既存の設定を編集します。

ステップ 3　CLI 内で、loadconfig コマンドを使用して、ステップ 2 で示されたディレクトリに格納したコンフィギュレーション ファイルをロードするか、テキスト（XML 構文）を CLI に直接貼り付けます。

この例では、changed.config.xml という名前のファイルがアップロードされ、変更が保存されます。

```
mail3.example.com> loadconfig

1. Paste via CLI
2. Load from file
[1]> 2

Enter the name of the file to import:
[]> changed.config.xml

Values have been loaded.
Be sure to run "commit" to make these settings active.
mail3.example.com> commit
```

この例では、新しいコンフィギュレーション ファイルをコマンド ラインに直接貼り付けます（空白行で Ctrl を押した状態で D を押すと貼り付けコマンドが終了します）。次に、システム セットアップ ウィザードを使用して、デフォルトのホスト名、IP アドレス、およびゲートウェイ情報を変更します。（詳細は、「システム セットアップ ウィザードの実行」（P.2-10）を参照してください）。これで、変更が確定されます。

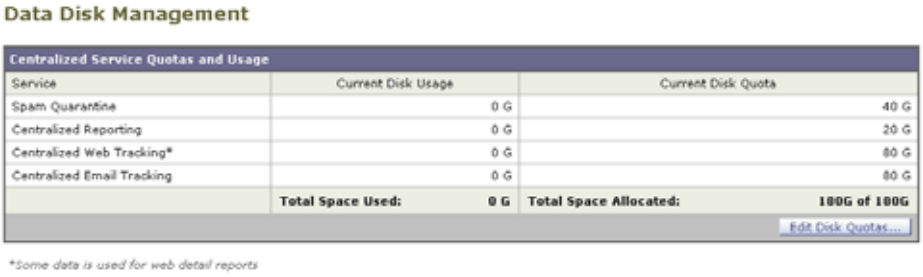
```
mail3.example.com> loadconfig

1. Paste via CLI
2. Load from file
[1]> 1

Paste the configuration file now. Press CTRL-D on a blank line when done.

[The configuration file is pasted until the end tag </config>. Control-D is entered on a
separate line.]

Values have been loaded.
Be sure to run "commit" to make these settings active.

mail3.example.com> commit

Please enter some comments describing your changes:
```

```
[]> pasted new configuration file and changed default settings
```

ディスク使用量の管理

[Management Appliance] > [System Administration] > [Disk Management] ページを使用して、セキュリティ管理アプライアンスでのモニタリング サービス（Cisco IronPort スパム隔離、中央集中型レポーティング、中央集中型 Web トラッキング、および中央集中型電子メール トラッキング）に割り当てられたディスク領域量を表示または変更します。これらの 4 つのサービスに割り当てられるディスクの合計容量は、次の例に示されているように、アプライアンスのモニタリング サービスに割り当てられるディスク領域の合計容量になります。

図 13-23　[Disk Management] ページ



複数のサービスがイネーブルの場合のディスク領域に関する重要な情報

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 レポーティングだけをイネーブルにすると、領域はすべて電子メール レポーティング専用になります。反対に、中央集中型 Web レポーティングをオンにすると、領域はすべて Web レポーティング データに使用されます。両方をオンにした場合、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。

使用可能な最大ディスク領域

表 13-6 は、セキュリティ管理アプライアンスでの中央集中型レポーティング、中央集中型電子メール トラッキング、中央集中型 Web トラッキング、および Cisco IronPort スパム隔離（ISQ）に使用可能なディスク領域の最大量を示しています。サイズはすべてギガバイト（GB）単位で表示されています。

表 13-6　使用可能な最大ディスク領域

使用可能なディスク領域	ハードウェア プラットフォーム									
	M160	M170	M600	M650	M660	M670	M1000	M1050	M1060	M1070
ISQ + レポーティング + 電子メール トラッキング + Web トラッキング	165	165	187	187	681	681	429	429	1053	1409
ISQ 最大	70	70	100	100	150	150	200	200	265	265

（注）　レポーティング（単なるカウンター）や、トラッキング（限定的な量のヘッダー情報だけを保存）とは異なり、ISQ は実際にハード ディスク上の隔離を受けたメッセージのすべてのメッセージ本文を保存するため、他の機能よりも、メッセージごとの使用ディスク領域が非常に多くなります。このように大量のディスク領域が使用されるため、すべてのハード ドライブを ISQ に割り当てると、アプライアンスがロックされる場合があります。このため、ISQ のディスク クォータには、単なる使用可能なディスク領域よりも厳しい制限があります。

ディスク領域量の再割り当てについて

[Edit Disk Quotas] をクリックして、各サービスに割り当てられているディスク領域の量を変更できます。たとえば、中央集中型トラッキングで、中央集中型レポーティングや Cisco IronPort スパム隔離よりも多くのハード ドライブ スペースが継続的に必要な場合は、中央集中型トラッキング サービスに割り当てらた領域を調整できます。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。

既存の割り当て量を少なくした場合、新しい割り当て量内にすべてのデータが収まるようになるまで、最も古いデータから削除されます。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。

中央集中型 Web レポーティングをイネーブルにしているが、レポーティングにディスク領域が割り当てられていない場合、ディスク領域が割り当てられるまで、中央集中型 Web レポーティングが機能しません。

ディスク領域量の再割り当て

各モニタリング サービスに割り当てられたディスク領域量を変更するには、次の手順を実行します。

ステップ 1　セキュリティ管理アプライアンスで、[Management Appliance] > [System Administration] > [Disk Management] を選択します。

ステップ 2　[Edit Disk Quotas] をクリックします。

ステップ 3　[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。

ISQ 以外のすべてのサービスに対して、0 からディスクの合計量までの値を入力できます。4 つすべてのサービスの合計ディスク クォータが、表示されている合計ギガバイト数になる必要があります。たとえば、使用可能な合計ディスク領域が 200 GB の場合に、中央集中型レポーティングに 25 GB、Cisco IronPort スパム隔離に 10 GB、中央集中型電子メール トラッキングに 35 GB を割り当てた場合、使用可能なディスク合計量の 200 GB を保つには、中央集中型 Web トラッキングに割り当てられるのは最大 130 GB になります。

ステップ 4　[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、[Set New Quotas] をクリックします。

ステップ 6　[Commit] をクリックして変更を保存します。

プリファレンスの 設定

セキュリティ管理アプライアンス 上で設定されている管理ユーザ

ローカル認証されたユーザは次のプリファレンスを選択できます。このプリファレンスは、ユーザがセキュリティ管理アプライアンスにログインするたびに適用されます。

- 言語（GUI および PDF レポートに適用）
- ランディング ページ（ログイン後に表示されるページ）
- レポート ページのデフォルトの時間範囲（使用可能なオプションは、電子メールおよび Web レポーティング ページのサブセットです）
- レポート ページの表に表示する行数

実際のオプションは、ユーザ ロールによって異なります。

これらのプリファレンスを設定するには、[Options] > [Preferences] を設定します。（[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、確定します。

ヒント　[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 [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、[Options] メニューで表示言語を直接選択できます。

CHAPTER 14

ロギング

セキュリティ管理アプライアンスの重要な機能に、ロギング機能があります。AsyncOS はさまざまな種類のログを生成し、さまざまな種類の情報を記録します。セキュリティ管理アプライアンスは、コマンドライン インターフェイス（CLI）外の、システム情報の重要なリソースとしてこれらのログを出力します。ログ ファイルには、システムのさまざまなコンポーネントによる通常動作、および例外が記録されます。この情報は、Cisco IronPort アプライアンスをモニタリングする場合に役立ちます。ログは、トラブルシューティングおよびパフォーマンスの評価にも使用できます。

ロギングの概要

ログは、AsyncOS の日常動作に関する重要な情報を収集する効率的な方法です。ログ ファイルには、Cisco IronPort アプライアンスのアクティビティに関する情報が記録されます。情報は、ログ ファイルのタイプによって異なります。たとえば、Cisco IronPort スパム隔離ログは、隔離に関する情報を記録し、Cisco IronPort メール テキスト ログは、アプライアンスを通過した電子メールに関する情報を記録します。

ほとんどのログは、プレーン テキスト（ASCII）形式で記録されますが、トラッキング ログはリソースの効率性を保つためにバイナリ形式で記録されます。ASCII テキスト情報は、任意のテキスト エディタで読むことができます。

ロギングとレポーティング

ロギング データは、メッセージ フローのデバッグ、基本的な日常の動作に関する情報の確認（FTP 接続の詳細、HTTP ログ ファイルなど）、アーカイブのコンプライアンスの目的に使用します。

このロギング データには、電子メール セキュリティ アプライアンスから直接アクセスすることも、任意の外部 FTP サーバに送信してアーカイブまたは読み取ることもできます。アプライアンスに FTP 接続してログにアクセスすることも、バックアップの目的でプレーン テキストのログを外部サーバにプッシュすることもできます。

レポーティング データを表示するには、アプライアンスのグラフィカル ユーザ インターフェイスの [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、セキュリティ管理アプライアンス以外には送信できません。

（注）　セキュリティ管理アプライアンスは、Cisco IronPort スパム隔離（ISQ）データの例外を含む、すべてのレポーティングおよびトラッキング情報を取り出します。ISQ データは、ESA から渡されます。

ログ タイプ

ログ サブスクリプションはログ タイプを名前、ログ レベル、およびファイル サイズや宛先情報などのその他の特性に関連付けます。コンフィギュレーション履歴ログ以外のすべてのログ タイプで、複数のサブスクリプションを使用できます。ログ タイプによってログに記録されるデータが決まります。ログ サブスクリプションを作成するときにログ タイプを選択します。詳細については、「ログ サブスクリプション」（P.14-22）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 14-1　　ログ タイプ

ログ タイプ	説明
認証ログ	認証ログには、ローカルまたは外部認証されたユーザおよびセキュリティ管理アプライアンスへの GUI および CLI の両方のアクセスについて、成功したログインと失敗したログイン試行が記録されます。 外部認証がオンの場合、デバッグおよびより詳細なモードでは、すべての LDAP クエリーがこれらのログに表示されます。
バックアップ ログ	バックアップ ログはバックアップ プロセスを開始から終了まで記録します。 バックアップ スケジューリングに関する情報は、SMA ログ内にあります。
CLI 監査ログ	CLI 監査ログには、システム上のすべての CLI アクティビティが記録されます。
コンフィギュレーション履歴ログ	コンフィギュレーション履歴ログは、どのようなセキュリティ管理アプライアンスの変更がいつ行われたかの情報を記録します。ユーザが変更をコミットするたびに、新しいコンフィギュレーション履歴ログが作成されます。
FTP サーバ ログ	FTP ログには、インターフェイスでイネーブルになっている FTP サービスの情報が記録されます。接続の詳細とユーザ アクティビティが記録されます。
HTTP ログ	HTTP ログには、インターフェイスでイネーブルになっている HTTP サービスおよびセキュア HTTP サービスに関する情報が記録されます。HTTP を介してグラフィカル ユーザ インターフェイス（GUI）にアクセスするため、HTTP ログは基本的に、CLI 監査ログの GUI 版になっています。セッション データ（新規セッション、期限切れセッションなど）、およびグラフィカル ユーザ インターフェイスでアクセスされたページが記録されます。
Haystack ログ	Haystack ログには、データ処理をトラッキングする Web トランザクションが記録されます。
テキスト メール ログ	テキスト メール ログには、電子メール システムの動作（メッセージの受信、メッセージの配信試行、接続の開始と終了、メッセージのバウンスなど）に関する情報が記録されます。 メール ログに添付ファイル名が含まれる場合に関する重要な情報については、「トラッキング サービスの概要」（P.6-1）を参照してください。

表 14-1　ログ タイプ（続き）

ログ タイプ	説明
LDAP デバッグ ログ	[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、[Test Server] ボタンや [Test Queries] ボタンをクリックした結果が記録されます。 失敗した LDAP 認証の詳細については、認証ログを参照してください。
NTP ログ	NTP ログには、アプライアンスと任意の設定済みネットワーク タイム プロトコル（NTP）サーバとの通信が記録されます。NTP サーバの設定の詳細については、「システム時刻の設定」（P.13-47）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た、レポーティング クエリーに関連付けられたアクションが記録されます。
SMA ログ	SMA ログには、一般的なセキュリティ管理アプライアンス プロセスに関連付けられたアクションが記録されます。中央集中型レポーティング、中央集中型トラッキング、Cisco IronPort スパム隔離サービスのプロセスは含まれません。 これらのログには、バックアップ スケジューリングに関する情報が含まれます。
SNMP ログ	SNMP ログには、SNMP ネットワーク管理エンジンに関連するデバッグ メッセージが記録されます。トレースまたはデバッグ モードでは、セキュリティ管理アプライアンスへの SNMP 要求が含まれます。
セーフリスト/ブロックリスト ログ	セーフリスト/ブロックリスト ログには、セーフリスト/ブロックリストの設定およびデータベースに関するデータが記録されます。
スパム隔離 GUI ログ	Cisco IronPort スパム隔離 GUI ログには、GUI を介した隔離設定、エンド ユーザ認証、エンド ユーザ アクション（例：電子メールの解放）など、Cisco IronPort スパム隔離 GUI に関連するアクションが記録されます。
スパム隔離ログ	Cisco IronPort スパム隔離ログには、Cisco IronPort スパム隔離プロセスに関連付けられたアクションが記録されます。
ステータス ログ	ステータス ログには、`status detail` および `dnsstatus` などの CLI ステータス コマンドで検出されたシステム統計情報が記録されます。記録期間は、`logconfig` の `setup` サブコマンドを使用して設定します。ステータス ログでレポートされるカウンタまたはレートは、前回カウンタがリセットされた時点からの値です。
システム ログ	システム ログには、ブート情報、DNS ステータス情報、および `commit` コマンドを使用してユーザが入力したコメントが記録されます。システム ログは、アプライアンスの状態のトラブルシューティングに役立ちます。
トラッキング ログ	トラッキング ログには、トラッキング サービスのプロセスに関連付けられたアクションが記録されます。トラッキング ログは、メール ログのサブセットになっています。
アップデータ ログ	時間帯のアップデートなど、サービス アップデートに関する情報。

ログ タイプの比較

表 14-2 に、各ログ タイプの特徴をまとめます。

表 14-2　ログ タイプの比較

						次の情報を格納					
	トランザクション	ステートレス	テキストとして記録	バイナリとして記録	ヘッダー ロギング	定期的なステータス情報	メッセージ受信情報	配信情報	個々のハードバウンス	個々のソフトバウンス	設定情報
認証ログ	•		•								
バックアップ ログ	•		•								
CLI 監査ログ	•		•			•					
コンフィギュレーション履歴ログ	•		•								•
FTP サーバ ログ	•		•			•					
HTTP ログ	•		•			•					
Haystack ログ	•		•								
テキスト メール ログ	•		•		•	•	•	•	•	•	
LDAP デバッグ ログ	•		•								
NTP ログ	•		•			•					
レポーティング ログ	•		•			•					
レポーティング クエリー ログ	•		•			•					
SMA ログ	•		•			•					
SNMP ログ	•		•								
セーフリスト/ブロックリスト ログ	•		•			•					
スパム隔離 GUI	•		•			•					
スパム隔離	•		•			•					
ステータス ログ		•	•			•					
システム ログ	•		•			•					
トラッキング ログ	•			•	•		•	•	•	•	
アップデータ ログ	•		•								

ログの取得

ログ ファイルは、表 14-3 に示すファイル転送プロトコルを使用して取得できます。プロトコルは、グラフィカル ユーザ インターフェイスでサブスクリプションを作成または編集するときに設定するか、CLI の logconfig コマンドを使用して設定します。

表 14-3　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、Cisco IronPort 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、Cisco IronPort 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、Cisco IronPort 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、SSH1 または 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、Cisco IronPort 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。この方式は、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。使用されるポートは 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ているファイル名、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）などです。保存済みのステータスを持つログ ファイルのみを転送する必要があります。

ログのロールオーバーおよび転送スケジュール

ログ サブスクリプションを作成するときに、ログのロールオーバー、古いファイルの転送、および新しいファイルの作成のトリガーを指定します。

次のトリガーのいずれかを選択します。

- ファイル サイズ
- 時間
  - 指定した間隔で（秒、分、時間、または日数）

    値を入力するときは、画面の例に従います。

2 時間半など、複合間隔を入力するには、例 2h30m に従います。

または

– 毎日、指定した時刻に

または

– 選択した週の曜日の指定した時刻に

時刻を指定する場合は、24 時間形式を使用します。たとえば 11pm は 23:00 です。

1 日に複数のロールオーバー時間をスケジュール設定するには、時間をカンマで区切ります。たとえば、深夜と正午にログをロールオーバーするには、00:00, 12:00 と入力します。

アスタリスク（*）をワイルドカードとして使用できます。
たとえば、正確に毎時および 30 分ごとにログをロールオーバーするには、*:00, *:30 と入力します。

指定した制限に達すると（またはサイズおよび時間の両方に基づいた制限を設定している場合は最初の制限に達すると）、ログ ファイルがロールオーバーされます。FTP ポーリング転送メカニズムに基づいたログ サブスクリプションでは、ファイルが作成されると、それらのファイルが取得されるか、システムでログ ファイル用にさらにスペースが必要になるまで、Cisco IronPort 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。

