Cisco IronPort AsyncOS 7.5 for Email 日常管理ガイド

2011 年 8 月 23 日

Text Part Number: OL-25138-01-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 7.5 for Email 日常管理ガイド

CONTENTS

CHAPTER 1

Cisco IronPort 電子メール アプライアンスの管理

『*Cisco IronPort AsyncOS for Email 日常管理ガイド*』では、Cisco IronPort 電子メール セキュリティ アプライアンスの定期的な管理およびモニタリングの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。

この章は、次の内容で構成されています。

電子メール セキュリティ アプライアンスの関連資料

電子メール セキュリティ アプライアンスの関連資料は、次のとおりです。

- 『*Cisco IronPort AsyncOS for Email 日常管理ガイド*』。このマニュアルでは、Cisco IronPort アプライアンスの管理およびモニタリングを行うためにシステム管理者が使用する、一般的な日常業務（電子メール セキュリティ モニタを使用した電子メール トラフィックの表示、電子メール メッセージのトラッキング、システム検疫の管理、アプライアンスのトラブルシューティングなど）を実行する方法について説明します。また、電子メール セキュリティ モニタ ページ、AsyncOS ログ、CLI サポート コマンド、検疫など、システム管理者が定期的に使用する機能についての参考情報も含まれています。

- 『*Cisco IronPort AsyncOS for Email Configuration Guide*』。このマニュアルは、新しい Cisco IronPort アプライアンスを設定しており、このアプライアンスの電子メール配信機能に関する知識を必要とするシステム管理者に推奨されます。このマニュアルでは、アプライアンスを既存のネットワーク インフラストラクチャに設置し、電子メール ゲートウェイ アプライアンスとして設定する方法について説明します。電子メール パイプライン、Outbreak フィルタ、コンテンツ フィルタ、電子メールの暗号化、アンチウイルス スキャン、アンチスパム スキャンなど電子メール配信機能に関する参考情報および設定方法についても説明します。
- 『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』。このマニュアルでは、Cisco IronPort アプライアンスの高度な機能を設定する方法について説明します。LDAP を使用するためのアプライアンスの設定、電子メール ポリシーを施行するためのメッセージ フィルタの作成、複数のアプライアンスのクラスタ化、アプライアンスでのリスナーのカスタマイズなどの項目が含まれています。設定に加えて、メッセージ フィルタ ルールおよびアクション、コンテンツ ディクショナリおよびメッセージ フィルタ ルールで使用される正規表現、LDAP クエリー構文および属性などの高度な機能に関する参考資料も紹介します。
- 『*Cisco IronPort AsyncOS CLI Reference Guide*』。このマニュアルでは、AsyncOS Command Line Interface（CLI; コマンドライン インターフェイス）のコマンドの詳細なリストおよびコマンドの使用例を示します。システム管理者は、Cisco IronPort アプライアンスで CLI を使用する際の参考資料としてこのマニュアルを使用できます。

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。これらのマニュアルは、Cisco IronPort アプライアンスに同梱の Documentation CD および Cisco IronPort Customer Support Portal で入手できます。詳細については、「Cisco IronPort サポート コミュニティ」（P.1-6）を参照してください。

このマニュアルの使い方

このマニュアルは、Cisco IronPort 電子メール セキュリティ アプライアンスの定期的な管理およびモニタリングの方法を学習するための資料として使用します。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。目次および「このマニュアルの構成」（P.1-3）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。このマニュアルには、ユーザの追加、サポート コマンドの使用方法などアプライアンスの使用期間を通じ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版は、Cisco IronPort Customer Support Portal で入手できます。このマニュアルの HTML オンライン ヘルプ版には、右上隅の [Help and Support] リンクをクリックして、アプライアンス GUI から直接アクセスすることもできます。

始める前に

このマニュアルを読み始める前に、『*Cisco 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。このマニュアルでは、電子メール配信用に Cisco IronPort C シリーズ アプライアンスまたは X シリーズ アプライアンスを設定済みであることを前提としています。

Cloud Email Security ユーザ向けの注意事項

3.0.0 リリースから、Cisco IronPort には、Cisco IronPort Cloud Email Security を強化する、基礎となるテクノロジーのための新しいフォーム ファクタが導入されました。つまり、Cloud Email Security を、シスコが管理するデータセンター内の仮想アプライアンスまたはハードウェア アプライアンスで強化できるようになりました。この変更はまた、Cisco IronPort Hybrid Email Security 製品のクラウド レイヤにも適用されます。つまり、このマニュアルに記載されている「アプライアンス」、「電子メール セキュリティ アプライアンス（ESA）」、または「セキュリティ管理アプライアンス（SMA）」はすべて、物理アプライアンスまたは仮想アプライアンスを指します。使用できる機能はどちらのフォーム ファクタでも同じであるため、ユーザは、このサービスのコンシューマへのシームレスな移行を体験できます。

このマニュアルの構成

第 1 章「Cisco IronPort 電子メール アプライアンスの管理」は、Cisco IronPort アプライアンスの概要について説明し、エンタープライズ ネットワークにおける主な機能および役割を明示します。

第 2 章「電子メール セキュリティ モニタの使用方法」は、企業のすべての着信電子メール トラフィックを完全に可視化する、強力な Web ベースのコンソールであるメール フロー モニタ機能について説明します。

第 3 章「電子メール メッセージのトラッキング」は、ローカル メッセージ トラッキングについて説明します。メッセージ トラッキングを使用すると、特定のメッセージが配信されたか、ウイルスを含むことが検出されたか、スパム検疫エリアに配置されたかを確認できます。

第 4 章「検疫」では、メッセージの保留および処理に使用される専用のキューまたはリポジトリについて説明します。検疫エリア内のメッセージは、検疫の設定方法に基づいて、配信するか削除することができます。これには、IronPort スパム検疫も含まれます。

第 5 章「ロギング」では、Cisco IronPort アプライアンスのロギングおよびログ サブスクリプション機能について説明します。

第 6 章「CLI による管理およびモニタリング」では、ゲートウェイを通過するメール フローをモニタする際に使用可能な CLI のコマンドについて説明します。

第 7 章「GUI でのその他の作業」では、GUI を使用した Cisco IronPort アプライアンスの管理およびモニタリングの典型的な管理タスクについて説明します。

第 8 章「一般的な管理タスク」では、ユーザの追加、コンフィギュレーション ファイルの管理、SSH キーの管理など Cisco IronPort アプライアンスの管理およびモニタリングに使用される典型的な管理コマンドについて説明します。この章では、テクニカル サポートの依頼方法、Cisco IronPortCisco IronPort アプライアンスへのリモート アクセスを Cisco IronPort Customer Support に許可する方法、および機能キーの使用方法についても説明します。

第 9 章「テストとトラブルシューティング」では、システム パフォーマンスのテストおよび設定に関する問題のトラブルシューティングに使用される、いわゆる *ブラック ホール リスナー*を作成するプロセスについて説明します。

