Cisco IronPort AsyncOS 7.7 for Security Management ユーザ ガイド

2011 年 7 月 12 日

Text Part Number: OL-23827-01-J

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

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

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

Cisco IronPort AsyncOS 7.7 for Security Management ユーザ ガイド

CONTENTS

CHAPTER 1

Security Management アプライアンスをご使用の前に

『*Cisco IronPort AsyncOS for Security Management ユーザ ガイド*』では、Cisco IronPort Security Management 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。

ここでは、次の内容について説明します。

Security Management アプライアンスの概要

セキュリティの展開が複雑化していく中で、小規模な組織でさえ、業務用システム、マネージド サービス、リモート作業者、および協力関係にある外注パートナーという、複雑な組織インフラストラクチャを持っています。分散化したエン

タープライズ全体にわたって統一されたセキュリティおよび適合性ポスチャを確保するには、正しいコンポーネントを適切な場所に配置するだけでは十分ではありません。この複雑性をすべて考慮に入れた管理が必要となります。

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。

Security Management アプライアンスは、統合的な管理プラットフォームであり、電子メールと Web のセキュリティの管理、トラブルシューティングの実行、さらに数ヵ月または数年にも及ぶデータ ストレージの領域管理を行うことができます。

Cisco IronPort Security Management アプライアンスは、企業のポリシー設定と監査情報をモニタするように設計されており、ハードウェア、オペレーティング システム（AsyncOS）、および Cisco IronPort Email Security アプライアンス（ESA）と Web セキュリティ アプライアンス（WSA）用のサポート サービスが結合されています。

Security Management アプライアンスは、重要なポリシーおよびランタイム データを集中管理および統合することにより、管理者とエンドユーザに、Web セキュリティ アプライアンスと Email Security アプライアンスのレポート作成および監査情報の管理のための単一のインターフェイスを提供します。さらに、最大 150 の Web セキュリティ アプライアンスのポリシー定義およびポリシー導入を一元的に管理できます。

Security Management アプライアンスによって、Email Security アプライアンスと Web セキュリティ アプライアンスの最大パフォーマンスが保証され、また導入の柔軟性が向上することにより、企業ネットワークの整合性が保護されます。セキュリティ動作を単一の Security Management アプライアンスで行うか、複数のアプライアンスに負荷分散するかを調整できます。

Security Management アプライアンスにより、安定性、スケーラビリティ、および速度が向上します。Security Management アプライアンスは、Web セキュリティ アプライアンスと Email Security アプライアンスの単一の管理プラットフォームであり、電子メールおよび Web のセキュリティ管理者は、そのシステム上のアプライアンスを把握および制御し、さらに柔軟に対応できるようになります。

（注） Security Management アプライアンスは、中央集中型トラッキング、レポーティング、および検疫管理のための堅牢なアプリケーションですが、Security Management アプライアンスを中央集中型の電子メール管理、または「クラスタリング」に使用することは推奨していません。

Security Management アプライアンスでサポートされるサービス

Security Management 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、ネットワークを把握することは電子メールの管理に非常に重要であり、レポーティングによって可能になります。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。

- ネットワーク全体にわたる電子メール トラッキングを全体的な視点から表示
- アンチウイルス、スパム、および着信または発信メール使用状況カウンタなど、複数のセキュリティ サービスを相互に関連付ける直感的なレポートの定量化

レポートには、ブロックされたスパム、および電子メールに起因する脅威に関する統計情報も含まれます。また、他のレポートでは、内部ユーザの行動を把握することにより、企業ポリシーへの準拠を維持することができます。これらのレポートは、ボタンを 1 回クリックするだけで PDF に変換でき、レポートをスケジュール設定して電子メールで簡単に配信したり、CSV にエクスポートして電子メールを詳細に処理することもできます。

Security Management アプライアンスでは、複数の Email Security アプライアンスからほぼリアルタイムでデータを収集することにより、総合的な把握が可能です。このような把握は、レポートの作成以外でも行われます。詳細なメッセージ トラッキングによってコンプライアンス違反防止が容易になり、また「1 時間前に送信した電子メールはどうなりましたか」というような質問にも答えられるようになります。

Security Management アプライアンスは直感的なユーザ インターフェイスを備えており、検索結果を迅速に提供します。また、検索をインタラクティブに絞り込むことにより、電子メール管理者は平凡な検索作業に時間を費やさなくても済むようになります。

Email Security アプライアンスの制御は、集中管理機能を通して Security Management アプライアンス上で実行できます。この機能を Email Security アプライアンス上で使用できることにより、一貫性のある統合的なポリシーを集中管理できます。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 メンバーシップを利用して、固有のポリシーを準備する場合があります。その場合、ポリシー割り当てのレベルを設定できます。ロールベース アクセスにより、モニタリング タスクを分散化できます。

Security Management アプライアンスが中央集中型スパム検疫を備えていることから、エンド ユーザは独自の検疫を管理できます。

Web セキュリティ管理

Web セキュリティ管理者にとって、マルウェア プログラムとネットワーク上の疑わしい Web サイトは非常に大きな懸念材料です。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危険にさらし、知的財産を流出させる可能性のある Web ベースのマルウェアやスパイウェア プログラムから企業ネットワークを保護する、堅牢で、安全で、効率的なデバイスです。Web セキュリティ アプライアンスは、Cisco IronPort の SMTP セキュリティ アプリケーションを拡張して、HTTP、HTTPS、および FTP などの標準通信プロトコルに対する保護を包含します。

悪意のあるプログラムや Web サイトに関する情報を、Security Management アプライアンスのレポートから入手できます。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、Security Management 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、Security Management 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 スパム検疫：**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の集約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と Web メッセージを追跡します。
- **Cisco IronPort 中央集中型コンフィギュレーション マネージャ：**複数の Email Security 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するポリシー定義とポリシーの展開を管理します。

今回のリリースでの変更点

ここでは、AsyncOS 7.7 for Security Management の新機能および拡張機能について説明します。このリリースの詳細については、次の URL で入手できる製品リリース 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、以前に追加された機能や拡張機能を確認すると役立つ場合もあります。上記のリンクで、すべてのリリースのリリース ノートを入手できます。

表 1-1 に、このバージョンの AsyncOS for Security Management に含まれる新機能および拡張機能をまとめます。

表 1-1　AsyncOS 7.7 for Security Management の新機能

機能	説明
新機能：	
委任管理のためのカスタム電子メール ユーザ ロール	AsyncOS 7.7 では、Security Management アプライアンス上で、以下の電子メール セキュリティ関連機能への管理アクセスに対するカスタム ユーザ ロールを設計できます。 • すべての電子メール 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 • スパム検疫 詳細については、「カスタム ユーザ ロールへの管理委任」の項を参照してください。
Technician ロール	AsyncOS 7.7 の新機能。事前定義された Technician ロールでは、システム アップグレード、アプライアンスのリブート、機能キーの管理、および Security Management アプライアンスのアップグレードに必要なその他のタスクを実行できます。 詳細については、「ユーザ ロール」の項を参照してください。
DLP トラッキング権限	AsyncOS 7.7 では、管理者ユーザは、DLP ポリシー違反と一致するメッセージ トラッキングのコンテンツを表示できます。このアクセスをイネーブルまたはディセーブルにすることにより、機密情報の可視性を制御できます。 詳細については、「メッセージ トラッキングでの機密情報へのアクセスのディセーブル化」の項を参照してください。
制限のあるユーザ アカウントとパスワード設定	AsyncOS 7.7 では、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できます。使用可能なパスワード制限には、必須文字、パスワード長、およびパスワード ライフタイムが含まれます。また、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も定義できます。 詳細については、「制限ユーザ アカウントとパスワードの設定」の項を参照してください。

表 1-1　AsyncOS 7.7 for Security Management の新機能 （続き）

機能	説明
IP-Based アクセス	AsyncOS 7.7 では、Security Management アプライアンスにアクセスするユーザの IP アドレスを制御できます。ユーザは、定義したアクセス 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。組織のネットワークで、リモート ユーザのマシンと Security Management 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 7.7 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。 詳細については、「IP ベースのネットワーク アクセスの設定」の項を参照してください。
Web UI セッション タイムアウト	AsyncOS 7.7 では、Security Management 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。 詳細については、「Web UI セッション タイムアウトの設定」の項を参照してください。
パケット キャプチャ	AsyncOS 7.7 ではパケット キャプチャ制御が提供されており、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。この機能を使用すると、ネットワーク設定をデバッグし、アプライアンスに到達する、またはアプライアンスから送出されるネットワーク トラフィックを検出できます。 詳細については、「パケット キャプチャ」の項を参照してください。
時間帯の更新	AsyncOS 7.7 からは、AsyncOS のアップグレードとは独立して時間帯ファイルを更新できるようになりました。[Management Appliance] > [System Administration] > [Time Settings] ページで、時間帯ファイルの更新を確認し、手動で時間帯を更新できます。 詳細については、「時間帯ファイルの更新」の項を参照してください。
機能拡張：	
ウイルス感染フィルタ レポート	ウイルス感染フィルタ レポートが拡張され、名前が感染フィルタ レポートに変更されました。現在、このレポートには、マルウェアの配布、詐欺、およびフィッシングの試行に関する情報が含まれます。 詳細については、「[Outbreak Filters] ページ」の項を参照してください。

表 1-1　AsyncOS 7.7 for Security Management の新機能 （続き）

機能	説明
PDF レポートの機能拡張	AsyncOS 7.7 の新機能として、英語以外の言語で PDF レポートを生成できます。また、すべての非 ASCII 文字を PDF レポートに正しく出力できます。現在、複数のレポートを含む PDF レポートに、PDF の先頭へのリンクが含まれるようになりました。 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」の項を参照してください。
添付ファイルの検索	AsyncOS 7.7 では、[Message Tracking] でメッセージを添付ファイル名によって検索できます。 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。

このマニュアルの使い方

このガイドを情報源として使用し、Cisco IronPort 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。目次を参照して、お使いのシステムに関連する章を確認してください。

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。

このマニュアルは、印刷物として配布されます。また、PDF ファイル、HTML など電子的にも配布されます。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 ポータルで入手できます。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 からマニュアルの HTML オンライン ヘルプ バージョンに直接アクセスできます。

はじめる前に

このマニュアルを読み始める前に、『*IronPort Quickstart Guide*』およびアプライアンスの最新の製品リリース ノートを確認してください。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。

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。

Email Security アプライアンス

次の Email Security アプライアンスでは、Data 1 ポートに IP アドレスとして 192.168.42.42 が事前設定されています。

- X1000T
- C650
- C350

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

Web セキュリティ アプライアンス

次の Web セキュリティ アプライアンスでは、IP アドレスとして 192.168.42.42 が事前設定されています。

- S1050

- S650
- S350

Cisco IronPort S1050、S650、および S350 アプライアンスには、システムの背面パネルに次のイーサネット インターフェイスが搭載されています。

- M1
- P1
- P2
- T1
- T2

Security Management アプライアンス

次の Security Management アプライアンスでは、Data 1 ポートに IP アドレスとして 192.168.42.42 が事前設定されています。

- M160
- M600
- M650
- M660
- M670
- M1000
- M1050
- M1060

表記法

コマンドの説明では、次の表記法を使用しています。

- 波カッコ（{ }）は、選択すべき必須の要素を示します。
- 角カッコ（[ ]）は、省略可能な要素を示します。
- 縦線（|）は、二者択一、つまりどちらか一方を選択する要素を区切ります。

- 記載されているとおりに入力するコマンドおよびキーワードは、**太字**で示しています。
- ユーザが値を指定する引数は、*イタリック体*で示しています。

例を挙げて説明する場合は、次の表記法を使用しています。

- 画面に表示される情報は、screen フォントで示しています。
- ユーザが入力する情報は、**太字の** screen フォントで示しています。
- ユーザが値を指定する変数は、*イタリック体の* screen フォントで示しています。

（注） 「*注釈*」です。役立つ情報や、このマニュアル以外の参考資料などを紹介しています。

詳細情報の入手先

Cisco IronPort では、Security Management アプライアンスおよび関連製品について、より深く学ぶための次のリソースを提供しています。

- 「ドキュメント セット」（P.1-11）
- 「Cisco IronPort 技術トレーニング」（P.1-12）
- 「ナレッジ ベース」（P.1-13）
- 「シスコ サポート コミュニティ」（P.1-14）
- 「Cisco IronPort カスタマー サポート」（P.1-14）

ドキュメント セット

Cisco IronPort アプライアンスのドキュメント セットには、次のマニュアルや資料が含まれます（すべてのタイプがすべてのアプライアンスとリリースに使用できるわけではありません）。

- すべての製品のリリース ノート
- 『Quickstart Guide』と『Getting Started 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*』
- 安全性および準拠性に関する情報
- プラグインおよび API のマニュアル
- ハードウェアおよびファームウェアに関する情報
- ホワイト ペーパー
- ソリューションのマニュアル

このマニュアルでは、内容に関する追加情報を得るために他のマニュアルを参照することがあります。

Cisco IronPort アプライアンスのマニュアルは、次の場所から入手できます。

マニュアルの内容	入手場所
Security Management アプライアンス	http://www.cisco.com/en/US/products/ps10155/tsd_products_support_series_home.html
Email Security 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 技術トレーニング

Cisco IronPort Systems 技術トレーニング サービスは、Cisco IronPort セキュリティ製品およびソリューションの評価、統合、導入、保守、およびサポートに必要な知識とスキルを得られるよう支援します。

次のいずれかの方法で Cisco IronPort 技術トレーニング サービスにお問い合わせください。

トレーニング：登録およびトレーニング全般に関するお問い合わせ先は次のとおりです。

- http://training.ironport.com
- training@ironport.com

認定：証明書および認定試験に関するお問い合わせ先は次のとおりです。

- http://training.ironport.com/certification.html
- certification@ironport.com

ナレッジ ベース

Cisco IronPort ナレッジ ベースなどのリソースが提供される Customer Support Portal には、次の URL でアクセスできます。

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

（注） サイトにアクセスするには、Support Portal アカウントが必要です。アカウントをお持ちでない場合は、Support Portal のログイン ページで [Request an Account] リンクをクリックします。一般的に、Support Portal にアクセスできるのは、Cisco IronPort のお客様、パートナー、および従業員だけです。

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

Cisco IronPort カスタマー サポート

Cisco IronPort 製品のサポートは、年中無休の 24 時間体制で、電話、電子メール、またはオンラインでご依頼いただけます。

Customer Support の営業時間（月曜から金曜までの 1 日 24 時間）中は、依頼を受けてから 1 時間以内にエンジニアがご連絡します。

カスタマー サポートの営業時間外に緊急のサポートを必要とする重大な問題を報告する場合は、次のいずれかの方法で Cisco IronPort にご連絡ください。

U.S. フリー ダイヤル：1 (877) 646-4766

各国語版：http://cisco.com/web/ironport/contacts.html

サポート サイト：http://www.cisco.com/web/ironport/index.html

サポートをリセラーまたは別のサプライヤから購入された場合、製品のサポートについてはそのリセラーまたはサプライヤに直接お問い合わせください。

サード パーティ コントリビュータ

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

契約の全文については、次の URL を参照してください（Cisco IronPort Support Portal にログイン後）。

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

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

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。

Cisco IronPort に対するコメントの送付

Cisco IronPort Technical Publications チームでは、より充実した製品マニュアルを提供すべく努めています。ご意見やご要望をお寄せください。ご意見は、次の電子メール アドレスまでお送りください。

contentsecuritydocs@cisco.com

メッセージの件名行には、表紙上のこのマニュアルのタイトルと発行日をご記入ください。

CHAPTER 2

セットアップおよび設置

この章では、システム セットアップ ウィザードを使用して、Security Management アプライアンスを設定するプロセスについて説明します。この章の手順に従う前に、アプライアンスに付属の『*Cisco IronPort M-Series Quickstart Guide*』で説明されている手順を実行してください。

（注） システム セットアップ ウィザードを実行した後、中央集中型トラッキングや Cisco IronPort 中央集中型コンフィギュレーション マネージャなどの管理機能を使用する前に、Security Management アプライアンス、Email Security アプライアンス、および Web セキュリティ アプライアンスを設定する必要があります。Cisco IronPort アプライアンスの設定の詳細については、第 3 章「アプライアンスの設定」を参照してください。

この章は、次の項で構成されています。

設置計画

Security Management アプライアンスを使用すると、非武装地帯（DMZ）内に存在するセキュリティの高いゲートウェイ システムから、エンド ユーザ アプリケーション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　Security Management アプライアンスを含む一般的なネットワーク設定

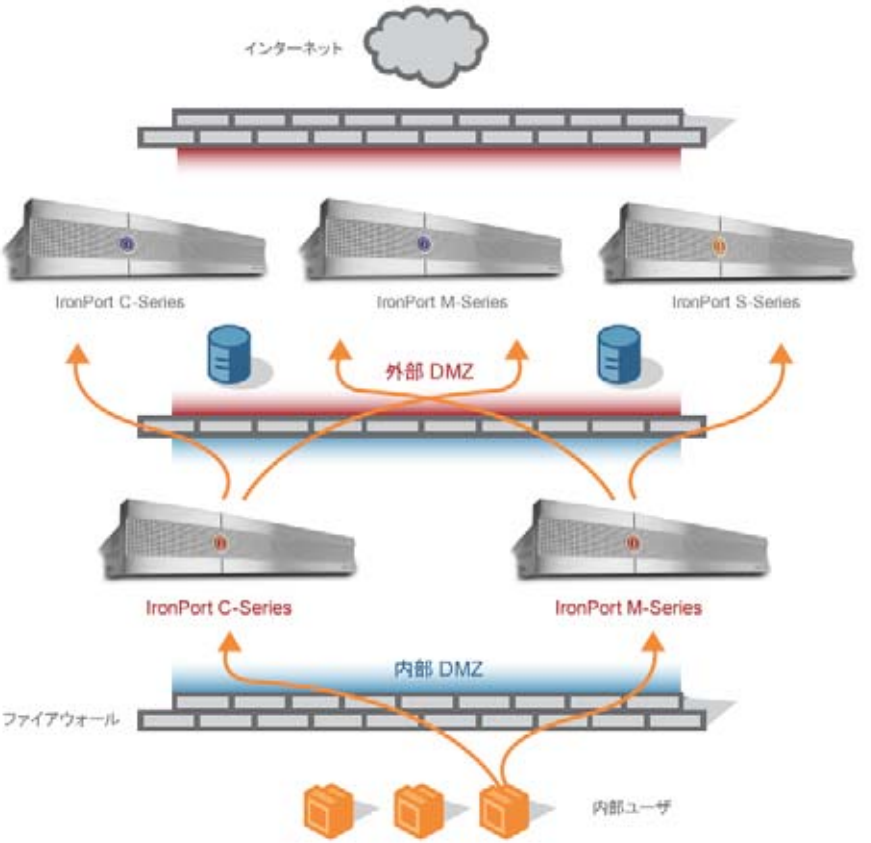


図 2-1 は、Security Management アプライアンスおよび複数の DMZ を含む、一般的なネットワーク構成を示しています。内部ネットワークで、DMZ の外側に Security Management アプライアンスを導入します。管理対象 Email Security アプライアンス（Cisco IronPort C-Series）および管理対象 Web セキュリティ アプライアンス（Cisco IronPort S-Series）へのすべての接続は、Security Management アプライアンス（Cisco IronPort M-Series）によって開始されます。

企業データセンターは Security Management 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 Email Security 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、Security Management アプライアンスは、外部 Cisco IronPort スパム検疫としても使用できます。

Email Security 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 Security Management 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。

Security Management アプライアンスを外部スパム検疫として使用する場合のメール フロー

メールは、Email Security アプライアンスから Security Management アプライアンスに送信されます。Security Management アプライアンスにメールを送信する Email Security アプライアンスが Security Management アプライアンスからメッセージの返信を受けた場合、メッセージの再処理を行いません。メッセージは HAT およびその他のポリシーやスキャン設定をバイパスします。この処理が機能するためには、Security Management アプライアンスの IP アドレスが、受信メッセージと送信メッセージの両方で同じになっている必要があります。IP アドレスが異なる場合、Email Security アプライアンスが Security Management アプライアンスからメッセージを受信すると、そのメッセージを別の着信メッセージであるかのように再び処理します。

（注）　Security Management アプライアンス上での受信および送信では、必ず同じ IP アドレスを使用してください。

Security Management アプライアンスは、Cisco IronPort スパム検疫設定で指定されている IP アドレスから検疫対象のメールを受け入れます。Security Management アプライアンスでローカル検疫を設定するには、「IronPort スパム検疫の設定」（P.7-3）を参照してください。

（注）　Security Management アプライアンスでのローカル検疫は、メールを送信するその他の Cisco IronPort アプライアンスで、*外部*検疫と呼ばれます。

Security Management アプライアンスによってリリースされたメールは、スパム検疫設定の定義に従い、プライマリ ホストおよびセカンダリ ホスト（Cisco IronPort アプライアンスまたはその他のグループウェア ホスト）に配信されます（「IronPort スパム検疫の設定」（P.7-3）を参照）。Security Management アプライアンスにメールを配信する Cisco IronPort アプライアンスの数にかかわらず、リリースされたすべてのメール、通知、およびアラートは、単一のホスト（グループウェアまたは Cisco IronPort アプライアンス）に送信されます。Security Management アプライアンスからの配信によって、プライマリ ホストが過負荷にならないように注意してください。

中央集中型管理と Security Management アプライアンス

Security Management 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 Cisco IronPort 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 Security Management アプライアンスにメッセージを配信し、外部スパム検疫にメッセージを保存できます。

物理寸法

Cisco IronPort M1000/1050 および M600/650 Security Management アプライアンスには、次の物理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 Security Management アプライアンスには、次の物理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 M160 Security Management アプライアンスには、次の物理寸法が適用されます。

- 高さ：4.20 cm（1.68 インチ）
- 幅：レールを取り付けて 48.26 cm（19.00 インチ）（レールを取り付けない場合は 17.5 インチ）
- 奥行：57.60 cm（22.70 インチ）
- 重量：最大 7.80 kg（21.6 ポンド）

セットアップの準備

Security Management アプライアンスを設定するには、グラフィカル ユーザ インターフェイス（GUI）のシステム セットアップ ウィザードを使用する必要があります。Security Management アプライアンスは、コマンド ライン インターフェイス（CLI）によるシステム設定をサポートしません。このウィザードの実行方法の詳細については、「システム セットアップ ウィザードについて」（P.2-10）を参照してください。

GUI にログインするには、PC と Security Management 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。オプションで、PC とネットワーク間（たとえば、イーサネット ハブ）およびネットワークと Security Management アプライアンスの管理ポート間を、イーサネット接続を介して接続できます。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 Security Management アプライアンスの [Management Appliance] > [Network] > [IP Interfaces] ページに移動し、Security Management 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。

システム セットアップ手順について

Security Management アプライアンスを設定するには、次の手順を実行します。

ステップ 1　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。

ステップ 2　システム セットアップに関する情報を収集します。

ステップ 3　Web ブラウザを起動し、アプライアンスの IP アドレスを入力します

ステップ 4　システム セットアップ ウィザードを実行してシステムを設定します。

ネットワーク アドレスと IP アドレスの割り当ての決定

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動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。

セットアップ情報の収集

次の表を使用して、システム セットアップに関する情報を収集します。収集した情報は、システム セットアップ ウィザードの実行中に必要となります。

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

表 2-1　システム セットアップ ワークシート

1	通知		システム アラートが送信される電子メール アドレス：
2	システム時刻		NTP サーバ（IP アドレスまたはホスト名）：
3	admin パスワード		「admin」アカウントの新しいパスワードを選択：
4	AutoSupport		Cisco IronPort AutoSupport をイネーブルにするかどうか。 ___ はい ___ いいえ
5	ホスト名		Security Management 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

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　Security Management アプライアンス上のグラフィカル ユーザ インターフェイスにアクセスするには、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。

ログイン画面が表示されます。

ステップ 2　出荷時に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、Security Management アプライアンスにログインします。

- ユーザ名：**admin**
- パスワード：**ironport**

（注）　セッションが 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。

Security Management アプライアンスの Web インターフェイスへのアクセス

Security Management 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 スパム検疫エンド 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 スパム検疫 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（Security Management 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 で HTTP によって admin Web インターフェイスにアクセスしている場合、同じブラウザでポート 83 から HTTPS で Cisco IronPort スパム検疫のエンド ユーザ Web インターフェイスにアクセスすると、admin Web インターフェイスに戻る際に再認証を要求されます。

Security Management 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

Security Management 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*。
- Security Management 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 ウィザードについて

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。**

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*。システム セットアップ ウィザードを実行する前に、表 2-1 に示す必要な情報を収集しておくと、セットアップを短時間で簡単に完了することができます。

Security Management 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　**Security Management 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。Security Management 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。**

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。具体的には次のとおりです。

- Firefox 1.0 以上
- Windows XP：IE 6.02 以上
- Windows Vista：Internet Explorer 7.0 以上
- Mozilla 1.76 以上
- Netscape 7.1 以降

- Mac OS X：Safari 2.0.4 以降
- Opera 10.0.x

GUI には、1024x768 ピクセル以上のブラウザ サイズが必要です。

（注） Windows XP オペレーティング システム上の Internet Explorer 6.0 と Opera 10.0.x、および Mac OS X 上の Safari 3.1 には、条件付きでサポートされています。条件付きサポートでは、重大な機能バグには対処されますが、軽微な問題または表示上の問題は修正されません。

セッションは、非アクティブな状態が 30 分続くと自動的にタイムアウトします。

（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、Security Management 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。

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。

サポート言語

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（簡体字と繁体字）
- ロシア語

システム セットアップ ウィザードの実行

ウィザードを起動するには、「ブラウザ要件」（P.2-10）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。

システム セットアップ ウィザードでは、次の設定作業が順に示されます。

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
- 管理パスワード

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。

ステップ 1：エンド ユーザ ライセンス契約書の確認

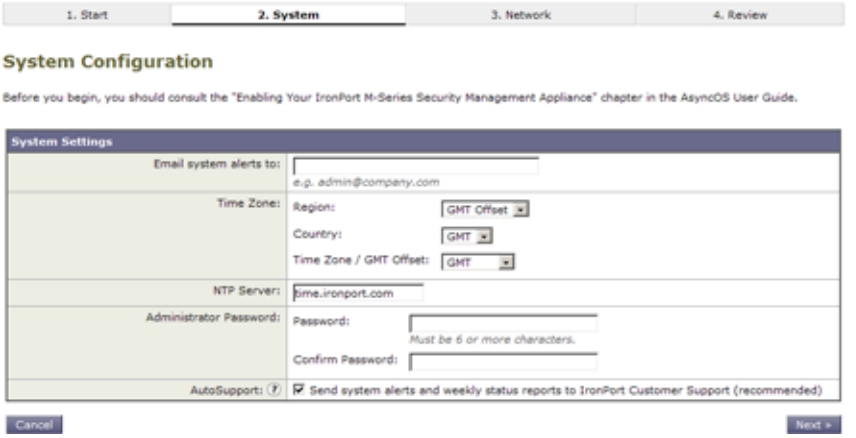
ライセンス契約書の参照から開始します。ライセンス契約書を参照し、同意する場合は、同意することを示すチェックボックスをオンにし、[Begin Setup] をクリックして続行します。

図 2-2　　ライセンス契約書の確認

ステップ 2：システム設定の実行

システム セットアップ ウィザードの設定を開始すると、[System Configuration] ページが表示されます。このページでは、システム設定を実行できます。

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



電子メール システム アラートの設定

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.12-82）を参照してください。

時間の設定

Security Management 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、Security Management 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.12-105）を参照してください。

（注）　レポートのデータを収集すると、Security Management 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.12-105）の手順で実装された設定を使用して適用されます。Security Management 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.3-17）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。

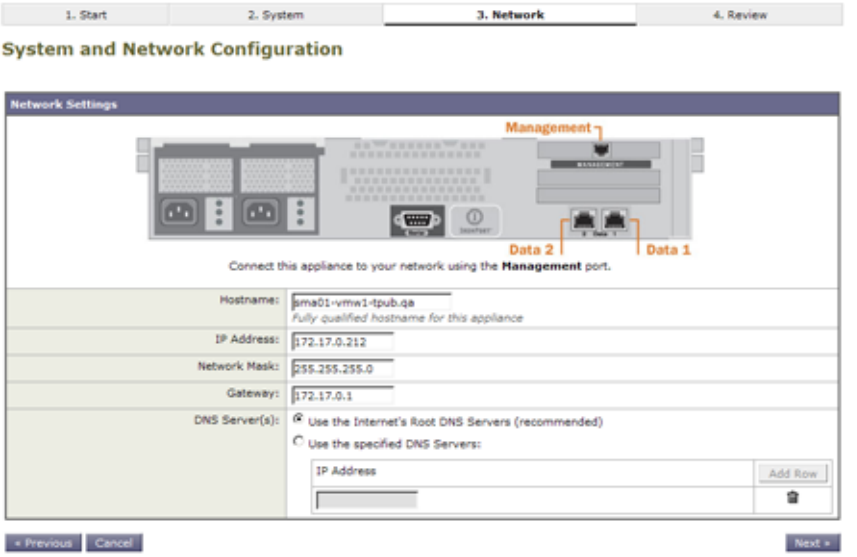
AutoSupport のイネーブル化

Cisco IronPort AutoSupport 機能（デフォルトでイネーブル）で、Security Management 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.12-85）を参照してください。

ステップ 3：ネットワーク設定の実行

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）　Security Management 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

Security Management 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。

Security Management 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。

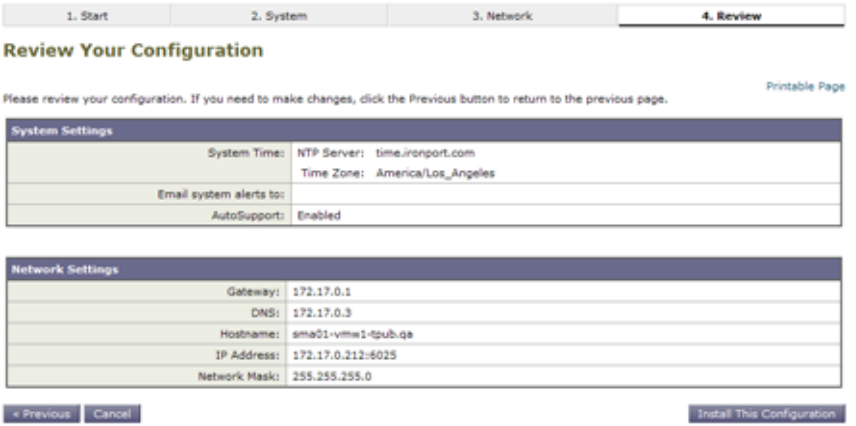
（注）　指定した DNS サーバの初期プライオリティは 0 です。詳細については、「ドメイン ネーム システム設定値の設定」（P.12-97）を参照してください。

（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、稼動中の 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動中の 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。

ステップ 4：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

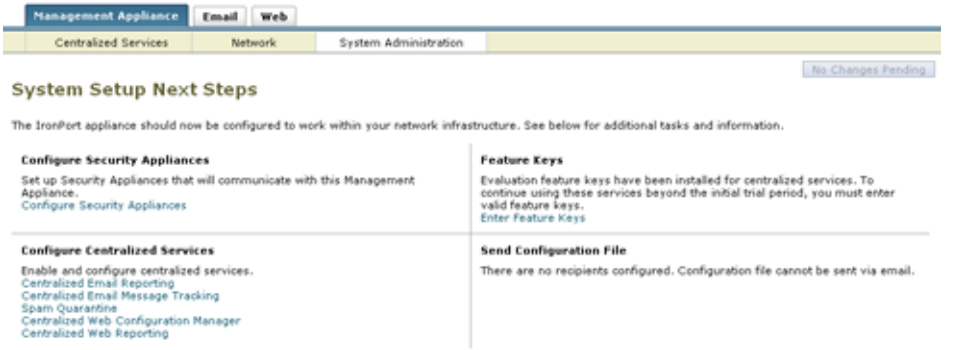


情報を確認した後、[Install This Configuration] をクリックします。次に、表示される確認ダイアログ ボックスで [Install] をクリックします。

次の手順

システム セットアップ ウィザードによって Security Management 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。アプライアンス設定の詳細については、第 3 章「アプライアンスの設定」を参照してください。

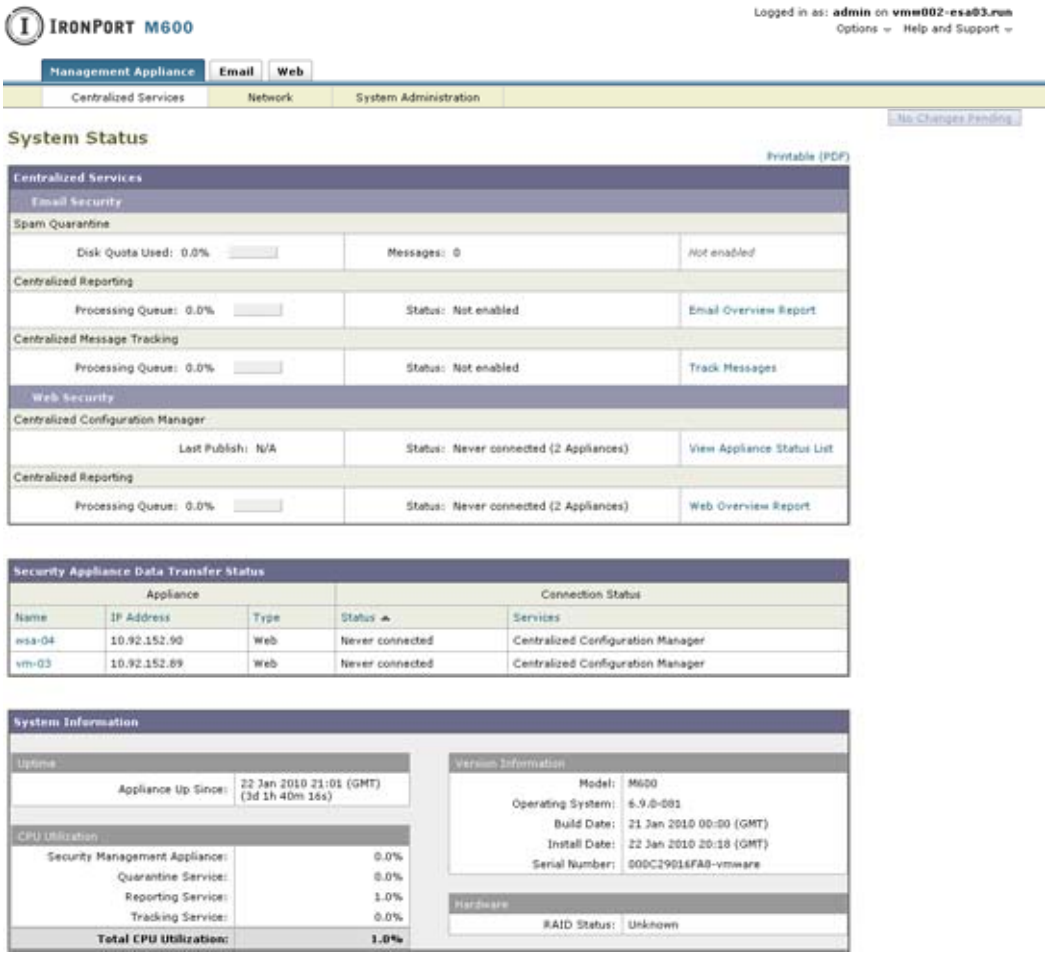
Security Management アプライアンスをインストールし、システム セットアップ ウィザードを実行した後、アプライアンス上の他の設定を修正して、モニタリング サービスを設定できます。

モニタリング サービスの設定の詳細については、第 9 章「システム ステータスのモニタリング」を参照してください。

Security Management アプライアンスのユーザ インターフェイス

初めて Security Management アプライアンスにログインすると、最初のページとして [System Status] ページが表示されます。

図 2-7　Security Management 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



[System Status] ページには、次のような Security Management 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 スパム検疫、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）
- **システム稼動時間：**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

[System Status] ページの詳細については、第 9 章「システム ステータスのモニタリング」を参照してください。

[System Status] ページのタブ

[System Status] ページでは、管理者ユーザとオペレータ ユーザが、以下のタブを使用できます。

- [Management Appliance] タブ : [Centralized Services]（[System Status]、[Security Appliances]。[Email] : [Spam Quarantine]、[Centralized Reporting]、[Centralized Message Tracking]。[Web] : [Centralized Web Reporting]、[Centralized Configuration Manager]）、[Network]（[IP Interfaces]、[SMTP Routes]、[DNS]、[Routing]）、[System Administration]（[Users]、[User Roles]、[Alerts]、[Log Subscriptions]、[Return Addresses]、[LDAP]、[Disk Management]、[Shutdown/Reboot]、[Configuration File]、[System Upgrade]。[System Time] : [Time Zone]、[Time Settings]。[Feature Keys] : [Feature Key Settings]、[Feature Keys]、[Update Settings]。[System Setup] : [System Setup Wizard]、[Next Steps]）
- [Email] タブ : [Reporting]（[Overview]、[Incoming Mail]、[Outgoing Destinations]、[Outgoing Senders]、[Internal Users]、[DLP Incidents]、[Content Filters]、[Virus Types]、[TLS Connections]、[Virus Outbreaks]、[System Capacity]、[Reporting Data Availability]、[Scheduled Reports]、[Archived Reports]）、[Message Tracking]（[Message Tracking]、[Message Tracking Data Availability]）、[Message Quarantine]（Spam Quarantine）
- [Web] タブ : [Reporting]（[Overview] : [Users]、[Web Sites]、[URL Categories]、[Application Visibility]。[Security] : [Anti-Malware]、[Client Malware Risk]、[Web Reputation Filters]、[L4 Traffic Monitor]、[Reporting by User Location]。[Reporting Services] : [Web Tracking]、[System Capacity]、[Data Availability]、[Scheduled Reports]、[Archived Reports]）、[Utilities]（[Web Appliance Status]、[Security Services Display]、[Configuration Masters]。[Publish] : [Publish to Web Appliances]、[Publish History]）、[Configuration Master 5.7]（[Web Security Manager] : [Identities, Decryption Policies]、[Routing Policies]、[Access Policies]、[Proxy Bypass]、[Custom URL Categories]、[Time

Ranges])、[Configuration Master 6.3]（[Web Security Manager] : [Identities]、[Decryption Policies]、[Routing Policies]、[Access Policies]。[Data Loss Prevention] : [Cisco IronPort Data Security Policies]、[External DLP Policies]、[Proxy Bypass]。[Custom Policy Elements] : [Custom URL Categories]、[Time Ranges])、[Configuration Master 7.1]（[Authentication] : [Identities]、[SaaS Policy]。[Web Policies] : [Decryption Policies]、[Routing Policies]、[Access Policies]、[Overall Bandwidth Limits]。[Data Loss Prevention] : [Cisco IronPort Data Security Policies]、[External DLP Policies]、[Outbound Malware Scanning]。[Custom Policy Elements] : [Custom URL Categories]、[Time Ranges]。[Global Settings] : [Bypass Settings])。

他のユーザに管理責任を分散する場合、それらのユーザはアクセスを許可された情報のみを表示できます。詳細については、「ユーザ ロール」（P.12-43）、「Custom Email User ロールの使用」（P.12-54）、「Custom Email User ロールについて」（P.12-49）、および「Custom Web User ロールについて」（P.12-55）を参照してください。

[Commit Changes] ボタン

Security Management 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 2-8　[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。

Security Management 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 Security Management 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」（P.2-22）
- 「機能キーでの作業」（P.2-31）

テクニカル サポート

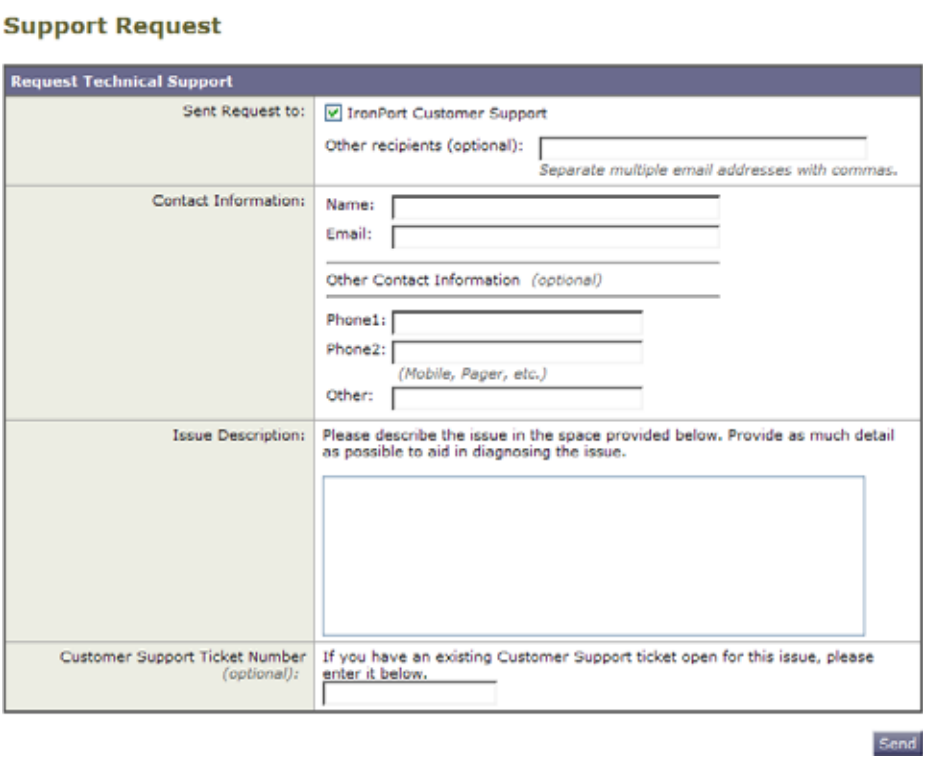
GUI の右上にある [Help and Support] メニューを使用して、Cisco IronPort カスタマー サポートに関連する機能にアクセスします。

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

[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。

図 2-9　[Support Request] ページ



Cisco IronPort カスタマー サポート要求を作成するには、次の手順を実行します。

ステップ 1　[Help and Support] > [Open a Support Case] ページで、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 2　問題の内容を入力します。

ステップ 3　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 4　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 5　[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、「Cisco IronPort カスタマー サポート」（P.1-14）を参照してください。

リモート アクセス

アプライアンスへの Cisco IronPort カスタマー サポート リモート アクセスを許可するには、[Remote Access] ページを使用します。

リモート アクセスをイネーブルにするには、次の手順を実行します。

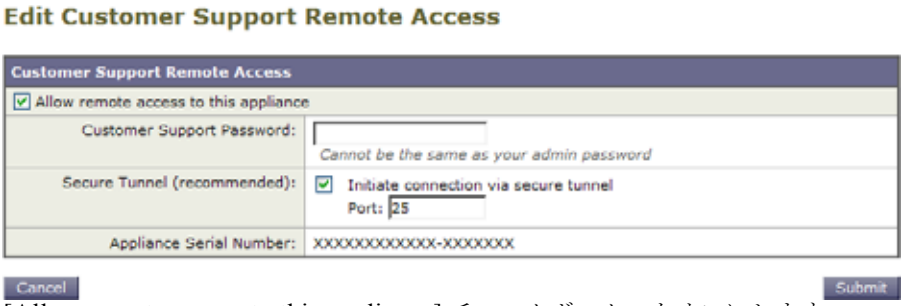
ステップ 1　Security Management アプライアンス GUI の右側で、[Help and Support] > [Remote Access] を選択します。

[Customer Support Remote Access] ウィンドウが表示されます。

ステップ 2　[Edit Remote Access Settings] を選択します。

[Edit Customer Support Remote Access] ページが表示されます。

図 2-10　[Edit Customer Support Remote Access] ページ



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　[Submit] をクリックし、[Commit] をクリックして変更を確定します。

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、ユーザが自分のシステムを設定し、設定を理解し、また問題レポートを調査するのを支援するためなどの作業で、Cisco IronPort カスタマー サポートが使用します。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、Security Management 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、Security Management 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。Security Management 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。

Security Management 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.2-26）
- 「GUI からのパケット キャプチャの開始」（P.2-27）

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

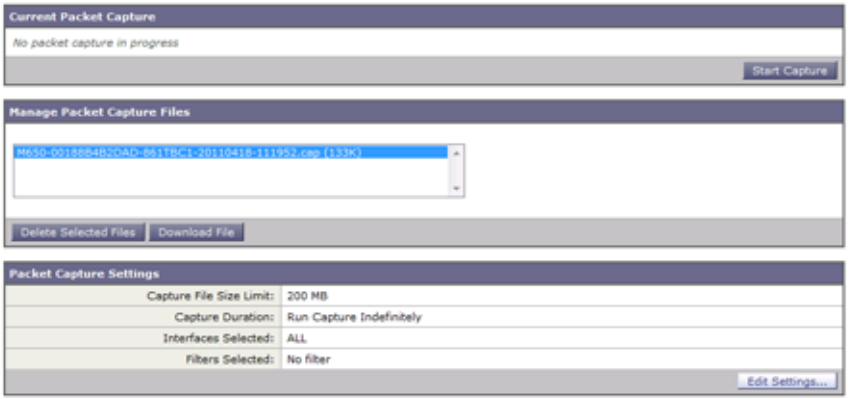
パケット キャプチャを開始するには、コマンド ライン プロンプトから **packetcapture > start** コマンドを入力します。実行されているパケット キャプチャを停止する必要がある場合は、**packetcapture > stop** コマンドを実行します。アプライアンスは、セッションが終了するとパケット キャプチャを停止します。

GUI からのパケット キャプチャの開始

Security Management アプライアンス上でパケット キャプチャを開始するには、次の手順を実行します。

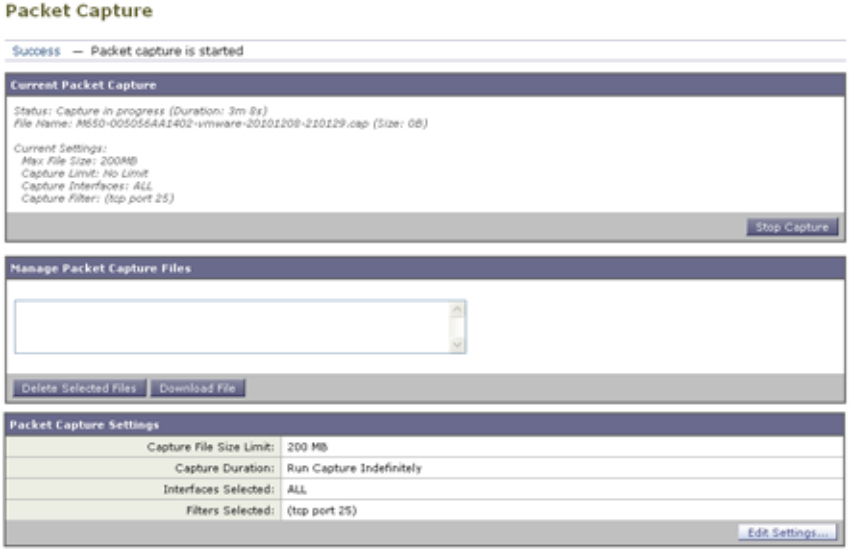
ステップ 1　Security Management アプライアンス上で、[Help and Support] > [Packet Capture] を選択します。

ステップ 2　[Packet Capture] ページが表示されます。



ステップ 3　[Start Capture] を選択します。

ステップ 4　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.2-29）
- 「GUI からのパケット キャプチャ設定の編集」（P.2-29）

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

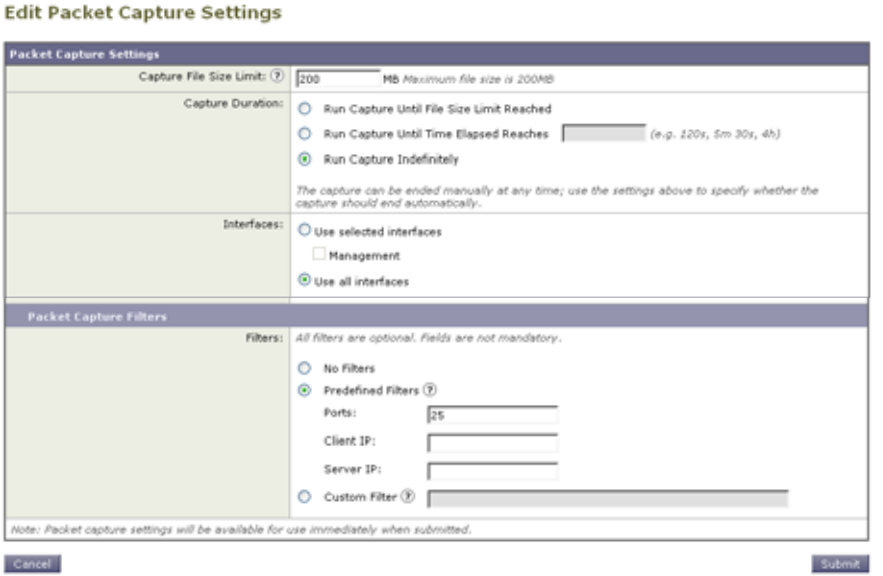
GUI からパケット キャプチャ設定を編集するには、次の手順を実行します。

ステップ 1　Security Management アプライアンス上で、[Help and Support] > [Packet Capture] を選択します。

パケット キャプチャ

ステップ 2　[Edit Settings] を選択します。

ステップ 3　[Edit Packet Capture Settings] ページが表示されます。



ステップ 4　表 2-2 に、設定可能なパケット キャプチャの項目を示します。

表 2-2　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。

表 2-2　パケット キャプチャ設定オプション（続き）

オプション	説明
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 5　[Submit] をクリックして、ページ上の変更を送信します。

（注）　AsyncOS は新しいパケット キャプチャ設定を使用します（これらを送信後）。この場合、変更を確定する必要はありません。

機能キーでの作業

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。

メイン Security Management 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。

[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。

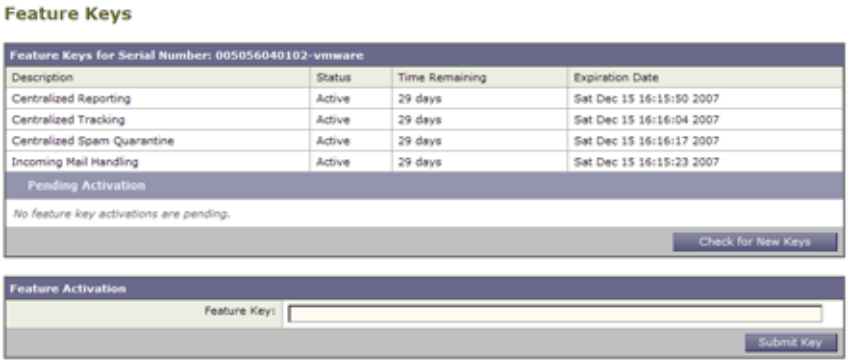
[Feature Keys] ページ

Security Management 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 2-11　[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。

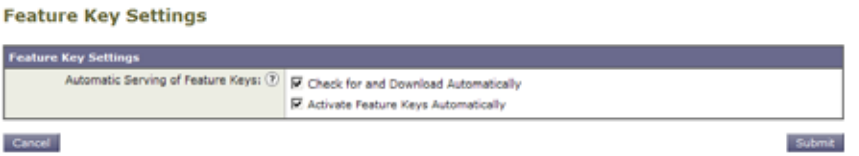
[Pending Activation] リストの新しい機能キーをアクティベートするには、そのキーを選択し（[Select] チェックボックスを選択）、[Activate Selected Keys] をクリックします。

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 2-12　[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。

SMA 互換性マトリクス

このセクションでは、Security Management アプライアンスの AsyncOS 7.7 と、Email Security アプライアンスと Web セキュリティ アプライアンスのさまざまな AsyncOS リリースとの間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 Security Management 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 2-3　Security Management アプライアンスと Email Security アプライアンスの互換性

バージョン	レポーティング	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	サポートあり
ESA 6.4	サポートあり	サポートあり	サポートあり	サポートあり
ESA 6.5	サポートあり	サポートあり	サポートあり	サポートあり
ESA 7.0	サポートあり	サポートあり	サポートあり	サポートあり
ESA 7.1	サポートあり	サポートあり	サポートあり	サポートあり
ESA 7.5	サポートあり	サポートあり	サポートあり	サポートあり

表 2-4　Security Management 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（バージョン 5.7、6.3、および 7.1）
WSA 5.6	機能は使用不可	サポートしない	サポートしない
WSA 5.7	機能は使用不可	5.7 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 6.0	機能は使用不可	サポートしない	サポートしない
WSA 6.3	機能は使用不可	5.7 と 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	サポートあり	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 バージョンと正確に一致している必要があります。

a. 表中の ICCM 公開行と拡張ファイル公開行は、公開先が Web セキュリティ アプライアンスです。

表 2-5　（WSA のある導入環境のみ）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：	Web セキュリティ アプライアンス バージョンからのソース コンフィギュレーション ファイル：
5.7	N/A	Web セキュリティ アプライアンス 5.7
6.3	Configuration Master 5.7	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

CHAPTER 3

アプライアンスの設定

この章は、次の項で構成されています。

アプライアンスの設定の概要

Security Management アプライアンスでシステム セットアップ ウィザードを実行後は、Security Management アプライアンスおよびその他の Cisco IronPort アプライアンスを設定し、それらが通信できるようにする必要があります。

Cisco IronPort アプライアンスを設定するには、次の手順を実行します。

ステップ 1 **Web セキュリティ アプライアンス。**ネットワーキング、認可、およびセキュリティ サービスを設定し、ポリシーを設定してテストします。『*Cisco IronPort AsyncOS for Web User Guide*』を参照してください。

ステップ 2 **Security Management アプライアンス。**管理サービスをイネーブルにします。その他の Cisco IronPort アプライアンスを管理する Security Management アプライアンスで、サービスをイネーブルにする必要があります。次のサービスを 1 つ以上イネーブルにできます。

- 電子メールおよび Web 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
- 電子メール アプライアンスの中央集中型トラッキング
- （電子メール用）Cisco IronPort スパム検疫
- （Web 用）Cisco IronPort 中央集中型コンフィギュレーション マネージャ

「Security Management アプライアンスでのサービスのイネーブル化」（P.3-3）を参照してください。

（注） アプライアンスで発生した Web イベント数をレポートするためのカウンタが、Web セキュリティ アプライアンスに追加されました。Email Security アプライアンスには、発生した電子メール イベント数をレポートするためのカウンタが追加されました。これで、[Management Appliance] > [Centralized Services] によって、Security Management アプライアンスで電子メール カウンタと Web カウンタの両方が中央集中化されます。電子メール カウンタと Web カウンタは、Security Management アプライアンスの中央集中型レポーティング ディスク領域を共有します。中央集中型レポーティングだけをオンにすると、電子メール カウンタがすべての領域を使用します。反対に、中央集中型 Web レポーティングだけをオンにすると、Web カウンタがすべてのディスク領域を使用します。両方をオンにすると、電子メールと Web レポーティングによって領域が共有されます。領域は、先着順に割り当てられます。この時点では、電子メール カテゴリと Web カテゴリで中央集中型レポーティング ディスク領域を共有する方法がありません。

ステップ 3　**Security Management アプライアンス。**管理対象の Email Security アプライアンスおよび Web セキュリティ アプライアンスを追加します。Security Management アプライアンスで [Management Appliance] > [Centralized Services] > [Security Appliances] を選択し、Cisco IronPort アプライアンスを追加します。「管理対象アプライアンスの追加」（P.3-11）を参照してください。

ステップ 4　**Email Security アプライアンス。**管理対象の Web セキュリティ アプライアンスおよび Email Security アプライアンスで、モニタリング サービスとセキュリティ サービスを設定します。第 9 章「システム ステータスのモニタリング」を参照してください。

Security Management アプライアンスでのサービスのイネーブル化

Security Management アプライアンスを使用して Email Security アプライアンスおよび Web セキュリティ アプライアンスを管理するには、Security Management アプライアンス上で適切なサービスをイネーブルにする必要があります。

中央集中型レポーティングおよび中央集中型トラッキングのため、または外部 Cisco IronPort スパム検疫として Security Management アプライアンスを使用するには、まず Email Security アプライアンス上にモニタリング サービスを設定する必要があります。

（注）　Security Management アプライアンス上でサービスをイネーブルにした後、適切な Cisco IronPort アプライアンスを管理対象アプライアンスとして追加していない場合は、追加する必要があります。詳細については、「管理対象アプライアンスの追加」（P.3-11）を参照してください。

Security Management アプライアンス上で電子メール セキュリティ サービスまたは Web セキュリティ サービスのいずれかをイネーブルにする場合は、次の項を参照してください。

- 「Security Management 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とディセーブル化」（P.3-3）
- 「Security Management 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とディセーブル化」（P.3-5）
- 「Security Management 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とディセーブル化」（P.3-6）

Security Management 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とディセーブル化

（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.12-123）を参照してください。Security Management アプライアンス

上で電子メール レポーティングをイネーブルにすると、モニタリング サービスを使用して、電子メール トラフィックのレポートを作成し、メッセージ ルーティングを追跡し、また疑わしいメッセージとスパム メッセージを外部 Cisco IronPort スパム検疫に配信することができます。Email Security アプライアンスのモニタリング サービスを設定する方法の詳細については、『*Cisco IronPort AsyncOS for Email User Guide*』を参照してください。Security Management アプライアンスでのモニタリング サービスの詳細については、第 9 章「システム ステータスのモニタリング」を参照してください。

Security Management 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には、次の手順を実行します。

ステップ 1　Security Management 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　[Email Reporting Service] セクションで [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。

[Centralized Reporting] ページが表示されます。

ステップ 4　[Submit] をクリックしてページでの変更を送信し、[Commit Changes] をクリックして変更を確定します。

中央集中型電子メール レポーティングをイネーブルにすると、管理対象の Email Security アプライアンスの電子メール レポーティング グループを作成できます。「電子メール レポーティング グループの作成」（P.4-4）を参照してください。中央集中型電子メール レポーティングの使用方法の詳細については、第 4 章「中央集中型電子メール レポーティングの使用」を参照してください。

中央集中型電子メール レポーティングのディセーブル化

Security Management アプライアンスで中央集中型電子メール レポーティングをディセーブルにするには、次の手順を実行します。

ステップ 1　Security Management 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　[Reporting Services] セクションで [Edit Settings] をクリックします。

ステップ 3　[Enable Centralized Reporting Service] チェックボックスをオフにします。

ステップ 4　[Submit] をクリックしてページでの変更を送信し、[Commit Changes] をクリックして変更を確定します。

Security Management 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とディセーブル化

（注）　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.12-123）を参照してください。

Security Management アプライアンス上で Web レポーティングをイネーブルにすると、サービスの表示とモニタ、および Web トラフィックのレポートを実行できます。Email Security アプライアンスでモニタリング サービスを設定する方法の詳細については、『*Cisco IronPort AsyncOS for Security Management ユーザ ガイド*』を参照してください。Security Management アプライアンスでモニタリング サービスを設定する方法の詳細については、第 9 章「システム ステータスのモニタリング」を参照してください。

Security Management アプライアンスで中央集中型 Web レポーティングをイネーブルにするには、次の手順を実行します。

ステップ 1　Security Management 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 2　[Web Reporting Service] セクションで [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中央集中型 Web 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。

[Centralized Web Reporting] ページが表示されます。

ステップ 4　[Submit] をクリックしてページでの変更を送信し、[Commit Changes] をクリックして変更を確定します。

Web の中央集中型レポーティングをイネーブルにすると、Security Management アプライアンスのページから Web アプライアンスを追加するか、または [Disk Management] ページからディスク領域を適切に割り当てることができます。さらに、Web レポーティングを設定し、Web レポートのユーザ名とロールを表示するか、または匿名表示することができます。Web レポートの設定の詳細については、「中央集中型 Web レポーティングの設定」（P.5-3）を参照してください。

これらの項目の詳細については、「管理対象アプライアンスの追加」（P.3-11）または「ディスク使用量の管理」（P.12-123）を参照してください。

中央集中型 Web レポーティングのディセーブル化

Security Management アプライアンスで中央集中型 Web レポーティングをディセーブルにするには、次の手順を実行します。

ステップ 1　Security Management 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 2　[Edit Settings] をクリックします。

ステップ 3　[Web Reporting Service] セクションで [Enable Centralized Reporting Service] チェックボックスをオフにします。

ステップ 4　[Submit] をクリックしてページでの変更を送信し、[Commit Changes] をクリックして変更を確定します。

Security Management 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とディセーブル化

Security Management アプライアンス上で電子メール メッセージ トラッキングをイネーブルにすると、モニタリング サービスを使用して、電子メール トラフィックのレポートを作成し、メッセージ ルーティングを追跡し、また疑わしいメッセージとスパム メッセージを外部 Cisco IronPort スパム検疫に配信することができます。Email Security アプライアンスのモニタリング サービスを設定する方法の詳細については、『*Cisco IronPort AsyncOS for Email User Guide*』を

参照してください。Security Management アプライアンスでのモニタリング サービスの詳細については、第 9 章「システム ステータスのモニタリング」を参照してください。

Security Management アプライアンスで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には、次の手順を実行します。

ステップ 1　Security Management 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. Security Management アプライアンスでの変更を**送信**し、確定します。

ステップ 2　Email Security アプライアンスの場合：

a. 電子メール メッセージへ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 Email Security 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。（この機能は AsyncOS Release 7.5 で導入されました）。

b. [Security Services] > [Message Tracking] で、[Edit Settings] をクリックして [Centralized Tracking] を選択します。

c. Email Security アプライアンスでの変更を送信し、確定します。

中央集中型トラッキングの使用に関する詳細については、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。

中央集中型電子メール トラッキングのディセーブル化

Security Management アプライアンスで中央集中型電子メール トラッキングをディセーブルにするには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Management Appliance] > [Centralized Services] > [Email] > [Centralized Message Tracking] 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　[Enable Centralized Message Tracking Service] チェックボックスをオフにします。

ステップ 4　[Submit] をクリックしてページでの変更を送信し、[Commit Changes] をクリックして変更を確定します。

Security Management アプライアンスでの Cisco IronPort スパム検疫のイネーブル化とディセーブル化

（注）　Security Management アプライアンス上で Cisco IronPort スパム検疫をイネーブルにすると、モニタリング サービスを使用して、電子メール トラフィックのレポートを作成し、メッセージ ルーティングを追跡し、また疑わしいメッセージとスパム メッセージを外部 Cisco IronPort スパム検疫に配信することができます。Email Security アプライアンスのモニタリング サービスを設定する方法の詳細については、『*Cisco IronPort AsyncOS for Email User Guide*』を参照してください。Security Management アプライアンスでのモニタリング サービスの詳細については、第 9 章「システム ステータスのモニタリング」を参照してください。

Security Management アプライアンスで Cisco IronPort スパム検疫をイネーブルにするには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Management Appliance] > [Centralized Services] > [Email] > [Spam Quarantine] を選択します。

[Spam Quarantine] ページが表示されます。

ステップ 2　[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 スパム検疫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。

[Edit Cisco IronPort Spam Quarantine] ページが表示されます。

ステップ 4　（任意）スパム検疫設定を編集し、検疫へのアクセスを設定します。詳細については、「IronPort スパム検疫の設定」（P.7-3）を参照してください。

ステップ 5　[Submit] をクリックしてページでの変更を送信し、[Commit Changes] をクリックして変更を確定します。

Cisco IronPort スパム検疫のディセーブル化

Security Management アプライアンスで Cisco IronPort スパム検疫をディセーブルにするには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Management Appliance] > [Centralized Services] > [Email] > [Spam Quarantine] を選択します。

[Spam Quarantine] ページが表示されます。

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 Cisco IronPort Spam Quarantine] チェックボックスをオフにします。

ステップ 4　[Submit] をクリックしてページでの変更を送信し、[Commit Changes] をクリックして変更を確定します。

Security Management 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 マネージャのイネーブル化とディセーブル化

Security Management アプライアンスで 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には、次の手順を実行します。

ステップ 1　Security Management 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。

[Centralized Configuration Manager] ページが表示され、サービスがイネーブルになっているのが示されます。

ステップ 4　[Submit] をクリックしてページでの変更を送信し、[Commit Changes] をクリックして変更を確定します。

Cisco IronPort 中央集中型コンフィギュレーション マネージャのディセーブル化

Security Management アプライアンスで Cisco IronPort 中央集中型コンフィギュレーション マネージャをディセーブルにするには、次の手順を実行します。

ステップ 1　Security Management 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　[Edit Settings] をクリックします。

ステップ 3　[Enable Centralized Configuration Manager Service] チェックボックスをオフにします。

ステップ 4　[Submit] をクリックしてページでの変更を送信し、[Commit Changes] をクリックして変更を確定します。

管理対象アプライアンスの追加

Security Management アプライアンスでモニタリング サービスをイネーブルにした後、管理対象のアプライアンスの接続情報を追加する必要があります。「SMA 互換性マトリクス」（P.2-33）の定義に従って、サポートされる電子メールおよび Web セキュリティ アプライアンスに接続できます。

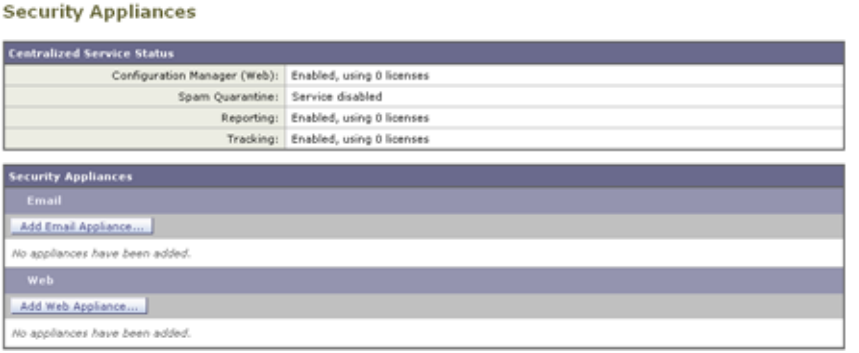
リモート アプライアンスを追加すると、Security Management アプライアンスによって、リモート アプライアンスの製品名と追加するアプライアンスのタイプが比較されます。たとえば、[Add Web Security Appliance] ページを使用してアプライアンスを追加すると、そのアプライアンスは Web セキュリティ アプライアンスであって Email Security アプライアンスではないことを確認するために、Security Management アプライアンスによってリモート アプライアンスの製品名がチェックされます。また、Security Management アプライアンスは、リモート アプライアンスのモニタリング サービスもチェックして、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。

管理対象アプライアンスを Security Management アプライアンスに追加するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Management Appliance] > [Centralized Services] > [Security Appliances] を選択します。

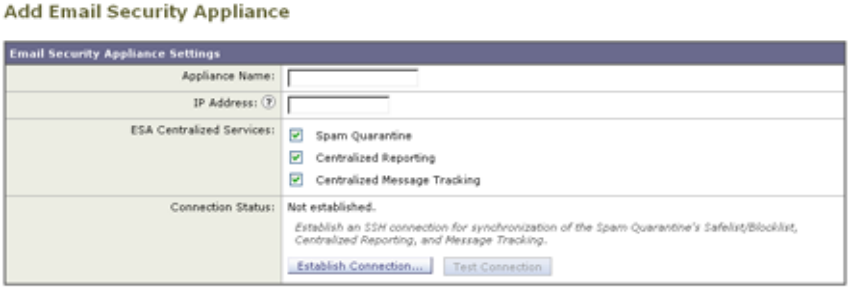
[Security Appliances] ページが表示されます。

図 3-1　[Security Appliances] ページ



ステップ 2　[Add Email Appliance] ボタンをクリックして、[Add Email Security Appliance] ページを表示します。

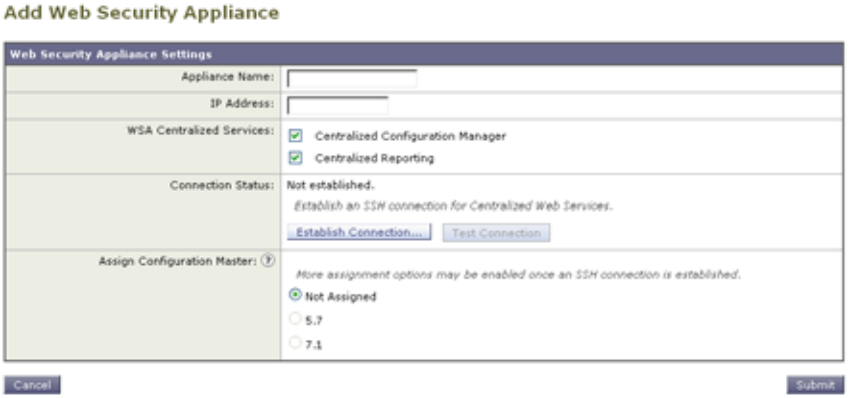
図 3-2　[Add Email Security Appliance] ページ



または

[Add Web Appliance] ボタンをクリックして、[Add Web Security Appliance] ページを表示します。

図 3-3　[Add Web Security Appliance] ページ



ステップ 3　[Appliance Name] テキスト フィールドおよび [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 4　Cisco IronPort アプライアンスを管理する際に使用するサービスを選択します。

（注）　Security Management アプライアンスでイネーブルにしたサービスのみ選択できます。詳細については、「Security Management アプライアンスでのサービスのイネーブル化」（P.3-3）を参照してください。

ステップ 5　[Establish Connection] をクリックします。

[SSH Connection] ダイアログボックスが表示されます。

図 3-4　[SSH Connection] ダイアログボックス

ステップ 6　[Username] および [Password] テキスト フィールドに、Cisco IronPort アプライアンス上の管理者アカウントのログイン資格情報を入力します。

（注）　ログイン資格情報を入力すると、Security Management 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、Security Management アプライアンスには保存されません。

ステップ 7　[Establish Connection] をクリックして、モニタリング サービス用の接続を確立します。

ステップ 8　[Test Connection] をクリックして、リモート アプライアンスのモニタリング サービスが正しく設定され、互換性があることを確認します。

ステップ 9　Web セキュリティ アプライアンスを追加する場合は、アプライアンスを割り当てる Configuration Master を選択します。

各 Configuration Master には、Web セキュリティ アプライアンスのバージョンごとの設定が含まれています。Security Management アプライアンスは、互換性のある AsyncOS のバージョンを実行する Web セキュリティ アプライアンスにのみ Configuration Master を公開できます（たとえば、Web セキュリティ アプ

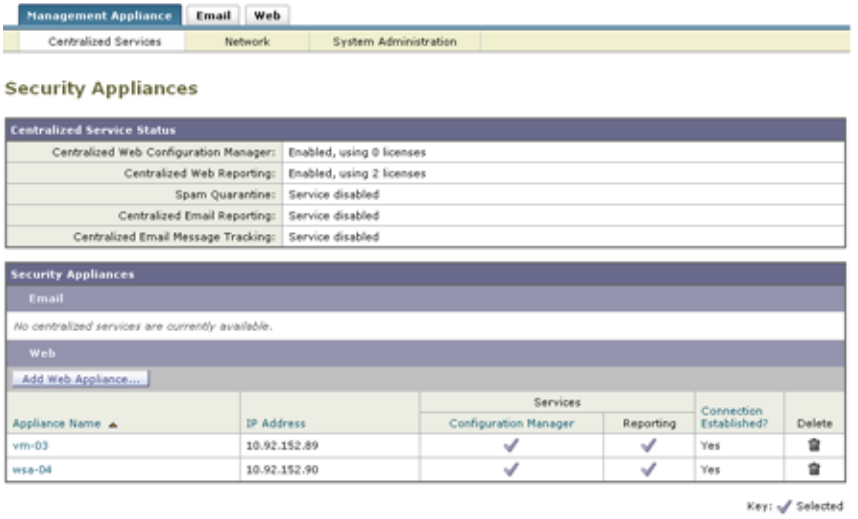
ライアンスが AsyncOS 6.3 を実行している場合、Configuration Master として 6.3.0 を選択します）。[Web] > [Utilities] > [Configuration Masters] を選択して、後で Web セキュリティ アプライアンスを割り当てることもできます（「Web セキュリティ アプライアンスと Configuration Master の関連付け」（P.8-8）を参照）。

Configuration Master および Web セキュリティ アプライアンスの管理の詳細については、第 8 章「Web セキュリティ アプライアンスの管理」を参照してください。

ステップ 10　[Submit] をクリックしてページでの変更を送信し、[Commit Changes] をクリックして変更を確定します。

[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。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、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。

図 3-5　[Security Appliances] ページの管理対象アプライアンス



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 Security Management 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編集

管理対象アプライアンスの設定を編集するには、次の手順を実行します。

ステップ 1　Security Management 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）。Email Security 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での変更を送信し、[Commit Changes] をクリックして変更を確定します。

管理対象アプライアンスの削除

管理対象アプライアンスのリストから Cisco IronPort アプライアンスを削除するには、次の手順を実行します。

ステップ 1　Security Management 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確定します。

レポートの概要

すべての Cisco IronPort アプライアンスには、Email Security アプライアンス、Web セキュリティ アプライアンス、および Security Management アプライアンスに共通する基本概念、設定、およびページがあります。レポート情報には、次の内容があります。

- 「レポーティング オプション」（P.3-16）
- 「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.3-17）
- 「[Interactive Report] ページ」（P.3-18）
- 「インタラクティブ レポートの時間範囲の選択」（P.3-18）
- 「Security Management アプライアンスのレポート フィルタ」（P.3-19）
- 「レポート データの印刷とエクスポート」（P.3-21）

レポーティング オプション

データを表示および保存するための多くのオプションが用意されています。

- 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し、表示しているレポートの PDF を生成する

- いくつかの事前定義されたレポート タイプの PDF または CSV ファイルを随時オンデマンドで生成する
- 事前定義された PDF または CSV レポートの自動作成を指定した時間にスケジュールする
- スケジュールされたレポートまたはオンデマンド レポートを、選択した受信者に電子メールで送る
- 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