デフォルトでイネーブルになるログ

セキュリティ管理アプライアンスは、次のログ サブスクリプションがイネーブルに事前設定されています。

表 14-4　事前設定されたログ サブスクリプション

ログ名	ログ タイプ	取得方法
cli_logs	CLI 監査ログ	FTP ポーリング
euq_logs	Cisco IronPort スパム隔離ログ	FTP ポーリング
euqgui_logs	Cisco IronPort スパム隔離 GUI ログ	FTP ポーリング
gui_logs	HTTP ログ	FTP ポーリング
mail_logs	Cisco IronPort テキスト メール ログ	FTP ポーリング
reportd_logs	レポーティング ログ	FTP ポーリング
reportqueryd_logs	レポーティング クエリー ログ	FTP ポーリング
slbld_logs	セーフリスト/ブロックリスト ログ	FTP ポーリング
smad_logs	SMA ログ	FTP ポーリング
system_logs	システム ログ	FTP ポーリング
trackerd_logs	トラッキング ログ	FTP ポーリング

事前定義されているすべてのログ サブスクリプションでは、ログ レベルが Information に設定されています。ログ レベルの詳細については、「ログ レベルの設定」（P.14-23）を参照してください。

適用されているライセンス キーによっては、追加のログ サブスクリプションを設定できます。ログ サブスクリプションの作成および編集については、「ログ サブスクリプション」（P.14-22）を参照してください。

ログ タイプ

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

コンフィギュレーション履歴ログの使用

コンフィギュレーション履歴ログは、コンフィギュレーション ファイルで構成され、ユーザの名前、ユーザが変更を行った設定の場所の説明、変更を保存するときにユーザが入力したコメントがリストされた追加のセクションがあります。ユーザが変更をコミットするたびに、変更後のコンフィギュレーション ファイルを含む新しいログが作成されます。

コンフィギュレーション履歴ログの例

次のコンフィギュレーション履歴ログの例は、システムにログインできるローカル ユーザを定義するテーブルに、ユーザ（admin）がゲスト ユーザを追加したことを示しています。

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<!--
 XML generated by configuration change.
 Change comment: added guest user
 User: admin
 Configuration are described as:
```

```
 This table defines which local users are allowed to log into the system.
 Product: Cisco IronPort M160 Messaging Gateway(tm) Appliance
 Model Number: M160
 Version: 6.7.0-231
 Serial Number: 000000000ABC-D000000
 Number of CPUs: 1
 Memory (GB): 4
 Current Time: Thu Mar 26 05:34:36 2009
 Feature "Cisco IronPort 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 14-5 に、CLI 監査ログに記録される統計情報を示します。

表 14-5　CLI 監査ログの統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
PID	コマンドが入力された特定の CLI セッションのプロセス ID。
メッセージ	メッセージは、入力された CLI コマンド、CLI 出力（メニュー、リストなど）、および表示されるプロンプトで構成されます。

CLI 監査ログの例

次の CLI 監査ログの例は、`who` および `textconfig` CLI コマンドが入力された PID 16434 の情報を示しています。

```
Thu Sep 9 14:35:55 2004 Info: PID 16434: User admin entered 'who'; prompt was
'¥nmail3.example.com> '
Thu Sep 9 14:37:12 2004 Info: PID 16434: User admin entered 'textconfig'; prompt was
'¥nUsername Login Time Idle Time Remote Host What¥n
======== ========== ========= =========== ====¥n
admin  Wed 11AM 3m 45s  10.1.3.14 tail¥nadmin  02:32PM  0s   10.1.3.14
cli¥nmail3.example.com> '
Thu Sep 9 14:37:18 2004 Info: PID 16434: User admin entered ''; prompt was '¥nThere are no
text resources currently defined.¥n¥n¥nChoose the operation you want to perform:¥n- NEW -
Create a new text resource.¥n- IMPORT - Import a text resource from a file.¥n[]> '
```

FTP サーバ ログの使用

表 14-6 に、FTP サーバ ログに記録される統計情報を示します。

表 14-6　FTP サーバ ログの統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
ID	接続 ID。FTP 接続ごとの別個の ID。
メッセージ	ログ エントリのメッセージ セクションは、ログファイルのステータス情報、または FTP 接続情報（ログイン、アップロード、ダウンロード、ログアウトなど）になります。

FTP サーバ ログの例

次の FTP サーバ ログの例には、接続（ID:1）が記録されています。着信接続の IP アドレスのほか、アクティビティ（ファイルのアップロードとダウンロード）およびログアウトが示されています。

```
Wed Sep 8 18:03:06 2004 Info: Begin Logfile
Wed Sep 8 18:03:06 2004 Info: Version: 4.0.0-206 SN: 00065BF3BA6D-9WFWC21
Wed Sep 8 18:03:06 2004 Info: Time offset from UTC: 0 seconds
Wed Sep 8 18:03:06 2004 Info: System is coming up
Fri Sep 10 08:07:32 2004 Info: Time offset from UTC: -25200 seconds
Fri Sep 10 08:07:32 2004 Info: ID:1 Connection from 10.1.3.14 on 172.19.0.86
Fri Sep 10 08:07:38 2004 Info: ID:1 User admin login SUCCESS
Fri Sep 10 08:08:46 2004 Info: ID:1 Upload wording.txt 20 bytes
Fri Sep 10 08:08:57 2004 Info: ID:1 Download words.txt 1191 bytes
Fri Sep 10 08:09:06 2004 Info: ID:1 User admin logout
```

HTTP ログの使用

表 14-7 に、HTTP ログに記録される統計情報を示します。

表 14-7　HTTP ログに記録される統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
ID	セッション ID。
req	接続元マシンの IP アドレス。
user	接続ユーザのユーザ名。
メッセージ	実行されたアクションに関する情報。GET コマンド、POST コマンド、またはシステム ステータスなどが含まれる場合があります。

HTTP ログの例

次の HTTP ログの例は、管理者ユーザによるグラフィカル ユーザ インターフェイスの使用（システム セットアップ ウィザードの実行など）を示しています。

```
Wed Sep 8 18:17:23 2004 Info: http service on 192.168.0.1:80 redirecting to https port 443
Wed Sep 8 18:17:23 2004 Info: http service listening on 192.168.0.1:80
```

```
Wed Sep 8 18:17:23 2004 Info: https service listening on 192.168.0.1:443
Wed Sep 8 11:17:24 2004 Info: Time offset from UTC: -25200 seconds
Wed Sep 8 11:17:24 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg POST
/system_administration/system_setup_wizard HTTP/1.1 303
Wed Sep 8 11:17:25 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/system_administration/ssw_done HTTP/1.1 200
Wed Sep 8 11:18:45 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/monitor/incoming_mail_overview HTTP/1.1 200
Wed Sep 8 11:18:45 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/monitor/mail_flow_graph?injector=&width=365&interval=0&type=recipientsin&height=190
HTTP/1.1 200
Wed Sep 8 11:18:46 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/monitor/classification_graph?injector=&width=325&interval=0&type=recipientsin&height=190
HTTP/1.1 200
Wed Sep 8 11:18:49 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/monitor/quarantines HTTP/1.1 200
```

Cisco IronPort スパム隔離ログの使用

表 14-8 に、Cisco IronPort スパム隔離ログに記録される統計情報を示します。

表 14-8　Cisco IronPort スパム隔離ログの統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
メッセージ	メッセージは、実行されたアクション（メッセージの隔離、隔離領域からの解放など）で構成されます。

Cisco IronPort スパム隔離ログの例

次のログの例は、隔離から admin@example.com に 2 個のメッセージ（MID 8298624 と MID 8298625）が解放されたことを示しています。

```
Mon Aug 14 21:41:47 2006 Info: ISQ: Releasing MID [8298624, 8298625] for all
Mon Aug 14 21:41:47 2006 Info: ISQ: Delivering released MID 8298624 (skipping work queue)
Mon Aug 14 21:41:47 2006 Info: ISQ: Released MID 8298624 to admin@example.com
Mon Aug 14 21:41:47 2006 Info: ISQ: Delivering released MID 8298625 (skipping work queue)
Mon Aug 14 21:41:47 2006 Info: ISQ: Released MID8298625 to admin@example.com
```

Cisco IronPort スパム隔離 GUI ログの使用

表 14-9 に、Cisco IronPort スパム隔離 GUI ログに記録される統計情報を示します。

表 14-9　Cisco IronPort スパム隔離 GUI ログの統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
メッセージ	メッセージは、ユーザ認証など、実行されたアクションで構成されます。

Cisco IronPort スパム隔離 GUI ログの例

次のログの例は、成功した認証、ログイン、およびログアウトを示しています。

表 14-10　Cisco IronPort スパム隔離 GUI ログの例

```
Fri Aug 11 22:05:28 2006 Info: ISQ: Serving HTTP on 192.168.0.1, port 82
Fri Aug 11 22:05:29 2006 Info: ISQ: Serving HTTPS on 192.168.0.1, port 83
Fri Aug 11 22:08:35 2006 Info: Authentication OK, user admin
Fri Aug 11 22:08:35 2006 Info: logout:- user:pqufOtL6vyI5StCqhCfO
session:10.251.23.228
Fri Aug 11 22:08:35 2006 Info: login:admin user:pqufOtL6vyI5StCqhCfO
session:10.251.23.228
Fri Aug 11 22:08:44 2006 Info: Authentication OK, user admin
```

Cisco IronPort テキスト メール ログの使用

これらのログには、電子メールの受信、電子メールの配信、およびバウンスの詳細が記録されます。ステータス情報も、1 分ごとにメール ログに書き込まれます。これらのログは、特定のメッセージの配信を理解し、システム パフォーマンスを分析するうえで有益な情報源となります。

これらのログに、特別な設定は必要ありません。ただし、添付ファイル名を表示するには、適切なシステムの設定が必要です。添付ファイル名は、常に記録されるわけではありません。詳細については、「トラッキング サービスの概要」（P.6-1）を参照してください。

表 14-11 に、テキスト メール ログに表示される情報を示します。

表 14-11　テキスト メール ログの統計情報

統計	説明
ICID	Injection Connection ID（インジェクション接続 ID）。システムに対する個々の SMTP 接続を表す数値 ID です。システムへの 1 つの SMTP 接続で、単一のメッセージまたは多数のメッセージを送信できます。
DCID	Delivery Connection ID（配信接続 ID）。別のサーバに対する個々の SMTP 接続を表す数値 ID であり、この接続で 1 個から数千個のメッセージが配信されます。1 つのメッセージ送信で一部または全部の RID が一緒に配信されます。
RCID	RPC Connection ID（RPC 接続 ID）。Cisco IronPort スパム隔離に対する個々の RPC 接続を表す数値 ID です。この ID を使用して、Cisco IronPort スパム隔離との間で送受信されるメッセージを追跡します。
MID	メッセージ ID。この ID を使用して、メッセージのフローをログで追跡します。
RID	受信者 ID。各メッセージ受信者には、ID が割り当てられます。
New	新規の接続が開始されました。
Start	新規のメッセージが開始されました。

例

ログ ファイルを解釈するためのガイドとして、次のサンプルを使用してください。

（注）　ログ ファイルの各行には、番号が*割り当てられません*。ここでは、単にサンプル用として番号が割り当てられています。

表 14-12　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 14-13 を使用してください。

表 14-13　テキスト メール ログの例の詳細

行番号	説明
1	システムに対して新しい接続が開始され、インジェクション ID（ICID）「5」が割り当てられました。この接続は管理 IP インターフェイスで受信され、10.1.1.209 のリモート ホストで開始されました。
2	クライアントから MAIL FROM コマンドが実行された後、メッセージにメッセージ ID（MID）「6」が割り当てられました。
3	送信者アドレスが識別され、受け入れられます。
4	受信者が識別され、受信者 ID（RID）「0」が割り当てられました。
5	MID 5 が受け入れられ、ディスクに書き込まれ、確認応答されました。
6	受信が成功し、受信接続が終了しました。
7	メッセージ配信プロセスが開始されました。192.168.42.42 から 10.5.3.25 への配信に、配信接続 ID（DCID）「8」が割り当てられました。
8	RID「0」へのメッセージ配信が開始されました。
9	RID「0」への MID 6 の配信に成功しました。
10	配信接続が終了しました。

テキスト メール ログ エントリの例

次の例で、さまざまなケースに基づくログ エントリを示します。

メッセージ受信

1 人の受信者に対するメッセージが Cisco IronPort 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 Cisco IronPort 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 5*XX* 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。Cisco IronPort アプライアンスは送信者に通知し、キューから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 Cisco IronPort アプライアンスにインジェクトされます。最初の配信試行で、メッセージはソフト バウンスして、その後の配信キューに入れられます。2 回めの試行でメッセージは正常に配信されます。

```
Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 5 interface 172.19.0.11 address
63.251.108.110
Mon Mar 31 20:00:23 2003 Info: Delivery start DCID 3 MID 4 to RID [0, 1]
```

```
Mon Mar 31 20:00:23 2003 Info: Delayed: DCID 5 MID 4 to RID 0 - 4.1.0 - Unknown address
error ('466', ['Mailbox temporarily full.'])[]
Mon Mar 31 20:00:23 2003 Info: Message 4 to RID [0] pending till Mon Mar 31 20:01:23 2003
Mon Mar 31 20:01:28 2003 Info: DCID 5 close
Mon Mar 31 20:01:28 2003 Info: New SMTP DCID 16 interface PublicNet address 172.17.0.113
Mon Mar 31 20:01:28 2003 Info: Delivery start DCID 16 MID 4 to RID [0]
Mon Mar 31 20:01:28 2003 Info: Message done DCID 16 MID 4 to RID [0]
Mon Mar 31 20:01:33 2003 Info: DCID 16 close
```

メッセージ スキャン結果（scanconfig）

次のプロンプトで、メッセージの構成要素を分解できない場合（添付ファイルを削除する場合）の動作を scanconfig コマンドを使用して決定した場合、

```
If a message could not be deconstructed into its component parts in order to remove
specified attachments, the system should:
1. Deliver
2. Bounce
3. Drop
[3]>
```

メール ログに以下が表示されます。

scanconfig で、メッセージを分解できない場合に配信するように設定した場合。

```
Tue Aug 3 16:36:29 2004 Info: MID 256 ICID 44784 From: <test@virus.org>
Tue Aug 3 16:36:29 2004 Info: MID 256 ICID 44784 RID 0 To: <joe@example.com>
Tue Aug 3 16:36:29 2004 Info: MID 256 Message-ID '<137398.@virus.org>'
Tue Aug 3 16:36:29 2004 Info: MID 256 Subject 'Virus Scanner Test #22'
Tue Aug 3 16:36:29 2004 Info: MID 256 ready 1627 bytes from <test@virus.org>
Tue Aug 3 16:36:29 2004 Warning: MID 256, Message Scanning Problem: Continuation line seen
before first header
Tue Aug 3 16:36:29 2004 Info: ICID 44784 close
Tue Aug 3 16:36:29 2004 Info: MID 256 antivirus positive 'EICAR-AV-Test'
Tue Aug 3 16:36:29 2004 Info: Message aborted MID 256 Dropped by antivirus
Tue Aug 3 16:36:29 2004 Info: Message finished MID 256 done
```

scanconfig で、メッセージを分解できない場合にドロップするように設定した場合。

```
Tue Aug 3 16:38:53 2004 Info: Start MID 257 ICID 44785
Tue Aug 3 16:38:53 2004 Info: MID 257 ICID 44785 From: test@virus.org
Tue Aug 3 16:38:53 2004 Info: MID 257 ICID 44785 RID 0 To: <joe@example.com>
Tue Aug 3 16:38:53 2004 Info: MID 257 Message-ID '<392912.@virus.org>'
Tue Aug 3 16:38:53 2004 Info: MID 25781 Subject 'Virus Scanner Test #22'
Tue Aug 3 16:38:53 2004 Info: MID 257 ready 1627 bytes from <test@virus.org>
Tue Aug 3 16:38:53 2004 Warning: MID 257, Message Scanning Problem: Continuation line seen
before first header
Tue Aug 3 16:38:53 2004 Info: Message aborted MID 25781 Dropped by filter 'drop_zip_c'
Tue Aug 3 16:38:53 2004 Info: Message finished MID 257 done
Tue Aug 3 16:38:53 2004 Info: ICID 44785 close
```