付録 A「Accessing the Appliance」では、ファイルをアップロードおよびダウンロードするために Cisco IronPort アプライアンスにアクセスする方法について説明します。

印刷時の表記法

書体	意味	例
AaBbCc123	コマンド、ファイル、およびディレクトリの名前、画面に表示されるコンピュータの出力。	`Please choose an IP interface for this Listener.` `sethostname` コマンドは、Cisco IronPort アプライアンスの名前を設定します。
AaBbCc123	画面に表示されるコンピュータの出力ではなく、ユーザによる入力。	`mail3.example.com>` **`commit`** `Please enter some comments describing your changes:` `[]>` **`Changed the system hostname`**
AaBbCc123	書名、新規用語、強調表示される用語、およびコマンド ライン変数。コマンド ライン変数の場合、イタリック体のテキストは、実際の名前または値のプレースホルダです。	『*Cisco IronPort Quickstart Guide*』を参照してください。 Cisco IronPort アプライアンスは、発信パケットを送信するためのインターフェイスを一意に選択できる*必要があります*。 `Before you begin, please reset your password to a new value.` `Old password:` **`ironport`** `New password:` *`your_new_password`* `Retype new password:` **`your_new_password`**

詳細情報の入手先

IronPort では、電子メール セキュリティ アプライアンスについての理解を深めて頂くために次の資料を提供しています。

Knowledge Base

Customer Support Portal の Cisco IronPort Knowledge Base には、次の URL からアクセスできます。

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

（注）　アカウントをお持ちでない場合は、[Cisco IronPort Support] ページの [Register to Log In] リンクをクリックします。通常、Knowledge Base にアクセスできるのは、シスコのカスタマー、パートナー、および社員だけです。

Knowledge Base には、Cisco IronPort 製品に関する豊富な情報が用意されています。

通常、記事は次のカテゴリのいずれかに分類されています。

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

Knowledge Base 内の各記事には、一意の回答 ID 番号がついています。

Cisco IronPort サポート コミュニティ

Cisco IronPort サポート コミュニティは、Cisco IronPort 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 Cisco IronPort 製品に関する技術情報について話し合う場を提供します。このフォーラムにトピックを投稿して質問したり、他の Cisco IronPort ユーザと情報を共有したりできます。

Customer Support Portal の Cisco IronPort サポート コミュニティには、次の URL からアクセスします。

https://supportforums.cisco.com/index.jspa

シスコのテクニカル サポート

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

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

以下を含むさまざまな作業にこの Web サイトが役立ちます。

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

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

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

http://www.cisco.com/jp/go/tac

CHAPTER 2

電子メール セキュリティ モニタの使用方法

Cisco IronPort アプライアンスの電子メール セキュリティ モニタ機能は、企業のすべての着信電子メール トラフィックを完全に可視化する、強力な Web ベースのコンソールです。

電子メール セキュリティ モニタ機能は密接にシステムに組み込まれており、評価フィルタリング、アンチスパム、アンチウイルス スキャン、Outbreak フィルタ、ポリシーの施行（コンテンツ フィルタ、データ損失防止など）、およびメッセージ配信など、電子メール配信プロセスの各ステップからデータを収集します。データベースは、IP アドレスによる各電子メール送信者の識別と記録を行いつつ、SenderBase 評価サービスと連携してリアルタイムの ID 情報を収集します。ユーザは、すべての電子メール送信者のローカル メール フロー履歴をただちに報告し、インターネット上の送信者のグローバル情報を含むプロファイルを表示できます。電子メール セキュリティ モニタ機能では、セキュリティ チームが、ユーザへのメール送信者、ユーザによって送受信されるメールの量、およびセキュリティ ポリシーの有効性の「ループを閉じる」ことができます。

この章では、次の方法について説明します。

- 発着するメッセージ フローをモニタするための電子メール セキュリティ モニタ機能へのアクセス。
- 送信者の SenderBase Reputation Score（SBRS; SenderBase 評価スコア）に対するクエリーによる、メール フロー ポリシーの決定（ホワイトリスト、ブラックリスト、およびグレーリストの更新）。ネットワーク オーナー、ドメイン、さらには個別の IP アドレスについてもクエリーを実行できます。
- メール フロー、メール ステータスおよびシステムに送受信されたメールに関する報告。

この章は、次の内容で構成されています。

電子メール セキュリティ モニタの概要

電子メール セキュリティ モニタ データベースでは、着信メールの所定の電子メール送信者について、次の重要パラメータを取得します。

- メッセージの量
- 接続履歴
- 受け入れられた接続と拒否された接続の比率
- 受け入れ率と調整上限値
- 評価フィルタの一致率
- スパムの疑いのある、および明白にスパムと識別されるアンチスパム メッセージの数
- アンチ ウイルス スキャンによって検出されたウイルス陽性メッセージの数

アンチスパム スキャンの詳細については、『*Cisco IronPort AsyncOS Configuration Guide*』の「Anti-Spam」の章を参照してください。アンチウイルス スキャンについては、『*Cisco IronPort AsyncOS Configuration Guide*』の「Anti-Virus」の章を参照してください。

電子メール セキュリティ モニタ機能は、内部ユーザ（電子メール受信者）またはメッセージの送信者を含む、特定のメッセージによってトリガーされたコンテンツ フィルタに関する情報も取得します。

電子メール セキュリティ モニタ機能は GUI だけで使用でき、電子メール トラフィックおよび Cisco IronPort アプライアンス（検疫、作業キュー、発生など）のステータスへのビューを提供します。アプライアンスは、送信者が標準のトラフィック プロファイルの範囲に該当しない場合に識別します。識別された送信者はインターフェイスで強調表示されるので、送信者を送信者グループに割り当てるか、送信者のアクセス プロファイルを変更することによって是正措置を取ることができます。または、引き続き AsyncOS のセキュリティ サービスに対応

させることができます。送信メールにも同様のモニタリング機能があり、メールキューの上位ドメインおよび受信ホストのステータスにビューを提供します（「[Delivery Status Details] ページ」（P.2-30）を参照）。

（注）　電子メール セキュリティ モニタ機能では、アプライアンスの再起動時に作業キューに存在したメッセージの情報は報告されません。

電子メール セキュリティ モニタと集中管理

このバージョンの AsyncOS では、クラスタ化された Cisco IronPort アプライアンスの電子メール セキュリティ モニタ レポートを集約できません。すべてのレポートは、マシン レベルに制限されます。つまりレポートは、グループ レベルまたはクラスタ レベルでは実行できません。個別のマシンのみで実行できます。

[Archived Reports] ページについても同様です。設定されている各マシンは、独自のアーカイブを備えています。したがって、「レポート生成」機能は、選択したマシンのみで実行されます。

[Scheduled Reports] ページは、マシン レベルに制限されません。したがって、複数のマシンで設定を共有できます。マシン レベルで実行された、個別のスケジュール設定されたレポートは、インタラクティブ レポートとまったく同様なので、クラスタ レベルでスケジュール設定されたレポートを設定する場合、クラスタ内の各マシンが独自のレポートを送信します。