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

Security Management 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取得し、これらのアプライアンスからのデータを集約します。アプライアンスによっては、Security Management アプライアンスのレポート データに含める一部のメッセージで、多少の時間がかかることがあります。データの詳細については、[System Status] ページを確認してください。

（注） Security Management アプライアンスは、レポートのデータを収集する際に、Security Management 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。Security Management 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.12-105）を参照してください。

レポート データを保存する方法

すべてのアプライアンスには、レポート データが保存されています。表 3-1 は、各アプライアンスがデータを保存する時間間隔を示しています。

表 3-1　Email Security アプライアンスおよび Web セキュリティ アプライアンスのレポート データ ストレージ

	毎分	毎時	毎日	毎週	毎月	毎年
C-Series または S-Series 上でのローカル レポート	•	•	•	•	•	

表 3-1　Email Security アプライアンスおよび Web セキュリティ アプライアンスのレポート データ ストレージ （続き）

C-Series または S-Series 上での中央集中型レポート	•	•	•	•		
M-Series		•	•	•	•	•

[Interactive Report] ページ

アプライアンスのすべてのレポート ページは、インタラクティブ レポート ページです。このため、システム内の 1 つまたはすべての管理対象 Email Security アプライアンスおよび Web セキュリティ アプライアンスの情報をモニタできます。インタラクティブ レポート ページでは、異なる時間範囲の中央集中型トラッキングおよびレポート データを表示でき、ページごとに表示するカラムのタイプを指定できます。

各アプライアンスのインタラクティブ レポート ページの詳細については、次の項を参照してください。

- 「[Email Reporting] タブの使用」（P.4-6）
- 「Web セキュリティ アプライアンス用のインタラクティブ レポート ページ」（P.5-10）

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 Security Management 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 3-2　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 ヵ月間と当月の経過した日数	•			
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	月の最初の日の 00:00 から月の最後の日の 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。

Security Management アプライアンスのレポート フィルタ

AsyncOS には、前年をカバーするレポート（[Last Year] レポート）のデータの集約を制限できるレポート フィルタがあります。1 ヵ月分に大量の一意のエントリが存在することで、集約されたレポートのパフォーマンスが低下する場合に

は、これらのフィルタを使用できます。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、変更を確定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、Security Management 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、Security Management 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、Security Management 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

ページ右上の [Printable PDF] リンクをクリックすると、すべてのレポート ページを読みやすい印刷形式の PDF 版で生成できます。

さらに、[Export] リンクをクリックすると、グラフと他の raw データをカンマ区切り（CSV）形式でエクスポートできます。大部分のレポートでは、CSV 形式のスケジューリングを行うことができます。ただし、CSV 形式で拡張レポートをスケジュールすることはできません。

PDF レポートまたは CSV レポートを、その個々のレポートの特定のロケールでスケジュール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、現在選択され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。

（注）　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。

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、Email Security 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。これらの各サブページには、[Incoming Mail] レポート ページからアクセスできます。

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。

（注）　PDF への印刷の唯一の例外は、[Web Tracking] ページを使用している場合です。[Web Tracking] ページからは、[Printable Download] リンクを使用しないと印刷できません。このリンクでは、現在のページ、または最大 10,000 のトランザクションの PDF への出力、あるいは CSV ファイルへのすべてのデータの出力を選択できます。

レポート データのエクスポート

Security Management アプライアンスの大部分のレポート ページには、エクスポート リンクが表示されています。このリンクから、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。

エクスポートされた CSV データは、Security Management アプライアンスでの設定にかかわらず、すべてのメッセージ トラッキングおよびレポーティング データを GMT で示します。GMT 時間変換の目的は、アプライアンスとは独立してデータを使用できるようにすること、または複数の時間帯でアプライアンスからのデータを参照することです。

次の例は、Anti-Malware カテゴリ レポートの raw データ エクスポートのエントリであり、太平洋夏時間（PDT）が GMT - 7 時間で表示されています。

```
Begin Timestamp, End Timestamp, Begin Date, End Date, Name,
Transactions Monitored, Transactions Blocked, Transactions Detected

1159772400.0, 1159858799.0, 2006-10-02 07:00 GMT, 2006-10-03 06:59
GMT, Adware, 525, 2100, 2625
```

表 3-3　raw データ エントリの表示

カテゴリ ヘッダー	値	説明
Begin Timestamp	1159772400.0	エポックから秒数によるクエリー開始時刻。
End Timestamp	1159858799.0	エポックから秒数によるクエリー終了時刻。
Begin Date	2006-10-02 07:00 GMT	クエリーの開始日。
End Date	2006-10-03 06:59 GMT	クエリーの終了日。
Name	Adware	マルウェア カテゴリの名前。

表 3-3　raw データ エントリの表示 （続き）

カテゴリ ヘッダー	値	説明
Transactions 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。

CHAPTER 4

中央集中型電子メール レポーティングの使用

この章は、次の項で構成されています。

レポーティングの概要

電子メール レポーティング機能では、電子メールのトラフィック パターンおよびセキュリティ リスクをモニタできるように、個別または複数の電子メール セキュリティ アプライアンスから情報を収集します。リアルタイムに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、一定の間隔で実行するようにレポートのスケジュールを設定することもできます。レポーティング機能を使用すると、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では、ネットワークの現状を把握できる概要レポートの収集だけではなく、ドリル ダウンして特定のドメイン、ユーザ、またはカテゴリのトラフィックの詳細を表示することもできます。

中央集中型トラッキング機能では、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を追跡できます。

電子メール レポーティングを使用する前に

（注）　Email Security アプライアンスの電子メール レポーティングを表示するには、1 つまたは複数の Email Security アプライアンスを追加して設定する必要があります。Email Security アプライアンスの追加の詳細については、「管理対象アプライアンスの追加」（P.3-11）を参照してください。Email Security アプライアンスの設定の詳細については、『*Cisco IronPort AsyncOS for Email Security Configuration Guide*』を参照してください。

Security Management アプライアンスで電子メール レポーティング データを表示する方法はいくつかあります。電子メール レポーティングを開始するには、次の手順を使用します。

- 電子メール レポーティングをイネーブルにするには、「中央集中型電子メール レポーティングの設定」（P.4-3）を参照してください。
- 電子メール レポーティング グループを作成するには、「電子メール レポーティング グループの作成」（P.4-4）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 ページを表示して理解するには、「電子メール レポーティング ページの概要」（P.4-12）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、「オンデマンドでのレポートの生成」（P.4-74）を参照してください。
- 指定した間隔や時刻に自動的に実行されるよう、レポートのスケジュールを設定するには、「スケジュール設定されたレポート」（P.4-76）を参照してください。
- アーカイブ済みのオンデマンド レポートおよびスケジュール設定されたレポートを表示するには、「アーカイブ済みのレポート」（P.4-79）を参照してください。

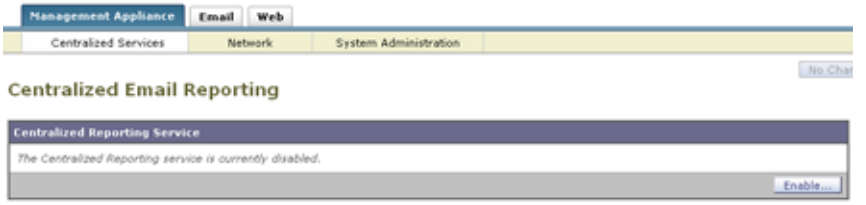
中央集中型電子メール レポーティングの設定

Security Management アプライアンスで電子メール レポーティングを使用するには、すべての電子メール レポーティングがイネーブルになるよう、Security Management アプライアンスを設定する必要があります。

中央集中型電子メール レポーティングを設定するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Management Appliance] > [Centralized Services] > [Email] > [Centralized Reporting] を選択します。

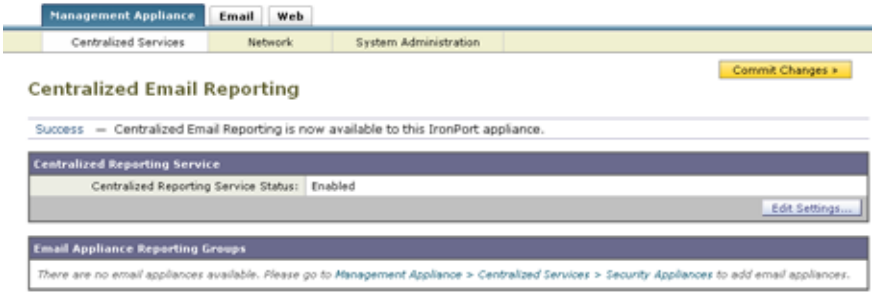
[Centralized Email Reporting] ページが表示されます。



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。

次のウィンドウが表示され、Security Management 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確認できます。



中央集中型レポーティングをイネーブルにすると、設定を編集できるようになります。

ステップ 3　[Edit Settings] をクリックします。

ステップ 4　[Edit Centralized Email Reporting Service Settings] ページが表示されます。

ステップ 5　[Enable Centralized Reporting Services] チェックボックスをクリックします。

Email Security アプライアンスでデータが保存されるのは、ローカル レポーティングを使用する場合だけです。Email Security アプライアンスで中央集中型レポーティングがイネーブルになっている場合、Email Security アプライアンスはシステム キャパシティとシステム ステータスを除いて、レポート データを保持しません。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。

ステップ 6　[Submit] をクリックして変更を送信し、[Commit Changes] をクリックしてアプライアンスでの変更を確定します。

（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.12-123）を参照してください。

電子メール レポーティング グループの作成

Security Management アプライアンスからのレポーティング データを表示する、Email Security 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

電子メール レポーティング グループを追加するには、次の手順を実行します。

ステップ 1　メイン Security Management 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　[Add Group] をクリックします。

[Add Email Reporting Group] ページが表示されます。

図 4-1　[Add Email Reporting Group] ページ

ステップ 3　グループの一意の名前を入力します。

Email Security アプライアンスで、Security Management アプライアンスに追加した Email Security 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）　Email Security アプライアンスを Security Management 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、Security Management 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 Email Security 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での変更を送信し、[Commit Changes] をクリックして変更を確定します。

（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

電子メール レポーティング グループを編集または削除するには、次の手順を実行します。

ステップ 1　メイン Security Management アプライアンスのウィンドウで、[Management Appliance] > [Centralized Services] > [Email] > [Centralized Reporting] を選択します。

[Centralized Reporting] ページが表示されます。このページでは、Email Security アプライアンス レポーティング グループを表示できます。

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ます。

[Edit Email Reporting Group] ページが表示されます。このページでは、グループを編集できます。

ステップ 3　[Submit] をクリックしてページでの変更を送信し、[Commit Changes] をクリックして変更を確定します。

[Email Reporting] タブの使用

[Email] > [Reporting] タブには、レポーティング データの複数の表示オプションが表示されます。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）　レポーティング オプションの要約については、「レポーティング オプション」（P.3-16）を参照してください。

表 4-1　[Email Reporting] タブの詳細

[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のグラフや要約テーブルが含まれます。 詳細については、「電子メール レポーティングの [Overview] ページ」（P.4-12）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 Email Security 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.4-17）を参照してください。
[Outgoing Destinations] ページ	[Outgoing Destinations] ページには、組織が電子メールを送信する宛先のドメインについての情報が表示されます。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.4-31）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.4-33）を参照してください。

表 4-1　[Email Reporting] タブの詳細（続き）

[Email Reporting] メニュー	アクション
[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.4-36）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、データ損失防止（DLP）ポリシー違反インシデントに関する情報が示されます。 詳細については、「[DLP Incident Summary] ページ」（P.4-40）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。また、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.4-43）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、Email Security アプライアンスで稼動し、Security Management 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.4-45）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.4-48）を参照してください。

表 4-1　[Email Reporting] タブの詳細（続き）

[Email Reporting] メニュー	アクション
[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検疫されたメッセージに関する情報が示されます。このページを使用して、ウイルス攻撃に対する保護をモニタします。 詳細については、「[Outbreak Filters] ページ」（P.4-51）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 Security Management 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.4-55）を参照してください。
[Data Availability] ページ	各アプライアンスの Security Management 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.4-65）を参照してください。
スケジュール設定されたレポート	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」（P.4-76）を参照してください。
アーカイブ済みのレポート	アーカイブ済みのレポートを表示および管理できます。詳細については、「アーカイブ済みのレポート」（P.4-79）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。「オンデマンドでのレポートの生成」（P.4-74）を参照してください。

インタラクティブ レポートの表示

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。

- **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.3-18）を参照してください。

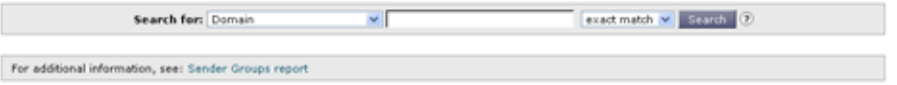
- **表示する表カラムを選択する**。表の下にある [Columns] リンクをクリックして、表示または非表示にするカラムを選択します。各カラムの説明については、「中央集中型電子メール レポーティング ページのインタラクティブ カラム」（P.E-5）を参照してください。
- ドラッグおよびドロップして、**表カラムを並べ替える**。
- **カラム見出しをクリックすると**、そのカラム内のデータで表がソートされます。
- **表示されるデータをフィルタリングする**。詳細については、「Security Management アプライアンスのレポート フィルタ」（P.3-19）を参照してください。
- **含める特定の情報を検索する**。「インタラクティブ レポート ページの検索」（P.4-10）を参照してください。

（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。

インタラクティブ レポート ページの検索

インタラクティブな電子メール レポーティング ページの多くには、[Search For:] ドロップダウン メニューが含まれています。

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 メニューでは、次のようないくつかの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。

IP アドレス検索では、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」は範囲 17.0.0.0 ～ 17.255.255.255 で検索するため、17.0.0.1 には一致しますが、172.0.0.1 には一致しません。完全一致検索の場合は、4 つすべてのオクテットを入力します。IP アドレス検索は、Classless Inter-Domain Routing（CIDR）形式（17.16.0.0/12）もサポートしています。

レポート ページのレポーティング フィルタ

AsyncOS には、前年をカバーするレポート（[Last Year] レポート）のデータの集約を制限できるレポート フィルタがあります。1 ヵ月分に大量の一意のエントリが存在することで、集約されたレポートのパフォーマンスが低下する場合には、これらのフィルタを使用できます。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。

レポーティング フィルタをイネーブルにする方法の詳細については、「Security Management アプライアンスのレポート フィルタ」（P.3-19）を参照してください。

レポート ページからのレポートの印刷とエクスポート

「レポート データの印刷とエクスポート」（P.3-21）を参照してください。

レポートとレポート ページについてのその他の情報

- 「レポーティング オプション」（P.3-16）
- 「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.3-17）

電子メール レポーティング ページの概要

ここでは、Security Management アプライアンスで電子メール レポーティングに使用されるさまざまなレポート ページについて説明します。

次の内容で構成されています。

電子メール レポーティングの [Overview] ページ

Security Management アプライアンスの [Email] > [Reporting] > [Overview] ページには、Email Security アプライアンスからの電子メール メッセージ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。

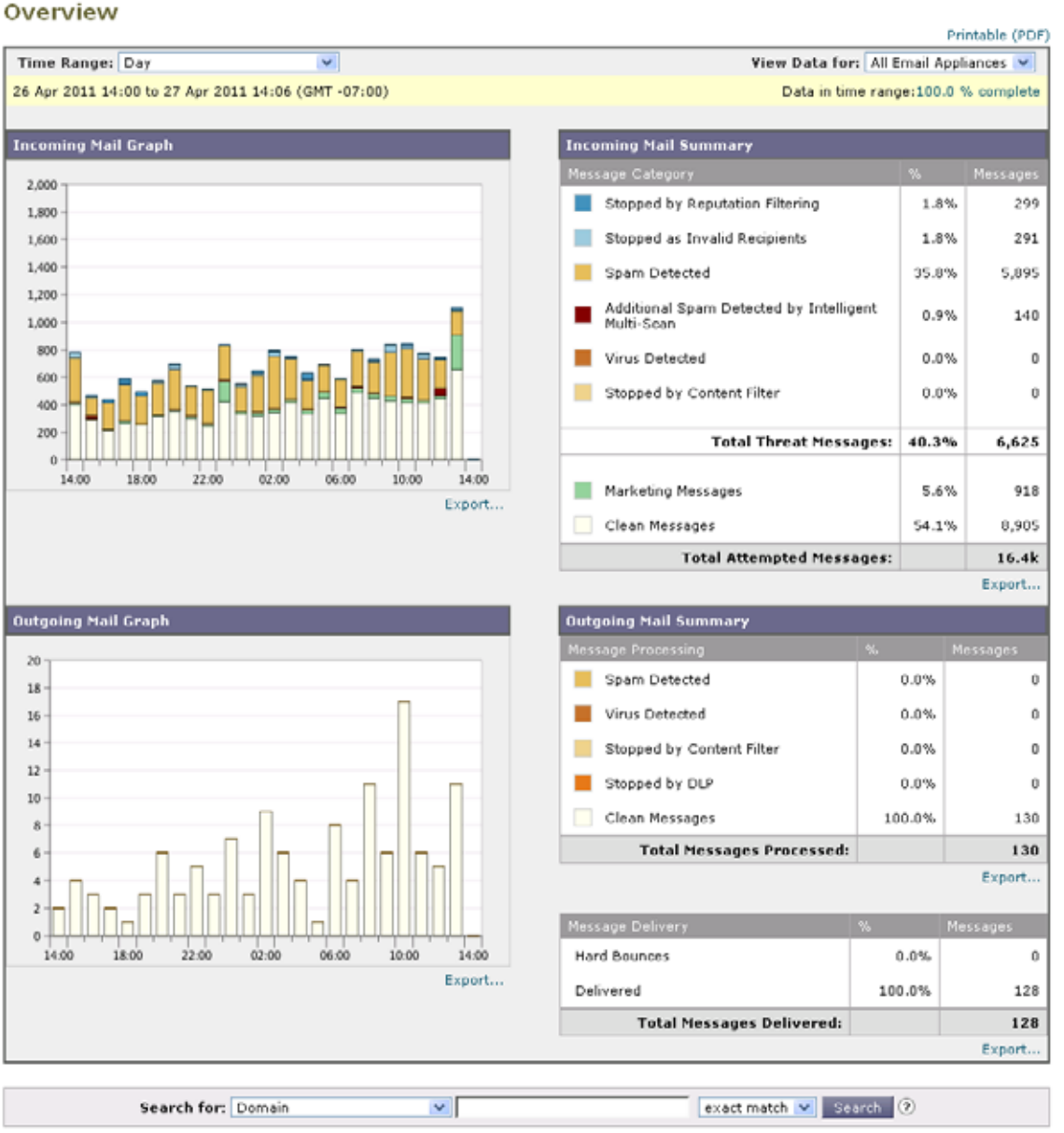
[Overview] ページを表示するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Management Appliance] > [Email] > [Reporting] > [Overview] を選択します。

[Overview] ページが表示されます。

図 4-2 に、[Overview] ページを示します。

図 4-2　[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 グラフを使用すると、アプライアンスとのすべてのメール フローをモニタできます。

（注）　[Domain-Based Executive Summary] レポートと [Executive Summary] レポートは、電子メール レポーティングの [Overview] ページに基づいて作成され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の詳細については、「スケジュール設定されたレポート」（P.4-76）を参照してください。

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

表 4-2　[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のあるドロップダウン 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.3-18）を参照してください。
Incoming Mail Graph	[Incoming Mail Graph] には、受信メールの詳細がリアルタムにグラフで表示されます。
Outgoing Mail Graph	[Outgoing Mail Graph] には、送信メールの詳細がリアルタムにグラフで表示されます。
Incoming Mail Summary	[Incoming Mail Summary] では、レピュテーション フィルタリング（SBRS）によって阻止されたメッセージの割合と数、個々の受信者、検出されたスパム、検出されたウイルスとして阻止されたメッセージの割合と数、コンテンツ フィルタによって阻止されたメッセージの割合と数、「クリーン」であると認識されたメッセージの割合と数が表示されます。
Outgoing Mail Summary	[Outgoing Mail Summary] セクションには、発信脅威およびクリーン メッセージについての情報が表示されます。また、配信されたウイルスがハードバウンスされたメッセージの詳細も表示されます。

着信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基づいて受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。

評価フィルタ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。

電子メール メッセージをアプライアンス別に分類する方法

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。

- 感染フィルタの検疫
  (この場合、メッセージが検疫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、または検疫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 4-3　[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（「着信メッセージのカウント方法」（P.4-15）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 4-3　[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

Security Management アプライアンスの [Incoming Mail] > [Reporting] > [Incoming Mail] ページには、管理対象の Security Management 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。（脅威メッセージの総数およびクリーン メッセージの総数によって）上位送信者を集約するメール トレンド グラフと、[Incoming Mail Details] インタラクティブ テーブルの 2 つのメイン セクションで構成されます。

[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。

- Security Management 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。
- 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.4-30）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 評価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 Cisco SenderBase 評価スコア、ドメインが直近に一致した送信者グループなど IronPort SenderBase 評価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 Addresses
- Domains
- Network Owners

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

さらに、[Incoming Mail Details] ページの [Incoming Mail Details] セクションでは、[Senders 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.4-25）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、Email Security 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 4-4　[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（「着信メッセージのカウント方法」（P.4-15）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。

表 4-4　[Incoming Mail] 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	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、Security Management 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。

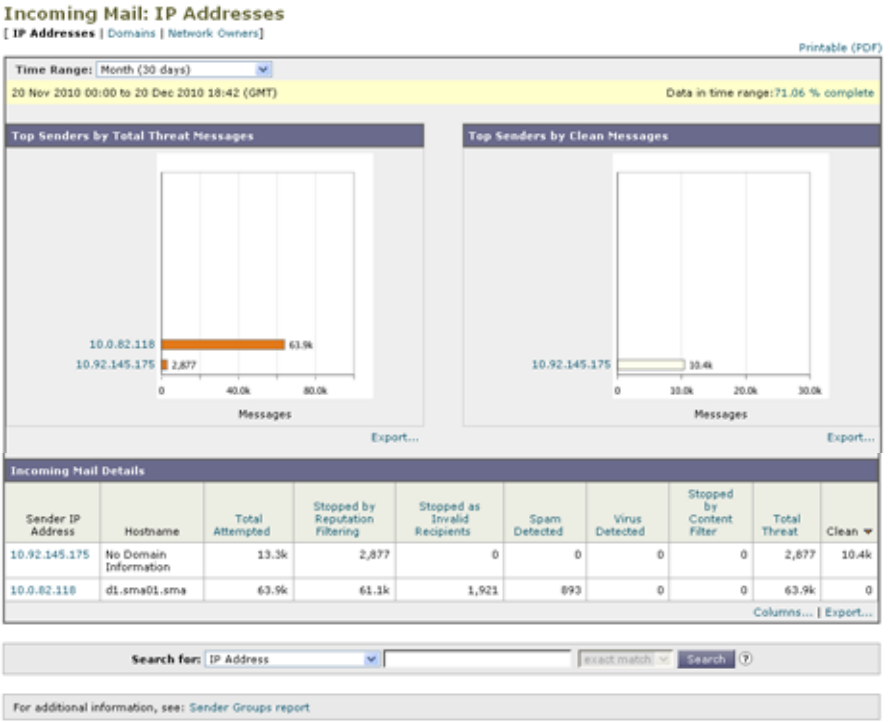
トップレベル ページ（この場合には [Incoming Mail] レポート ページ）の右上にある [Printable PDF] リンクをクリックすると、これらの各サブレポート ページの結果を、1 つの統合レポートに生成できます。「電子メール レポーティング ページの概要」（P.4-12）の重要な情報を参照してください。

[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　Security Management アプライアンスで、[Email] > [Reporting] > [Incoming Mail] を選択します。

[Incoming Mail Page] ページが表示されます。この例では、[IP Address] ビューが選択されています。

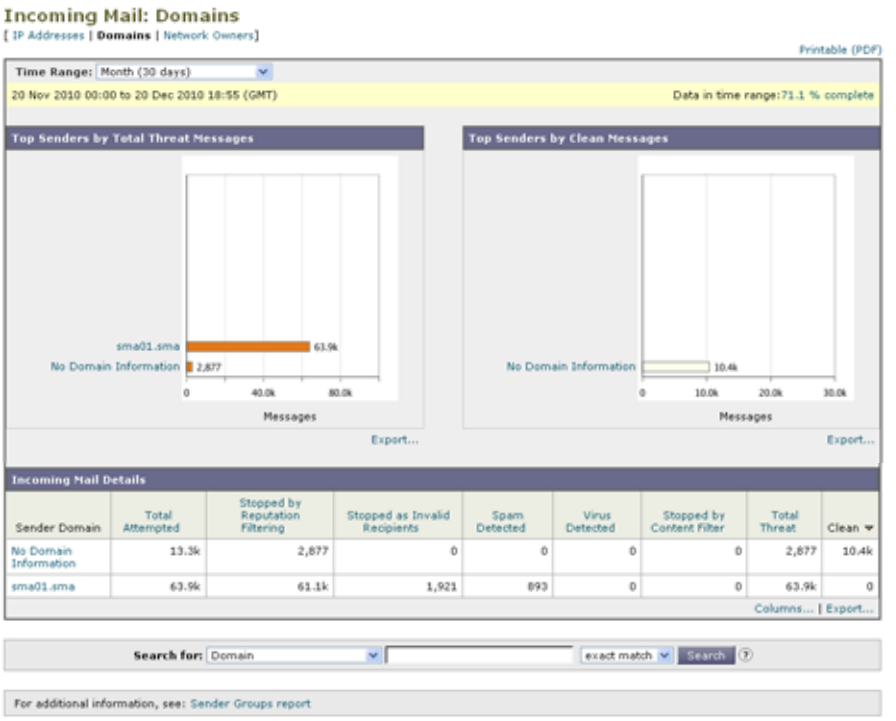
図 4-3　[Incoming Mail] ページ：[IP Address] ビュー



[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.4-24）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 4-4　[Incoming Mail] ページ：[Domain] ビュー



[Incoming Mail] ページから、印刷用の PDF を CSV ファイルに印刷またはエクスポート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.4-12）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。「スケジュール設定されたレポート」（P.4-76）を参照してください。

[No Domain Information] リンク

Security Management 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は、送信者の検証によって管理できます。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.3-18）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、Email Security 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。

*二重 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。二重 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 評価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.4-25）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.4-30）を参照してください。

[Sender Profile] ページ

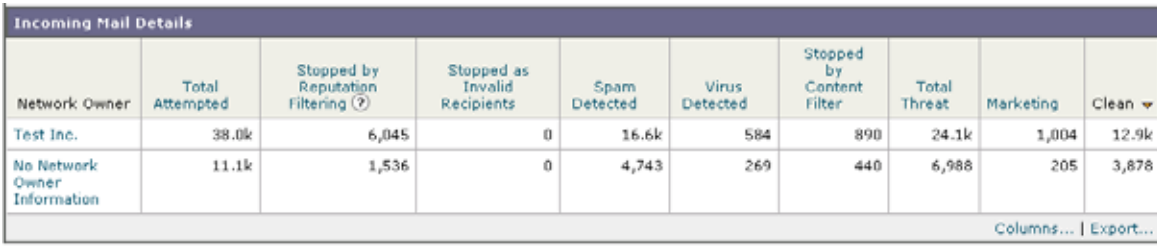
[Incoming Mail] ページで [Incoming Mail Details] インタラクティブ テーブルの送信者をクリックすると、[Sender Profile] ページが表示されます。ここには、特定の IP アドレス、ドメイン、またはネットワーク オーナー（組織）の詳細情報が表示されます。[Incoming Mail] ページまたは他の [Sender Profile] ページにある対応するリンクをクリックすると、IP アドレス、ドメイン、またはネットワーク オーナーの [Sender Profile] ページにアクセスできます。

*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 アドレスの送信者プロファイル 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 4-5　　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。

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

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

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

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

SenderBase 評価サービスによって提供されるすべての情報を示すページを表示するには、[More from SenderBase] をクリックします。

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

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

図 4-6　ネットワーク オーナーの現在の情報

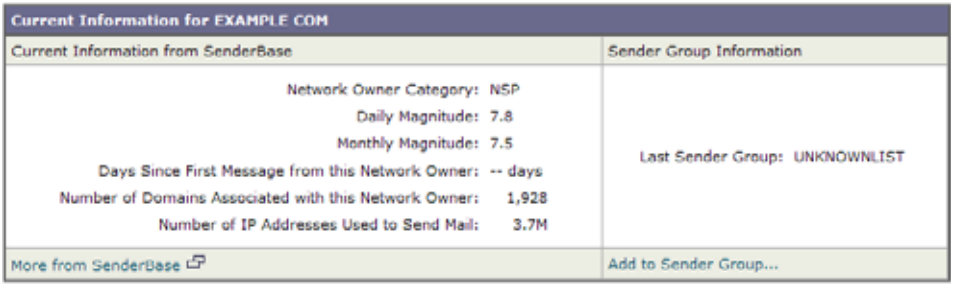


図 4-7　ドメイン プロファイル ページ

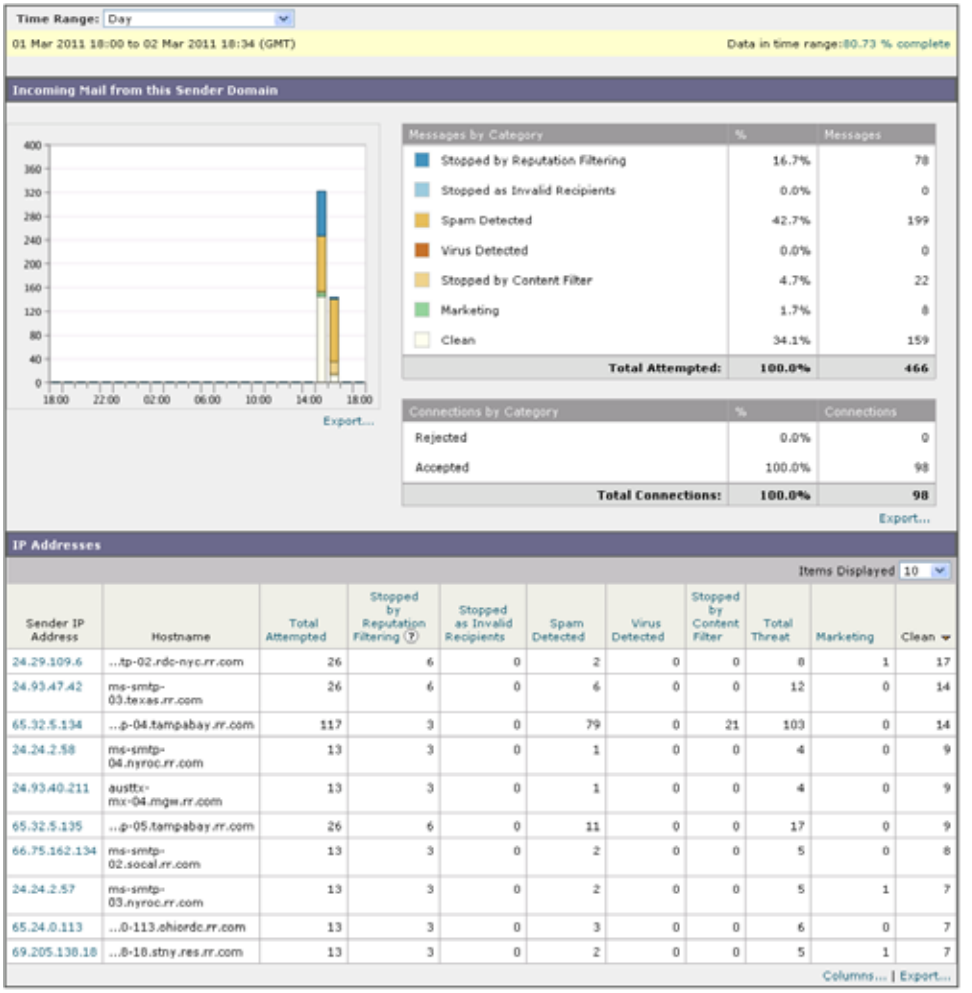


図 4-8　ネットワーク オーナー プロファイル ページ

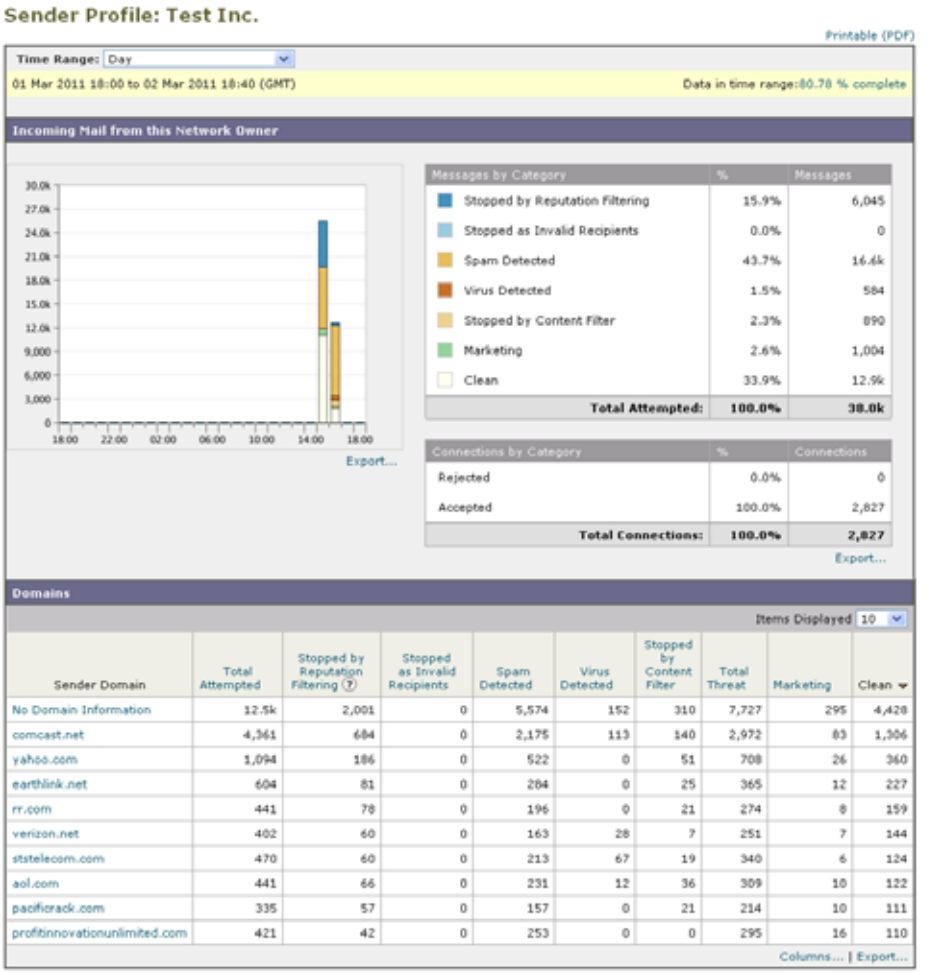
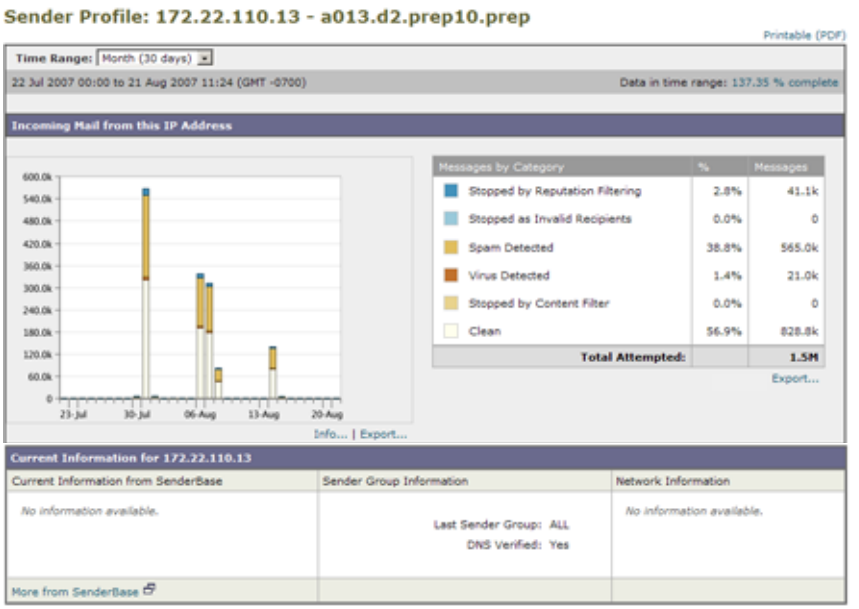


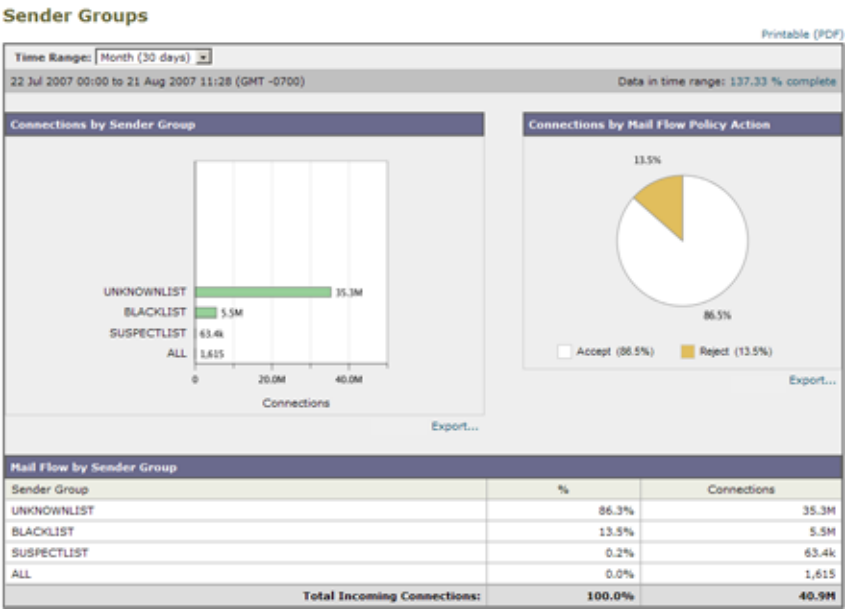
図 4-9　IP アドレス プロファイル ページ



[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。

図 4-10　[Sender Groups] レポート ページ



[Sender Groups] レポート ページから、印刷用の PDF を CSV ファイルに印刷またはエクスポート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.4-12）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。「スケジュール設定されたレポート」（P.4-76）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。

- Email Security 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。

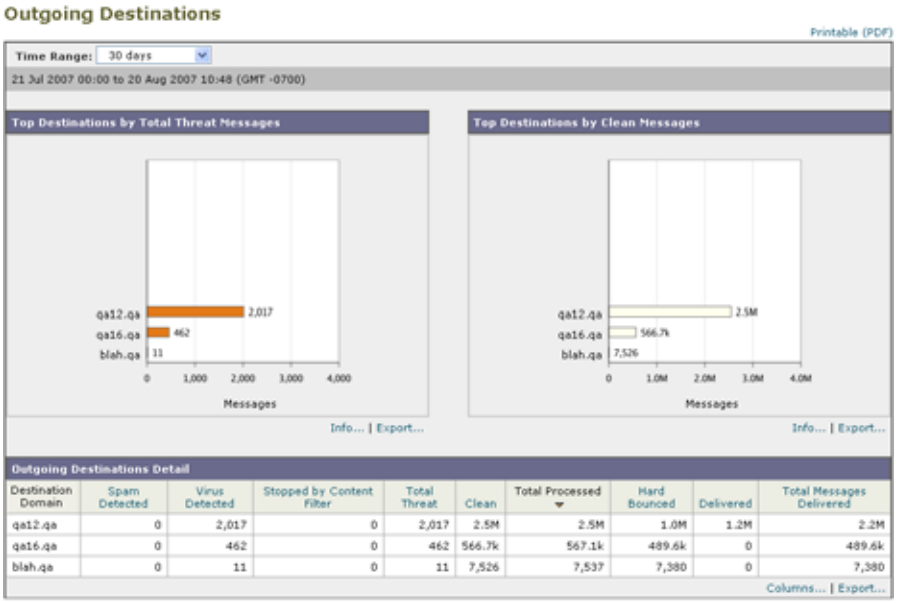
- クリーン、スパム陽性、またはコンテンツ フィルタによる阻止のメールの割合。
- 配信されたメッセージおよび宛先サーバによってハードバウンスされたメッセージの数。

[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　Security Management 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 4-11　[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 4-5　[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.3-18）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、印刷用の PDF を CSV ファイルに印刷またはエクスポート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.4-12）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。「スケジュール設定されたレポート」（P.4-76）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。

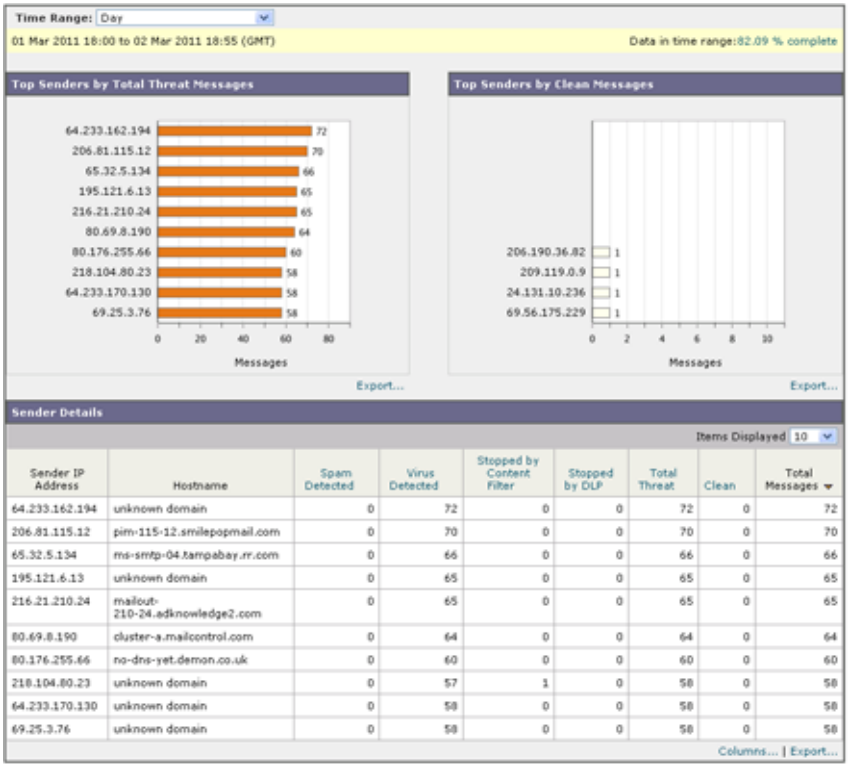
- 最も多くのメールを送信するドメイン
- 配信が試行された場所で処理された受信者の総数。

[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　Security Management 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 4-12　[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 4-6　[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.3-18）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 Email Security 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、印刷用の PDF を CSV ファイルに印刷またはエクスポート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.4-12）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。「スケジュール設定されたレポート」（P.4-76）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。

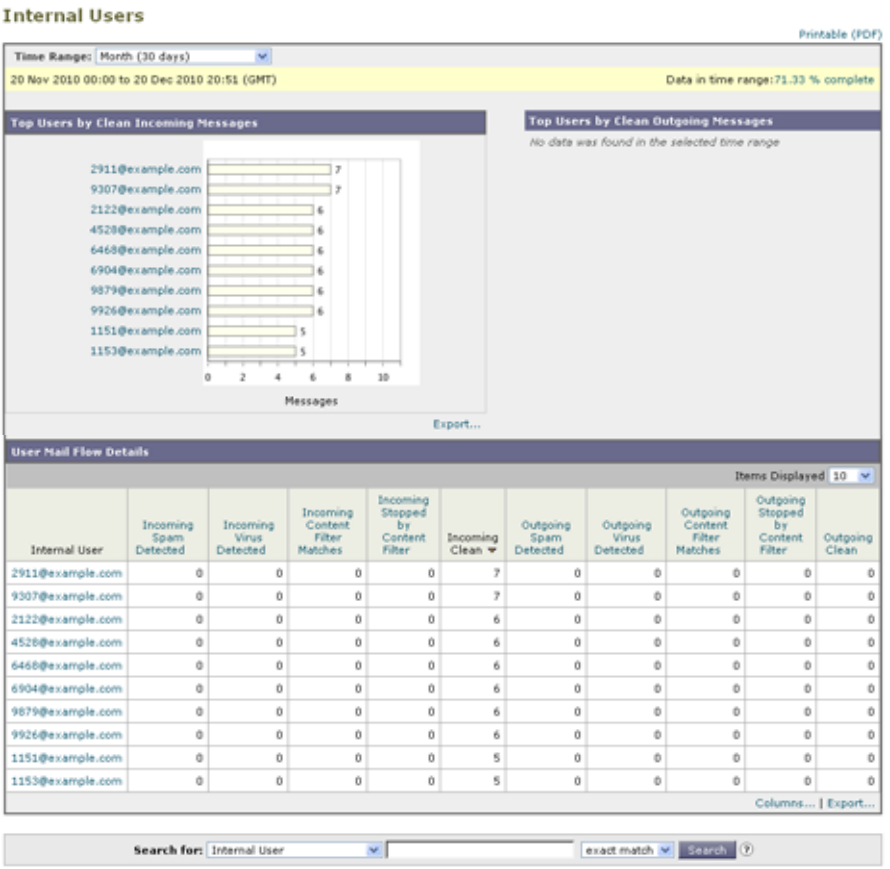
- 最も多くの外部メールを送信したユーザ。
- 最も多くのクリーン電子メールを受信したユーザ
- 最も多くのスパムを受信したユーザ
- 特定のコンテンツ フィルタをトリガーしたユーザ。
- 特定のユーザからの電子メールを阻止したコンテンツ フィルタ。

[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　Security Management 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 4-13　[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 4-7　[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.3-18）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）。
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.4-39）を参照してください。

[Internal Users] ページから、印刷用の PDF を CSV ファイルに印刷またはエクスポート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.4-12）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。「スケジュール設定されたレポート」（P.4-76）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。

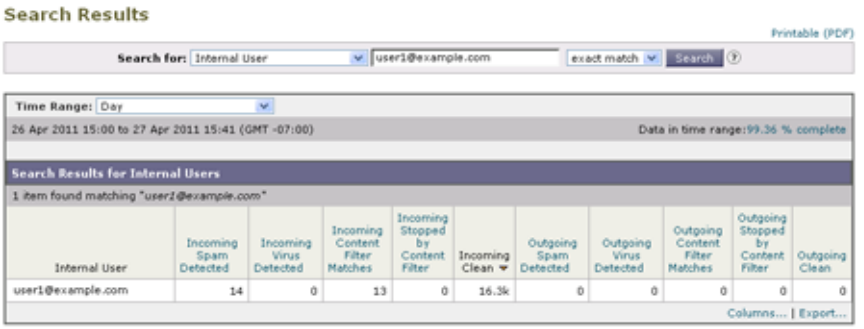
コンテンツ フィルタの詳細情報を対応するコンテンツ フィルタ情報ページに表示するには、そのコンテンツ フィルタ名をクリックします（「[Content Filters] ページ」（P.4-43）を参照）。この方法を使用すると、特定のコンテンツ フィルタに一致したメールを送受信したすべてのユーザのリストも表示できます。

（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 4-14　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。

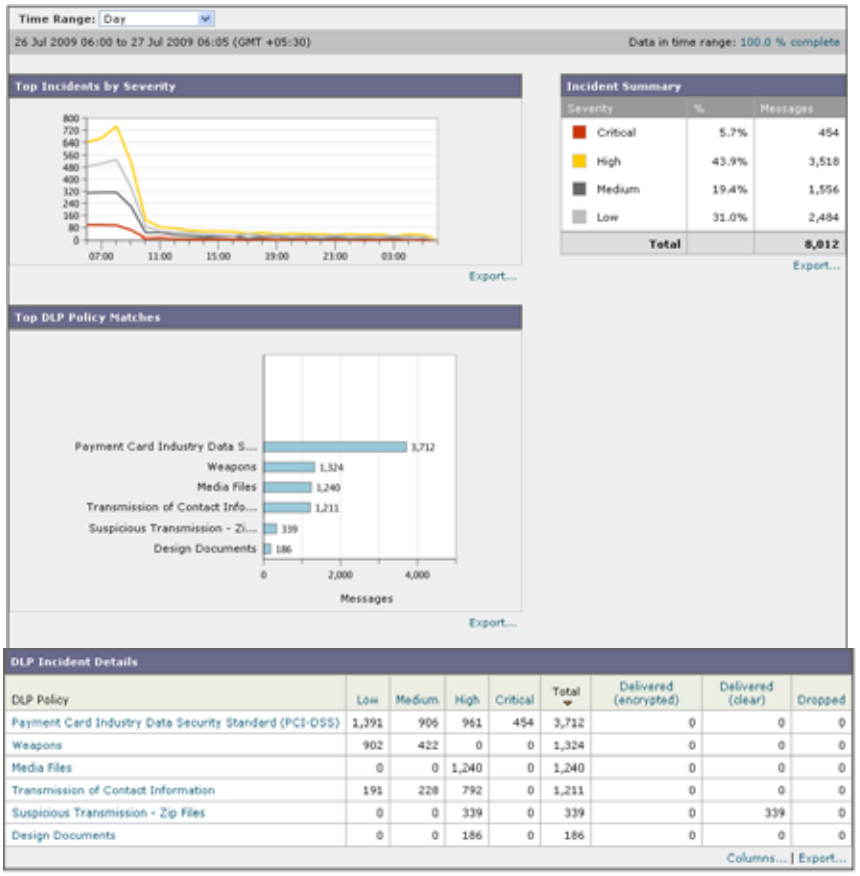
- ユーザが送信した機密データの種類
- これらの DLP インシデントの重大度
- これらのメッセージのうち、配信されたメッセージの数
- これらのメッセージのうち、ドロップされたメッセージの数
- これらのメッセージの送信者

[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　Security Management 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 4-15　[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 4-8　[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.3-18）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。
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.4-42）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.4-43）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.4-36）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。

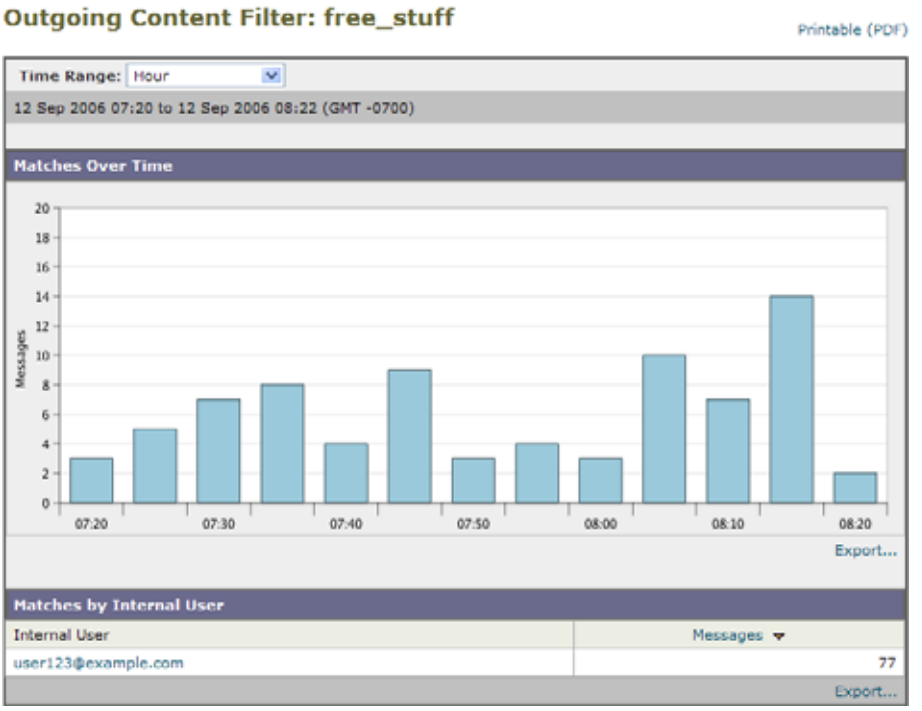
- 受信メールまたは送信メールによってトリガーされた回数の最も多いコンテンツ フィルタ。
- 特定のコンテンツ フィルタをトリガーしたメールを送受信した上位ユーザ。

[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　Security Management 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 4-16　[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.4-45）を参照してください。

[Content Filters] ページから、印刷用の PDF を CSV ファイルに印刷またはエクスポート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.4-12）を参照してください。

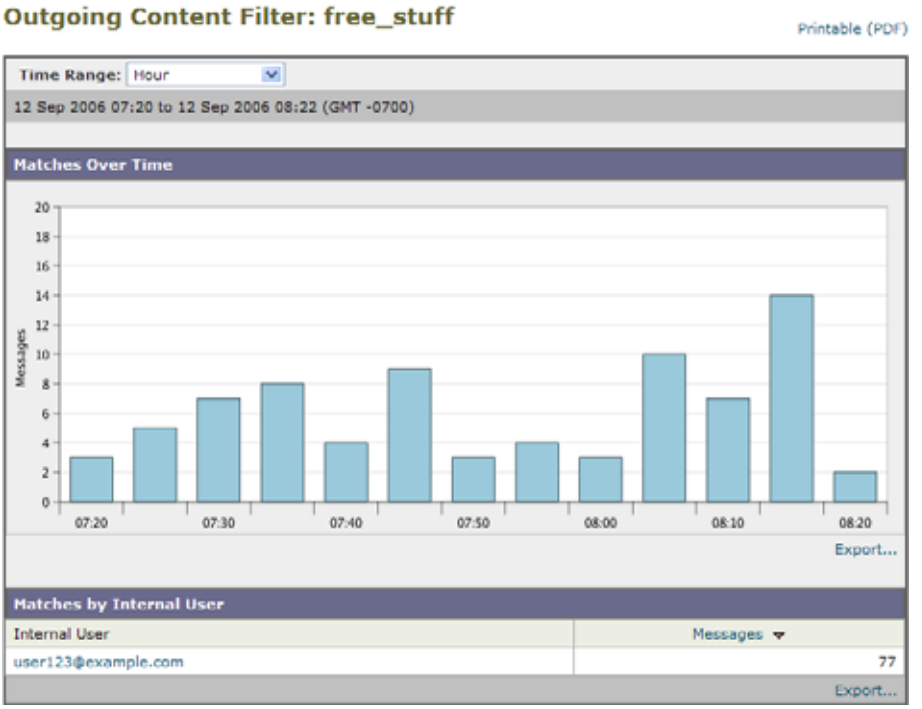
（注）　[Content Filter] ページのスケジュール設定されたレポートを生成できます。「スケジュール設定されたレポート」（P.4-76）を参照してください。

[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.4-39）を参照してください。

図 4-17　[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、Email Security アプライアンスで稼動し、Security Management 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検疫するフィルタ アクションを作成することが推奨されます。

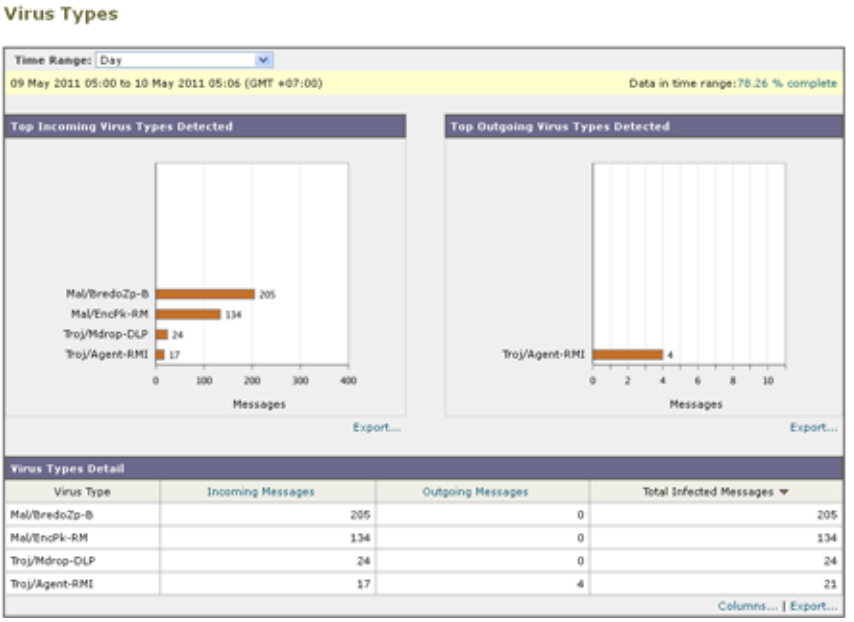
（注）　ウイルス感染フィルタでは、ユーザが介入することなく、これらの種類のウイルスに感染したメッセージを隔離することができます。

[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　Security Management 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 4-18　[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 4-9　[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.3-18）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、印刷用の PDF を CSV ファイルに印刷またはエクスポート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.4-12）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。「スケジュール設定されたレポート」（P.4-76）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　Security Management 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 4-19　[TLS Connections Report] ページ：[Incoming Connections]

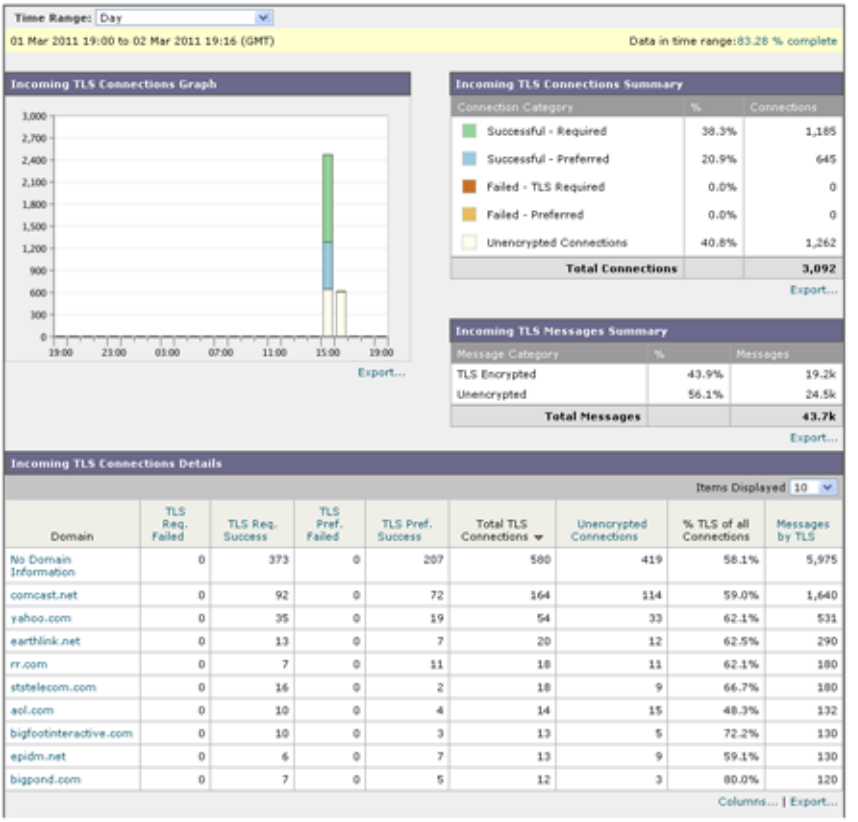
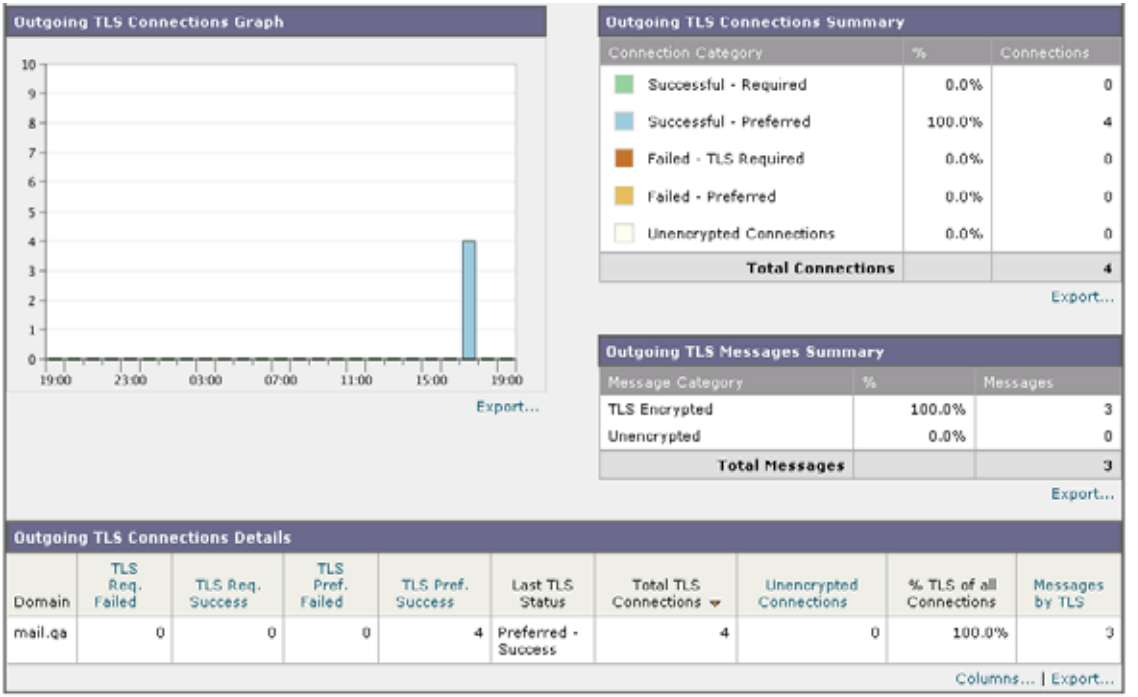


図 4-20　[TLS Connections Report] ページ : [Outgoing Connections]



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 4-10　[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.3-18）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。

表 4-10　[Email] > [Reporting] > [TLS Connections] ページの詳細（続き）

セクション	説明
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。
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。

[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検疫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 ルールによって検疫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、Outbreak 検疫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、Outbreak 検疫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、感染フィルタの検疫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。検疫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、メッセージが検疫エリア内にあるときでも、メッセージの検疫ルール（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。（検疫エリアに入った時点ではなく）解放時にメッセージを集計することにより、件数の変動による混乱を防ぎます。

[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

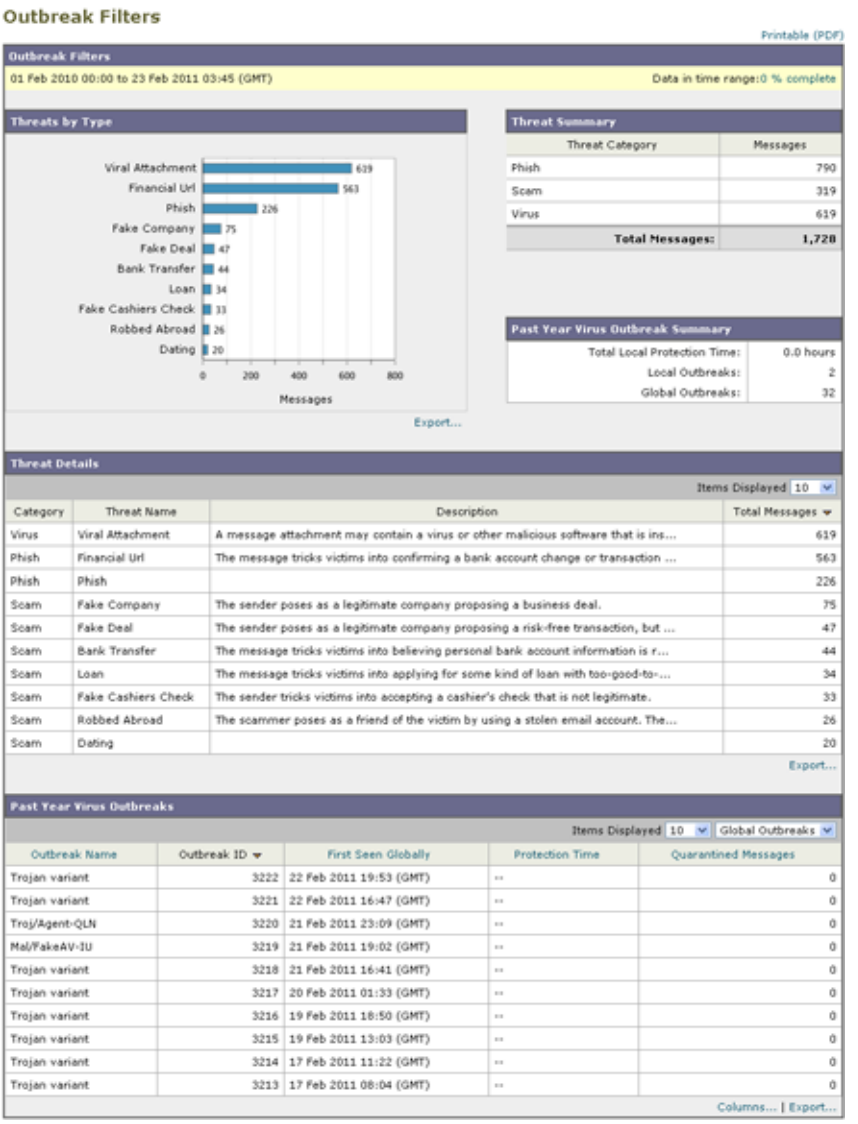
セージ数が含まれます。左側のメニューを使用して、グローバル発生またはローカル発生のいずれか、および表示するメッセージの数を選択できます。カラムヘッダーをクリックすることにより、表示をソートできます。

[First Seen Globally] の時間は、世界最大の電子メールおよび Web モニタリングネットワークである SenderBase のデータに基づいて、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、Security Management 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。

- Email Security 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 Email Security 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**：「通常」のメッセージ量と環境内での「異常」な増加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.4-57）および「[System Capacity] : [Outgoing Mail]」（P.4-60）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.4-56）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。

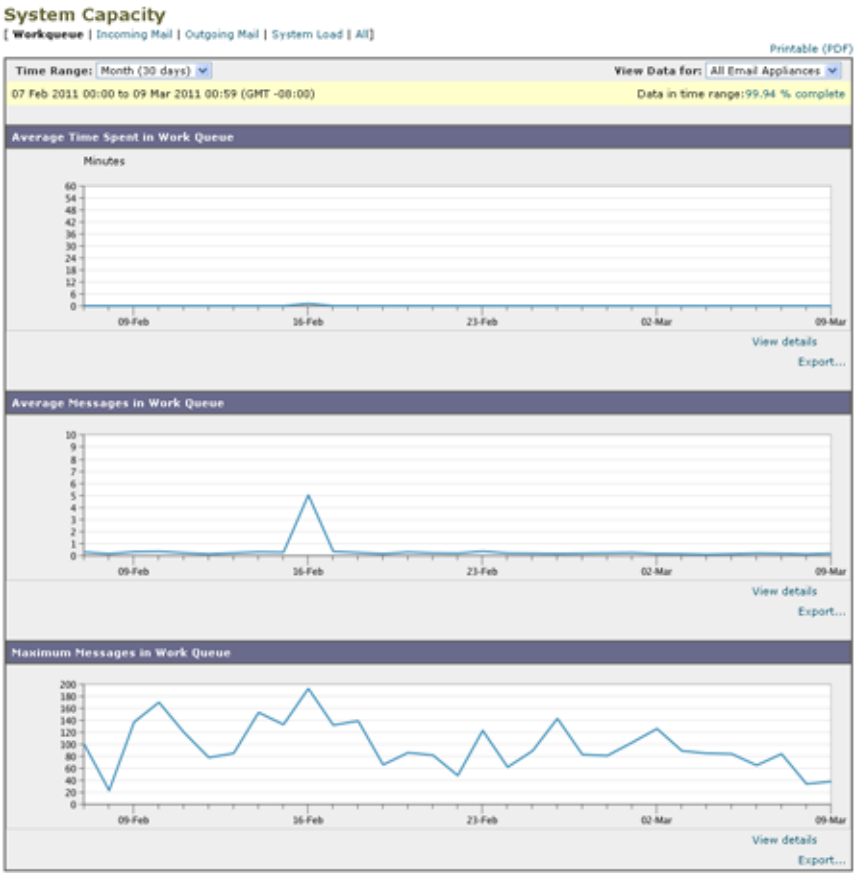
特定のグラフの [View Details] リンクをクリックすると、個々の電子メール セキュリティ アプライアンスのデータおよびセキュリティ管理アプライアンスに接続されたアプライアンスのデータ全体が表示されます。

[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]



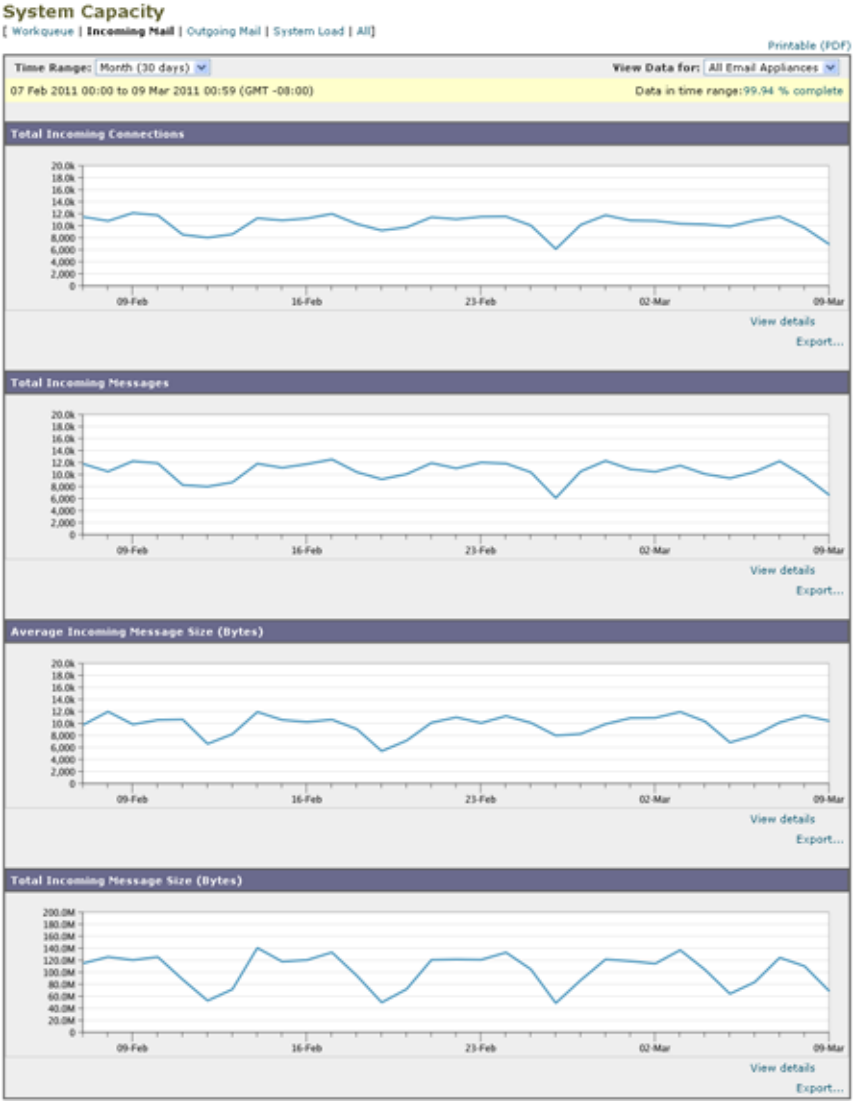
[System Capacity] : [Incoming Mail]

[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。

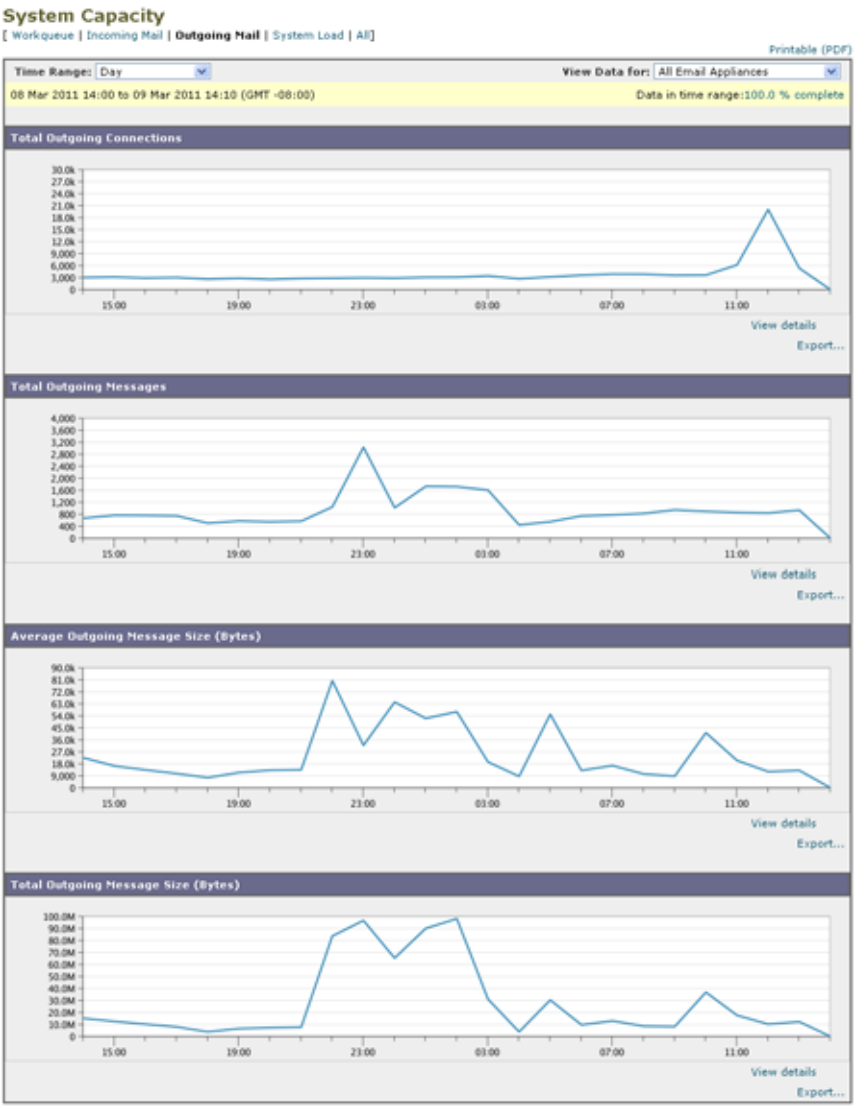
図 4-23　[System Capacity] : [Incoming Mail]