添付ファイルのあるメッセージ

この例では、添付ファイル名の識別をイネーブルにするように、条件「Message Body Contains」を含むコンテンツ フィルタが設定されています。

```
Sat Apr 23 05:05:42 2011 Info: New SMTP ICID 28 interface Management (192.0.2.10)
address 224.0.0.10 reverse dns host test.com verified yes
Sat Apr 23 05:05:42 2011 Info: ICID 28 ACCEPT SG UNKNOWNLIST match sbrs[-1.0:10.0]
SBRS 0.0
```

```
Sat Apr 23 05:05:42 2011 Info: Start MID 44 ICID 28
Sat Apr 23 05:05:42 2011 Info: MID 44 ICID 28 From: <sender1@example.com>
Sat Apr 23 05:05:42 2011 Info: MID 44 ICID 28 RID 0 To: <recipient1@example.org>
Sat Apr 23 05:05:42 2011 Info: MID 44 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>'
Sat Apr 23 05:05:42 2011 Info: MID 44 Subject 'Message 001'
Sat Apr 23 05:05:42 2011 Info: MID 44 ready 240129 bytes from <sender1@example.com>
Sat Apr 23 05:05:42 2011 Info: MID 44 matched all recipients for per-recipient
policy DEFAULT in the inbound table
Sat Apr 23 05:05:42 2011 Info: ICID 28 close
Sat Apr 23 05:05:42 2011 Info: MID 44 interim verdict using engine: CASE
spam negative
Sat Apr 23 05:05:42 2011 Info: MID 44 using engine: CASE spam negative
Sat Apr 23 05:05:43 2011 Info: MID 44 attachment 'Banner.gif'
Sat Apr 23 05:05:43 2011 Info: MID 44 attachment '=D1=82=D0=B5=D1=81=D1=82.rst'
Sat Apr 23 05:05:43 2011 Info: MID 44 attachment 'Test=20Attachment.docx'
Sat Apr 23 05:05:43 2011 Info: MID 44 queued for delivery
```

3 つの添付ファイルの 2 番めが Unicode であることに注意してください。Unicode を表示できない端末では、このような添付ファイルは quoted-printable 形式で表示されます。

生成またはリライトされたメッセージ

リライト/リダイレクト アクションなどの一部の機能（`alt-rcpt-to` フィルタ、アンチスパム RCPT リライト、`bcc()` アクション、アンチウイルス リダイレクションなど）によって、新しいメッセージが作成されます。ログに目を通して結果を確認し、必要に応じて MID や、場合によっては DCID を追加します。次のようなエントリが可能です。

```
Tue Jun 1 20:02:16 2004 Info: MID 14 generated based on MID 13 by bcc filter 'nonetest'
```

または

```
Tue Jan 6 15:03:18 2004 Info: MID 2 rewritten to 3 by antispam
Fri May 14 20:44:43 2004 Info: MID 6 rewritten to 7 by alt-rcpt-to-filter filter
'testfilt'
```

（注）「Rewritten」エントリは、新しい MID の使用を示すログの行の後に表示されます。

Cisco IronPort スパム隔離へのメッセージの送信

メッセージを隔離領域に送信すると、メール ログでは、RPC 接続を識別する RPC 接続 ID（RCID）を使用して、隔離領域との間の移動が追跡されます。次のメール ログでは、メッセージにスパムのタグが付けられ、Cisco IronPort スパム隔離に送信されています。

```
Wed Feb 14 12:11:40 2007 Info: Start MID 2317877 ICID 15726925
Wed Feb 14 12:11:40 2007 Info: MID 2317877 ICID 15726925 From: <HLD@chasehf.bfi0.com>
Wed Feb 14 12:11:40 2007 Info: MID 2317877 ICID 15726925 RID 0 To:
<stevel@healthtrust.org>
Wed Feb 14 12:11:40 2007 Info: MID 2317877 Message-ID
'<W1TH05606E5811BEA0734309D4BAF0.323.14460.pimailer44.DumpShot.2@email.chase.com>'
Wed Feb 14 12:11:40 2007 Info: MID 2317877 Subject 'Envision your dream home - Now make it
a reality'
Wed Feb 14 12:11:40 2007 Info: MID 2317877 ready 15731 bytes from <HLD@chasehf.bfi0.com>
Wed Feb 14 12:11:40 2007 Info: MID 2317877 matched all recipients for per-recipient policy
DEFAULT in the inbound table
Wed Feb 14 12:11:41 2007 Info: MID 2317877 using engine: CASE spam suspect
Wed Feb 14 12:11:41 2007 Info: EUQ: Tagging MID 2317877 for quarantine
Wed Feb 14 12:11:41 2007 Info: MID 2317877 antivirus negative
```

```
Wed Feb 14 12:11:41 2007 Info: MID 2317877 queued for delivery
Wed Feb 14 12:11:44 2007 Info: RPC Delivery start RCID 756814 MID 2317877 to local Cisco
IronPort Spam Quarantine
Wed Feb 14 12:11:45 2007 Info: EUQ: Quarantined MID 2317877
Wed Feb 14 12:11:45 2007 Info: RPC Message done RCID 756814 MID 2317877
Wed Feb 14 12:11:45 2007 Info: Message finished MID 2317877 done
```

NTP ログの使用

表 14-14 に、NTP ログに記録される統計情報を示します。

表 14-14　NTP ログに記録される統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
メッセージ	メッセージは、サーバへの簡易ネットワーク タイム プロトコル（SNTP）クエリーまたは adjust: メッセージで構成されます。

NTP ログの例

次の NTP ログの例は、アプライアンスから NTP ホストへの 2 度のポーリングを示しています。

```
Thu Sep 9 07:36:39 2004 Info: sntp query host 10.1.1.23 delay 653 offset -652
Thu Sep 9 07:36:39 2004 Info: adjust: time_const: 8 offset: -652us next_poll: 4096
Thu Sep 9 08:44:59 2004 Info: sntp query host 10.1.1.23 delay 642 offset -1152
Thu Sep 9 08:44:59 2004 Info: adjust: time_const: 8 offset: -1152us next_poll: 4096
```

レポーティング ログの使用

表 14-15 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 14-15　レポーティング ログの統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
メッセージ	メッセージは、ユーザ認証など、実行されたアクションで構成されます。

レポーティング ログの例

次のレポーティング ログの例は、情報ログ レベルに設定されたアプライアンスを示しています。

```
Wed Oct 3 13:39:53 2007 Info: Period minute using 0 (KB)
Wed Oct 3 13:39:53 2007 Info: Period month using 1328 (KB)
Wed Oct 3 13:40:02 2007 Info: Update 2 registered appliance at 2007-10-03-13-40
Wed Oct 3 13:40:53 2007 Info: Pages found in cache: 1304596 (99%). Not found: 1692
Wed Oct 3 13:40:53 2007 Info: Period hour using 36800 (KB)
Wed Oct 3 13:40:53 2007 Info: Period day using 2768 (KB)
Wed Oct 3 13:40:53 2007 Info: Period minute using 0 (KB)
Wed Oct 3 13:40:53 2007 Info: Period month using 1328 (KB)
Wed Oct 3 13:40:53 2007 Info: HELPER checkpointed in 0.00580507753533 seconds
```

```
Wed Oct 3 13:41:02 2007 Info: Update 2 registered appliance at 2007-10-03-13-41
Wed Oct 3 13:41:53 2007 Info: Pages found in cache: 1304704 (99%). Not found: 1692
Wed Oct 3 13:41:53 2007 Info: Period hour using 36800 (KB)
Wed Oct 3 13:41:53 2007 Info: Period day using 2768 (KB)
Wed Oct 3 13:41:53 2007 Info: Period minute using 0 (KB)
Wed Oct 3 13:41:53 2007 Info: Period month using 1328 (KB)
Wed Oct 3 13:42:03 2007 Info: Update 2 registered appliance at 2007-10-03-13-42
```

レポーティング クエリー ログの使用

表 14-16 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 14-16　レポーティング クエリー ログの統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
メッセージ	メッセージは、ユーザ認証など、実行されたアクションで構成されます。

レポーティング クエリー ログの例

次のレポーティング クエリー ログの例は、アプライアンスによって、2007 年 8 月 29 日から 10 月 10 日までの期間で毎日の発信メール トラフィック クエリーが実行されていることを示しています。

```
Tue Oct 2 11:30:02 2007 Info: Query: Closing interval handle 811804479.
Tue Oct 2 11:30:02 2007 Info: Query: Closing interval handle 811804480.
Tue Oct 2 11:30:02 2007 Info: Query: Closing query handle 302610228.
Tue Oct 2 11:30:02 2007 Info: Query: Merge query with handle 302610229 for
['MAIL_OUTGOING_TRAFFIC_SUMMARY.
DETECTED_SPAM', 'MAIL_OUTGOING_TRAFFIC_SUMMARY.DETECTED_VIRUS',
'MAIL_OUTGOING_TRAFFIC_SUMMARY.THREAT_CONTEN
T_FILTER', 'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_CLEAN_RECIPIENTS',
'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_RECI
PIENTS_PROCESSED'] for rollup period "day" with interval range 2007-08-29 to 2007-10-01
with key constraints
 None sorting on ['MAIL_OUTGOING_TRAFFIC_SUMMARY.DETECTED_SPAM'] returning results from 0
to 2 sort_ascendin
g=False.
Tue Oct 2 11:30:02 2007 Info: Query: Closing query handle 302610229.
Tue Oct 2 11:30:02 2007 Info: Query: Merge query with handle 302610230 for
['MAIL_OUTGOING_TRAFFIC_SUMMARY.
TOTAL_HARD_BOUNCES', 'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_RECIPIENTS_DELIVERED',
'MAIL_OUTGOING_TRAFFIC_SUMM
ARY.TOTAL_RECIPIENTS'] for rollup period "day" with interval range 2007-08-29 to
2007-10-01 with key constra
ints None sorting on ['MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_HARD_BOUNCES'] returning
results from 0 to 2 sort
_ascending=False.
Tue Oct 2 11:30:02 2007 Info: Query: Closing query handle 302610230.
```

セーフリスト/ブロックリスト ログの使用

表 14-17 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 14-17　セーフリスト/ブロックリスト ログの統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
メッセージ	メッセージは、ユーザ認証など、実行されたアクションで構成されます。

セーフリスト/ブロックリスト ログの例

次のセーフリスト/ブロックリスト ログの例は、アプライアンスによって 2 時間ごとにデータベースのスナップショットが作成されていることを示しています。送信者がデータベースに追加された時刻も表示されます。

```
Fri Sep 28 14:22:33 2007 Info: Begin Logfile Fri Sep 28 14:22:33 2007 Info: Version:
6.0.0-425 SN: XXXXXXXXXXXX-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 14-18 に、SMA ログに記録される統計情報を示します。

表 14-18　SMA ログの統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
メッセージ	メッセージは、ユーザ認証など、実行されたアクションで構成されます。

次の SMA ログの例は、電子メール セキュリティ アプライアンスからトラッキング ファイルをダウンロードする中央集中型トラッキング サービスと、電子メール セキュリティ アプライアンスからレポーティング ファイルをダウンロードする中央集中型レポーティング サービスを示しています。

```
Wed Oct 3 13:26:39 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from 172.29.0.17
- /export/tracki
ng/tracking.@20071003T202244Z_20071003T202544Z.s
Wed Oct 3 13:28:11 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from 172.29.0.15
- /export/tracki
ng/tracking.@20071003T202443Z_20071003T202743Z.s
Wed Oct 3 13:28:46 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from 172.29.0.17
- /export/tracki
```

```
ng/tracking.@20071003T202544Z_20071003T202844Z.s
Wed Oct 3 13:31:27 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from 172.29.0.15
- /export/tracki
ng/tracking.@20071003T202743Z_20071003T203043Z.s
Wed Oct 3 13:31:28 2007 Info: TRANSFER: Plugin REPORTINGPLUGIN downloading from
172.29.0.15 - /reporting/ou
tgoing_queue/rpx.2007-10-03-20-15Z.000F1F6ECA7C-2RWDB51.v1.tgz
Wed Oct 3 13:31:53 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from 172.29.0.17
- /export/tracki
ng/tracking.@20071003T202844Z_20071003T203144Z.s
Wed Oct 3 13:32:31 2007 Info: TRANSFER: Plugin REPORTINGPLUGIN downloading from
172.29.0.17 - /reporting/ou
tgoing_queue/rpx.2007-10-03-20-15Z.0019B9B316E4-JZ41PC1.v1.tgz
Wed Oct 3 13:34:40 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from 172.29.0.15
- /export/tracki
ng/tracking.@20071003T203043Z_20071003T203343Z.s
```

ステータス ログの使用

ステータス ログには、`status`、`status detail`、および `dnsstatus` を含む CLI ステータス コマンドで検出されたシステム統計情報が記録されます。記録期間は、`logconfig` の `setup` サブコマンドを使用して設定します。ステータス ログでレポートされるカウンタまたはレートは、前回カウンタがリセットされた時点からの値です。

ステータス ログの読み取り

表 14-19 に、ステータス ログ ラベル、およびそれと一致するシステム統計情報を示します。

表 14-19　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 14-19　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	グローバル配信停止リストとの一致数。
ActvRcp	アクティブ受信者。
UnatmptRcp	未試行受信者。
AtmptRcp	試行受信者。
CrtCncIn	現在の着信接続。
CrtCncOut	現在の発信接続。
DnsReq	DNS 要求。
NetReq	ネットワーク要求。
CchHit	キャッシュ ヒット。
CchMis	キャッシュ ミス。
CchEct	キャッシュ例外。
CchExp	キャッシュ期限切れ。
CPUTTm	アプリケーションが使用した合計 CPU 時間。
CPUETm	アプリケーションが開始されてからの経過時間。
MaxIO	メール プロセスに対する 1 秒あたりの最大ディスク I/O 動作。
RamUsd	割り当て済みのメモリ（バイト単位）。
SwIn	スワップインされたメモリ
SwOut	スワップアウトされたメモリ
SwPgIn	ページインされたメモリ
SwPgOut	ページアウトされたメモリ
MMLen	システム内の合計メッセージ数。
DstInMem	メモリ内の宛先オブジェクト数。
ResCon	リソース保持の tarpit 値（大量のシステム負荷により、着信メールの受け入れがこの秒数だけ遅延します）。
WorkQ	作業キューにある現在のメッセージ数。
QuarMsgs	システム隔離にある個々のメッセージ数（複数の隔離領域に存在するメッセージは一度だけカウントされます）。
QuarQKUsd	システム隔離メッセージによって使用されたキロバイト数。
LogUsd	使用されたログ パーティションの割合。
CASELd	CASE スキャンで使用された CPU の割合。

表 14-19　ステータス ログの統計情報（続き）

統計	説明
TotalLd	CPU の合計消費量。
LogAvail	ログ ファイルに使用できるディスク領域の大きさ。
EuQ	Cisco IronPort スパム隔離内のメッセージ数。
EuqRls	Cisco IronPort スパム隔離解放キュー内のメッセージ数。

ステータス ログの例

```
Fri Feb 24 15:14:39 2006 Info: Status: CPULd 0 DskIO 0 RAMUtil 2 QKUsd 0 QKFre 8388608
CrtMID 19036 CrtICID 35284 CrtDCID 4861 InjMsg 13889 InjRcp 14230 GenBncRcp 12 RejRcp 6318
DrpMsg 7437 SftBncEvnt 1816 CmpRcp 6813 HrdBncRcp 18 DnsHrdBnc 2 5XXHrdBnc 15 FltrHrdBnc 0
ExpHrdBnc 1 OtrHrdBnc 0 DlvRcp 6793 DelRcp 2 GlbUnsbHt 0 ActvRcp 0 UnatmptRcp 0 AtmptRcp 0
CrtCncIn 0 CrtCncOut 0 DnsReq 143736 NetReq 224227 CchHit 469058 CchMis 504791 CchEct
15395 CchExp 55085 CPUTTm 228 CPUETm 181380 MaxIO 350 RAMUsd 21528056 MMLen 0 DstInMem 4
ResCon 0 WorkQ 0 QuarMsgs 0 QuarQKUsd 0 LogUsd 3 AVLd 0 BMLd 0 CASELd 3 TotalLd 3 LogAvail
17G EuQ 0 EuqRls 0
```

システム ログの使用

表 14-20 に、システム ログに記録される統計情報を示します。

表 14-20　システム ログの統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
メッセージ	ログに記録されたイベント。

システム ログの例

次のシステム ログの例は、commit を実行したユーザの名前と入力されたコメントを含む、いくつかの commit エントリを示しています。