[Preview This Report] ボタンは、ログインホストに対して常に実行できます。

電子メール セキュリティ モニタ ページ

電子メール セキュリティ モニタ機能は、GUI へのアクセス後に最初に表示されるページです。電子メール セキュリティ モニタ機能を表示するには、GUI にアクセスします（『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Overview」の章を参照）。[Monitor] メニューに [Overview] ページが表示されます。システム設定ウィザード（または CLI の `systemsetup` コマンド）を完了し、変更を保存した場合、アプライアンスで電子メールを受信するために少なくとも 1 つのパブリック リスナーを設定済みである必要があります。アプライアンスが電子メールを受信している場合、[Overview] ページにはデータが読み込まれます。

電子メール セキュリティ モニタ機能は、[Monitor] メニューで使用可能なすべてのページ（ただし [Quarantines] ページは除く）で構成されます。

GUI でこれらのページを使用して、Cisco IronPort アプライアンスのリスナーに接続しているドメインをモニタできます。お使いのアプライアンスの「メール フロー」のモニタ、ソート、分析、および分類を実行し、正規メールの大量送信者と「スパマー」（未承諾の商業用メールの大量送信者）またはウイルス送信者の疑いのあるユーザとを区別できます。これらのページは、システムへの着信接続のトラブルシューティングにも役立ちます（SBRS スコア、ドメインに対する直近の送信グループの一致など重要情報を含みます）。

これらのページは、アプライアンスに関連するメール、さらにゲートウェイの範囲を超えて存在するサービス（Cisco IronPort SenderBase 評価サービス、IronPort アンチスパム スキャン サービス、アンチウイルス スキャン セキュリティ サービス、コンテンツ フィルタ、および Outbreak フィルタ）に関連するメールの分類に役立ちます。

ページ右上の [Printable PDF] リンクをクリックすると、すべての電子メール セキュリティ モニタ ページを読みやすい印刷形式の PDF 版で生成できます。英語以外の言語での PDF の生成については、「レポートに関する注意事項」（P.68）を参照してください。

[Export] リンクでは、グラフおよび他のデータを Comma Separated Value（CSV; カンマ区切り値）形式にエクスポートできます。

エクスポートされた CSV データは、電子メール セキュリティ アプライアンスでの設定にかかわらず、すべてのメッセージ トラッキングおよびレポーティング データを GMT で示します。GMT 時間への変換の目的は、アプライアンスに依存せずにデータを使用したり、複数の時間帯にあるアプライアンスからのデータを参照する際にデータを使用したりできるようにするためです。

（注） ローカライズされた CSV データをエクスポートする場合、一部のブラウザでは見出しが正しく表示されないことがあります。これは、ローカライズされたテキストに対して、一部のブラウザが適切な文字セットを使用していないためです。この問題を回避するには、ファイルをディスクに保存し、[File] > [Open] を使用してファイルを開きます。ファイルを開いたら、ローカライズされたテキストを表示するための文字セットを選択します。

レポート データのエクスポートの自動化の詳細については、「CSV データの取得」（P.2-63）を参照してください。

検索と電子メール セキュリティ モニタ

電子メール セキュリティ モニタ ページの多くには、検索フォームが含まれています。次の 4 種類の項目を検索できます。

- 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
- 発信ドメインの配信ステータス

ドメイン、ネットワーク オーナー、および内部ユーザの検索では、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（たとえば、「ex」で始まる場合は「example.com」に一致します）を検索するかを選択します。

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」と入力すると、17.0.0.0 ～ 17.255.255.255 の範囲が検索されます。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 オクテットすべてを入力するだけです。IP アドレス検索は、CIDR 形式（17.16.0.0/12）もサポートしています。

すべての検索は、ページで現在選択されている時間範囲に限定されます。

[Overview] ページ

[Overview] ページには、検疫および（このページの [System Overview] セクションの）Outbreak フィルタのステータスの概要などお使いの Cisco IronPort アプライアンスのメッセージ アクティビティの概要が示されます。[Overview] ページには、グラフや、送受信メッセージの詳細なメッセージ数も表示されます。このページを使用して、ゲートウェイから出入りするすべてのメールのフローをモニタできます。送受信メールの [Summary Detail] では、クリーン、Stopped By Reputation Filtering（SBRS）、無効な受信者として停止、スパム検出、ウイルス検出、コンテンツフィルタによる停止、および「クリーン」と見なされるメッセージに分類されたメッセージの数と割合が示されます。

[Overview] ページは、Cisco IronPort アプライアンスが、着信メール（たとえば、評価フィルタリングによって阻止されたメッセージ）に関して Cisco IronPort SenderBase 評価サービスと連携する方法を強調表示します。[Overview] ページでは、次の操作を実行できます。

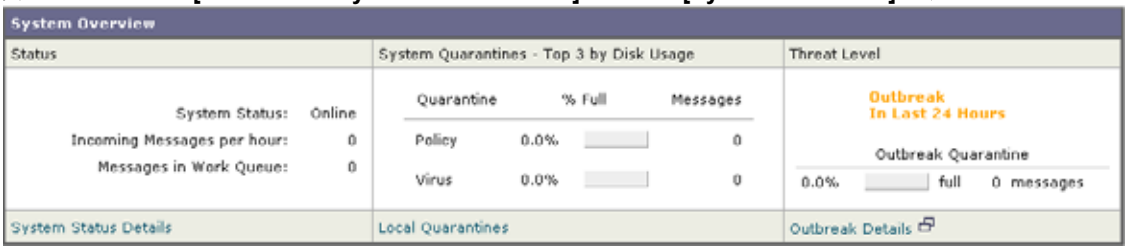
- ゲートウェイを「出入り」するすべてのメールのメール トレンド グラフを表示する。
- 試行されたメッセージ、Stopped By Reputation Filtering（SBRS）メッセージ、受信者が無効なメッセージ、スパムとしてマークされたメッセージ、ウイルス陽性としてマークされたメッセージ、およびクリーン メッセージの数を経時的に表示する。
- システム ステータスおよびローカル検疫のサマリーを表示する。
- Cisco IronPort Threat Operations Center（TOC）で入手可能な情報に基づいて、現在のウイルスの発生情報やウイルス以外の発生情報を確認する。

[Overview] ページは、[System Overview] セクションおよび送受信メールのグラフとサマリーのセクションの 2 つに分かれています。

System Overview

[Overview] ページの [System Overview] セクションは、システム ダッシュボードとして機能し、システムおよび作業キュー ステータス、検疫ステータス、発生アクティビティなどのアプライアンスに関する詳細を示します。

図 2-1　[Email Security Monitor Overview] ページの [System Overview] セクション



Status

このセクションでは、アプライアンスおよび着信メール処理の現在のステータスの概要が示されます。

[System Status]：次のいずれかの状態です。

- Online
- Resource Conservation
- Delivery Suspended
- Receiving Suspended
- Work Queue Paused
- Offline