[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、Email Security 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、および検疫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。

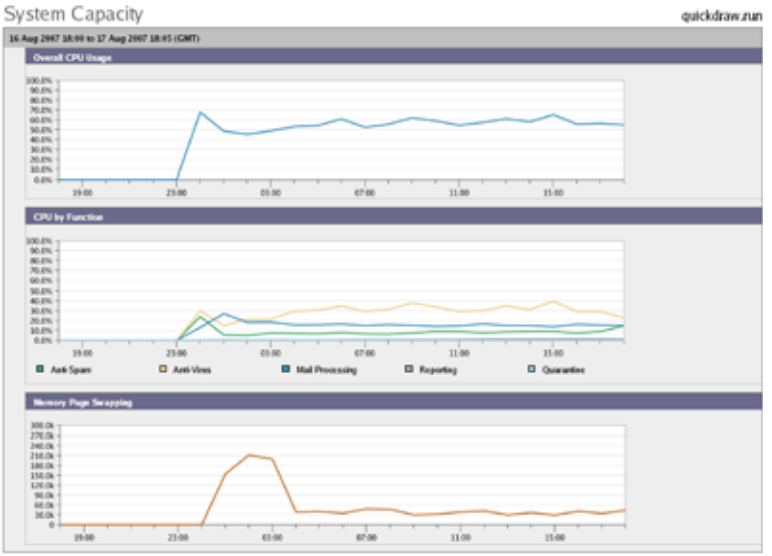
図 4-25　[System Capacity] : [System Load]

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。

[Data Availability] ページ

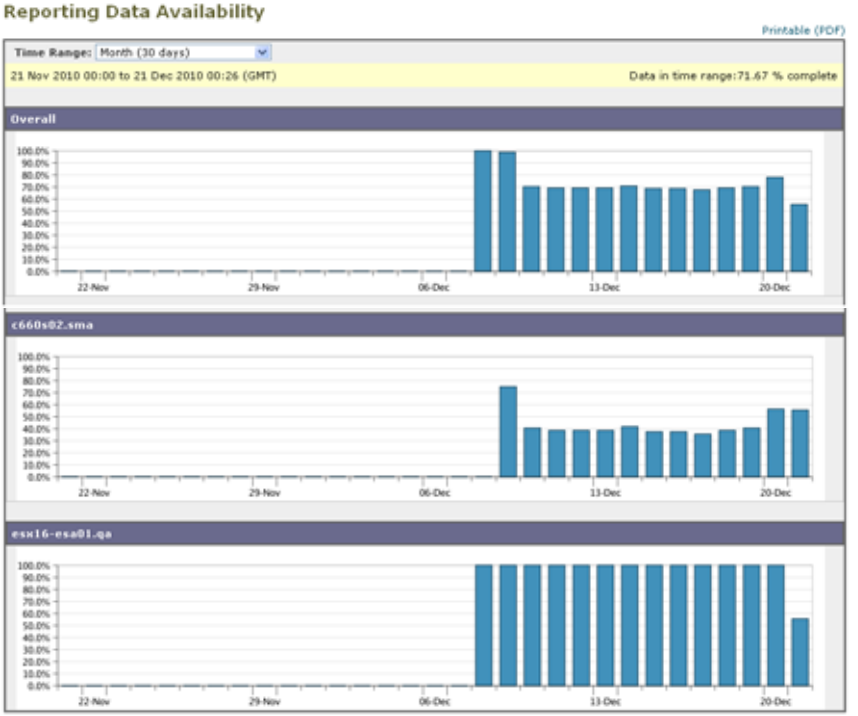
[Email] > [Reporting] > [Data Availability] ページでは、リソース使用率および電子メール トラフィックの障害のある場所がリアルタイムに表示されるようにデータを表示、更新およびソートできます。

[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　Security Management アプライアンスのページで、[Email] > [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、Security Management 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レポートとオンデマンド レポートについて

使用可能なレポートの種類

インタラクティブ レポート ページから使用できるレポートに加えて、次の種類のレポートを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.4-43）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.4-40）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。Email Security 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.4-68）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.4-68）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.4-17）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.4-36）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.4-51）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.4-31）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.4-33）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.4-33）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.4-30）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.4-55）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.4-48）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.4-45）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）　PDF レポートまたは CSV レポートを、その個々のレポートの特定のロケールでスケジュール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.3-21）の重要な情報を参照してください。

アーカイブ済みレポートの保存

レポートの保存期間や、アーカイブ済みレポートがいつシステムから削除されるかについては、「アーカイブ済みのレポート」（P.4-79）を参照してください。

その他のレポート タイプ

Security Management 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 Security Management 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 Email Security 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） Security Management 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、Email Security アプライアンスと Security Management 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。

Security Management 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、Email Security アプライアンスおよび Security Management 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、Email Security アプライアンスの CLI で **reportingconfig -> mailsetup -> tld** を実行し、Security Management 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　Security Management 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。

[Add Scheduled Report] ページが表示されます。

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。

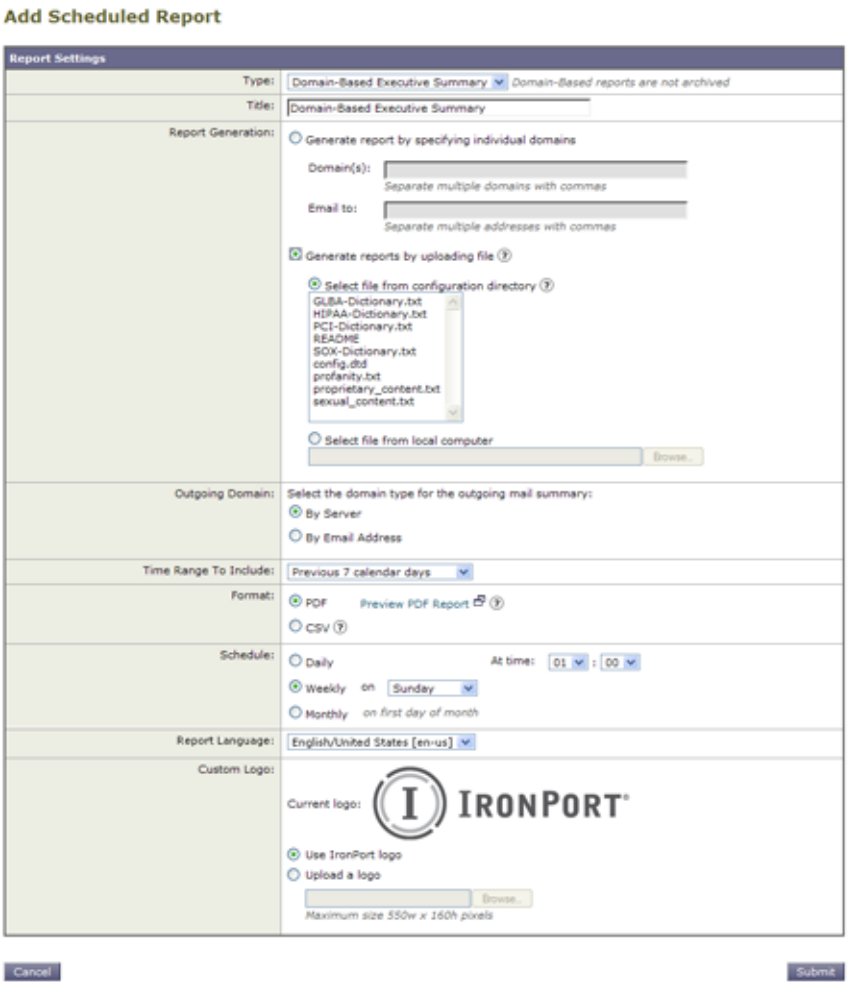
a. [Email] > [Reporting] > [Archived Reports] を選択します。

b. [Generate Report Now] をクリックします。

[Generate Report] ページが表示されます。

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.4-72）を参照してください。

（注） 外部アカウント（Yahoo! Mail や Gmail）にレポートを送信する場合、外部アカウントのホワイトリストにレポーティング返信アドレスを追加して、レポートの電子メールが誤ってスパムに分類されないようにすることが推奨されます。

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。

選択肢は次のとおりです。

- [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]。カンマ区切りの表データを含む 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 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.3-21）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での変更を送信し、[Commit Changes] をクリックして変更を確定します。

[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、Email Security 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。Security Management 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.4-12）を参照してください。

オンデマンドでのレポートの生成

「電子メール レポーティング ページの概要」（P.4-12）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レポートとオンデマンド レポートについて」（P.4-66）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 CSV ファイルをいつでも生成できます。

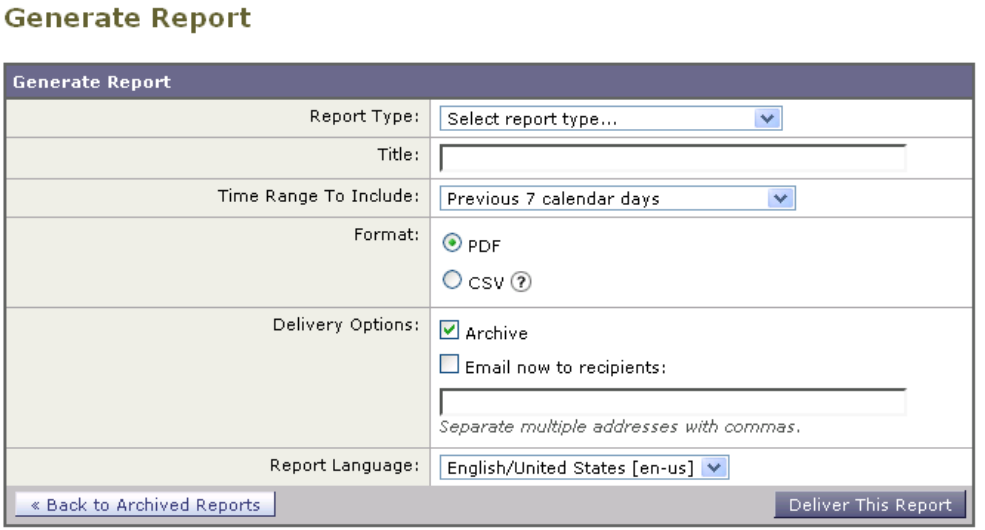
オンデマンド レポートを生成するには、次の手順を実行します。

ステップ 1　Security Management 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。

[Generate Report] ページが表示されます。

図 4-29　[Generate Report] ページ



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。

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レポートとオンデマンド レポートについて」（P.4-66）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.4-68）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。（ウイルス発生レポートでは、このオプションを使用できません）。

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。

選択肢は次のとおりです。

- [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]。カンマ区切りの表データを含む 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.3-21）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。

スケジュール設定されたレポート

「スケジュール設定されたレポートとオンデマンド レポートについて」（P.4-66）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.4-76）
- 「スケジュール設定されたレポートの編集」（P.4-78）
- 「スケジュール設定されたレポートの中止」（P.4-79）

スケジュール設定されたレポートの追加

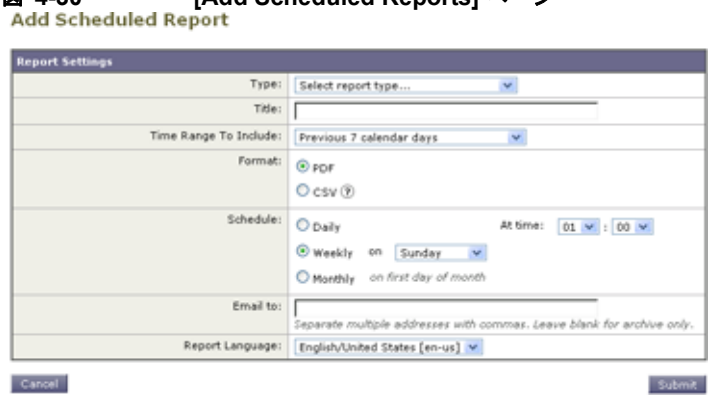
スケジュール設定された電子メール レポートを追加するには、次の手順を実行します。

ステップ 1　Security Management 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。

[Add Scheduled Report] ページが表示されます。

図 4-30　[Add Scheduled Reports] ページ



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。

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レポートとオンデマンド レポートについて」（P.4-66）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.4-68）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。（ウイルス発生レポートでは、このオプションを使用できません）。

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。大部分のレポートでは、CSV のスケジューリングを行うことができます。

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.3-21）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

スケジュール設定されたレポートを編集するには、次の手順を実行します。

ステップ 1　Security Management 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。

[Edit Scheduled Report] ページが表示されます。

ステップ 3　[Edit Scheduled Report] ページから、レポート設定を変更します。

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] 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　Security Management 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.4-81）を参照してください。

アーカイブ済みのレポート

（注）　[Generate Report Now] をクリックしてレポートをすぐに生成する方法の詳細については、「オンデマンドでのレポートの生成」（P.4-74）を参照してください。

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。

Security Management 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「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

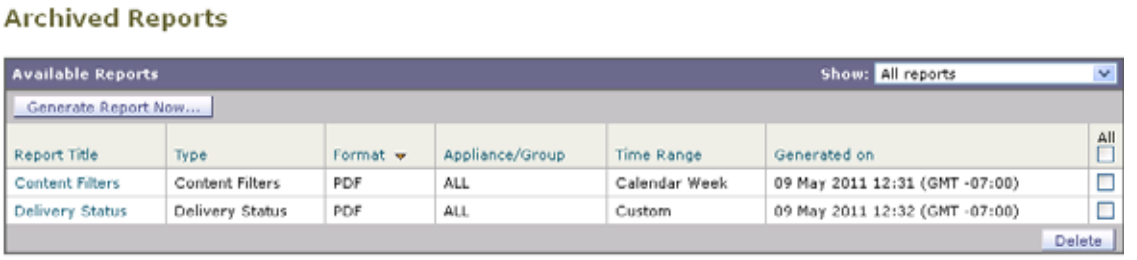
[Email] > [Reporting] > [Archived Reports] ページには、生成されたがまだ消去されておらず、アーカイブすることを指定した、スケジュール設定されたレポートとオンデマンド レポートが表示されます。

アーカイブ済みのレポートにアクセスするには、次の手順を実行します。

ステップ 1　Security Management アプライアンスのウィンドウで、[Email] > [Reporting] > [Archived Reports] を選択します。

[Archived Reports] ページが表示されます。

図 4-31　　アーカイブ済みのレポート



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

「アーカイブ済みのレポート」（P.4-79）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　Security Management 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.4-79）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

この章は、次の項で構成されています。

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集約してデータを記録し、それを Web トラフィック パターンとセキュリティ リスクのモニタに使用できます。リアルタイムに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、一定の間隔で実行するようにレポートのスケジュールを設定することもできます。レポーティング機能を使用すると、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では、管理者がネットワークの現状を把握できる概要レポートの収集だけではなく、ドリル ダウンして特定のドメイン、ユーザ、またはカテゴリのトラフィックの詳細を表示することもできます。

ドメイン情報

ドメインに対しては、ドメイン レポートに出力する次のデータ要素を、Web レポーティング機能で生成できます。たとえば、Facebook.com ドメインに関するレポートを生成する場合は、レポートに次のような情報が含まれます。

- 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

ユーザに対しては、ユーザ レポートに出力するデータ要素を、Web レポーティング機能で生成できます。たとえば、「Jamie」というタイトルのユーザ レポートでは、レポートに次のような情報が含まれます。

- 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だった上位 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、カテゴリ「Sports」に対して、レポートに次のような情報が含まれます。

- 「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。

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.13-2）を参照してください。

（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、この章で説明する Web トラッキング機能を使用します。

Web レポーティングを使用する前に

（注）　Web セキュリティ アプライアンスの Web レポーティングを表示するには、Web セキュリティ アプライアンスを追加して設定する必要があります。Web セキュリティ アプライアンスの追加については、「管理対象アプライアンスの追加」（P.3-11）を参照してください。また、これらのアプライアンスの設定については、『*Cisco IronPort AsyncOS 7.1 for Web User Guide*』を参照してください。

Security Management アプライアンスで Web レポーティング データを表示する方法はいくつかあります。Web レポーティングを開始するには、次の手順を使用します。

- Web レポーティングをイネーブルにするには、「中央集中型 Web レポーティングの設定」（P.5-3）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 ページを表示および管理するには、「Web レポーティング ページの概要」（P.5-12）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スケジュール設定されたレポートを作成するには、「レポートのスケジューリング」（P.5-83）を参照してください。
- 以前に実行したレポート（スケジュール設定されたレポートと [Generate Report Now] で生成したレポートの両方）のアーカイブ版を表示する方法については、「レポートのアーカイブ」（P.5-90）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

Security Management アプライアンスで Web レポーティングを使用するには、すべての Web レポーティングがイネーブルになるよう、Security Management アプライアンスを設定する必要があります。さらに、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。

中央集中型 Web レポーティングを設定するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Management Appliance] > [Centralized Services] > [Web] > [Centralized Reporting] を選択します。

[Centralized Web Reporting] ページが表示されます。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。

ステップ 2　[Edit Settings] をクリックします。

ステップ 3　[Edit Centralized Web Reporting Service Settings] ページが表示されます。

ステップ 4　[Enable Centralized Web Report Services] チェックボックスをクリックします。

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になっている場合、Web セキュリティ アプライアンスはシステム キャパシティとシステム ステータスを除いて、レポート データを保持しません。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。

ステップ 5　スケジュール設定されたレポートでユーザ名が認識できない状態でレポートを生成するには、[Anonymize usernames in reports] チェックボックスをオンにします。デフォルト設定では、スケジュール設定されたレポートにすべてのユーザ名が表示されます。

（注）　管理者ステータスを持っている場合は、常にユーザ名が表示されます。

ステップ 6　[Submit] をクリックして変更を送信し、[Commit Changes] をクリックしてアプライアンスでの変更を確定します。

（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.12-123）を参照してください。

[Web Reporting] タブの使用

[Web] > [Reporting] タブには、レポーティング データの複数の表示オプションが表示されます。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] タブ上のカテゴリの中で、スケジュール設定されたレポートを生成できるものについては、「レポートのスケジューリング」（P.5-83）を参照してください。

表 5-1　[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、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のグラフや要約テーブルが含まれます。詳細については、「Web レポーティングの [Overview] ページ」（P.5-12）を参照してください。
[Users] ページ	[Users] ページには、個々のユーザの Web トラッキング情報を表示するための Web トラッキング リンクがあります。 [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] 表に表示されている個々のユーザをクリックすると、そ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 [Users] 表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。このページから、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。 詳細については、「[Users] ページ」（P.5-16）を参照してください。システム内の特定のユーザについては、「[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を表示できます。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。

表 5-1　[Web Reporting] タブの詳細（続き）

[Web Reporting] メニュー	アクション
[URL Categories] ページ	[URL Categories] ページでは、サイト上でアクセスされている次のような上位 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。 このページでは、カスタム URL カテゴリの作成、編集、または削除を行うこともできます。詳細については、「[URL Categories] ページ」（P.5-28）を参照してください。
[Application Visibility] ページ	[Application Visibility] ページでは、Security Management 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.5-36）を参照してください。
セキュリティ	
[Anti-Malware] ページ	[Anti-Malware] ページでは、指定した時間範囲内にレイヤ 4 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。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.5-40）を参照してください。

表 5-1　[Web Reporting] タブの詳細（続き）

[Web Reporting] メニュー	アクション
[Client Malware Risk] ページ	[Client Malware Risk] ページは、クライアント マルウェア リスク アクティビティのモニタに使用できる、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。 詳細については、「[Client Malware Risk] ページ」（P.5-50）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.5-58）を参照してください。
[L4 Traffic Monitor Data] 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 Data] ページ」（P.5-64）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.5-67）を参照してください。
レポーティング	

表 5-1　[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、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）をトラッキングし、表示することができます。 これには、時間範囲やユーザ ID とクライアント IP アドレスなどの情報が含まれ、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。 詳細については、「[Web Tracking] ページ」（P.5-70）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 Security Management 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.5-76）を参照してください。
[Data Availability] ページ	各アプライアンスの Security Management 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.5-81）を参照してください。
レポートのスケジューリング	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、「レポートのスケジューリング」（P.5-83）を参照してください。
レポートのアーカイブ	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、「レポートのアーカイブ」（P.5-90）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、「レポートのスケジューリング」（P.5-83）を参照してください。

Web セキュリティ アプライアンス用のインタラクティブ レポート ページ

すべての Web レポーティング ページは、インタラクティブなレポート ページになっています。このため、システム内の 1 つまたはすべての管理対象 Web セキュリティ アプライアンスの情報をモニタできます。

インタラクティブ レポート ページでは、異なる時間範囲の中央集中型レポートを表示でき、ページごとに表示するカラムのタイプを指定できます。多くのレポート ページにはインタラクティブなカラムがあり、そのページでデータを表示する際に各カラムのデータをニーズに応じてソートできるように、これらのカラムを設定できます。レポート ページ上のインタラクティブなカラムの設定については、「レポート ページのカラムの設定」（P.5-10）を参照してください。

（注）　レポート ページによっては、一部のカラムを使用できないことがあります。特定のレポート ページで使用可能なカラムを確認するには、各レポート ページの [Column] リンクをクリックします。「中央集中型 Web レポーティング ページのインタラクティブ カラム」（P.E-1）に、このリリースのレポーティング ページで使用可能なカラムの説明があります。

また、カラムの内容が得られた [Web Tracking] ページへのリンクが、そのカラムに表示されることがあります。

レポーティング ページでの時間範囲の設定については、「インタラクティブ レポートの時間範囲の選択」（P.3-18）を参照してください。

レポート ページのカラムの設定

レポート ページのカラムを設定するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスのページで、[Web] > [Reporting] > [*Your_Web_Reporting_Page*] を選択します。

ステップ 2　[Columns] をクリックします。

表示するカラムを選択するためのポップアップ ウィンドウが表示されます。

ステップ 3　ポップアップ ウィンドウで、各カテゴリの横のチェックボックスをオンにします。
オプションを選択したら、[Done] をクリックします。これで、インタラクティブなカラム見出しを使用して、各カラムのデータをニーズに合わせてソートすることができます。

（注）　各レポート ページのいくつかのカラムには、Web トラッキングの詳細へのリンクが表示されます。

レポート ページからのレポートの印刷

ページ右上の [Printable PDF] リンクをクリックすると、すべてのレポート ページを読みやすい印刷形式の PDF 版で生成できます。[Export] リンクをクリックすると、グラフやその他のデータをカンマ区切り値（CSV）形式でエクスポートできます。大部分のレポートでは、CSV 形式のスケジューリングを行うことができます。ただし、CSV 形式で拡張レポートをスケジュールすることはできません。

レポート ページからの印刷の詳細については、「レポート データの印刷とエクスポート」（P.3-21）を参照してください。

各ページに表示される [Export] リンクは、raw データをエクスポートするために使用されます。

レポート ページのレポーティング フィルタ

AsyncOS には、前年をカバーするレポート（[Last Year] レポート）のデータの集約を制限できるレポート フィルタがあります。1 ヵ月分に大量の一意のエントリが存在することで、集約されたレポートのパフォーマンスが低下する場合には、これらのフィルタを使用できます。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。

レポーティング フィルタをイネーブルにする方法の詳細については、「Security Management アプライアンスのレポート フィルタ」（P.3-19）を参照してください。

Web レポーティング ページの概要

ここでは、Security Management アプライアンスで Web レポーティングに使用されるさまざまなレポート ページについて説明します。

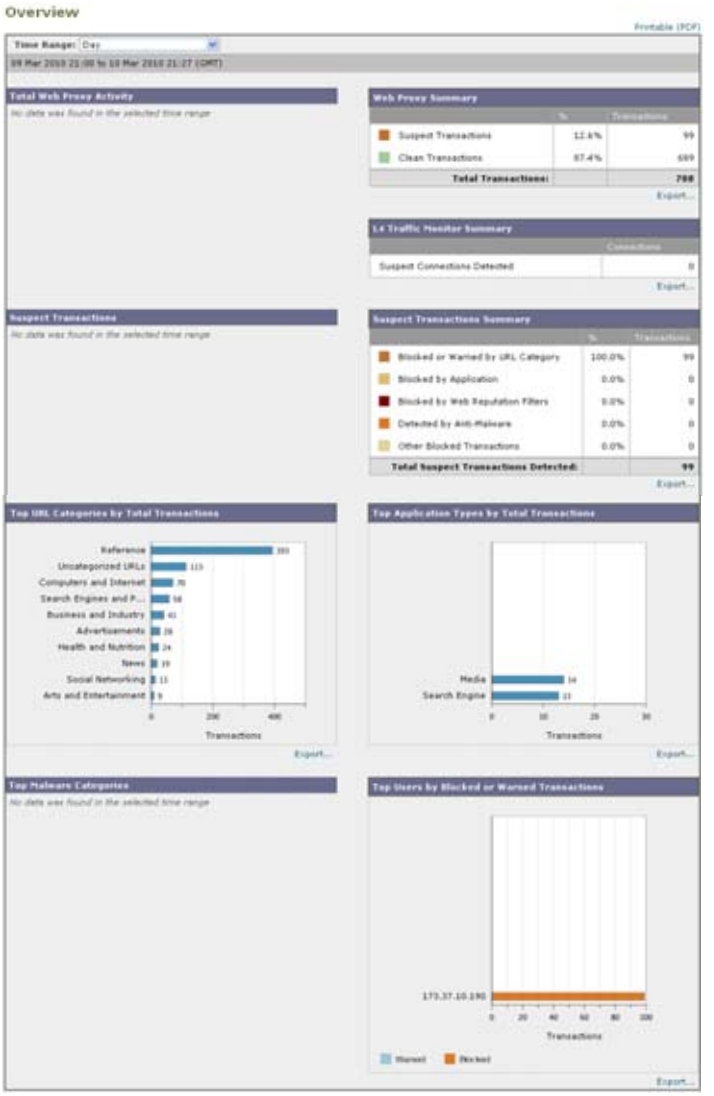
次の内容で構成されています。

Web レポーティングの [Overview] ページ

[Web] > [Reporting] > [Overview] ページには、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のグラフや要約テーブルが含まれます。

図 5-1 に、[Overview] ページを示します。

図 5-1　[Web] > [Reporting] > [Overview] ページ



[Overview] ページの上の部分には、URL とユーザの使用状況に関する統計、Web プロキシ アクティビティ、およびトランザクションに関するさまざまな要約が表示されます。トランザクションの要約には、たとえば疑わしいトランザク

ションに関する詳細なトレンドが表示され、このグラフの横に、ブロックされた疑わしいトランザクションの数およびどの方法でブロックされているかが示されます。

[Overview] ページの下半分には、使用状況に関する情報が表示されます。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 タイプとカテゴリ、およびこれらのブロックや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] ページのさまざまなセクションについて説明します。

表 5-2　[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.3-18）を参照してください。
Total Web Proxy Activity	このセクションでは、Security Management アプライアンスによって現在管理されている Web セキュリティ アプライアンスからレポートされる 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、または問題のないプロキシ アクティビティの比率を、トランザクションの総数とともに表示できます。
L4 Traffic Monitor Summary	このセクションには、Security Management アプライアンスによって現在管理されている Web セキュリティ アプライアンスから報告されるレイヤ 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。

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

セクション	説明
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。
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のアプリケーション タイプが表示されます。実際のアプリケーション タイプの名前（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）などがあります。
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、ブロックまたは警告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。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、「中央集中型 Web レポーティングの設定」（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。その方法の例については、「例 4：プライバシーおよびユーザ名の非表示」（P.D-12）を参照してください。

[Overview] ページから、印刷用の PDF を CSV ファイルに印刷またはエクスポート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、「レポート ページからのレポートの印刷」（P.5-11）を参照してください。

（注）　ユーザ向けに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リング」（P.5-83）を参照してください。

[Users] ページ

[Web] > [Reporting] > [Users] ページには、個々のユーザの Web レポーティング情報を表示するためのリンクが提供されています。

[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。

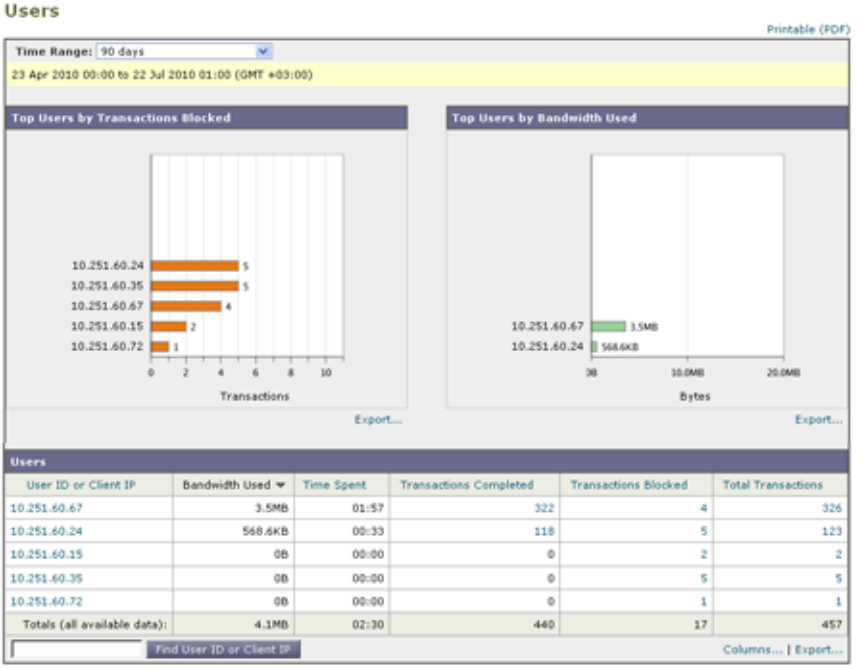
（注）　Security Management アプライアンスがサポートできる Web セキュリティ アプライアンス上の最大ユーザ数は 500 です。

[Users] 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　Security Management アプライアンスのウィンドウで、[Web] > [Reporting] > [Users] を選択します。

[Users] ページが表示されます。

図 5-2　[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 5-3　[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.3-18）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、「中央集中型 Web レポーティングの設定」（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。その方法の例については、「例 4：プライバシーおよびユーザ名の非表示」（P.D-12）を参照してください。

表 5-3　[Web] > [Reporting] > [Users] ページの詳細（続き）

セクション	説明
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	[Users] テーブルはインタラクティブなテーブルになっていて、ユーザ情報を無数の方法でソートし、テーブルを表示するたびにルックアンドフィールを変えることができます。各カラムの情報は、カラム見出しをクリックすることで昇順または降順にソートできます。 このテーブルに表示されるカラムはカスタマイズ可能です。[Users] テーブルのカラムの設定については、「Web セキュリティ アプライアンス用のインタラクティブ レポート ページ」（P.5-10）を参照してください。 インタラクティブな [Users] テーブルに表示するカラム カテゴリを選択した後に、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、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） **このページでユーザを追加または削除することはできません。**

ユーザの追加または削除の詳細については、「GUI でのユーザ管理」（P.12-59）を参照してください。ユーザ ロール自体の詳細については、「ユーザ ロール」（P.12-43）および表 12-2（P.12-44）を参照してください。ユーザ ロールのカスタマイズについては、「Custom Web User ロールの作成」（P.12-56）を参照してください。

（注）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。
Security Management アプライアンスで LDAP 認証を設定するには、[Management Appliance] > [System Administration] > [LDAP] > [Add LDAP Server Profile] を選択します。[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。これで、[Users] ページと [User Details] ページにユーザ名が表示されるようになります。

[Users] ページから、印刷用の PDF を CSV ファイルに印刷またはエクスポート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、「レポート ページからのレポートの印刷」（P.5-11）を参照してください。ユーザ向けにスケジュール設定された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リング」（P.5-83）を参照してください。

（注）このページのスケジュール設定されたレポート内で、ユーザ情報を認識できないようにすることができます。ユーザ情報を認識不可能にする方法については、「Security Management 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とディセーブル化」（P.3-5）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-2）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 5-3　[User Details] ページ

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

表 5-4　[Web] > [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）	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.3-18）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。
Trend by Total Transaction	このグラフには、特定のユーザの Web トランザクションの経時的なトレンドが示されます。基本的には、この特定のユーザがその Web にいつアクセスしたか、および閲覧トラフィックを送信した回数が示されます。 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関して、指定した時間範囲内の一致したすべてのカテゴリが表示されます。インタラクティブなカラム見出しを使用するとデータをソートできます。また、[Items Displayed] メニューによって、リストに表示される URL カテゴリの数を変更できます。 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。

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

セクション	説明
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。
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。セクション下部のテキスト フィールドにマルウェア脅威の名前を入力し、[Find Malware Threat] をクリックします。マルウェア脅威の名前は正確に一致している必要はありません。
Policies Matched	このセクションでは、この特定のユーザに適用されている特定のポリシーを検索できます。 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。

[User Details] ページのいくつかのセクションでは、表示するカラムを設定できます。カラムの設定については、「Web セキュリティ アプライアンス用のインタラクティブ レポート ページ」（P.5-10）を参照してください。

インタラクティブなセクションに表示するカテゴリを選択後、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。

[Users Details] ページの使用例については、「例 1：ユーザの調査」（P.D-2）を参照してください。

[Web Sites] ページ

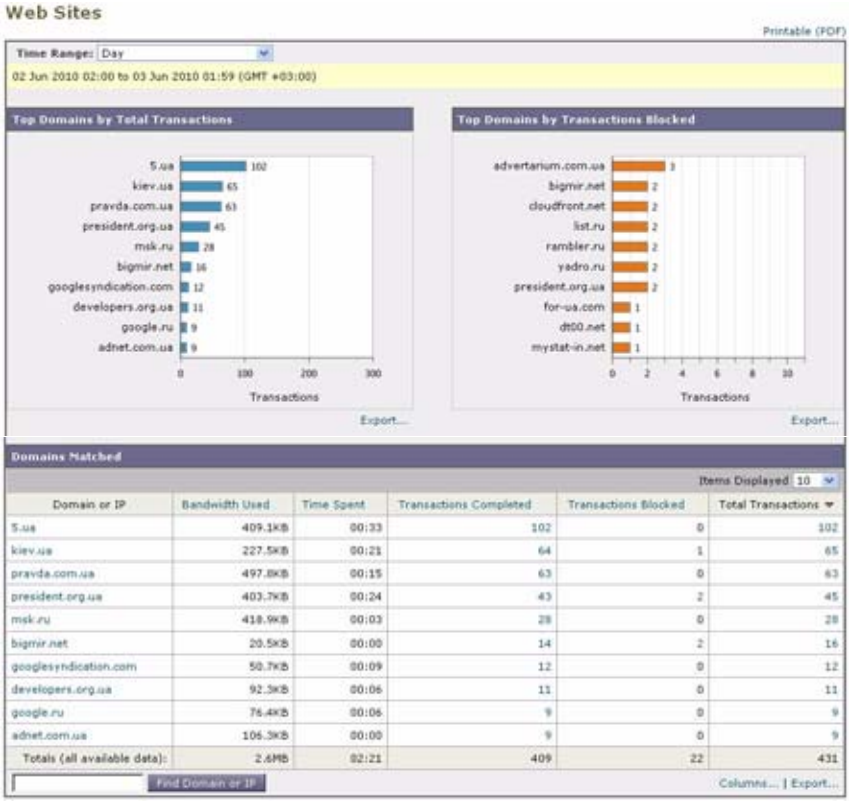
[Web] > [Reporting] > [Web Sites] ページでは、管理対象のアプライアンスで発生しているアクティビティ全体を集約したものです。このページでは、特定の時間範囲内にアクセスされたリスクの高い Web サイトをモニタできます。

[Web Site] 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　Security Management アプライアンスのウィンドウで、[Web] > [Reporting] > [Web Sites] を選択します。

[Web Sites] ページが表示されます。

図 5-4　[Web Sites] ページ



[Web Sites] ページには次の情報が表示されます。

表 5-5　[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.3-18）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 5-5　[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] ページが表示され、トラッキング情報および特定のドメインがブロックされた原因を確認できます。 [Domains Matched] セクションに表示するカラムを設定することができます。このセクションのカラムの設定については、「Web セキュリティ アプライアンス用のインタラクティブ レポート ページ」（P.5-10）を参照してください。 [Domains Matched] テーブルに表示するカテゴリを選択後、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。 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。[Time Range] ドロップダウン リストを使用して、特定の時間範囲（時間、日、または週）でドメインの使用状況が表示されるようにこのテーブルを変更できます。 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-7）を参照してください。

[Web Sites] ページから、[Top Domains by Total Transaction] および [Domains Matched] の情報を印刷したり、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、「レポート ページからのレポートの印刷」（P.5-11）を参照してください。

（注）　[Web Sites] 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、「レポートのスケジューリング」（P.5-83）を参照してください。

[URL Categories] ページ

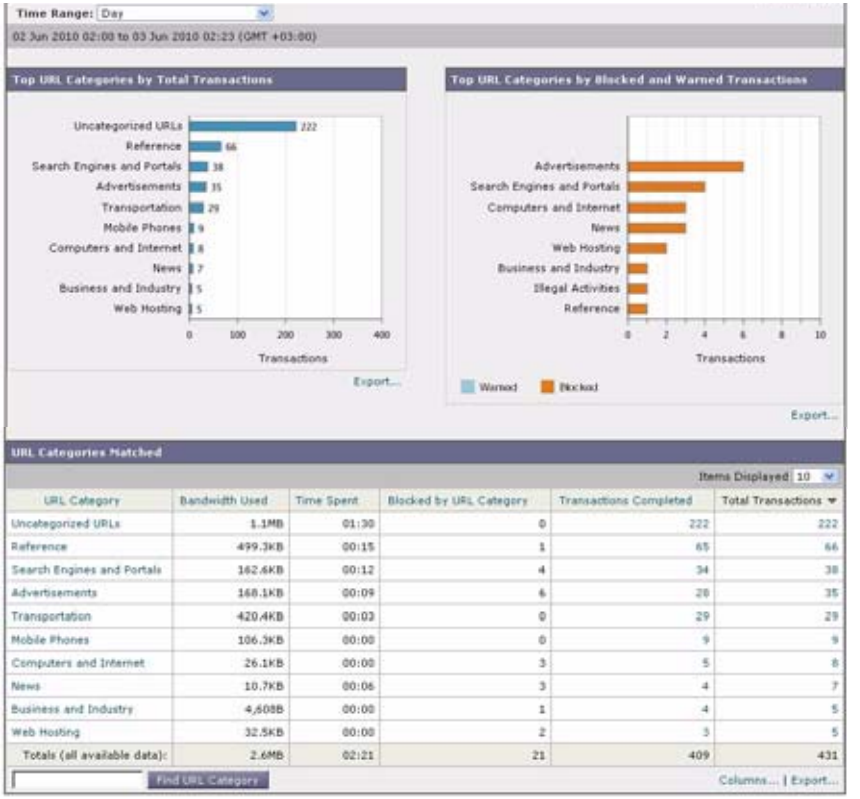
[Web] > [Reporting] > [URL Categories] ページでは、システム上のユーザがアクセスしている URL カテゴリを表示できます。

[URL Categories] 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　Security Management アプライアンスのウィンドウで、[Web] > [Reporting] > [URL Categories] を選択します。

[URL Categories] ページが表示されます。

図 5-5　[URL Categories] ページ



[URL Categories] ページには次の情報が表示されます。

表 5-6　[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）	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.3-18）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 5-6　[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、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。[Items Displayed] メニューから、リストに表示する URL カテゴリの数を変更できます。 [URL Categories] セクションに表示するカラムを設定することができます。このセクションのカラムの設定については、「Web セキュリティ アプライアンス用のインタラクティブ レポート ページ」（P.5-10）を参照してください。 [URL Categories Matched] 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、[URL Category] セクション内で特定の URL カテゴリを検索できます。セクション下部のテキスト フィールドに特定の URL カテゴリ名を入力し、[Find URL Category] をクリックします。 [URL Categories] ページでの未分類の URL の比率は、通常 15 ～ 20% 程度です。未分類の URL の比率がこれを上回る場合は、次のオプションを検討してください。 • 特定のローカライズされた URL の場合は、カスタム URL カテゴリを作成し、特定のユーザまたはグループ ポリシーに適用できます。詳細については、「カスタム URL カテゴリ」（P.5-33）を参照してください。

[URL Categories] ページから、ページの各セクションを印刷したり、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、「レポート ページからのレポートの印刷」（P.5-11）を参照してください。

（注）　[URL Categories] 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、「レポートのスケジューリング」（P.5-83）を参照してください。さらに、URL カテゴリに関してより詳細なレポートを生成できます。「Top URL Categories — Extended」（P.5-87）および「Top Application Types — Extended」（P.5-88）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。欠落が存在しない場合は何も表示されません。

[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] ページの利点の 1 つは、[Application Visibility] ページおよび [Users] ページと組み合わせて使用して、特定のユーザだけでなく、特定のユーザがアクセスを試みているアプリケーションまたは Web サイトのタイプも調査できることです。

たとえば、[URL 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。同じページのインタラクティブな [URL Categories] 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、特定のユーザの使用状況が目立っているので、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関する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：アクセスの多い URL カテゴリの調査」（P.D-8）を参照してください。

カスタム URL カテゴリ

Security Management アプライアンスでは、Web セキュリティ アプライアンスと同様に、多数の定義済み URL カテゴリ（Web-based Reporting など）がデフォルトで用意されています。ただし、特定のホスト名と IP アドレスを指定する、ユーザ定義のカスタム URL カテゴリを作成することもできます。内部サイトや確実に信頼できる外部サイトのグループには、カスタム URL カテゴリを作成することを推奨します。

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

複数のカスタム URL カテゴリを作成し、各カテゴリに同じ URL を含めることができます。カスタム URL カテゴリの順序は重要です。リストの上位にあるカテゴリが、下位にあるカテゴリよりも優先されます。これらのカスタム URL カテゴリを同じアクセス ポリシー グループ、復号化ポリシー グループ、または Cisco IronPort Data Security ポリシー グループに入れ、各カテゴリに異なるアクションを定義した場合は、より上位にあるカスタム URL カテゴリのアクションが有効となります。

カスタム URL カテゴリを作成、編集、または削除するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスのウィンドウで、[Web] > [Configuration Master 7.1] > [Custom URL Categories] を選択します。

[Custom URL Categories] ページが表示されます。

既存のカスタム URL カテゴリを編集するには、URL カテゴリの名前をクリックします。カスタム URL カテゴリを削除するには、削除するカスタム URL カテゴリの横にあるごみ箱をクリックします。

図 5-6　[Custom URL Categories] ページ

ステップ 2　カスタム URL カテゴリを作成または編集するには、[Add Custom Category] をクリックします。

[Create Custom URL Categories: Add Category] ページが表示されます。

図 5-7　カスタム URL カテゴリの作成

ステップ 3　カスタム URL カテゴリを作成または編集するには、次の設定を該当するフィールドに入力します。

- [Category Name] : URL カテゴリの名前を入力します。この名前は、ポリシー グループに URL フィルタリングを設定するときに表示されます。
- [List Order] : カスタム URL カテゴリのリストにおけるこのカテゴリの順序をテキスト フィールドに入力します。最上位の URL カテゴリには、**1** を入力します。URL フィルタリング エンジンでは、指定した順序でカスタム URL カテゴリに対してクライアント要求が評価されます。
- [Sites] : カスタム カテゴリに属する 1 つまたは複数のアドレスを入力します。

  複数のアドレスは、改行またはカンマで区切って入力します。アドレスは次のいずれかの形式を使用して入力できます。

  - IP アドレス。10.1.1.0 など
  - CIDR アドレス。10.1.1.0/24 など
  - ドメイン名。example.com など
  - ホスト名。crm.example.com など
  - ホスト名の一部。.example.com など

（注） .example.com などのホスト名の一部を入力すると、www.example.com も一致します。

- [Advanced] : [Regular Expressions] テキスト フィールドに、入力したパターンと一致する複数の Web サーバを指定するための正規表現を入力できます。

（注） URL フィルタリング エンジンでは、URL がまず [Sites] フィールドに入力したアドレスと比較されます。トランザクションの URL が [Sites] フィールドの入力内容と一致した場合は、ここで入力した式との比較は行われません。

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

[Sort URLs] をクリックすると、サイト URL が英数字順にソートされます。リスト順序でサイトに対して入力した元の順序は、ソートすると無効になります。

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] をクリックしてアプライアンスへの変更を確定します。

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 は、次の URL の Cisco IronPort サポート ポータルに報告できます。

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

報告内容は、今後のルール アップデート用に評価されます。

Web レピュテーション フィルタリングと、アンチマルウェア フィルタリングがイネーブルになっていることを確認してください。

多くの場合、疑わしいコンテンツを含む URL とマルウェアの相関性は高く、今後のフィルタで検出される可能性が高くなります。URL フィルタリングで判定できない場合は、他のダウンストリーム フィルタで悪質なトラフィックが検出されるように、システム パイプラインが設定されます。この機能の詳細については、『*Cisco IronPort AsyncOS for Web User Guide*』を参照してください。

[Application Visibility] ページ

（注）　Application Visibility の詳細については、『*Cisco IronPort AsyncOS for Web 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、Security Management 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。

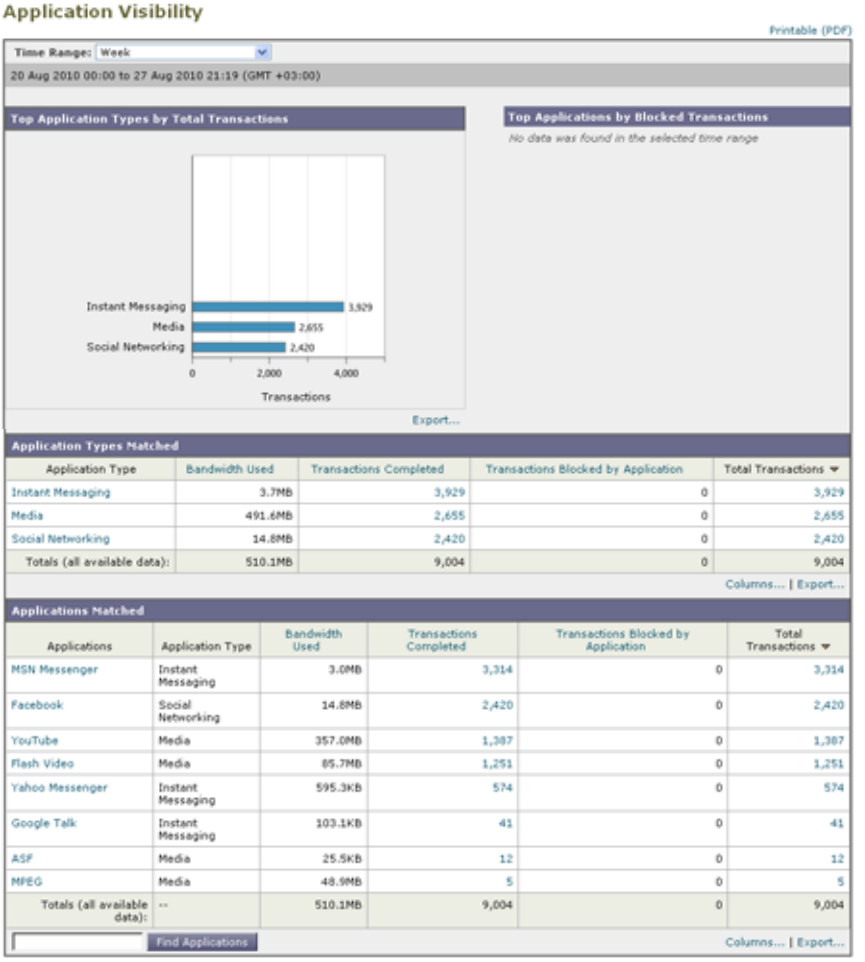
（注） Application Visibility and Control（AVC）エンジンを使用して Facebook アクティビティを制御する方法の詳細については、『*Cisco IronPort AsyncOS for Web User Guide*』の「Understanding Application Visibility and Control」を参照してください。

[Application Visibility] 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　Security Management アプライアンスのウィンドウで、[Web] > [Reporting] > [Application Visibility] を選択します。

[Application Visibility] ページが表示されます。

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 5-7　[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.3-18）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。

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

セクション	説明
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、「Web セキュリティ アプライアンス用のインタラクティブ レポート ページ」（P.5-10）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。

（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、「レポートのスケジューリング」（P.5-83）を参照してください。

[Anti-Malware] ページ

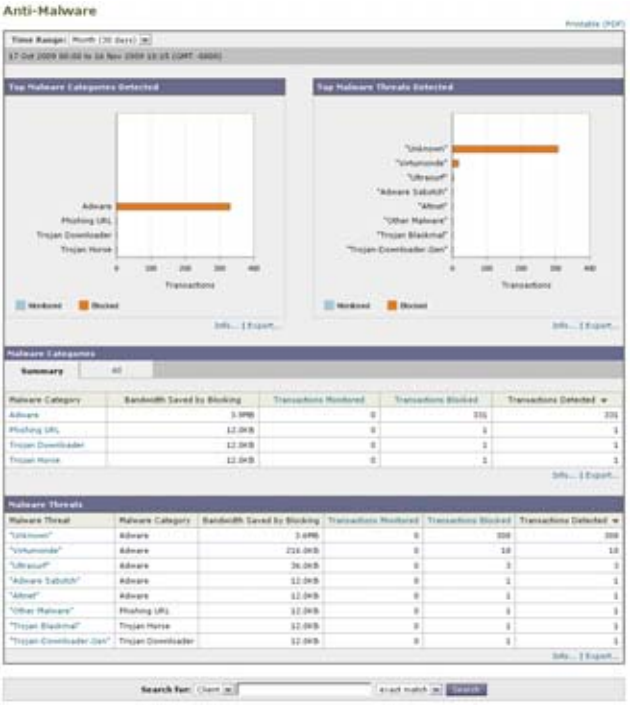
[Web] > [Reporting] > [Anti-Malware] ページは、特に DVS エンジン（WebRoot、Sophos、McAfee など）に基づいた、セキュリティ関連のレポーティング ページです。このページでは、さまざまな Web ベースのマルウェア脅威を識別および停止でき、検出されたマルウェアをモニタできます。

[Anti-Malware] 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　Security Management 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。

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 5-8　[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.3-18）を参照してください。
Top Malware Categories Detected	このセクションには、選択した DVS エンジンによって所定のカテゴリ タイプで検出された上位のマルウェア 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 5-9（P.5-45）を参照してください。
Top Malware Threats Detected	このセクションには、使用する DVS エンジンで検出された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 Detected] セクションに表示されている個々のマルウェア カテゴリに関する詳細情報が表示されます。 [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。 有効なマルウェア カテゴリの詳細については、表 5-9（P.5-45）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。

[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。

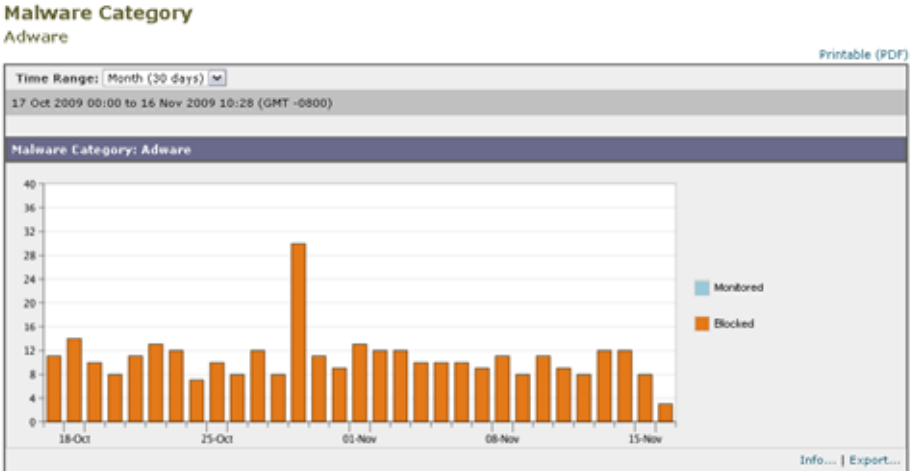
ステップ 1　Security Management アプライアンスのウィンドウで、[Web] > [Reporting] > [Anti-Malware] を選択します。

[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



[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。

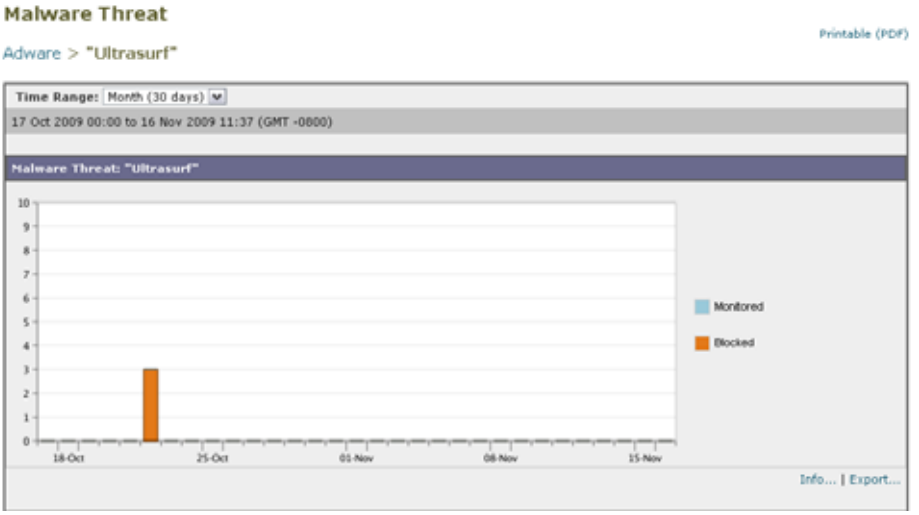
ステップ 1　Security Management アプライアンスのウィンドウで、[Web] > [Reporting] > [Anti-Malware] を選択します。

[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



（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、「レポートのスケジューリング」（P.5-83）を参照してください。

マルウェアのカテゴリについて

表 5-9 に、Security Management アプライアンスおよび Web セキュリティ アプライアンスでブロックできる、さまざまなマルウェアのカテゴリを示します

表 5-9　マルウェアのカテゴリについて

マルウェアのタイプ	説明
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。バリアントの中には、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。
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。
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。

表 5-9　マルウェアのカテゴリについて（続き）

マルウェアのタイプ	説明
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、通常はユーザが気付く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/サイトからダウンロードで命令を取得するため、インストールごとにペイロードが異なる場合があります。
トロイの木馬	トロイの木馬は、安全なアプリケーションを装う有害なプログラムです。ウイルスとは異なり、トロイの木馬は自己複製しません。
トロイのフィッシャ	トロイのフィッシャは、感染したコンピュータに潜んで特定の Web ページがアクセスされるのを待つか、または感染したマシンをスキャンして銀行サイト、オークション サイト、あるいはオンライン支払サイトに関係するユーザ名とパスワードを探します。
ウイルス	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。

アンチマルウェアの設定

（注） Security Management アプライアンスでアンチマルウェア機能を使用するには、事前に Web セキュリティ アプライアンスでグローバル設定を指定し、各種のポリシーに特定の設定を適用する必要があります。詳細については、『*Cisco IronPort AsyncOS for Web User Guide*』の「Configuring Anti-Malware Scanning」を参照してください。

アンチマルウェアを設定するには、まず次の 2 つの設定を指定する必要があります。

- **グローバルなアンチマルウェア設定。**オブジェクト スキャン パラメータを設定し、URL を照合するためのグローバル設定を指定します。さらに、どのようなときに URL をブロックするか、または処理の続行を許可するかを制御します。

- **アクセス ポリシーのアンチマルウェア設定。**マルウェア スキャンの判定に基づいたマルウェア カテゴリのモニタまたはブロックをイネーブルにします。

ステップ 1　Security Management アプライアンスのウィンドウで、[Configuration Master 7.1] > [Access Policies] を選択します。

[Access Policies] ウィンドウが表示されます。

ステップ 2　[Web Reputation and Anti-Malware Filtering] カラムで、設定するアクセス ポリシーのポリシー名のリンクをクリックします。

そのポリシーの [Access Policies: Reputation and Anti-Malware Settings] ウィンドウが表示されます。

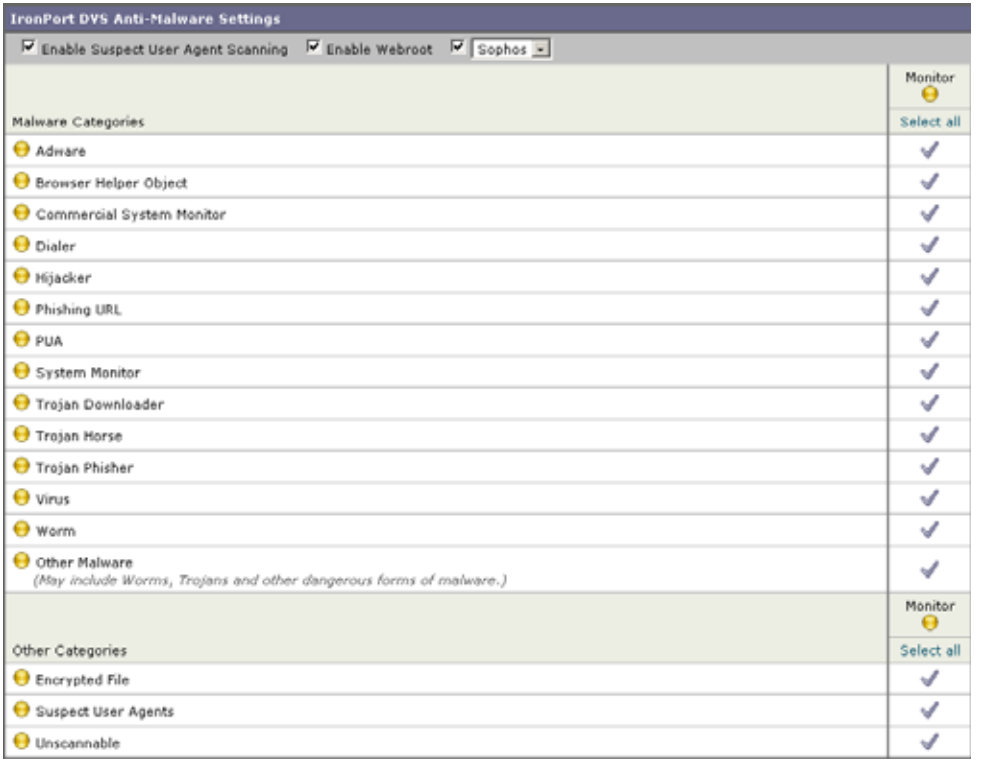
このページでは、マルウェア スキャンの判定に基づいたマルウェア カテゴリのモニタまたはブロックをイネーブルにすることができます。

ステップ 3　[Web Reputation and Anti-Malware Settings] セクションで、ドロップダウン メニューから [Define Web Reputation and Anti-Malware Custom Settings] を選択します（まだ選択されていない場合）。

これにより、このアクセス ポリシーに対して、グローバル ポリシーとは異なる Web レピュテーション設定およびアンチマルウェア設定を指定できます。

ステップ 4　[Cisco IronPort DVS Anti-Malware Settings] セクションで、ポリシーのアンチマルウェア設定を必要に応じて指定します。

図 5-12　アクセス ポリシーのアンチマルウェア設定



ステップ 5　ポリシーのアンチマルウェア設定を必要に応じて指定します。

表 5-10 に、アクセス ポリシーに対して指定できるアンチマルウェア設定を示します。

表 5-10　アクセス ポリシーに対するアンチマルウェア設定

設定	説明
Enable Suspect User Agent Scanning	HTTP 要求ヘッダーに指定されたユーザ エージェント フィールドに基づいて、アプライアンスがトラフィックをスキャンできるようにするかどうかを選択します。 この設定をオンにした場合は、ページ下部の [Additional Scanning] セクションで、疑わしいユーザ エージェントをモニタするかブロックするかを選択できます。
Enable Webroot	アプライアンスがトラフィックをスキャンする際に、Webroot スキャン エンジンを使用できるようにするかどうかを選択します。Webroot スキャンをイネーブルにすると、このページの [Malware Categories] で、追加カテゴリをモニタするかブロックするかを選択できます。
Enable Sophos	アプライアンスがトラフィックをスキャンする際に、Sophos スキャン エンジンを使用できるようにするかどうかを選択します。Sophos スキャンをイネーブルにすると、このページの [Malware Categories] で、追加カテゴリをモニタするかブロックするかを選択できます。
Enable McAfee	アプライアンスがトラフィックをスキャンする際に、McAfee スキャン エンジンを使用できるようにするかどうかを選択します。McAfee スキャンをイネーブルにすると、このページの [Malware Categories] で、追加カテゴリをモニタするかブロックするかを選択できます。

表 5-10　アクセス ポリシーに対するアンチマルウェア設定（続き）

設定	説明
Malware Categories	各種のマルウェア カテゴリを、マルウェア スキャンの判定に基づいてモニタするかブロックするかを選択します。 このセクションに表示されるカテゴリは、上でイネーブルにするスキャン エンジンによって異なります。
Additional Scanning	このセクションに表示されたオブジェクトおよび応答のタイプを、モニタするかブロックするかを選択します。 **注：**設定された最大時間に達するか、またはシステムが一時的なエラー状態に陥ると、URL トランザクションがスキャン不可と分類されます。たとえば、スキャン エンジンのアップデートや AsyncOS のアップグレードが行われている間は、トランザクションがスキャン不可と分類されることがあります。マルウェア スキャンの判定である SV_TIMEOUT および SV_ERROR は、スキャン不可のトランザクションと見なされます。

ステップ 6　[Submit] をクリックしてページ上の変更を送信し、[Commit Changes] をクリックしてアプライアンスへの変更を確定します。

アンチマルウェアの詳細および Web セキュリティ アプライアンスでこの機能を設定する方法については、『*Cisco IronPort AsyncOS for Web User Guide*』の「Configuring Anti-Malware Scanning」を参照してください。

[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。

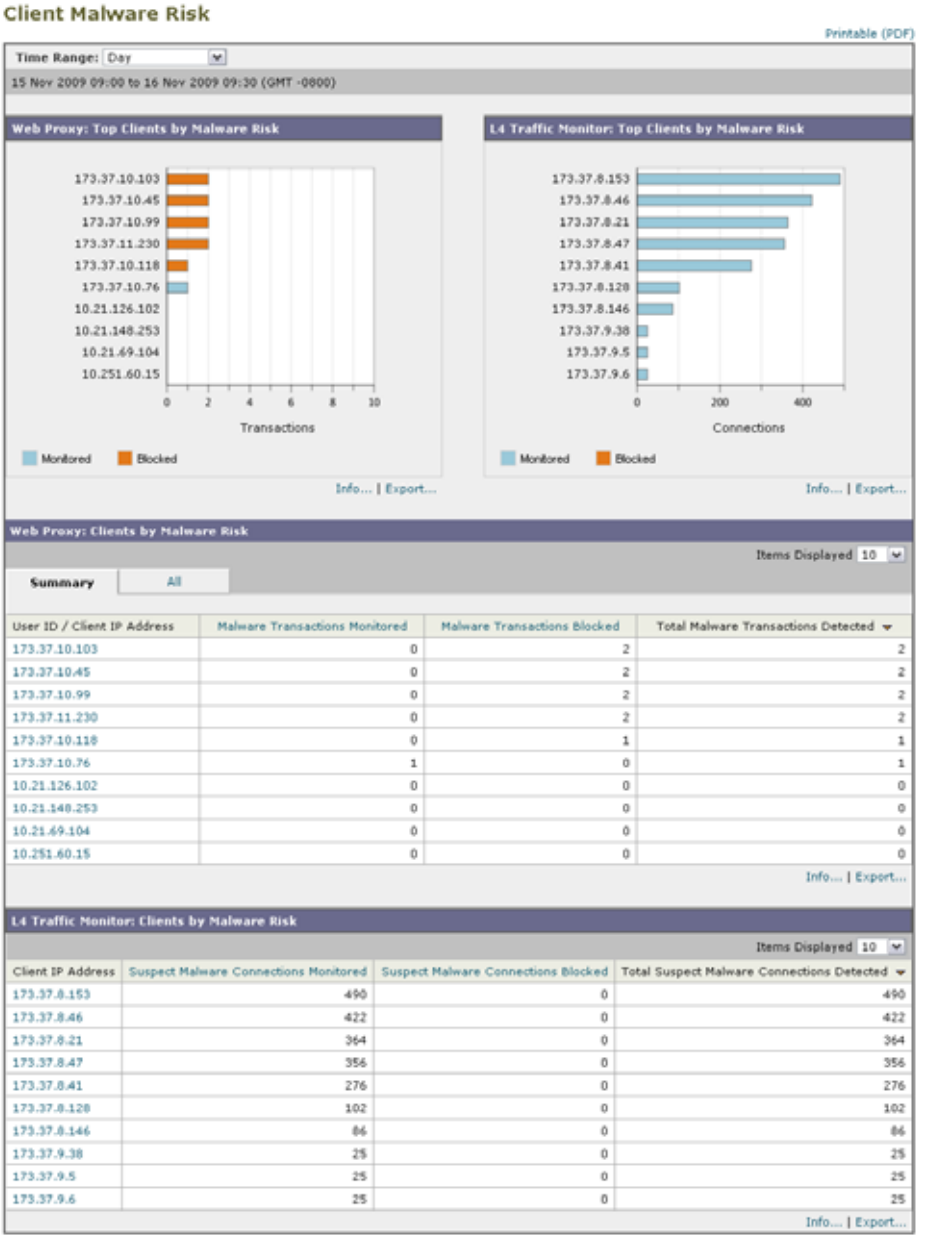
さらに [Client Malware Risk] ページでは、特定の IP アドレスの L4TM アクティビティを確認できます。

[Client Malware Risk] 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　Security Management アプライアンスのウィンドウで、[Web] > [Reporting] > [Client Malware Risk] を選択します。

[Client Malware Risk] ページが表示されます。

図 5-13　[Client Malware Risk] ページ



[Client Malware Risk] ページには次の情報が表示されます。

表 5-11　[Web] > [Reporting] > [Client Malware Risk] 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.3-18）を参照してください。
Web Proxy: Top Clients by Malware Risk	このセクションには、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。この情報はグラフ形式で表示されます。
L4 Traffic Monitor: Top Clients by Malware Risk	このセクションには、L4 トラフィック モニタリングのリスクが発生した上位 10 人のユーザが表示されます。この情報はグラフ形式で表示されます。
Web Proxy: Clients by Malware Risk	[Web Proxy: Clients by Malware Risk] インタラクティブ 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。 ユーザ ID とクライアント IP アドレスはインタラクティブになっており、各クライアントの詳細情報を提供する [Client Details] ページへのリンクがあります。クライアント ページの詳細については、[Client Details] ページを参照してください。 インタラクティブ テーブルのリンクをクリックすると、個々のユーザ、およびマルウェアのリスクをトリガーしているそのユーザのアクティビティをさらに詳しく表示できます。たとえば、ユーザ/IP アドレスのカラム内のリンクをクリックすると、その IP アドレスのユーザ ページが表示されます。
L4 Traffic Monitor: Clients by Malware Risk	[Web Proxy: Clients Malware Risk] インタラクティブ テーブルには、個々のユーザおよび L4 トラフィック モニタリング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に関する詳細情報が表示されます。ユーザ/IP アドレスのカラム内のリンクをクリックすると、その IP アドレスのユーザ ページが表示されます。

（注）　[Anti-Malware] 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、「レポートのスケジューリング」（P.5-83）を参照してください。

[Client Details] ページ

[Web Proxy: Clients by Malware Risk] セクションで個々のクライアントのハイパーテキスト リンクをクリックすると、特定のユーザのページが表示され、指定した時間範囲における特定のクライアントの Web アクティビティおよびマルウェア リスクのデータがすべて示されます。

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

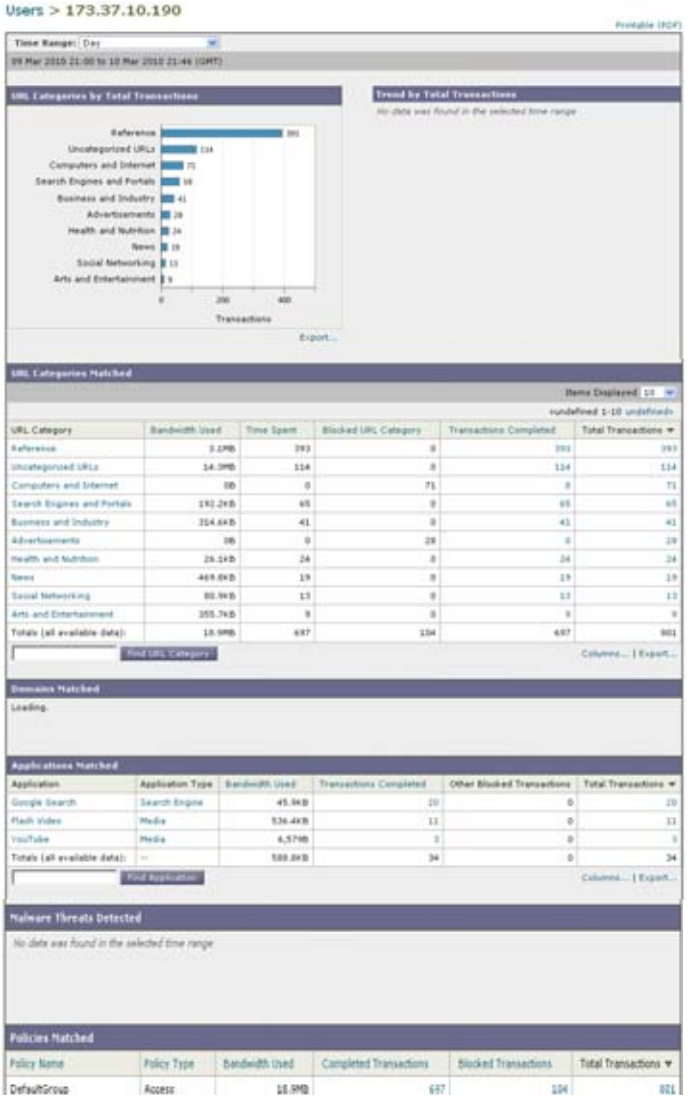
ステップ 1　Security Management アプライアンスのウィンドウで、[Web] > [Reporting] > [Client Malware Risk] を選択します。

[Client Malware Risk] ページが表示されます。

ステップ 2　[User/IP address] カラム内のリンクをクリックします。

[Client Details] ページが表示されます。

図 5-14　[Client Details] ページ



[Client Details] ページには次の情報が表示されます。

表 5-12　[Web] > [Reporting] > [Client Malware Risk] > [Client 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）	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.3-18）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。
Trend by Total Transaction	このグラフには、特定のユーザの Web トランザクションの経時的なトレンドが示されます。基本的には、この特定のユーザがその Web にいつアクセスしたか、および閲覧トラフィックを送信した回数が示されます。 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、指定した時間範囲内にマルウェア リスクとなる可能性があった一致カテゴリがすべて表示されます。インタラクティブなカラム見出しを使用するとデータをソートできます。また、[Items Displayed] メニューによって、リストに表示される URL カテゴリの数を変更できます。 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。 URL カテゴリの詳細については、「[URL Categories] ページ」（P.5-28）を参照してください。

表 5-12　[Web] > [Reporting] > [Client Malware Risk] > [Client Details] ページの詳細（続き）

セクション	説明
Domains Matched	[Domains Matched] セクションでは、このユーザがアクセスした、マルウェア リスクの可能性がある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、マルウェア リスクの可能性がある特定のアプリケーションを確認できます。 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。システム管理者が、すべての Flash ビデオにマルウェア リスクがあると判断した可能性があります。このため、このアプリケーションは [Applications Matched] セクションに表示されます。 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。
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、マルウェア リスクの可能性がある上位のマルウェア脅威を確認できます。セクション下部のテキスト フィールドにマルウェア脅威の名前を入力し、[Find Malware Threat] をクリックします。マルウェア脅威の名前は正確に一致している必要はありません。
Policies Matched	このセクションでは、この特定のユーザに適用され、特定のアクションを潜在的なマルウェア リスクと定義している特定のポリシーを確認できます。 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。

他の Web レポーティング ページと同様に、[Client Details] ページのすべてのテーブルでは、インタラクティブ リンクを通じて他の詳細情報を表示でき、ページのデータをユーザのニーズに合わせて表示できるように、対話型カラム見出しを設定して各カラムのデータをソートすることができます。カラムの設定の詳細については、「Web セキュリティ アプライアンス用のインタラクティブ レポート ページ」（P.5-10）を参照してください。

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

[Web 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 User Guide*』の「Web Reputation Filters」を参照してください。