```
Wed Sep 8 18:02:45 2004 Info: Version: 6.0.0-206 SN: XXXXXXXXXXXX-XXX
Wed Sep 8 18:02:45 2004 Info: Time offset from UTC: 0 seconds
Wed Sep 8 18:02:45 2004 Info: System is coming up
Wed Sep 8 18:02:49 2004 Info: bootstrapping DNS cache
Wed Sep 8 18:02:49 2004 Info: DNS cache bootstrapped
Wed Sep 8 18:13:30 2004 Info: PID 608: User admin commit changes: SSW:Password
Wed Sep 8 18:17:23 2004 Info: PID 608: User admin commit changes: Completed Web::SSW
Thu Sep 9 08:49:27 2004 Info: Time offset from UTC: -25200 seconds
Thu Sep 9 08:49:27 2004 Info: PID 1237: User admin commit changes: Added a second CLI log
for examples
Thu Sep 9 08:51:53 2004 Info: PID 1237: User admin commit changes: Removed example CLI
log.
```

トラッキング ログについて

トラッキング ログには、AsyncOS の電子メール動作に関する情報が記録されます。ログ メッセージは、メール ログに記録されたメッセージのサブセットです。

トラッキング ログは、メッセージ トラッキング データベースを作成するため、メッセージ トラッキング コンポーネントで使用されます。ログ ファイルはデータベースの作成プロセスで消費されるので、トラッキング ログは一過性のものになります。トラッキング ログの情報は、人による読み取りや解析を目的とした設計になっていません。

トラッキング ログは、リソースの効率性を保つためにバイナリ形式で記録され、転送されます。情報は、論理的にレイアウトされ、Cisco IronPort 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、Cisco IronPort アプライアンスに、またはリモートに保存される個々のログ ファイルが作成されます。ログ サブスクリプションは、プッシュ（別のコンピュータに配信）またはプル（アプライアンスから取得）されます。一般に、ログ サブスクリプションには次の属性があります。

表 14-21　ログ ファイルの属性

属性	説明
Log Type	記録される情報のタイプと、ログ サブスクリプションの形式を定義します。詳細については、「ログ タイプ」（P.14-2）を参照してください。
Name	後で参照するための、ログ サブスクリプションのわかりやすい名前。
Log Filename	ディスクに書き込むときのファイルの物理名。システムに複数の Cisco IronPort アプライアンスがある場合、ログ ファイルを生成したアプライアンスを識別できる一意のログ ファイル名を使用します。
Rollover by File Size	ファイルの最大サイズ。このサイズに到達すると、ロールオーバーされます。
Rollover by Time	時間に基づいてログ ファイルをロールオーバーするタイミング。「ログのロールオーバーおよび転送スケジュール」（P.14-5）のオプションを参照してください。
Log Level	各ログ サブスクリプションの詳細レベル。
Retrieval Method	ログ ファイルを Cisco IronPort アプライアンスから転送するときに使用する方式。

[Management Appliance] > [System Administration] > [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」（P.14-2）を参照）。ほとんどのログ タイプで、ログ サブスクリプションの *ログ レベル*の入力も要求されます。

（注）　コンフィギュレーション履歴ログのみ：コンフィギュレーション履歴ログからコンフィギュレーションをロードする可能性がある場合は、コンフィギュレーションにマスクされたパスワードが含まれているとロードできないことに注意してください。[Management Appliance] > [System Administration] > [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、[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 14-22　ログ レベル

ログ レベル	説明
Critical	エラーだけがログに記録されます。最も省略されたログ レベル設定です。このログ レベルでは、パフォーマンスおよび重要なアプライアンスのアクティビティをモニタすることはできません。ただし、詳細ログ レベルのように、ログ ファイルがすぐに最大サイズに達することはありません。このログ レベルは、syslog レベル Alert と同等です。
Warning	すべてのシステム エラーと警告が記録されます。このログ レベルでは、パフォーマンスおよび重要なアプライアンスのアクティビティをモニタすることはできません。Critical ログ レベルよりは早く、ログ ファイルが最大サイズに達します。このログ レベルは、syslog レベル Warning と同等です。
Information	システムの動作が逐次記録されます。たとえば、接続のオープンや配信試行が記録されます。Information レベルは、ログに推奨される設定です。このログ レベルは、syslog レベル Info と同等です。
Debug	Information ログ レベルよりも詳細な情報が記録されます。エラーをトラブルシューティングするときは、Debug ログ レベルを使用します。この設定は一時的に使用し、後でデフォルト レベルに戻します。このログ レベルは、syslog レベル Debug と同等です。
Trace	使用可能なすべての情報が記録されます。Trace ログ レベルは、開発者にのみ推奨されます。このレベルを使用すると、システムのパフォーマンスが大きく低下するので、推奨されません。このログ レベルは、syslog レベル Debug と同等です。

GUI でのログ サブスクリプションの作成

ステップ 1　[Management Appliance] > [System Administration] > [Log Subscriptions] ページで、[Add Log Subscription] をクリックします。

ステップ 2　ログ タイプを選択し、ログ名（ログ ディレクトリ用）とログ ファイル自体の名前を入力します。

ステップ 3　該当する場合は、最大ファイル サイズを指定します。

ステップ 4　該当する場合は、ログをロールオーバーする日、時刻、または時間間隔を指定します。詳細については、「ログのロールオーバーおよび転送スケジュール」（P.14-5）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、[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

ステップ 1　[Log Subscriptions] ページの [Log Name] カラムにあるログ名をクリックします。

ステップ 2　ログ サブスクリプションを更新します。

ステップ 3　変更を送信し、保存します。

ロギングに対するグローバル設定

システムは、テキスト メール ログおよびステータス ログ内にシステム メトリックを定期的に記録します。[Log Subscriptions] ページの [Global Settings] セクションにある [Edit Settings] ボタン（または、CLI の `logconfig -> setup` コマンド）を使用して、次の情報を設定します。

- システムが測定を記録するまで待機する時間（秒単位）
- メッセージ ID ヘッダーを記録するかどうか
- リモート応答ステータス コードを記録するかどうか
- 元のメッセージのサブジェクト ヘッダーを記録するかどうか
- メッセージごとにログに記録するヘッダー

すべての Cisco IronPort ログには、次の 3 項目を任意で記録できます。

- [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
  ```

- [Remote Response]：このオプションを設定すると、可能な場合はすべてのメッセージのリモート応答ステータス コードがログに記録されます。次に例を示します。

```
Tue Apr 6 14:38:34 2004 Info: MID 1 RID [0] Response 'queued as 9C8B425DA7'
```

リモート応答文字列は、SMTP 会話配信時の DATA コマンドへの応答後に受信される、人が読み取ることのできるテキストです。この例では、接続ホストが data コマンドを実行した後のリモート応答が、「queued as 9C8B425DA7」となります。

```
[...]
250 ok hostname
250 Ok: queued as 9C8B425DA7
```

文字列の先頭にある空白や句読点、および 250 応答の OK 文字は除去されます。文字列の末尾については、空白だけが除去されます。たとえば、Cisco IronPort 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 Cisco IronPort アプライアンスである場合は、「Message MID accepted」というエントリがログに記録されます。

- [Original Subject Header]：このオプションをイネーブルにすると、各メッセージの元のサブジェクト ヘッダーがログに記録されます。

```
Tue May 31 09:20:27 2005 Info: Start MID 2 ICID 2
Tue May 31 09:20:27 2005 Info: MID 2 ICID 2 From: <mary@example.com>
Tue May 31 09:20:27 2005 Info: MID 2 ICID 2 RID 0 To: <joe@example.com>
Tue May 31 09:20:27 2005 Info: MID 2 Message-ID '<44e4n$2@example.com>'
Tue May 31 09:20:27 2005 Info: MID 2 Subject 'Monthly Reports Due'
```

メッセージ ヘッダーのロギング

場合によっては、メッセージがシステムを通過するときに、メッセージのヘッダーの存在と内容を記録する必要があります。[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。Cisco IronPort アプライアンスは、指定されたメッセージ ヘッダーをテキスト メール ログおよびトラッキング ログに記録します。ヘッダーが存在する場合、システムはヘッダーの名前と値を記録します。ヘッダーが存在しない場合は、ログに何も記録されません。

（注） システムは、ロギングに指定したヘッダーに関係なく、メッセージの記録処理中に随時、メッセージに存在するすべてのヘッダーを評価します。

（注） SMTP プロトコルについての RFC は、`http://www.faqs.org/rfcs/rfc2821.html` にあります。この RFC には、ユーザ定義のヘッダーが規定されています。

（注） `logheaders` コマンドを使用してヘッダーをログに記録するように設定している場合、ヘッダー情報は配信情報の後に表示されます。

表 14-23　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

ステップ 1　[Log Subscriptions] ページの [Global Settings] セクションにある [Edit Settings] ボタンをクリックします。

ステップ 2　システム メトリクスの頻度、メール ログにメッセージ ID ヘッダーを加えるかどうか、リモート応答を加えるかどうか、および各メッセージの元のサブジェクト ヘッダーを加えるかどうかを指定します。

これらの設定の詳細については、「ロギングに対するグローバル設定」（P.14-24）を参照してください。

ステップ 3　ログに加えるその他のヘッダーを入力します。各エントリはカンマで区切ります。

ステップ 4　変更を送信し、保存します。

ログ サブスクリプションのロールオーバー

AsyncOS がログ ファイルをロールオーバーすると、次のことが行われます。

- ロールオーバーのタイムスタンプで新規のログ ファイルが作成され、文字「**c**」の拡張子によって現在のファイルとして指示されます。
- 現在のログ ファイルが、保存済みを示す文字「**s**」の拡張子付きに名前変更されます。
- 新たに保存されたログ ファイルがリモート ホストに転送されます（プッシュ ベースの場合）。
- 同じサブスクリプションから以前に失敗したログ ファイルが転送されます（プッシュ ベースの場合）。
- 保持するファイルの合計数を超えた場合は、ログ サブスクリプション内の最も古いファイルが削除されます（ポーリング ベースの場合）。

ログ サブスクリプション内のログのロールオーバー

「ログのロールオーバーおよび転送スケジュール」（P.14-5）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

ステップ 1　[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　[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　[Rollover Now] ボタンをクリックします。

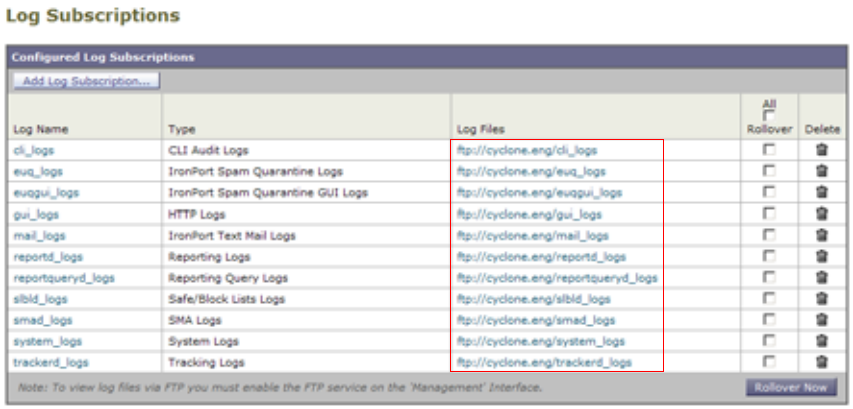
CLI を介したログの即時ロールオーバー

`rollovernow` コマンドを使用して、一度にすべてのログ ファイルをロールオーバーするか、リストから特定のログ ファイルを選択します。

グラフィカル ユーザ インターフェイスでの最近のログ エントリの表示

GUI を介してログ ファイルを表示するには、[Log Subscriptions] ページのテーブルの [Log Files] カラムにあるログ サブスクリプションをクリックします。ログ サブスクリプションへのリンクをクリックすると、パスワードを入力するプロンプトが表示されます。次に、そのサブスクリプションのログ ファイルのリストが表示されます。いずれかのログ ファイルをクリックして、ブラウザに表示したり、ディスクに保存したりすることができます。グラフィカル ユーザ インターフェイスを介してログを表示するには、管理インターフェイスで FTP サービスをイネーブルにしておく必要があります。

図 14-1　　グラフィカル ユーザ インターフェイスでのログ ファイルの表示



最新のログ エントリの表示（tail コマンド）

AsyncOS では、アプライアンスに設定されたログの最新エントリを表示する `tail` コマンドをサポートしています。`tail` コマンドを実行し、現在設定されているログのうち、表示するログの番号を選択します。Ctrl を押した状態で C を押して、`tail` コマンドを終了します。

（注）　コンフィギュレーション履歴ログは、`tail` コマンドを使用して表示することができません。FTP または SCP を使用する必要があります。

例

次に、`tail` コマンドを使用してシステム ログを表示する例を示します `tail` コマンドは、次の例のように、表示するログの名前をパラメータとして指定することもできます。

```
tail system_logs

Welcome to the Cisco IronPort M600 Messaging Gateway(tm) Appliance
example.srv> tail

Currently configured logs:
1. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
2. "euq_logs" Type: "Cisco IronPort Spam Quarantine Logs" Retrieval: FTP Poll
3. "euqgui_logs" Type: "Cisco IronPort Spam Quarantine GUI Logs" Retrieval: FTP Poll
4. "gui_logs" Type: "HTTP Logs" Retrieval: FTP Poll
5. "mail_logs" Type: "Cisco IronPort Text Mail Logs" Retrieval: FTP Poll
6. "reportd_logs" Type: "Reporting Logs" Retrieval: FTP Poll
7. "reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: FTP Poll
8. "slbld_logs" Type: "Safe/Block Lists Logs" Retrieval: FTP Poll
```

```
9. "smad_logs" Type: "SMA Logs" Retrieval: FTP Poll
10. "system_logs" Type: "System Logs" Retrieval: FTP Poll
11. "trackerd_logs" Type: "Tracking Logs" Retrieval: FTP Poll
Enter the number of the log you wish to tail.
[]> 10

Press Ctrl-C to stop.
Thu Sep 27 00:18:56 2007 Info: Begin Logfile
Thu Sep 27 00:18:56 2007 Info: Version: 6.0.0-422 SN: 001143583D73-FT9GP61
Thu Sep 27 00:18:56 2007 Info: Time offset from UTC: 0 seconds
Thu Sep 27 00:18:47 2007 Info: System is coming up.
Thu Sep 27 00:23:05 2007 Warning: DNS query network error '[Errno 64] Host is down' to
'172.16.0.3' looking up 'downloads.cisco.com'
Fri Sep 28 22:20:08 2007 Info: PID 688: User admin commit changes:
Fri Sep 28 23:06:15 2007 Info: PID 688: User admin commit changes:
^Cexample.srv>
.
```

ホスト キーの設定

`logconfig -> hostkeyconfig` サブコマンドを使用して、Cisco IronPort 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 キーを管理する方法については、『*Cisco IronPort AsyncOS for Email Security Daily Management Guide*』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 14-24　ホスト キーの管理：サブコマンドのリスト

コマンド	説明
New	新しいキーを追加します。
Edit	既存のキーを変更します。
Delete	既存のキーを削除します。
Scan	ホスト キーを自動的にダウンロードします。
Print	キーを表示します。
Host	システム ホスト キーを表示します。これは、リモート システムの「known_hosts」ファイルに配置される値です。
Fingerprint	システム ホスト キーのフィンガープリントを表示します。
User	リモート マシンにログをプッシュするシステム アカウントの公開キーを表示します。これは、SCP プッシュ サブスクリプションを設定するときに表示されるキーと同じです。これは、リモート システムの「authorized_keys」ファイルに配置される値です。