詳細については、第 6 章「CLI による管理およびモニタリング」を参照してください。

[Incoming Messages]：1 時間あたりの着信メールの平均レート。

[Work Queue]：作業キュー内の処理待ちメッセージの数。

[System Status] ページに移動するには、[System Status Details] リンクをクリックします。

System Quarantines

このセクションには、アプライアンスでのディスク使用量別の上位 3 つの検疫に関する情報（検疫の名前、検疫の使用度（ディスク領域）、現在の検疫エリア内のメッセージ数など）が表示されます。

[Local Quarantines] ページに移動するには、[Local Quarantines] リンクをクリックします。

Virus Threat Level

このセクションには、Cisco IronPort Threat Operations Center（TOC）によって報告された発生ステータスが示されます。たとえば、図 2-1 は、直近 24 時間にウイルスの発生が確認されたことを示します。また、検疫の使用度（ディスク領域）、検疫内のメッセージ数など、Outbreak 検疫のステータスを示します。Outbreak 検疫は、アプライアンスで Outbreak フィルタ機能をイネーブルに設定した場合のみ表示されます。

（注） 脅威レベル インジケータを機能させるためには、ファイアウォールで「downloads.ironport.com」に対してポート 80 を開く必要があります。あるいは、ローカル更新サーバを指定した場合は、脅威レベル インジケータがそのアドレスを使用します。また、[Service Updates] ページを使用してダウンロード

用のプロキシを設定済みの場合、脅威レベル インジケータは、正しくアップデートされます。詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「System Administration」の章を参照してください。

外部の Cisco IronPort TOC Web サイトを閲覧するには、[Outbreak Details] リンクをクリックします。このリンクを機能させるには、お使いの Cisco IronPort アプライアンスでインターネットに接続できる必要があります。[Separate Window] アイコン（  ）は、クリックすると別個のウィンドウにリンクが開かれることを示します。これらのウィンドウを表示できるようにするには、ブラウザのポップアップ ブロッカを設定する必要があります。

送受信のサマリーとグラフ

送受信のサマリーのセクションでは、システム上のすべてのメール アクティビティのリアルタイム アクティビティへのアクセスが提供され、送受信メールのグラフとメール サマリーで構成されています。ユーザは、[Time Range] メニューを使用して報告対象となるタイムフレームを選択できます。選択したタイムフレームは、すべての電子メール セキュリティ モニタ ページで使用されます。メッセージの各タイプまたはカテゴリに関する説明は以下のとおりです（「電子メールの分類」（P.2-9）を参照）。

メール トレンド グラフ（左側、図 2-2）では、リアルタイムでの着信メールの分析結果が示されます。

メール トレンド グラフでは、メール フローが視覚的に表示されますが、サマリー テーブル（右側、図 2-2）では、同じ情報の数値的な内訳が示されます。サマリー テーブルには、各メッセージ タイプの割合と実数（試行されたメッセージ、脅威メッセージ、クリーン メッセージの総数を含む）が含まれています。

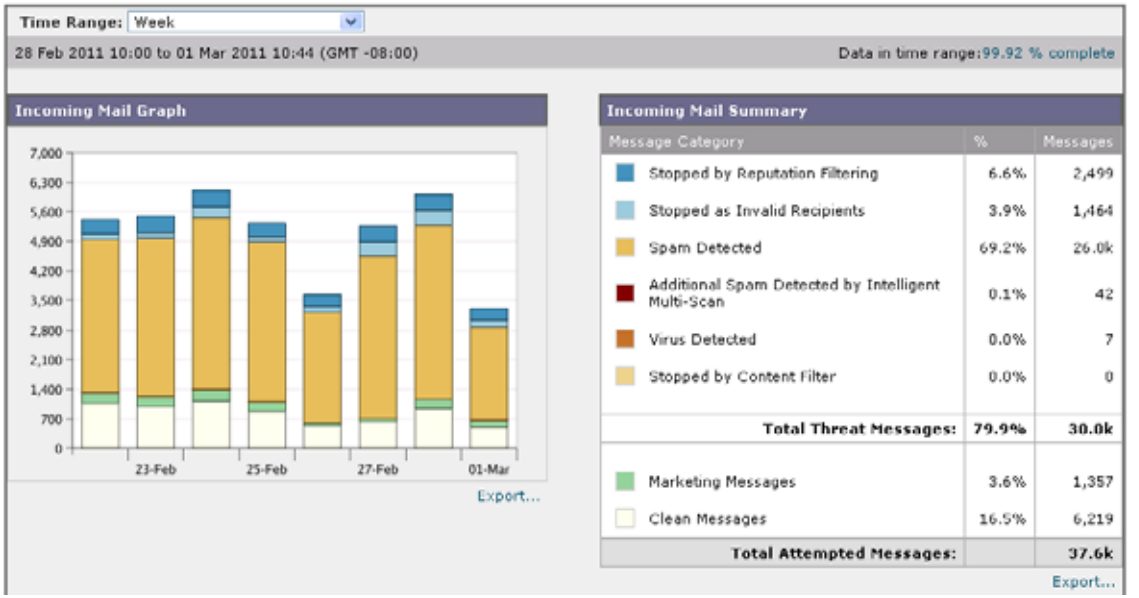
送信グラフおよびサマリーでも、送信メールに関する同様の情報が示されます。

電子メール セキュリティ モニタでのメッセージ集計に関する注意事項

電子メール セキュリティ モニタが着信メールの集計に使用する方法は、メッセージあたりの受信者の数によって異なります。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、この送信者からの 3 通として集計されます。

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。この乗数はシスコ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。

図 2-2　受信メールのグラフとサマリー テーブル



電子メールの分類

[Overview] ページおよび [Incoming Mail] ページで報告されるメッセージは、次のように分類されます。

[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（「電子メール セキュリティ モニタでのメッセージ集計に関する注意事項」（P.2-8）を参照）を乗じた値に受信調整によってブロックされたすべての受信者数を加えた値。

[Invalid Recipients]：従来の LDAP 拒否によって拒否されたすべての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、および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。

（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。

[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。

[Clean Messages]：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、ウイルス陽性またはスパム陽性としてマークされたにもかかわらず配信されたメッセージは集計されないので、実際のメッセージの配信数と、このクリーン メッセージの数は異なる可能性があります。

（注） メッセージフィルタに一致し、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ないメッセージは、クリーンとして処理されます。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。

メッセージの分類方法

メッセージは電子メール パイプラインを通過するので、複数のカテゴリに該当する場合があります。たとえば、スパム陽性またはウイルス陽性とマークされたメッセージが、コンテンツ フィルタにも一致することがあります これらの優先ルールに続いて、Outbreak フィルタによる検疫（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）の次にスパム陽性、ウイルス陽性、および一致するコンテンツ フィルタなどさまざまな判定が行われます。