[Web Reputation Filters] 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　Security Management アプライアンスのウィンドウで、[Web] > [Reporting] > [Web Reputation Filters] を選択します。

[Web Reputation Filters] ページが表示されます。

図 5-15　[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 5-13　[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.3-18）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	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」の場合は、トランザクションがアンチマルウェア 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)	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。

上記の最初の 4 つのセクションには、印刷可能なファイルにデータをエクスポートするための [Export] ハイパーテキスト リンクが表示されています。印刷可能なファイルについては、「レポート ページからのレポートの印刷」（P.5-11）を参照してください。

[Web Reputation Actions] テーブルには、設定可能なインタラクティブ カラムがあります。インタラクティブ カラムの設定の詳細については、「レポート ページのカラムの設定」（P.5-10）および「中央集中型 Web レポーティング ページのインタラクティブ カラム」（P.E-1）を参照してください。

Web レピュテーション スコアの設定

Security Management アプライアンスおよび Web セキュリティ アプライアンスをインストールしてセットアップすると、Web セキュリティ アプライアンスで Web レピュテーション スコアのデフォルトの設定が指定されます。ただし、Web レピュテーションのスコアを付けるためのこれらのしきい値の設定は、必要に応じて変更できます。

アクセス ポリシーおよび復号化ポリシーのグループに対して、Web レピュテーション フィルタの設定を指定する必要があります。

アクセス ポリシーに対する Web レピュテーション フィルタの設定

アクセス ポリシー グループに対する Web レピュテーション フィルタの設定を編集するには、次の手順を実行します。

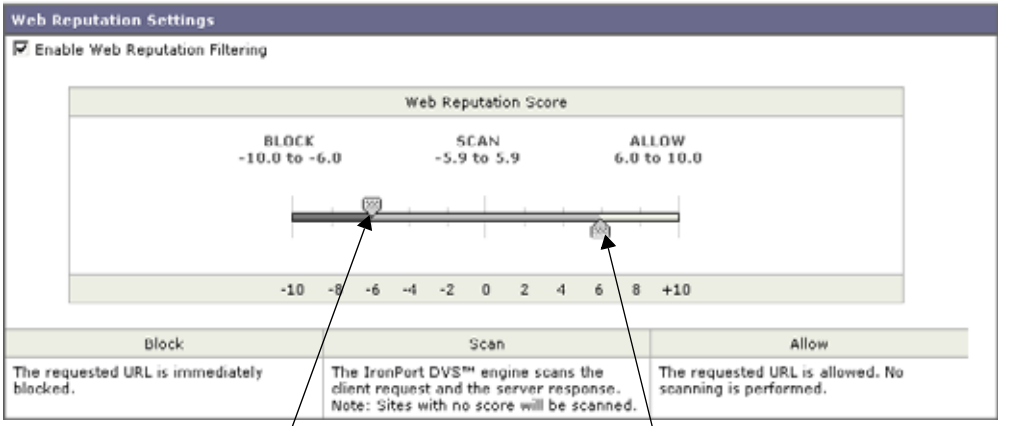
ステップ 1　Security Management アプライアンスのウィンドウで、[Configuration Master 7.1] > [Access Policies] を選択します。

ステップ 2　[Web Reputation and Anti-Malware Filtering] カラムで、編集するアクセス ポリシー グループのリンクをクリックします。

ステップ 3　[Web Reputation and Anti-Malware Settings] セクションで、[Enable Web Reputation Filters] チェックボックスをオンにします（オフになっている場合）。

[Web Reputation Score] ボックスが表示されます。

図 5-16　アクセス ポリシーに対する Web レピュテーション フィルタの設定



これらのマーカーを動かして、Web レピュテーションのしきい値を変更します

これにより、グローバル ポリシー グループの Web レピュテーションおよびアンチマルウェアの設定をオーバーライドできます。

ステップ 4　[Enable Web Reputation Filtering] チェックボックスがオンになっていることを確認します。

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

ステップ 6　[Submit] をクリックしてページ上の変更を送信し、[Commit Changes] をクリックしてアプライアンスへの変更を確定します。

この時点で、復号化ポリシーに対して Web レピュテーションを設定する必要があります。復号化ポリシーに対する Web レピュテーション フィルタ設定の編集または指定については、『*Cisco IronPort AsyncOS for Web User Guide*』の「Web Reputation Filters」を参照してください。

[L4 Traffic Monitor Data] ページ

[Web] > [Reporting] > [L4 Traffic Monitor] ページは、指定した時間範囲内に L4 トラフィック モニタが検出したマルウェア ポートとマルウェア サイトに関する情報を表示する、セキュリティ関連のレポーティング ページです。

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

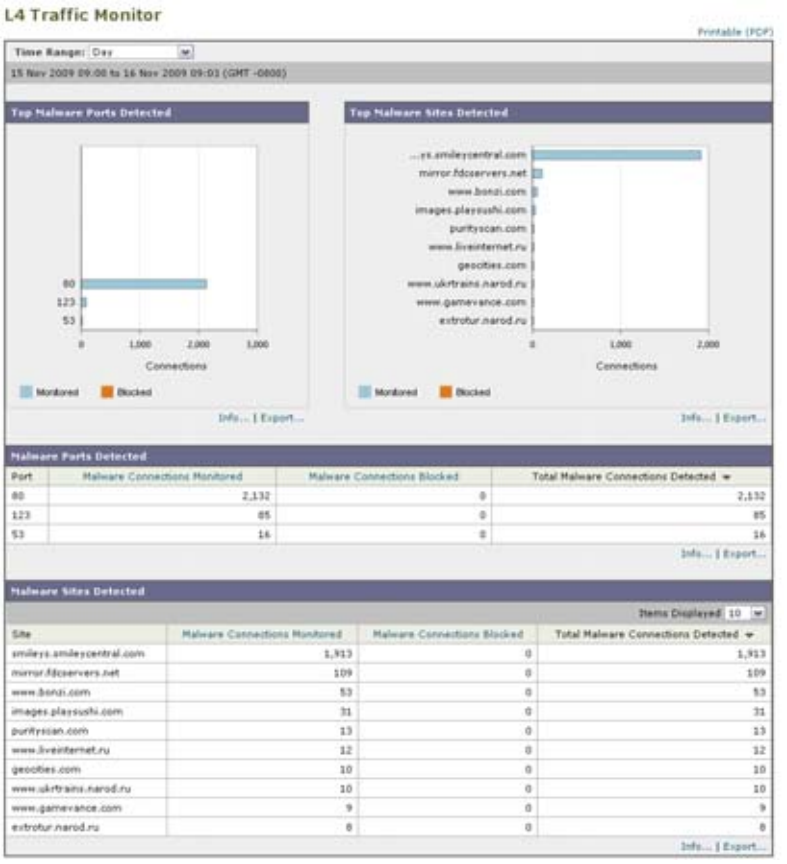
レポートの上部には、上位の各マルウェア ポートおよび各マルウェア Web サイトの接続数が表示されます。レポートの下部には、検出されたマルウェア ポートとマルウェア サイトが表示されます。

[L4 Traffic Monitor Data] 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　Security Management アプライアンスのウィンドウで、[Web] > [Reporting] > [L4 Traffic Monitor] を選択します。

[L4 Traffic Monitor] ページが表示されます。

図 5-17　[L4 Traffic Monitor] ページ



[L4 Traffic Monitor] ページには次の情報が表示されます。

表 5-14　[Web] > [Reporting] > [L4 Traffic Monitor] 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.3-18）を参照してください。
Top Malware Ports Detected	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 ポートがグラフ形式で表示されます。
Top Malware Sites Detected	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。 このビューでは、L4 トラフィック モニタによって検出された、モニタされたドメインまたはブロックされたドメインが、色分けされたグラフで表示されます。
Malware Ports Detected	[Malware Ports Detected] テーブルには、L4 トラフィック モニタによって検出されたすべてのポートが表示されます。
Malware Sites Detected	[Malware Sites Detected] テーブルには、L4 トラフィック モニタによって検出されたすべてのドメインが表示されます。

上記のすべてのセクションには、印刷可能なファイルにデータをエクスポートするための [Export] ハイパーテキスト リンクが表示されます。印刷可能なファイルについては、「レポート ページからのレポートの印刷」（P.5-11）を参照してください。

L4 トラフィック モニタの設定

L4 トラフィック モニタは、Security Management アプライアンスのシステム セットアップ ウィザード（[Management Appliance] > [System Administration] > [System Setup Wizard] を選択）を使用した初期システム セットアップの中で、イネーブルにすることができます。

デフォルトでは、L4 トラフィック モニタがイネーブルになり、すべてのポートでトラフィックをモニタするように設定されます。これには、DNS やその他のサービスが含まれます。

正しいクライアント IP アドレスをモニタするには、ネットワーク アドレス変換（NAT）が行われる前にファイアウォール内で必ず L4 トラフィック モニタを設定する必要があります。

L4 トラフィック モニタの設定の詳細については、『*Cisco IronPort AsyncOS for Web User Guide*』を参照してください。システム セットアップ ウィザードの詳細については、「システム セットアップ ウィザードについて」（P.2-10）を参照してください。

（注）　[L4 Traffic Monitor] 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、「レポートのスケジューリング」（P.5-83）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。

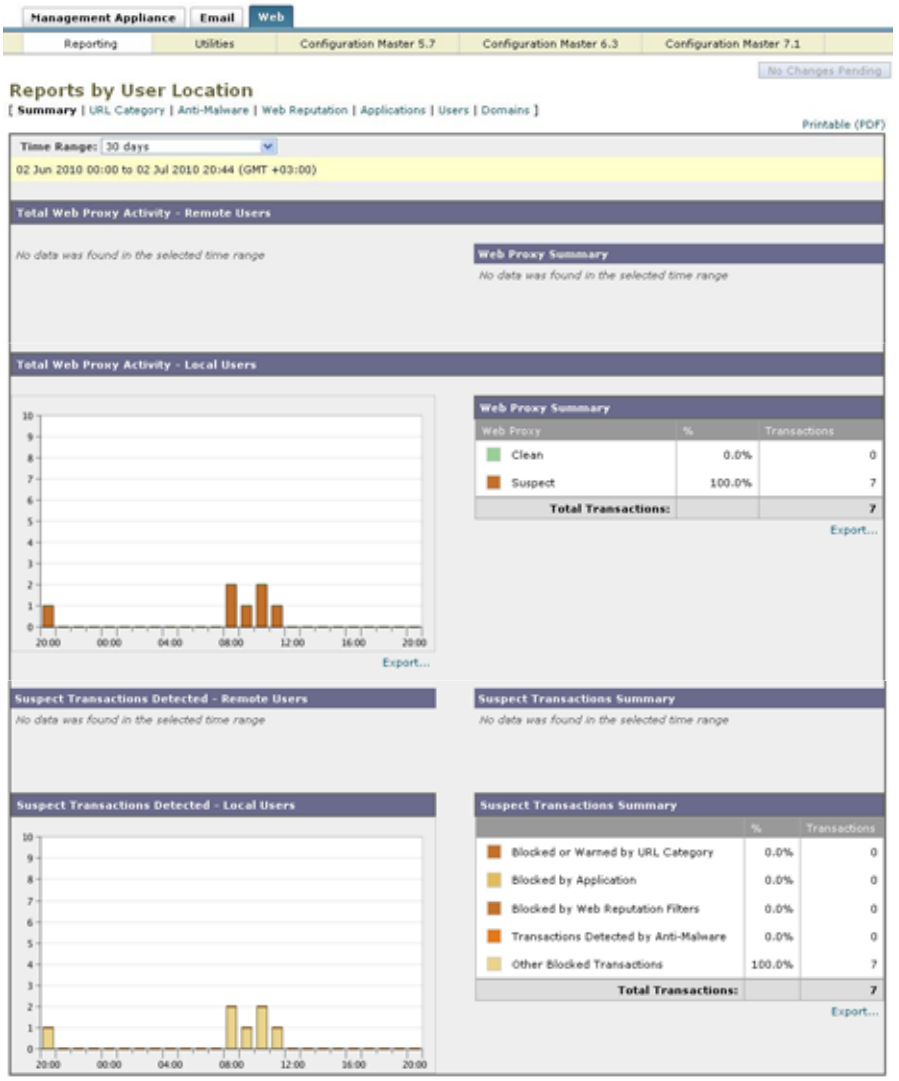
- ローカル ユーザおよびリモート ユーザがアクセスしている URL カテゴリ。
- ローカル ユーザおよびリモート ユーザがアクセスしているサイトによってトリガーされているアンチマルウェア アクティビティ。
- ローカル ユーザおよびリモート ユーザがアクセスしているサイトの Web レピュテーション。
- ローカル ユーザおよびリモート ユーザがアクセスしているアプリケーション。
- ユーザ（ローカルおよびリモート）。
- ローカル ユーザおよびリモート ユーザがアクセスしているドメイン。

[Reports by User Location] 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　Security Management アプライアンスのウィンドウで、[Web] > [Reporting] > [Reports by User Location] を選択します。

[Reports by User Location] ページが表示されます。

図 5-18　[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 5-15　[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.3-18）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。

（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、「レポートのスケジューリング」（P.5-83）を参照してください。

[Web Tracking] ページ

[Web] > [Reporting] > [Web Tracking] ページでは、基本的な Web 関連情報（Web セキュリティ 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）をトラッキングし、表示することができます。これには、時間範囲やユーザ ID とクライアント IP アドレスなどの情報が含まれ、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。

マルウェア情報のフィルタリング、および WBRS のスコア範囲またはレピュテーション脅威による Web サイトのトラッキングも、Web トラッキングの重要な要素です。[Web Tracking] ページでは、これらすべての基準を検索し、モニタすることができます。Web トラッキングの結果からデータを除外する方法はありませんが、トラッキングする基準を決定した後に、基準をさらに追加して結果セットを絞り込むことができます。

[Web Tracking] ページでは、管理者がデフォルトの Web トラッキング結果ビューを使用してユーザに関する簡単な情報を確認したり、詳細な Web トラッキング結果ビューを使用してより詳細な情報を確認したりできるように設計されています。

[Web Tracking] ページを他の Web レポーティング ページと組み合わせて使用する例については、「[URL Categories] ページとその他のレポーティング ページの併用」（P.5-32）を参照してください。

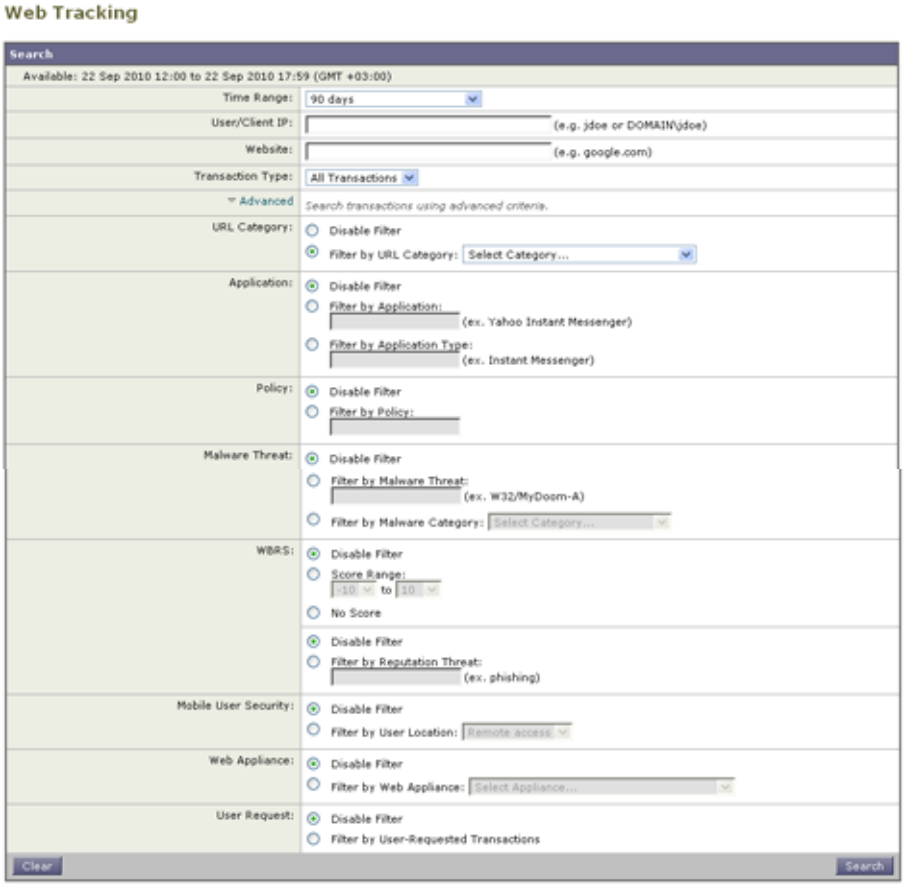
（注） Web レポーティングでは、アクセスされる特定の URL に限らず、ユーザがアクセスするすべてのドメイン情報を取得できる点に注意してください。ユーザがアクセスしている特定の URL、その URL にアクセスした時刻、その URL が許可されているかどうかなどの情報を得るには、[Web Tracking] ページを使用します。

[Web Tracking] 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　Security Management アプライアンスのウィンドウで、[Web] > [Reporting] > [Web Tracking] を選択します。

[Web Tracking] ページが表示されます。

図 5-19　[Web Tracking] ページ



（注）　上に示す [Web Tracking] ページは、[Advanced] の各フィールドが表示された状態のものです。

[Web Tracking] ページには次の情報が表示されます。

デフォルトの Web トラッキング結果

- 時間範囲
- ユーザ / クライアント IP

- Web サイト
- トランザクション タイプ

詳細な基準の Web トラッキング結果

- URL カテゴリ
- アプリケーション
- ポリシー
- マルウェアの脅威
- Web ベースのレポーティング システム（WBRS）
- モバイル ユーザのセキュリティ
- Web アプライアンス
- ユーザ要求

Web トラッキングの設定

Web トラッキング結果は、次の 2 つのビューで表示できます。

- デフォルトの Web トラッキング結果
- 詳細な Web トラッキング結果

デフォルトの Web トラッキング結果

デフォルトの Web トラッキング ビューでは、Web トラッキングの結果を、ユーザ名または IP アドレス、トランザクション タイプなどの基本的な基準でフィルタリングできます。

デフォルトの Web トラッキングの結果を収集するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Web] > [Reporting] > [Web Tracking] を選択します。

[Web Tracking] ページが表示されます。

ステップ 2　[Time Range] ドロップダウン リストで、トラッキングする時間範囲を選択します。

時間範囲および Security Management アプライアンスでの時間範囲の機能については、「インタラクティブ レポートの時間範囲の選択」（P.3-18）を参照してください。

ステップ 3　[User/Client IP] にユーザまたはクライアント IP アドレスを入力し [Website] フィールドに入力します。

これらの Web サイトおよびユーザまたはクライアント IP アドレスに関して、情報がトラッキングされます。

ステップ 4　[Transaction Type] ドロップダウン リストで、トラッキングするトランザクションのタイプを選択します。

選択肢は、[All Transactions]、[Completed]、[Blocked]、[Monitored]、[Warned] です。

ステップ 5　[Search] をクリックします。

デフォルト ビューの結果は、カラムで設定できません。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。デフォルト ビューの結果は、次のページのようになります。

図 5-20　デフォルトの Web トラッキング ビューの [Results] ページ

[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 Web サイト

  [Transaction] カラムで [Display Details] をクリックすると、トランザクションに関する詳細情報が表示されます。
- Disposition

[Disposition] カラムには、トランザクションがブロックされた理由、つまりポリシーによってブロックされたのか、WBRS スコアによってブロックされたのかなどが表示されます。

- Bandwidth
- User ID/Client IP

詳細な Web トラッキング結果

詳細な Web トラッキング ビューでは、より詳細な基準を使用して Web トラッキングの結果をフィルタリングできます。たとえば、WBRS レピュテーション スコア、URL カテゴリ、Web レピュテーションの脅威などによってフィルタリングできます。

詳細な Web トラッキングの結果を収集するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスのウィンドウで、[Web] > [Reporting] > [Web Tracking] を選択します。

[Web Tracking] ページが表示されます。

ステップ 2　[Time Range] ドロップダウン リストで、トラッキングする時間範囲を選択します。

時間範囲および Security Management アプライアンスでの時間範囲の機能については、「インタラクティブ レポートの時間範囲の選択」（P.3-18）を参照してください。

ステップ 3　[User/Client IP] にユーザまたはクライアント IP アドレスを入力し [Website] フィールドに入力します。

これらの Web サイトおよびユーザまたはクライアント IP アドレスに関して、情報がトラッキングされます。

ステップ 4　[Transaction Type] ドロップダウン リストで、トラッキングするトランザクションのタイプを選択します。

選択肢は、[All]、[Completed]、[Blocked]、[Monitored]、[Warned] です。

ステップ 5　[Advanced] の矢印をクリックしてページを展開し、詳細な基準を表示します。

ステップ 6　[Filter by URL Category] の横のオプション ボタンをクリックして、URL カテゴリをディセーブルまたはイネーブルにします。

URL カテゴリによるフィルタリングをイネーブルにすると、[Filter By URL Category] ドロップダウン リストの選択肢を選択して、イネーブルにするカテゴリを選択できます。

ステップ 7　特定のポリシーでフィルタリングするには、[Filter by Policy] の横のオプション ボタンをクリックし、テキスト フィールドにポリシー名を入力します。

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。

ステップ 8　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] の横のオプション ボタンをクリックし、テキスト フィールドに脅威の名前を入力します。

ステップ 9　WBRS のスコア範囲を指定するには、[Score Range] の横のオプション ボタンをクリックします。

このフィルタをディセーブルにするには、[WBRS] セクションの [Disable Filter] オプション ボタンをクリックします。WBRS スコア範囲情報の詳細については、『*Cisco IronPort AsyncOS for Web User Guide*』を参照してください。

ステップ 10　レピュテーションの脅威で Web トラッキングをフィルタリングするには、[WBRS] セクションで [Filter by Reputation Threat] オプション ボタンをクリックします。このフィルタをディセーブルにするには、このセクションの [Disable Filter] オプション ボタンをクリックします。

ステップ 11　特定のモバイル ユーザ セキュリティでフィルタリングするには、[Filter by User Location] の横のオプション ボタンをクリックし、テキスト フィールドに位置を入力します。このフィルタをディセーブルにするには、このセクションの [Disable Filter] オプション ボタンをクリックします。

ステップ 12　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。このフィルタをディセーブルにするには、このセクションの [Disable Filter] オプション ボタンをクリックします。

ステップ 13　特定のユーザ要求でフィルタリングするには、[Filter by User-Requested Transaction] 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。このフィルタをディセーブルにするには、このセクションの [Disable Filter] オプション ボタンをクリックします。

ステップ 14　ページ ビューの結果をイネーブルにするには、[Enable Page] ビューの結果の横にあるチェックボックスをオンにします。

ステップ 15　[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。

ステップ 16　[Transaction] カラムで [Display Details] をクリックすると、トランザクションに関する詳細情報が表示されます。

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-2）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 Security Management 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たものになっ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。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。
- 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。

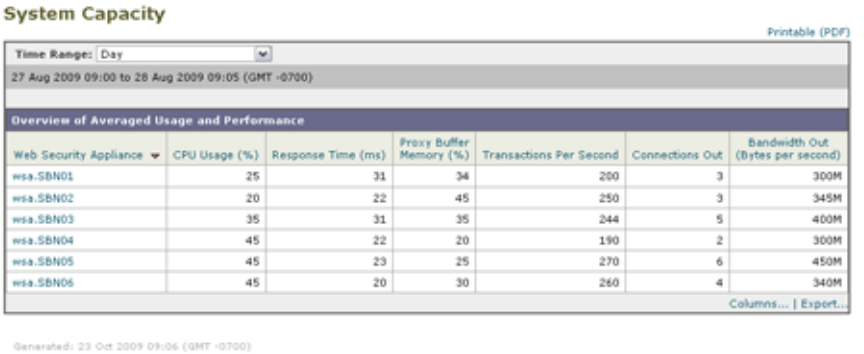
（注） 他のレポートで時間範囲に [Year] を選択した場合は、最も大きな時間範囲である 90 日を選択することを推奨します。

[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　Security Management 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 5-21　[System Capacity] ページ



ステップ 2　[Overview of Averaged Usage and Performance] インタラクティブ テーブルの Web Security Appliance カラムで特定のアプライアンスをクリックし、そのアプライアンスのシステム キャパシティを表示します。

このユーザに関する [System Capacity] グラフが表示されます。[System Capacity] ページでは、次の 2 種類の情報を表示できます。

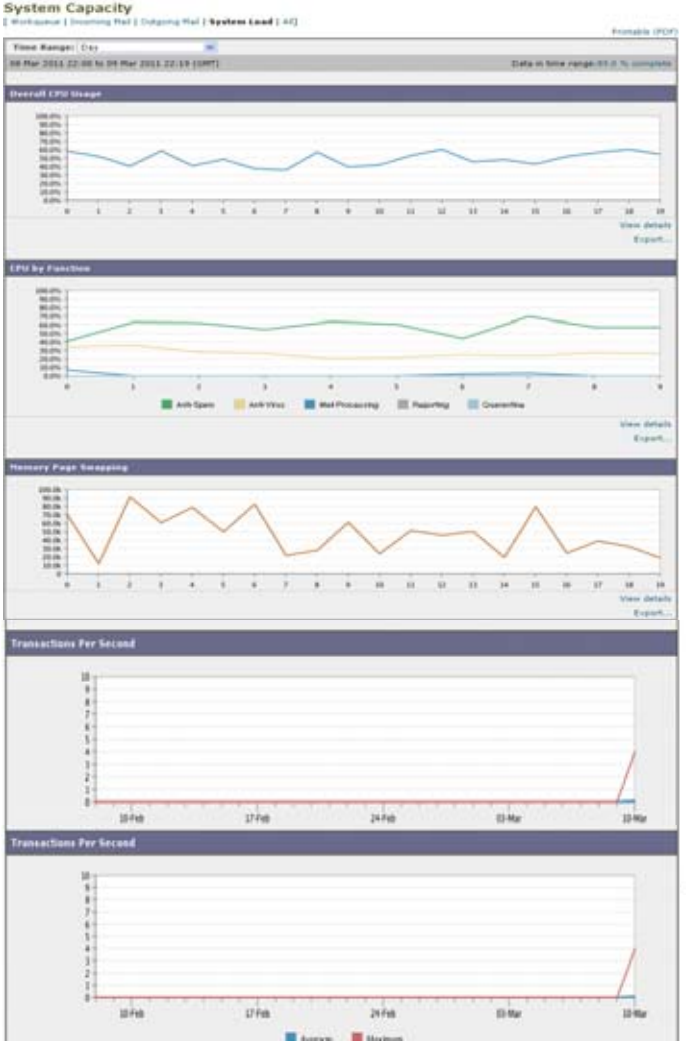
- [System Capacity] : [System Load]
- [System Capacity] : [Network Load]

[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 5-22　[System Capacity]：[System Load]

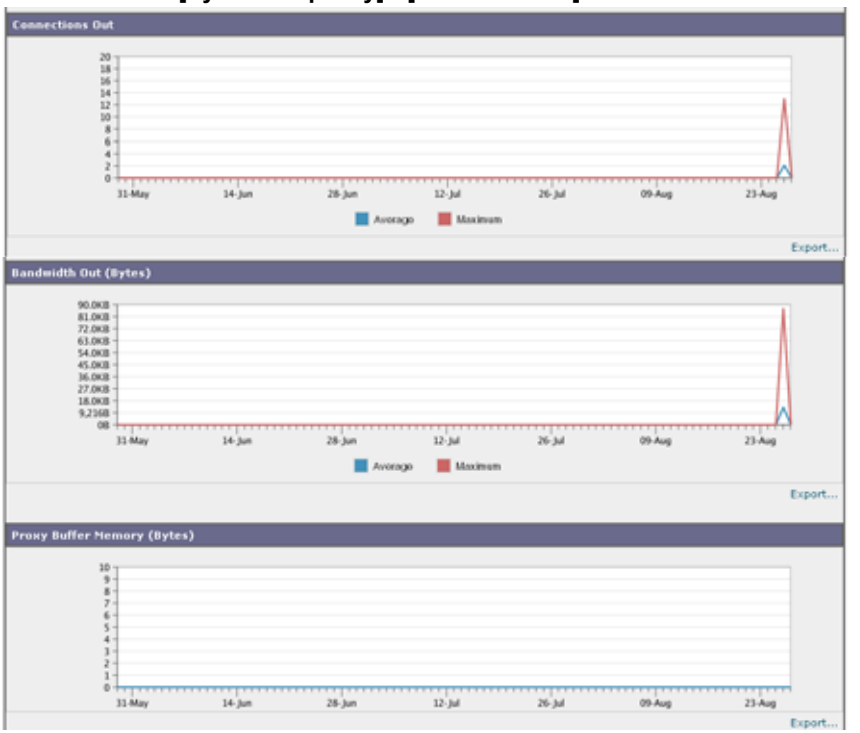


[System Capacity]：[Network Load]

[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。

図 5-23　[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 *常に* 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以外は、プロキシ バッファ メモリ スワッピングは正常であり、起こり得る挙動です。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。

[System Capacity] のカラム設定は、[System Capacity] ページの [Overview of Averaged Usage and Performance] セクションで指定できます。インタラクティブ カラムの設定の詳細については、「レポート ページのカラムの設定」（P.5-10）および「中央集中型 Web レポーティング ページのインタラクティブ カラム」（P.E-1）を参照してください。

[Data Availability] ページ

[Web] > [Reporting] > [Data Availability] ページでは、リソース使用率および Web 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。

[Data Availability] 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　Security Management アプライアンスのページで、[Web] > [Reporting] > [Data Availability] を選択します。

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

図 5-24　[Web Reporting Data Availability] ページ


Web Reporting Data Availability

Printable (PDF)

Web Reporting Data Range

	Web Reporting		Web Tracking and Reporting Detail			
Web Security Appliance	From	To	From	To	Missing Data	Status
wsa.SBN01	22 May 2009 10:20	06 Nov 2009 09:01	07 Aug 2009 10:01	06 Nov 2009 09:01	No	OK
wsa.SBN02	22 May 2009 10:20	06 Nov 2009 08:48	07 Aug 2009 10:01	06 Nov 2009 08:48	No	Not updated in 12 minutes
wsa.SBN03	22 May 2009 10:20	06 Nov 2009 08:57	07 Aug 2009 10:01	06 Nov 2009 08:57	No	OK
wsa.SBN04	22 May 2009 10:20	06 Nov 2009 08:57	07 Aug 2009 10:01	06 Nov 2009 08:57	No	OK
wsa.SBN05	22 May 2009 10:20	06 Nov 2009 08:57	07 Aug 2009 10:01	06 Nov 2009 08:57	Yes	OK
wsa.SBN06	22 May 2009 10:20	06 Nov 2009 08:59	07 Aug 2009 10:01	06 Nov 2009 08:59	No	OK
Overall:	22 May 2009 10:20 (GMT -07:00)	06 Nov 2009 09:01 (GMT -08:00)	07 Aug 2009 10:01 (GMT -07:00)	06 Nov 2009 09:01 (GMT -08:00)		

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。

（注）　[Web Reporting Data Availability] ページでは、個々の Web アプライアンスおよび電子メール アプライアンス上で Web レポーティングと電子メール レポーティングの両方がディセーブルになっている場合にのみ、Web レポーティングがディセーブルと報告されます。Web レポーティングがディセーブルになると、Security Management 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 Security Management 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.12-123）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。

さらに、Web レポーティングまたは Web トラッキングのいずれかで設定された範囲全体にギャップがある場合は、[Missing Data] カラムに「Yes」が表示されます。

ステップ 2　Web Security Appliance カラムで、データ アベイラビリティ情報が必要な特定のアプライアンスをクリックします。

そのアプライアンスの [Web Reporting Data Availability] が表示されます。このウィンドウには次の情報が表示されます。

- 受信したデータ
- この特定のアプライアンスの有効な日付範囲。
  この情報は [Overview] ページにも反映されます。[Web Reporting] セクションと [Web Tracking and Reporting Details] セクションの [From] および [To] の各見出しはハイパーリンクになっており、特定のユーザの特定の Web 詳細情報を表示することができます。

  データは、特定の期間における時間間隔についてのみ表示されます。

ステップ 3　[Items Displayed] ドロップダウン メニューから、表示するレコード数を選択できます。

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] をクリックしてアプライアンスへの変更を確定します。

（注） 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。

レポートのスケジューリング

日単位、週単位、または月単位で実行されるようにレポートをスケジュール設定することができます。スケジュール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。

レポートをスケジュール設定できるレポート タイプは次のとおりです。

- [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.5-12）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.5-16）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.5-28）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.5-87）を参照してください。
- [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.5-36）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.5-88）を参照してください。
- [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.5-40）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.5-50）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.5-58）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 Data] ページ」（P.5-64）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.5-67）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.5-76）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管理

ここでは、次の内容について説明します。

（注）　スケジュール設定されたレポートでは、すべてのユーザ情報を認識できないようにすることができます。レポートでユーザ名が認識できない状態でレポートを生成するには、[Anonymize usernames in reports] チェックボックスをオンにします。デフォルト設定では、すべてのレポートにすべてのユーザ名が表示されます。

Security Management 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「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

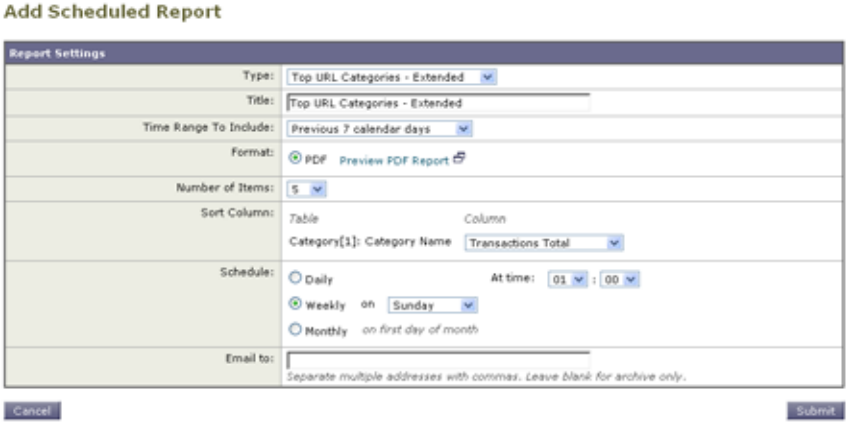
スケジュール設定された Web レポートを追加するには、次の手順を実行します。

ステップ 1　Security Management 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] ページが表示されます。

図 5-25　[Add Scheduled Reports] ページ



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。大部分のレポートでは、CSV のスケジューリングを行うことができます。

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　[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　[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 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 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 11　[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

Security Management アプライアンスの [Web] > [Reporting] セクションでは、追加で 2 種類の拡張レポートを生成できます。次のものがあります。

- 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。しかし、ネットワーク管理者は、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 人のユーザの帯域幅使用状況をモニタする、詳細なレポートを必要としているとします。この場合管理者は、[Top URL Categories — Extend] レポートを使用します。

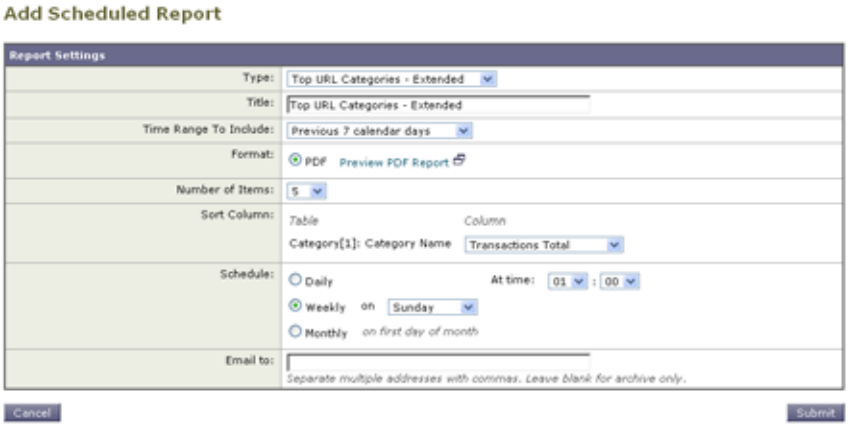
（注）　このタイプのレポートで生成できる最大レポート数は 20 です。

[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　Security Management 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 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　[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 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。

ステップ 11　[Submit] をクリックします。

Top Application Types — Extended

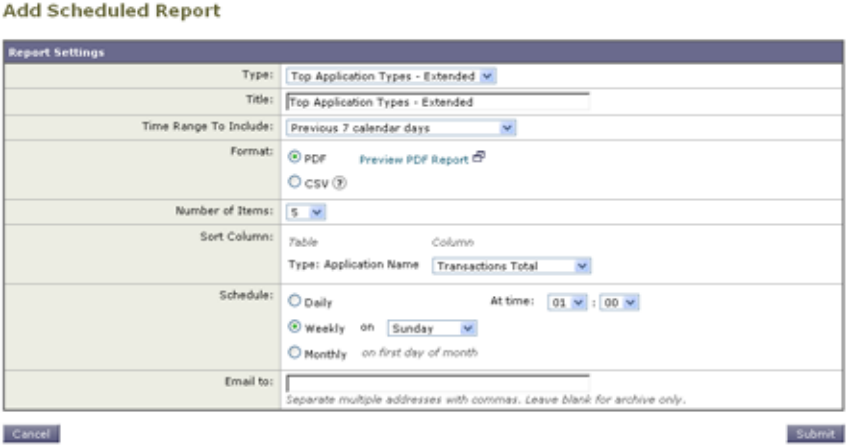
[Top Application Type — Extended] レポートを生成するには、次の手順を実行します。

ステップ 1　Security Management 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。



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、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　[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 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。

ステップ 11　[Submit] をクリックします。

レポートのアーカイブ

[Web] > [Reporting] > [Archived Reports] ページには、使用可能なアーカイブ済みのレポートのリストが表示されます。[Report Title] カラムのレポート名はインタラクティブとなっていて、各レポートのビューにリンクしています。[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。

（注）　[Report Type] カラムに表示される各レポートは、ハイパーテキスト リンクになっています。このハイパーテキスト リンクをクリックすると、そのレポートに関する情報にアクセスできます。

また、インタラクティブなカラム見出しを使用して、各カラムのデータをニーズに合わせてソートすることができます。

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

[Generate Report Now] オプション

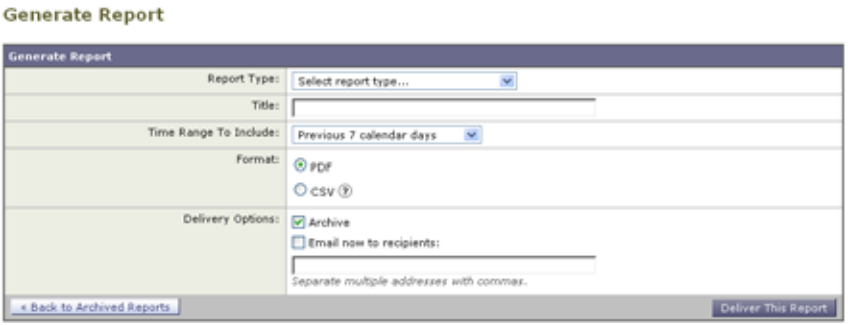
[Web] > [Archived Reports] ページの [Generate Report Now] オプションを使用すると、各レポート タイプのオンデマンド データ表示を生成できます。この機能を使用してレポートを生成するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスのウィンドウで、[Web] > [Reporting] > [Archived Reports] を選択します。

[Archived Reports] ページが表示されます。

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

図 5-26　オンデマンド レポートの生成



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。

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。

選択肢は次のとおりです。

- [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]。カンマ区切りの表データを含む 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　[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。

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

CHAPTER 6

電子メール メッセージのトラッキング

この章は、次の項で構成されています。

トラッキング サービスの概要

Security Management アプライアンスのトラッキング サービスは、Email Security アプライアンスを補完します。Security Management アプライアンスでは、電子メール管理者は、そのすべての Email Security 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 つの場所で追跡します。

Security Management アプライアンスにより、Email Security アプライアンスが処理するメッセージのステータスを容易に検索できます。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により、ヘルプ デスク コールを迅速に解決できます。管理者は、Security Management アプライアンスにより、ある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、スパム検疫に入れられたか、それともメール ストリームの他の場所にあるのかを判断することができます。

grep や同様のツールを使用してログ ファイル全体を検索する代わりに、Security Management 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。

次のトラッキング クエリーがあります。

- **エンベロープ情報：**照合するテキスト ストリングを入力することにより、特定のエンベロープ送信者またはエンベロープ受信者のメッセージを検索します。
- **件名ヘッダー：**件名行のテキスト文字列を照合します。警告：規制によりそのようなトラッキングが禁止されている環境では、このタイプの検索を使用しないでください。
- **時間枠：**指定した日付と時刻の間に送信されたメッセージを検索します。
- **送信元 IP アドレスまたは拒否された接続：**特定の IP アドレスからのメッセージを検索します。または、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：**添付ファイル名に基づいてメッセージを検索できます。クエリーした名前の添付ファイルを少なくとも 1 つ含むメッセージが、検索結果に表示されます。

  パフォーマンス上の理由から、OLE オブジェクトなどの添付ファイル内にあるファイル名や、.ZIP ファイルなどのアーカイブ内にあるファイル名はトラッキングされません。

  トラッキングできない添付ファイルもあります。パフォーマンス上の理由から、添付ファイル名のスキャンは、たとえばメッセージやコンテンツのフィルタリング、DLP、または免責事項スタンプなど、その他のスキャン動作の一部としてのみ実行されます。添付ファイル名を使用できるのは、添付ファイルが添付された状態で行われる本文スキャンを通過したメッセージだけです。次に、添付ファイル名が表示されない場合のいくつかの例を示します（ただし、この場合に限定されません）。

  - システムがコンテンツ フィルタのみを使用し、アンチスパム フィルタ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場合や、メッセージの添付ファイルが除去された場合
  - 本文スキャンが行われる前に、メッセージ分裂ポリシーによっていくつか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、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 Virus Outbreak 検疫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探します。

- **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）を識別することによってメッセージを検索します。
- **Email Security アプライアンス（ホスト）**：検索条件を特定の Email Security アプライアンスに絞り込みます。または、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について

中央集中型メッセージ トラッキングを設定するには、次の項を参照してください。

- 「Security Management 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とディセーブル化」（P.3-6）。
- 「メッセージ トラッキングでの機密情報へのアクセスのディセーブル化」（P.12-63）

トラッキング クエリーのセットアップについて

Security Management アプライアンスのトラッキング サービスにより、管理者は、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、ハード バウンスまたは配信されたかどうか等）などの指定した基準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るようになります。管理者はメッセージ トラッキングにより、メッセージ フローを詳しく表示できます。また、処理イベント、添付ファイル名、またはエンベロープとヘッダーの情報など、メッセージの詳細情報を確認するために、特定の電子メール メッセージについて「掘り下げる」こともできます。

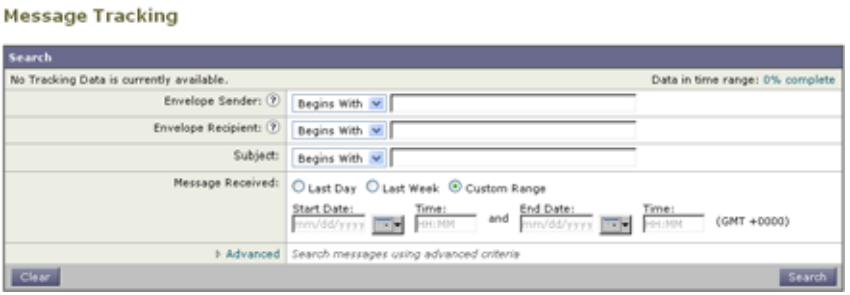
（注） このトラッキング コンポーネントにより個々の電子メール メッセージの詳細な情報が提供されますが、このコンポーネントを使用してメッセージの内容を読むことはできません。

指定した基準と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するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスのウィンドウで、[Email] > [Message Tracking] > [Message Tracking] を選択します。

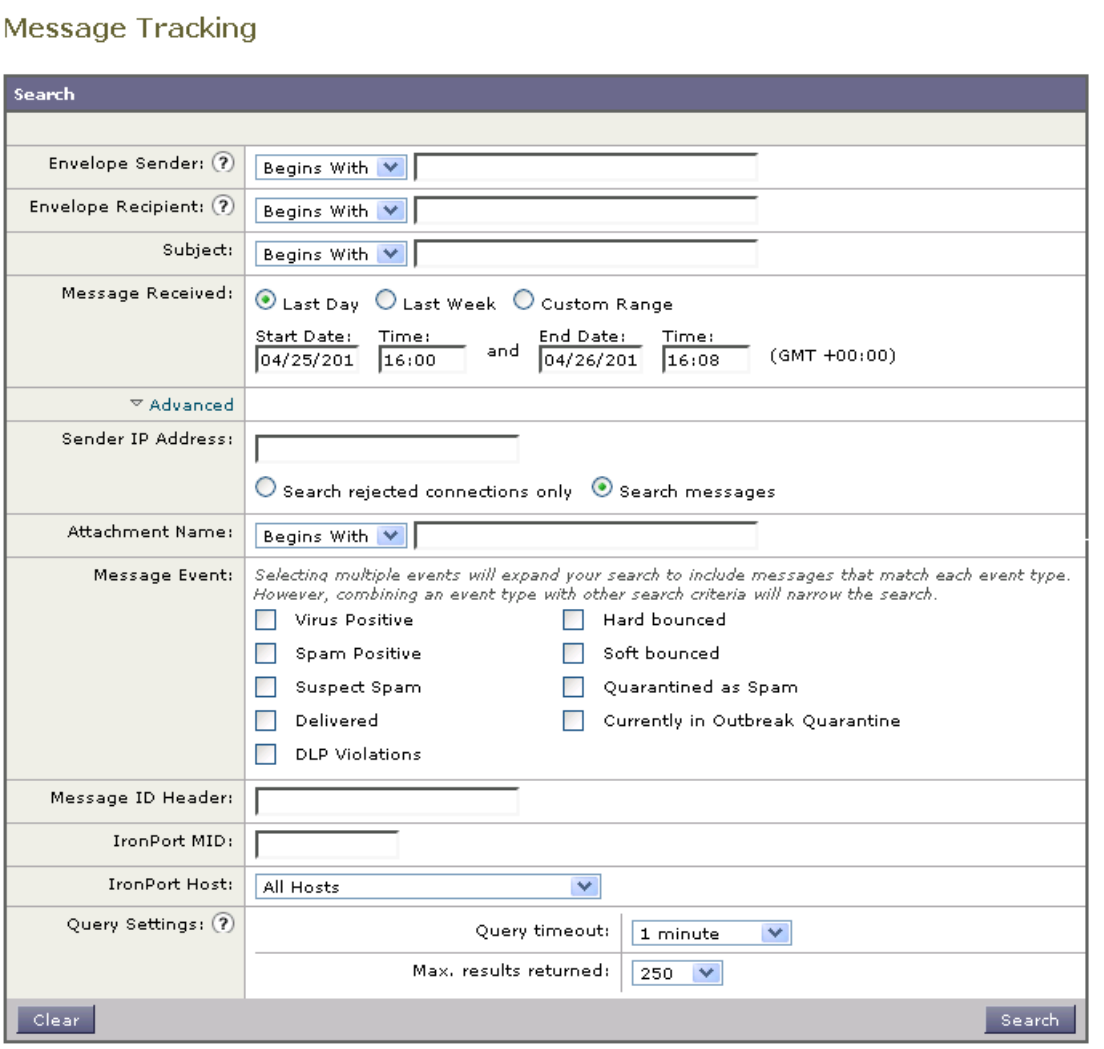
[Message Tracking] ページが表示されます。

図 6-1　[Message Tracking] ページ



必要に応じて、[Advanced] リンクをクリックして、トラッキング用の詳細オプションを表示します。

図 6-2　トラッキング用の詳細オプション



（注）　トラッキングでは、ワイルドカード文字や正規表現はサポートされません。トラッキングの検索では、大文字と小文字が区別されません。

ステップ 2　追跡する電子メール メッセージを特定します。

メッセージ トラッキング クエリーを実行する場合は、次の検索パラメータを使用します。

- [Envelope Sender] : [Begins With]、[Is]、または [Contains] を選択し、エンベロープ送信者として検索するテキスト文字列を入力します。有効なパラメータ値は、電子メール アドレス、ユーザ名、添付ファイル名、およびドメインです。
- [Envelope Recipient] : [Begins With]、[Is]、または [Contains] を選択し、エンベロープ受信者として検索するテキストを入力します。有効なパラメータ値は、電子メール アドレス、ユーザ名、添付ファイル名、およびドメインです。

  Email Security アプライアンスでエイリアス拡張用のエイリアス テーブルを使用する場合、検索では、元のエンベロープ アドレスの代わりに、拡張された受信者アドレスが検出されます。それ以外の場合、メッセージ トラッキング クエリーは、元のエンベロープ受信者アドレスを検出します。
- [Subject] : [Begins With]、[Is]、[Contains]、または [Is Empty] を選択し、メッセージ件名行に対して検索するテキスト文字列を入力します。

（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、クエリーの日付と時間範囲を指定します。過去 24 時間以内のメッセージを検索する場合は [Last Day] オプションを使用し、過去全 7 日間と検索当日の経過した時間までのメッセージを検索する場合は [Last 7 Days] オプションを使用します。

  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。終了日に現在の日付を指定し、終了時間を 23:59 に指定すると、クエリーは、現在の日付の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間を表示するときは、そのアプライアンスの現地時間で表示されます。

メッセージは、Email Security アプライアンスでログに記録され、Security Management アプライアンスで取得されてから結果に表示されます。ログのサイズとポーリングの頻度によっては、電子メール メッセージが送信された時間とそれがトラッキングとレポーティングの結果に実際に表示される時間との間にわずかな差が生じることがあります。

- [Sender IP Address]：送信元 IP アドレスを入力し、メッセージを検索するか、または拒否された接続のみ検索するかを選択します。
- [Message Event]：追跡するイベントを選択します。オプションには、[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ます）、[Hard Bounced]、[Soft Bounced]、[Currently in Outbreak Quarantine]、および [Quarantined as Spam] があります。トラッキング クエリーに追加するほとんどの条件とは異なり、イベントは「OR」演算子で追加できます。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] と Cisco [IronPort MID]：メッセージ ID ヘッダーと Cisco IronPort メッセージ ID（MID）のいずれかまたは両方のテキスト文字列を入力します。
- [Query Settings]：ドロップダウン メニューで、クエリーがタイムアウトになるまで実行する期間を選択します。オプションには、[1 minute]、[2 minutes]、[5 minutes]、[10 minutes]、および [No time limit] があります。また、クエリーから返される、結果の最大数（最大 1000 個）も選択します。
- [Attachment Name]：[Begins With]、[Is]、または [Contains] を選択し、検索する 1 つの添付ファイル名を ASCII または Unicode のテキスト文字列で入力します。

ステップ 3　[Search] をクリックします。

検索クエリーの実行

クエリーを実行してメッセージを検索するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスのウィンドウで、[Email] > [Message Tracking] > [Message Tracking] を選択します。

ステップ 2　必要な検索フィールドを入力します。

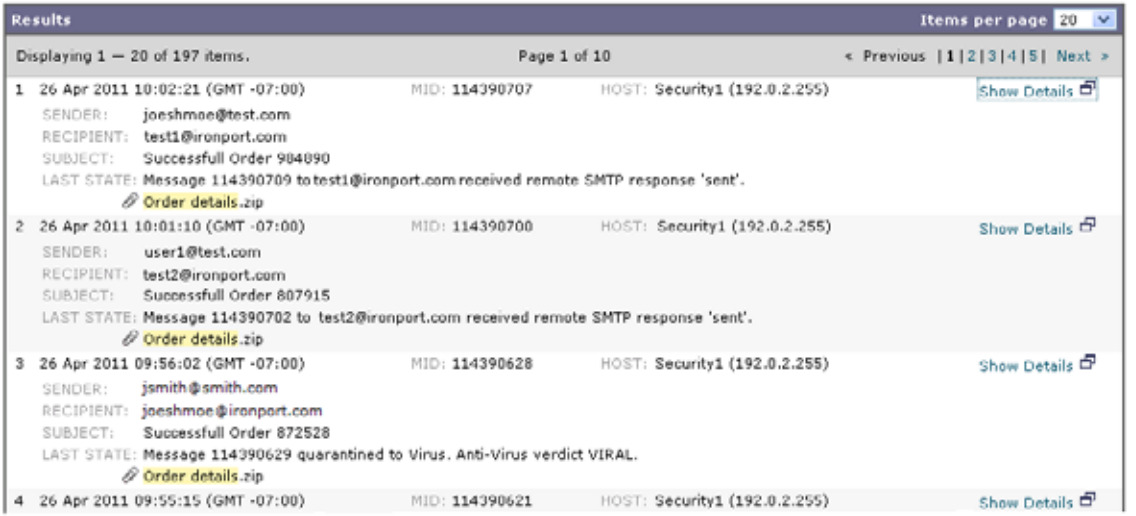
使用可能な検索フィールドの詳細については、「トラッキング クエリーのセットアップについて」（P.6-3）を参照してください。

すべてのフィールドを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、検索フィールドに指定された「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 3　[Search] をクリックし、クエリーを送信します。

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 6-3　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。

返される行数が [Items per page] フィールドで指定した値よりも大きい場合、結果は複数ページで表示されます。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。または、次の項で説明するように、結果セットを絞り込むことによって検索精度を高めることができます。

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代わりに、結果のリストにある行内の値をクリックすることによって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して、その日付に受信されたメッセージだけを表示します。

結果セットを絞り込むには、次の手順を実行します。

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、検索精度を高めます。

- Date and time
- Message ID（MID）
- Host（Email Security アプライアンス）
- Sender
- Recipient
- メッセージの件名行、または件名の最初の単語

ステップ 2　値をクリックして、検索を精密化します。

[Results] セクションには、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の一覧が表示されます。[Message Event] オプションを除き、クエリー条件は「AND」演算子で追加されます。結果セットのメッセージは、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）　受信者が 50 以上のメッセージは、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、将来のリリースの AsyncOS で解決される予定です。

メッセージごとに、日付/時刻、送信者、受信者、件名、最後の状態、メッセージに含まれる添付ファイル、Cisco IronPort メッセージ ID（MID）、および Cisco IronPort ホスト（Email Security アプライアンス）の情報が表示されます。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.6-10）を参照してください。

（注）　Security Management 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。さらに多く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てください。

メッセージの詳細

メッセージ ヘッダーや処理の詳細など、個々の電子メール メッセージに関する詳細情報を表示するには、検索結果リスト内の任意の項目に関して [Show Details] をクリックします。メッセージの詳細を表示し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.6-11）
- 「Sending Host Summary」（P.6-11）
- 「Processing Details」（P.6-12）

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] : Email Security アプライアンスがメッセージを受信した時間。

[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 Email Security 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、トラッキング結果内の件名行は「(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。メッセージが最初に作成されたときに、メッセージ内に挿入されます。「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] : メッセージを処理する Email Security 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。または、この値は「N/A」です。

[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] : 逆引き DNS（PTR）ルックアップで確認された送信元ホストのホスト名。

[IP Address] : 送信元ホストの IP アドレス。

[SBRS Score]：SenderBase 評価スコア。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ステータス イベントが表示されます。

エントリには、メール ポリシーの処理（アンチスパム スキャンやアンチウイルス スキャンなど）とメッセージ分割など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た場合、配信の詳細がここに表示されます。

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。

このコンテンツには、通常、企業の機密情報や、クレジット カード番号、健康診断結果などの個人情報が含まれるため、アプライアンスに対して管理者レベルのアクセス権を持たないユーザに対しては、このコンテンツへのアクセスをディセーブルにしたい場合があります。「メッセージ トラッキングでの機密情報へのアクセスのディセーブル化」（P.12-63）を参照してください。

CHAPTER 7

Cisco IronPort スパム検疫の管理

この章は、次の項で構成されています。

Cisco IronPort スパム検疫について

Cisco IronPort スパム検疫は、エンド ユーザ宛のスパムおよびその疑いのあるメッセージを保管するために使用される、特別な種類の検疫です。（エンド ユーザとはメール ユーザのことで、AsyncOS ユーザではありません）。*ローカルな* Cisco IronPort スパム検疫は、電子メール セキュリティ アプライアンスに常駐しています。メッセージを、別の Cisco IronPort アプライアンス（通常は Security Management アプライアンス）に常駐している*外部の* Cisco IronPort スパム検疫に送信することもできます。

（注）　*システム検疫*は Email Security 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検疫されたメッセージを保持します。

Cisco IronPort スパム検疫は「誤検出」（正規の電子メールがスパムとして検疫または削除されること）が問題になる組織にセーフガード メカニズムを提供します。Cisco IronPort スパム検疫を使用すると、メッセージをスパムであると最終的に判断する前に、エンド ユーザおよび管理者が、スパムのフラグが設定されたメッセージを確認できます。さらに、セーフリスト/ブロックリスト機能がイネーブルの場合、エンド ユーザはスパムのマークが付けられたメッセージに対して制御を実行できます。

（注）　指定されたユーザまたはユーザ グループに対してのみ、Cisco IronPort スパム検疫へのエンド ユーザ アクセスを実装できます。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 ユーザが検疫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。

スパムおよびその疑いのあるメッセージが検疫されたことをユーザに通知する電子メールを送信するように、AsyncOS を設定することができます。通知には、現在 Cisco IronPort スパム検疫エリアにあるそのユーザ宛のメッセージのサマリーが含まれます。ユーザはメッセージを表示し、電子メール受信トレイに送信するか、削除するかを決定できます。また、ユーザは検疫されたメッセージを検索できます。通知メッセージを通じて検疫にアクセスすることも、Web ブラウザを使用して直接検疫にアクセスすることもできます。（検疫にエンド 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 ユーザ検疫へのアクセスの設定」（P.7-8）を参照してください）。

デフォルトでは、Cisco IronPort スパム検疫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検疫スペースがすべて消費されることを避けるために、AsyncOS は Cisco IronPort スパム検疫から定期的にメールを削除します。

すべての Administrator レベルのユーザ（デフォルトの admin ユーザなど）は、Cisco IronPort スパム検疫へのアクセスおよび変更ができます。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検疫へのアクセス権が割り当てられているユーザは、検疫の内容の表示および管理ができますが、検疫設定の変更はできません。Cisco IronPort スパム検疫へのエンド 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、検疫エリアにある自分のメッセージにアクセスできます。

IronPort スパム検疫の設定

Cisco IronPort スパム検疫設定を Security Management アプライアンスで編集する前に、Cisco IronPort スパム検疫サービスを Security Management アプライアンスでイネーブルにする必要があります。サービスをイネーブルにする方法の詳細については、「Security Management アプライアンスでの Cisco IronPort スパム検疫のイネーブル化とディセーブル化」（P.3-8）を参照してください。

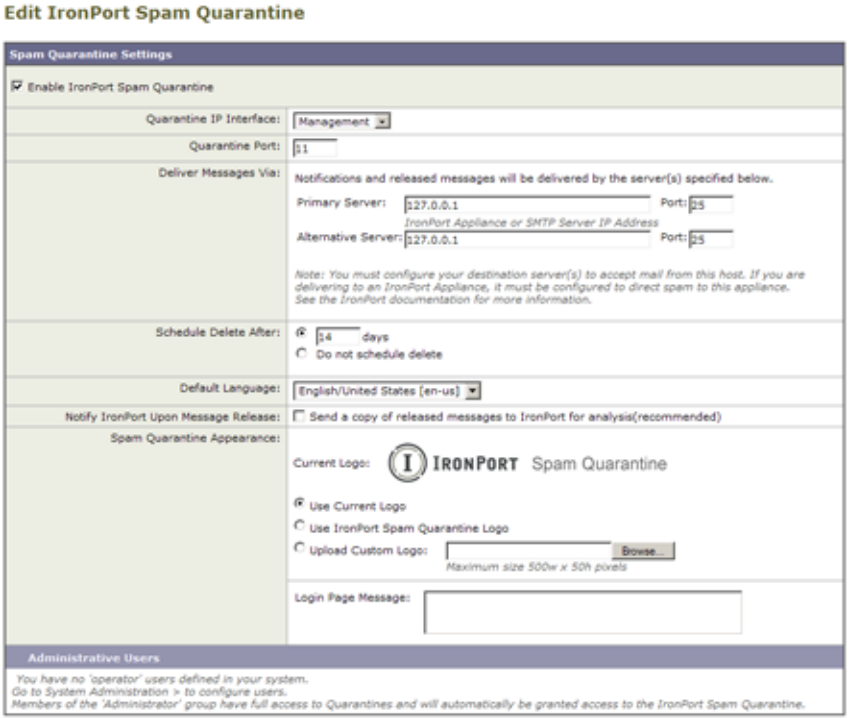
Cisco IronPort スパム検疫設定を編集するには、次の手順を実行します。

ステップ 1　Security Management 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　[Cisco IronPort Spam Quarantine Settings] セクションで [Edit Settings] をクリックします。

[Edit Cisco IronPort Spam Quarantine] ページが表示されます。

図 7-1　Cisco IronPort スパム検疫設定の編集



ステップ 3　[Quarantine IP Interface] セクションで、検疫に使用する適切な IP インターフェイスとポートを、ドロップダウン リストから指定します。

デフォルトでは、検疫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 Security Management アプライアンスのインターフェイスです。検疫ポートは、送信アプライアンスが外部検疫設定で使用しているポート番号です。

ステップ 4　[Deliver Messages Via] セクションで、メールを配信するプライマリ宛先および代替宛先を、対応するテキスト フィールドに入力します。

宛先は、SMTP、グループウェア サーバ、または別のアプライアンスです。

ステップ 5　[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、検疫を設定することを推奨します。検疫エリアの容量がいっぱいになると、古いメッセージから順に削除されます。

ステップ 6　[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 スパム検疫にアクセスしたときに表示される言語です。

ステップ 7　（任意）解放されたメッセージのコピーを分析のために Cisco IronPort に送信するには、[Notify Cisco IronPort upon Message Release] で、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、検疫を設定することを推奨します。

ステップ 8　（任意）[Spam Quarantine Appearance] セクションで、エンド ユーザが検疫を表示した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] を選択した場合、ユーザがログインして検疫されたメッセージを表示すると、Cisco IronPort スパム検疫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 スパム検疫のロゴが使用されます。

ステップ 9　（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 ユーザに対して検疫へのログイン プロンプトを表示するときに表示されます。

ステップ 10　オプションで、Cisco IronPort スパム検疫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 スパム検疫の管理ユーザの設定」（P.7-6）を参照してください。

ステップ 11　オプションで、エンド ユーザ 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 アクセスと通知の設定」（P.7-7）を参照してください。

ステップ 12　変更を送信し、保存します。

Cisco IronPort スパム検疫の管理ユーザの設定

Cisco IronPort スパム検疫のメッセージを管理する役割を、他のユーザに分散できます。他のユーザがこの機能にアクセスできるようにするには、このセクションの手順を使用してください。

Operator、Read-Only Operator、Help Desk、Guest のいずれかのロールが割り当てられているか、スパム検疫へのアクセス権が含まれているカスタム ユーザ ロールが割り当てられたユーザが、スパム検疫のメッセージを管理できます。

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、常にスパム検疫にアクセスできるので、この手順を使用してスパム検疫機能に関連付ける必要はありません。

（注） Administrator レベルでないユーザは、スパム検疫エリアのメッセージにアクセスできますが、検疫設定の編集はできません。Administrator レベルのユーザは、メッセージへのアクセスと設定の編集ができます。

ユーザがスパム検疫を管理できるようにするには、次の手順を実行します。

ステップ 1　ユーザを作成し、そのユーザにスパム検疫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.12-43）を参照してください。

ステップ 2　Security Management 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。[Edit Spam Quarantine] ページが表示されます。

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　スパム検疫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　[Submit] をクリックし、変更内容を確定させます。

エンド ユーザ アクセスと通知の設定

基本的な Cisco IronPort スパム検疫設定の他に、検疫のその他の設定ができます。追加の設定は、[Edit Cisco IronPort Spam Quarantine] ページの [Spam Quarantine Settings] セクションの下に表示されます。

次の追加設定ができます。

- [End user access to the quarantine] : 詳細については、「エンド ユーザ検疫へのアクセスの設定」（P.7-8）を参照してください。
- [Spam notifications] : 詳細については、「スパム通知のイネーブル化」（P.7-9）を参照してください。

追加の設定にアクセスするには、[Management Appliance] > [Centralized Services] > [Spam Quarantine] を選択して、[Cisco IronPort Spam Quarantine Settings] セクションの [Edit Settings] ボタンをクリックします。[Edit Cisco IronPort Spam Quarantine] ページをスクロール ダウンして、追加の設定を表示します。

図 7-2　Cisco IronPort スパム検疫の追加設定の編集

（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 ユーザ検疫へのアクセスの設定

Cisco IronPort スパム検疫へのエンド ユーザ アクセスを設定するには、次の手順を実行します。

ステップ 1　Security Management 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。[Edit Cisco IronPort Spam Quarantine] ページが表示されます。

ステップ 3　[Edit Cisco IronPort Spam Quarantine] ページの [Enable End-User Quarantine Access] チェックボックスをオンにします。

図 7-3　Cisco IronPort スパム検疫へのエンド ユーザ アクセスのイネーブル化

ステップ 4　エンド ユーザが検疫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、または認証なしを使用できます。

- [Mailbox authentication] : 認証用の LDAP がないサイトの場合、検疫は、ユーザの電子メール アドレスとパスワードの正当性を、それらのユーザのメールボックスが保持されている標準ベースの IMAP または POP サーバに対して検証できます。Web UI にログインしたときに、ユーザは電子メール アドレスとパスワードを入力します。検疫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、検疫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検疫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 サーバがバナー内で APOP サポートをアドバタイズしている場合、セキュリティ上の理由から（つまり、パスワードが平文で送信されるのを回避するために）、アプライアンスは APOP のみを使用します。一部のユーザに対して APOP がサポートされていない場合は、APOP をアドバタイズしないように POP サーバを設定する必要があります。

- [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] 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.10-3）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 スパム検疫へのエンド 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検疫にアクセスでき、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 5　検疫からメッセージを解放する前に、メッセージ本文を表示するかどうかを指定します。このチェックボックスをオンにすると、ユーザは、Cisco IronPort スパム検疫ページからメッセージ本文を表示できなくなります。代わりとして、検疫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 6　[Submit] をクリックし、[Commit] をクリックして変更を確定します。

スパム通知のイネーブル化

スパム通知とは、Cisco IronPort スパム検疫内にメッセージが存在するときに、エンド 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、そのユーザ宛の検疫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検疫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、[Edit Cisco IronPort Spam Quarantine] ページで指定され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 またはメールボックス認証を使用せずに検疫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検疫にアクセスします（その検疫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、ユーザは検疫の 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検疫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検疫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 アクセスと通知の設定」（P.7-7）を参照してください。

スパム通知を設定するには、次の手順を実行します。

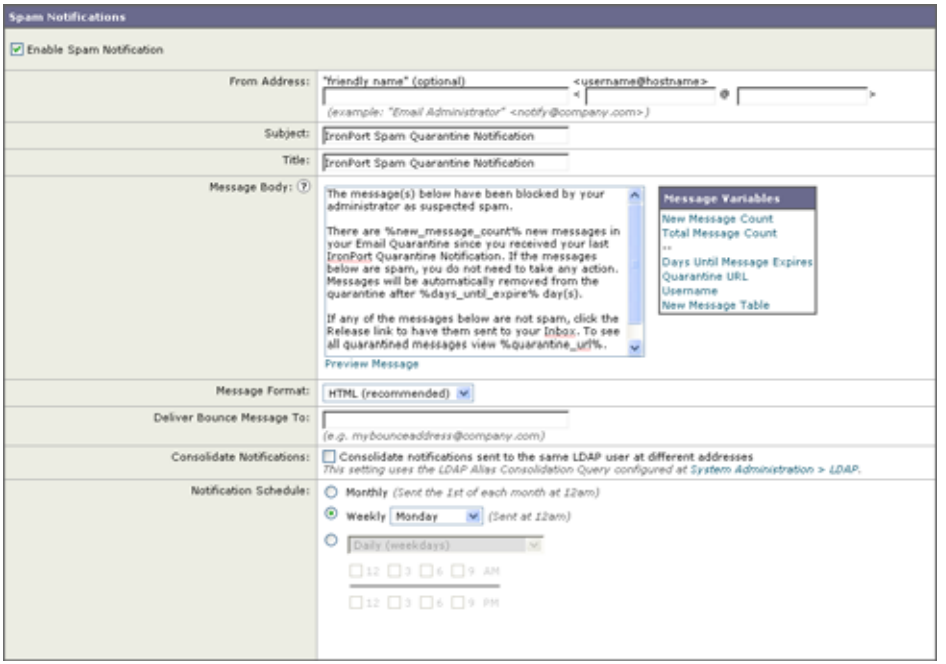
ステップ 1　Security Management アプライアンスで、[Management Appliance] > [Centralized Services] > [Spam Quarantine] を選択します。

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。

[Edit Cisco IronPort Spam Quarantine] ページが表示されます。

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。

図 7-4　スパム通知の設定



ステップ 4　通知の差出人アドレスを入力します。ユーザは、このアドレスを、自分の電子メール クライアントでサポートされる「ホワイトリスト」に追加できます。

ステップ 5　通知の件名を入力します。

ステップ 6　通知のカスタマイズされたタイトルを入力します。

ステップ 7　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 ユーザ検疫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%）：検疫にログインし、メッセージを表示するための URL
- [Username]（%username%）
- [New Message Table]（%new_quarantine_messages%）：検疫エリア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 8　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 9　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 10　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 11　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 12　[Submit] をクリックし、[Commit] をクリックして変更を確定します。

スパムを転送する電子メール セキュリティ アプライアンスの設定

Security Management アプライアンスで Cisco IronPort スパム検疫を設定した後、Email Security アプライアンスが Security Management アプライアンスにスパムまたはその疑いのあるメッセージを転送するようにシステムで設定する必要があります。

スパムを転送するように Email Security アプライアンスを設定するには、次のタスクを実行します。

- **外部検疫の設定**：Email Security アプライアンスの外部検疫設定で、Security Management アプライアンス名および Cisco IronPort スパム検疫用の接続情報を指定する必要があります。詳細については、「外部検疫の設定」（P.7-13）を参照してください。

- **管理対象アプライアンスの追加または更新**：Email Security アプライアンスを Security Management アプライアンスの管理対象アプライアンスとして追加または更新する必要があります。また、Email Security アプライアンスからのスパムを検疫するオプションを選択する必要があります。詳細については、「管理対象アプライアンスの追加と更新、および検疫スパム オプションの使用」（P.7-14）を参照してください。

外部検疫の設定

Email Security アプライアンスで Security Management アプライアンスの Cisco IronPort スパム検疫を使用するには、Email Security アプライアンスの外部検疫を設定する必要があります。

（注）　これまで、Email Security アプライアンスに別の外部スパム検疫を設定していた場合は、まず、その外部スパム検疫設定をディセーブルにする必要があります。

外部検疫を設定するには、次の手順を**すべての** Email Security アプライアンスで実行する必要があります。

ステップ 1　[Security Services] > [External Spam Quarantine] ページで、[Configure] ボタンをクリックします。

ステップ 2　チェックボックスを選択して、外部スパム検疫をイネーブルにします。

ステップ 3　Cisco IronPort スパム検疫の名前を入力します。検疫がある Security Management 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 4　Security Management アプライアンスの管理インターフェイスの IP アドレスを入力します。

ステップ 5　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。ここで入力するポート番号は、Security Management 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 [Edit Cisco IronPort Spam Quarantine] ページで入力した検疫ポート番号と同じにする必要があります。詳細については、「IronPort スパム検疫の設定」（P.7-3）を参照してください。

ステップ 6　オプションで、チェックボックスを選択し、セーフリスト/ブロックリスト機能をイネーブルにします。セーフリスト/ブロックリスト機能をイネーブルにする場合は、ブロックリストに含まれている送信者からのメッセージを検疫するか、

削除するかを選択します。セーフリスト/ブロックリスト機能の詳細については、「エンド ユーザのセーフリスト/ブロックリスト機能のイネーブル化」（P.7-19）を参照してください。

ステップ 7　[Submit] をクリックし、[Commit] をクリックして変更を確定します。

管理対象アプライアンスの追加と更新、および検疫スパム オプションの使用

Email Security アプライアンスで Security Management アプライアンスの Cisco IronPort スパム検疫を使用するには、Security Management アプライアンスの管理対象アプライアンスとして追加する必要があります。または、すでに Email Security 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は、検疫スパム オプションを使用するように管理対象アプライアンス設定を更新する必要があります。

Security Management アプライアンスで [Management Appliance] > [Centralized Services] > [Security Appliances] を選択し、管理対象 Email Security アプライアンスを追加します。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」（P.3-11）を参照してください。

注意　管理対象アプライアンスを追加するときに、アプライアンスからのスパムを検疫するようにオプションを選択してください。

すでに Email Security アプライアンスが Security Management アプライアンスの管理対象アプライアンスとして存在する場合は、検疫スパム オプションを使用するように管理対象アプライアンス設定を更新する必要があります。

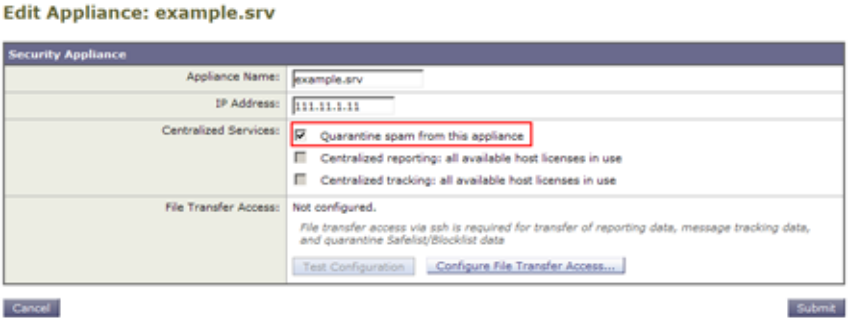
検疫スパム オプションを使用するように管理対象アプライアンス設定を更新するには、次の手順を実行します。