次の例では、コマンドによってホスト キーがスキャンされ、ホストに追加されます。

```
mail3.example.com> logconfig

Currently configured logs:
[ list of logs ]
```

```
Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
[]> hostkeyconfig

Currently installed host keys:
1. mail3.example.com ssh-dss [ key displayed ]

Choose the operation you want to perform:
- NEW - Add a new key.
- EDIT - Modify a key.
- DELETE - Remove a key.
- SCAN - Automatically download a host key.
- PRINT - Display a key.
- HOST - Display system host keys.
- FINGERPRINT - Display system host key fingerprints.
- USER - Display system user keys.
[]> scan

Please enter the host or IP address to lookup.
[]> mail3.example.com

Choose the ssh protocol type:
1. SSH1:rsa
2. SSH2:rsa
3. SSH2:dsa
4. All
[4]>

SSH2:dsa
mail3.example.com ssh-dss
[ key displayed ]

SSH2:rsa
mail3.example.com ssh-rsa
[ key displayed ]

SSH1:rsa
mail3.example.com 1024 35
[ 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 15

トラブルシューティング

セキュリティ管理アプライアンスからのカスタマー サポートへのアクセス

カスタマー サポートに連絡する必要がある場合、またはセキュリティ管理アプライアンスの機能をアクティブにする必要がある場合には、次のコマンドと機能が役立ちます。

テクニカル サポート

GUI の右上にある [Help and Support] メニューを使用して、Cisco IronPort カスタマー サポートに関連する機能にアクセスします。

テクニカル サポート機能には、[Open a Support Case] ページと [Remote Access] ページの 2 つのページが含まれます。

サポート要求の作成

[Help and Support] > [Open a Support Case] ページ、または **supportrequest** コマンドを使用すると、アプライアンスの設定をカスタマー サポートまたは他のユーザに送信したり、サポートを必要とする問題を説明するコメントを入力することができます。**supportrequest** コマンドの詳細については、『*Cisco IronPort AsyncOS CLI Reference Guide*』を参照してください。このコマンドを使用するには、アプライアンスがインターネットにメールを送信できる必要があります。

ステップ 1 [Help and Support] > [Open a Support Case] を選択します。

ステップ 2 連絡先情報（名前、電子メール アドレス、および電話番号）を入力します。

ステップ 3 問題の内容を入力します。

ステップ 4 オプションで、[Other recipients] フィールドに、追加受信者の電子メール アドレスを入力します。

デフォルトでは、フォームの上部にあるチェックボックスを選択した場合、サポート要求（コンフィギュレーション ファイルを含む）は、Cisco IronPort カスタマー サポートに送信されます。また、コンフィギュレーション ファイルを他の電子メール アドレスに送信することもできます。複数のアドレスを指定する場合は、カンマで区切ります。

ステップ 5　この問題に関してすでにカスタマー サポート チケットをお持ちの場合は、ページの下部にチケット番号を入力してください。

ステップ 6　[Send] をクリックします。

トラブル チケットが自動的に作成されます。詳細については、「シスコのテクニカル サポート」（P.1-5）を参照してください。

カスタマー サポートのリモート アクセスのイネーブル化

ステップ 1　セキュリティ管理アプライアンス GUI の右側で、[Help and Support] > [Remote Access] を選択します。

ステップ 2　[Edit Remote Access Settings] を選択します。

ステップ 3　[Allow remote access to this appliance] チェックボックスをオンにします。

ステップ 4　カスタマー サポート パスワードを入力します。

ステップ 5　カスタマー サポート エンジニアからオプションを変更するよう指示された場合を除いて、[Secure Tunnel] を選択したままにし、ポート番号は 25 のままにします。

ステップ 6　変更を送信し、保存します。

リモート アクセスをイネーブルにすると、デバッグとシステムへの一般的なアクセスのために、カスタマー サポートが使用する特別なアカウントが有効になります。これは、Cisco IronPort カスタマー サポートがシステムの設定、設定の理解、および問題レポートの調査でカスタマーを補助するなど作業に使用します。また、CLI で **techsupport** コマンドを使用することもできます。

セキュアなトンネルの使用をイネーブルにすると、アプライアンスが、指定されたポートを介してサーバ **upgrades.cisco.com** への SSH トンネルを作成します。デフォルトでは、この接続はポート 25 で行われます。システムは、電子メール メッセージを送信するために、このポートを介して一般的なアクセスを行う必要があるため、このポートは大部分の環境で機能します。**upgrades.cisco.com** への接続が確立されたら、カスタマー サポートは SSH トンネルを使用してアプライアンスへのアクセスを取得できます。ポート 25 を介した接続が許可されている限り、これにより、大部分のファイアウォールの制限がバイパスされます。また、CLI で **techsupport tunnel** コマンドを使用することもできます。

リモート アクセス モードとトンネル モードの両方で、パスワードが必要です。これは、システムへのアクセスに使用されるパスワードではないことを理解しておくことが重要です。そのパスワードとシステムのシリアル番号がカスタマー サポート担当者に提供された後で、アプライアンスへのアクセスに使用されるパスワードが生成されます。

テクニカル サポート トンネルがイネーブルになると、**upgrades.cisco.com** に 7 日間接続されたままになります。7 日の経過後も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。SSH トンネル接続に設定されたタイムアウトはリモート アクセス アカウントに適用されません。リモート アクセス アカウントは、特に非アクティブ化するまでアクティブのままになります。

パケット キャプチャ

場合によっては、セキュリティ管理アプライアンスの問題発生時に Cisco IronPort カスタマー サポートに問い合わせたときに、セキュリティ管理アプライアンスとのネットワーク状況について尋ねられることがあります。セキュリティ管理アプライアンスでは、アプライアンスが接続されたネットワークで送受信されている TCP/IP と他のパケットを傍受および表示できます。

パケット キャプチャを実行してネットワーク設定をデバッグしたり、どのようなネットワーク トラフィックがアプライアンスに到達または送出されているかを検出する場合があります。

アプライアンスは、取り込んだパケット アクティビティをファイルに保存し、そのファイルをローカルに格納します。パケット キャプチャ ファイルの最大サイズ、パケット キャプチャの実行時間、およびキャプチャを実行するネットワーク インターフェイスを設定できます。また、フィルタを使用して、特定のポートからのトラフィックや特定のクライアントまたはサーバの IP アドレスからのトラフィックにパケット キャプチャを制限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 [Help and Support] > [Packet Capture] ページに、ハード ドライブ上に格納された完全なパケット キャプチャ ファイルの一覧が表示されます。パケット キャプチャの実行中は、[Packet Capture] ページに、ファイル サイズや経過時間などの現在の統計情報を示すことにより、進行中のキャプチャのステータスが表示されます。

[Download File] ボタンを使用してパケット キャプチャ ファイルをダウンロードし、デバッグやトラブルシューティングのために電子メールで Cisco IronPort カスタマー サポートに転送できます。また、1 つまたは複数のファイルを選択して、[Delete Selected Files] をクリックすることにより、パケット キャプチャ ファイルを削除することもできます。

（注）　CLI で、**packetcapture** コマンドを使用します。このコマンドは、UNIX の **tcpdump** コマンドと類似しています。

パケット キャプチャの開始

パケット キャプチャを開始するには、次の 2 つの方法があります。

- 「コマンド ライン プロンプトからのパケット キャプチャの開始」（P.15-3）
- 「GUI からのパケット キャプチャの開始」（P.15-3）

コマンド ライン プロンプトからのパケット キャプチャの開始

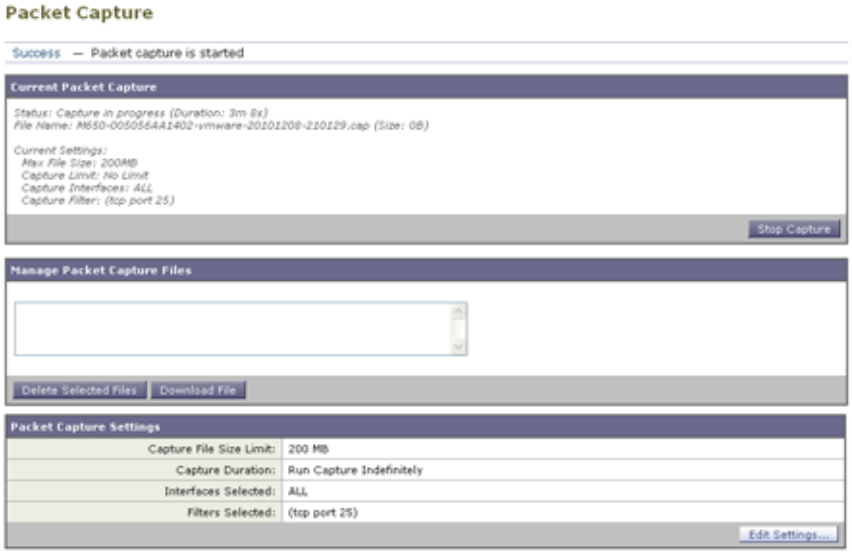
パケット キャプチャを開始するには、コマンド ライン プロンプトから **packetcapture > start** コマンドを入力します。実行されているパケット キャプチャを停止する必要がある場合は、**packetcapture > stop** コマンドを実行します。アプライアンスは、セッションが終了するとパケット キャプチャを停止します。

GUI からのパケット キャプチャの開始

ステップ 1　セキュリティ管理アプライアンス上で、[Help and Support] > [Packet Capture] を選択します。

ステップ 2　[Start Capture] を選択します。

ステップ 3　次の図に、実行中のパケット キャプチャ プロセスを示します。



実行されているキャプチャを停止するには、[Stop Capture] をクリックします。以前に開始されたキャプチャは、セッション間で維持されます。

（注）　GUI では、GUI で開始されたパケット キャプチャだけが表示されます。**packetcapture > start** コマンドを使用してコマンド ライン プロンプトから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、コマンド ラインでは、**packetcapture > start** コマンドを使用してコマンド ライン プロンプトから開始された現在のパケット キャプチャの実行ステータスだけが表示されます。キャプチャは一度に 1 つだけ実行できます。

パケット キャプチャ設定の編集

パケット キャプチャの編集には、次の 2 つの方法があります。

- 「コマンド ライン プロンプトからのパケット キャプチャ設定の編集」（P.15-4）
- 「GUI からのパケット キャプチャ設定の編集」（P.15-4）

コマンド ライン プロンプトからのパケット キャプチャ設定の編集

CLI でパケット キャプチャ設定を編集するには、コマンド ライン プロンプトから **packetcapture > setup** コマンドを実行します。

GUI からのパケット キャプチャ設定の編集

ステップ 1　セキュリティ管理アプライアンス上で、[Help and Support] > [Packet Capture] を選択します。

ステップ 2　[Edit Settings] を選択します。

ステップ 3　表 15-1 に、設定可能なパケット キャプチャの項目を示します。

表 15-1　パケット キャプチャ設定オプション

オプション	説明
Capture file size limit	すべてのパケット キャプチャ ファイルの最大ファイル サイズ（メガバイト単位）。
Capture Duration	パケット キャプチャの実行時間を選択します。 • [Run Capture Until File Size Limit Reached]。パケット キャプチャは、ファイル サイズ制限に到達するまで実行されます。 • [Run Capture Until Time Elapsed Reaches]。パケット キャプチャは、設定された時間が経過するまで実行されます。時間は秒単位（s）、分単位（m）、または時間単位（h）で入力できます。単位を指定せずに時間の長さを入力すると、AsyncOS は、デフォルトで秒を使用します。このオプションは GUI でのみ使用できます。 **（注）** パケット キャプチャ ファイルは 10 個の部分に分割されます。全体の時間が経過する前にパケット キャプチャ ファイルが最大サイズ制限に到達した場合は、そのファイルの最も古い部分が削除され（データが破棄されます）、現在のパケット キャプチャ データで新しい部分が開始されます。パケット キャプチャ ファイルは一度に 1/10 だけ破棄されます。 • [Run Capture Indefinitely]。パケット キャプチャは、手動で停止するまで実行されます。 **（注）** 手動でパケット キャプチャを停止する前にパケット 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 キャプチャはいつでも手動で停止できます。
Interface	パケット キャプチャを実行するネットワーク インターフェイスを選択します。
Filters	パケット キャプチャで保存されるデータの量を削減するために、パケット キャプチャにフィルタを適用するかどうかを選択します。 事前定義されたフィルタを使用して、ポート、クライアント IP、またはサーバ IP（GUI のみ）でフィルタリングすることか、または `host 10.10.10.10 && port 80` など、UNIX の **tcpdump** コマンドでサポートされる任意の構文を使用してカスタム フィルタを作成することができます。

ステップ 4　変更を送信します。これらの変更はすぐに有効になり、保存は不要です。

APPENDIX A

IP インターフェイスおよびアプライアンスへのアクセス

アプライアンスで作成する任意の IP インターフェイスには、さまざまなサービスを通してアクセスできます。

デフォルトでは、各インターフェイスに対して次のサービスがイネーブルまたはディセーブルに設定されています。

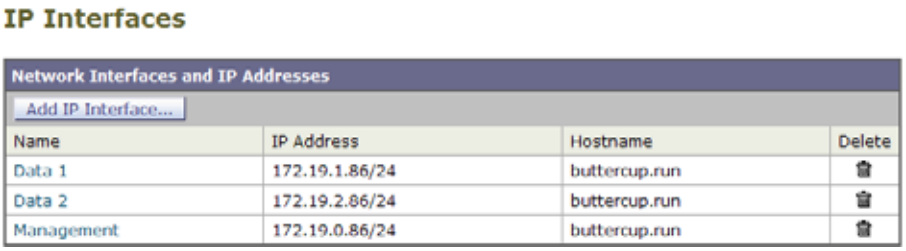
表 A-1　IP インターフェイスに対してデフォルトでイネーブルになるサービス

		デフォルトでイネーブルかどうか	
サービス	**デフォルト ポート**	**管理インターフェイス**	**新規作成された IP インターフェイス**
FTP	21	No	No
Telnet	23	Yes	No
SSH	22	Yes	No
HTTP	80	Yes	No
HTTPS	443	Yes	No

IP インターフェイス

IP インターフェイスには、ネットワークへの個別の接続に必要なネットワーク設定データが含まれています。1 つの物理イーサネット インターフェイスに対して複数の IP インターフェイスを設定できます。IP インターフェイス経由の Cisco IronPort スパム隔離へのアクセスも設定できます。電子メール配信および仮想ゲートウェイの場合、各 IP インターフェイスは特定の IP アドレスおよびホスト名を持つ 1 つの仮想ゲートウェイ アドレスとして機能します。また、インターフェイスは個別のグループに（CLI を介して）「参加」させることもできます。その場合、システムは、電子メールの配信時にこれらのグループを順番に繰り返して使用します。仮想ゲートウェイの参加またはグループ化は、大規模な電子メール キャンペーンを複数のインターフェイス間でロード バランシングする際に役立ちます。
VLAN を作成し、他のインターフェイスと同様に（CLI を介して）設定することもできます。詳細については、『*Cisco IronPort AsyncOS for Email Security Advanced Configuration Guide*』の「Advanced Networking」の章を参照してください。

図 A-1　[IP Interfaces] ページ



IP インターフェイスの設定

[Management Appliance] > [Network] > [IP Interfaces] ページ（および `interfaceconfig` コマンド）では、IP インターフェイスを追加、編集、または削除できます。

（注）　セキュリティ管理アプライアンス上の管理インターフェイスに関連付けられた名前またはイーサネット ポートを変更することはできません。さらに、セキュリティ管理アプライアンスは後述のすべての機能をサポートしているわけではありません（たとえば、仮想ゲートウェイ）。

IP インターフェイスを設定する場合は、次の情報が必要です。

表 A-2　IP インターフェイス コンポーネント

名前	インターフェイスのニックネーム。
IP アドレス	同じサブネットに含まれる IP アドレスを、別々の物理イーサネット インターフェイスには設定できません。
ネットマスク（サブネットマスク）	ネットマスクを標準のドット付きオクテット形式（たとえば、255.255.255.0）または 16 進形式（たとえば、0xffffff00）で入力できます。デフォルトのネットマスクは 255.255.255.0、一般的なクラス C 値です。
ブロードキャスト アドレス	AsyncOS はデフォルトのブロードキャスト アドレスを IP アドレスおよびネットマスクから自動的に計算します。
ホスト名	インターフェイスに関連するホスト名。ホスト名は、SMTP カンバセーション中のサーバの特定に使用されます。各 IP アドレスに関連付けられた有効なホスト名を入力する必要があります。ソフトウェアは、DNS によってホスト名が一致する IP アドレスに正しく解決されたり、または逆引き DNS によって所定のホスト名が解決されることをチェックしません。
許可されるサービス	FTP、SSH、Telnet、Cisco IronPort スパム隔離、HTTP、および HTTPS はインターフェイス上でイネーブルまたはディセーブルにできます。サービスごとにポートを設定できます。Cisco IronPort スパム隔離の HTTP/HTTPS、ポート、および URL も設定できます。

（注）　第 2 章「セットアップ、インストール、および基本設定」の説明に従ってシステム セットアップ ウィザードを完了し、変更を保存している場合は、アプライアンス上に管理インターフェイスがすでに設定されているはずです。

GUI を使用した IP インターフェイスの作成

ステップ 1　[Management Appliance] > [Network] > [IP Interfaces] を選択します。

ステップ 2　[Add IP Interface] をクリックします。

ステップ 3　インターフェイスの名前を入力します。

ステップ 4　イーサネット ポートを選択し、IP アドレスを入力します。

ステップ 5　IP アドレスに対応するネットマスクを入力します。

ステップ 6　インターフェイスのホスト名を入力します。

ステップ 7　この IP インターフェイス上でイネーブルにする各サービスの横にあるチェックボックスをオンにします。必要に応じて、対応するポートを変更します。

ステップ 8　アプライアンス管理用にインターフェイスで HTTP から HTTPS へのリダイレクトをイネーブルにするかどうかを選択します。

ステップ 9　Cisco IronPort スパム隔離を使用している場合は、HTTP、HTTPS、またはその両方を選択し、それぞれにポート番号を指定できます。HTTP 要求を HTTPS にリダイレクトするかどうかも選択できます。最後に、IP インターフェイスが Cisco IronPort スパム隔離のデフォルト インターフェイスであるかどうか、およびホスト名を URL として使用するかまたはカスタム URL を指定するかを指定できます。

ステップ 10　変更を送信し、保存します。

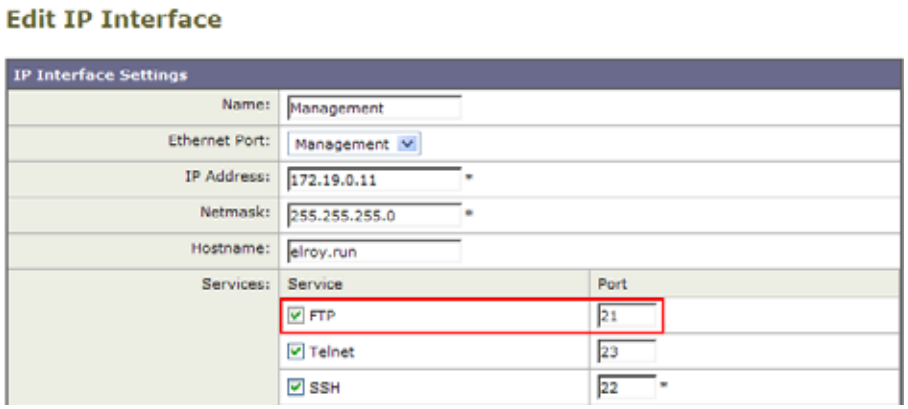
FTP 経由でのアプライアンスへのアクセス

警告　**[Management Appliance] > [Network] > [IP Interfaces] ページまたは `interfaceconfig` コマンドからサービスをディセーブルにすることにより、アプライアンスへの接続方法に応じて、GUI または CLI から切断できます。別のプロトコル、シリアル インターフェイス、または管理ポートのデフォルト設定を使用してアプライアンスに再接続できない場合は、このコマンドでサービスをディセーブルにしないでください。**

ステップ 1　[Management Appliance] > [Network] > [IP Interfaces] ページ（または `interfaceconfig` コマンド）を使用して、インターフェイスに対して FTP アクセスをイネーブルにします。

この例では、管理インターフェイスはポート 21（デフォルト ポート）上での FTP アクセスをイネーブルにするように編集されています。

図 A-2　[Edit IP Interface] ページ



（注）　次のステップに移る前に、変更を保存することを忘れないでください。

ステップ 2　FTP 経由でインターフェイスにアクセスします。インターフェイスに対して正しい IP アドレスを使用していることを確認します。

例：