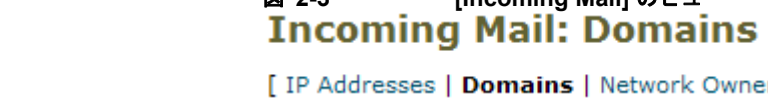
たとえば、メッセージがスパム陽性とマークされると、アンチスパム設定がスパム陽性のメッセージをドロップするように設定されている場合には、このメッセージがドロップされ、スパム カウンタが増分します。さらに、スパム陽性のメッセージを引き続きパイプラインで処理し、以降のコンテンツ フィルタがこのメッセージをドロップ、バウンス、または検疫するようにアンチスパム設定が設定されている場合にも、スパム カウンタは増分します。メッセージがスパム陽性またはウイルス陽性ではない場合、コンテンツ フィルタ カウントが増分するだけです。

[Incoming Mail] ページ

[Incoming Mail] ページでは、お使いのアプライアンスに接続するすべてのリモート ホストの電子メール セキュリティ モニタ機能によって収集されたリアルタイム情報に関して報告を行うメカニズムが提供されます。これにより、メール送信者の IP アドレス、ドメイン、および組織（ネットワーク オーナー）に関する詳細を収集できます。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できます。

[Incoming Mail] ページには、[Domain]、[IP Address]、および [Network Owner] の 3 種類のビューが用意されており、システムに接続するリモート ホストのスナップショットが選択したビューで提供されます。

図 2-3　[Incoming Mail] のビュー



アプライアンスで設定済みのすべてのパブリック リスナーにメールを送信した上位ドメイン（ビューに応じて、IP アドレスまたはネットワーク オーナー）の表（[Incoming Mail Details]）が表示されます。ゲートウェイに入ったすべてのメールのフローをモニタできます。任意のドメイン/IP/ネットワーク オーナーをクリックしてドリルダウンし、送信者プロファイル ページ（クリックしたドメイン/IP/ネットワーク オーナーに固有の [Incoming Mail] ページ）のこの送信者に関する詳細にアクセスできます。

[Incoming Mail] は、一連のページ（[Incoming Mail]、送信者プロファイル、および送信者グループ レポート）を含むように拡張することもできます。
[Incoming Mail] ページでは、次の操作を実行できます。

- メール送信者の IP アドレス、ドメイン、または組織（ネットワーク オーナー）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 アクションによる接続を確認する。詳細については、「送信者グループ レポート」（P.2-25）を参照してください。
- 試行されたものの、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など、メール送信者に関する詳細な統計情報を確認する。
- 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ドリルダウンと分析を行い、送信者に関する詳細を取得する。
- 特定の送信者をドリルダウンして、送信者の 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 Cisco 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をドリルダウンする。
- ドメインに関する情報を収集したら、（必要に応じて）ドメイン、IP アドレス、またはネットワーク オーナーのプロファイル ページから [Add to Sender Group] をクリックして、既存の送信者グループに IP アドレス、ドメイン、または組織を追加できます。『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Configuring the Gateway to Receive Email」の章を参照してください。

Incoming Mail

[Incoming Mail] ページでは、システムで設定済みのすべてのパブリック リスナーのリアルタイム アクティビティへのアクセスが提供され、受信数の上位ドメイン（脅威メッセージの総数別およびクリーン メッセージの総数別）および [Incoming Mail Details] リストという 2 つのセクションで構成されます。

図 2-4　着信メールのグラフ：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

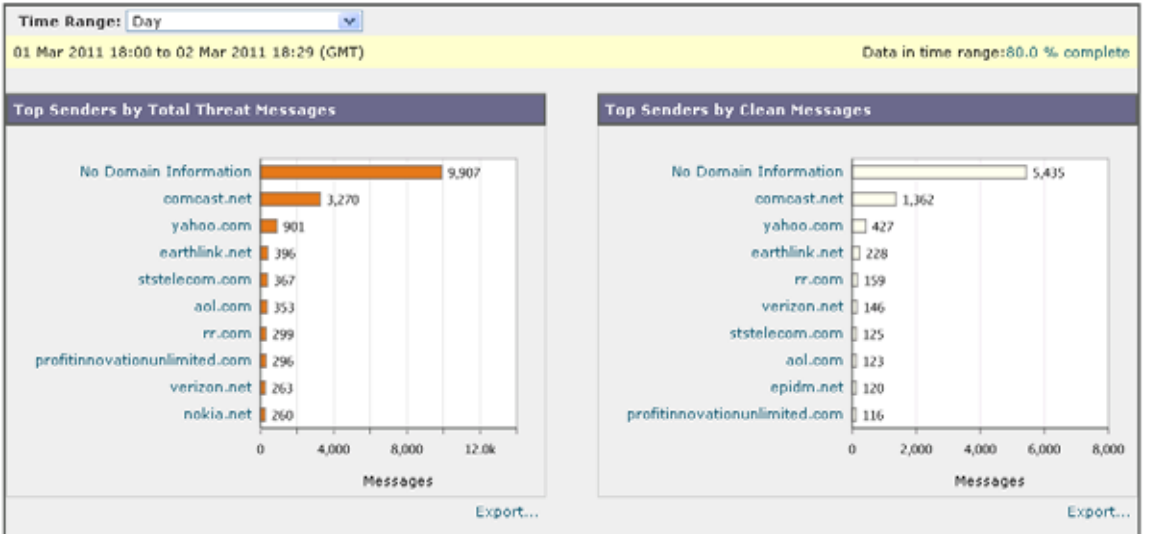


図 2-5　Incoming Mail Details

Incoming Mail Details

Items Displayed 10

Sender Domain	Total Attempted	Stopped by Reputation Filtering	Stopped as Invalid Recipients	Spam Detected	Virus Detected	Stopped by Content Filter	Total Threat	Marketing	Clean
No Domain Information	15.7k	2,415	0	6,881	196	415	9,907	344	5,435
comcast.net	4,715	687	0	2,217	162	204	3,270	83	1,362
yahoo.com	1,367	222	0	606	18	55	901	39	427
earthlink.net	636	81	0	289	0	26	396	12	228
rr.com	466	78	0	199	0	22	299	8	159
verizon.net	416	60	0	168	28	7	263	7	146
ststelecom.com	498	60	0	221	67	19	367	6	125
aol.com	486	66	0	238	12	37	353	10	123
epidm.net	355	48	0	137	20	23	228	7	120
profitinnovationunlimited.com	428	42	0	254	0	0	296	16	116

Columns... | Export...