ステップ 1　Security Management 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　セキュリティ アプライアンスのリストで、Email Security アプライアンスの名前をクリックします。

ステップ 3　[Edit Appliance: <appliance_name>] ページで、図 7-5 に示すように、アプライアンスからのスパムを検疫するオプションを選択します。

図 7-5　スパムを検疫するための管理対象アプライアンスの編集



ステップ 4　[Submit] をクリックし、[Commit] をクリックして変更を確定します。

Cisco IronPort スパム検疫内のメッセージの管理

ここでは、管理者が Cisco IronPort スパム検疫内のメッセージを管理する方法について説明します。管理者が検疫を表示する場合、その検疫エリア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 スパム検疫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 スパム検疫にアクセスし、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 スパム検疫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

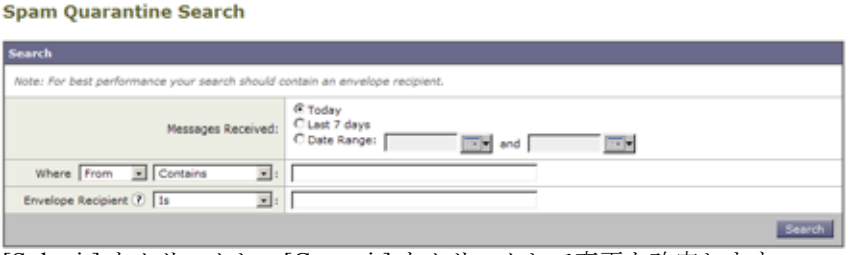
Cisco IronPort スパム検疫内のメッセージにアクセスするには、次の手順を実行します。

ステップ 1　Security Management 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] リンクをクリックします。

[Spam Quarantine Search] ページが表示されます。

図 7-6　[Spam Quarantine Search] ページ



ステップ 3　[Submit] をクリックし、[Commit] をクリックして変更を確定します。

Cisco IronPort スパム検疫内でのメッセージの検索

Cisco IronPort スパム検疫内のメッセージを検索するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Email] > [Message Quarantine] > [Spam Quarantine] を選択します。

ステップ 2　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 3　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 4　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 5　[Search] をクリックします。

検索基準に一致するメッセージがページの [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 スパム検疫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 スパム検疫内のメッセージの表示

メッセージのリストにより、Cisco IronPort スパム検疫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検疫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 スパム検疫では、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 スパム検疫内のメッセージの配信

メッセージを解放して配信するには、メッセージの横のチェックボックスをオンにして [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 スパム検疫からのメッセージの削除

Cisco IronPort スパム検疫では、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 スパム検疫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 スパム検疫内のすべてのメッセージを削除するには、検疫をディセーブルにして（「Security Management アプライアンスでの Cisco IronPort スパム検疫のイネーブル化とディセーブル化」（P.3-8）を参照）、[Management Appliance] > [Centralized Services] > [Spam Quarantine] ページの [Delete All] リンクをクリックします。

エンド ユーザのセーフリスト/ブロックリスト機能のイネーブル化

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。ブロックリストによって、その他のユーザおよびドメインからのメールは常にスパムとして処理されます。セーフリストとブロックリストの設定は、Cisco IronPort スパム検疫から設定されます。そのため、Cisco IronPort スパム検疫をイネーブルにし、この機能を使用するように設定する必要があります。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、Email Security 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 Security Management 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 Email Security 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.7-22）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.7-21）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 スパム検疫に関連するため、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 User 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は、自分のセーフリストとブロックリストの設定がそのリスナー上で受信されたメールに適用されなくなります。同様に、一部のメッセージ受信者についてアンチスパム スキャンをスキップするメールフロー ポリシーを作成すると、それらの受信者は、自分のセーフリストとブロックリストの設定が適用されなくなります。

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.7-23）を参照してください。

セーフリスト/ブロックリスト設定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 スパム検疫をイネーブル化する必要があります。Cisco IronPort スパム検疫のイネーブル化の詳細については、「Security Management アプライアンスでの Cisco IronPort スパム検疫のイネーブル化とディセーブル化」（P.3-8）を参照してください。

Security Management アプライアンスでセーフリスト/ブロックリスト機能をイネーブル化および設定するには、次の手順を実行します。

ステップ 1　Security Management 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、ユーザが各セーフリストおよびブロックリストに含めることのできるアドレスまたは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　更新の頻度を選択します。この値によって、AsyncOS がシステムにある Email Security 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　[Submit] をクリックし、[Commit] をクリックして変更を確定します。

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、Security Management 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。

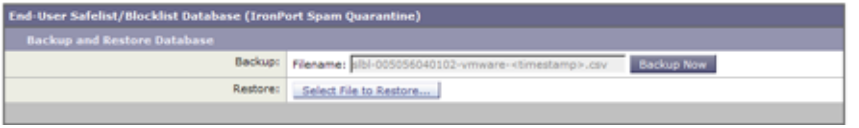
データベースをバックアップすると、アプライアンスによって、.csv ファイルが次の命名規則に従って `/configuration` ディレクトリに保存されます。

slbl-<serial number>-<timestamp>.csv

GUI から、次の方法を使用して、データベースのバックアップおよび復元を実行できます。

ステップ 1　Security Management 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] セクションに移動します。



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　データベースを復元するには、[Select File to Restore] をクリックします。

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設定とデータベースの同期

Security Management 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 Security Management 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」（P.3-11）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「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、Email Security 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 データベースに対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場合、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裂します。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 に送信されるメッセージは、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検疫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、Email Security アプライアンスの外部スパム検疫設定で指定します。詳細については、「外部検疫の設定」（P.7-13）を参照してください。

メッセージを検疫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、最終的に検疫されます。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。管理者は、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.12-82）を参照してください。

ログ ファイルの詳細については、第 13 章「ロギング」（P.1）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。ユーザは、この送信者をユーザのブロックリストに追加して、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することができます。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 スパム検疫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検疫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 スパム検疫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

各エントリは、次の形式でセーフリストとブロックリストに追加できます。

- user@domain.com
- server.domain.com
- domain.com

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

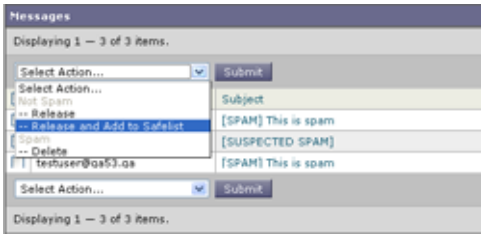
エンド ユーザは、次の 2 つの方法で送信者をセーフリストに追加できます。Cisco IronPort スパム検疫から、グラフィカル ユーザ インターフェイスの右上にある [Options] メニューをクリックし、[Safelist] を選択して、手動で送信者をセーフリストに追加できます。

図 7-7　エンド ユーザ検疫のセーフリスト

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 スパム検疫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 スパム検疫に保持されている場合、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 7-8　　エンド ユーザ検疫のセーフリスト



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 ユーザ検疫から [Options] > [Blocklist] を選択します。

図 7-9　　ブロックリストへの送信者の追加

エンド ユーザ検疫から、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。

Email Security 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検疫されます。

CHAPTER 8

Web セキュリティ アプライアンスの管理

この章は、次の項で構成されています。

Web セキュリティ アプライアンスの管理の概要

AsyncOS for Security Management を使用すると、地理的に離れたネットワークにわたって、均一の Web セキュリティ ポリシーおよびカスタム URL カテゴリを適用できます。Web セキュリティ アプライアンスの設定は、Security Management アプライアンスの GUI から直接編集および公開できます。

Web セキュリティ アプライアンスの管理プロセスは次のとおりです。

ステップ 1 **Web セキュリティ アプライアンス。**AsyncOS 7.1 for Web にアップグレードします。『*Cisco IronPort AsyncOS 7.0 for Web User Guide*』または『*Cisco IronPort AsyncOS 7.1 for Web User Guide*』を参照してください。

ステップ 2 **Web セキュリティ アプライアンス。**ネットワーキング、認可、およびセキュリティ サービスを設定します。『*Cisco IronPort AsyncOS 7.1 for Web User Guide*』を参照してください。

「Configuration Master の使用に関する重要事項」（P.8-3）の設定要件を満たすようにしてください。

ステップ 3　**Web セキュリティ アプライアンス。**ポリシーの設定とテストを行います。『*Cisco IronPort AsyncOS 7.1 for Web User Guide*』を参照してください。

ステップ 4　**（任意）Web セキュリティ アプライアンス。**希望どおりの設定になったら、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、Security Management アプライアンスの Configuration Master の設定を迅速化できます）。『*Cisco IronPort AsyncOS 7.1 for Web User Guide*』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 2-5（WSA のある導入環境のみ）Configuration Master の互換性」（P.2-36）を参照してください。

ステップ 5　**Security Management 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ます。「Security Management アプライアンスでのサービスのイネーブル化」（P.3-3）を参照してください。

ステップ 6　**Security Management アプライアンス。**Web セキュリティ アプライアンスを Security Management アプライアンスに追加します。「管理対象アプライアンスの追加」（P.3-11）を参照してください。

ステップ 7　**Security Management アプライアンス。**[Security Services] の設定を編集して、Web セキュリティ アプライアンスに現在設定されている状態に合わせます。「セキュリティ サービスの設定の編集」（P.8-4）を参照してください。

ステップ 8　**Security Management アプライアンス。**Configuration Master を初期化します。「Configuration Master の初期化」（P.8-8）を参照してください。

ステップ 9　**Security Management 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」（P.8-8）を参照してください。

ステップ 10　**Security Management アプライアンス。**ポリシー、カスタム URL カテゴリ、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。「Configuration Master の設定」（P.8-10）を参照してください。

ステップ 11　**Security Management アプライアンス。**必要に応じて、Security Management アプライアンスのバックアップ、復元、アップグレードを行います。「Security Management アプライアンスのバックアップ」（P.12-8）を参照してください。

ステップ 12　**Security Management アプライアンス。**設定を Web セキュリティ アプライアンスに公開します。「Web セキュリティ アプライアンスへの設定の公開」（P.8-14）を参照してください。

Configuration Master の操作

Configuration Master を使用すると、特定の設定（特に、Web セキュリティ アプライアンスの [Web Security Manager] メニューの下の設定）を Web セキュリティ アプライアンスに公開できます。

AsyncOS for Security Management では、複数の Configuration Master が提供されるため、各種の機能を含むさまざまなバージョンの AsyncOS for Web Security を Web セキュリティ アプライアンスが実行している、異種の導入環境を集中管理することができます。

Security Management アプライアンスの GUI の [Web] セクション内にあるそれぞれの Configuration Master には、特定バージョンの AsyncOS for Web Security の設定が格納されています。

Configuration Master を設定するためのオプションについては、「Configuration Master の設定」（P.8-10）を参照してください。

Configuration Master の使用に関する重要事項

（注）　複数の Web セキュリティ アプライアンスがある場合は、それぞれの Web セキュリティ アプライアンスをチェックし、同名のレルムの設定が同一の場合を除いて、[Network] > [Authentication] のすべてのレルム名がアプライアンス間で一意になっていることを確認します。

（注）　Security Management アプライアンスは、互換性のある AsyncOS のバージョンを実行する Web セキュリティ アプライアンスにのみ Configuration Master を公開できます（たとえば、Web セキュリティ アプライアンスが AsyncOS 6.3 を実行している場合、それを Configuration Master 6.3 に割り当てます）。「管理対象アプライアンスの追加」（P.3-11）を参照してください。

セキュリティ サービスの設定の編集

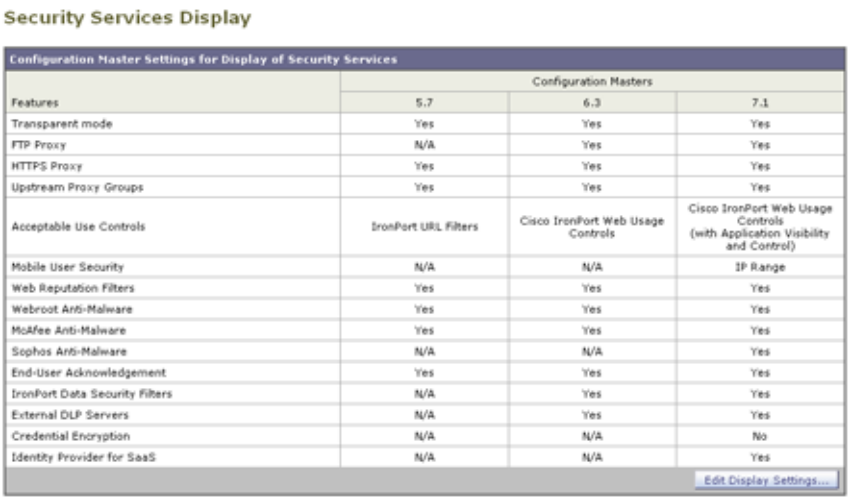
Configuration Master の使用を開始する前に、セキュリティ サービスの設定を編集して、Web セキュリティ アプライアンスの設定を反映するよう Configuration Master の表示をカスタマイズします。これらの設定により、Security Management アプライアンスでの設定に適切な機能を使用できるようになります。

デフォルトでは、[Web] > [Utilities] > [Security Services Display] ページに、すべての Configuration Master の設定が表示されます。機能に対して [N/A] とある場合、その機能は、そのバージョンの AsyncOS for Web Security で使用できないことを示します。

[Security Services Display] ページで選択されていない機能は、それらの機能が、Web セキュリティ アプライアンスでイネーブルにされていても、Configuration Master を使用して設定することはできません。

警告　**Configuration Master の設定を管理対象の Web セキュリティ アプライアンスに対して適切に公開するには、Configuration Master のセキュリティ サービスの設定が、Web セキュリティ アプライアンスでの設定と一致している必要があります。Configuration Master のセキュリティ サービスの設定を変更しても、Web セキュリティ アプライアンスの設定が自動的に変更されることはありません。Configuration Master の公開を行う前に、[Web] > [Utilities] > [Web Appliance Status] ページをチェックして、セキュリティ サービスの設定と Web セキュリティ アプライアンスでの設定の間に不一致がないか調べることをお勧めします（「Web セキュリティ アプライアンスのステータスの表示」（P.8-23）を参照）。不一致に気づいた場合は、セキュリティ サービスの設定（「セキュリティ サービスの設定の編集」（P.8-4）を参照）、または Web セキュリティ アプライアンスでの設定のいずれかを変更する必要があります。**

図 8-1　[Security Services Display] ページ



Security Services Display

Configuration Master Settings for Display of Security Services

Features	Configuration Masters 5.7	6.3	7.1
Transparent mode	Yes	Yes	Yes
FTP Proxy	N/A	Yes	Yes
HTTPS Proxy	Yes	Yes	Yes
Upstream Proxy Groups	Yes	Yes	Yes
Acceptable Use Controls	IronPort URL Filters	Cisco IronPort Web Usage Controls	Cisco IronPort Web Usage Controls (with Application Visibility and Control)
Mobile User Security	N/A	N/A	IP Range
Web Reputation Filters	Yes	Yes	Yes
Webroot Anti-Malware	Yes	Yes	Yes
McAfee Anti-Malware	Yes	Yes	Yes
Sophos Anti-Malware	N/A	N/A	Yes
End-User Acknowledgement	Yes	Yes	Yes
IronPort Data Security Filters	N/A	Yes	Yes
External DLP Servers	N/A	Yes	Yes
Credential Encryption	N/A	N/A	No
Identity Provider for SaaS	N/A	N/A	Yes

Edit Display Settings...

セキュリティ サービスの設定を編集するには、次の手順を実行します。

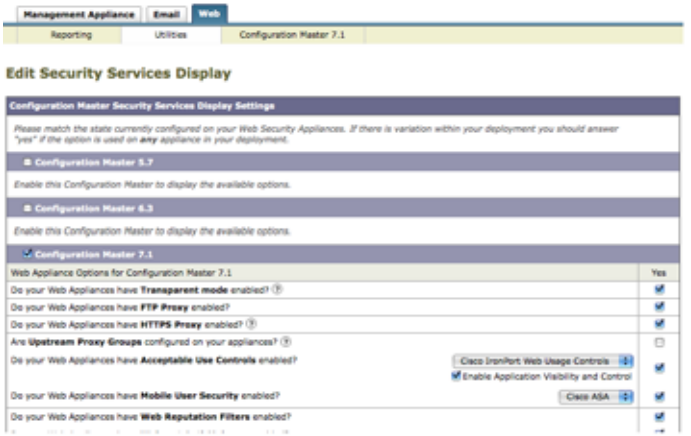
ステップ 1　Security Management アプライアンスで、[Web] > [Utilities] > [Security Services Display] を選択します。

ステップ 2　[Edit Settings] をクリックします。

[Edit Security Services Display] ページが表示され、Configuration Master に表示される機能がリストされます。

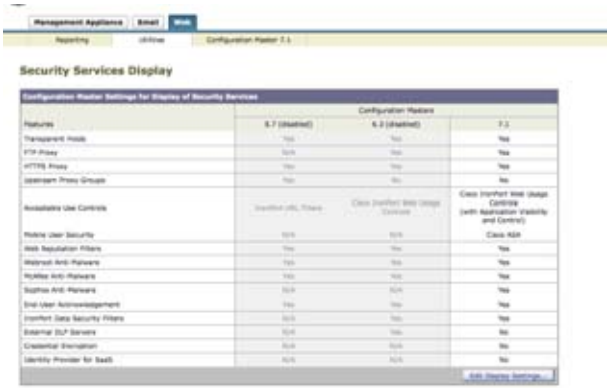
（注）　Web Proxy は機能としてリストされていません。Web Proxy は Web セキュリティ アプライアンスの管理対象ポリシー タイプのいずれかを実行するために、イネーブルになっていると見なされるからです。Web Proxy がディセーブルの場合は、Web セキュリティ アプライアンスに公開されるすべてのポリシーが無視されます。

ステップ 3　（任意）Configuration Master のいずれかを使用しない場合は、それを非表示にするために、[Edit Security Services Display] ページで対応する Configuration Master のチェックボックスをオフにします。



（注） Configuration Master を非表示にすると、それに対するすべての参照が、対応する [Configuration Master] タブを含む GUI から削除されます。Configuration Master を使用する保留中の公開ジョブは削除され、非表示のすべての Configuration Master に割り当てられている Web セキュリティ アプライアンスが、未割り当て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。

たとえば、Configuration Master 5.7 および 6.3 がディセーブルにされている [Security Services Display] ページは、次のようになります。



ステップ 4　機能が 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かどうかを反映するため、[Yes] チェックボックスをオンまたはオフにします。導入環境内で設定が一定でない場合は、導入された*いずれか*のアプライアンスで機能がイネーブルにされていれば、このチェックボックスを選択します。

機能は次のとおりです。

- トランスペアレント プロキシ 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。
- FTP プロキシ。*Configuration Master 6.3 および 7.1 のみ。*
- 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。使用するサービスとして、Cisco IronPort URL Filters または Cisco IronPort Web Usage Controls を選択します。
- Web レピュテーション フィルタ。
- Webroot アンチマルウェア。
- McAfee アンチマルウェア。
- エンド ユーザ承認。
- Cisco IronPort データ セキュリティ フィルタ。*Configuration Master 6.3 および 7.1 のみ。*
- 外部 DLP サーバ。*Configuration Master 6.3 および 7.1 のみ。*

ステップ 5　[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 6　[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 7　[Submit] をクリックし、[Commit] をクリックして変更を確定します。

Configuration Master の初期化

ステップ 1　メイン Security Management アプライアンスで、[Web] > [Utilities] > [Configuration Masters] を選択します。

[Configuration Master] ページが表示されます。

ステップ 2　[Options] カラムの [Initialize] をクリックします。

ステップ 3　[Configuration Master] ページで次の操作を実行します。

- 以前のリリースに対する既存の Configuration Master があり、その同じ設定を新しい Configuration Master に使用するか、その設定で開始する場合は、[Copy Configuration Master] を選択します。

  Configuration Master のバージョンの互換性については、「表 2-5（WSA のある導入環境のみ）Configuration Master の互換性」（P.2-36）を参照してください。
- そうでない場合は、[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。

Web セキュリティ アプライアンスと Configuration Master の関連付け

集中管理するそれぞれの Web セキュリティ アプライアンスについて、ポリシー設定を、そのアプライアンスの AsyncOS バージョンと一致する Configuration Master に関連付ける必要があります。たとえば、Web セキュリティ アプライアンスが AsyncOS 6.3 for Web を実行中の場合は、それを Configuration Master 6.3 に関連付ける必要があります。これは、Web セキュリティ アプライアンスを Security Management アプライアンスに追加するとき（「管理対象アプライアンスの追加」（P.3-11）を参照）、または [Web] > [Utilities] > [Configuration Masters] ページで行うことができます。

このリリースでは、5.7、6.3、7.1 の 3 つの Configuration Master が使用可能です。

（注） Web セキュリティ アプライアンスを Configuration Master に関連付けても、新しい設定がアプライアンスに自動的に公開されることはありません。設定は、手動でアプライアンスに公開する必要があります。「Web セキュリティ アプライアンスへの設定の公開」（P.8-14）を参照してください。

アプリケーションを Configuration Master に関連付けるには、次の手順を実行します。

ステップ 1　メイン Security Management アプライアンスで、[Web] > [Utilities] > [Configuration Masters] を選択します。

[Configuration Master] ページが表示されます。

ステップ 2　[Edit Appliance Assignment List] をクリックして、[Configuration Master Assignments] ページを表示します。

ステップ 3　関連付けるアプライアンスの行でクリックし、[Masters] カラムにチェックマークを入れます。

（注） Configuration Master が非表示の場合、ページにその Configuration Master のカラムは表示されません。非表示の Configuration Master をイネーブルにするには、[Web] > [Utilities] > [Security Services Display] に移動します。「セキュリティ サービスの設定の編集」（P.8-4）を参照してください。

ステップ 4　[Submit] をクリックし、[Commit] をクリックして変更を確定します。

（注） Configuration Master のアップグレード方法、またはアプライアンスに関連付ける方法の例については、「例 5：既存の Security Management アプライアンスでの新しい Configuration Master へのアップグレード」（P.D-16）を参照してください。

Configuration Master の設定

Configuration Master を設定するには、次のようにいくつかの方法があります。

- 以前のリリースからのアップグレードの場合：以前の既存の Configuration Master を新しい Configuration Master のバージョンにコピーまたはインポートします。
- Web セキュリティ アプライアンスをすでに設定してあり、同じ設定を複数の Web セキュリティ アプライアンスに使用する場合：すでに設定済みの 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 ファイルをインポートします。

  「Configuration Master への既存の Web セキュリティ アプライアンス設定の取り込み」（P.8-10）を参照してください。
- ポリシー、URL カテゴリ、バイパス設定を Web セキュリティ アプライアンスでまだ設定していない場合は、該当する Configuration Master を Security Management アプライアンスで設定します。

  詳細については、「Configuration Master を使用した Web セキュリティ機能の設定について」（P.8-12）を参照してください。

（注） Configuration Master に加えた変更は、編集した設定を公開するまで、その Configuration Master に割り当てられた Web セキュリティ アプライアンスに適用されません。「Web セキュリティ アプライアンスへの設定の公開」（P.8-14）を参照してください。

Configuration Master への既存の Web セキュリティ アプライアンス設定の取り込み

すでに実際に設定があり、それを Web セキュリティ アプライアンスの 1 つから使用する場合には、コンフィギュレーション ファイルを Security Management アプライアンスにインポートして、Configuration Master にデフォルトのポリシー設定を作成できます。Configuration Master は、同じバージョンの Web セキュリティ アプライアンスからのコンフィギュレーション ファイルを受け入れます。

たとえば、Configuration Master に XML ファイルをロードする場合、そのファイルは、Configuration Master 自体と同じバージョンからのものにする必要があります。つまり、6.3 の Configuration Master に取り込むことができるのは、6.3 マシンからのファイルのみです。また、7.1 の Configuration Master に取り込むことができるのは、7.1 マシンからのファイルのみです。

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 2-5（WSA のある導入環境のみ）Configuration Master の互換性」（P.2-36）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　メイン Security Management 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] を選択します。

[Import Web Configuration] ページが表示されます。この例では、Configuration Master 7.1 が選択されています。

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。

図 8-2　[Import Web Configuration] ページ

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] をクリックしてインポート プロセスに進むか、[Cancel] をクリックします。

Configuration Master を使用した Web セキュリティ機能の設定について

Web セキュリティ アプライアンスの機能を Security Management アプライアンスの GUI で直接設定して、その設定変更を、Configuration Master に割り当てられている Web セキュリティ アプライアンスに公開することができます。

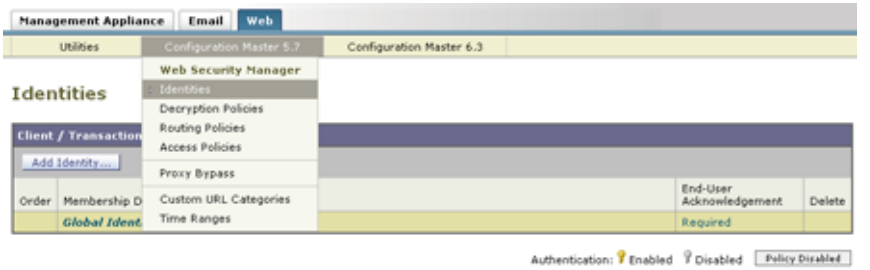
Security Management アプライアンスの GUI の [Web] セクション内にあるそれぞれの Configuration Master には、特定バージョンの AsyncOS for Web Security の設定が格納されています。このリリースの AsyncOS for Security Management には、AsyncOS 5.7 for Web Security、AsyncOS 6.3 for Web Security、および AsyncOS 7.1 for Web Security をサポートしている Configuration Master が含まれています。

Configuration Master 5.7 の使用

Configuration Master 5.7 を使用すると、ID、復号化ポリシー、ルーティング ポリシー、アクセス ポリシー、および時間ベースのポリシーを設定したり、Web プロキシをバイパスしたり、カスタム URL カテゴリを作成したりできます。

これらの機能を Configuration Master で設定する方法は、Web セキュリティ アプライアンスで設定する方法と同じです。『*Cisco IronPort AsyncOS for Web User Guide*』を参照してください。

図 8-3　Configuration Master 5.7



Configuration Master 6.3 の使用

Configuration Master 6.3 を使用すると、ID、復号化ポリシー、ルーティング ポリシー、アクセス ポリシー、時間ベースのポリシー、Cisco IronPort データ セキュリティ ポリシー、および外部 DLP ポリシーを設定したり、Web プロキシをバイパスしたり、カスタム URL カテゴリを作成したりできます。

これらの機能を Configuration Master で設定する方法は、Web セキュリティ アプライアンスで設定する方法と同じです。『*Cisco IronPort AsyncOS for Web User Guide*』を参照してください。

図 8-4　Configuration Master 6.3

Configuration Master 7.1 の使用

Security Management アプライアンスで、Configuration Master 7.1 がサポートされるようになりました。Configuration Master 7.1 を使用すると、認証 ID、SaaS ポリシーを設定したり、復号化ポリシー、ルーティング ポリシー、アクセ

ス ポリシー、定義済みの時間範囲、および全体的な帯域幅制限を含む Web ポリシーを定義したりできます。また、この Configuration Master には、AVC、Sophos、クレデンシャル暗号化、Mobile User Security（MUS）も含まれています。さらに、Cisco IronPort データ セキュリティ ポリシーや外部 DLP ポリシーを定義したり、Web プロキシをバイパスしたり、外部 URL ポリシーを含むカスタム URL カテゴリを作成することもできます。

これらの機能を Configuration Master で設定する方法は、Web セキュリティ アプライアンスで設定する方法と同じです。『*Cisco IronPort AsyncOS for Web User Guide*』を参照してください。

図 8-5　Configuration Master 7.1

Web セキュリティ アプライアンスへの設定の公開

AsyncOS for Security Management には、2 種類の設定公開方法があります。どちらのタイプも Configuration Master の GUI で同じページから開始し、両方のタイプを何回でも実行できますが、それぞれのタイプで結果は異なるものになります。

Configuration Master の公開

Configuration Master で設定を編集した後で、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 を使用して編集できるのは、ポリシー（アクセス、復号化、SaaS、L4 Traffic Manager、ルーティングおよび ID を含む）、プロキシ バイパス リスト、発信マルウェア スキャン、時間範囲、ポリシー タグ、URL タグ、カスタム URL カテゴリ、FTP プロキシ（Configuration Master 6.3 および 7.1 のみ）、Cisco IronPort データ セキュリティ フィルタ（Configuration Master 6.3 および 7.1 のみ）、および外部 DLP サーバ（Configuration Master 6.3 および 7.1 のみ）という Web セキュリティ アプライアンスの設定変数のみです。

Configuration Master を使用して他の設定変数（たとえば、ユーザ、アラート、およびログ サブスクリプション）を編集することはできません。

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 アプライアンスで、既存のポリシー情報が上書きされます。

（注） Security Management 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、Security Management 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」（P.8-16）を参照してください。Configuration Master の詳細については、「Configuration Master の操作」（P.8-3）を参照してください。

拡張ファイル公開

拡張ファイル公開は、Configuration Master の公開とは完全に独立しています。また、[Configuration Master Publish] セクションにリストされている設定のいずれにも影響を与えません。さらに、ネットワーク/インターフェイス設定、DNS、SNTPD、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、時間設定、L4TM 設定、認証リダイレクト ホスト名にも影響を与えません。

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。

拡張ファイル公開は、ポリシー以外の設定変数のみ（たとえば、ユーザ、アラート、ログ サブスクリプション）を上書きします。拡張ファイル公開を使用して、管理対象の Web セキュリティ アプライアンスでポリシー情報を変更することはできません。つまり、Configuration Master の公開によって設定を変更できる場合、拡張ファイル公開を使用してその変更を行うことはできません。

「拡張ファイル公開の使用」（P.8-20）を参照してください。

（注） 公開タイプが Web セキュリティ アプライアンスでのネットワーク設定に影響することもありません。ネットワーク設定は、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 User Guide*』を参照してください。

Configuration Master の公開

（注） 6.3 を実行中のアプライアンスを、5.7 の Configuration Master に割り当てることができます。バージョンは同一である必要はありませんが、アプライアンスのバージョンよりも新しい Configuration Master に、そのアプライアンスを割り当てることはできません。

警告 **Configuration Master の設定を管理対象の Web セキュリティ アプライアンスに対して適切に公開するには、Configuration Master の許容範囲内の使用制御が、Web セキュリティ アプライアンスの設定と一致している必要があります。Configuration Master のこれらの設定を変更しても、Web セキュリ**

ティ アプライアンスの設定が自動的に変更されることはありません。Configuration Master の公開を行う前に、[Web] > [Utilities] > [Web Appliance Status] ページをチェックして、許容範囲内の使用の設定と Web セキュリティ アプライアンスでの設定の間に不一致がないか調べることをお勧めします（「Web セキュリティ アプライアンスのステータスの表示」（P.8-23）を参照）。それらが一致しない場合、公開は失敗します。その他のすべての不一致では、それらのポリシーが使用不可になり、その詳細は [Publish History] ページで確認できます。不一致に気づいた場合は、許容範囲内の使用制御の設定（「セキュリティ サービスの設定の編集」（P.8-4）を参照）か、Web セキュリティ アプライアンスでの設定かのいずれかを変更する必要があります。

Configuration Master を Web セキュリティ アプライアンスに今すぐ公開するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Web] > [Utilities] > [Publish to Web Appliances] を選択します。

ステップ 2　[Publish Configuration Now] をクリックします。

[Publish Configuration Now] ページが表示されます。

図 8-6　[Publish Configuration Now] ページ

ステップ 3　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 4　公開する Configuration Master を選択します。

あるいは、拡張ファイル公開を実行する場合は、[Advanced file options] を選択します。「拡張ファイル公開の使用」（P.8-20）を参照してください。

ステップ 5　Configuration Master の公開先となる Web セキュリティ アプライアンスを選択します。Configuration Master に割り当てられているすべてのアプライアンスに設定を公開するには、[All assigned appliances] を選択します。

または

Configuration Master に割り当てられているアプライアンスのリストを表示するには、[Select appliances in list] を選択します。設定の公開先となるアプライアンスを選択します。

ステップ 6　[Publish] をクリックします。[Publish in Progress] ページが表示されます。赤い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示しています。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。

Configuration Master を後で Web セキュリティ アプライアンスに公開するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Web] > [Utilities] > [Publish to Web Appliances] を選択します。

ステップ 2　[Schedule a Job] をクリックします。

[Schedule a Job] ページが表示されます。

図 8-7　[Schedule a Job] ページ

ステップ 3　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 4　Configuration Master を公開する日時を入力します。

ステップ 5　公開する Configuration Master を選択します。

あるいは、拡張ファイル公開を実行する場合は、[Advanced file options] を選択します。「拡張ファイル公開の使用」（P.8-20）を参照してください。

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

Configuration Master に割り当てられているアプライアンスのリストを表示するには、[Select appliances in list] を選択します。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　[Submit] をクリックします。

ステップ 8　スケジュールされているジョブのリストは、[Web] > [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。

publishconfig コマンドの使用

Security Management アプライアンスでは、次の CLI コマンドを使用して Configuration Master の変更を公開できます。

publishconfig config_master [--*job_name*] [--*host_list* | *host_ip*]

ここで、**config_master** は 5.7、6.3、または 7.1 のいずれかです。このキーワードは必須です。*job_name* オプションは省略可能で、指定しなかった場合は生成されます。

host_list オプションは、公開する Web セキュリティ アプライアンスのホスト名または IP アドレスのリストで、指定しなかった場合は Configuration Master に割り当てられているすべてのホストに公開されます。*host_ip* オプションには、カンマで区切って複数のホスト IP アドレスを指定できます。

publishconfig コマンドが成功したことを確認するには、**smad_logs** ファイルを調べます。[Web] > [Utilities] > [Web Appliance Status] を選択することで、Security Management 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。

拡張ファイル公開の使用

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.8-20）
- 「拡張ファイル公開：[Publish Later]」（P.8-21）

拡張ファイル公開：[Publish Configuration Now]

拡張ファイル公開の [Publish Configuration Now] を実行するには、次の手順に従います。

ステップ 1　メイン Security Management アプライアンスのウィンドウで、[Web] > [Utilities] > [Publish to Web Appliances] を選択します。

ステップ 2　[Publish Configuration Now] をクリックします。

[Publish Configuration Now] ページが表示されます。

図 8-8　[Publish Configuration Now] ページ

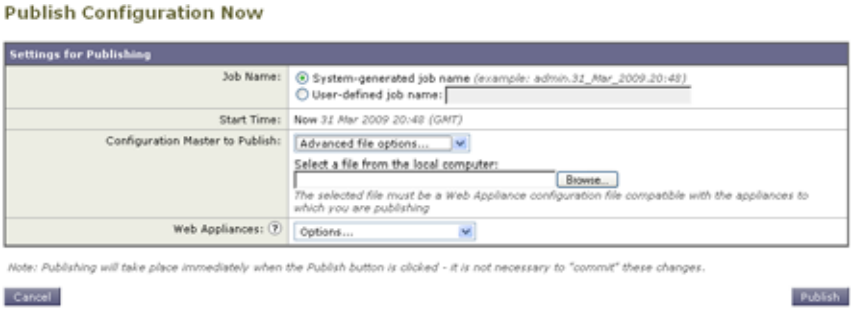
ステップ 3　デフォルトでは [System-generated job name] が選択されています。あるいは、ユーザ定義のジョブ名（80 文字以下）を入力します。

ステップ 4　[Advanced file options] を選択します。

ステップ 5　[Browse] をクリックし、公開するファイルを選択します。

[Publish Configuration Now] ページが表示されます。

図 8-9　[Publish Configuration Now] ページ



ステップ 6　[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 7　[Publish] をクリックします。

拡張ファイル公開：[Publish Later]

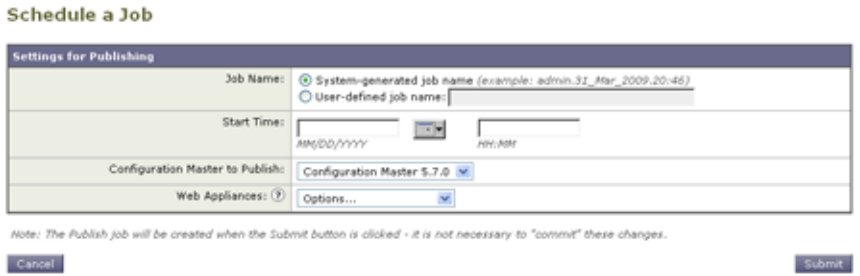
拡張ファイル公開の [Publish Later] を実行するには、次の手順に従います。

ステップ 1　Security Management アプライアンスで、[Web] > [Utilities] > [Publish to Web Appliances] を選択します。

ステップ 2　[Schedule a Job] をクリックします。

[Schedule a Job] ページが表示されます。

図 8-10　[Schedule a Job] ページ

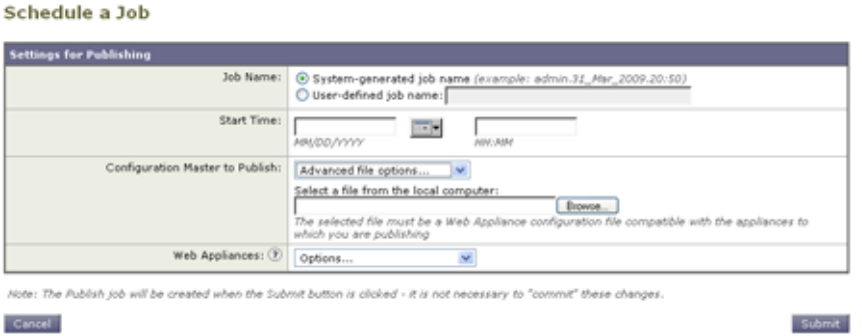


ステップ 3　デフォルトでは [System-generated job name] が選択されています。あるいは、ユーザ定義のジョブ名（80 文字以下）を入力します。

ステップ 4　設定を公開する日時を入力します。

ステップ 5　[Advanced file options] を選択して [Browse] をクリックし、公開するファイルを選択します。

図 8-11　[Schedule a Job] ページ : [Advanced File Options]



ステップ 6　[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 7　[Publish] をクリックします。

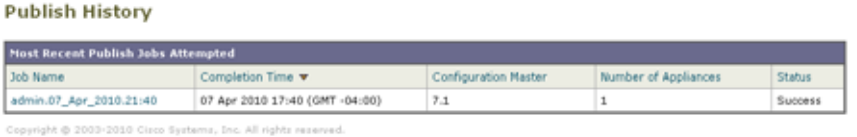
公開履歴の表示

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。

公開履歴を表示するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Web] > [Utilities] > [Publish History] を選択します。

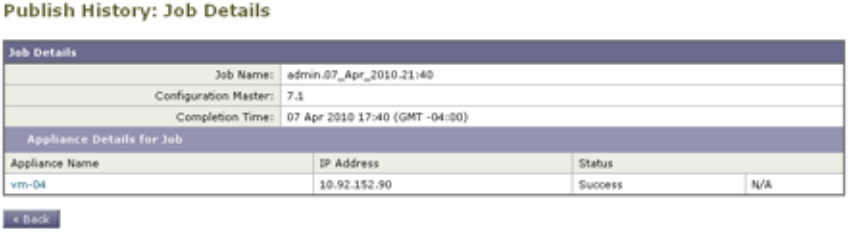
[Publish History] ページが表示されます。



[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。

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。

[Publish History: Job Details] ページが表示されます。



[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 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 Security Management 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、公開履歴などがあります。

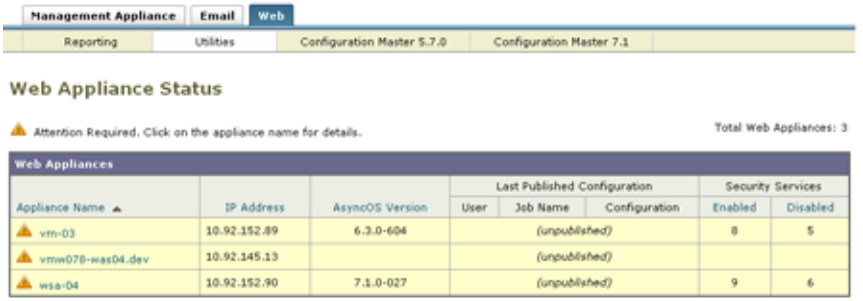
（注）　Security Management アプライアンスに追加するすべての Web アプライアンスは、[Web] > [Utilities] > [Web Appliance Status] ページにエントリが表示されます。ただし、表示可能なデータがあるのは、集中管理をサポートするマシンのみです。管理がサポートされるバージョンは、6.0 を除く、5.7 以降のすべてのバージョンの Web セキュリティ アプライアンスです。したがって、5.7、6.3、または 7.1 を実行中のすべてのアプライアンスはデータが表示されます。6.0 バージョンでは、使用可能な情報がないことを示すエラー メッセージが表示されます。

Web セキュリティ アプライアンスのステータスを表示するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Web] > [Utilities] > [Web Appliances Status] を選択します。

[Web Appliances Status] ページが表示されます。

図 8-12　[Web Appliances Status] ページ



[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。

Web セキュリティ アプライアンスのステータスに関する詳細を表示するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Web] > [Utilities] > [Web Appliances Status] を選択します。

ステップ 2　表示するアプライアンスの名前をクリックします。

詳細には次の情報が含まれます。

- システム ステータス情報（稼動時間、アプライアンスのモデルおよびシリアル番号、AsyncOS バージョン、ビルドの日付、AsyncOS インストールの日時、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）
- Web セキュリティ機能（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）
- 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（認証レルムの名前/プロトコル/サーバ、認証シーケンスでのレルムの名前と順序、認証失敗時にトラフィックをブロックするか許可するか）

ステップ 3　詳細を更新するには、たとえば、新しいアプライアンスを追加した場合、またはアプライアンスの情報がまだ使用できないことを示すメッセージが表示された場合には、[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。

特定の Web セキュリティ アプライアンスに関するきめ細かな詳細を確認するには、[Web Appliance] カラムのハイパーテキスト リンクをクリックします。次のページが表示されます。

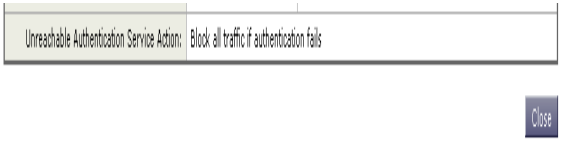


図 8-13　[Web Appliance Status Details] ページ

（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、Security Management 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。

CHAPTER 9

システム ステータスのモニタリング

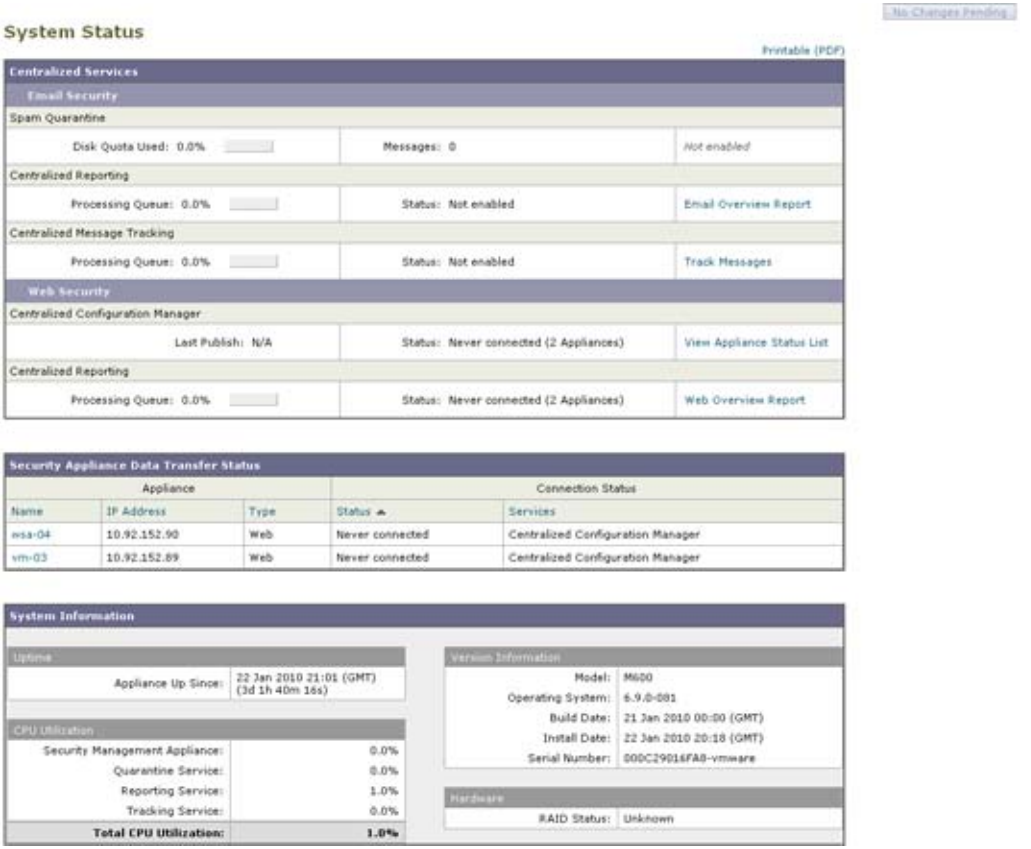
この章は、次の項で構成されています。

Security Management アプライアンスのステータスのモニタリング

[System Status] ページは、Security Management アプライアンスのグラフィカル ユーザ インターフェイスにアクセスしたときに、最初に表示されるページです。GUI へのアクセス方法の詳細については、「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）を参照してください。

グラフィカル ユーザ インターフェイスの任意の場所から [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、ステータス情報は [System Information] セクションだけに表示されます。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。サービスのイネーブル化、管理対象アプライアンスの追加、および両方のステータスの表示に関する詳細については、第 3 章「アプライアンスの設定」（P.1）および「管理対象アプライアンスのステータスの表示」（P.9-8）を参照してください。

Centralized Services

[Centralized Services] セクションには、Security Management 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 Security Management アプライアンスで、[Management Appliance] > [Centralized Services] > [System Status] を選択し、管理対象 Email Security アプライアンス、Web セキュリティ アプライアンス、および Security Management 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要約情報を表示します。

[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] セクションには、Email Security アプライアンスだけに関係する情報が表示されます。[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 スパム検疫で保持されているメッセージの数、および検疫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 スパム検疫の詳細については、第 7 章「Cisco IronPort スパム検疫の管理」（P.1）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、Security Management 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、Security Management 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 Email Security アプライアンスから転送され、Security Management 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動しています。この場合は、Security Management 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 Security Management 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。この割合は、Security Management アプライアンスの処理負荷の大まかな概算にすぎません。

[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 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 Email Security アプライアンスと Security Management 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 データによって消費された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」（P.1）を参照してください。

Web Security

[Web Security] セクションには、Web セキュリティ アプライアンスだけに関係する情報が表示されます。[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、Security Management 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、Security Management 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、Security Management 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動しています。この場合は、Security Management 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 Security Management 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。この割合は、Security Management アプライアンスの処理負荷の大まかな概算にすぎません。

[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」の Web レポーティング ページの概要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後の更新を表示できます。[View Appliance Status List] をクリックすると、Security Management アプライアンスのアプライアンスのステータスが個別に表示されます。現在、システムで表示できるアプライアンス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.9-8）を参照してください。

Security Appliance Data Transfer Status

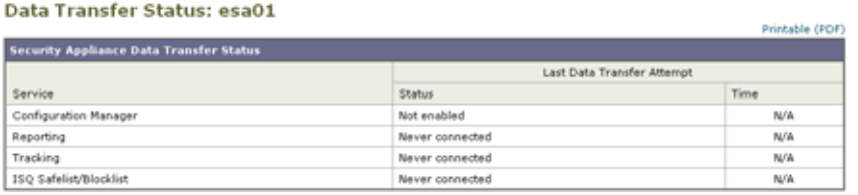
集中管理機能を実行するうえで、Security Management アプライアンスは、管理対象アプライアンスから Security Management アプライアンスにデータが正常に転送されることを前提としています。[Security Appliance Data Transfer Status] セクションには、Security Management アプライアンスで管理される各アプライアンスのステータス情報が表示されます。

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。10 台を超えるアプライアンスを Security Management アプライアンスで管理する場合は、[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] セクションには、特定のアプライアンスに関する接続ステータスの問題が表示されます。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] ページを表示してください。

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。

Email Security 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 Email Security 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 Email Security アプライアンスでイネーブルになっていますが、Email Security アプライアンスと Security Management 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]：Email Security アプライアンスが Security Management 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]：Email Security アプライアンスと Security Management 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]：Email Security アプライアンスと Security Management 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 マネージャが 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 Security Management 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 Security Management 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 Security Management 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]：Security Management 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]：Security Management 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]：Security Management 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 Security Management 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。

アプライアンスに関して「File transfer failure」ステータスが表示された場合、アプライアンスをモニタして、障害の原因がネットワークの問題か、アプライアンスの設定の問題かを判断します。ネットワークの問題によってデータを転送できないのではなく、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。

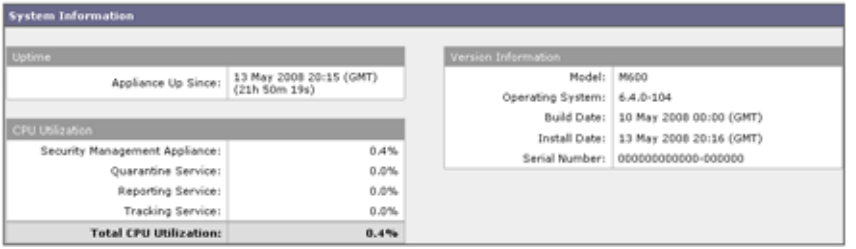
System Information

[System Status] ページの [System Information] セクションには、Security Management 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、各モニタリング サービスが占有する Security Management アプライアンスの CPU 処理能力の割合です。この割合によって、3 つの主なサービスが現在使用している CPU 量が示されます。Security Management 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。

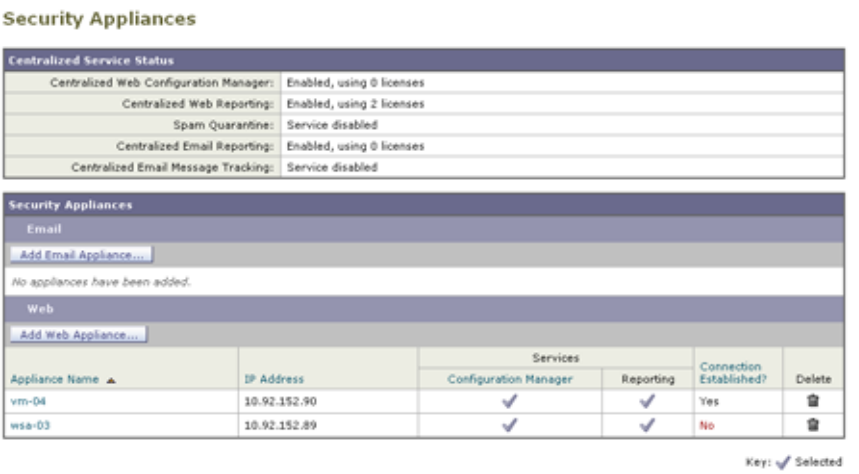
管理対象アプライアンスのステータスの表示

[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。

Security Management 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化され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」（P.3-11）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

Security Management アプライアンスでは、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。

- 「Email Security 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.9-10）
- 「Web Security 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.9-11）

Email Security 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

Email Security アプライアンスからのレポーティング データを Security Management 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　Security Management アプライアンスで、[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 9-5　[Reporting Data Availability] ページ

[Reporting Data Availability] ページから、指定された期間に Security Management アプライアンスが Email Security 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、その期間に受信したデータの完全さを示しています。

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。Security Management アプライアンスが Email Security 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）　ハードウェア障害などが原因で Email Security アプライアンスを交換する必要があった場合、交換した Email Security アプライアンスからのデータは失われませんが、Security Management アプライアンスで正しく表示されません。

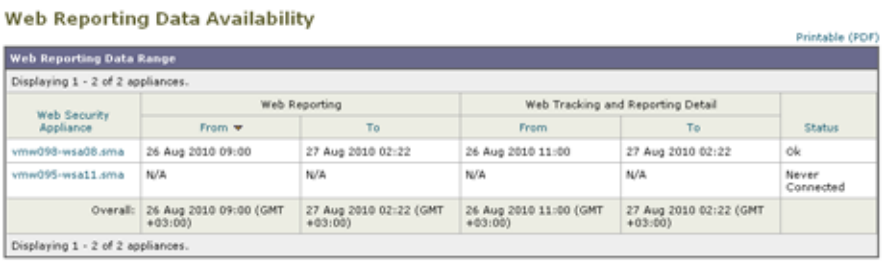
Web Security アプライアンスのデータ アベイラビリティのモニタリング

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 Security Management 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　Security Management アプライアンスで、[Web] > [Reporting] > [Data Availability] を選択します。

[Data Availability] ページが表示されます。

[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。



（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 Security 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。Security Management 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。欠落が存在しない場合は何も表示されません。

Web セキュリティ アプライアンスの [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

Security Management 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.9-12）
- 「Web トラッキング データ ステータス」（P.9-14）

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

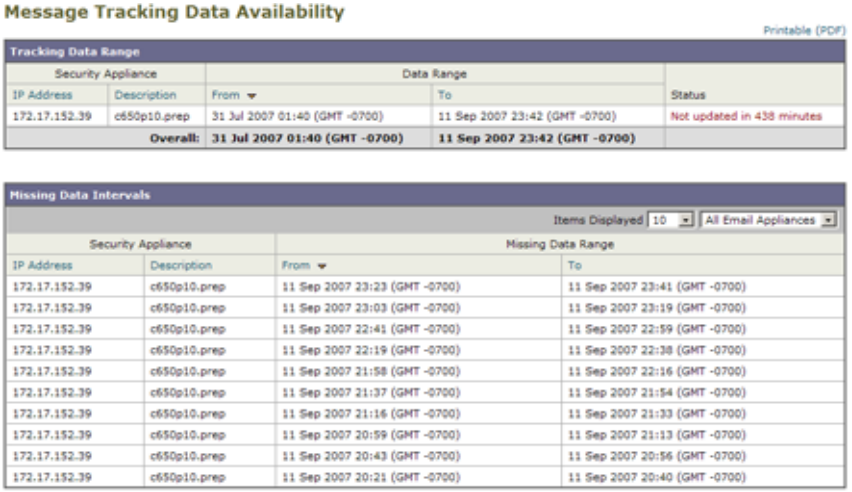
（注） Email Security アプライアンスは、アプライアンスから取得したレポーティング データとトラッキング データのコピーを作成し、データ ファイルのコピーをデフォルト ディレクトリとは別の追加フォルダに保存します。次に、これらのフォルダのいずれかからデータを取り出すように、Security Management アプライアンスを設定できます。

電子メール トラッキング データ ステータスをモニタするには、次の手順を実行します。

ステップ 1　メイン Security Management アプライアンスで、[Email] > [Message Tracking] > [Message Tracking Data Availability] を選択します。

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

図 9-6　[Message Tracking Data Availability] ページ



[Message Tracking Data Availability] ページを使用して、Security Management アプライアンスのデータ欠落インターバルを表示できます。データ欠落インターバルとは、Security Management アプライアンスが組織の Email Security 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 Email Security 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

Security Management アプライアンスからの Web トラッキング データ ステータスをモニタするには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Web] > [Reporting] > [Web Tracking] を選択します。

[Web Tracking Search] ダイアログボックスが表示されます。

ステップ 2　[Time Range] ドロップダウン リストから、情報を表示する時間範囲を選択します。

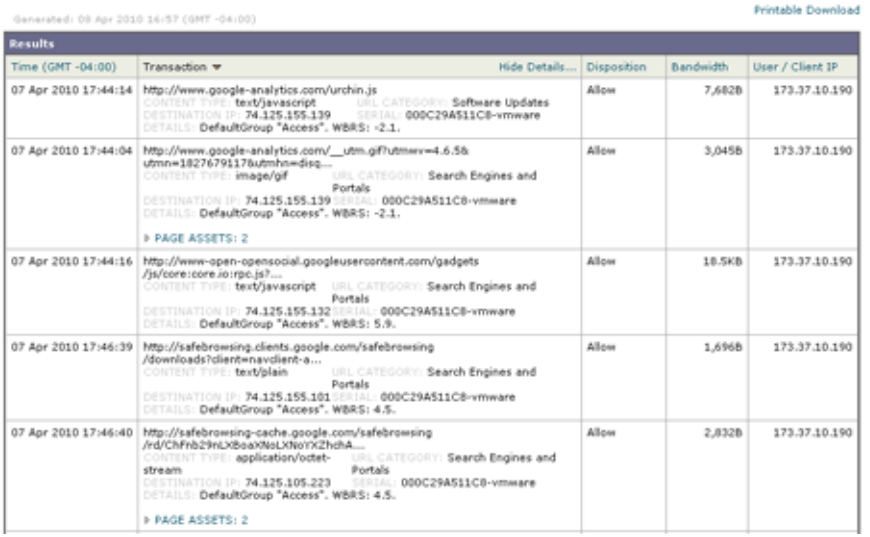
ステップ 3　[User/Client IP] または [Website] テキスト フィールドに、値を入力します。

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。

ステップ 5　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.5-70）を参照してください。

CHAPTER 10

LDAP クエリー

この章は、次の内容で構成されています。

概要

エンドユーザのパスワードおよび電子メール エイリアスを企業の LDAP ディレクトリ（Microsoft Active Directory、SunONE Directory Server、OpenLDAP ディレクトリなど）で維持する場合、LDAP ディレクトリを使用すると、Cisco IronPort スパム検疫にアクセスするユーザを認証できます。ユーザが Cisco IronPort スパム検疫の Web UI にログインするときに、LDAP サーバがログイン名とパスワードを検証し、AsyncOS が対応する電子メール エイリアスのリストを取得します。ユーザのいずれかの電子メール エイリアスに送信された検疫済みメッセージは、アプライアンスが上書きしていない限り、Cisco IronPort スパム検疫で表示できます。

Cisco IronPort スパム検疫との連携に必要な 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。

- サーバ名とポート
- ベース DN
- サーバに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.10-3）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、複数の LDAP サーバに接続するように AsyncOS を設定できます。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.10-17）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検疫クエリーを使用することも、特定の LDAP 実装およびスキーマに合わせてカスタマイズした独自のクエリーを作成することもできます。次に、スパム通知、および検疫へのエンドユーザ 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.10-6）を参照してください。

ステップ 3　Cisco IronPort スパム検疫に対して、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。

エンドユーザが、自分の検疫エリアのメッセージを表示および管理できるように、Cisco IronPort スパム検疫への LDAP エンドユーザ アクセスをイネーブルにします。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、「IronPort スパム検疫の設定」（P.7-3）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。

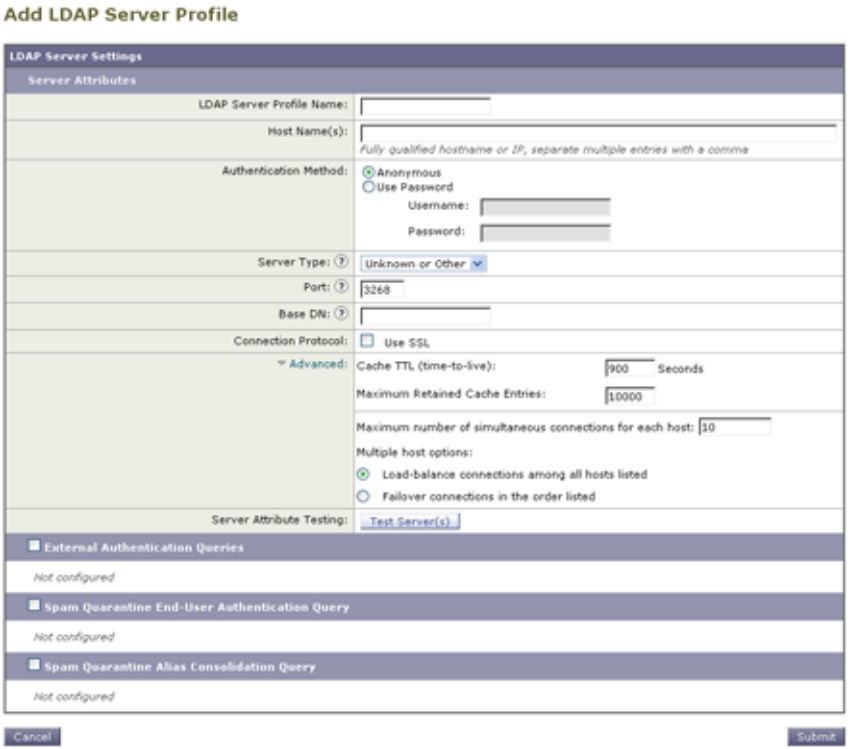
LDAP サーバ プロファイルを作成するには、次の手順を実行します。

ステップ 1　メイン Security Management 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。

[Add LDAP Server Profile] ページが表示されます。

図 10-1　　LDAP サーバ プロファイルの設定



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.10-17）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）　レポートにクライアント 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]、[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、マルチサーバ環境でグローバル カタログにアクセスするための Active Directory 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。このユーザのエントリは、次のようなエントリになります。

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

ステップ 9　[Advanced] の下で、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 バランシングを行うように LDAP サーバ プロファイルを設定した場合、リストで指定された LDAP サーバ間でこれらの接続が分散されます。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.10-19）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 スパム検疫に対して LDAP 認証をイネーブルにした場合、アプライアンスによってエンドユーザ検疫用に 20 の追加接続が許可され、合計 30 の接続が許可されます。

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.10-6）を参照してください。

ステップ 14 スパム検疫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検疫にログインするときにそのユーザを検証する、検疫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 エイリアスごとに検疫通知を受信しないように、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.10-6）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、スパム検疫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 [Submit] をクリックし、[Commit] をクリックして変更を確定します。

Windows 2000 では、Active Directory サーバ設定で TLS を介した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 と Windows 2003 の組み合わせでは、TLS 認証が機能します。

（注）　サーバ設定の数に制限はありませんが、サーバごとに設定できるエンドユーザ認証クエリー、およびエイリアス統合クエリーはそれぞれ 1 つだけです。

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 スパム検疫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。

- **スパム検疫へのエンドユーザ認証のクエリー。**詳細については、「スパム検疫へのエンドユーザ認証のクエリー」（P.10-8）を参照してください。
- **スパム検疫のエイリアス統合のクエリー。**詳細については、「スパム検疫のエイリアス統合のクエリー」（P.10-10）を参照してください。

検疫機能のエンドユーザ アクセス検証またはスパム通知に 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。検疫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。既存のすべてのアクティブ クエリーはディセーブルになります。Security Management アプライアンスで [Management Appliance] > [System Administration] > [LDAP] ページを選択すると、アクティブ クエリーの横にアスタリスク（*）が表示されます。

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.10-12）および「チェーン クエリー」（P.10-14）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.10-11）を参照してください。

スパム検疫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 スパム検疫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 or Other :**（ブランク）

デフォルトでは、プライマリ メール属性は **mail** です。独自のクエリーとメール属性を入力できます。クエリーを CLI で作成するには、**ldapconfig** コマンドの `isqauth` サブコマンドを使用します。

（注）　ユーザのログイン時に各自の電子メール アドレス全体を入力させる場合は、`(mail=smtp:{a})` というクエリー文字列を使用します。

Active Directory エンドユーザ認証の設定の例

ここでは、Active Directory サーバとエンドユーザ認証クエリーの設定の例を示します。この例では、Active Directory サーバに対してパスワード認証を使用し、Active Directory サーバに対するエンドユーザ認証にはデフォルトのクエリー文字列を使用し、メール属性は `mail` と `proxyAddresses` を使用します。

表 10-1　LDAP サーバとスパム検疫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 サーバに対して匿名認証を使用し、OpenLDAP サーバに対するエンドユーザ認証にはデフォルトのクエリー文字列を使用し、メール属性は `mail` と `mailLocalAddress` を使用します。

表 10-2　LDAP サーバとスパム検疫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`

スパム検疫のエイリアス統合のクエリー

スパム通知を使用する場合は、スパム検疫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検疫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、受信者の代替メール アドレ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、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 サーバとスパム検疫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）

表 10-3　LDAP サーバとスパム検疫のエイリアス統合の設定例：Active Directory（続き）

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 サーバとスパム検疫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。クエリー接続テストの段階ごとに、詳細が表示されます。たとえば、SMTP 認証の最初の段階が成功したか、失敗したか、BIND 照合結果として true と false のどちらが返されたかが表示されます。

ldaptest コマンドは、次の例のようにバッチ コマンドとして使用できます。

```
ldaptest LDAP.isqalias foo@cisco.com
```

クエリーに入力する変数名では、大文字と小文字が*区別されます*。また、正しく動作するためには、LDAP 実装と一致している必要があります。たとえば、メール属性に `mailLocalAddress` と入力したときに実行されるクエリーは、`maillocaladdress` と入力したときとは異なります。

クエリーをテストするには、テスト パラメータを入力して、[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すると、「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。ドメインベース クエリーが使用されるのは、複数の LDAP サーバがそれぞれ異なるドメインに関連付けられているが、エンドユーザ検疫アクセスのクエリーをすべての LDAP サーバに対して実行する必要がある場合です。たとえば、Bigfish という企業がドメイン Bigfish.com、Redfish.com、および Bluefish.com を所有し、各ドメインに関連付けられている従業員に対して異なる LDAP サーバを使用しているとします。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 スパム検疫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ドメインごとに 1 つずつ、LDAP サーバ プロファイルを作成します。各サーバ プロファイルに、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.10-3）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 スパム検疫のアクティブ 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.10-13）を参照してください。

ステップ 3　Cisco IronPort スパム検疫に対して、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、「IronPort スパム検疫の設定」（P.7-3）を参照してください。

ドメインベース クエリーの作成

Security Management アプライアンスでドメインベース クエリーを作成するには、次の手順を実行します。

ステップ 1　Security Management 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。

[Add Domain Assignments] ページが表示されます。

図 10-2　　ドメインベース クエリーの設定

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、クエリーのタイプを 1 つ指定します。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 リストに設定されます。

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。

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 スパム検疫でドメインベース 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、エンドユーザ認証にドメインベース クエリーを使用する場合、Cisco IronPort スパム検疫のアクティブな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確定します。

（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 によって順番に実行される一連の LDAP クエリーで構成されます。AsyncOS は、この「チェーン」に含まれる一連のクエリーを順に実行し、LDAP サーバから肯定的なレスポンスが返されるか、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と、実行を停止します。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。両方のタイプの LDAP ディレクトリに対して確実にクエリーを実行するには、チェーン クエリーを使用します。

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 スパム検疫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.10-3）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 スパム検疫のアクティブ 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.10-15）を参照してください。

ステップ 3　Cisco IronPort スパム検疫に対して、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。スパム検疫の詳細については、「IronPort スパム検疫の設定」（P.7-3）を参照してください。

チェーン クエリーの作成

チェーン クエリーを作成するには、次の手順を実行します。

（または、CLI で `ldapconfig` コマンドの `advanced` サブコマンドを実行します）。

ステップ 1　Security Management 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 1　[LDAP Server Profiles] ページの [Advanced] をクリックします。

ステップ 2　[Add Chained Query] をクリックします。

[Add Chained Query] ページが表示されます。

図 10-3　　チェーン クエリーの設定

ステップ 3　チェーン 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。

チェーン クエリーを作成するときは、すべてのコンポーネント クエリーが同じクエリー タイプになります。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 5　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した場合、一般的なクエリーが詳細なクエリーの後で実行されるように、並べ替えることがあります。

ステップ 6　[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 7　Cisco IronPort スパム検疫でドメイン 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、エンドユーザ認証にチェーン クエリーを使用する場合、Cisco IronPort スパム検疫のアクティブなエンドユーザ認証クエリーになります。

ステップ 8　[Submit] をクリックし、[Commit] をクリックして変更を確定します。

（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。

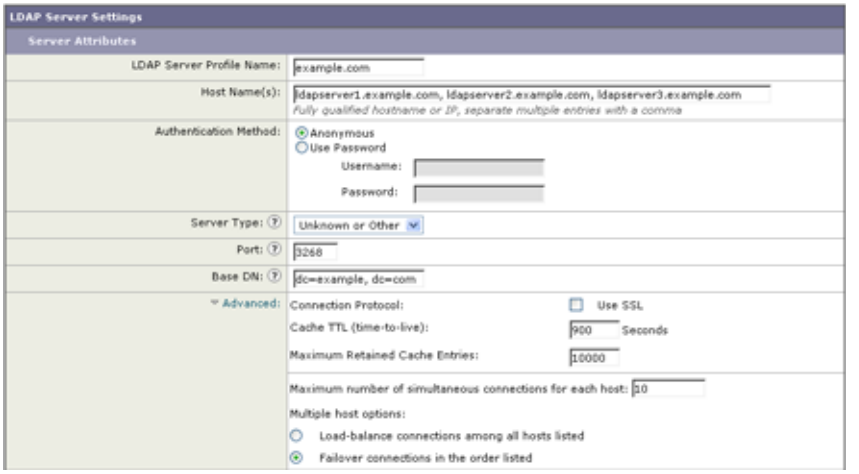
Cisco IronPort アプライアンスが 2 番目以降の LDAP サーバに接続した場合は、指定された時間が経過するまで、そのサーバに接続したままになります。この時間が経過すると、アプライアンスはリスト内の最初のサーバに対して再接続を試行します。

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

LDAP フェールオーバーを行うように Cisco IronPort アプライアンスを設定するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Management Appliance] > [System Administration] > [LDAP] を選択します。

[LDAP Server Setup] ページが表示されます。



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。

この例では、LDAP サーバ名が example.com です。

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　[Submit] をクリックし、[Commit] をクリックして保存します。

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。

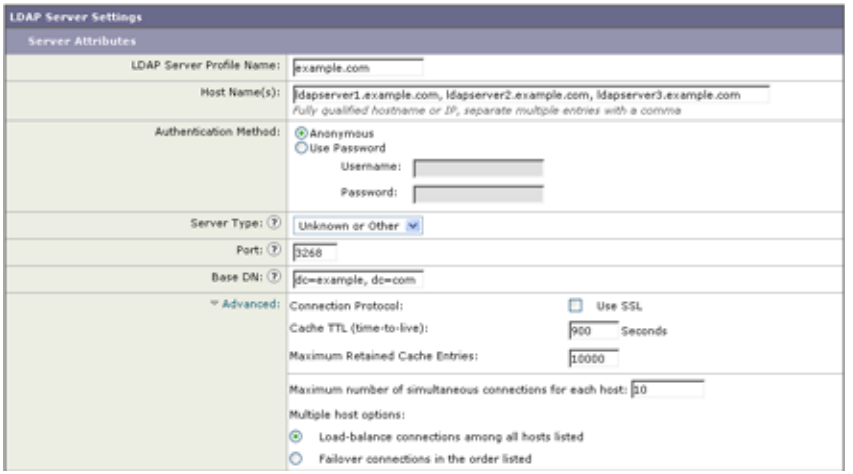
リストで指定された LDAP サーバの 1 つが応答しなくなった場合は、Cisco IronPort アプライアンスからの接続の負荷は残りの LDAP サーバに分散されます。

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

LDAP ロード バランシングを行うように Cisco IronPort アプライアンスを設定するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Management Appliance] > [System Administration] > [LDAP] を選択します。

[LDAP Server Setup] ページが表示されます。



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。

この例では、LDAP サーバ名が example.com です。

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　[Submit] をクリックし、[Commit] をクリックして保存します。

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ログインできるようになります。LDAP サーバに対する認証クエリーを設定したら、アプライアンスによる外部認証の使用をイネーブルにします（GUI の [Management Appliance] > [System Administration] > [Users] ページまたは CLI の **userconfig** コマンドを使用します）。

ユーザの外部認証を設定するには、次の手順を実行します。

ステップ 1　**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 プロファイルで、LDAP ディレクトリ内のユーザ アカウントを検索するためのクエリーを作成します。

ステップ 2　**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。

ステップ 3　**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、『*Cisco IronPort AsyncOS for Email User Guide*』の「Adding Users」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。詳細については、「LDAP クエリーのテスト」（P.10-11）を参照してください。

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`

グループ メンバーシップ クエリー

AsyncOS も、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、および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します。ディレクトリ グループ メンバーシップ内のメンバーシップによって、そのユーザのシステム内のアクセス許可が決まります。GUI の [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

サーバ タイプ	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 member of 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

サーバ タイプ	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`

CHAPTER 11

SMTP ルーティングの設定

この章では、Security Management 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機能について説明します。

この章は、次の項で構成されています。

- 「ローカル ドメインの電子メールのルーティング」（P.11-1）（[SMTP Routes] ページおよび **smtproutes** コマンド）

ローカル ドメインの電子メールのルーティング

Security Management アプライアンスは、次の場所に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
- SMTP ルーティングの影響を受けるアラート
- 指定した宛先に電子メールで送信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。

Email Security 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 セットアップ ウィザードを完了して変更を確定すると、そのときに入力した RAT エントリごとにアプライアンス上の最初の SMTP ルート エントリが定義されます。

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.11-4）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 の両方がマッピングと一致します。