```
ftp 192.168.42.42
```

ブラウザの多くは、FTP 経由でもインターフェイスにアクセスできます。

例：

```
ftp://192.10.10.10
```

ステップ 3　実行しようとする特定のタスクのディレクトリを参照します。FTP 経由でインターフェイスにアクセスしたら、次のディレクトリを参照してファイルをコピーおよび追加（「GET」および「PUT」）できます。表 A-3 を参照してください。

表 A-3　アクセスできるディレクトリ

ディレクトリ名	説明
/avarchive /bounces /cli_logs /delivery /error_logs /ftpd_logs /gui_logs /mail_logs /rptd_logs /sntpd.logs /status /system_logs	[Management Appliance] > [System Administration] > [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、『*Cisco IronPort AsyncOS for Email Security Advanced Configuration Guide*』の「Logging」の章を参照してください。 各ログ ファイル タイプの違いについては、「Logging」章の「Log File Type Comparison」を参照してください。
/configuration	次のページおよびコマンドからのデータのエクスポート先ディレクトリ、またはインポート元（保存）ディレクトリ。 • 仮想ゲートウェイ マッピング（`altsrchost`） • XML 形式の設定データ（`saveconfig`、`loadconfig`） • ホスト アクセス テーブル（HAT）ページ（`hostaccess`） • 受信者アクセス テーブル（RAT）ページ（`rcptaccess`） • SMTP ルート ページ（`smtproutes`） • エイリアス テーブル（`aliasconfig`） • マスカレード テーブル（`masquerade`） • メッセージ フィルタ（`filters`） • グローバル配信停止データ（`unsubscribe`） • `trace` コマンドのテスト メッセージ

表 A-3　アクセスできるディレクトリ（続き）

ディレクトリ名	説明
/MFM	メール フロー モニタリング データベース ディレクトリには、GUI から使用できるメール フロー モニタ機能のデータが含まれます。各サブディレクトリには、各ファイルのレコード形式を文書化した README ファイルが含まれます。 記録を残すためにこれらのファイルを異なるマシンにコピーしたり、ファイルをデータベースにロードして独自の分析アプリケーションを作成することができます。レコード形式は、すべてのディレクトリ内にあるすべてのファイルで同じです。この形式は今後のリリースで変更される場合があります。
/periodic_reports	システムで設定されているすべてのアーカイブ済みレポートが保管されます。

ステップ 4　ご使用の FTP プログラムを使用して、適切なディレクトリに対するファイルのアップロードおよびダウンロードを行います。

セキュア コピー（scp）アクセス

クライアント オペレーティング システムでセキュア コピー（scp）コマンドがサポートされている場合は、表 A-3（P.A-5）に示すディレクトリ間でファイルをコピーできます。たとえば、次の例では、ファイル `/tmp/test.txt` は、クライアント マシンからホスト名 `mail3.example.com` を持つアプライアンスの configuration ディレクトリにコピーされます。

（注）　このコマンドでは、ユーザ（admin）のパスワードを求めるプロンプトが表示されます。この例を参考用としてだけ示します。オペレーティング システムのセキュア コピーの実装方法によって異なる場合があります。

```
% scp /tmp/test.txt admin@mail3.example.com:configuration
The authenticity of host 'mail3.example.com (192.168.42.42)' can't be established.
DSA key fingerprint is 69:02:01:1d:9b:eb:eb:80:0c:a1:f5:a6:61:da:c8:db.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'mail3.example.com ' (DSA) to the list of known hosts.
admin@mail3.example.com's password: (type the password)
test.txt    100% |***************************| 1007  00:00
%
```

この例では、同じファイルがアプライアンスからクライアント マシンにコピーされます。