[Incoming Mail Details] リストに含まれるデータの説明については、「[Incoming Mail Details] リスト」（P.2-14）を参照してください。

メール トレンド グラフにおける時間範囲に関する注意事項

電子メール セキュリティ モニタ機能は、ゲートウェイに流入するメールに関するデータを常に記録します。データは 60 秒ごとに更新されますが、システムに表示されるデータは、現在のシステム時間よりも 120 秒遅れます。表示される結果に含める時間範囲を指定できます。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。

表 2-1 の時間範囲オプションから選択します。

表 2-1　電子メール セキュリティ モニタ機能で使用可能な時間範囲

GUI で選択した時間範囲	定義
Hour	直近の 60 分 + 最大 5 分
Day	直近の 24 時間と直近の 60 分
Week	直近の 7 日 + 当日の経過した時間
30 days	直近の 30 日 + 当日の経過した時間
90 days	直近の 90 日 + 当日の経過した時間
Yesterday	00:00 ～ 23:59（午前 0 時～午後 11:59）
Previous Calendar Month	その月の最初の日の 00:00 ～その月の最後の日の 23:59
Custom Range	指定した開始の日付と時間および終了の日付と時間で囲まれた範囲

集中化レポーティングをイネーブルにしていると、表示される時間範囲オプションが異なります。詳細については、『*Cisco IronPort AsyncOS for Email Security Configuration Guide*』の「Cisco IronPort M-Series Security Management Appliance」の章にある集中化レポーティング モードに関する情報を参照してください。

[Incoming Mail Details] リスト

アプライアンスのパブリック リスナーに接続した上位送信者が、[Incoming Mail] ページの下部にある受信された外部ドメイン リストの表に選択したビューで表示されます。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。各種のカテゴリの説明については、「電子メールの分類」（P.2-9）を参照してください。

*ダブル DNS ルックアップ*の実行によって、リモート ホストの IP アドレス（つまり、ドメイン）が取得され、有効性が検証されます。ダブル DNS ルックアップおよび送信者の検証の詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Configuring the Gateway to Receive Email」の章を参照してください。

送信者の詳細のリストには、[Summary] と [All] の 2 つのビューがあります。

デフォルトの [Sender Detail] ビューでは、各送信者が試行したメッセージの総数が示され、カテゴリ別の内訳が含まれます。カテゴリは、[Overview] ページの [Incoming Mail Summary] グラフと同じ（クリーン メッセージ、評価フィルタリングによる阻止、無効な受信者、スパムを検出、コンテンツ フィルタによる阻止の数）です。また、脅威メッセージ（評価によって阻止されたメッセージや、無効な受信者、スパム、およびウイルスとして阻止されたメッセージ）の総数も示されます。

[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）

- 接続あたりのメッセージ数に使用される、保守的に見積もった乗数

アプライアンスに重い負荷がかけられている場合、拒否された接続の正確な数を送信者別に維持できません。その代わりに、拒否された接続の数は、各時間間隔で最も顕著だった送信者についてのみ維持されます。この場合、表示される値は「下限」、つまり少なくともこの数のメッセージが阻止されたと解釈できます。

（注） [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が、負荷のために常に限定的です。

表示できる追加のカラムは次のとおりです。

[Connections Rejected]：HAT ポリシーによってブロックされたすべての接続。アプライアンスに重い負荷がかけられている場合、拒否された接続の正確な数を送信者別に維持できません。その代わりに、拒否された接続の数は、各時間間隔で最も顕著だった送信者についてのみ維持されます。

[Connections Accepted]：受け入れられたすべての接続。

[Stopped by Recipient Throttling] : [Stopped by Reputation Filtering] のコンポーネントです。HAT 上限値（1 時間当たりの最大受信者数、メッセージあたりの最大受信者数、または接続あたりの最大メッセージ数）のいずれかを超えたために、阻止された受信メッセージの数を表します。この値と、拒否されたか、TCP 拒否の接続に関連する受信メッセージの予測値とが合計されて、[Stopped by Reputation Filtering] が算出されます。

テーブルの下部にある [Column] リンクをクリックすると、カラムの表示/非表示が切り替わります。

このリストは、カラム見出しリンクをクリックするとソートされます。カラム見出しの横にある小さな三角形は、データの現在のソートに使用されているカラムを示します。

[Total Threat] :（評価により阻止された、無効な受信者、スパム、およびウイルスとして阻止された）脅威メッセージの総数

「No Domain Information」

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。『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Configuring the Gateway to Receive Email」の章を参照してください。

リストに表示される送信者の数は、[Items Displayed] メニューから選択できます。

詳細の問い合わせ

電子メール セキュリティ モニタのテーブルに表示された送信者については、その送信者（または [No Domain Information] リンク）をクリックして特定の送信者に関する詳細をドリルダウンします。結果は送信者プロファイル ページに表示され、Cisco 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ドリルダウンできます（「データが読み込まれる報告ページ：送信者プロファイル ページ」（P.2-17）を参照）。

[Incoming Mail] ページの下部にある [Sender Groups Report] リンクをクリックして、別のレポート（送信者グループ レポート）を表示することもできます。送信者グループ レポートの詳細については、「送信者グループ レポート」（P.2-25）を参照してください。

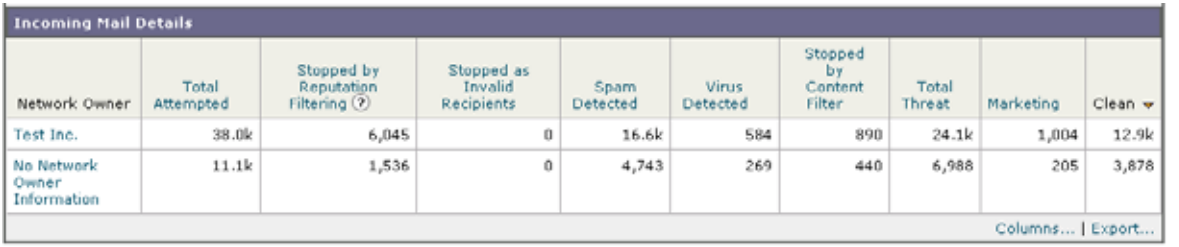
データが読み込まれる報告ページ：送信者プロファイル ページ

[Incoming Mail] ページにある [Incoming Mail Details] テーブルをクリックすると、その結果として*送信者プロファイル ページ*が表示されます。このページには、特定の IP アドレス、ドメイン、または組織（ネットワーク オーナー）のデータが含まれています。送信者プロファイル ページには、送信者の詳細情報が示されます。任意のネットワーク オーナーまたは IP アドレスの送信者プロファイル ページは、[Incoming Mail] ページまたは他の送信者プロファイル ページで特定の項目をクリックしてアクセスできます。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あり、ドメインは、IP アドレスを含むエンティティです。この関係および SenderBase 評価サービスとの関係の詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Configuring the Gateway to Receive Email」の章を参照してください。

IP アドレス、ネットワーク オーナーおよびドメイン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、こ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。グラフの下には、この送信者に関連するドメインまたは IP アドレスを表示する表（個々の IP アドレスの送信者プロファイル ページには、詳細なリストは含まれません）、および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があります。

- 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 2-6　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...