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。

SMTP ルート テーブルは、電子メール配信ごとに上から下へ読み込まれます。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、こちらのが使用されます。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 エントリを表示すると、デフォルトの SMTP ルートは ALL: としてリストされます。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。

デフォルトの SMTP ルートは、[Management Appliance] > [Network] > [SMTP Routes] ページまたは **smtproutes** コマンドを使用して設定します。

SMTP ルートの定義

Email Security 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 台以上のホストが応答していない場合、メッセージは到達可能なホストの 1 台に配信されます。すべての設定済みホストが応答していない場合は、メールはそのホスト用にキューに入れられます（MX レコードの使用にフェールオーバーすることはありません）。

SMTP ルートの制限

最大 10,000 個のルートを定義できます。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 ルートおよびアラート

[Management Appliance] > [System Administration] > [Alerts] ページ（または **alertconfig** コマンド）で Security Management アプライアンスに指定されたアドレスにアプライアンスから送信されるアラートは、これらの宛先に対して定義された SMTP ルートに従います。

SMTP ルート、メール配信、およびメッセージ分裂

着信：1 つのメッセージに 10 人の受信者がいて、全員が同じ Exchange サーバに属する場合、AsyncOS では TCP 接続を 1 つ開き、メール ストアには 10 の別々のメッセージではなく、メッセージを 1 つのみ配置します。

発信：同様に機能しますが、1 つのメッセージが 10 の異なるドメインの 10 人の受信者に送られる場合、AsyncOS では 10 の MTA に対する 10 の接続を開き、それぞれに 1 つずつ電子メール配信を行います。

分裂：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。

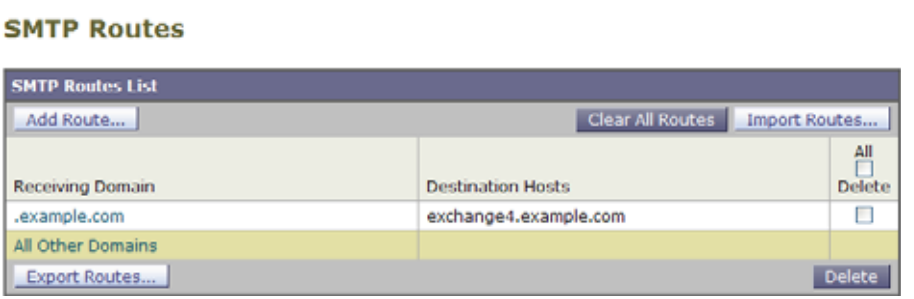
Security Management アプライアンスでの SMTP ルートの管理

SMTP ルートを Security Management アプライアンスで管理するには、次を実行します。

ステップ 1　Security Management アプライアンスで、[Management Appliance] > [Network] > [SMTP Routes] を選択します。

[SMTP Routes] ページが表示されます。

図 11-1　[SMTP Routes] ページ



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 エントリは、エクスポートまたはインポートできます。

SMTP ルートの追加

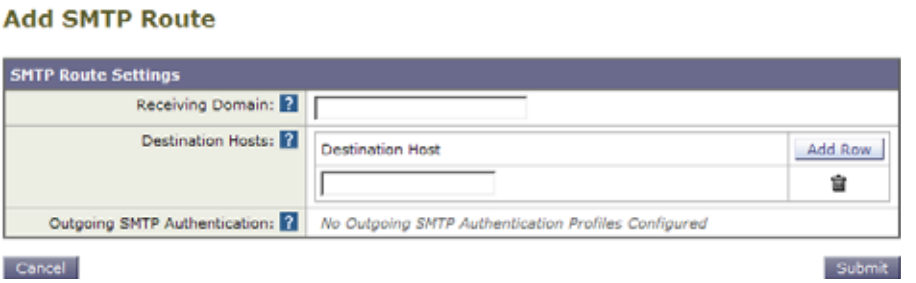
SMTP ルートを追加するには、次を実行します。

ステップ 1　Security Management 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。

[Add SMTP Route] ページが表示されます。

図 11-2　[Add SMTP Route] ページ



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「:< *ポート番号*>」を追加します（例：`example.com:25`）。

ステップ 5　[Submit] をクリックします。

ステップ 6　[SMTP Routes] ページが表示され、変更が反映されます。

ステップ 7　[Commit Changes] をクリックし、オプションでコメントを必要に応じて追加して、[Commit Changes] をクリックします。

SMTP ルートの編集

SMTP ルートを編集するには、次を実行します。

ステップ 1　Security Management 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。

[Edit SMTP Route] ページが表示されます。

ステップ 3　ルートを編集します。

ステップ 4　[Submit] をクリックします。

ステップ 5　[SMTP Routes] ページが表示され、変更が反映されます。

ステップ 6　[Commit Changes] をクリックし、オプションでコメントを必要に応じて追加して、[Commit Changes] をクリックします。

SMTP ルートの削除

SMTP ルートを削除するには、次を実行します。

ステップ 1　Security Management 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

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。SMTP ルートをエクスポートするには、次の手順に従います。

ステップ 1　[SMTP Routes] ページの [Export SMTP Routes] をクリックします。[Export SMTP Routes] ページが表示されます。

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。SMTP ルートをインポートするには、次の手順に従います。

ステップ 1　[SMTP Routes] ページの [Import SMTP Routes] をクリックします。[Import SMTP Routes] ページが表示されます。

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。インポートによって、既存のすべての SMTP ルートが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。

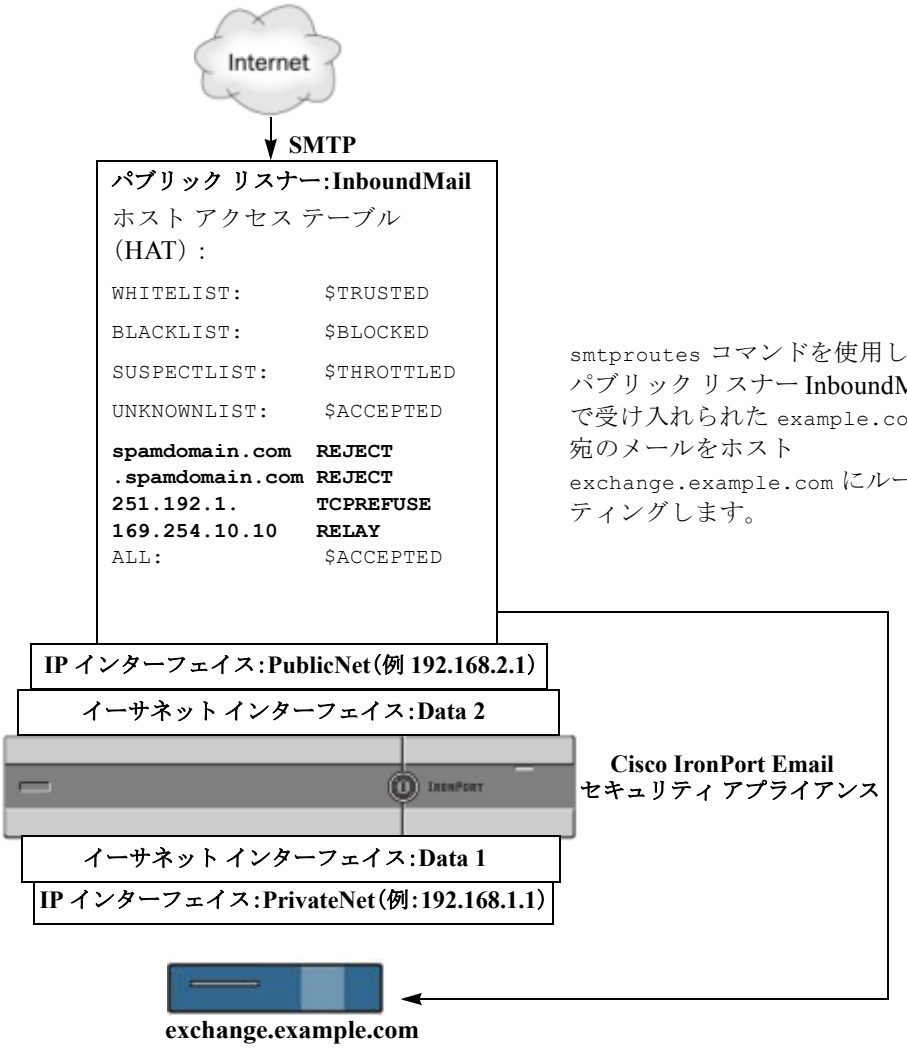
ファイルには「コメント」を格納できます。文字「#」で始まる行はコメントと見なされ、AsyncOS によって無視されます。例：

```
# 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 11-3　パブリック リスナーに定義されている SMTP ルート



CHAPTER 12

一般的な管理タスク

大部分のシステム管理タスクは、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行えます。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-4）を参照してください。

この章は、次の項で構成されています。

- 「生成されたメッセージの返信アドレスの設定」（P.12-81）
- 「アラートの管理」（P.12-82）
- 「ネットワーク設定値の変更」（P.12-95）
- 「システム時刻の設定」（P.12-105）
- 「コンフィギュレーション ファイルの管理」（P.12-110）
- 「ディスク使用量の管理」（P.12-123）

CLI コマンドを使用したメンテナンス タスクの実行

ここで説明されている操作およびコマンドを使用して、Security Management アプライアンスでメンテナンス関連のタスクを実行できます。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**

Security Management アプライアンスのシャットダウン

Security Management 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。

Security Management アプライアンスのリブート

Security Management 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。

Security Management 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、Security Management アプライアンスをオフライン状態にします。`suspend` および `offline` コマンドを使用して、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。

アプライアンスをオフライン状態に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。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アプライアンスをリブートする場合、システムをオンライン状態に戻すには **resume** コマンドを使用する必要があります。

関連項目：

- 『*Cisco IronPort AsyncOS for Email 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> r
esume


Receiving resumed.

Mail delivery resumed.

mail3.example.com>
```

出荷時デフォルト値へのリセット

アプライアンスを物理的に移動するときに、出荷時の初期状態に戻すことができます。[Management Appliance] > [System Administration] > [Configuration File] ページの [Reset Configuration] セクションか、**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お勧めします。

（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

Cisco IronPort アプライアンスに現在インストールされている AsyncOS のバージョンを判別するには、次の手順を実行します。

ステップ 1　Security Management 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。

Security Management 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

Security Management 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」Security Management アプライアンスにコピーし、元の「ソース」Security Management 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。Security Management 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 Security Management 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 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 スパム検疫、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。

バックアップ機能では **backupconfig** コマンドを使用して、Security Management 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。

バックアップの制約事項

バックアップをスケジュール設定する前に、次の制約事項を考慮してください。

制約事項	要件
アプライアンスの容量	ターゲット アプライアンスには、ソース アプライアンスの容量以上の容量が必要です。
アプライアンスのバージョン	セキュリティ管理データ用の AsyncOS 7.7 は、セキュリティ管理用の AsyncOS 7.7 を実行している別の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 Security Management アプライアンスをアップグレードしてください。
アプライアンス間の通信	ソースとターゲットの Security Management アプライアンスは、SSH を使用して通信できる必要があります。このため次のようになります。 • 両方のアプライアンスでポート 22 が開いている。デフォルトで、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。 • A レコードと PTR レコードの両方を使用して、ドメイン ネーム サーバ（DNS）が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る。

制約事項	要件
複数、同時、および チェーン バックアップ	Security Management アプライアンスからのデータは、1 つの Security Management アプライアンスだけ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。 ある Security Management アプライアンスでバックアップがスケジュール設定されている場合、その Security Management アプライアンスに別のバックアップをスケジュール設定することはできません。別の Security Management アプライアンスにバックアップをスケジュール設定するには、まず、現在実行中のバックアップまたは将来のバックアップをすべてキャンセルします。

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。日次バックアップには、それぞれ 3 時間かかることがあります。週次および月次のバックアップには、さらに時間がかかる可能性があります。この時間は一定ではありません。

初期バックアップ後のバックアップ プロセスでは、最後のバックアップから変更されたファイルのみが転送されます。このため、その後のバックアップにかかる時間は初期バックアップの場合よりも短くなります。後続のバックアップに必要な時間は、累積されたデータ量、変更されたファイル数、および最後のバックアップ以降どの程度のファイルが変更されたかによって異なります。

バックアップ中のサービスのアベイラビリティ

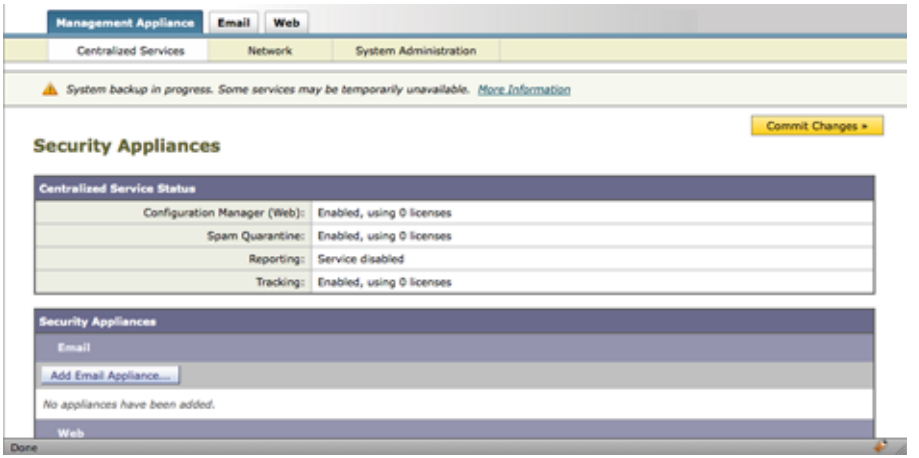
バックアップ プロセスのフェーズと、それらがサービスのアベイラビリティに及ぼす影響は次のとおりです。

- 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。初期シャットダウン後、ソースとターゲットのアプライアンス間でデータを転送しているときに収集されたすべての差が、ターゲット アプライアンスにコピーされ、ソースとターゲットの両方でサービスが開始されます。これにより、ソース アプライアンスで最大限の稼動時間が維持され、どちらのアプライアンスでもデータは失われなくなります。

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、Security Management 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。バックアップがキャンセルされても、バックアップ プロセスによって、ターゲット マシンにバックアップ済みのデータが消去されることはありません。

バックアップのスケジュール作成

（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。

Security Management アプライアンスでは、次の 2 つのタイプのバックアップをスケジュール設定できます。

- 定期バックアップ：定期バックアップには、事前設定した時間内に繰り返し行うバックアップと、事前設定した時間に 1 回行うバックアップがあります。
- 即時バックアップ：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。

定期バックアップ

（注） ログ ファイルは、定期的に保存することもできます。このプロセスの詳細については、「ログ サブスクリプション」（P.13-37）を参照してください。

定期バックアップをスケジュール設定するには、次の手順を実行します。

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　コマンド プロンプトで **Schedule** と入力し、Enter を押します。

ステップ 4　ターゲット Security Management 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、Security Management 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 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、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]：即時バックアップを開始できます。

ステップ 5　**1** を入力して、Enter を押します。

次の選択肢が表示されます。1.[Daily]、2.[Weekly]、3.[Monthly]。

ステップ 6　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 7　バックアップを開始する特定の日時を入力し、Enter を押します。

ステップ 8　バックアップ プロセスの名前を入力します。

後でこのバックアップ プロセスを確認できるよう、わかりやすい任意の名前にしてください。

これがバックアップのフェーズ 1 です。

コマンドライン プロンプトに **Status** と入力すると、次のように表示されます。

```
Phase: One
Centralized Email Tracking: Completed
Centralized Spam Quarantine: Completed
Centralized Email Reporting: Completed
Centralized Web Reporting: In Progress
```

この出力は、データを新しいターゲット マシンに転送中であることを示しています。

フェーズ 2 の最後で、データの転送は完了します。コマンドライン プロンプトに **Status** と入力すると、次のように表示されます。

```
Phase: Two
Centralized Email Tracking: Completed
Centralized Spam Quarantine: Completed
Centralized Email Reporting: Completed
Centralized Web Reporting: Completed
```

ステップ 9　データの転送が完了したら、バックアップが正常にスケジュール設定されたことを確認します。コマンド プロンプトで **View** と入力して、Enter を押します。

ステップ 10　完全なバックアップの詳細については、「その他の重要なバックアップ タスク」（P.12-15）を参照してください。

即時バックアップ

インスタント バックアップを開始するには、次の手順を実行します。

（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 Security Management 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、Security Management 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 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　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するには、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 7　完全なバックアップの詳細については、「その他の重要なバックアップ タスク」（P.12-15）を参照してください。

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、次のことを検討してください。

- 設定内容を保存する方法については、「コンフィギュレーション ファイルの管理」（P.12-110）を参照してください。
- Security Management 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、第 13 章「ロギング」を参照してください。

新しい Security Management アプライアンス ハードウェアのアップグレード

古い Security Management 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 Security Management 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 12-1　新しい Security Management 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 Security Management 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、Security Management 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 Security Management 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 Security Management 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、Security Management アプライアンスでのソフトウェア アップグレードに関連する次の内容について説明します。

アップグレードする前に：重要な手順

次の手順を実行して、アップグレードの準備を行います。

ステップ 1　次のようにして、データの消失を防止します。

- 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.12-123）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。

（注）　アップグレード後、再びリスナーをイネーブルにします。

AsyncOS をアップグレードする前に、アップグレードおよびアップデート設定が正しく設定されていることを確認します。詳細については、「アップグレードおよびサービス アップデートの設定」（P.12-34）を参照してください。

リモート アップグレードと ストリーミング アップグレード

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」）である、リモート アップグレードとストリーミング アップグレードを使用できます。

リモート アップグレードでは、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。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。

ストリーミング アップグレードでは、Cisco IronPort アプライアンスは HTTP を介して Cisco IronPort アップデート サーバから直接 AsyncOS アップグレードをダウンロードします。各 Cisco IronPort アプライアンスは、アップグレードを別個にダウンロードします。

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。

2 つのアップグレード方式を切り替えるには、[Management Appliance] > [System Administration] > [Update Settings] ページを使用します（ストリーミング アップグレードがデフォルトです）。CLI で **updateconfig** コマンドを使用する方法もあります。

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。

（注）　どちらのアップグレード方式を使用しても、アップグレードの完了後は、**saveconfig** コマンドを使用して設定を保存するかどうか判断する必要があります。詳細については、「コンフィギュレーション ファイルの管理」（P.12-110）を参照してください。

クラスタ化されたシステムのアップグレード

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。

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、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。

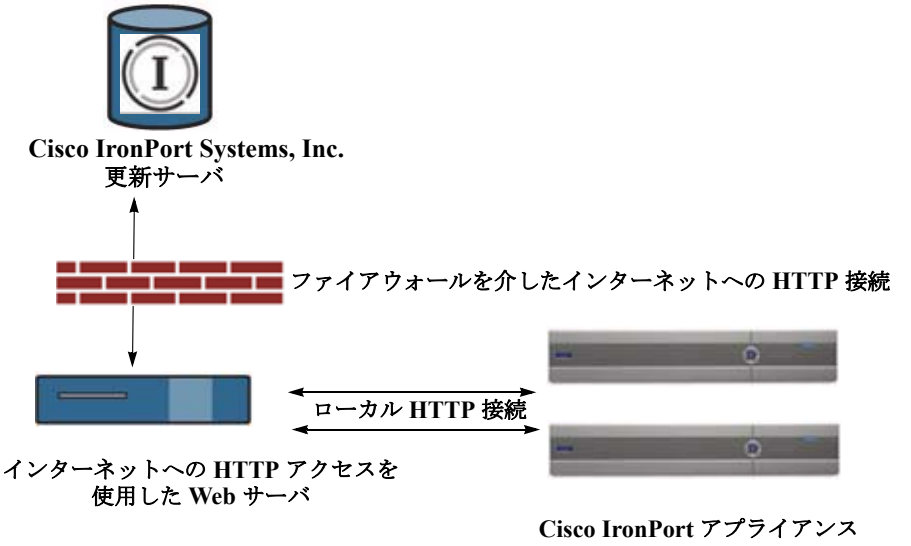
図 12-2　　ストリーミング アップデート方式

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 12-3　　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　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 2　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 3　[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 4　[Management Appliance] > [System Administration] > [System Upgrade] を選択します。

ステップ 5　[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。

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）。

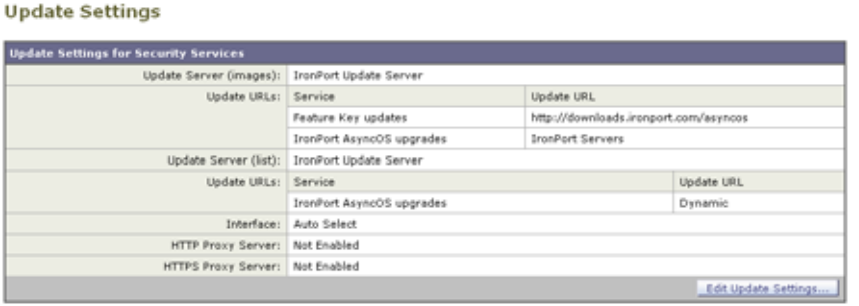
ネットワーク上の Cisco IronPort アプライアンスに使用可能なアップグレードを、`http://updates.ironport.com/fetch_manifest.html` で選択したバージョンに限定する XML ファイルを、ローカル サーバでホスティングすることもできます。この場合でも、Cisco IronPort アプライアンスは Cisco IronPort Systems アップデート サーバからアップグレードをダウンロードします。アップグレード リストをローカル サーバにホスティングする場合は、zip ファイルをダウンロードして、`asyncos/phoebe-my-upgrade.xml` 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。

GUI を使用したアップグレードの取得

（ストリーミングまたはローカル ソースで）アップグレードを取得する場所を指定するには、Security Management アプライアンスで、[Management Appliance] > [System Administration] > [Update Settings] を選択します。

図 12-4　[Update Settings] ページ



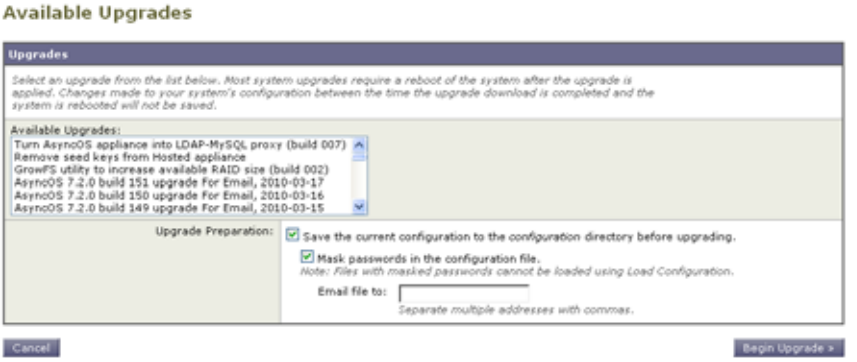
GUI からの AsyncOS のアップグレード

アップデートを設定後に AsyncOS をアップグレードするには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Management Appliance] > [System Administration] > [System Upgrade] > [Available Upgrades] を選択します。

[Available Upgrades] ページが表示されます。

図 12-5　[Available Upgrades] ページ



ステップ 2　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。

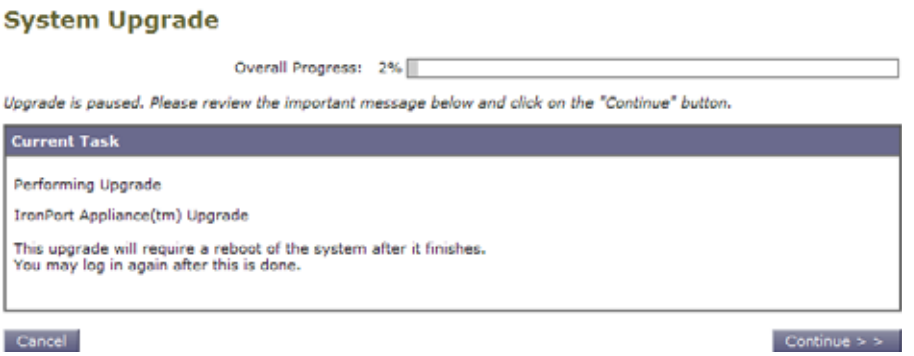
ステップ 3　アップグレード前に設定ディレクトリに現在の設定を保存する場合は、[Upgrade Preparation] セクションでチェックボックスをオンにします。この設定が推奨されます。

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。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。

ステップ 4　[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。

ステップ 5　プロンプトが表示されたら、変更点を確認するか、新しいライセンス契約を読んで、同意します。

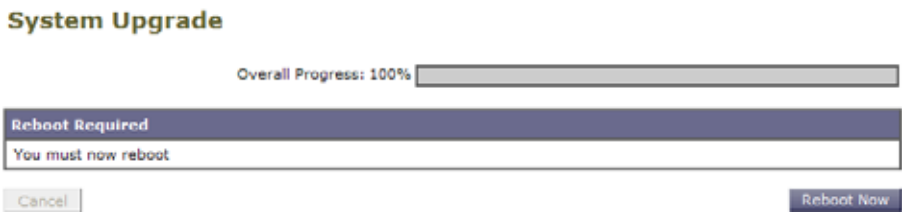
図 12-6　アップグレードの経過表示



ステップ 6　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 7　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。

図 12-7　アップグレードの完了



ステップ 8　[Reboot Now] をクリックします。

ステップ 9　アプライアンスが再度起動したら、サインインします。

ステップ 10　AsyncOS 7.2 よりも前のリリースからアップグレードする場合は、[Web] タブを最初にクリックしたときに、最新の Configuration Master を開始するようにプロンプトが出されます。詳細については、「Configuration Master の初期化」（P.8-8）を参照してください。

以前のバージョンの AsyncOS 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。

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

前の認定バージョンの AsyncOS に復元するには、次の手順を実行します。

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　Email Security 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　戻し先のバージョンの XML 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 11　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 12　Email Security 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 13　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動します。

（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。

CLI を使用したアップグレードの取得

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。

（注）　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。

updateconfig コマンド

updateconfig コマンドを使用すると、Cisco IronPort アプライアンスに AsyncOS アップグレードなどのサービス アップデートを探す場所を指示できます。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。リモート アップグレードの場合、updateconfig コマンドを発行して、アプライアンスがローカル アップデート サーバ（上記で設定したローカル サーバ）を使用するように設定します。

```
mail3.example.com> updateconfig

Service (images):                Update URL:
-------------------------------------------------------------------------
Feature Key updates              http://downloads.ironport.com/asyncos
Timezone rules                   IronPort Servers
IronPort AsyncOS upgrades        IronPort Servers

Service (list):                  Update URL:
-------------------------------------------------------------------------
Timezone rules                   IronPort Servers
IronPort AsyncOS upgrades        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]> 2

Enter the HTTP base URL of the update server using the format
(http://optionalname:password@local.server:port/directory/). The
default HTTP port is 80; you do not need to specify the port unless
you wish to use a non-standard port. The optional username/password
will be presented using HTTP BASIC_AUTH.
[http://downloads.ironport.com/]>enter URL of the local server here
```

（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。

upgrade コマンド

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。

```
mail3.example.com> upgrade

Would you like to save the current configuration to the configuration
directory before upgrading? [Y]> y

Do you want to include passwords? Please be aware that a configuration
without passwords will fail when reloaded with loadconfig. [N]> y

Email a copy? [N]> y

Enter email addresses. Separate multiple addresses with commas.
[]> admin@example.com

Upgrades available.
1. AsyncOS 7.7.0 For Security Management upgrade

[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
IronPort Security Management Appliance(tm) Upgrade
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]>

System rebooting.  Please wait while the queue is being closed.
```

アップグレード方式の違い（リモートとストリーミング）

従来の方式（ストリーミング アップグレード）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

時間帯ルールや AsyncOS アップグレードなど、Security Management アプライアンスがセキュリティ サービス アップデートをダウンロードする方法を設定できます。たとえば、ファイル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 の [Management Appliance] > [System Administration] > [Update Settings] ページか、CLI で `updateconfig` コマンドを使用して設定できます。

[Update Settings] ページまたは `updateconfig` CLI コマンドを使用して Cisco IronPort AsyncOS をアップグレードすることもできます。詳細については、「AsyncOS のアップグレード」（P.12-18）を参照してください。

（注） 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。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。アップデートに関して、ファイアウォール設定にスタティック IP アドレスが必要だと判断した場合、次の指示に従ってアップデート設定値を編集し、Cisco IronPort カスタマー サポートに必要な URL アドレスを問い合わせて取得します。

アップデート設定の編集

Cisco IronPort アプライアンスのアップデート設定を編集するには、[Edit Update Settings] ボタンをクリックして、[Edit Update Settings] ページを表示します。

表 12-1 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 12-1　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、Cisco IronPort アップデート サーバです。 次の条件のいずれかが該当する場合は、ローカル Web サーバを選択します。 • 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できますが、Cisco IronPort カスタマー サポートから提供されたスタティック アドレスを入力する必要があります。 • 一時的に、ローカル Web サーバに保存されたアップグレード イメージをダウンロードする場合。イメージをダウンロードした後、この設定を変えて Cisco IronPort アップデート サーバ（または使用している場合にはスタティック アドレス）に戻し、セキュリティ コンポーネントが自動的にアップデートされるようにすることをお勧めします。 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。

表 12-1　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
Update Servers (lists)	利用可能なアップグレードおよびセキュリティ 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、Cisco IronPort アップデート サーバです。ローカル Web サーバに保存されたアップグレード イメージを一時的にダウンロードする場合は、ローカル Web サーバを選択できます。イメージをダウンロードした後、この設定を変えて Cisco IronPort アップデート サーバに戻し、セキュリティ コンポーネントが自動的にアップデートされるようにすることをお勧めします。 ローカル アップデート サーバを選択した場合、サーバのファイル名およびポート番号を含む、リストのマニフェスト XML ファイルの完全なパスを入力します。ポートのフィールドを空のままにした場合、AsyncOS はポート 80 を使用します。サーバが認証を必要とする場合、有効なユーザ名とパスワードも入力します。 詳細については、「リモート アップグレードと ストリーミング アップグレード」（P.12-19）および「リモート アップグレードの概要」（P.12-21）を参照してください。
Automatic Updates	時間帯ルールなど、リストされているセキュリティ アップデートに対する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。
Interface	リストされたセキュリティ コンポーネントのアップデート、および Cisco IronPort AsyncOS のアップグレードをアップデート サーバに問い合わせるときに、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。

表 12-1　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
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。

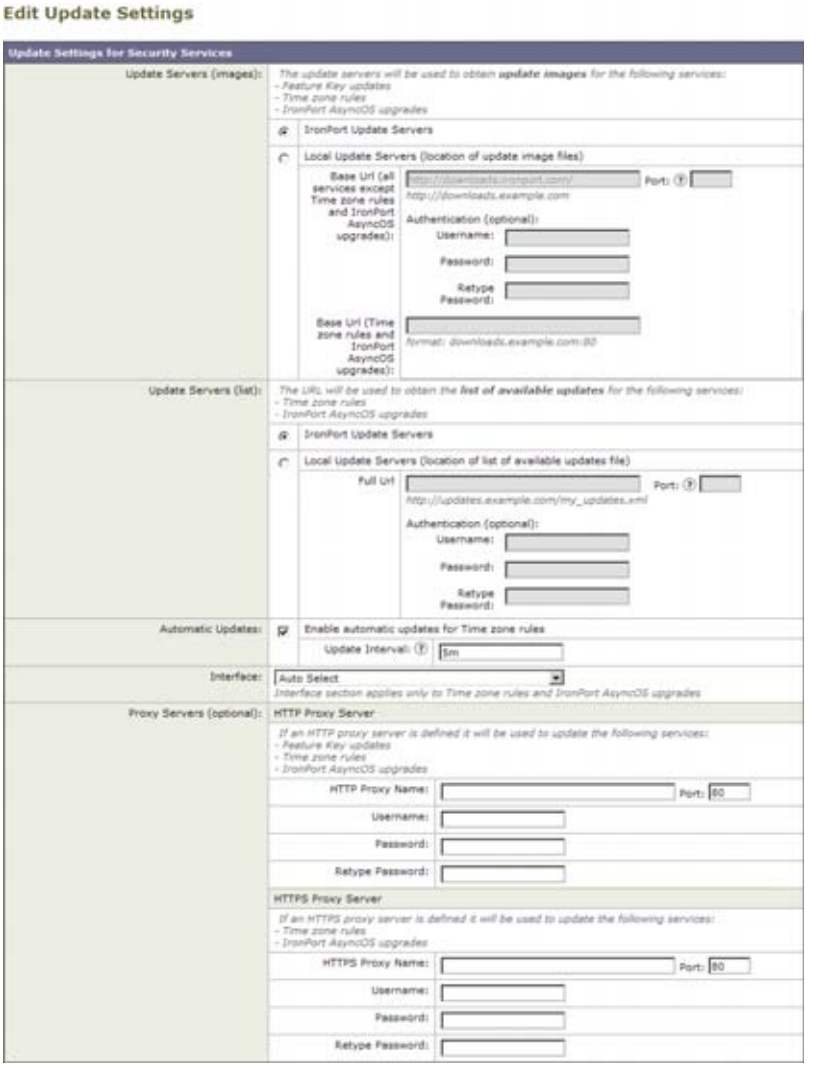
GUI からのアップデートおよびアップグレード設定値の設定

AsyncOS アップデートおよびアップグレード設定を編集するには、次の手順を実行します。

ステップ 1　[Management Appliance] > [System Administration] > [Update Settings] ページに移動し、[Edit Update Settings] をクリックします。[Edit Update Settings] ページが表示されます。

図 12-8 に、[Edit Update Settings] ページで設定できるオプションを示します。

図 12-8　[Edit Update Settings] ページ



ステップ 2　表 12-1（P.12-35）にある設定値を設定します。

ステップ 3　変更を送信し、保存します。

Security Management アプライアンスでのディザスタ リカバリ

ディザスタ リカバリによって、Security Management アプライアンスに突然障害が生じた場合に備えることができます。このような時点で障害管理やディザスタ リカバリを行うことは、データの保全に不可欠です。その場合は、システムでデータ整合性が保たれるように、データの実装および回復方法を把握しておくことが重要です。

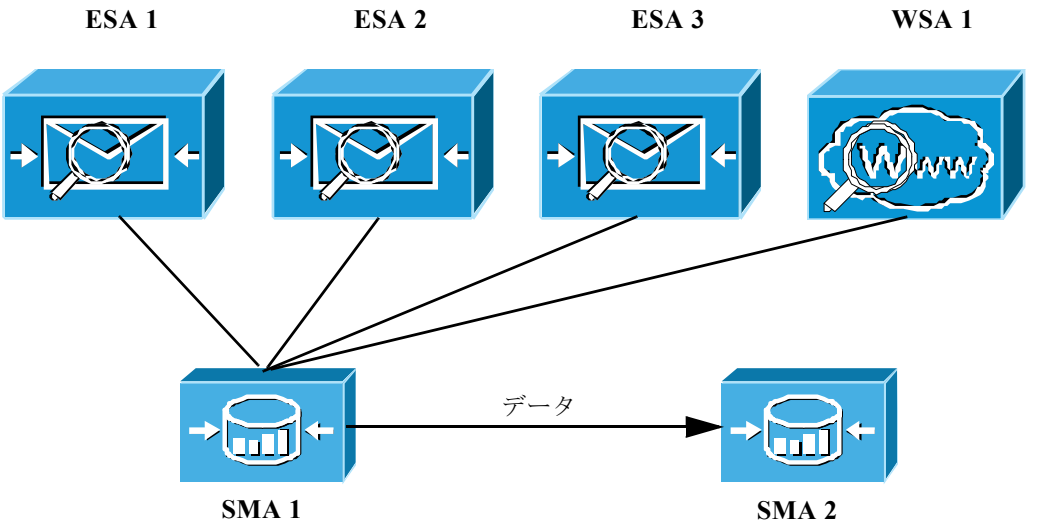
（注）　異なるサイズの Security Management アプライアンス間でデータを転送することはできますが、データの転送先となるアプライアンスには同等以上のサイズが割り当てられている必要があります。

これは推奨事項であり、Security Management アプライアンスのサイズの大きいものから小さいものへのディザスタ リカバリおよびバックアップを禁止する厳密なルールはありません。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 Security Management アプライアンスにあれば、ソースからターゲットへのバックアップをスケジュール設定できます。つまり、ターゲット アプライアンスのすべてのデータに割り当てられているディスク容量が、ソース アプライアンスのものよりも大きい必要があります。

たとえば、ソース アプライアンスが M1060 でターゲット アプライアンスが M650 であり、ソースよりもターゲットのほうが小さい場合、大きいほうの M1060 ですべてのデータに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 のアプライアンスにあるスペースと数字が一致するようにしてください。これは、GUI の [Disk Management] ページから行えます。また、小さいほうの M650 に格納できるサイズよりも多くのデータを、大きいほうの M1060 に置かないでください。

最初に、一般的な環境と設定を確認しておきます。一般的な環境では、アプライアンス設定は次の図 12-9 の設定のようになります。

図 12-9　ディザスタ リカバリ：一般的な環境



この環境では、SMA 1 がプライマリ Security Management アプライアンスであり、電子メール レポーティング、トラッキング、ISQ、および Web レポーティングの各データを ESA 1-3 および WSA 1 から受け取ります。SMA 2 がデータを受け取ると、SMA 1 でバックアップが実行され、フェールオーバー用に SMA 1 にあるすべてのデータがコピーされて SMA 2 に保存されます。Security Management アプライアンスのバックアップの詳細については、「Security Management アプライアンスのバックアップ」（P.12-8）を参照してください。

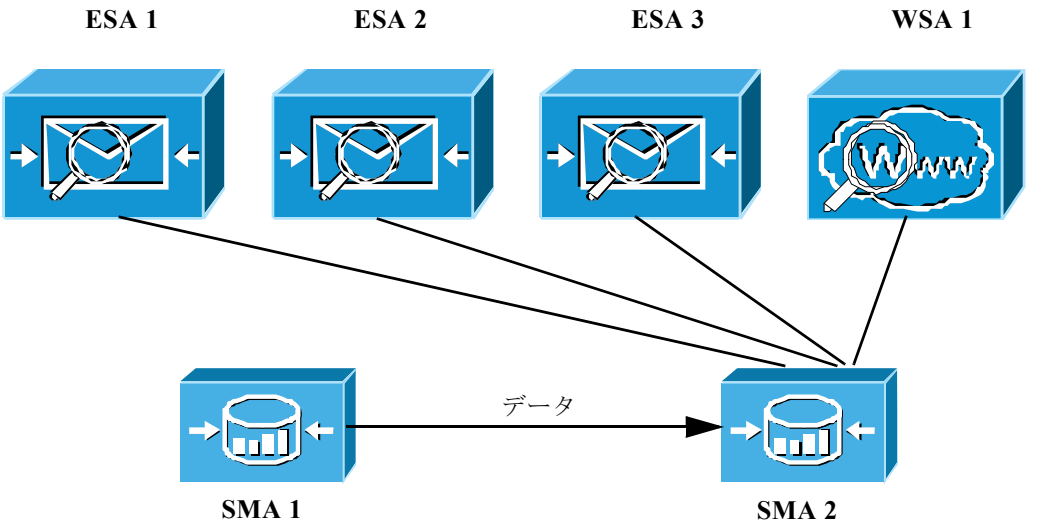
ここで、SMA 1 に障害が発生し始めていることが検出されたとします。レポートの受信速度が遅くなったり、データが壊れていたり、Security Management アプライアンスで障害が発生し始めていることを示す兆候が出ているなどです。次の手順に従って、ディザスタ リカバリを開始します。

ステップ 1　SMA1 から SMA 2 にインスタント バックアップを開始します。

この実行方法については、「即時バックアップ」（P.12-14）の手順を参照してください。

バックアップの実行後、環境設定は図 12-10 のようになります。

図 12-10　ディザスタ リカバリ：パート 1：インスタント バックアップ



すべてのデータが SMA 1 から SMA 2 へすぐに転送されます。また、ESA 1-3 と WSA 1 からもすべてのデータが SMA 2 に転送されます。これで、SMA 2 がプライマリ アプライアンスになりました。この時点で、手動で SMA 2 を設定する必要があります。

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。

- SMA 2 で、[Network] > [IP Interfaces] > [Add IP Interfaces] を選択します。
- [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　すべてのアプライアンスを新しい Security Management アプライアンス（SMA 2）に追加します。

アプライアンスの追加方法については、「管理対象アプライアンスの追加」（P.3-11）を参照してください。

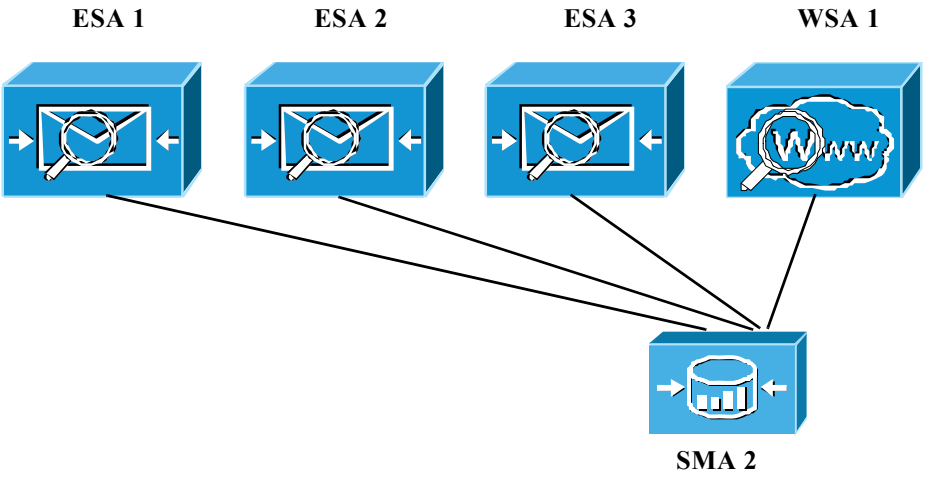
ステップ 5　新しい Security Management アプライアンス（SMA 2）ですべてのサービスをイネーブルにします。

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。サービスのイネーブル化の詳細については、「Security Management アプライアンスでのサービスのイネーブル化」（P.3-3）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、図 12-11 に示すように、すべてのデータが SMA2 に送られるようになりました。

図 12-11　ディザスタ リカバリ：パート 2：新しい Security Management アプライアンス



（注）　**saveconfig** コマンドを使用して定期的に設定を保存していた場合、**loadconfig** コマンドを使用して、保存したこのコンフィギュレーション ファイルを新しい Security Management アプライアンス（この例では SMA 2）にロードし、ステップ 2 で説明されているように、新しい ID アドレスを設定できます。コンフィギュレーション ファイルには、SMA 2 が機能するために必要なすべての情

報が含まれているわけではありません。新しい Security Management アプライアンスに、すべてのアプライアンスを追加する必要があります。ここで、各アプライアンスへの接続を確立し、接続をテストする必要があります。

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、他のユーザに管理タスクを分散できます。

Security Management 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。

事前定義ロールの詳細については、「ユーザ ロール」（P.12-43）を参照してください。

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 ロールへの管理委任」（P.12-49）を参照してください。

ユーザ アカウントの詳細については、「GUI でのユーザ管理」（P.12-59）を参照してください。

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 12-2　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	アプライアンス
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、および **revert**（**ESA のみ**）コマンドを発行できるのは **admin** ユーザだけです。	あり / あり	Security Management アプライアンス
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。 Email Security アプライアンスでは、以前は **admin** ユーザだけが使用できた機能を、Administrator ロールが割り当てられたユーザがすべて使用できるようになりました。	あり / あり	Security Management アプライアンス、Web セキュリティ アプライアンス Email Security アプライアンス

表 12-2　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	アプライアンス
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 • `upgradecheck` コマンドによる、使用可能なアップグレードの確認 • **upgradeinstall** コマンドによる、アップグレードのインストール • 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	Security Management アプライアンス、Web セキュリティ アプライアンス、Email Security アプライアンス
Technician	Technician ロールを持つユーザ アカウントは、管理機能キーのアップグレードやリブートなどのシステム管理アクティビティを開始できます。このロールには、ポリシー、HAT、または RAT など、電子メール特有の機能へのアクセス権はありません。	なし / なし	Security Management アプライアンス、Web セキュリティ アプライアンス Email Security アプライアンス

表 12-2　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	アプライアンス
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変更を行って送信できますが、保存できません。また、このロールを持つユーザは Cisco IronPort スパム検疫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	Security Management アプライアンス、Web セキュリティ アプライアンス Email Security アプライアンス
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 スパム検疫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	Security Management アプライアンス、Web セキュリティ アプライアンス、Email Security アプライアンス
Web Administrator	Web Administrator ロールを持つユーザ アカウントは、[User Role] メニューでのみ、すべての設定へのアクセス権を持っています。	あり / なし	Security Management アプライアンス

表 12-2　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	アプライアンス
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	Security Management アプライアンス
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	Security Management アプライアンス
Email Administrator	Email Administrator ロールを持つユーザ アカウントは、Cisco IronPort スパム検疫およびシステム検疫権など、[Email] メニューでのみ、すべての設定へのアクセス権を持ちます。	なし / なし	Security Management アプライアンス
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 スパム検疫の管理 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 スパム検疫の管理を行うには、そのスパム検疫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	Security Management アプライアンス、Email Security アプライアンス

表 12-2　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	アプライアンス
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 ロールへの管理委任」（P.12-49）を参照してください。	なし / なし	Security Management アプライアンス、Email Security アプライアンス

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、「外部認証」（P.12-71）を参照してください。

ユーザがスパム検疫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 スパム検疫の管理ユーザの設定」（P.7-6）を参照してください。

カスタム ユーザ ロールへの管理委任

Administration 権限を持つユーザは、Security Management 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、次を参照してください。

- 「Custom Email User ロールについて」（P.12-49）
- 「Custom Web User ロールについて」（P.12-55）

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 Security Management 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
- スパム検疫

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 Email Security アプライアンスから直接作成することもできます。Email Security アプライアンスのカスタム ユーザ ロールは、Security Management 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」セクションを参照してください。

電子メール レポーティング

次のセクションで説明するように、電子メール レポートへのアクセス権をカスタム ユーザ ロールに付与できます。

Security Management 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 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 Email Security 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 Sender
- 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 Email Security 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 Email Security 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、Security Management 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 トラッキングでの機密情報へのアクセスのディセーブル化」（P.12-63）を参照してください。

Security Management 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。

検疫

カスタム ロールに検疫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 Security Management アプライアンスのスパム検疫メッセージを検索、表示、配信、または削除できます。

ユーザがスパム検疫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 スパム検疫の管理ユーザの設定」（P.7-6）を参照してください。

Security Management アプライアンスからこの検疫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、スパム検疫の詳細については、「Cisco IronPort スパム検疫の管理」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、およびスパム検疫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 Email Security 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　メイン Security Management アプライアンスで、[Management Appliance] > [System Administration] > [User Roles] を選択します。

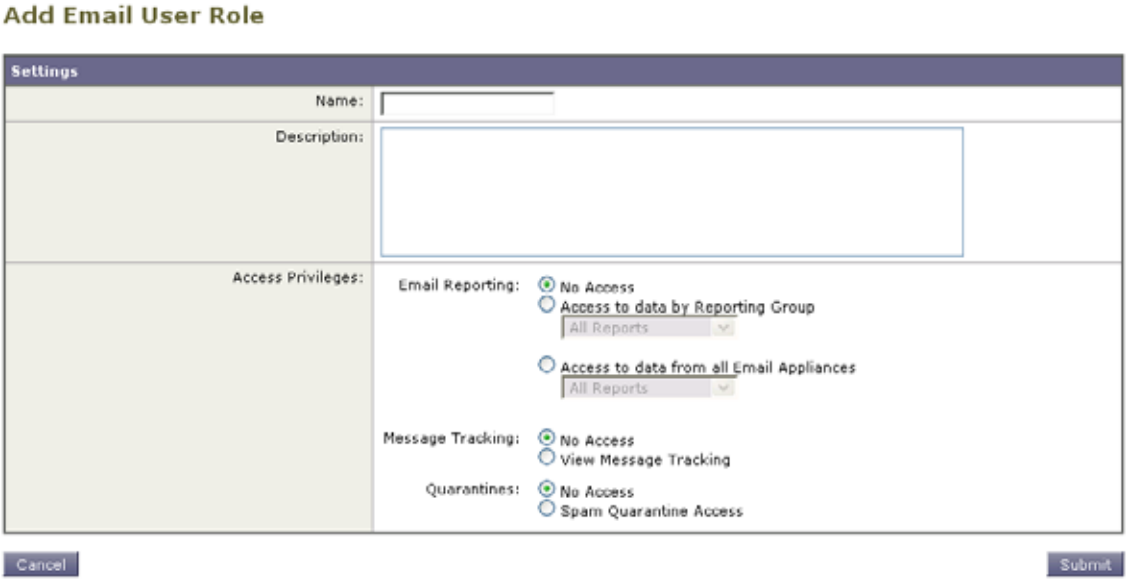
[User Roles] ページが表示されます。

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。

[Add Email User Role] ページが表示されます。

図 12-12　[Add Email User Role] ページ



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検疫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 スパム検疫の管理ユーザの設定」（P.7-6）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。

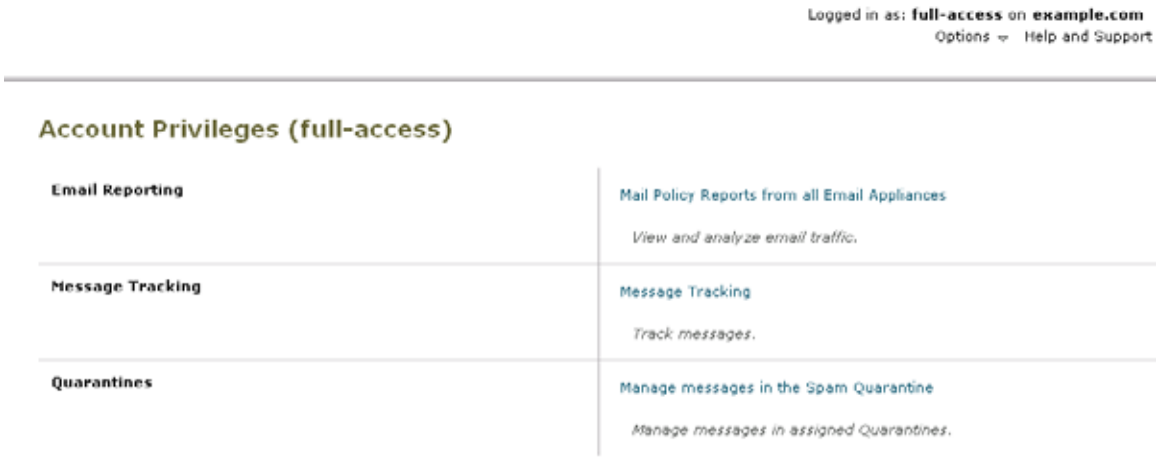
ステップ 3　変更を送信し、保存します。

ステップ 4　このロールにスパム検疫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 スパム検疫の管理ユーザの設定」（P.7-6）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、Security Management 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 12-13　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。

Security Management 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

Custom Web User ロールを作成するには、次の手順を実行します。

ステップ 1　メイン Security Management アプライアンスで、[Management Appliance] > [System Administration] > [User Roles] を選択します。

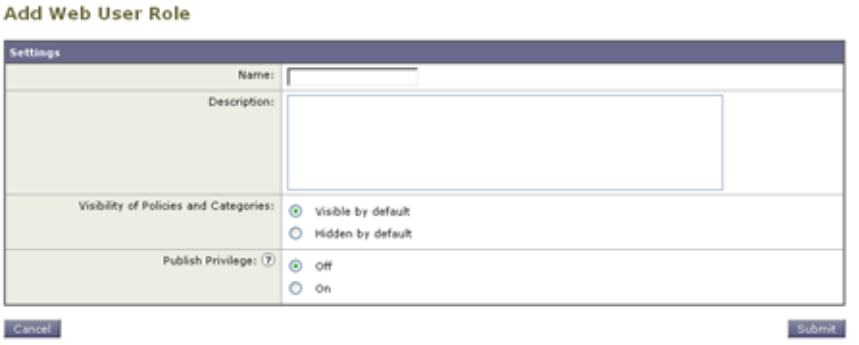
[User Roles] ページが表示されます。

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。

[Add Web User Role] ページが表示されます。

図 12-14　[Add Web User Role] ページ



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」のスケジュール設定されたレポートの管理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。

図 12-15　[User Roles] ページ

（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

Custom Web User ロールの設定を編集するには、次の手順を実行します。

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。

GUI でのユーザ管理

管理タスクを実行するには、ユーザ アカウントを使用して、ユーザ ロールを割り当てることができます。

Cisco IronPort アプライアンスにはユーザ アカウントを追加するための 2 つの方法が用意されています。1 つは、ユーザ アカウントをアプライアンス自体に作成する方法で、もう 1 つは、独自の中央集中型認証システムを使用してユーザ認証をイネーブルにする方法です。これには、LDAP または RADIUS ディレクトリを使用できます。ユーザ、または外部認証ソースへの接続の管理は、GUI の [Management Appliance] > [System Administration] > [Users] ページで（または CLI で **userconfig** コマンドを使用して）行うことができます。ユーザの認証に外部ディレクトリを使用する方法の詳細については、「外部認証」（P.12-71）を参照してください。

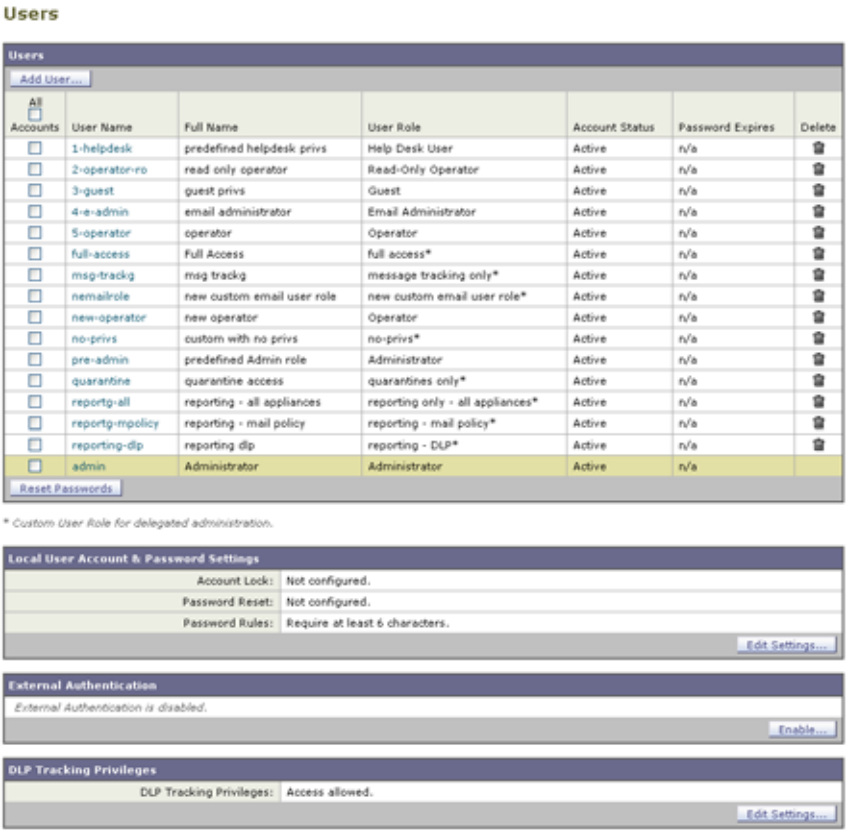
アプライアンスに作成できるユーザ アカウントの数に制限はありません。

ユーザ アカウントを管理するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Management Appliance] > [System Administration] > [Users] を選択します。

[Users] ページが表示されます。

図 12-16　[Users] ページ



[Users] ページには、システムの既存の管理ユーザが一覧（ユーザ名、氏名、およびユーザ ロールを含む）で表示されます。[Users] ページには、外部認証がイネーブルであるかどうかと、認証タイプも表示されます。

（注）　アスタリスクは、委任された管理に応じてユーザに割り当てられたカスタム ユーザ ロールを示します。ユーザのカスタム ロールが削除された場合は、[Unassigned] と赤く表示されます。ユーザ ロールの詳細（説明など）については、「ユーザ ロール」（P.12-43）を参照してください。

[Users] ページからは、次の操作が行えます。

- 新しいユーザの追加。
- ユーザの削除。
- ユーザの編集（admin ユーザのパスワード変更など）。
- 外部認証設定の編集。

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 Security Management アプライアンスに直接追加します。

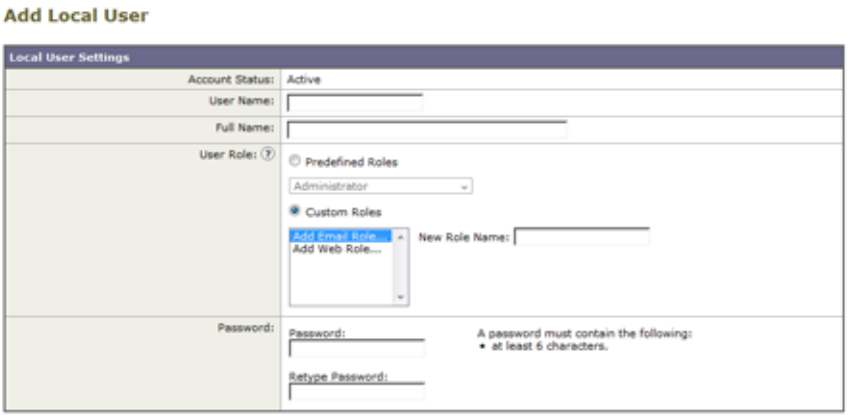
ステップ 1　カスタム ユーザ ロールを割り当てる場合は、そのロールを先に定義しておくことをお勧めします。「カスタム ユーザ ロールへの管理委任」（P.12-49）を参照してください。

ステップ 2　Security Management 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。

[Add Local User] ページが表示されます。

図 12-17　　ユーザの追加



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。

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 12-2 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.12-52）または「Custom Web User ロールの作成」（P.12-56）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　[Submit] をクリックして、ユーザを追加します。

ステップ 9　[Commit] をクリックして変更を確定します。

ステップ 10　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 ロールへの管理委任」（P.12-49）を参照してください。

ユーザの編集

ユーザを編集（パスワードの変更など）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。[Edit Local User] ページが表示されます。

ステップ 2　ユーザに対して変更を行います。

ステップ 3　[Submit] をクリックし、[Commit] をクリックして変更を確定します。

ユーザの削除

ユーザを削除するには、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確定します。

メッセージ トラッキングでの機密情報へのアクセスのディセーブル化

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、メッセージ トラッキングへのアクセス権を持つ、管理者以外のユーザには表示されないようにすることができます。管理者ユーザは、常にこのコンテンツを表示できます。

管理者以外のユーザに機密情報を表示し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] > [System Administration] > [Users] ページに移動します。

ステップ 2　[DLP Tracking Privileges] の下にある [Edit Settings] をクリックします。

[DLP Tracking Privileges] ページが表示されます。

図 12-18　[DLP Tracking Privileges] ページ

ステップ 3　[Allow access to DLP Matched Content in Message Tracking results] チェックボックスをオフにします。

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。

複数のユーザをサポートする追加コマンド：who、whoami、last

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
```

制限ユーザ アカウントとパスワードの設定

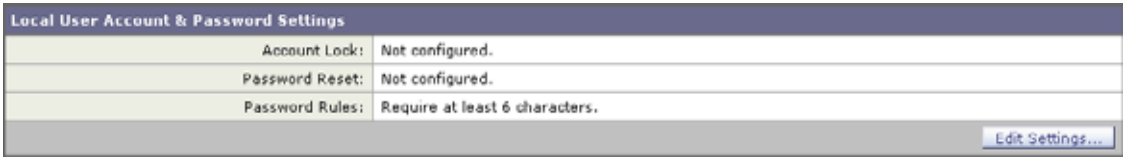
ユーザ アカウントとパスワードの制限を定義して、組織全体にパスワード ポリシーを強制的に適用することができます。ユーザ アカウントとパスワードの制限は、Cisco IronPort アプライアンスに定義されたローカル ユーザに適用されます。次の設定値を設定できます。

- **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。

ユーザ アカウントおよびパスワードの制限は、[Local User Account] および [Password Settings] セクションの、[Management Appliance] > [System Administration] > [Users] ページで定義できます。

図 12-19 に、[Users] ページの [Local User Account] および [Password Settings] セクションを示します。

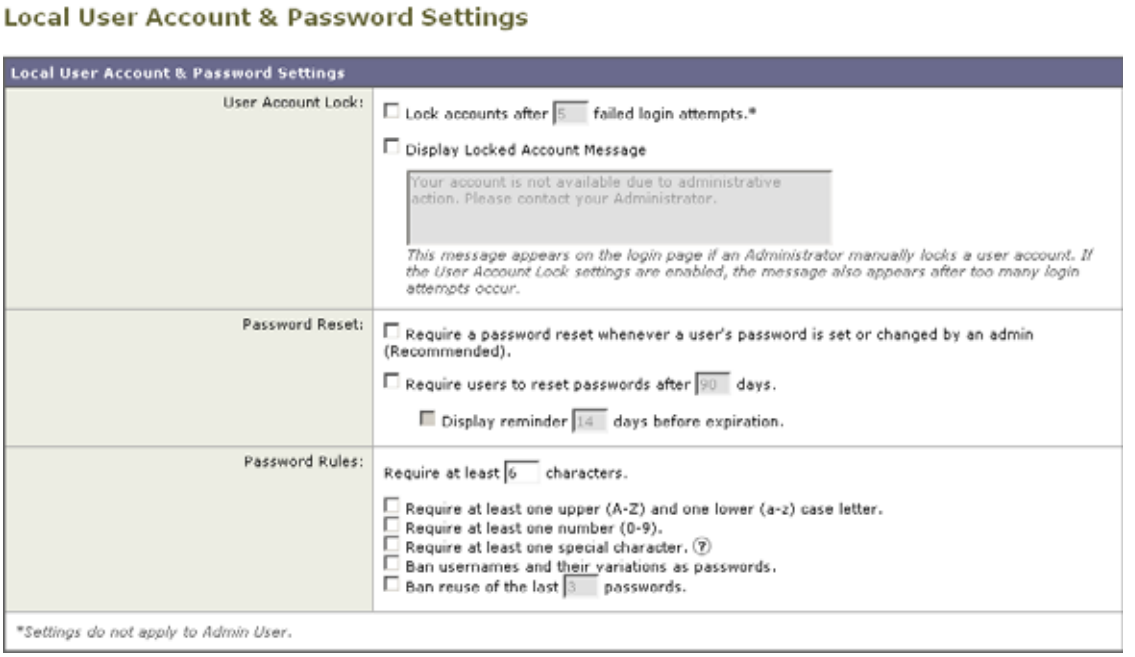
図 12-19　[Users] ページ、[Local User Account] および [Password Settings] セクション



ユーザ アカウントとパスワードの制限を設定するには、次の手順を実行します。

ステップ 1　[Management Appliance] > [System Administration] > [Users] ページの [Local User Account and Password Settings] セクションで、[Edit Settings] をクリックします。[Local User Account and Password Settings] ページが表示されます。

図 12-20　ユーザ アカウントとパスワード制限の設定



ステップ 2　表 12-4 に示す設定値を設定します。

表 12-4　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」セキュリティ 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。

表 12-4　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。 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。

表 12-4　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: 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。 ~ ?!@ # $ % ^ & * - _ + = ¥ | / [ ] ( ) < > { } ` ' " ; : , .
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 3　変更を送信し、保存します。

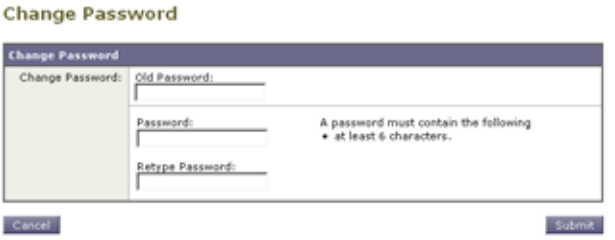
パスワードの変更

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、「ユーザの編集」（P.12-62）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、「ユーザの編集」（P.12-62）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。

GUI 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。

図 12-21　[Change Password] ページ



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、確認のためにもう一度新しいパスワードを入力します。[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。

外部認証

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、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。

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。

ステップ 1　Security Management アプライアンスで、[Management Appliance] > [System Administration] > [Users] を選択します。

（注）　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、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。

図 12-22　外部認証の確立

（注）　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、コマンドライン プロンプトで **userconfig** コマンドと **external** サブコマンドを使用します。

LDAP 認証のイネーブル化

ユーザを認証するために LDAP ディレクトリを使用する以外に、LDAP グループを Cisco IronPort ユーザ ロールに割り当てることができます。たとえば、IT というグループ内のユーザに Administrator ユーザ ロールを割り当て、Support というグループのユーザに Help Desk User ロールを割り当てることができます。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。

LDAP を使用して外部認証をイネーブルにする前に、LDAP サーバ プロファイルと LDAP サーバの外部認証クエリーを定義します。詳細は、『*Cisco IronPort AsyncOS for Email Advanced User Guide*』の LDAP クエリーに関する章を参照してください。

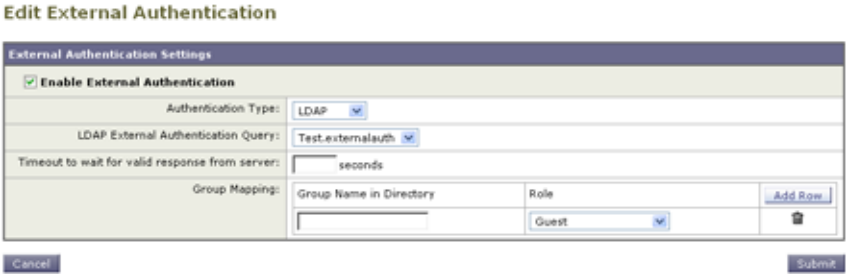
LDAP を使用して外部認証をイネーブルにするには、次の手順を実行します。

ステップ 1　Security Management 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。

[Edit External Authentication] ページが表示されます。

図 12-23　　LDAP を使用した外部認証のイネーブル化



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　[Submit] をクリックし、[Commit] をクリックして変更を確定します。

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。

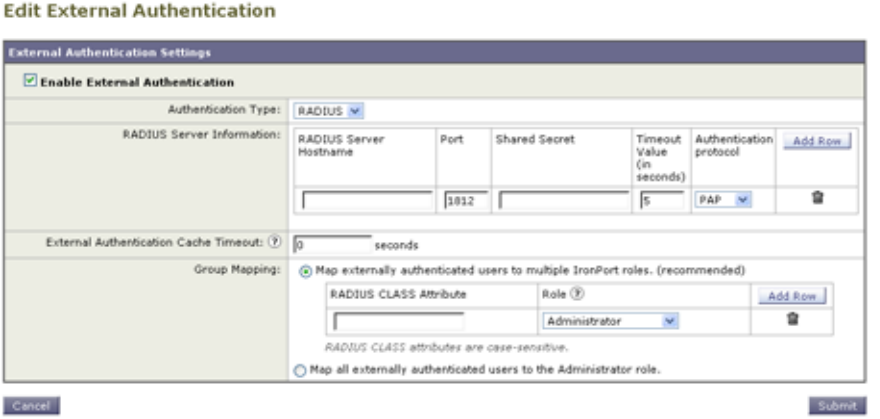
RADIUS を使用して外部認証をイネーブルにするには、次の手順を実行します。

ステップ 1　[Management Appliance] > [System Administration] > [Users] ページで、[Enable] をクリックします。[Edit External Authentication] ページが表示されます。

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。

図 12-24　RADIUS を使用した外部認証のイネーブル化



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。

Security Management アプライアンスへのアクセス権の設定

AsyncOS では、Security Management アプライアンスへのユーザのアクセス権管理を、管理者が制御できます。これを使用して、Web UI セッションのタイムアウトや、ユーザと組織のプロキシ サーバからアプライアンスへのアクセス元となる IP アドレスを指定する、アクセス リストなどを管理できます。

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 Security Management 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

Security Management 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 Security Management 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 Email Security 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.
```

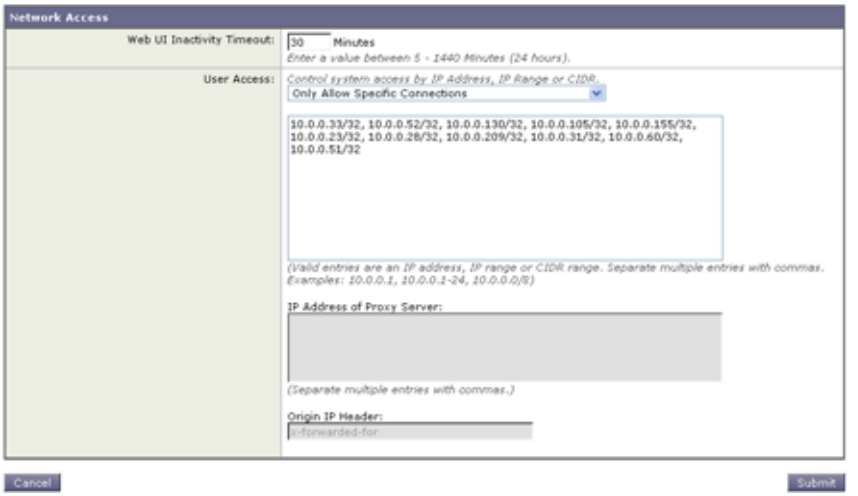
このヘッダーの値はカンマ区切りの IP アドレスのリストであり、左端のアドレスがリモート ユーザ マシンのアドレスで、その後に、接続要求を転送した一連の各プロキシのアドレスが続きます。（ヘッダー名は設定可能です）。Security Management アプライアンスは、ヘッダーから取得したリモート ユーザの IP アドレスおよび接続プロキシの IP アドレスを、アクセス リスト内の許可されたユーザ IP アドレスおよびプロキシ IP アドレスと照合します。

（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 12-25 は、Security Management 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 12-25　[Network Access] の設定



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。

Security Management アプライアンスのアクセス リストを作成するには、次の手順を実行します。

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　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。

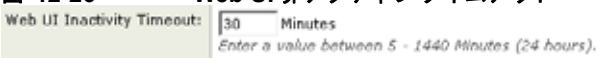
Web UI セッション タイムアウトの設定

Security Management 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 スパム検疫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。

図 12-26　Web UI 非アクティブ タイムアウト



Web UI セッションに非アクティブ タイムアウトを定義するには、次の手順を実行します。

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。

アクティブなセッションの表示

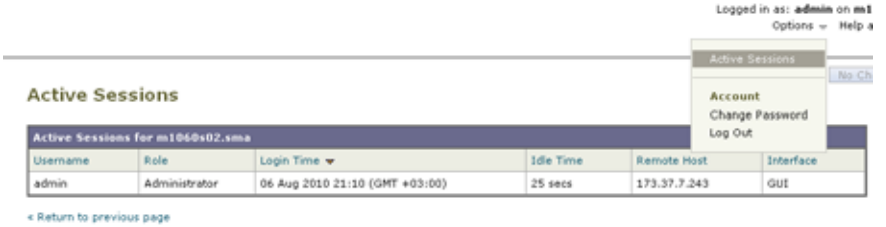
Security Management アプライアンスでは、アプライアンス上のすべてのアクティブなセッションと、ログインしているユーザを表示できます。

アクティブなセッションを表示するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスのページで、[Options] > [Active Sessions] を選択します。

[Active Sessions] ページが表示されます。

図 12-27　[Active Sessions] ページ



[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。

生成されたメッセージの返信アドレスの設定

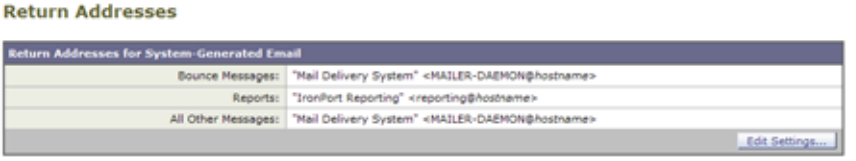
次の場合に対して、AsyncOS で生成されたメールのエンベロープ送信者を設定できます。

- 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 12-28　[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.12-89）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.12-90）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。

- System
- Hardware

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。

SMTP ルートおよびアラート

アプライアンスから [Alert Recipient] セクションで指定されたアドレスに送信されるアラートは、該当の送信先に対して定義された SMTP ルートに従います。

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 はシステムの稼動時間、**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.12-89）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

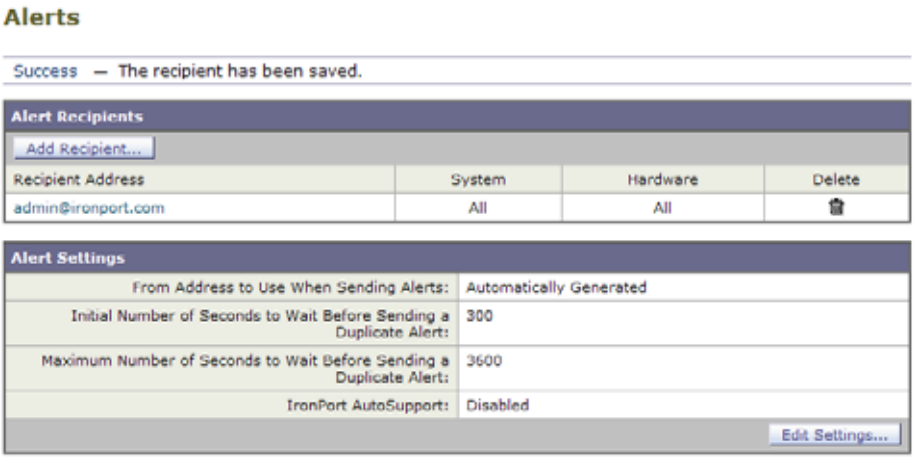
```
Date: 23 Mar 2007 21:10:19 +0000

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: XXXXXXXXXXXX-XXXXXXX

Timestamp: Tue May 10 09:39:24 2007
```

```
For more information about this error, please see

    http://support.ironport.com

If you need further information, contact your support provider.
```