```
% scp admin@mail3.example.com:configuration/text.txt .
admin@mail3.example.com's password: (type the password)
test.txt    100% |***************************| 1007  00:00
```

Cisco IronPort 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、セキュア コピー（scp）を FTP に代わる方法として使用できます。

（注）　operators グループおよび administrators グループのユーザだけが、アプライアンスへのアクセスにセキュア コピー（scp）を使用できます。詳細については、「AsyncOS の以前のバージョンへの復元」（P.13-31）を参照してください。

シリアル接続によるアクセス

シリアル接続を使用してアプライアンスに接続している場合、図 A-3 にシリアル ポート コネクタのピン番号を示し、表 A-4 にシリアル ポート コネクタのピン割り当ておよびインターフェイス信号を定義します。

図 A-3　　シリアル ポートのピン番号

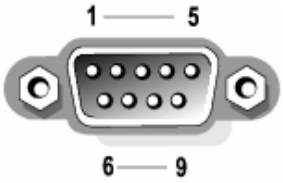


表 A-4　　シリアル ポートのピン割り当て

ピン	信号	I/O	定義
1	DCD	I	データ キャリア検出
2	SIN	I	シリアル入力
3	SOUT	O	シリアル出力
4	DTR	O	データ ターミナル レディ
5	GND	n/a	信号用接地
6	DSR	I	データ セット レディ
7	RTS	I	送信要求
8	CTS	O	送信可
9	RI	I	リング インジケータ
シェル	n/a	n/a	シャーシ アース

APPENDIX B

ネットワークと IP アドレスの割り当て

この付録では、ネットワーク アドレスと IP アドレスの割り当てに関する一般的なルールについて説明し、ネットワークに Cisco IronPort 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

Cisco IronPort X1050、C650、および C350 アプライアンスには、構成（オプションの光ネットワーク インターフェイスがあるかどうか）に応じて最大 4 個のイーサネット インターフェイスがシステムの背面パネルにあります。次のラベルが付いています。

- Management
- Data1
- Data2
- Data3
- Data4

IP アドレスとネットマスクの選択

ネットワークを設定するとき、Cisco IronPort アプライアンスは発信パケットを送信するために独自のインターフェイスを選択できなければなりません。この要件によって、イーサネット インターフェイスの IP アドレスとネットマスクの選択に関して、いくつかのことが決まります。単一のネットワークに配置できるインターフェイスは 1 つのみというのがルールです（ネットマスクがインターフェイスの IP アドレスに適用されることでそのように定められます）。

IP アドレスは、指定されたネットワークの物理インターフェイスを識別します。物理イーサネット インターフェイスは、パケットを受け取る IP アドレスを複数持つことができます。複数の IP アドレスを持つイーサネット インターフェイスは、パケットの送信元アドレスとして任意の IP アドレスを 1 つ使用して、インターフェイスからパケットを送信できます。このプロパティは、仮想ゲートウェイ テクノロジーの実装で使用されます。

ネットマスクの目的は、IP アドレスをネットワーク アドレスとホスト アドレスに分割することです。ネットワーク アドレスは、IP アドレスのネットワーク部分（ネットマスクと一致するビット）と見なすことができます。ホスト アドレスは、IP アドレスの残りのビットです。4 オクテット アドレスの有効なビット数は、クラスレス ドメイン間ルーティング（CIDR）形式で表現されることがあります。これは、スラッシュ記号、後にビット数（1 ～ 32）が続きます。

ネットマスクは、単純にバイナリの 1 を数える方法で表現できます。255.255.255.0 は「/24」になり、255.255.240.0 は「/20」になります。

インターフェイス設定のサンプル

ここでは、いくつかの代表的なネットワークに基づいたインターフェイスの設定例を示します。この例では、Int1 と Int2 の 2 つのインターフェイスを使用します。Cisco IronPort アプライアンスの場合は、これらのインターフェイス名を、3 つの Cisco IronPort 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で表現できます。

ネットワーク 1：

個別のインターフェイスは別のネットワーク上に存在するように示す必要があります。

インターフェイス	IP アドレス	ネットマスク	ネット アドレス
Int1	192.168.1.10	255.255.255.0	192.168.1.0/24
Int2	192.168.0.10	255.255.255.0	192.168.0.0/24

192.168.1.x にアドレス指定されたデータ（ここで X は自身のアドレスを除く 1 ～ 255 のいずれか。この場合は 10）は、Int1 に進みます。192.168.0.x にアドレス指定されたデータは、Int2 から送出されます。この形式ではない一部の他のアドレスに向かう（最も考えられるのは WAN またはインターネットからの）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いずれかのネットワーク上にある必要があります。そして、デフォルト ゲートウェイがパケットを転送します。

ネットワーク 2：

2 つの異なるインターフェイスのネットワーク アドレス（IP アドレスのネットワーク部分）は同じにすることができません。

イーサネット インターフェイス	IP アドレス	ネットマスク	ネット アドレス
Int1	192.168.1.10	255.255.0.0	192.168.0.0/16
Int2	192.168.0.10	255.255.0.0	192.168.0.0/16

これは、2 つのイーサネット インターフェイスが同じネットワーク アドレスを持つという、競合した状態を表しています。Cisco IronPort アプライアンスからのパケットが 192.168.1.11 に送信された場合、パケットの配信にどのイーサネット インターフェイスを使用する必要があるかを決定する方法はありません。2 つのイーサネット インターフェイスが 2 つの物理ネットワークに別々に接続されている場合、パケットは誤ったネットワークに配信される可能性があり、そうするとそのパケットの送信先を見つけることはできません。Cisco IronPort 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、Cisco IronPort 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

グラフィカル ユーザ インターフェイスまたは CLI で、インターフェイスを選択可能なコマンドや関数を実行する際にインターフェイスを選択した場合（たとえば、AsyncOS のアップグレードや DNS の設定など）、ルーティング（デフォルト ゲートウェイ）が選択した内容よりも優先されます。

たとえば、3 つのネットワーク インターフェイスがそれぞれ別のネットワーク セグメントに設定された次のような Cisco IronPort 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。

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（192.19.1.100）の IP 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 インターフェイスから発生することが予想されます。しかし、トラフィックは、デフォルト ゲートウェイとして設定したインターフェイス（ここでは Management）から送出されますが、送信元アドレスは Data1 の IP になります。

サマリー

Cisco IronPort 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、Cisco IronPort 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

Cisco IronPort アプライアンスの接続時の戦略

Cisco IronPort アプライアンスを接続する際には、次の点に留意してください。

- 通常、管理トラフィック（CLI、Web インターフェイス、ログ配信）は、電子メール トラフィックよりもはるかに少量です。
- 2 つのイーサネット インターフェイスが、同じネットワーク スイッチに接続されているが別のホスト ダウンストリーム上の単一のインターフェイスとのトークで終了する場合、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 で動作しているインターフェイスでの SMTP カンバセーションは、100Base-T で動作している同じインターフェイスでのカンバセーションよりも少し高速ですが、速くなるのは理想的な条件下でのみです。
- 配信ネットワークの別の箇所にボトルネックがある場合、ネットワークへの接続を最適化しても意味はありません。ボトルネックは、インターネットへの接続および接続プロバイダーのさらにアップストリームで最も頻繁に発生します。

接続に使用する Cisco IronPort アプライアンス 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。ネットワーク トポロジまたはデータ ボリュームが必要としない場合は、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。

APPENDIX C

ファイアウォール情報

次の表は、Cisco IronPort アプライアンスを正常に動作させるために開けなければならないことがあるポートのリストです（デフォルト値を示す）。

表 C-1　　ファイアウォール ポート

ポート	プロトコル	In/Out	ホスト名	説明
20/21	TCP	In または Out	AsyncOS IP、FTP サーバ	ログ ファイルのアグリゲーションの FTP。
22	SSH	Out	AsyncOS IP	中央集中型コンフィギュレーション マネージャのコンフィギュレーションの配信。 バックアップにも使用されます。
22	TCP	In	AsyncOS IP	CLI への SSH アクセス、ログ ファイルのアグリゲーション。
22	TCP	Out	SCP サーバ	ログ サーバへの SCP 配信。
23	Telnet	In	AsyncOS IP	CLI への Telnet アクセス。
23	Telnet	Out	Telnet サーバ	Telnet アップグレード。
25	TCP	Out	Any	電子メール送信用 SMTP。
25	TCP	In	AsyncOS IP	バウンスされた電子メールを受信する SMTP または外部のファイアウォールから電子メールをインジェクトする場合。
80	HTTP	In	AsyncOS IP	システム モニタリングのための GUI への HTTP アクセス。
80	HTTP	Out	downloads.cisco.com	サービス アップデート、AsyncOS アップグレードを除く。
80	HTTP	Out	updates.cisco.com	AsyncOS アップグレード。
82	HTTP	In	AsyncOS IP	Cisco IronPort スパム隔離の表示に使用。
83	HTTPS	In	AsyncOS IP	Cisco IronPort スパム隔離の表示に使用。
53	UDP/TCP	Out	DNS サーバ	インターネット ルート サーバまたはファイアウォール外部の DNS サーバを使用するように設定されている場合の DNS。また、SenderBase クエリーの場合。
110	TCP	Out	POP サーバ	Cisco IronPort スパム隔離のためのエンドユーザの POP 認証。

表 C-1　ファイアウォール ポート（続き）

123	UDP	Out	NTP サーバ	タイム サーバがファイアウォール外部の場合、NTP。
143	TCP	Out	IMAP サーバ	Cisco IronPort スパム隔離のためのエンドユーザの IMAP 認証。
161	UDP	In	AsyncOS IP	SNMP クエリー。
162	UDP	Out	管理ステーション	SNMP トラップ。
389 3268	LDAP	Out	LDAP サーバ	LDAP ディレクトリ サーバがファイアウォール外部の場合、LDAP。Cisco IronPort スパム隔離のための LDAP 認証。
636 3269	LDAPS	Out	LDAPS	LDAPS：ActiveDirectory のグローバル カタログ サーバ。
443	TCP	In	AsyncOS IP	システム モニタリングのための GUI への HTTP（https）アクセス。
443	TCP	Out	update-static.cisco.com	アップデート サーバの最新のファイルを確認します。
443	TCP	Out	phonehome.senderbase.org	アウトブレイク フィルタの受信/送信。
514	UDP/TCP	Out	Syslog サーバ	Syslog ロギング。
2222	CCS	In および Out	AsyncOS IP	クラスタ通信サービス（中央集中型管理用）。
6025	TCP	In	AsyncOS IP	外部 Cisco IronPort スパム隔離がイネーブルの場合、Cisco IronPort スパム隔離データをセキュリティ管理アプライアンスに送信。

APPENDIX D

例

この付録では、セキュリティ管理アプライアンスを実装するいくつかの一般的な方法について、図を使用して説明します。次の項目を取り上げます。

Web セキュリティ アプライアンスの例

ここでは、セキュリティ管理アプライアンスおよび Web セキュリティ アプライアンスを使用した例について説明します。

（注） これらのシナリオはすべて、セキュリティ管理アプライアンスおよびWeb セキュリティ アプライアンスで Web レポーティングおよび Web トラッキングをイネーブルがイネーブルにされていることを前提としています。Web トラッキングおよび Web レポーティングをイネーブルにする方法については、第 5 章「中央集中型 Web レポーティングの使用方法」を参照してください。

例 1：ユーザの調査

次に、システム管理者が会社で特定のユーザを調査する例を示します。

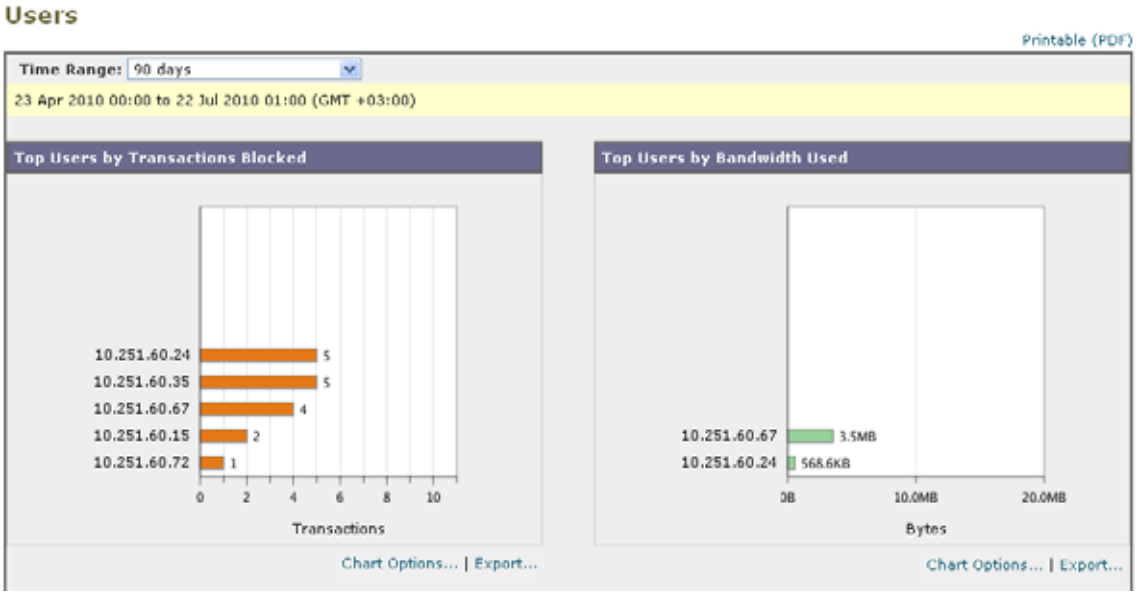
このシナリオでは、ある従業員が勤務中に不適切な Web サイトにアクセスしている、という苦情を管理者が受け取っています。それを調査するには、システム管理者が Web アクティビティの詳細をトラッキングする必要があります。

Web アクティビティがトラッキングされると、従業員の参照履歴に関する情報が記載された Web レポートが作成されます。

ステップ 1 セキュリティ管理アプライアンスで、[Web] > [Reporting] > [Users] を選択します。

ステップ 2 [Users] テーブルで、調査する [User ID] または [Client IP address] をクリックします。

ユーザ ID またはクライアント IP アドレスがわからない場合は、ユーザ ID またはクライアント IP アドレスをわかる範囲でテキスト フィールドに入力し、[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。[Users] テーブルに、指定したユーザ ID およびクライアント IP アドレスが入力されます。この例では、クライアント IP アドレス 10.251.60.24 の情報について検索しています。



ステップ 3　IP アドレス [10.251.60.24] をクリックします。

10.251.60.24 のユーザの詳細ページが表示されます。

Users > 10.251.60.24

Printable (PDF)

Time Range: 90 days

31 Aug 2011 00:00 to 29 Nov 2011 15:00 (GMT -08:00)

URL Categories by Total Transactions

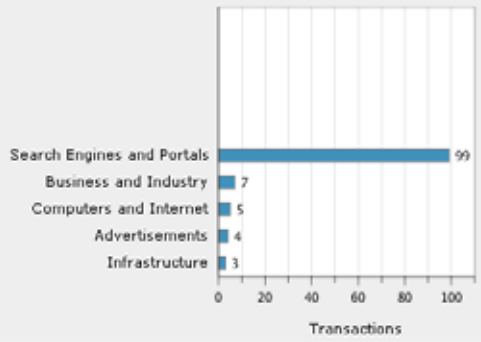


Chart Options... | Export...

Trend by Total Transactions

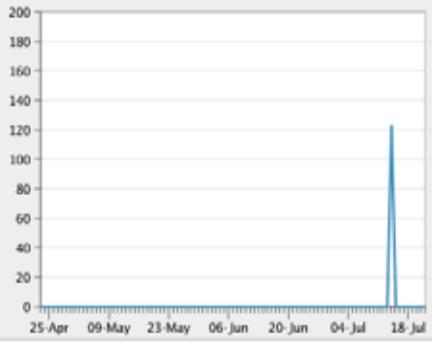


Chart Options... | Export...

URL Categories Matched

URL Category	Bandwidth Used	Time Spent	Blocked URL Category	Transactions Completed	Total Transactions
Search Engines and Portals	447.4KB	00:21	0	99	99
Business and Industry	15.5KB	00:06	0	7	7
Computers and Internet	84.4KB	00:06	0	5	5
Advertisements	16.9KB	00:00	0	4	4
Infrastructure	4,540B	00:00	0	3	3
Totals (all available data):	568.6KB	00:33	0	118	118

Find URL Category

Columns... | Export...

Domains Matched

Domain or IP	Bandwidth Used	Time Spent	Transactions Completed	Transactions Blocked	Total Transactions
[redacted].com	464.5KB	00:36	101	5	106
[redacted].com	83.1KB	00:06	4	0	4
[redacted].com	8,272B	00:00	4	0	4
[redacted].net	15.1KB	00:00	3	0	3
[redacted].com	6,391B	00:06	2	0	2
[redacted].com	1,365B	00:00	1	0	1
[redacted].com	1,231B	00:00	1	0	1
[redacted].com	1,047B	00:00	1	0	1
[redacted]	2,021B	00:00	1	0	1

Find Domain or IP

Columns... | Export...

Applications Matched

No data was found in the selected time range

Malware Threats Detected

No data was found in the selected time range

Policies Matched

Policy Name	Policy Type	Bandwidth Used	Completed Transactions	Blocked Transactions	Total Transactions

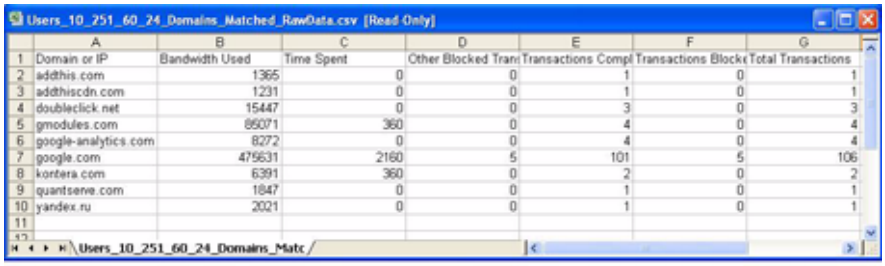
ユーザの詳細ページから総トランザクション別の URL カテゴリ、総トランザクション別のトレンド、一致する URL カテゴリ、一致するドメイン、一致するアプリケーション、検出されたマルウェアの脅威、および一致するポリシーを確認できます。

これらのカテゴリによって、10.251.60.24 のユーザがブロックされている URL（ページの [Domains] セクションに含まれる [Transactions Blocked] カラムに表示）にアクセスしようとしていたことなどがわかります。

ステップ 4　[Domains Matched] テーブルの下の [Export] をクリックし、ユーザがアクセスしようとしていたドメインおよび URL のリストを表示します。

図 D-1 に、ユーザからエクスポートされた情報のリストを示します。

図 D-1　　エクスポート データの例



	A	B	C	D	E	F	G
1	Domain or IP	Bandwidth Used	Time Spent	Other Blocked Tran	Transactions Compl	Transactions Blocke	Total Transactions
2	addthis.com	1365	0	0	1	0	1
3	addthiscdn.com	1231	0	0	1	0	1
4	doubleclick.net	15447	0	0	3	0	3
5	gmodules.com	86071	360	0	4	0	4
6	google-analytics.com	8272	0	0	4	0	4
7	google.com	479631	2160	5	101	5	106
8	kontera.com	6391	360	0	2	0	2
9	quantserve.com	1847	0	0	1	0	1
10	yandex.ru	2021	0	0	1	0	1
11							

ここから Web トラッキング機能を使用して、この特定のユーザの Web 使用状況をトラッキングし、表示することができます。

（注）　Web レポーティングでは、アクセスされる特定の URL に限らず、ユーザがアクセスするすべてのドメイン情報を取得できる点に注意してください。ユーザがアクセスしている特定の URL、その URL にアクセスした時刻、その URL が許可されているかどうかなどの情報を得るには、[Web Tracking] ページの [Proxy Services] タブを使用します。

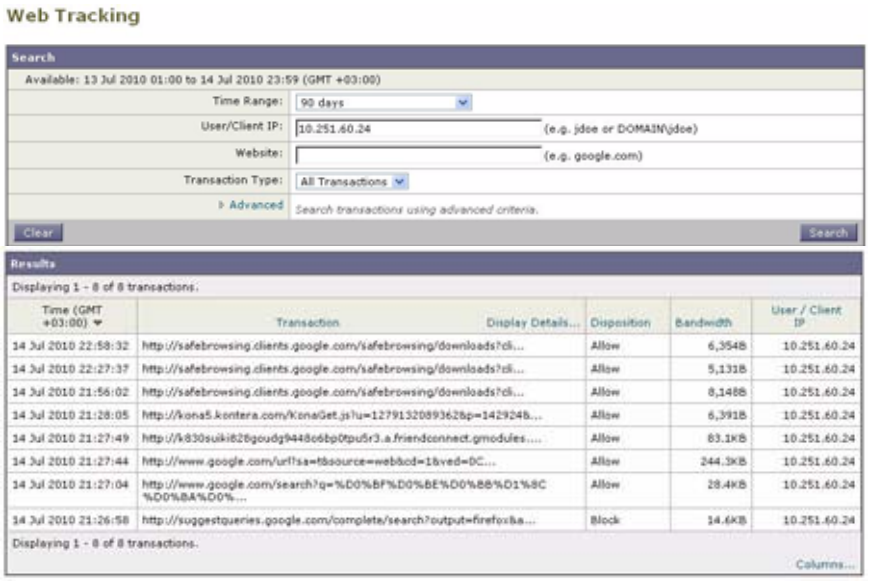
ステップ 5　[Web] > [Reporting] > [Web Tracking] を選択します。

ステップ 6　[Proxy Services] タブをクリックします。

ステップ 7　[User/Client IP Address] テキスト フィールドにユーザ名または IP アドレスを入力します。

この例では、ユーザ 10.251.60.24 の Web トラッキング情報を検索します。

検索結果が表示されます。



このページから、IP アドレス 10.251.60.24 に割り当てられているコンピュータのユーザがアクセスしたトランザクションおよび URL のすべてのリストを確認できます。

関連項目

表 D-1 に、この例で説明した項目を示します。各項目の詳細については、リンクをクリックしてください。

表 D-1　　ユーザの調査の関連項目

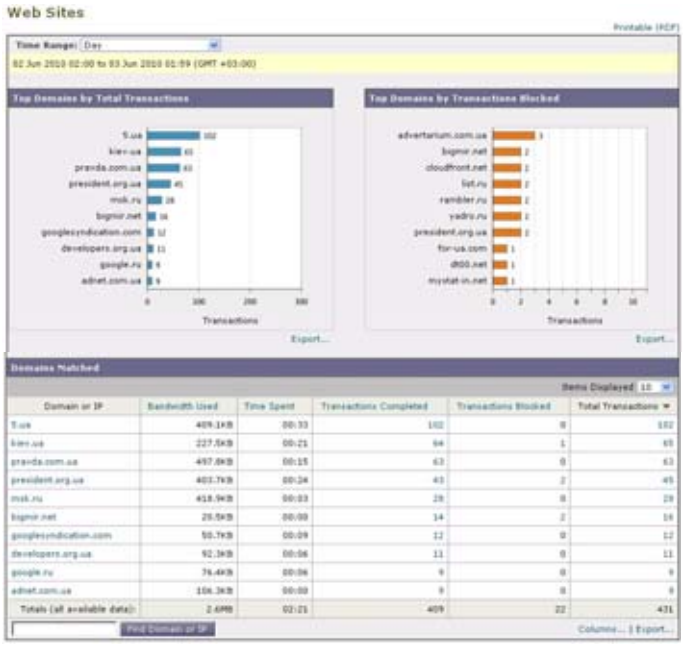
機能名	機能情報
[User] ページ	「[Users] ページ」（P.5-17）
[User Details] ページ	「[User Details] ページ」（P.5-20）
レポート データのエクスポート	「レポート データの印刷とエクスポート」（P.3-7）
[Web Tracking] ページの [Proxy Services] タブ	「[Proxy Services] タブ」（P.5-52）

例 2：URL のトラッキング

このシナリオでは、セールス マネージャが、会社のサイトへのアクセスで、先週の上位 5 位を知りたい場合を考えます。さらに、どのユーザがこれらの Web サイトにアクセスしているかについても知りたいとします。

ステップ 1　セキュリティ管理アプライアンスで、[Web] > [Reporting] > [Web Sites] を選択します。

[Web Sites] ページが表示されます。



ステップ 2　[Time Range] ドロップダウン リストから [Week] を選択します。

ステップ 3　[Domains] セクションをスクロール ダウンすると、アクセスされているドメインまたは Web サイトが表示されます。

アクセス上位 25 位までの Web サイトは、[Domains Matched] テーブルに表示されます。同じテーブルで [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 Sites] ページ	「[Web Sites] ページ」（P.5-24）

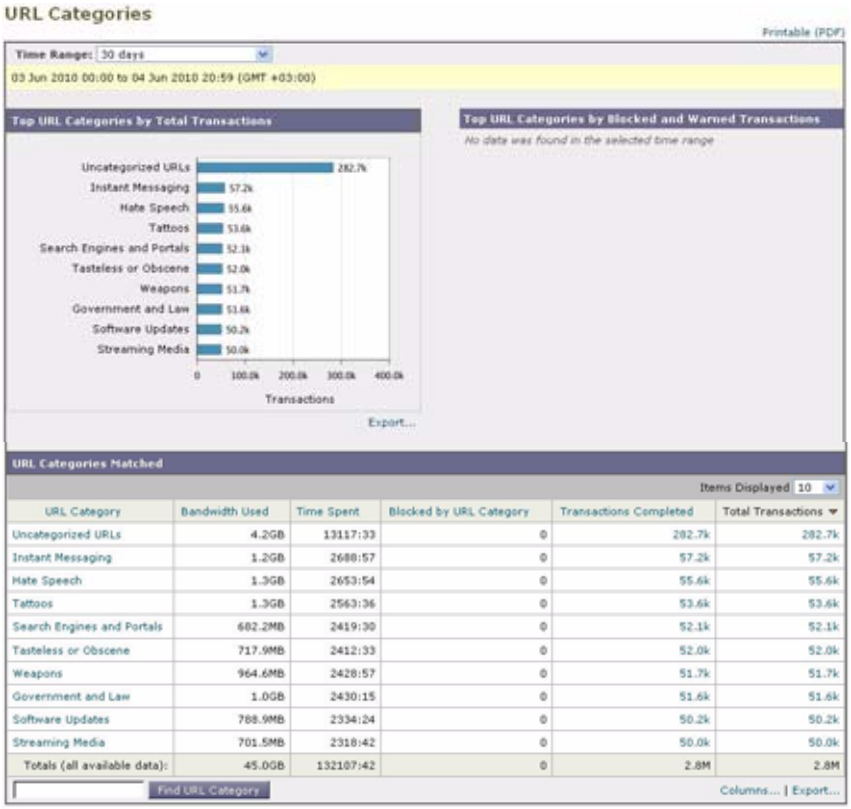
例 3：アクセス数の多い URL カテゴリの調査

このシナリオでは、従業員が最近 30 日間にアクセスした上位 3 位までの URL を、人事部長が知りたい場合を考えます。また、ネットワーク管理者が、帯域幅の使用上をモニタしたり、ネットワークで最も帯域幅を使用している URL を特定したりするためにこの情報を取得するとします。

次の例は、複数の観点を持つ複数の人のためにデータを収集するが、生成するレポートは 1 つだけで済む方法を示します。

ステップ 1　セキュリティ管理アプライアンスで、[Web] > [Reporting] > [URL Categories] を選択します。

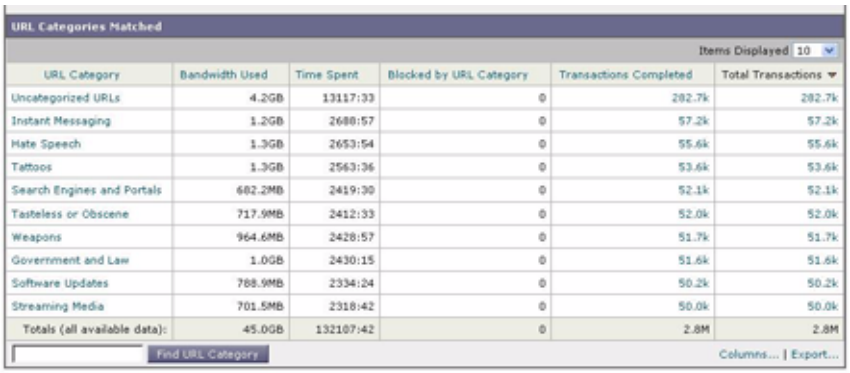
[URL Categories] ページが表示されます。



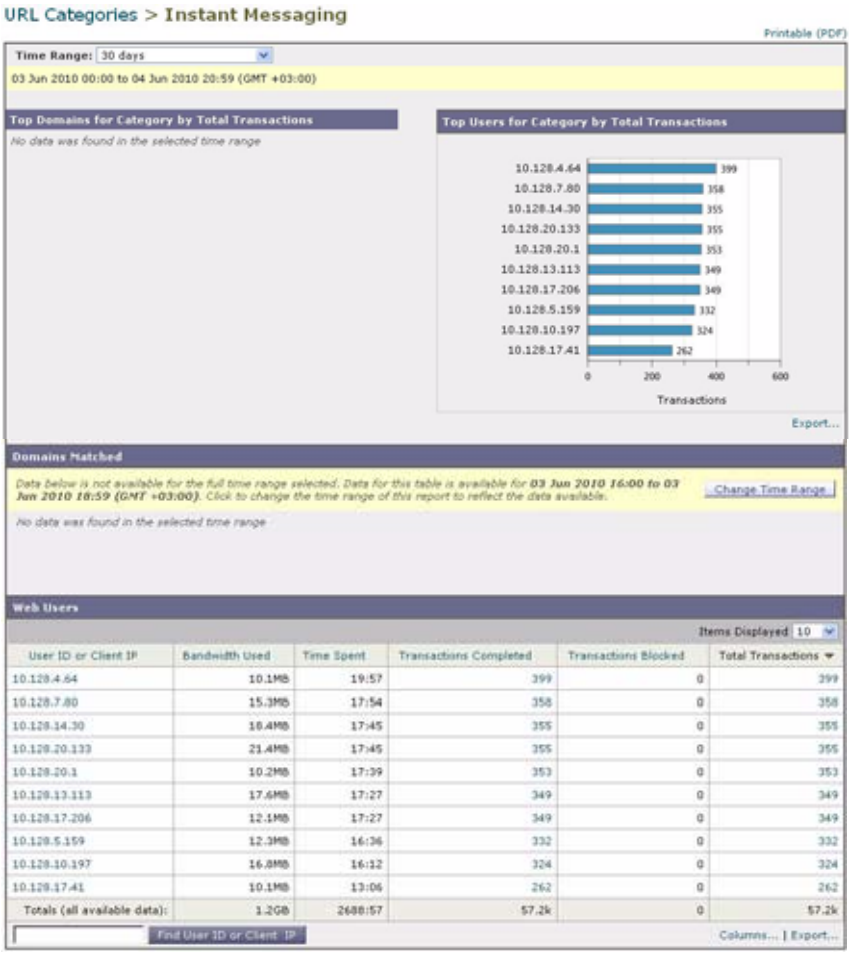
この例の [URL Categories] ページによると、総トランザクション別の上位 10 の URL カテゴリ グラフから、Instant Messaging、Hate Speech、Tattoo サイトなどの他に、282 k の未分類の URL にアクセスしていることがわかります。

ここで、[Export] リンクをクリックして raw データを Excel スプレッドシートにエクスポートすると、このファイルを人事部長に送信できます。ネットワーク マネージャに URL ごとの帯域幅の使用量を知らせる必要があります。

ステップ 2　[URL Categories Matched] テーブルをスクロールダウンし、[Bandwidth Used] カラムを表示します。



[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 [Export] リンクをクリックして、このファイルをネットワーク管理者に送信します。さらに細かく調べるには、[Instant Messaging] リンクをクリックすると、どのユーザが帯域幅を大量に使用しているかが特定されます。次のページが表示されます。



このページから、ネットワーク管理者が Instant Messaging サイトの上位 10 ユーザを知ることができます。

このページから、最近 30 日間で 10.128.4.64 のユーザが Instant Messaging サイトに 19 時間 57 分アクセスしており、この期間の帯域幅の使用量が 10.1 MB であることがわかります。

関連項目

表 D-3 に、この例で説明した項目を示します。各項目の詳細については、リンクをクリックしてください。

表 D-3　アクセスの多い URL カテゴリの調査の関連項目

機能名	機能情報
[URL Categories] ページ	「[URL Categories] ページ」（P.5-26）
レポート データのエクスポート	「レポート データの印刷とエクスポート」（P.3-7）

APPENDIX E

Cisco IronPort End User License Agreement

Cisco IronPort Systems, LLC Software License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("AGREEMENT") FOR THE LICENSE OF THE SOFTWARE (AS DEFINED BELOW). BY CLICKING THE ACCEPT BUTTON OR ENTERING "Y" WHEN PROMPTED, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY, COLLECTIVELY, THE "COMPANY") CONSENT TO BE BOUND BY AND BECOME A PARTY TO THE FOLLOWING AGREEMENT BETWEEN CISCO IRONPORT SYSTEMS, LLC, A DELAWARE CORPORATION ("IRONPORT") AND COMPANY (COLLECTIVELY, THE "PARTIES").BY CLICKING THE ACCEPT BUTTON OR ENTERING "Y" WHEN PROMPTED, YOU REPRESENT THAT (A) YOU ARE DULY AUTHORIZED TO REPRESENT YOUR COMPANY AND (B) YOU ACCEPT THE TERMS AND CONDITIONS OF THIS AGREEMENT ON BEHALF OF YOUR COMPANY, AND AS SUCH, AN AGREEMENT IS THEN FORMED.IF YOU OR THE COMPANY YOU REPRESENT (COLLECTIVELY, "COMPANY") DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, CLICK THE CANCEL BUTTON OR ENTER "N" WHEN PROMPTED AND PROMPTLY (BUT NO LATER THAT THIRTY (30) DAYS OF THE DELIVERY DATE, AS DEFINED BELOW) NOTIFY IRONPORT, OR THE RESELLER FROM WHOM YOU RECEIVED THE SOFTWARE, FOR A FULL REFUND OF THE PRICE PAID FOR THE SOFTWARE.

1. DEFINITIONS

1.1 "Company Service" means the Company's email or internet services provided to End Users for the purposes of conducting Company's internal business and which are enabled via Company's products as described in the purchase agreement, evaluation agreement, beta or pre-release agreement, purchase order, sales quote or other similar agreement between the Company and IronPort or its reseller ("Agreement") and the applicable user interface and IronPort's standard system guide documentation that outlines the system architecture and its interfaces (collectively, the "License Documentation").

1.2 "End User" means the employee, contractor or other agent authorized by Company to access to the Internet or use email services via the Company Service.