各送信者プロファイル 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。地震の測定に使用されるリヒター スケールと同様に、SenderBase マグニチュードは、10 を基数とする対数目盛を使用して算出されるメッセージの量の基準です。目盛の最大理論値は 10 に設定されます。これは、世界の電子メール メッセージの量（約 100 億メッセージ/日）に相当します。対数目盛を使用した場合、1 ポイントのマグニチュードの増加は、実際の量の 10 倍の増加に相当します。

  月単位マグニチュードは、直近 30 日間に送信された電子メールの量に基づいて割合が算出される点を除いて、日単位マグニチュードと同じ方法を使用して算出されます。
  - 平均マグニチュード（IP アドレスのみ）
  - 総累積量/30 日の量（IP アドレス プロファイル ページのみ）
  - Bonded Sender ステータス（IP アドレス プロファイル ページのみ）
  - SenderBase 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 プロファイル ページおよびドメイン プロファイル ページのみ）
  - このネットワーク オーナーに関連するドメインの数（ネットワーク オーナー プロファイル ページおよびドメイン プロファイル ページのみ）
  - このネットワーク オーナーの IP アドレスの数（ネットワーク オーナー プロファイル ページおよびドメイン プロファイル ページのみ）
  - 電子メールの送信に使用された IP アドレスの数（ネットワーク オーナー ページのみ）

  SenderBase 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] リンクをクリックします。

- **メール フロー統計**情報。送信者について収集された、指定した時間範囲にわたる電子メール セキュリティ モニタ情報を含みます。
- 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 アドレスをドリルダウンするか、ドリルアップして組織プロファイル ページを表示できます。また、そのテーブルの下部にある [Columns] リンクをクリックすることにより、[IP Addresses] テーブル内の送信者アドレスごとの [DNS Verified] ステータス、SBRS（SenderBase 評価スコア）、および [Last Sender Group] を表示することもできます。そのテーブル内の任意のカラムを非表示にすることもできます。

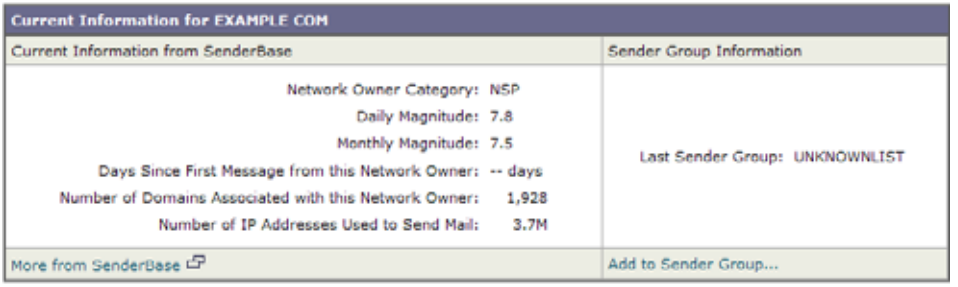
ネットワーク オーナー プロファイル ページから、そのテーブルの下部にある [Columns] リンクをクリックすることにより、[Domains] テーブル内のドメインごとの [Connections Rejected]、[Connections Accepted]、および [Stopped by Recipient Throttling] 情報を表示できます。そのテーブル内の任意のカラムを非表示にすることもできます。

システムの管理者の場合は、これらの各ページで（必要に応じて）エンティティのチェックボックスをクリックしてから [Add to Sender Group] をクリックし、送信者グループにネットワーク オーナー、ドメイン、または IP アドレスを追加することもできます。

また、送信者の現在の情報テーブルの送信者グループ情報の下にある [Add to Sender Group] リンクをクリックして、送信者グループに送信者を追加することもできます。送信者グループへの送信者の追加の詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Configuring the Gateway

to Receive Email」の章を参照してください。当然ながら、必ずしも変更を行う必要はありません。セキュリティ サービスに着信メールを処理させることもできます。