アラート受信者の管理

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、「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）を参照してください）。

図 12-29　[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。

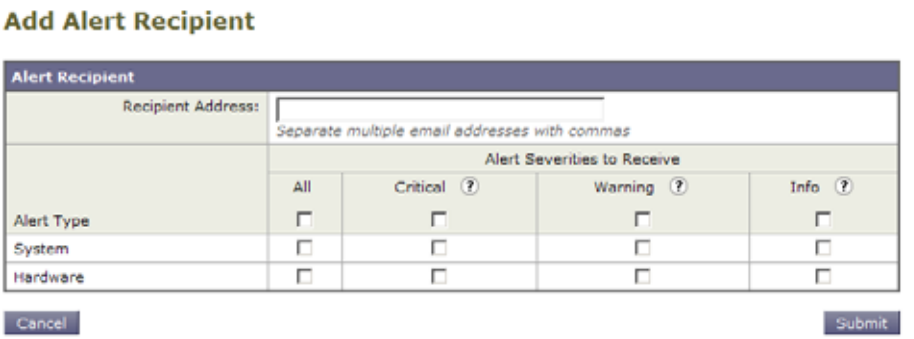
- アラート受信者の追加、設定、または削除。
- アラート設定値の変更。

新規アラート受信者の追加

新規アラート受信者を追加するには、次の手順を実行します。

ステップ 1　[Alerts] ページで [Add Recipient] をクリックします。[Add Alert Recipients] ページが表示されます。

図 12-30　　アラート受信者の追加



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

既存のアラート受信者を編集するには、次の手順を実行します。

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。[Configure Alert Recipient] ページが表示されます。

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

アラート受信者を削除するには、次の手順を実行します。

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

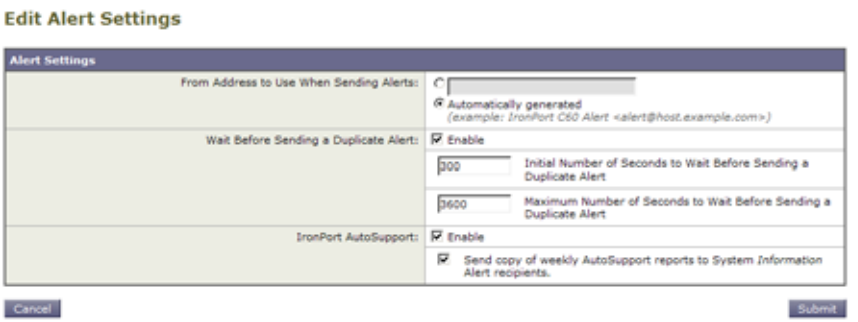
アラート設定はグローバルな設定であるため、すべてのアラートの動作に影響します。

アラート設定値の編集

アラート設定値を編集するには、次の手順を実行します。

ステップ 1　[Alerts] ページで [Edit Settings] をクリックします。[Edit Alert Settings] ページが表示されます。

図 12-31　アラート設定値の編集



ステップ 2　アラートの送信に使用する Header From: アドレスを入力するか、[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.12-84）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.12-85）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 12-5 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 12-5　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 12-6 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 12-6　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 12-6　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

表 12-6　システム アラートのリスト（続き）

アラート名	説明	重大度
MAIL.RES_CON_START_ALERT.QUEUE_SLOW	メール キューが過負荷となり、システム リソース節約がイネーブルになった場合に送信されます。	Critical
MAIL.RES_CON_START_ALERT.QUEUE	キュー使用率がシステム リソース節約しきい値を超過した場合に送信されます。	Critical
MAIL.RES_CON_START_ALERT.WORKQ	ワーク キューのサイズが大きすぎるため、リスナーが一時停止された場合に送信されます。	Critical
MAIL.RES_CON_START_ALERT	アプライアンスが「リソース節約」モードに入った場合に送信されます。	Critical
MAIL.RES_CON_STOP_ALERT	アプライアンスの「リソース節約」モードが解除された場合に送信されます。	Critical
MAIL.WORK_QUEUE_PAUSED_NATURAL	ワーク キューが中断された場合に送信されます。	Critical
MAIL.WORK_QUEUE_UNPAUSED_NATURAL	ワーク キューが再開された場合に送信されます。	Critical
NTP.NOT_ROOT	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

表 12-6　システム アラートのリスト（続き）

アラート名	説明	重大度
REPORTD.AGGREGATION_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_PUSH_FAILED	1 台以上のホストでコンフィギュレーションのプッシュに失敗した場合に送信されます。	Warning
SMAD.TRANSFER.TRANSFERS_STALLED	SMA ログがトラッキング データを 2 時間取得できなかった場合、またはレポーティング データを 6 時間取得できなかった場合に送信されます。	Warning
SMTPAUTH.FWD_SERVER_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 12-6　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 ウィザードについて」（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 12-7　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「二重 DNS ルックアップ」の実行を試みます。つまり、二重 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.12-97）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。

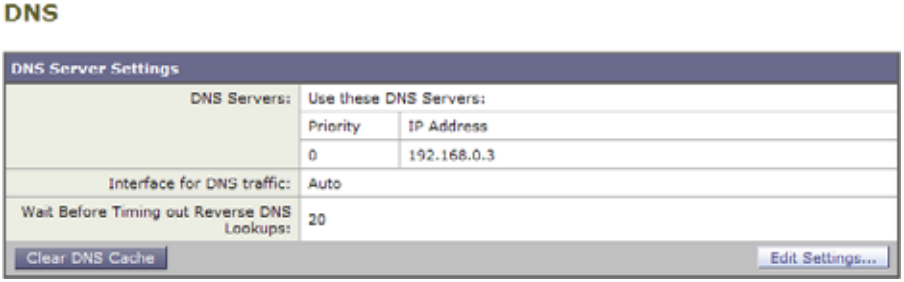
DNS キャッシュのクリア

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

GUI にログインして、[Management Appliance] > [Network] > [DNS] を選択します。

図 12-32　　[DNS] ページ

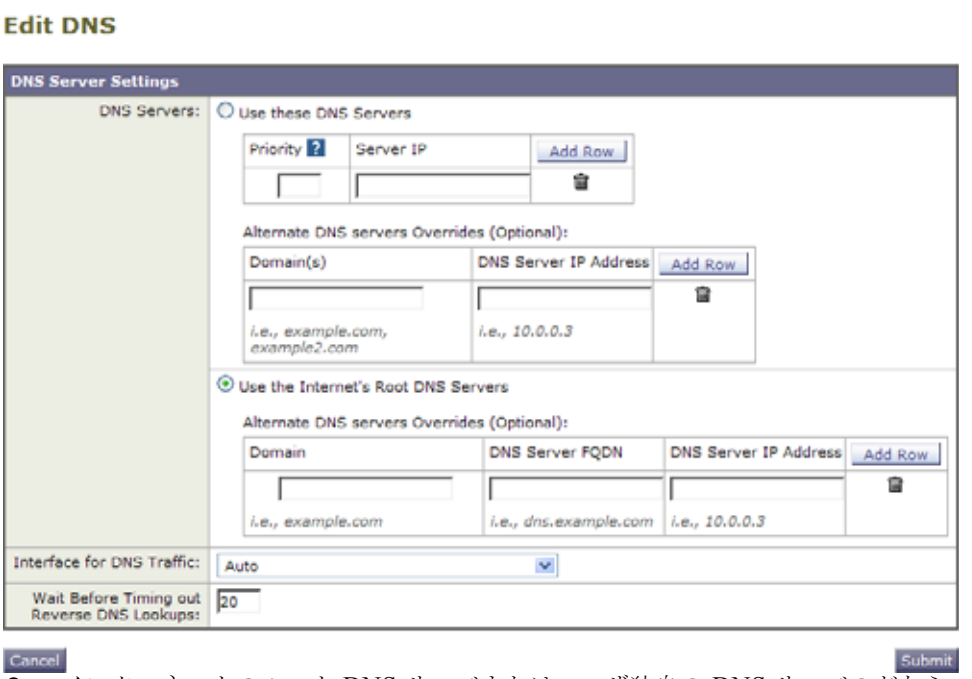


DNS 設定値を GUI から編集するには、次の手順を実行します。

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。

[Edit DNS] ページが表示されます。

図 12-33　[Edit DNS] ページ



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.12-97）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

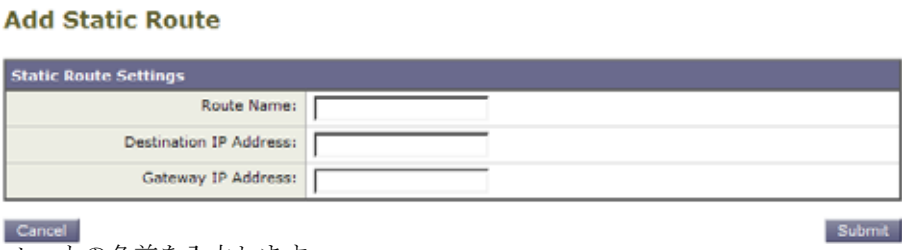
[Management Appliance] > [Network] > [Routing] ページを使用して、スタティック ルートの作成、編集、または削除を行えます。このページからデフォルト ゲートウェイの変更もできます。

スタティック ルートの追加

新しいスタティック ルートを作成するには、次の手順を実行します。

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。[Add Static Route] ページが表示されます。

図 12-34　スタティック ルートの追加



ステップ 2　ルートの名前を入力します。

ステップ 3　宛先 IP アドレスを入力します。

ステップ 4　ゲートウェイの IP アドレスを入力します。

ステップ 5　変更を送信し、保存します。

スタティック ルートの削除

スタティック ルートを削除するには、次の手順を実行します。

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

スタティック ルートを編集するには、次の手順を実行します。

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。[Edit Static Route] ページが表示されます。

ステップ 2　ルートの設定を変更します。

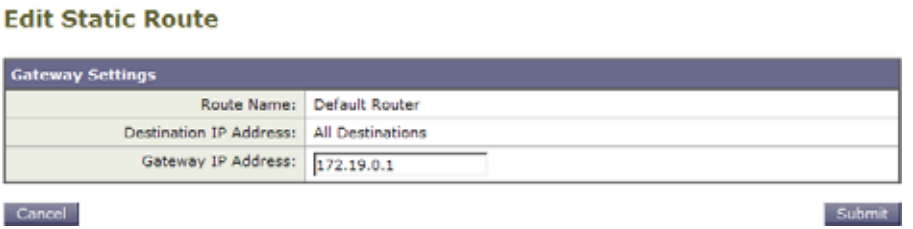
ステップ 3　変更を送信し、保存します。

デフォルト ゲートウェイの変更（GUI）

デフォルト ゲートウェイを変更するには、次の手順を実行します。

ステップ 1　[Routing] ページのルート リストで [Default Route] をクリックします。[Edit Static Route] ページが表示されます。

図 12-35　デフォルト ゲートウェイの編集



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.12-103）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、「ユーザの編集」（P.12-62）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

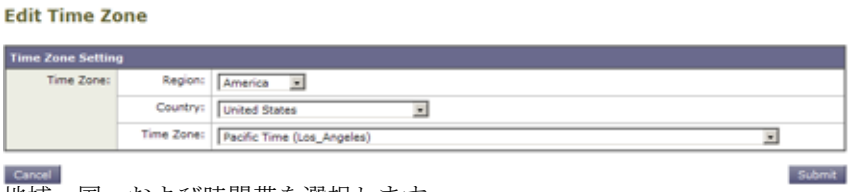
[Time Zone] ページ（GUI の [System Administration] メニューから利用可能）では、Cisco IronPort アプライアンスの時間帯が表示されます。特定の時間帯または GMT オフセットを選択できます。

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] ページで、[Edit Settings] をクリックします。[Edit Time Zone] ページが表示されます。

図 12-36　[Edit Time Zone] ページ



ステップ 2　地域、国、および時間帯を選択します。

ステップ 3　変更を送信し、保存します。

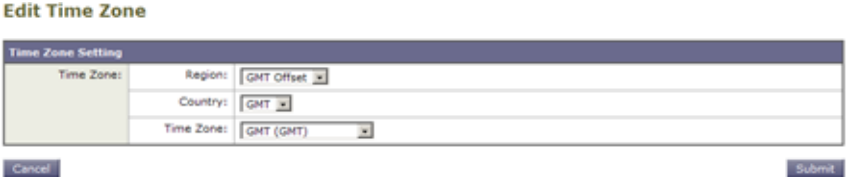
GMT オフセットの選択

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] ページで、[Edit Settings] をクリックします。[Edit Time Zone] ページが表示されます。

ステップ 2　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 12-37　GMT オフセットの設定



ステップ 3　[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。

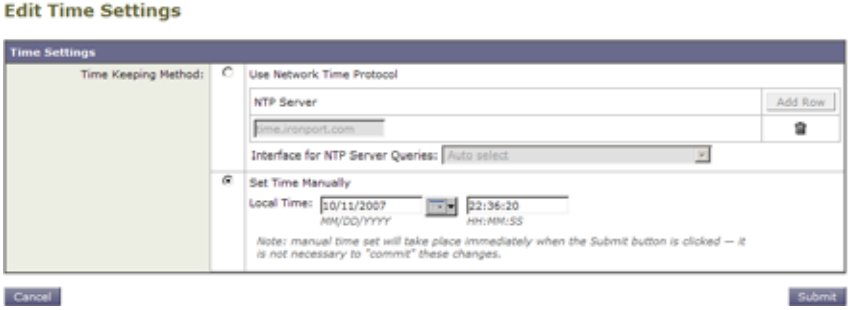
ステップ 4　変更を送信し、保存します。

（注）　Security Management アプライアンスは、レポートのデータを収集する際に、Security Management 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。Security Management 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.3-17）を参照してください。

時刻設定の編集（GUI）

Cisco IronPort アプライアンスの時刻設定を編集するには、[Management Appliance] > [System Administration] > [Time Setting] ページで、[Edit Settings] ボタンをクリックします。[Edit Time Setting] ページが表示されます。

図 12-38　[Edit Time Settings] ページ



ネットワーク タイム プロトコル（NTP）設定の編集（Time Keeping Method）

他のコンピュータとのシステム クロックの同期に NTP サーバを使用し、NTP サーバの設定値を編集するには、次の手順を実行します。

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。[Edit Time Setting] ページが表示されます。

ステップ 2　[Time Keeping Method] セクションで、[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、[Add Row] をクリックします。複数の NTP サーバを追加できます。

ステップ 4　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 5　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 6　変更を送信し、保存します。

NTP サーバを使用しないシステム時刻の設定

NTP サーバを使用せずに手動でシステム時刻を設定するには、次の手順を実行します。

ステップ 1　[Management Appliance] > [System Administration] > [Time Settings] ページで、[Edit Settings] をクリックします。[Edit Time Setting] ページが表示されます。

ステップ 2　[Time Keeping Method] セクションで、[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。

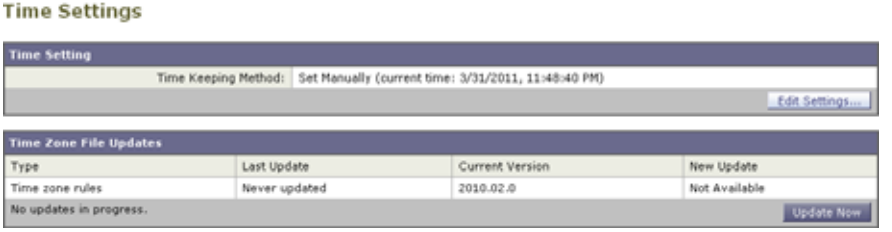
時間帯ファイルの更新

Security Management アプライアンスの各時間帯ファイルには、特定の時間帯の相対時刻を指定する規則が含まれています。AsyncOS の更新と更新の間であればいつでも、Security Management アプライアンスの時間帯ファイルを更新できます。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。

GUI で時間帯ファイルを更新するには、次の手順を実行します。

ステップ 1　[Management Appliance] > [System Administration] > [Time Settings] ページに移動します。



ステップ 2　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。

時間ベース ポリシーの時間範囲の定義

「営業時間」や「週末シフト」などの時間範囲を定義して、Web ベースのアクティビティを特定の日および時間に限定できます。たとえば、広帯域幅サイトまたは職務に関係のないサイトへの、業務時間内のアクセスをブロックできます。

詳細については、『*Cisco IronPort AsyncOS for Web Security User Guide*』の「Working with Time Based Policies」を参照してください。

時間範囲を追加または編集するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Web] > [Configuration Master] > [Defined Time Ranges] を選択します。

[Time Ranges] ページが表示されます。

ステップ 2　[Add Time Range] をクリックします。

[Add Time Range] ページが表示されます。

ステップ 3　[Time Range Name] テキスト フィールドに、時間範囲の名前を入力します。

ステップ 4　[Time Zone] 領域で、希望する時間帯に対応するオプション ボタンをクリックして選択します。選択肢は次のとおりです。

- Use Time Zone Setting from Appliance
- Specify Time Zone for this Time Range

対応するドロップダウン メニューから、地域、国、および時間帯を選択します。

ステップ 5　[Time Values] 領域で、定義した時間帯の曜日と時刻を選択します。

ステップ 6　[Add Row] をクリックします。

ステップ 7　[Submit] をクリックします。

コンフィギュレーション ファイルの管理

Cisco IronPort アプライアンス内の大部分の設定は、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。

- 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 Security Management アプライアンスから別の Security Management 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 Security Management 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 Email Security 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、Email Security アプライアンスから Security Management 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動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。

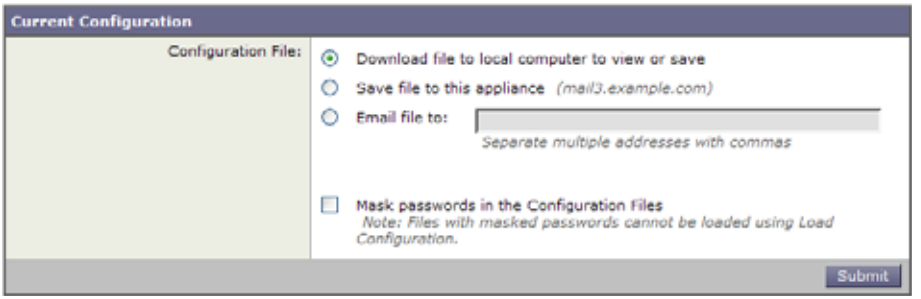
[Configuration File] ページには、次のセクションが含まれています。

- [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 12-39　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。

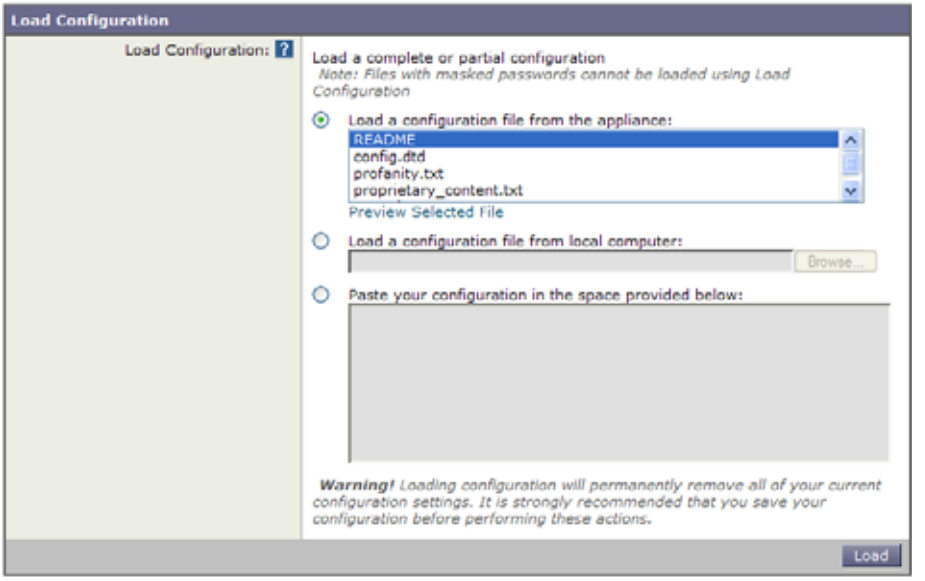
ステップ 1　`configuration` ディレクトリに情報を格納し、アップロードする

ステップ 2　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

ステップ 3　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 12-40　　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」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」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。

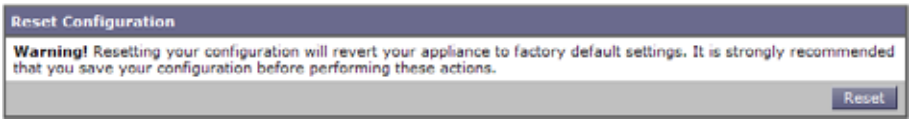
```
<?xml version="1.0" encoding="ISO-8859-1"?>
```

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 12-41　コンフィギュレーション ファイルのリセット



「出荷時デフォルト値へのリセット」（P.12-6）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（「出荷時デフォルト値へのリセット」（P.12-6）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.12-116）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.
```

Security Management 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。

ステップ 1　configuration ディレクトリに情報を格納し、アップロードする

ステップ 2　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.12-113）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.2-33）の表 2-5 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、Security Management 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

有効なデータセットを「ソース」アプライアンスから「ターゲット」Security Management アプライアンスに、元の「ソース」Security Management 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、「Security Management アプライアンスのバックアップ」（P.12-8）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「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 ウィザードについて」（P.2-10）を参照してください）。これで、変更が確定されます。

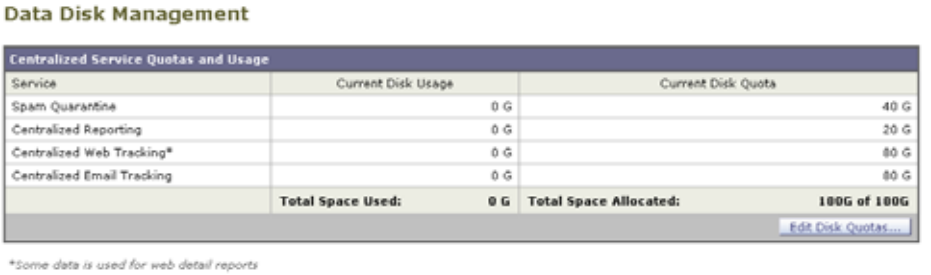
```
mail3.example.com> loadconfig


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、Security Management アプライアンスのモニタリング サービス（Cisco IronPort スパム検疫、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 12-42　[Disk Management] ページ



使用可能な最大ディスク領域

表 12-8 は、特定の Security Management 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 スパム検疫（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 12-8　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	M600	M650	M660	M670	M1000	M1050	M1060	M1070
レポーティング＋電子メール トラッキング＋ISQ＋Web トラッキング	180	186	186	450	700	405	405	800	1500
ISQ 最大値	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 ディスク上の検疫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 ドライブで ISQ 処理を行うと、マシンのロックアップが発生することがあります。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 クォータの編集

[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 スパム検疫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。

新しい割り当て量を変更し、現在の領域占有量よりも少なくなるようにした場合、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。

Web 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で [Enable] チェックボックスをオンにしたが、この操作用に割り当てられたディスク領域がない場合は、ディスク領域が割り当てられるまで Web レポーティングが機能し

ません。この設定の編集の詳細については、「Security Management 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とディセーブル化」（P.3-5）を参照してください。

モニタリング サービスのディスク クォータの再割り当て

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　Security Management 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。

そのサービスに対して、0 からディスク領域の合計量までの値を入力できます。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 スパム検疫に 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確定します。

CHAPTER 13

ロギング

Security Management 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、さまざまな情報が記録された、さまざまなタイプのログを生成します。Security Management アプライアンスは、システム情報の重要なリソースとして、コマンド ライン インタフェース（CLI）とは別に、これらのログを提供します。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するときに重要です。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。

この章は、次の項で構成されています。

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 スパム検疫ログは、検疫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、Email Security 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、Security Management アプライアンス以外には送信できません。

（注）　Security Management アプライアンスは、Cisco IronPort スパム検疫（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によって、ログ タイプと名前、ロギング レベル、およびその他の特性（ファイル サイズ、宛先情報など）が関連付けられます。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、そのログに記録されるデータが決定されます。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.13-37）を参照してください。

AsyncOS は、次のログ タイプを生成します。

表 13-1　　ログ タイプ

ログ タイプ	説明
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には、Security Management アプライアンスに加えられた変更、およびその変更を行ったユーザが記録されます。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。
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。
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。
Cisco IronPort スパム検疫ログ	Cisco IronPort スパム検疫ログには、Cisco IronPort スパム検疫プロセスに関連付けられたアクションが記録されます。
Cisco IronPort スパム検疫 GUI ログ	Cisco IronPort スパム検疫 GUI ログには、Cisco IronPort スパム検疫のグラフィカル ユーザ インターフェイスに関連付けられたアクションが記録されます。このアクションには、たとえば、グラフィカル ユーザ インターフェイスからの検疫の設定、エンドユーザ認証、エンドユーザのアクション（電子メールの解放など）が含まれます。
Cisco IronPort 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、「Security Management 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とディセーブル化」（P.3-6）および「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。
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 サーバを設定する方法については、「システム時刻の設定」（P.12-105）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。

表 13-1　ログ タイプ（続き）

ログ タイプ	説明
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。
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。
SMA ログ	SMA ログには、一般的な Security Management 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 スパム検疫サービスのプロセスは含まれません。
ステータス ログ	ステータス ログには、`status detail` や `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、およびユーザが `commit` コマンドを使用して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。

ログ タイプの比較

表 13-2 に、各ログ タイプの特徴をまとめます。

表 13-2　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
コンフィギュレーション履歴ログ	•		•								•
CLI 監査ログ	•		•			•					
FTP サーバ ログ	•		•			•					
HTTP ログ	•		•			•					
Cisco IronPort スパム検疫	•		•			•					
Cisco IronPort スパム検疫 GUI	•		•			•					
Cisco IronPort テキスト メール 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	•		•			•					
セーフリスト/ブロックリスト ログ	•		•			•					
SMA ログ	•		•			•					
ステータス ログ		•	•			•					
システム ログ	•		•			•					
トラッキング ログ	•			•	•		•	•	•	•	

ログの取得

ログ ファイルは、表 13-3 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 13-3　ログ転送プロトコル

FTP Poll	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 ポーリング方式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、保有するログ 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 Push	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 Push	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がドロップダウン 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されている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時点のタイムスタンプ、および単一文字のステータス コードで構成されます。次の例で、ディレクトリとファイル名の規則を示します。

```
/<Log_Name>/<Log_Filename>.@<timestamp>.<statuscode>
```

ステータス コードは、.c（「current（現在）」の意味）、または .s（「saved（保存済み）」の意味）です。転送できるのは、保存済みステータスのログ ファイルだけです。

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は、ログを作成し、最大ファイル サイズおよび最大時間の設定制限に基づいてログ ファイルをロールオーバー（転送）します。いずれかの制限に達すると、ログ ファイルは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。

デフォルトでイネーブルになるログ

Security Management 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なった状態で事前設定されています。

表 13-4　事前設定されているログ 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 Poll
euq_logs	Cisco IronPort スパム検疫ログ	FTP Poll
euqgui_logs	Cisco IronPort スパム検疫 GUI ログ	FTP Poll
gui_logs	HTTP ログ	FTP Poll
mail_logs	Cisco IronPort テキスト メール ログ	FTP Poll
reportd_logs	レポーティング ログ	FTP Poll
reportqueryd_logs	レポーティング クエリー ログ	FTP Poll
slbld_logs	セーフリスト/ブロックリスト ログ	FTP Poll
smad_logs	SMA ログ	FTP Poll

表 13-4　事前設定されているログ サブスクリプション（続き）

ログ名	ログ タイプ	取得方法
system_logs	システム ログ	FTP Poll
trackerd_logs	トラッキング ログ	FTP Poll

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.13-38）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.13-37）を参照してください。

ログの特徴

ここでは、次のログ タイプについて説明します。

ログ ファイル内のタイムスタンプ

次のログ ファイルには、ログ自体の開始日と終了日、AsyncOS のバージョン、および GMT オフセット（ログの開始時からの秒数）が含まれています。

- メール ログ
- セーフリスト/ブロックリスト ログ
- システム ログ

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 ファイルと、ユーザ名、ユーザが行った設定変更の説明、ユーザが変更をコミットしたときに入力したコメントをリストする追加のセクションで構成されています。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 13-5 に、CLI 監査ログに記録される統計情報を示します。

表 13-5　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========  ==========  =========  ===========  ====¥nadmin     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 13-6 に、FTP サーバ ログに記録される統計情報を示します。

表 13-6　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 13-7 に、HTTP ログに記録される統計情報を示します。

表 13-7　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。
ユーザ	接続元ユーザのユーザ名。
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、管理者ユーザとグラフィカル ユーザ インターフェイスとの対話（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=recipie
ntsin&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 スパム検疫ログの使用

表 13-8 に、Cisco IronPort スパム検疫ログに記録される統計情報を示します。

表 13-8　Cisco IronPort スパム検疫ログの統計情報

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（メッセージの検疫、検疫エリアからの解放など）で構成されます。

Cisco IronPort スパム検疫ログの例

次のログの例は、検疫から 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 スパム検疫 GUI ログの使用

表 13-9 に、Cisco IronPort スパム検疫 GUI ログに記録される統計情報を示します。

表 13-9　Cisco IronPort スパム検疫 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 スパム検疫 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 13-10　Cisco IronPort スパム検疫 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。「Security Management 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とディセーブル化」（P.3-6）および「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 13-11 に、テキスト メール ログに表示される情報を示します。

表 13-11　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 スパム検疫に対する個々の RPC 接続を表す数値 ID です。この ID を使用して、Cisco IronPort スパム検疫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 13-12　テキスト メール ログの詳細

```
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
1 verified yes
2 Mon Apr 17 19:57:20 2003 Info: Start MID 6 ICID 5
Mon Apr 17 19:57:20 2003 Info: MID 6 ICID 5 From:
3 <sender@remotehost.com>
Mon Apr 17 19:58:06 2003 Info: MID 6 ICID 5 RID 0 To:
4 <mary@yourdomain.com>
Mon Apr 17 19:59:52 2003 Info: MID 6 ready 100 bytes from
5 <sender@remotehost.com>
6 Mon Apr 17 19:59:59 2003 Info: ICID 5 close
Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 8 interface
7 192.168.42.42 address 10.5.3.25
Mon Mar 31 20:10:58 2003 Info: Delivery start DCID 8 MID 6 to RID
8 [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 13-13 を使用してください。

表 13-13　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。

表 13-13　テキスト メール ログの例の詳細（続き）

行番号	説明
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 *5XX* エラーを返しました。これは、メッセージをどちらの受信者にも配信できなかったことを示します。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 番目が Unicode であることに注意してください。Unicode を表示できない端末では、このような添付ファイルは quoted-printable 形式で表示されます。

生成またはリライトされたメッセージ

リライト/リダイレクト アクションなどの一部の機能（`alt-rcpt-to` フィルタ、アンチスパム RCPT リライト、`bcc()` アクション、アンチウイルス リダイレクションなど）によって、新しいメッセージが作成されます。ログに目を通して結果を確認し、必要に応じて MID や、場合によっては DCID を追加します。次のようなエントリが可能です。

```
Tue Jun  1 20:02:16 2004 Info: MID 14 generated based on MID 13 by bcc
filter 'nonetest'
```

または

```
Tue Jan  6 15:03:18 2004 Info: MID 2 rewritten to 3 by antispam

Fri May 14 20:44:43 2004 Info: MID 6 rewritten to 7 by alt-rcpt-to-filter
filter 'testfilt'
```

（注） 「Rewritten」エントリは、新しい MID の使用を示すログの行の後に表示されます。

Cisco IronPort スパム検疫へのメッセージの送信

メッセージを検疫エリアに送信すると、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、検疫エリア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 スパム検疫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 13-14 に、NTP ログに記録される統計情報を示します。

表 13-14　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 13-15 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 13-15　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 13-16 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 13-16　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 13-17 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 13-17　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 13-18 に、SMA ログに記録される統計情報を示します。

表 13-18　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、Email Security 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、Email Security 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 13-19 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 13-19　ステータス ログの統計情報

統計	説明
CPULd	CPU 使用率。
DskIO	Disk I/O 使用率。
RAMUtil	RAM 使用率。
QKUsd	使用されているキュー（キロバイト単位）。
QKFre	空いているキュー（キロバイト単位）。
CrtMID	メッセージ ID（MID）。
CrtICID	インジェクション接続 ID（ICID）。
CRTDCID	配信接続 ID（DCID）。
InjMsg	インジェクトされたメッセージ。
InjRcp	インジェクトされた受信者。
GenBncRcp	生成されたバウンス受信者。
RejRcp	拒否された受信者。
DrpMsg	ドロップされたメッセージ。
SftBncEvnt	ソフト バウンスされたイベント。
CmpRcp	完了した受信者。
HrdBncRcp	ハード バウンスされた受信者。
DnsHrdBnc	DNS ハード バウンス。
5XXHrdBnc	5XX ハード バウンス。
FltrHrdBnc	フィルタ ハード バウンス。
ExpHrdBnc	期限切れハード バウンス。
OtrHrdBnc	その他のハード バウンス。
DlvRcp	配信された受信者。
DelRcp	削除された受信者。
GlbUnsbHt	グローバル配信停止リストとの一致数。
ActvRcp	アクティブ受信者。

表 13-19　ステータス ログの統計情報（続き）

統計	説明
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	システム検疫にある個々のメッセージ数（複数の検疫エリアに存在するメッセージは一度だけカウントされます）。
QuarQKUsd	システム検疫メッセージによって使用されたキロバイト数。

表 13-19　ステータス ログの統計情報（続き）

統計	説明
LogUsd	使用されたログ パーティションの割合。
CASELd	CASE スキャンで使用された CPU の割合。
TotalLd	CPU の合計消費量。
LogAvail	ログ ファイルに使用できるディスク領域。
EuQ	Cisco IronPort スパム検疫内のメッセージ数。
EuqRls	Cisco IronPort スパム検疫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 13-20 に、システム ログに記録される統計情報を示します。

表 13-20　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

ここでは、次の項目について説明します。

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 13-21　　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.13-2）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 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。

表 13-21　ログ ファイルの属性（続き）

属性	説明
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。
Maximum 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。

[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.13-2）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 13-22　　ログ レベル

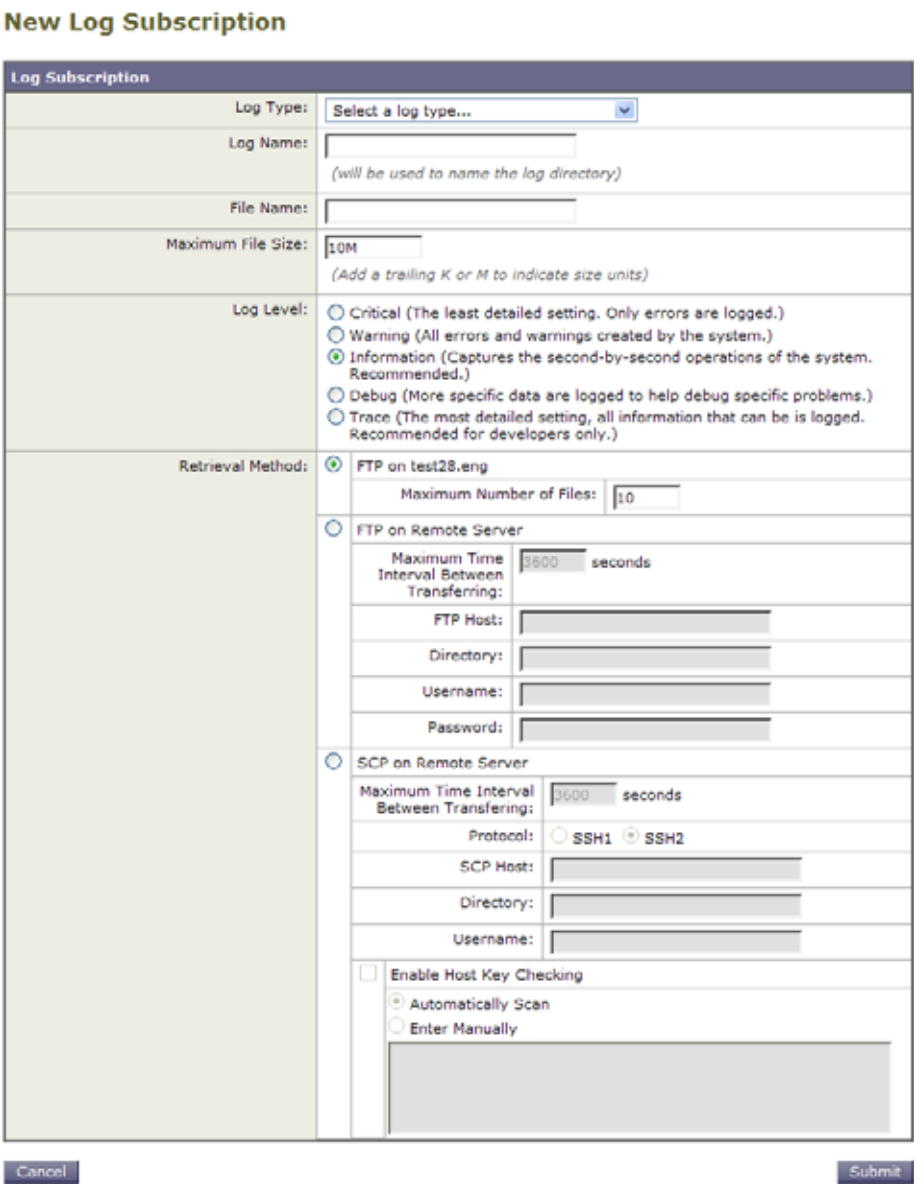
ログ レベル	説明
Critical	エラーだけがログに記録されます。最も省略されたログ レベル設定です。このログ レベルでは、パフォーマンスおよび重要なアプライアンスのアクティビティをモニタすることはできません。ただし、詳細ログ レベルのように、ログ ファイルがすぐに最大サイズに達することはありません。このログ レベルは、syslog レベル Alert と同等です。
Warning	すべてのシステム エラーと警告が記録されます。このログ レベルでは、パフォーマンスおよび重要なアプライアンスのアクティビティをモニタすることはできません。Critical ログ レベルよりは早く、ログ ファイル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

ログ サブスクリプションを作成するには、次の手順を実行します。

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。[New Log Subscription] ページが表示されます。

図 13-1　ログ サブスクリプションの新規作成



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、最大ファイル サイズとログ レベルを指定します。

ステップ 4　（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 5　ログの取得方法を設定します。

ステップ 6　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

ログ サブスクリプションを編集するには、次の手順を実行します。

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。[Edit Log Subscription] ページが表示されます。

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。例：

```
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。例：

```
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 13-23　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。

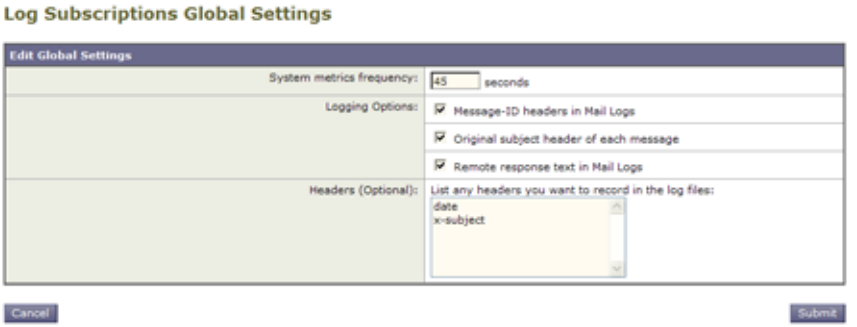
```
Tue May 31 10:14:12 2005 Info: Message done DCID 0 MID 3 to RID [0]
[('date', 'Tue, 31 May 2005 10:13:18 -0700'), ('x-subject', 'Logging this
header')]
```

GUI を使用したロギングのグローバル設定

ロギングのグローバル設定を行うには、次の手順を実行します。

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。[Log Subscriptions Global Settings] ページが表示されます。

図 13-2　ログ サブスクリプションのグローバル設定



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。

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。

ステップ 4　変更を送信し、保存します。

ログ サブスクリプションのロール オーバー

AsyncOS は、[Log Subscriptions Global Settings] ページ（または CLI の `logconfig` コマンド）での設定に基づいてログ ファイルをロールオーバーします。また、[Log Subscriptions] ページの [Rollover Now] ボタンをクリックするか、`rollovernow` コマンドを使用することによって、必要に応じてログ ファイルをロールオーバーできます。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）。

GUI を使用したログ サブスクリプションのロールオーバー

ログ サブスクリプションをロールオーバーするには、次の手順を実行します。

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。

ロールオーバー対象として 1 つまたは複数のログを選択すると、[Rollover Now] ボタンがイネーブルになります。

ステップ 3　[Rollover Now] ボタンをクリックして、選択したログをロール オーバーします。

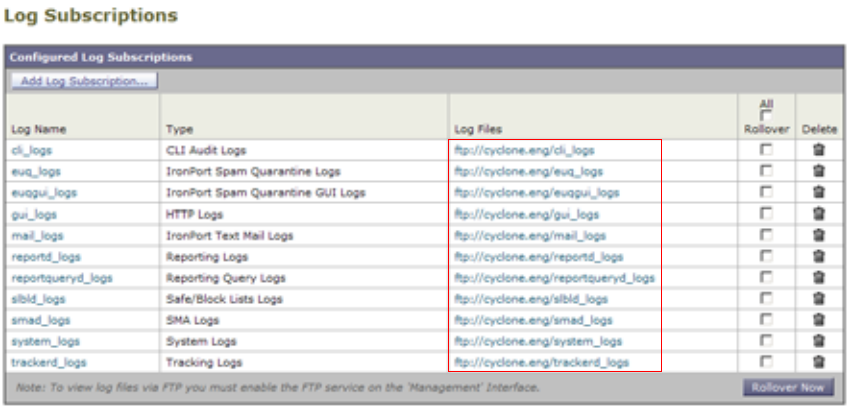
CLI を使用したログ サブスクリプションのロール オーバー

`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 13-3　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 User 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 13-24　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
```

APPENDIX A

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

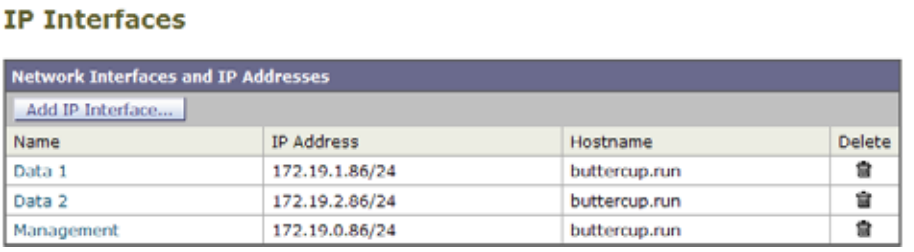
		デフォルトでイネーブルかどうか	
サービス	**デフォルト ポート**	**管理インターフェイス**	**新規作成された IP インターフェイス**
FTP	21	No	No
Telnet	23	Yes	No
SSH	22	Yes	No
HTTP	80	Yes	No
HTTPS	443	Yes	No

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 スパム検疫へのアクセスも設定できます。電子メール配信および仮想ゲートウェイでは、各 IP インターフェイスが特定の IP アドレスおよびホスト名を持つ 1 つの仮想ゲートウェイ アドレスとして動作します。インターフェ

イスを個別のグループに（CLI を使用して）「参加」させることもできます。システムは、電子メールの配信時にこれらのグループを順に使用します。仮想ゲートウェイへの参加またはグループ化は、複数のインターフェイス間で大規模な電子メール キャンペーンを負荷分散するために役立ちます。VLAN を作成し、他のインターフェイスの設定と同様に（CLI を使用して）VLAN を設定することもできます。詳細については、『*Cisco IronPort AsyncOS for Email Advanced User 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 ポートは変更できません。さらに、セキュリティ管理アプライアンスは、以降に説明する機能（仮想ゲートウェイなど）をすべてサポートするわけではありません。

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 インターフェイスのコンポーネント

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。

表 A-2　IP インターフェイスのコンポーネント（続き）

ネットマスク（またはサブネットマスク）	ネットマスクを標準のドット付きオクテット形式（255.255.255.0 など）または 16 進形式（0xffffff00 など）で入力できます。デフォルトのネットマスクは、一般的なクラス C の値である、255.255.255.0 です。
ブロードキャスト アドレス	AsyncOS は IP アドレスおよびネットマスクから、デフォルトのブロードキャスト アドレスを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。SMTP カンバセーション時に、このホスト名を使用してサーバを識別します。各 IP アドレスに関連付けられた有効なホスト名を、自分で入力する必要があります。ソフトウェアは、DNS でホスト名が一致する IP アドレスに正しく解決されるか、または逆引き DNS で指定されたホスト名に解決されるかどうか確認しません。
使用可能なサービス	FTP、SSH、Telnet、Cisco IronPort スパム検疫、HTTP、HTTPS、および HTTPS は、インターフェイスでイネーブルまたはディセーブルに設定できます。サービスごとにポートを設定できます。また、Cisco IronPort スパム検疫用に HTTP/HTTPS、ポート、および URL も指定できます。

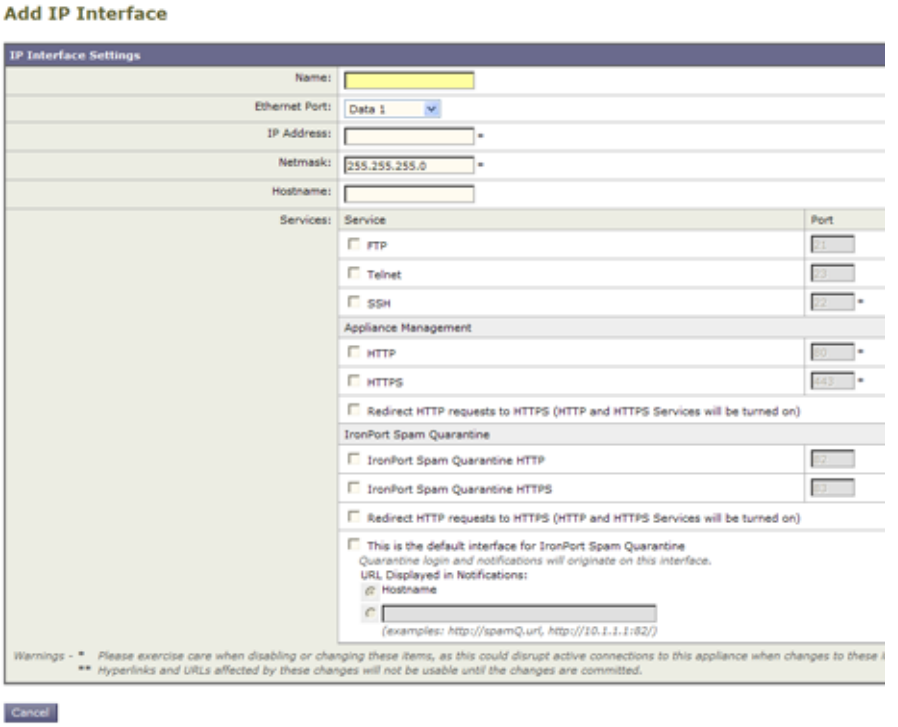
（注） 第 2 章「セットアップおよび設置」で説明されている System Setup Wizard を完了し、変更を確定している場合は、すでにアプライアンスにインターフェイスが 1 つまたは 2 つ設定されているはずです。（「論理 IP インターフェイスの割り当てと設定」セクションで入力した設定を参照してください）。また、管理インターフェイスも Cisco IronPort アプライアンスで設定されています。

GUI を使用した IP インターフェイスの作成

IP インターフェイスを作成するには、次の手順を実行します。

1. [Management Appliance] > [Network] > [IP Interfaces] ページで、[Add IP Interface] をクリックします。[Add IP Interface] ページが表示されます。

図 A-2　[Add IP Interface] ページ



2. インターフェイスの名前を入力します。
3. イーサネット ポートを選択し、IP アドレスを入力します。
4. IP アドレスに対応するネットマスクを入力します。
5. インターフェイスのホスト名を入力します。
6. この IP インターフェイス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。
7. 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。
8. Cisco IronPort スパム検疫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 スパム検疫のデフォルト インターフェイスであるかを指定し、ホスト名を URL として使用するかを指定するか、またはカスタム URL を指定することができます。

9. 変更を送信し、保存します。

FTP アクセス

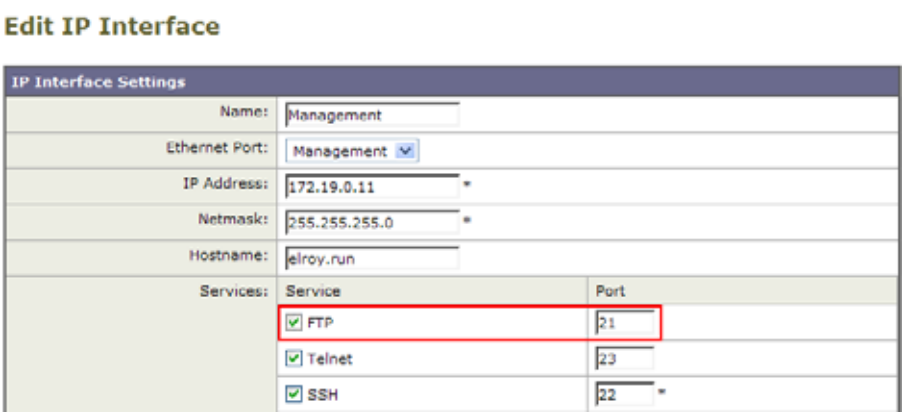
FTP 経由でアプライアンスにアクセスするには、次の手順を実行します。

警告　**アプライアンスへの接続方法によっては、[Management Appliance] > [Network] > [IP Interfaces] ページまたは `interfaceconfig` コマンドを使用してサービスをディセーブルにすることで、GUI または CLI から自分自身を切断できます。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。**

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がポート 21（デフォルト ポート）で 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-3　[Edit IP Interface] ページ