1.3 "Service(s)" means (i) the provision of the Software functionality, including Updates and Upgrades, and (ii) the provision of support by IronPort or its reseller, as the case may be.

1.4 "Software" means: (i) IronPort's proprietary software licensed by IronPort to Company along with IronPort's hardware products; (ii) any software provided by IronPort's third-party licensors that is licensed to Company to be implemented for use with IronPort's hardware products; (iii) any other IronPort software module(s) licensed by IronPort to Company along with IronPort's hardware products; and (iv) any and all Updates and Upgrades thereto.

1.5 "Updates" means minor updates, error corrections and bug fixes that do not add significant new functions to the Software, and that are released by IronPort or its third party licensors.Updates are designated by an increase to the Software's release number to the right of the decimal point (e.g., Software 1.0 to Software 1.1).The term Updates specifically excludes Upgrades or new software versions marketed and licensed by IronPort or its third party licensors as a separate product.

1.6 "Upgrade(s)" means revisions to the Software, which add new enhancements to existing functionality, if and when it is released by IronPort or its third party licensors, in their sole discretion.Upgrades are designated by an increase in the Software's release number, located to the left of the decimal point (e.g., Software 1.x to Software 2.0).In no event shall Upgrades include any new versions of the Software marketed and licensed by IronPort or its third party licensors as a separate product.

2. LICENSE GRANTS AND CONSENT TO TERMS OF DATA COLLECTION

2.1 License of Software.By using the Software and the License Documentation, Company agrees to be bound by the terms of this Agreement, and so long as Company is in compliance with this Agreement, IronPort hereby grants to Company a non-exclusive, non-sublicensable, non-transferable, worldwide license during the Term to use the Software only on IronPort's hardware products, solely in connection with the provision of the Company Service to End Users.The duration and scope of this license(s) is further defined in the License Documentation.Except as expressly provided herein, no right, title or interest in any Software is granted to the Company by IronPort, IronPort's resellers or their respective licensors.This license and any Services are co-terminus.

2.2 Consent and License to Use Data.Subject to Section 8 hereof, and subject to the IronPort Privacy Statement at http://www.ironport.com/privacy.html, as the same may be amended from time to time by IronPort with notice to Company, Company hereby consents and grants to IronPort a license to collect and use the data from the Company as described in the License Documentation, as the same may be updated from time to time by IronPort ("Data").To the extent that reports or statistics are generated using the Data, they shall be disclosed only in the aggregate and no End User identifying information may be surmised from the Data, including without limitation, user names, phone numbers, unobfuscated file names, email addresses, physical addresses and file content. Notwithstanding the foregoing, Company may terminate IronPort's right to collect and use Data at any time upon prior written or electronic notification, provided that the Software or components of the Software may not be available to Company if such right is terminated.

3. CONFIDENTIALITY.Each Party agrees to hold in confidence all Confidential Information of the other Party to the same extent that it protects its own similar Confidential Information (and in no event using less than a reasonable degree of care) and to use such Confidential Information only as permitted under this Agreement.For purposes of this Agreement "Confidential Information" means information of a party marked "Confidential" or information reasonably considered by the disclosing Party to be of a proprietary or confidential nature; provided that the Data, the Software, information disclosed in design reviews and any pre-production releases of the Software provided by IronPort is expressly designated Confidential Information whether or not marked as such.

4. PROPRIETARY RIGHTS; OWNERSHIP.Title to and ownership of the Software and other materials and all associated Intellectual Property Rights (as defined below) related to the foregoing provided by IronPort or its reseller to Company will remain the exclusive property of IronPort and/or its superior licensors.Company and its employees and agents will not remove or alter any trademarks, or other proprietary notices, legends, symbols, or labels appearing on or in copies of the Software or other materials delivered to Company by IronPort or its reseller.Company will not modify, transfer, resell for

profit, distribute, copy, enhance, adapt, translate, decompile, reverse engineer, disassemble, or otherwise determine, or attempt to derive source code for any Software or any internal data files generated by the Software or to create any derivative works based on the Software or the License Documentation, and agrees not to permit or authorize anyone else to do so.Unless otherwise agreed in writing, any programs, inventions, concepts, documentation, specifications or other written or graphical materials and media created or developed by IronPort or its superior licensors during the course of its performance of this Agreement, or any related consulting or professional service agreements, including all copyrights, database rights, patents, trade secrets, trademark, moral rights, or other intellectual property rights ("Intellectual Property Right(s)") associated with the performance of such work shall belong exclusively to IronPort or its superior licensors and shall, in no way be considered a work made for hire for Company within the meaning of Title 17 of the United States Code (Copyright Act of 1976).

5. LIMITED WARRANTY AND WARRANTY DISCLAIMERS

5.1 Limited Warranty.IronPort warrants to Company that the Software, when properly installed and properly used, will substantially conform to the specifications in the License Documentation for a period of ninety (90) days from the delivery date or the period set forth in the License Documentation, whichever is longer ("Warranty Period").FOR ANY BREACH OF THE WARRANTY CONTAINED IN THIS SECTION, COMPANY'S EXCLUSIVE REMEDY AND IRONPORT'S ENTIRE LIABILITY, WILL BE PROMPT CORRECTION OF ANY ERROR OR NONCONFORMITY, PROVIDED THAT THE NONCONFORMITY HAS BEEN REPORTED TO IRONPORT AND/OR ITS RESELLER BY COMPANY WITHIN THE WARRANTY PERIOD.THIS WARRANTY IS MADE SOLELY TO COMPANY AND IS NOT TRANSFERABLE TO ANY END USER OR OTHER THIRD PARTY.IronPort shall have no liability for breach of warranty under this Section or otherwise for breach of this Agreement if such breach arises directly or indirectly out of or in connection with the following: (i) any unauthorized, improper, incomplete or inadequate maintenance or calibration of the Software by Company or any third party; (ii) any third party hardware software, services or system(s); (iii) any unauthorized modification or alteration of the Software or Services; (iv) any unauthorized or improper use or operation of the Software or Company's failure to comply with any applicable environmental specification; or (v) a failure to install and/or use Updates, Upgrades, fixes or revisions provided by IronPort or its resellers from time to time.

5.2 WARRANTY DISCLAIMER.THE EXPRESS WARRANTIES SET FORTH IN SECTION 5.1 OF THIS AGREEMENT CONSTITUTE THE ONLY PERFORMANCE WARRANTIES WITH RESPECT TO THE SOFTWARE OR SERVICES.TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IRONPORT LICENSES THE SOFTWARE AND SERVICES HEREUNDER ON AN "AS IS" BASIS.EXCEPT AS SPECIFICALLY SET FORTH HEREIN, IRONPORT AND ITS SUPERIOR LICENSORS MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, OR STATUTORY (EITHER IN FACT OR BY OPERATION OF LAW), AND EXPRESSLY DISCLAIM ALL OTHER WARRANTIES, INCLUDING WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.NEITHER IRONPORT NOR ITS THIRD PARTY LICENSORS WARRANT THAT THE SOFTWARE OR SERVICES (1) IS FREE FROM DEFECTS, ERRORS OR BUGS, (2) THAT OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED, OR (3) THAT ANY RESULTS OR INFORMATION THAT IS OR MAY BE DERIVED FROM THE USE OF THE SOFTWARE WILL BE ACCURATE, COMPLETE, RELIABLE AND/OR SECURE.

6. LIMITATION OF LIABILITY.TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT WILL EITHER PARTY BE LIABLE TO THE OTHER FOR ANY LOSS OF PROFITS, COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, LOSS OF BUSINESS, LOSS OF USE OR DATA, INTERRUPTION OF BUSINESS, OR FOR INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES OF ANY KIND, EVEN IF SUCH PARTY RECEIVED ADVANCE NOTICE OF THE POSSIBILITY OF SUCH DAMAGES.IN NO EVENT SHALL THE LIABILITY OF EITHER PARTY ARISING UNDER ANY PROVISION OF THIS AGREEMENT, REGARDLESS OF WHETHER THE CLAIM FOR SUCH DAMAGES IS

BASED IN CONTRACT, TORT, OR OTHER LEGAL THEORY, EXCEED THE TOTAL AMOUNT PAID FOR THE SOFTWARE OR SERVICES DURING THE TWELVE (12) MONTHS PRIOR TO THE EVENT GIVING RISE TO SUCH LIABILITY.

7. TERM AND TERMINATION.The term of this Agreement shall be as set forth in the License Documentation (the "Term").If IronPort defaults in the performance of any material provision of this Agreement or the License Documentation, then Company may terminate this Agreement upon thirty (30) days written notice if the default is not cured during such thirty (30) day period.If Company defaults in the performance of any material provision of this Agreement or the License Documentation, IronPort may terminate this Agreement upon thirty (30) days written notice if the default is not cured during such thirty (30) day notice and without a refund.This Agreement may be terminated by one Party immediately at any time, without notice, upon (i) the institution by or against the other Party of insolvency, receivership or bankruptcy proceedings or any other proceedings for the settlement of such Party's debts, (ii) such other Party making a general assignment for the benefit of creditors, or (iii) such other Party's dissolution.The license granted in Section 2 will immediately terminate upon this Agreement's termination or expiration.Within thirty (30) calendar days after termination or expiration of this Agreement, Company will deliver to IronPort or its reseller or destroy all copies of the Software and any other materials or documentation provided to Company by IronPort or its reseller under this Agreement.

8. U.S.GOVERNMENT RESTRICTED RIGHTS; EXPORT CONTROL.The Software and accompanying License Documentation are deemed to be "commercial computer software" and "commercial computer software documentation", respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable.Any use, modification, reproduction, release, performance, display or disclosure of the Software and accompanying License Documentation by the United States Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement.Company acknowledges that the Software and License Documentation must be exported in accordance with U.S.Export Administration Regulations and diversion contrary to U.S.laws is prohibited.Company represents that neither the United States Bureau of Export Administration nor any other federal agency has suspended, revoked or denied Company export privileges.Company represents that Company will not use or transfer the Software for end use relating to any nuclear, chemical or biological weapons, or missile technology unless authorized by the U.S.Government by regulation or specific license.Company acknowledges it is Company's ultimate responsibility to comply with any and all import and export restrictions, and other applicable laws, in the U.S.or elsewhere, and that IronPort or its reseller has no further responsibility after the initial sale to Company within the original country of sale.

9. MISCELLANEOUS. This Agreement is governed by the laws of the United States and the State of California, without reference to conflict of laws principles.The application of the United Nations Convention of Contracts for the International Sale of Goods is expressly excluded.Nothing contained herein shall be construed as creating any agency, partnership, or other form of joint enterprise between the parties.Neither party shall be liable hereunder by reason of any failure or delay in the performance of its obligations hereunder (except for the payment of money) on account of (i) any provision of any present or future law or regulation of the United States or any applicable law that applies to the subject hereof, and (ii) interruptions in the electrical supply, failure of the Internet, strikes, shortages, riots, insurrection, fires, flood, storm, explosions, acts of God, war, terrorism, governmental action, labor conditions, earthquakes, or any other cause which is beyond the reasonable control of such party.This Agreement and the License Documentation set forth all rights for the user of the Software and is the entire agreement between the parties and supersedes any other communications with respect to the Software and License Documentation.The terms and conditions of this Agreement will prevail, notwithstanding any variance with the License Documentation or any purchase order or other written instrument submitted by a party, whether formally rejected by the other party or not.This Agreement may not be modified except by a written addendum issued by a duly authorized representative of IronPort, except that IronPort may modify the IronPort Privacy Statement at any time, in its discretion, via notification to Company of such modification that will be posted at http://www.ironport.com/privacy.html.No provision hereof shall be deemed waived unless such waiver shall be in writing and signed by IronPort or a duly

authorized representative of IronPort.If any provision of this Agreement is held invalid, the remainder of this Agreement shall continue in full force and effect.The parties confirm that it is their wish that this Agreement has been written in the English language only.

10. IRONPORT CONTACT INFORMATION. If Company wants to contact IronPort for any reason, please write to IronPort Systems, Inc., 950 Elm Avenue, San Bruno, California 94066, or call or fax us at tel: 650.989.6500 and fax: 650.989.6543.

INDEX

記号

A

B

C

D

F

G

H

I

L

M

N

O

P

R

S

T

U

う

え

お

か

き

く

け

こ

さ

し

す

せ

そ

た

ち

て

と

ね

は

ひ

ふ

ほ

み

む

め

も

ゆ

り

る

れ

ろ