（注）　次の手順に進む前に、必ず変更を確定してください。

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
   ```
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後は、次のディレクトリを参照し、ファイルをコピーおよび追加（「GET」および「PUT」）できます。表 A-3 を参照してください。

表 A-3　アクセスできるディレクトリ

ディレクトリ名	説明
/avarchive **/bounces** **/cli_logs** **/delivery** **/error_logs** **/ftpd_logs** **/gui_logs** **/mail_logs** **/rptd_logs** **/sntpd.logs** **/status** **/system_logs**	[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 Advanced User 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。

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
/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。 レコード管理のためにこれらのファイルを別のマシンにコピーしたり、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た、すべてのアーカイブ済みレポートが保存されるディレクトリ。

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-6）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 がクライアント マシンから、ホスト名が mail3.example.com のアプライアンスのコンフィギュレーション ディレクトリにコピーされます。

（注）　このコマンドでは、ユーザ（admin）のパスワードを求めるプロンプトが表示されます。この例は参考用としてだけ示します。実際のオペレーティング 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、「以前のバージョンの AsyncOS への復元」（P.12-26）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-4 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の定義を示します。

図 A-4　シリアル ポートのピン番号

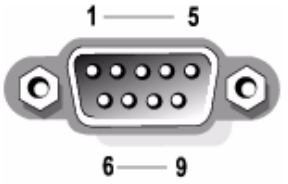


表 A-4　シリアル ポートのピン割り当て

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。

この付録では、次の内容について説明します。

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は、発信パケットを送信するインターフェイスを、Cisco IronPort アプライアンスが一意に選択できるようにする必要があります。この要件によって、イーサネット インターフェイスの IP アドレスとネットマスクの選択に関して、いくつかのことが決まります。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、Virtual Gateway テクノロジーの実装で使用されます。

ネットマスクの目的は、IP アドレスをネットワーク アドレスとホスト アドレスに分割することです。ネットワーク アドレスは、IP アドレスのネットワーク部分（ネットマスクと一致するビット）と見なすことができます。ホスト アドレスは、IP アドレスの残りのビットです。有効な 4 オクテット アドレスのビット数は、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。この形式では、スラッシュの後ろにビット数（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。

インターフェイスの設定例

ここでは、いくつかの代表的なネットワークに基づいたインターフェイスの設定例を示します。この例では、Int1 と Int2 の 2 つのインターフェイスを使用します。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：

各インターフェイスが、別のネットワークになっている必要があります。

インターフェイス	IP アドレス	ネットマスク	ネット アドレス
Int1	192.168.1.10	255.255.255.0	192.168.1.0/24
Int2	192.168.0.10	255.255.255.0	192.168.0.0/24

192.168.1.X にアドレス指定されたデータ（ここで X は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 から送出されます。192.168.0.X にアドレス指定されたデータは、Int2 から送出されます。これらの形式でないその他のアドレス（一般的には、外部の WAN またはインターネット）に向かうパケットは、デフォルト ゲートウェイに送信されます。デフォルト ゲートウェイは、これらのネットワークのいずれかに存在する必要があります。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、パケットの配信に使用するイーサネット インターフェイスを決定することができません。2 つのイーサネット インターフェイスが 2 つの物理ネットワークに別々に接続されている場合、パケットは誤ったネットワークに配信される可能性があり、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。

要約

Cisco IronPort アプライアンスは、パケットを配信でき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	不許可	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。ボトルネックが最も頻繁に発生するのは、インターネットへの接続、および接続プロバイダーが存在するアップストリームです。

接続に使用する Cisco IronPort アプライアンスのインターフェイス数と、インターフェイスのアドレスを指定する方法は、基になるネットワークの複雑さによって左右されます。ネットワーク トポロジまたはデータ量から必要になる場合を除いて、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 ファイル集約用 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。
22	TCP	In	AsyncOS IP	CLI への SSH アクセス、ログ ファイルの集約。 バックアップ用としても使用
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、またはインジェクトの場合はファイアウォール外部からの電子メールを受信する SMTP。

表 C-1　ファイアウォール ポート（続き）

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	AsyncOS アップグレードを除くサービス アップグレード。
80	HTTP	Out	updates.cisco.com	AsyncOS のアップグレード。
82	HTTP	In	AsyncOS IP	Cisco IronPort スパム検疫の表示に使用。
83	HTTPS	In	AsyncOS IP	Cisco IronPort スパム検疫の表示に使用。
53	UDP/TCP	Out	DNS サーバ	インターネット ルート サーバを使用するよう設定されている場合の DNS、またはファイアウォール外の他の DNS サーバ。SenderBase クエリーにも使用。
110	TCP	Out	POP サーバ	Cisco IronPort スパム検疫のためのエンドユーザの POP 認証。
123	UDP	Out	NTP サーバ	タイム サーバがファイアウォール外部の場合の NTP。
143	TCP	Out	IMAP サーバ	Cisco IronPort スパム検疫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 スパム検疫のための 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	更新サーバの最新ファイルの検証。

表 C-1　ファイアウォール ポート（続き）

443	TCP	Out	phonehome.senderbase.org	ウイルス感染フィルタの受信/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 スパム検疫がイネーブルの場合、Cisco IronPort スパム検疫データを Security Management アプライアンスに送信。

APPENDIX D

例

この付録では、Security Management 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、Security Management アプライアンスと Web セキュリティ アプライアンスの使用方法について説明します。

（注） 以下のすべてのシナリオでは、Security Management アプライアンス *および*ご使用の Web セキュリティ アプライアンスとで Web レポーティングと Web トラッキングをイネーブルにしていることを前提としています。Web レポーティ

ングと Web トラッキングをイネーブルにする方法については、Security Management 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とディセーブル化を参照してください。

例 1：ユーザの調査

この例では、システム管理者が会社内の特定のユーザを調査する方法について説明します。

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。

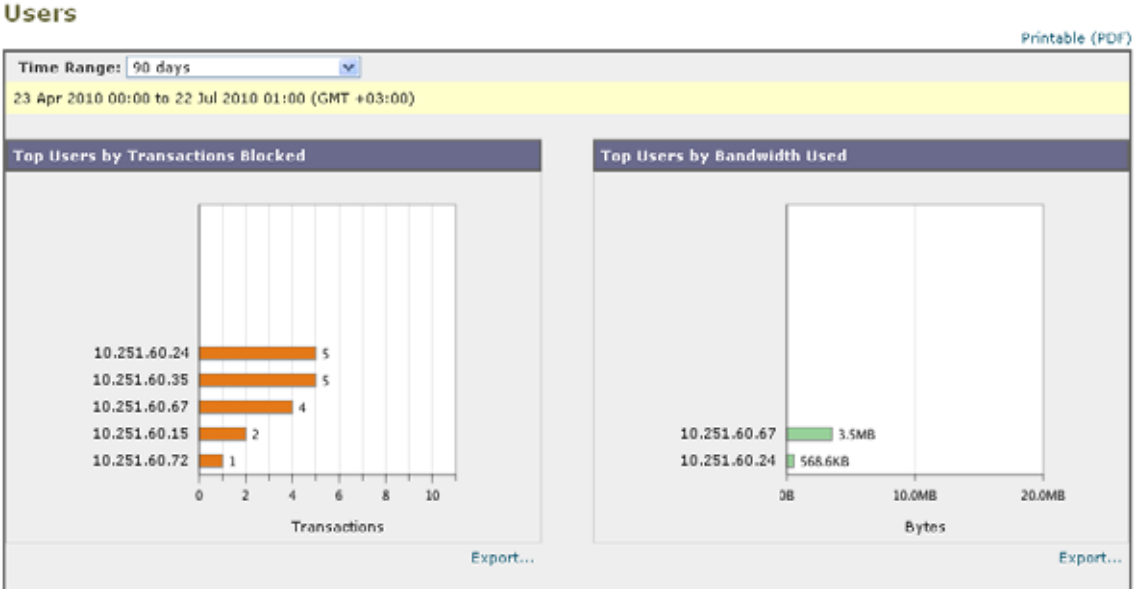
Web アクティビティがトラッキングされると、従業員の参照履歴に関する情報が記載された Web レポートが作成されます。

ステップ 1　Security Management アプライアンスで、[Web] > [Reporting] > [Users] を選択します。

[Users] ページが表示されます。

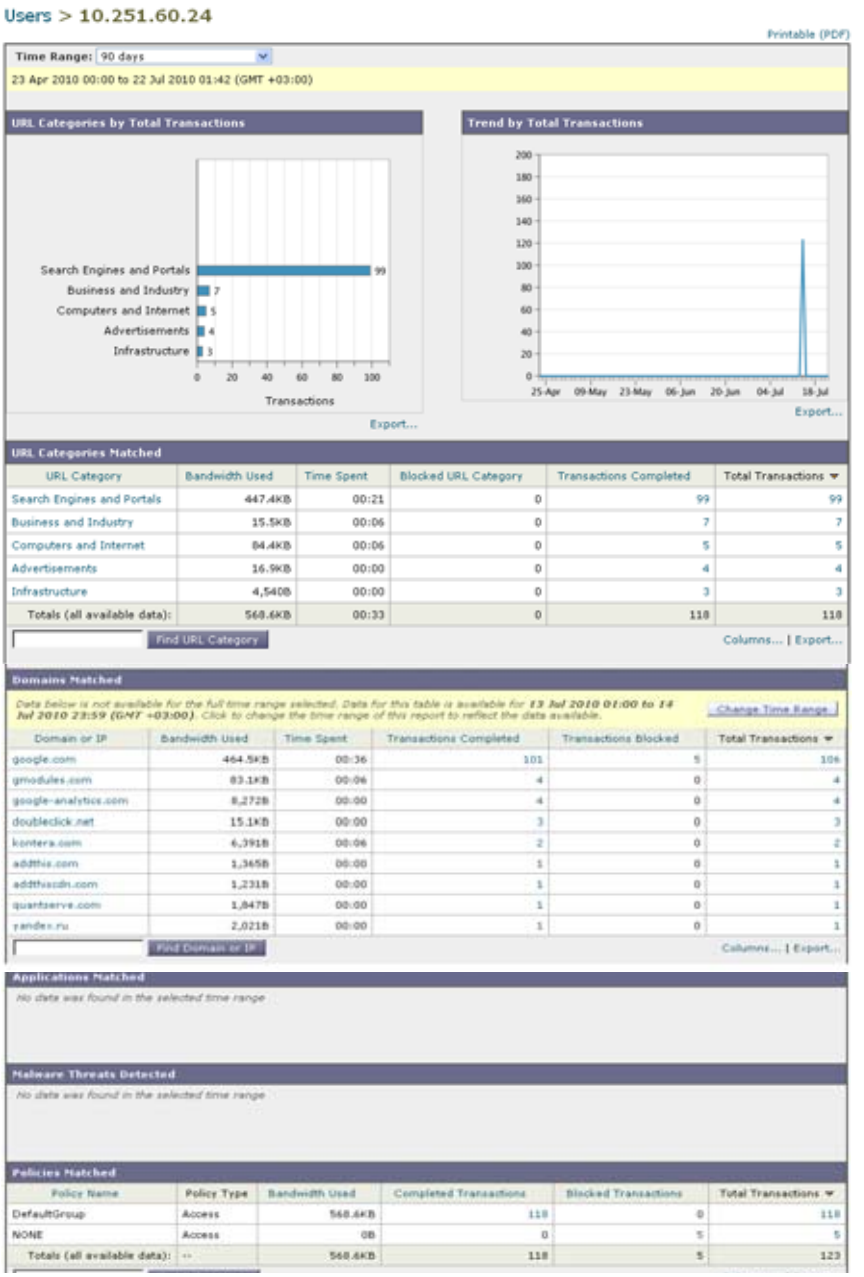
ステップ 2　[Users] テーブルで、調査する [User ID] または [Client IP address] をクリックします。

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] テーブルには、入力されたユーザ ID とクライアント IP アドレスが読み込まれます。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
23 Apr 2010 00:00 to 22 Jul 2010 01:42 (GMT +03:00)
URL Categories by Total Transactions
Search Engines and Portals 99
Business and Industry 7
Computers and Internet 5
Advertisements 4
Infrastructure 3
0 20 40 60 80 100
Transactions
Export...
Trend by Total Transactions
200 180 160 140 120 100 80 60 40 20 0
25-Apr 09-May 23-May 06-Jun 20-Jun 04-Jul 18-Jul
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
Data below is not available for the full time range selected. Data for this table is available for 13 Jul 2010 01:00 to 14 Jul 2010 23:59 (GMT +03:00). Click to change the time range of this report to reflect the data available.
Change Time Range
Domain or IP | Bandwidth Used | Time Spent | Transactions Completed | Transactions Blocked | Total Transactions
google.com | 464.5KB | 00:36 | 101 | 5 | 106
gmodules.com | 83.1KB | 00:06 | 4 | 0 | 4
google-analytics.com | 8,272B | 00:00 | 4 | 0 | 4
doubleclick.net | 15.1KB | 00:00 | 3 | 0 | 3
kontera.com | 6,391B | 00:06 | 2 | 0 | 2
addthis.com | 1,365B | 00:00 | 1 | 0 | 1
addthiscdn.com | 1,231B | 00:00 | 1 | 0 | 1
quantserve.com | 1,847B | 00:00 | 1 | 0 | 1
yandex.ru | 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
DefaultGroup | Access | 568.6KB | 118 | 0 | 118
NONE | Access | 0B | 0 | 5 | 5
Totals (all available data): | -- | 568.6KB | 118 | 5 | 123

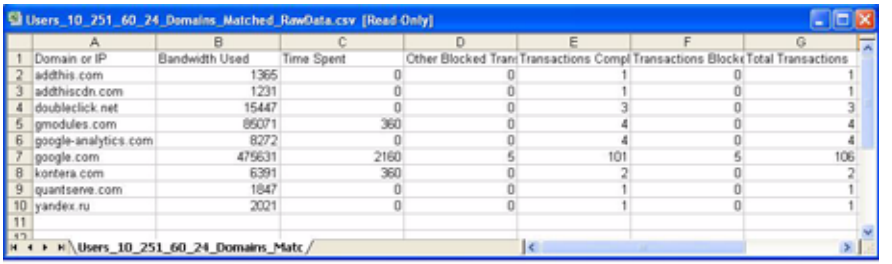
ユーザの詳細ページから総トランザクション別の URL カテゴリ、総トランザクション別のトレンド、一致する URL カテゴリ、一致するドメイン、一致するアプリケーション、検出されたマルウェアの脅威、および一致するポリシーを確認できます。

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] テーブルで [Export] をクリックすると、ユーザがアクセスしようとしたドメインと URL の完全なリストが表示されます。

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	475631	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。

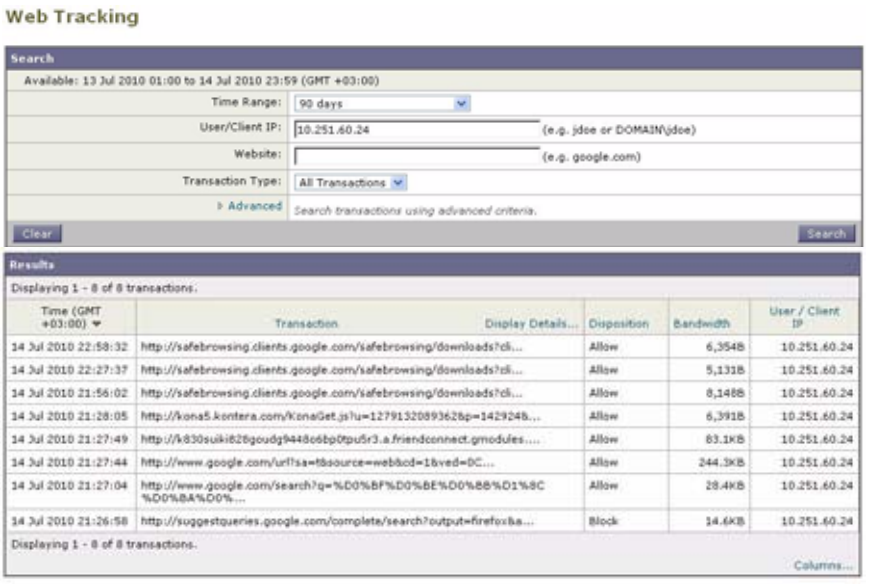
（注）　Web レポーティングでは、アクセスされる特定の URL に限らず、ユーザがアクセスするすべてのドメイン情報を取得できる点に注意してください。ユーザがアクセスしている特定の URL、その URL にアクセスした時刻、その URL が許可されているかどうかなどの情報を得るには、[Web Tracking] ページを使用します。

ステップ 5　[Web] > [Reporting] > [Web Tracking] を選択します。

ステップ 6　[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、10.251.60.24 のユーザの Web トラッキング情報を検索しています。

[Web Tracking] ページが表示されます。



このページから、10.251.60.24 のユーザがアクセスしたトランザクションの詳細なリストと URL 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

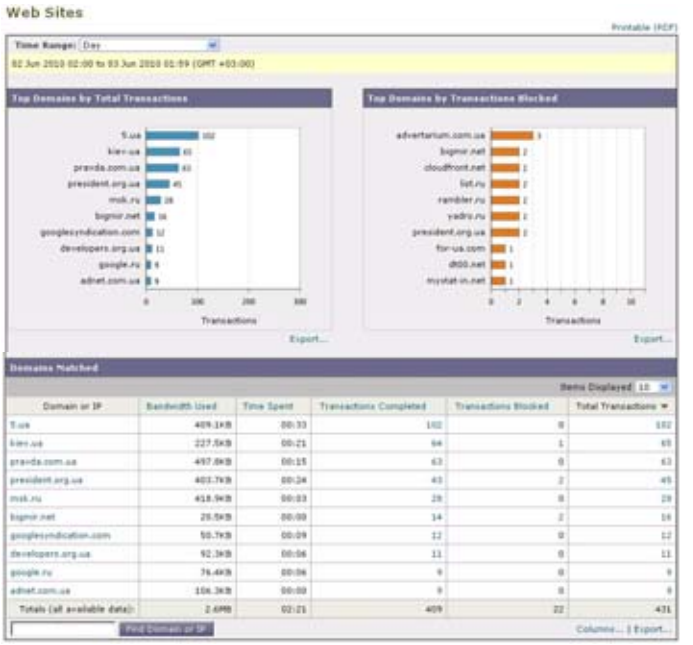
機能名	機能情報
[User] ページ	「[Users] ページ」（P.5-16）
[User Details] ページ	「[User Details] ページ」（P.5-20）
レポート データのエクスポート	「レポート データの印刷とエクスポート」（P.3-21）
Web トラッキング	「[Web Tracking] ページ」（P.5-70）

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　Security Management 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）

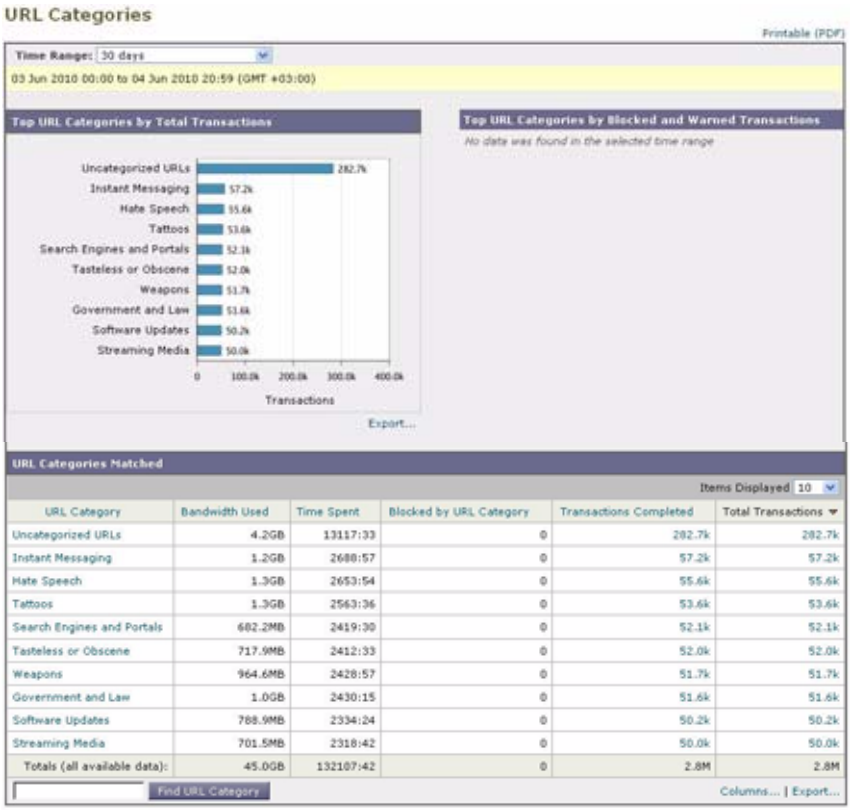
例 3：アクセスの多い URL カテゴリの調査

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　Security Management アプライアンスで、[Web] > [Reporting] > [URL Categories] を選択します。

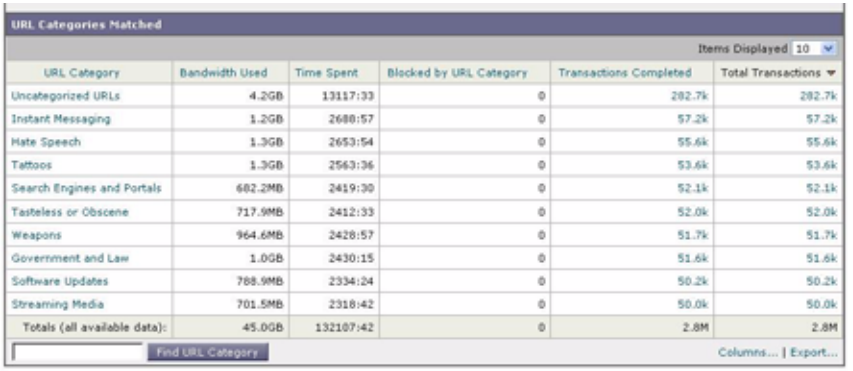
[URL Categories] ページが表示されます。



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未加工のデータを 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。



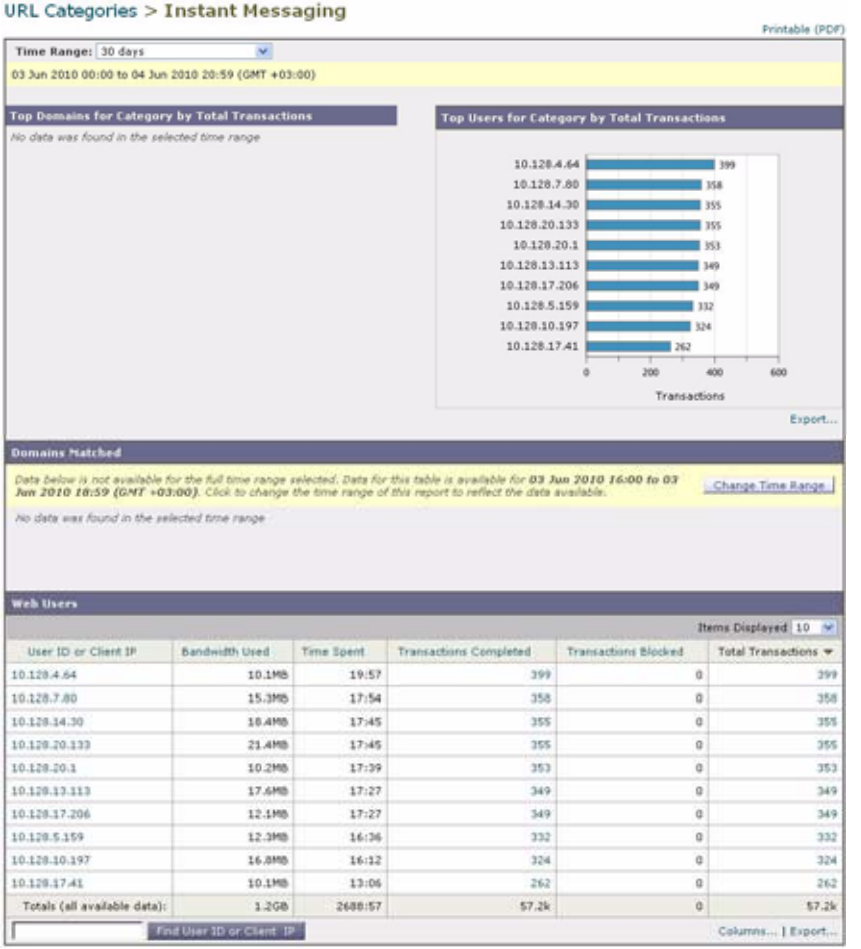
URL Categories Matched

Items Displayed 10

URL Category	Bandwidth Used	Time Spent	Blocked by URL Category	Transactions Completed	Total Transactions
Uncategorized URLs	4.2GB	13117:33	0	282.7k	282.7k
Instant Messaging	1.2GB	2680:57	0	57.2k	57.2k
Hate Speech	1.3GB	2653:54	0	55.6k	55.6k
Tattoos	1.3GB	2563:36	0	53.6k	53.6k
Search Engines and Portals	682.2MB	2419:30	0	52.1k	52.1k
Tasteless or Obscene	717.9MB	2412:33	0	52.0k	52.0k
Weapons	964.6MB	2428:57	0	51.7k	51.7k
Government and Law	1.0GB	2430:15	0	51.6k	51.6k
Software Updates	788.9MB	2334:24	0	50.2k	50.2k
Streaming Media	701.5MB	2318:42	0	50.0k	50.0k
Totals (all available data):	45.0GB	132107:42	0	2.8M	2.8M

Find URL Category　Columns... | Export...

[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.5-28）
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.3-21）

例 4：プライバシーおよびユーザ名の非表示

この例では、マネージャが一連のレポートを作成するが、従業員の個人情報は一切表示しない場合を考えます。

Security Management アプライアンスでは、[Reports] チェックボックスの [Anonymize User Names] をクリックすると、この操作をイネーブルまたはディセーブルにできます。この操作をイネーブルにすると、レポートを受け取った人にユーザ名を明らかにすることなく、レポートを生成して配布することができます。

次の例は、ユーザ名や IP アドレスなどの個人情報がレポートにどのように表示されるのか、およびユーザ名を匿名にするとどのようなレポートになるのかを示しています。

ユーザ名の匿名化のイネーブル化前

ステップ 1　Security Management アプライアンスで、[Management Appliance] > [Centralized Services] > [Web] > [Centralized Reporting] を選択します。

[Centralized Web Reporting] ページが表示されます。

（注）　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。「中央集中型 Web レポーティングの設定」（P.5-3）を参照してください。

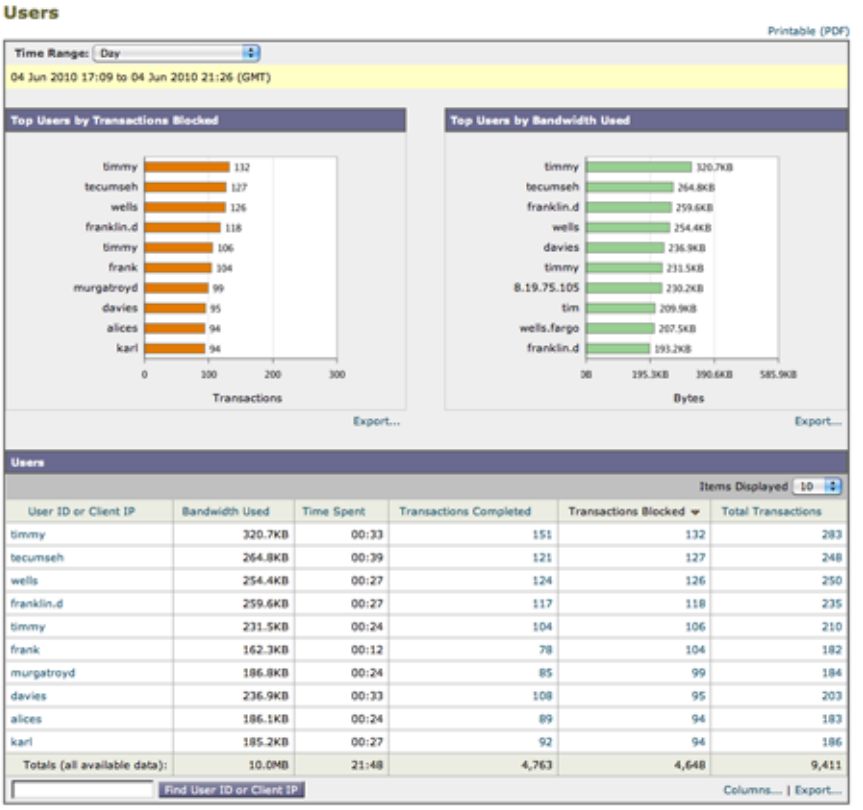
ステップ 2　[Edit Settings] をクリックします。

ステップ 3　[Anonymize User Names in Report] チェックボックスがオフになっていることを確認してください。

ステップ 4　[Submit] をクリックします。

ステップ 5　[Web] > [Users] を選択します。

ステップ 6　[Web Users] ページが表示されます。



この場合は、すべてのユーザ名が [Web] > [Users] ページに表示されます。

ユーザ名を確認したい場合は、この情報が表示されていても問題ありません。それに対して、この情報を他のグループに公開しない場合は、ユーザ名を非表示にする必要があります。

（注）　管理者ステータスを持っている場合は、常にユーザ名が表示されます。

ユーザ名の匿名化のイネーブル化後

レポート機能でユーザ名の匿名化を使用すると、同じレポートが次のようになります。

ステップ 1　Security Management アプライアンスで、[Management Appliance] > [Centralized Services] > [Web] > [Centralized Reporting] を選択します。

[Centralized Web Reporting] ページが表示されます。

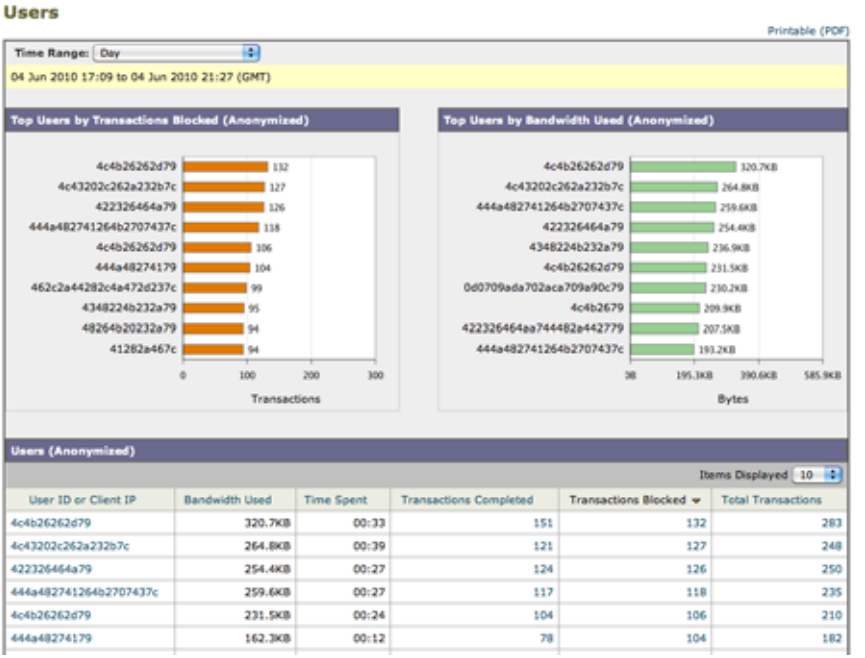
ステップ 2　[Edit Settings] をクリックします。

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

ステップ 4　[Submit] をクリックします。

ステップ 5　[Web] > [Users] を選択します。

ステップ 6　[Web Users] ページが表示されます。



この場合は、ユーザ名が [Web] > [Users] ページに表示されません。

関連項目

表 D-4 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-4　プライバシー情報の関連項目

機能名	機能情報
Web レポーティング	「Web レポーティングを使用する前に」（P.5-3）
Web レポーティングのイネーブル化	「中央集中型 Web レポーティングの設定」（P.5-3）
[User] ページ	「[Users] ページ」（P.5-16）

例 5：既存の Security Management アプライアンスでの新しい Configuration Master へのアップグレード

（注）　この例は、Configuration 6.3 を初期化済みであることを前提としています。

ここでは、既存の Security Management アプライアンスを新しい Configuration Master にアップグレードする方法について説明します。

この例では、ユーザが Configuration Master 6.3 を実行している既存の Security Management アプライアンスを Configuration Master 7.1 にアップグレードする場合を考えます。

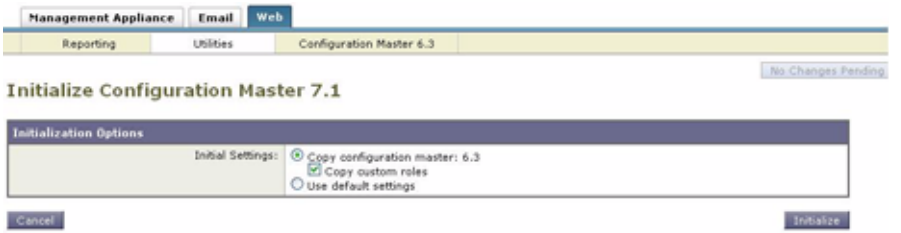
アップグレードを行う手順は、次のとおりです。

ステップ 1　Security Management アプライアンスで、[Web] > [Utilities] > [Configuration Masters] を選択します。

[Configuration Masters] ページが表示されます。

このページから、Configuration Master 6.3 がすでに初期化されていることと、Configuration Master 7.1 が初期化されていないことがわかります。また、唯一の Configuration Master（Configuration Master 6.3）が Security Management アプライアンスのタブの下に表示されていることも確認できます。

ステップ 2　7.1 の行で [Initialize] をクリックします。



ステップ 3　[Copy Configuration Master 6.3] オプション ボタンをクリックし、[Copy custom rules] チェックボックスをオンにします。

[Copying the custom rules] チェックボックスをオンにすると、現在 Configuration Master 6.3 に設定しているユーザ ロールまたは固有のポリシーを維持したまま、新規の Configuration Master 7.1 にデータを転送することができます。

ステップ 4　[Initialize] をクリックします。

Configuration Master 7.1 が初期化され、使用できるようになりました。

関連項目

表 D-5 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-5　新しい Configuration Master のアップグレードの関連項目

機能名	機能情報
Configuration Master	「Configuration Master の操作」（P.8-3）

例 6：既存の Web セキュリティ アプライアンスからのコンフィギュレーション ファイルのインポート

（注）　この例は、Configuration 6.3 を初期化済みであることを前提としています。

この例では、Web セキュリティ アプライアンスから既存のコンフィギュレーションを、既存の Security Management アプライアンスにインポートする方法について説明します。

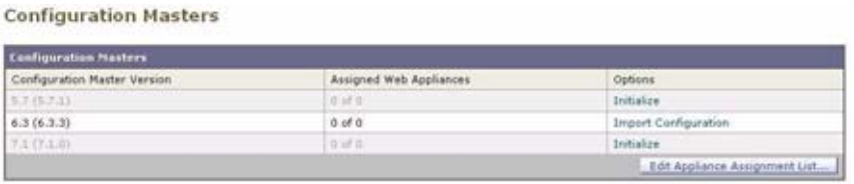
このシナリオでは、ユーザのすべての Web セキュリティ アプライアンスで中央集中型コンフィギュレーション管理を使用することを、ユーザが決定しています。これを行うため、ユーザは最近 Security Management アプライアンスを購入し、Web セキュリティ アプライアンスのすべての管理を行います。

ステップ 1　Security Management アプライアンスで、[Management Appliance] > [Centralized Services] > [Centralized Configuration Manager] を選択します。

ステップ 2　[Enable] をクリックします。

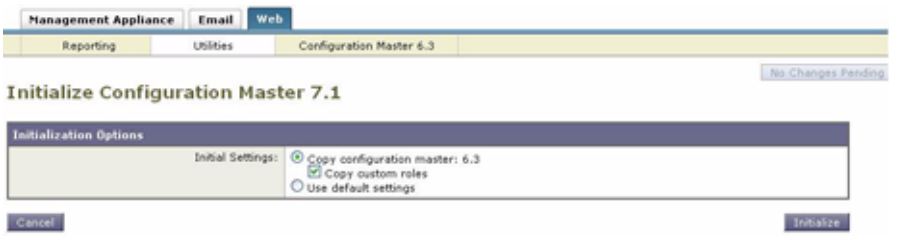
ステップ 3　[Web] > [Utilities] > [Configuration Masters] の順にクリックします。

[Configuration Masters] ページが表示されます。



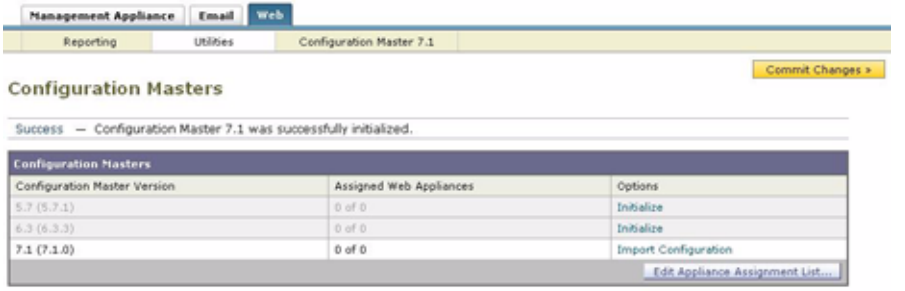
このページから、Configuration Master 6.3 がすでに初期化されていることと、Configuration Master 7.1 が初期化されていないことがわかります。また、唯一の Configuration Master（Configuration Master 6.3）が Security Management アプライアンスのタブの下に表示されていることも確認できます。

ステップ 4　7.1 の行で [Initialize] をクリックします。



ステップ 5　[Use Default Settings] オプション ボタンをクリックします。

[Configuration Masters] ページが表示され、初期化が成功したが示されます。



ステップ 6　[Import Configuration] をクリックします。

[Import Web Configuration] ページが表示されます。

ステップ 7　[Select Configuration Source] ドロップダウン メニューから [Web Configuration File] を選択します。

ステップ 8　[Load a Valid Configuration File from a Web Security Appliance] の横にあるテキスト フィールドで [Browse] をクリックし、Web セキュリティ アプライアンスからインポートする有効な XML ファイルを選択します。

ステップ 9　[Import] をクリックします。

選択した XML ファイルが Web セキュリティ アプライアンスからロードされます。

ステップ 10　[Confirm Import] をクリックします。

その他の考慮事項

Security Management アプライアンスに 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用意されています。たとえば、Security Management 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。Security Management アプライアンスがコンフィギュレーションを公開すると、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。

この方法では、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だけが問題となります。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」のポリシーを作成します。

関連項目

表 D-6 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-6　新しいコンフィギュレーション ファイルのインポートの関連項目

機能名	機能情報
Configuration Master	「Configuration Master の操作」（P.8-3）

例 7：リモート Web セキュリティ アプライアンスでのアクセス ポリシーのカスタマイズと、中央 Security Management アプライアンスでの管理

（注）　この例は、Configuration 6.3 を初期化済みであることを前提としています。

多くの顧客は、1 つの Security Management アプライアンスを使用して複数の Web セキュリティ アプライアンスの導入環境を管理したいと考えています。その場合、現地法が異なるため、地理的なロケーションによってアクセス ポリシーが変わる可能性があります。

たとえば、中国、北米、およびヨーロッパの従業員向けにカスタマイズされた一連のルールが必要なことがあります。ここでは、アクセス ポリシーはローカルに管理できます。

このシナリオでは、地理的にリモートの Web セキュリティ アプライアンス向けにアクセス ポリシーをカスタマイズし、Security Management アプライアンスのローカル管理者にアクセス ポリシーのローカル制御を許可する方法を説明します。

このシナリオでは、ID を作成して 3 つのロケーションそれぞれでユーザを識別し、その後そのロケーション向けに適切なアクセス ポリシーを作成します。次に、ロケーションの ID を、カスタマイズされたロケーションのアクセス ポリシーに追加する必要があります。ユーザがこの ID にタグ付けを行うと、この ID の一部であるポリシーが、ユーザのこのセットに適用されます。最後に、ローカルなアクセス ポリシーを維持するための委任管理者を作成する必要があります。

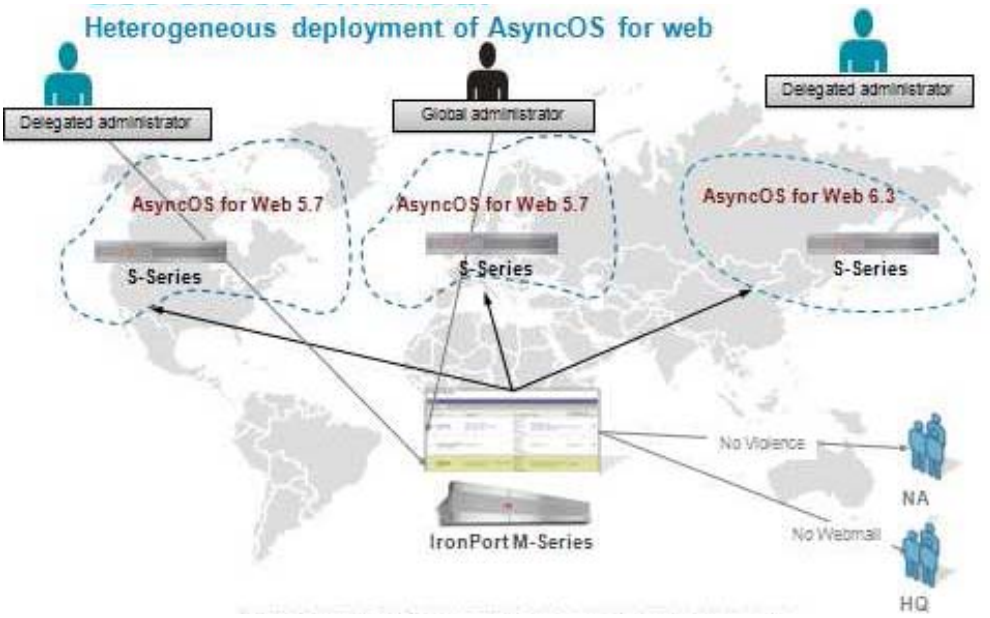
これを行うには、次の手順を実行します。

	アクション	説明
ステップ 1	アクセス ルールの設定	この例では、3 つのアクセス ルールを設定し、必要に応じてこれらのルールをアクセス ポリシーに組み込みます。 • ソーシャル ネットワーク アクセスのルールにより、ソーシャル ネットワークのサイトに対するアクセスが制限されます。 • 武器および暴力のアクセス ルールにより、武器のサイトと暴力のサイトに対するアクセスが制限されます。 • Web ベースの電子メール アクセス ルールにより、Web ベースの電子メールへのアクセスが制限されます。
ステップ 2	アクセス ルールの適用先の決定	ソーシャル ネットワーク アクセスのルールは、すべてのサイトに適用されます。可能であれば、このルールをグローバル アクセス ポリシーに組み込みます。 武器および暴力のルールは、北米（NA）のサイトに適用されます。このルールを NA アクセス ポリシーに組み込みます。Web ベースの電子メール アクセス ルールは、ヨーロッパの本社サイトに適用されます。このルールを HQ アクセス ポリシーに組み込みます。
ステップ 3	ID の作成	この手順により、ポリシーが適用されるユーザの ID と、このユーザが使用する Web セキュリティ アプライアンスの ID を作成できます。 個々のサイトは対応する Web セキュリティ アプライアンスと、ユーザが接続するサブネットによって識別されます。

	アクション	説明
ステップ 4	Configuration Master 5.7 用のカスタム URL カテゴリの作成	AsyncOS 5.7 にはソーシャル ネットワーク URL カテゴリがなく、6.3 には存在するため、AsyncOS 5.7 および 6.3 を実行する Web セキュリティ アプライアンス全体でポリシーを統一するため、カスタム URL カテゴリを作成する必要があります。
ステップ 5	アクセス ポリシーの作成と ID の追加	グローバル ポリシーでは、ソーシャル ネットワーク サイトへのアクセスが禁止されます。北米のアクセス ポリシーでは、武器および暴力サイトへのアクセスが禁止されます。ヨーロッパのアクセス ポリシーでは、Web ベースの電子メールへのアクセスが禁止されます。 さらに、アクセス ポリシーが適用されるユーザを指定する ID と、このポリシーが適用されるサイトを指定するカスタム URL カテゴリを追加する必要があります。
ステップ 6	委任管理者の作成	北米とヨーロッパ向けのローカル アクセス ポリシーは、ローカル ポリシーおよびローカル ルールに詳しい管理者により、ローカル サイトで維持されます。

図 D-2 に、この委任がどのように機能するかを示します。

図 D-2　委任管理



アクセス ルールの設定

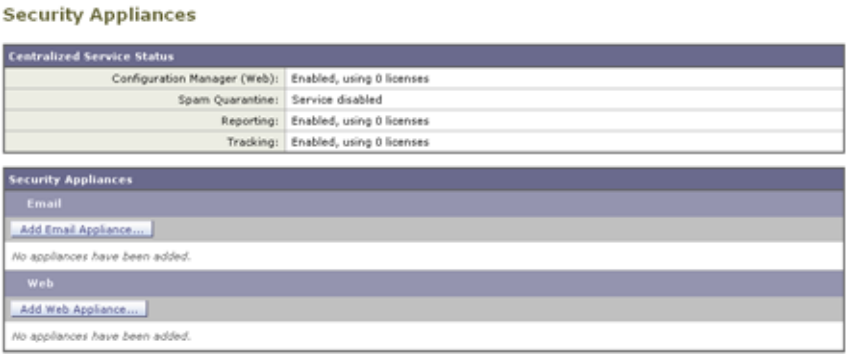
この例では、3 つのアクセス ルールを設定し、必要に応じてこれらのルールをアクセス ポリシーに組み込みます。

- ソーシャル ネットワーク アクセスのルールにより、ソーシャル ネットワークのサイトに対するアクセスが制限されます。
- 武器および暴力のアクセス ルールにより、武器のサイトと暴力のサイトに対するアクセスが制限されます。
- Web ベースの電子メール アクセス ルールにより、Web ベースの電子メールへのアクセスが制限されます。

ステップ 1　Security Management アプライアンスで、[Management Appliance] > [Centralized Services] > [Security Appliances] を選択します。

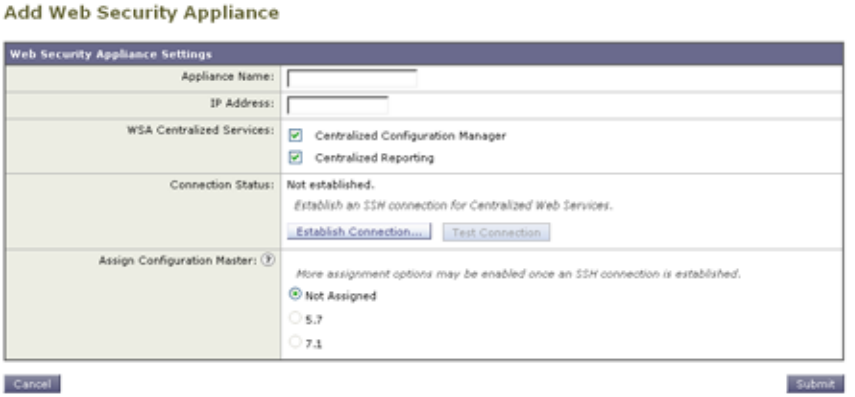
[Security Appliances] ページが表示されます。

図 D-3　[Security Appliances] ページ



ステップ 2　[Add Web Appliance] ボタンをクリックして、[Add Web Security Appliance] ページを表示します

図 D-4　[Add Web Security Appliance] ページ



ステップ 3　[Appliance Name] テキスト フィールドおよび [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。

この例では、アプライアンス名は、China、HQ および NA です。

（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 4　Cisco IronPort アプライアンスを管理する際に使用するサービスを選択します。

（注）　Security Management アプライアンスでイネーブルにしたサービスのみ選択できます。

ステップ 5　[Establish Connection] をクリックします。

[SSH Connection] ダイアログボックスが表示されます。

図 D-5　[SSH Connection] ダイアログボックス

ステップ 6　[Username] および [Password] テキスト フィールドに、Cisco IronPort アプライアンス上の管理者アカウントのログイン資格情報を入力します。

（注）　ログイン資格情報を入力すると、Security Management 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、Security Management アプライアンスには保存されません。

ステップ 7　[Establish Connection] をクリックして、モニタリング サービス用の接続を確立します。

ステップ 8　[Test Connection] をクリックして、リモート アプライアンスのモニタリング サービスが正しく設定され、互換性があることを確認します。

ステップ 9　Web セキュリティ アプライアンスを追加する場合は、アプライアンスを割り当てる Configuration Master を選択します。

各 Configuration Master には、Web セキュリティ アプライアンスのバージョンごとの設定が含まれています。Security Management アプライアンスは、互換性のある AsyncOS のバージョンを実行する Web セキュリティ アプライアンスにのみ Configuration Master を公開できます（たとえば、Web セキュリティ アプライアンスが AsyncOS 6.3 を実行している場合、Configuration Master として

6.3.0 を選択します）。[Web] > [Utilities] > [Configuration Masters] を選択して、後で Web セキュリティ アプライアンスを割り当てることもできます（「Web セキュリティ アプライアンスと Configuration Master の関連付け」（P.8）を参照）。

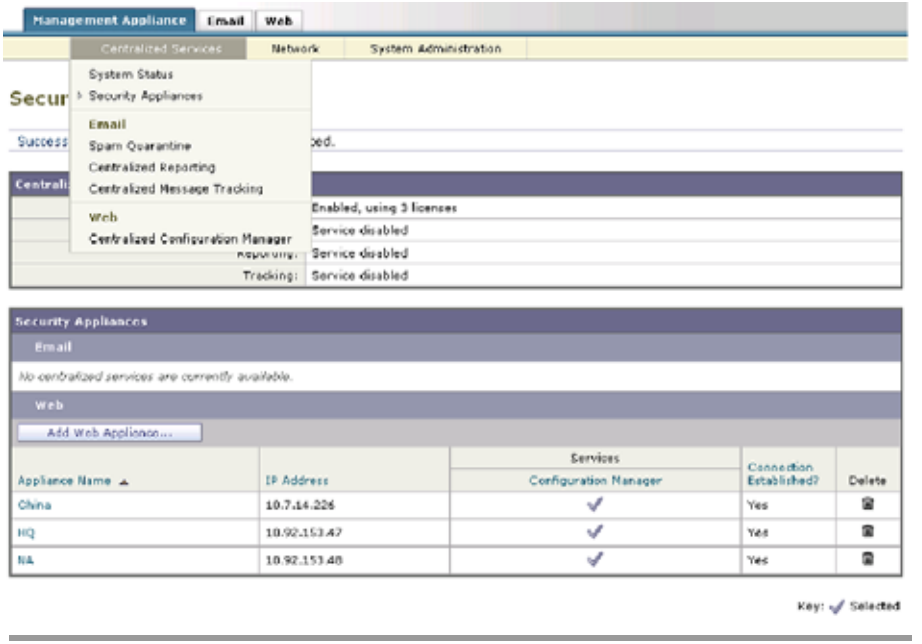
Configuration Master および Web セキュリティ アプライアンスの管理の詳細については、第 8 章「Web セキュリティ アプライアンスの管理」を参照してください。

ステップ 10　[Submit] をクリックしてページでの変更を送信し、[Commit Changes] をクリックして変更を確定します。

[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。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、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。

図 D-6 に、新たに追加された管理対象のアプライアンスが表示されます。

図 D-6　委任管理用に追加された Web セキュリティ アプライアンス



アクセス ルールの適用先の決定

この手順では、社内の全員に適用される次のグローバルなアクセス ポリシーを定義します。

- ソーシャル ネットワーク ルール

  このアクセス ポリシーはすべてのサイトに適用されます。

- 武器および暴力ルール

  このポリシーは北米拠点へローカルに適用されます。

- Web ベースの電子メール ルール

  このポリシーは HQ 拠点へローカルに適用されます。

（注） アクセス ポリシーの設定を開始する前に、中央集中型 Web コンフィギュレーション マネージャがイネーブルになっていることを確認します。

ステップ 1 Security Management アプライアンスで、[Web] > [Configuration Manager 7.1] > [Access Policies] を選択します。

ステップ 2 [Add Policy] をクリックします。

ステップ 3 [Access Policy:Add Group] ウィンドウで、[Social Networking Rule] と入力し、このポリシーをすべてのサイトに適用します。

ステップ 4 [Submit] をクリックします。

ステップ 5 [Web] > [Configuration Manager 7.1] > [Access Policies] に戻り、[Add Policy] をクリックします。

ステップ 6 [Access Policy:Add Group] ウィンドウで、[Weapons and Violence Rule] と入力し、このポリシーを北米のサイトに適用します。

ステップ 7 [Submit] をクリックします。

ステップ 8 最後に、[Web] > [Configuration Manager 7.1] > [Access Policies] に戻り、[Add Policy] をクリックします。

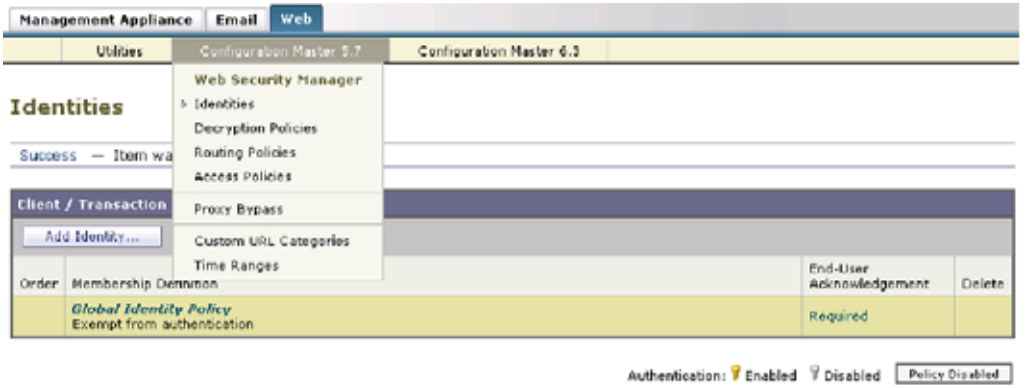
ステップ 9 [Access Policy:Add Group] ウィンドウで、[Web-based Email Rule] と入力し、このポリシーを HQ サイトに適用します。

ステップ 10 [Submit] をクリックします。

ID の作成

この手順により、ポリシーが適用されるユーザの ID と、このユーザが使用する Web セキュリティ アプライアンスの ID を作成できます。個々のサイトは対応する Web セキュリティ アプライアンスと、ユーザが接続するサブネットによって識別されます。

ステップ 1　[Web] > [Configuration Master 5.7] > [Identities] > [Add Identities] を選択し、中国拠点の ID を作成します。

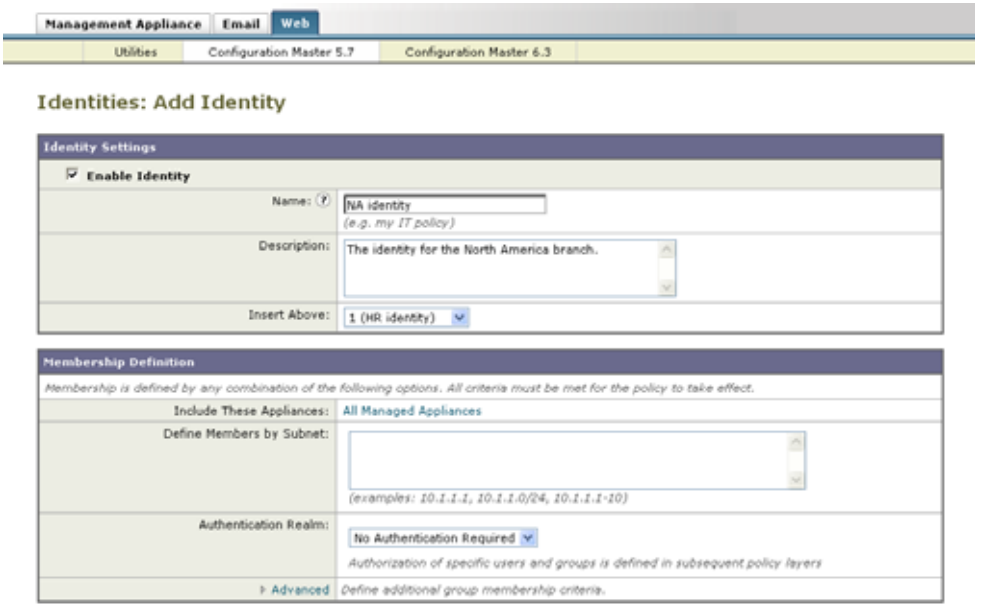


ステップ 2　[Web] > [Configuration Master 5.7] > [Identities] > [Add Identities] を選択し、北米拠点の ID を作成します。

武器および暴力ルールは、北米のサイトだけに適用されます。北米サイトの Web セキュリティ アプライアンスは AsyncOS 5.7 を実行しています。

ステップ 3　[Identity Settings] テキスト フィールドで、[NA identity] と入力します。

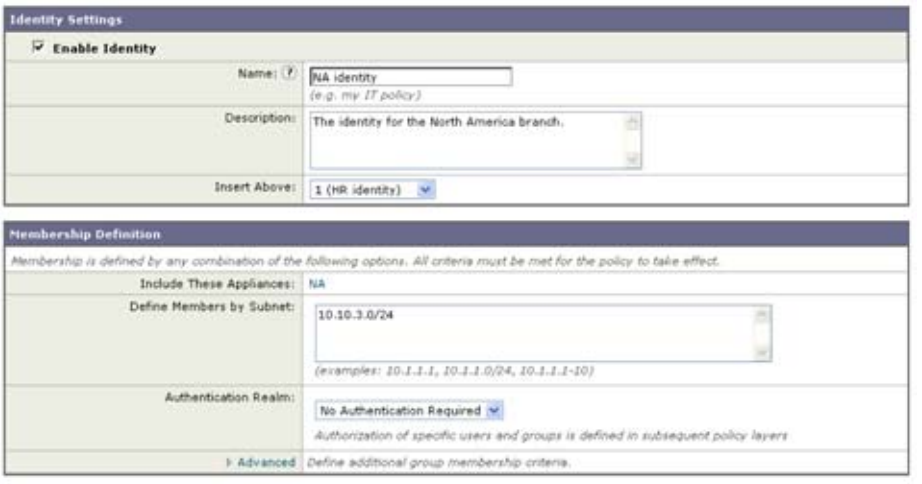
ステップ 4　[Include these Appliances] の横にある [All Managed Appliances] をクリックして、北米サイトのアプライアンスに ID を制限します。



ステップ 5　[Web] > [Identity Policies] > [Managed Appliances] を選択します。

ステップ 6　[NA] の横にあるチェックボックスをオンにします。

この例では、ユーザのグループが 10.10.3.0/24 サブネット上にあります。

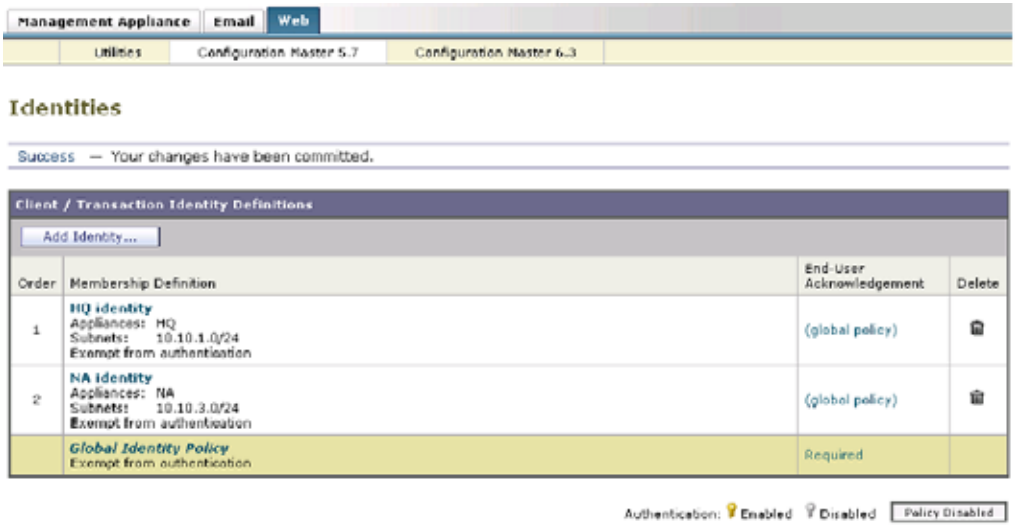


ステップ 7　NA に対して実行した手順（ステップ 2 ～ 6）と同じ手順で、**HQ** の ID を新たに作成します。

この ID の **HQ** Web セキュリティ アプライアンスのチェックボックスを選択します。この例のユーザのグループは 10.10.1.0/24 サブネット上にあります。

これで、図 D-7 に示すように 2 つの ID が作成されます。

図 D-7　作成された ID



Configuration Master 5.7 用のカスタム URL カテゴリの作成

AsyncOS 6.3 ではソーシャル ネットワーク URL カテゴリを使用できますが、AsyncOS 5.7 では使用できないため、カスタム URL カテゴリを作成する必要があります。

ソーシャル ネットワーク カスタム カテゴリには次のサイトが含まれます。

- myspace.com
- facebook.com
- linkedin.com

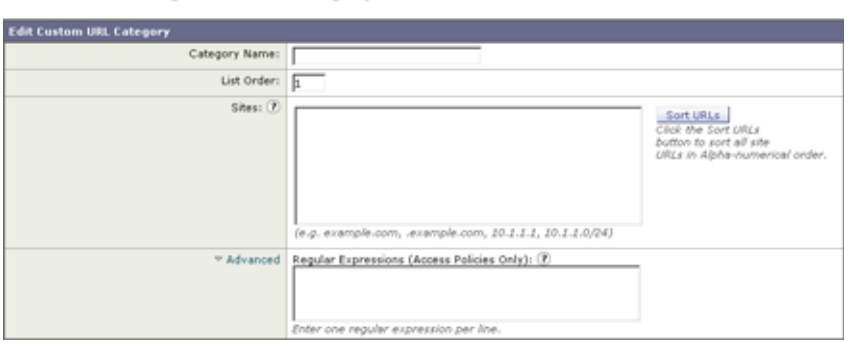
- twitter.com
- badoo.com

ステップ 1　Security Management アプライアンスで、[Web] > [Configuration Master 7.1] > [Custom URL Categories] を選択します。

[Custom URL Categories] ページが表示されます。

ステップ 2　[Add Custom Category] をクリックして、5.7 用のソーシャル ネットワークを作成します。

図 D-8　　カスタム URL カテゴリの作成

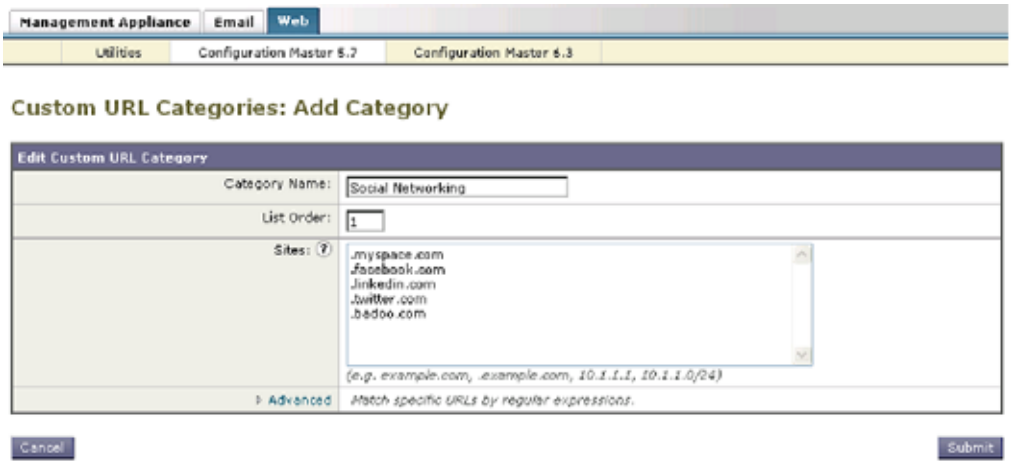


ステップ 3　カスタム URL カテゴリを作成または編集するには、次の設定を該当するフィールドに入力します。

- [Category Name] : URL カテゴリの名前を入力します。この名前は、ポリシー グループに URL フィルタリングを設定するときに表示されます。
- [Sites] : ソーシャル ネットワーク カテゴリに属するドメイン名を入力します。

  複数のアドレスは、改行またはカンマで区切って入力します。
  この例では、次のドメインを使用しています。
  - myspace.com
  - facebook.com
  - linkedin.com
  - twitter.com
  - badoo.com

図 D-9　　カスタム URL カテゴリ



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] をクリックしてアプライアンスへの変更を確定します。

アクセス ポリシーの作成と ID の追加

この手順では、ソーシャル ネットワーク サイトへのアクセスを制限するすべてのサイト向けのアクセス ポリシーを作成します。次の 3 つのポリシーを作成する必要があります。

- China Policy
- NA policy
- HQ policy

中国拠点の Web セキュリティ アプライアンスは、Configuration Master 6.3 だけを実行しています。中国拠点に対する唯一のアクセス ポリシー ルールは、ソーシャル ネットワーク サイトへのアクセスを禁止するルールです。ソーシャル ネットワーク カテゴリは Configuration Master 6.3 の URL カテゴリのセットに含まれているため、ソーシャル ネットワークが、アクセスが禁止されている URL カテゴリとして選択されていることを確認する必要があります。

ステップ 1　Security Management アプライアンスで、[Web] > [Configuration Master 6.3] > [Access Policies] を選択します。

ステップ 2　[URL Categories] カラムのリンクをクリックし、グローバル アクセス ポリシーを変更します。

ステップ 3　[Social Networking] が選択され、割り当てられた ID がブロックされていることを確認します。

NA 拠点の Web セキュリティ アプライアンスは AsyncOS 5.7 を実行しています。NA アクセス ポリシーには、次の 2 つのルールを適用する必要があります。

- 武器および暴力サイトへのアクセスを禁止するローカル ルール。
- ソーシャル ネットワーク サイトへのアクセスを禁止するルール。

ソーシャル ネットワーク カテゴリは 5.7 に含まれていないため、ソーシャル ネットワークを確実に禁止するには、ソーシャル ネットワークのカスタム URL カテゴリを作成する必要があります。

ステップ 4　Security Management アプライアンスで、[Web] > [Configuration Master 5.7] > [Access Policies] を選択します。

ステップ 5　[Add Policy] をクリックします。

ステップ 6　[Access Policies: Add Policy] ページで次の手順を実行します。

- [Policy Setting] セクションで [Enable Policy] チェックボックスをオンにします。
- [Policy Name] テキスト フィールドに [NA policy] と入力します。
- [Policy Member Definition] セクションで、ドロップダウン リストから [NA Identity] を選択します。

ステップ 7　[Submit] をクリックします。

[Submit] をクリックすると、[Access Policies] ページに戻ります。

ステップ 8　[Access Policies] ページの NA アクセス ポリシー行で、[URL Categories] カラムの [global policy] リンクをクリックします。

ステップ 9　Weapons URL カテゴリおよび Violence URL カテゴリが、このアクセス ポリシーに選択されていることを確認します。さらに、[Social Networking] カスタム URL カテゴリがブロックされていることを確認します。

最後に HQ 拠点ポリシーを処理する必要があります。HQ 拠点の Web セキュリティ アプライアンスは AsyncOS 5.7 を実行しています。NA アクセス ポリシーには、次の 2 つのルールを適用する必要があります。

- Web ベースの電子メール サイトへのアクセスを禁止するローカル ルール。
- ソーシャル ネットワーク サイトへのアクセスを禁止するルール。

ソーシャル ネットワーク カテゴリは 5.7 に含まれていないため、ソーシャル ネットワークを確実に禁止するには、ソーシャル ネットワークのカスタム URL カテゴリを作成する必要があります。

ステップ 10　Security Management アプライアンスで、[Web] > [Configuration Master 5.7] > [Access Policies] を選択します。

ステップ 11　[Add Policy] をクリックします。

ステップ 12　[Access Policies: Add Policy] ページで次の手順を実行します。

- [Policy Setting] セクションで [Enable Policy] チェックボックスをオンにします。
- [Policy Name] テキスト フィールドに [HQpolicy] と入力します。
- [Policy Member Definition] セクションで、ドロップダウン リストから [HQ Identity] を選択します。

ステップ 13　[Submit] をクリックします。

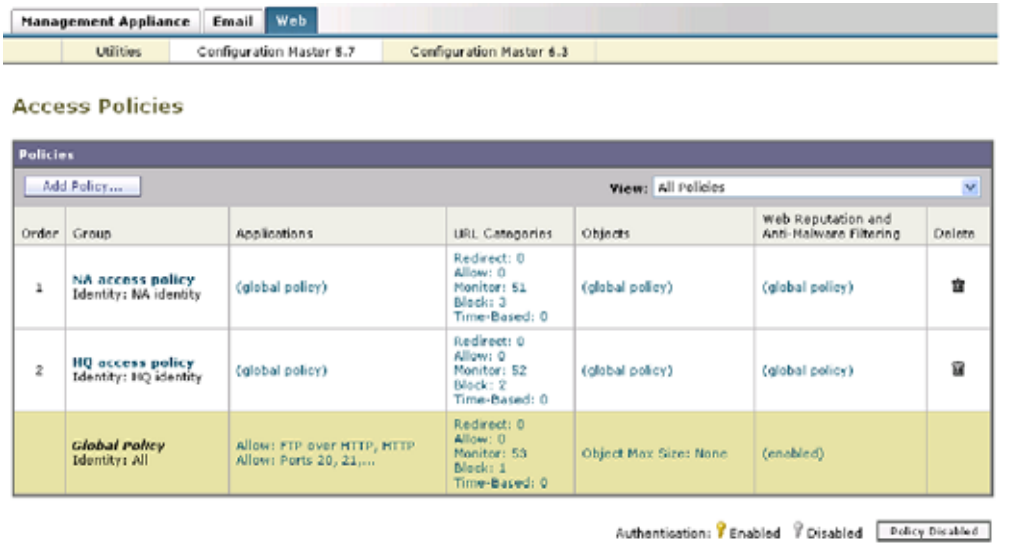
[Submit] をクリックすると、[Access Policies] ページに戻ります。

ステップ 14　[Access Policies] ページの HQ アクセス ポリシー行で、[URL Categories] カラムの [global policy] リンクをクリックします。

ステップ 15　[Social Networking] カスタム URL カテゴリがブロックされていることを確認します。さらに、[Web-based Email] カテゴリがブロックされていることを確認します。

これで、本社の Web セキュリティ アプライアンスにおけるデフォルトのソーシャル ネットワーク ポリシーが、新しいソーシャル ネットワーク ポリシーに置き換えられます。

図 D-10　　例 7 で完成したポリシー



委任管理者の作成

次に、委任管理者を追加する必要があります。それには、管理可能なアクセス ポリシーを割り当てる委任管理者の、Web ユーザ ロールを作成する必要があります。

ユーザ ロールを定義するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[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。

これにより、NA 拠点のユーザ ロールが追加されます。

ステップ 3　[Edit Web User Roles] ページの [Name] テキスト フィールドに **na_admin_role** と入力します。

ステップ 4　[Submit] をクリックします。

[User Roles] ページが表示されます。

ステップ 5　[Configuration Master 5.7] の下の [na_admin_role] 行で、[Access policies] をクリックします。

[Edit Access Policy Privileges: na_admin_role] ページが表示されます。

ステップ 6　[NA Access Policy] の横にあるチェックボックスをオンにして、NA 委任管理者用のユーザ ロールへの NA アクセス ポリシーを選択します。

ここでは、ソーシャル ネットワークのカスタム URL は、NA 拠点のユーザ ロールに追加されません。これは共有 URL カテゴリです。1 つのサイトでこれを変更すると、すべてのサイトに反映されます。このカテゴリは、メイン管理者の管理に任せることにします。これで、NA 拠点のユーザ ロール設定が完了しました。

委任ユーザのユーザ ロールが設定されたため、NA 拠点の委任管理者を作成できるようになりました。

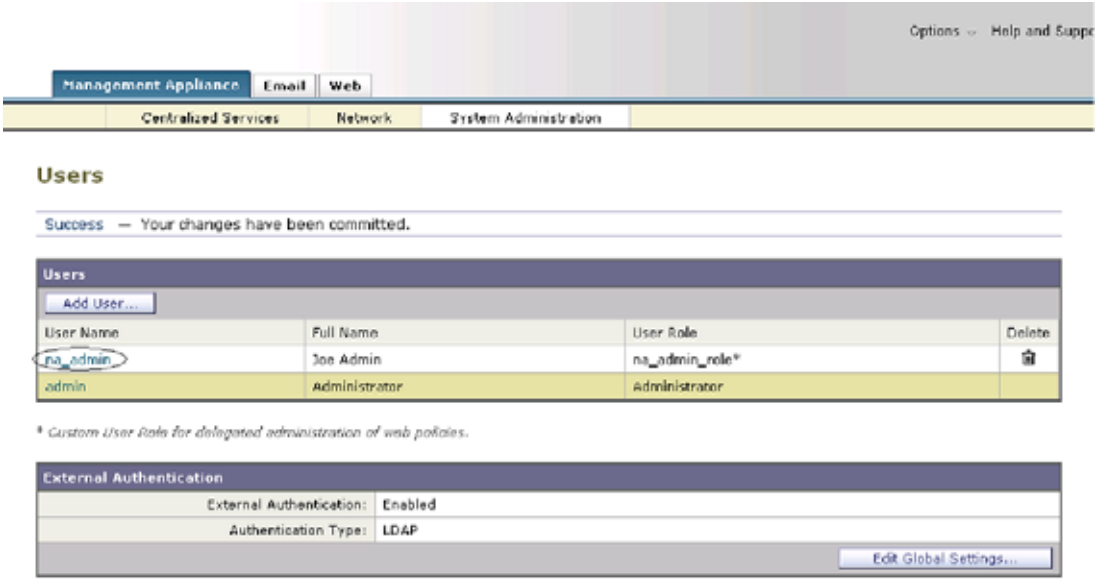
ステップ 7　Security Management アプライアンスで、[Management Appliance] > [System Administration] > [Users] を選択します。

ステップ 8　[Add User] をクリックします。

ステップ 9　[Custom Roles] オプション ボタンをクリックし、[Custom Roles] の下にあるウィンドウで [na_admin_role] を選択します。

ステップ 10　[Submit] をクリックします。

これで NA 委任管理者のロールが付与されます。



HQ 委任管理者のロールを持つユーザ ロールを新たに作成する必要があります。

ステップ 11　Security Management アプライアンスで、[Management Appliance] > [System Administration] > [Users] を選択します。

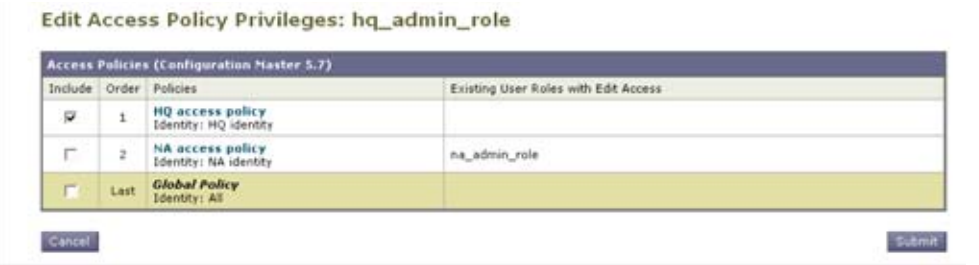
ステップ 12　[Add Users] をクリックします。

ステップ 13　[Edit User Roles] ページの [Name] テキスト フィールドに **hq_admin_role** と入力します。

ステップ 14　[Submit] をクリックします。

ステップ 15　[User Roles] ページにある [Configuration Master 5.7] の下の [hq_admin_role] 行で、[Access policies] をクリックします。

ステップ 16　[Edit Access Policies] ページで、[Include] チェックボックスをオンにして、HQ 委任管理者が HQ アクセス ポリシーを管理できるようにします。



ステップ 17　[Submit] をクリックします。

ステップ 18　Security Management アプライアンスで、[Management Appliance] > [System Administration] > [Users] を選択します。

ステップ 19　[Add User] をクリックします。

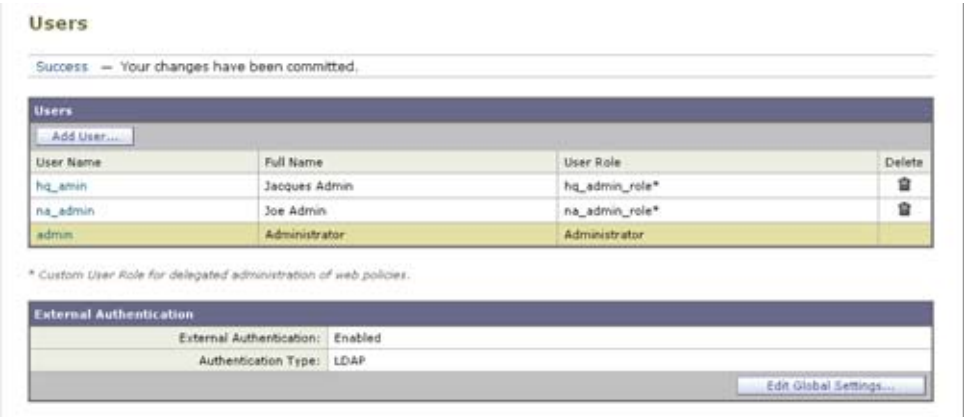
ステップ 20　[Custom Roles] オプション ボタンをクリックし、[Custom Roles] の下にあるウィンドウで [hq_admin_role] を選択します。

これで、HQ 管理者ロールが HQ 管理者に割り当てられます。

ステップ 21　[Submit] をクリックします。

図 D-11 に、割り当てられた委任管理者が表示された Users テーブルを示します。

図 D-11　　割り当てられた委任管理者



すべて完了しました。

これで、3 つの各ロケーションに、ユーザを識別する ID が作成されました。

この後、ロケーションに適切なアクセス ポリシーを作成し、ロケーションの ID を、ロケーションのカスタマイズされたアクセス ポリシーに追加しました。

さらに、AsyncOS 5.7 にはないカテゴリを追加するため、URL カテゴリを作成しました。

最後に、ローカルなアクセス ポリシーを維持するための委任管理者を作成しました。

関連項目

表 D-7 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-7　アクセス ポリシーのカスタマイズの関連項目

機能名	機能情報
[User] ページ	「[Users] ページ」（P.5-16）
[User Details] ページ	「[User Details] ページ」（P.5-20）
[Custom URL Categories] ページ	「カスタム URL カテゴリ」（P.5-33）

APPENDIX E

インタラクティブ カラム

この付録では、[Management Appliance]、[Web]、および [Email] の各アプライアンス レポート ページで使用可能なすべてのカラムとその意味について説明します。

中央集中型 Web レポーティング ページのインタラクティブ カラム

ここでは、Web セキュリティ アプライアンスの各種レポート ページで使用可能なインタラクティブ カラムについて説明します。

（注） レポート ページによっては、一部のカラムを使用できないことがあります。特定のレポート ページで使用可能なカラムを表示するには、各 [Web Reporting] ページのカラムのリンクをクリックします。また、カラムの内容が得られた [Web Tracking] ページへのリンクが、そのカラムに表示されることがあります。

表 E-1　中央集中型 Web レポーティング ページのインタラクティブ 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割合で表示されます。
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 E-1　中央集中型 Web レポーティング ページのインタラクティブ 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。ユーザの調査目的の場合は、各 URL カテゴリにユーザが費やした時間。URL のトラッキング時には、その特定の URL に各ユーザが費やした時間。 トランザクション イベントに「確認済み」のタグが付くと（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、アクティブな 1 分間に異なる 4 つのドメインに進んだ場合、そのユーザはそれぞれのドメインに 15 秒を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、アプライアンス経由で HTTP トラフィックを送信したユーザ名または IP アドレスとして定義され、Web サイトにアクセスし、それが AsyncOS で「ページ ビュー」と見なされます。 • 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、ユーザ ページ ビューを識別するためにベスト エフォート型の推測を行います。 単位は HH:MM 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	モニタ中の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。

表 E-1　中央集中型 Web レポーティング ページのインタラクティブ カラムの説明 （続き）

カラム名	説明
Warned URL Category	警告を開始し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 Application or Application Type	アプリケーション タイプのため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。
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総数。

中央集中型電子メール レポーティング ページのインタラクティブ カラム

ここでは、中央集中型 Email Security アプライアンスの各種レポート ページで使用可能なインタラクティブ カラムについて説明します。

表 E-2　インタラクティブ 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、コンテンツ フィルタによる阻止の 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 E-2　インタラクティブ 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。
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
Clean	すべてのクリーン メッセージ。
DNS Verified	検証されたすべてのドメイン名。
SBRS	送信者ベースのレピュテーション スコア。
Last Sender Group	最後の有効な送信者グループ。
Total Attempted	試行された着信メール メッセージの総数。
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。

表 E-2　インタラクティブ カラムの説明 （続き）

カラム名	説明
Incoming 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。
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 接続の総数。
Total Messages	TLS メッセージの総数。
Virus Outbreaks	
Outbreak Name	感染発生の名前。
Outbreak ID	感染発生 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	検疫に関係するメッセージ。

APPENDIX F

Cisco IronPort エンド ユーザ ライセンス契約書

この付録の内容は、次のとおりです。

Cisco IronPort Systems, LLC ソフトウェア使用許諾契約書

すべてのユーザに対する警告：本ソフトウェア（以下で定義）のライセンスについて、以下の法的な契約書（「契約書」）を注意深くお読みください。同意ボタンをクリックするか、質問に「Y」を入力することで、お客様（個人または単一の実在者のいずれかを指し、総称して「お客様」と呼びます）は、デラウェア州法人である Cisco IronPort Systems, LLC（以下「IronPort」）とお客様（総称して「両当事者」と呼びます）との間の以下の契約に従い、その当事者となることに同意したことになります。同意ボタンをクリックするか、質問に「Y」を入力することで、お客様は（A）お客様がお客様の会社を代表する権限を正式に与えられており、（B）お客様の会社を代表して本契約の条件に同意することを表明したことになり、それによって契約が成立します。お客様またはお客様が代表する会社（総称して「お客様」と呼びます）が本契約の条件に同意しない場合は、キャンセル ボタンをクリックするか、質問に「N」を入力し、速やかに（ただし後述のとおり納品日から 30 日以内に）、IronPort または本ソフトウェアの提供元である販売代理店に通知し、本ソフトウェアに対して支払った代金の全額の返金を受けてください。

1. 定義

1.1「お客様のサービス」とは、お客様の内部的なビジネスを遂行することを目的とし、購入契約、評価契約、ベータまたはプレリリース契約、注文書、見積書、お客様と IronPort またはその販売代理店との間のその他同様の契約（以下「契約」）、ならびにシステム アーキテクチャおよびそのインターフェイスの概要が記載されている該当するユーザ インターフェイスおよび IronPort の標準システム ガイド ドキュメント（総称して「ライセンス文書」と呼びます）で規定されているとおり、お客様の製品を通じて可能となる、エンド ユーザに提供される、お客様の電子メールまたはインターネット サービスを意味します。

1.2「エンド ユーザ」とは、お客様のサービスを通じてインターネットへアクセスすること、もしくは電子メール サービスを利用することをお客様が承認した従業員、請負業者、またはその他の代理人を意味します。

1.3「本サービス」とは、（i）アップデートおよびアップグレードを含む、本ソフトウェアの機能の提供、および（ii）場合によって IronPort またはその販売代理店によるサポートの提供を意味します。

1.4「本ソフトウェア」とは、（i）IronPort が所有し、IronPort のハードウェア製品とともに IronPort によってお客様にライセンス付与されるソフトウェア、（ii）IronPort のサードパーティ ライセンサーによって提供され、IronPort のハードウェア製品で使用するためにお客様にライセンス付与された任意のソフトウェア、（iii）IronPort のハードウェア製品とともに IronPort によってお客様にライセンス付与されたその他の任意の IronPort ソフトウェア モジュール、および（iv）それらに対するすべてのアップデートおよびアップグレードを意味します。

1.5「アップデート」とは、本ソフトウェアに大規模な新機能を追加せず、IronPort またはそのサード パーティ ライセンサーによってリリースされる、マイナー アップデート、エラー修正およびバグ修正を意味します。アップデートは、本ソフトウェアのリリース番号における小数点の右側の増加（たとえば、ソフトウェア 1.0 からソフトウェア 1.1 へ）により示されます。「アップデート」という用語は、IronPort またはそのサード パーティ ライセンサーにより個別の製品として販売およびライセンス付与されるアップグレードまたは新しいソフトウェア バージョンを明確に除外します。

1.6「アップグレード」は、本ソフトウェアに対する改訂を意味し、IronPort またはそのサードパーティ ライセンサーによりその独自の裁量でリリースされた場合に、新しい拡張機能を既存の機能に追加します。アップグレードは、本ソフトウェアのリリース番号における小数点の左側の増加（たとえば、ソフトウェア 1.x からソフトウェア 2.0 へ）により示されます。いかなる場合にも、アップグ

レードには、IronPort またはそのサード パーティ ライセンサーにより個別の製品として販売およびライセンス付与される本ソフトウェアの新しいバージョンは含まれません。

2. ライセンスの付与とデータ収集条件についての同意

2.1 ソフトウェアのライセンス。本ソフトウェアおよびライセンス文書を使用することにより、お客様は本契約の条件に従うことに同意し、お客様が本契約に準拠している限り、IronPort はお客様に、契約期間中、お客様のサービスをエンドユーザに提供することに関連してのみ、IronPort のハードウェア製品上でのみ本ソフトウェアを使用する非独占的、二次ライセンス不能、譲渡不能、世界的なライセンスを付与します。本ライセンスの期間と範囲は、ライセンス文書で別途規定します。本契約で明示する場合を除き、IronPort、IronPort の販売代理店、またはその各ライセンサーは、お客様に対し、いずれの本ソフトウェアにおける権利、権原、権益も付与しません。本ライセンスとすべての本サービスは同時に終結します。

2.2 データの使用についての同意とライセンス。本契約の第 8 項と、お客様への通知をもって IronPort により随時修正される可能性がある IronPort プライバシー声明（http://www.ironport.com/privacy.html）に従い、お客様は、IronPort により随時修正される可能性があるライセンス文書に規定されているとおり、お客様からデータ（以下「データ」）を収集し使用することに同意し、そのライセンスを IronPort に付与します。データを使用してレポートまたは統計情報を生成する範囲において、データは全体としてのみ開示され、ユーザ名、電話番号、難読化されていないファイル名、電子メール アドレス、物理アドレス、およびファイルの内容など、エンド ユーザの識別情報をデータから推測できないようにするものとします。上記にかかわらず、お客様は、事前に書面または電子的な手段で通知することで、IronPort がデータを収集および使用する権利をいつでも終了させることができますが、かかる権利が終了した場合、お客様は本ソフトウェアまたは本ソフトウェアのコンポーネントを利用できなくなります。

3. 機密性。各当事者は、相手方当事者のすべての機密情報を、自身の同様の機密情報を保護するのと同じ程度に（また、いかなる場合にも妥当な程度の注意を払って）秘密に保持し、かかる機密情報を本契約で許された範囲でのみ使用することに同意します。本契約での「機密情報」とは、「機密」と表示された当事者の情報または開示元の当事者が独占的または機密として見なすことが妥当な情報を意味します。ただし、IronPort によって提供される本ソフトウェアの設計レビューおよびあらゆる製造前のリリースで開示されたデータ、本ソフトウェア、情報は、機密と表示されているどうかにかかわらず明らかに機密情報と見なされます。

4. 財産権、所有権。IronPort またはその販売代理店によりお客様に提供された本ソフトウェアおよびその他の資料の権原および所有権、ならびに前記にかかわるすべての知的財産権（以下で定義）は、IronPort および/またはその上位ライセンサーの独占的所有物です。お客様ならびにその従業員および代理人は、IronPort またはその販売代理店によってお客様に提供された本ソフトウェアまたはその他の資料のコピーに現れる商標またはその他の所有権表記、説明文、記号またはラベルを削除または改変しないものとします。お客様は、本ソフトウェアまたは本ソフトウェアによって生成される内部データファイルの変更、変換、営利目的での転売、配布、複製、機能拡張、適合、翻訳、逆コンパイル、リバースエンジニアリング、逆アセンブルを行ったり、本ソフトウェアまたは本ソフトウェアによって生成される内部データ ファイルのソースコードを特定したり、取得しようとしたり、本ソフトウェアまたはライセンス文書に基づいて二次的著作物を作成したりしないものとし、他者によるそのような行為を許可または承認しないことに同意します。別途書面で合意しない限り、本契約または関連するすべてのコンサルティングまたはプロフェッショナル サービス契約の履行途中に IronPort またはその上位ライセンサーによって作成または開発されたプログラム、発明、概念、文書、仕様、またはその他の文書化された資料または図面による資料および媒体は、すべての著作権、データベース権、特許、企業秘密、商標、著作者人格権、またはかかる作業の遂行に関連するその他すべての知的財産権（「知的財産権」）を含め、IronPort またはその上位ライセンサーに独占的に属するものとし、合衆国法典第 17 編（1976 年著作権法）の意味の範囲内でお客様のために有償で行われた作業とは見なさないものとします。

5. 制限付き保証と保証の放棄

5.1 制限付き保証。IronPort はお客様に対し、本ソフトウェアが適切にインストールされ正しく使用されている場合に、ライセンス文書に記載された仕様に相当程度に従うことを、納品日から 90 日間か、ライセンス文書に記載されている期間のうちの長いほうの期間（以下「保証期間」）にわたり保証します。本項に記載されている保証のいずれかの違反に対し、お客様の唯一の法的救済および IronPort の全責任は、保証期間内にお客様によって不適合が IronPort および/またはその販売代理店に報告された場合に限り、誤りまたは不適合をすみやかに修正することです。この保証は、お客様に対してのみ行われ、エンド ユーザまたは他の第三者への譲渡はできません。本項で定める保証の違反、または本契約の違反に対し、かかる違反が直接的または間接的に次のいずれかから、またはそれに関連して生じた場合、IronPort は一切の責任を負いません。(i) お客様または第三者による、本ソフトウェアの無許可の、不適切な、不完全な、または不適当なメンテナンスまたはキャリブレーション、(ii) 第三者のハードウェア、ソフトウェア、サービスまたはシステム、(iii) 本ソフトウェアまたは本サービスの許可のない変更または改造、(iv) 本ソフトウェアの無許可の、もしくは不適切

な使用もしくは操作、またはお客様が該当する環境仕様に従わなかった場合、（v）IronPort またはその販売代理店から随時提供されるアップデート、アップグレード、修正、改訂をインストールおよび/または使用しなかった場合。

5.2 保証の否認。本契約書の 5.1 項に記載されている明示的な保証は、本ソフトウェアまたは本サービスに関する唯一の保証を構成します。適用法によって許される最大の限度まで、IronPort は本契約上の本ソフトウェアと本サービスのライセンスを「現状のまま」付与します。本契約で明示的に規定しない限り、IronPort およびその上位ライセンサーは、明示、黙示または制定法上の（事実上の、または法律の運用による）いかなる形の表明も保証も行わず、市場性または特定目的適合性の黙示的保証などを含むその他のあらゆる保証を明示的に否認します。IronPort もそのサード パーティ ライセンサーも、本ソフトウェアまたは本サービスが（1）不具合、エラー、バグを含まないこと、（2）本ソフトウェアの動作が中断しないこと、（3）本ソフトウェアの使用により得られるか得られる可能性がある結果または情報が正確で、完全で、信頼でき、安全であることを保証しません。

6. 責任制限。適用法で許される最大限度まで、いずれの当事者も相手方に対して、利益の損失、代替商品またはサービスの調達コスト、取引上の損失、使用またはデータの損失、事業の中断、またはあらゆる種類の間接的損害、特別損害、偶発的損害、結果的損害について、かかる当事者がかかる損害の可能性を示す事前通知を受け取っていた場合であっても、責任を負わないものとします。いかなる場合でも、本契約のいずれかの条項の下で生じる各当事者の責任は、かかる損害の請求が契約、不法行為、その他の法理論に基づくかどうかにかかわらず、そのような責任を生じさせる事象よりも前の 12 ヵ月間に、本ソフトウェアまたは本サービスに対して支払われた総額を超えないものとします。

7. 契約の期間および終了。本契約の期間（「契約期間」）は、ライセンス文書で規定するものとします。IronPort が本契約またはライセンス文書の重要な条項を履行しなかった場合、お客様は、書面で通知してから 30 日の間に不履行が解決されなかった場合、通知から 30 日後に本契約を終了させることができます。お客様が本契約またはライセンス文書の重要な条項を履行しなかった場合、IronPort は、書面で通知してから 30 日の間に不履行が解決されなかった場合、通知から 30 日後に返金することなく本契約を終了させることができます。本契約は、次の場合に、いずれかの当事者により、いつでもただちに通告なく終了させることができます。（i）相手方当事者によるまたは相手方当事者に対する債務超過、管財人管理または破産手続き、またはかかる当事者の負債の調停のためのその他の訴訟手続、（ii）相手方当事者による債権者への一括譲渡、（iii）相手方当事者の解散。本契約が終了または満了した場合、第 2 項で付与されたライセンスはただちに終了します。お客様は、本契約が終了または満了してから 30 暦日以内に、

本契約の下で IronPort またはその販売代理店によりお客様に提供された本ソフトウェアおよびその他すべての資料またはドキュメントのすべてのコピーを IronPort またはその販売代理店に返却または破棄するものとします。

8. U.S. 政府による権利の制限、輸出管理。本ソフトウェアおよび付随するライセンス文書は、該当する DFAR 227.7202 および FAR 12.212 に従い、それぞれ「商用コンピュータ ソフトウェア」および「商用コンピュータ ソフトウェア文書」と見なされます。米国政府による本ソフトウェアおよび付随するライセンス文書の使用、変更、複製、リリース、実行、表示、開示は、本契約の条項のみによって決定され、本契約の条項によって明示的に許される範囲を除き禁止されます。お客様は、本ソフトウェアおよびライセンス文書は米国の輸出管理規則に従って輸出しなければならず、米国の法律に反する行為は禁止されることを認めます。お客様は、米国輸出管理局もその他の連邦政府関係機関も、お客様が輸出する権利の停止、取り消し、拒否をしていないことを表明します。お客様は、お客様が本ソフトウェアを核兵器、科学兵器または生物兵器、ミサイル技術に関連して使用せず、これらの関連する最終使用のために譲渡しないことを表明します。ただし、米国政府により、規制または特定のライセンスによって許可されている場合を除きます。お客様は、米国およびその他の国におけるあらゆる輸入および輸出規制、その他の適用法に従うのは、最終的にお客様の責任であることを認め、IronPort またはその販売代理店が、元の販売国内でお客様に最初に販売した後はいかなる責任も負わないことを認めます。

9. 雑則。本契約は、法の抵触のルールを排除して、米国およびカリフォルニア州の法律に準拠します。国際物品売買契約に関する国連条約の適用は、明示的に除外されます。本契約に含まれるすべての規定は、両当事者間の代理関係、提携、その他の合同企業を構成するものと解釈されません。いずれの当事者も、下記による義務の不履行または履行遅延を理由とした責任を負わないものとします（金銭の支払いを除きます）。(i) 米国の現在もしくは将来の法令または本契約に適用される法律の条項、(ii) 電力供給の中断、インターネットの障害、ストライキ、品不足、暴動、反乱、火災、洪水、暴風雨、爆発、天災、戦争、テロ、政府の行動、労働条件、地震、またはかかる当事者の合理的な支配の及ばないその他の事由。本契約およびライセンス文書は、本ソフトウェアの使用に対するすべての権利を定め、両当事者間の完全な合意であり、本ソフトウェアおよびライセンス文書にかかわるその他のあらゆる通信に優先します。本契約の条件は、ライセンス文書、注文、当事者によって提出されたその他の書面との相違がある場合でも、相手方当事者によって正式に拒否されたかどうかにかかわらず、優先されます。本契約の変更は、IronPort の正式に認められた代表者が提供する書面での追記による場合を除き、禁止されます。ただし、IronPort は、お客様への通知により、IronPort プライバシー声明をその裁量においていつでも変更でき、その内容は http://www.ironport.com/privacy.html に掲載されます。本契約のいずれの条項も、権利放棄されたものと見なされません。ただし、かかる権利放棄が書面に

より IronPort または IronPort の正式に認められた代表者によって署名されたものである場合を除きます。本契約のいずれかの条項が無効とされた場合であっても、本契約の残りの部分は完全な効力を維持するものとします。両当事者は、本契約書が英語のみで書かれていることは各自が希望したものであることを認めます。

10. IronPort の連絡先情報。お客様が何らかの理由で IronPort に連絡する必要がある場合の連絡先は次のとおりです。住所：IronPort Systems, Inc., 950 Elm Avenue, San Bruno, California 94066、電話：650.989.6500、FAX：650.989.6543。

INDEX

記号

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W

X

あ

い

う

え

お

か

き

く

け

こ

さ

し

す

せ

た

ち

て

と

ね

は

ひ

ふ

へ

ほ

み

む

め

も

ゆ

り

る

れ

ろ