図 2-7　ネットワーク オーナーの現在の情報



送信者プロファイルの検索

特定の送信者を検索するには、[Quick Search] ボックスに IP アドレス、ドメイン、または組織名を入力します。

送信者プロファイル ページが送信者の情報と共に表示されます。「データが読み込まれる報告ページ：送信者プロファイル ページ」（P.2-17）を参照してください。

図 2-8　ドメイン プロファイル ページ（1/2）

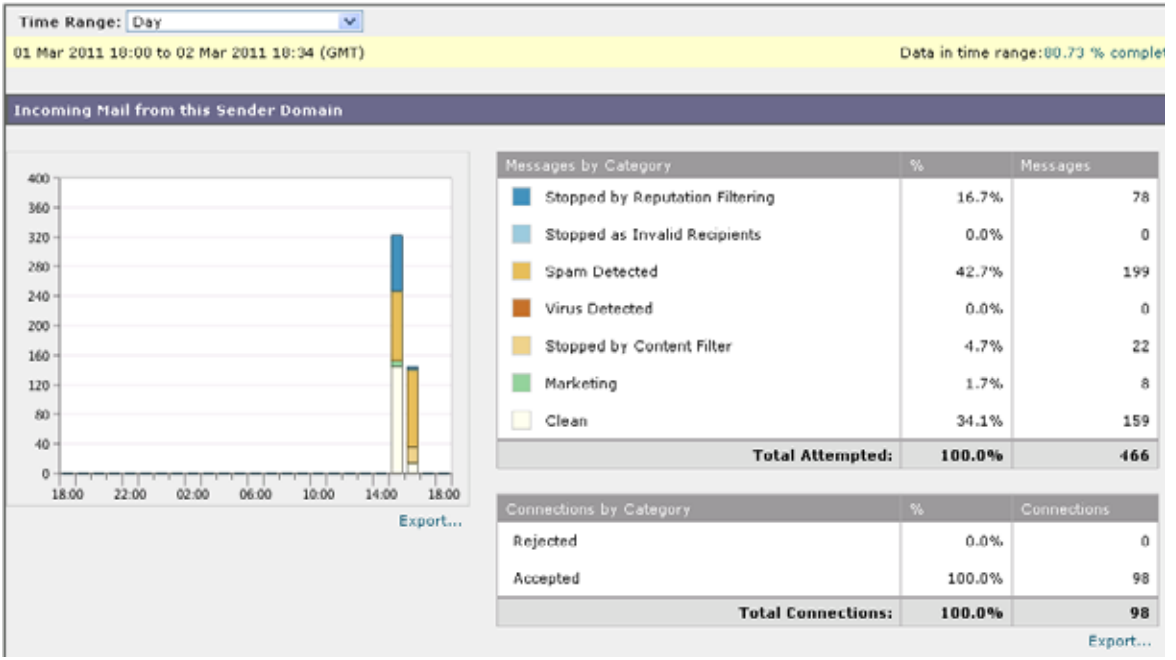


図 2-9　ドメイン プロファイル ページ（2/2）

IP Addresses

Items Displayed 10

Sender IP Address	Hostname	Total Attempted	Stopped by Reputation Filtering	Stopped as Invalid Recipients	Spam Detected	Virus Detected	Stopped by Content Filter	Total Threat	Marketing	Clean
24.29.109.6	...tp-02.rdc-nyc.rr.com	26	6	0	2	0	0	8	1	17
24.93.47.42	ms-smtp-03.texas.rr.com	26	6	0	6	0	0	12	0	14
65.32.5.134	...p-04.tampabay.rr.com	117	3	0	79	0	21	103	0	14
24.24.2.58	ms-smtp-04.nyroc.rr.com	13	3	0	1	0	0	4	0	9
24.93.40.211	austtx-mx-04.mgw.rr.com	13	3	0	1	0	0	4	0	9
65.32.5.135	...p-05.tampabay.rr.com	26	6	0	11	0	0	17	0	9
66.75.162.134	ms-smtp-02.socal.rr.com	13	3	0	2	0	0	5	0	8
24.24.2.57	ms-smtp-03.nyroc.rr.com	13	3	0	2	0	0	5	1	7
65.24.0.113	...0-113.ohiordc.rr.com	13	3	0	3	0	0	6	0	7
69.205.138.18	...8-18.stny.res.rr.com	13	3	0	2	0	0	5	1	7

Columns... | Export...

図 2-10　ネットワーク オーナー プロファイル ページ（1/2）

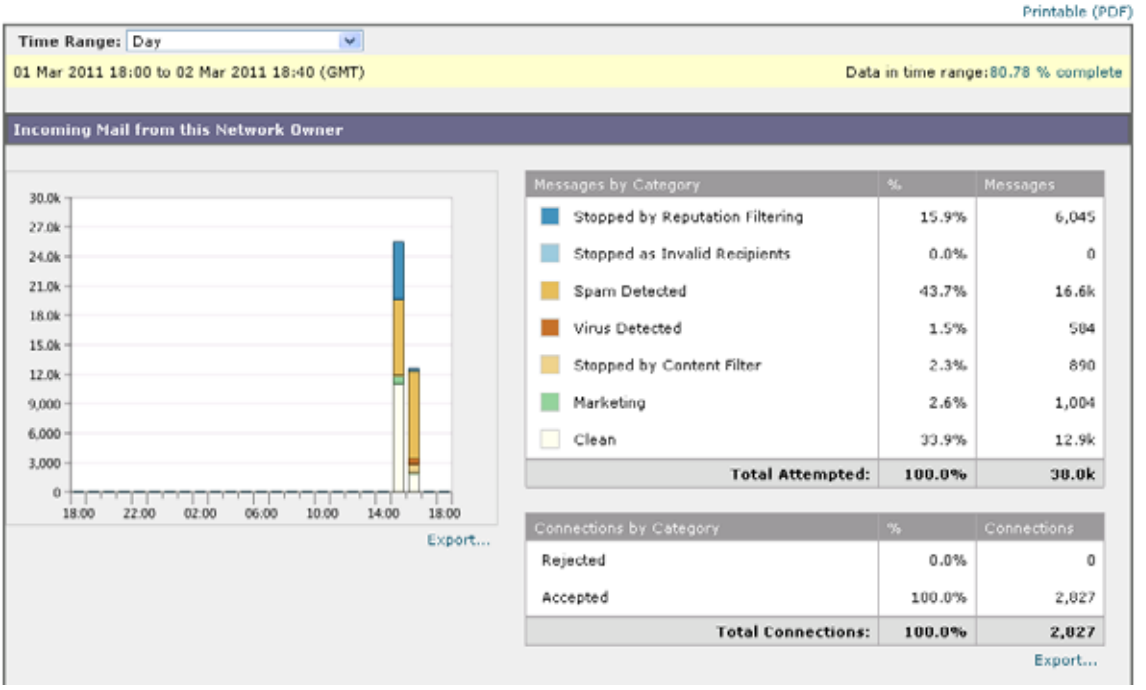


図 2-11　ネットワーク オーナー プロファイル ページ（2/2）

Domains

Sender Domain	Total Attempted	Stopped by Reputation Filtering	Stopped as Invalid Recipients	Spam Detected	Virus Detected	Stopped by Content Filter	Total Threat
No Domain Information	12.5k	2,001	0	5,574	152	310	7,727
comcast.net	4,361	684	0	2,175	113	140	2,972
yahoo.com	1,094	186	0	522	0	51	708
earthlink.net	604	81	0	284	0	25	365
rr.com	441	78	0	196	0	21	274
verizon.net	402	60	0	163	28	7	251
ststelecom.com	470	60	0	213	67	19	340
aol.com	441	66	0	231	12	36	309
pacificrack.com	335	57	0	157	0	21	214
profitinnovationunlimited.com	421	42	0	253	0	0	295

図 2-12　IP アドレス プロファイル ページ（1/2）

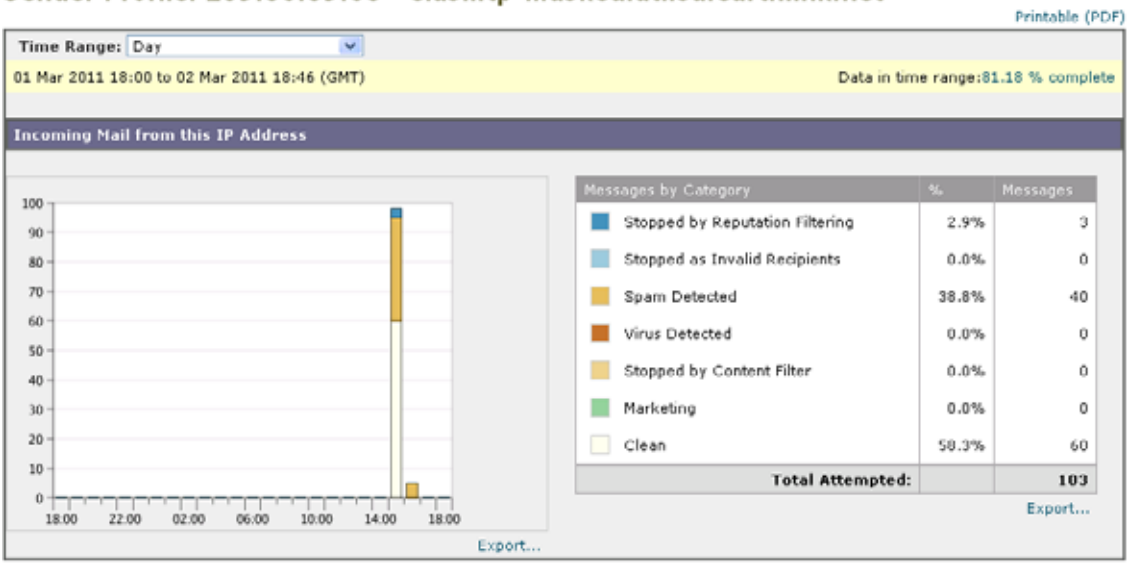
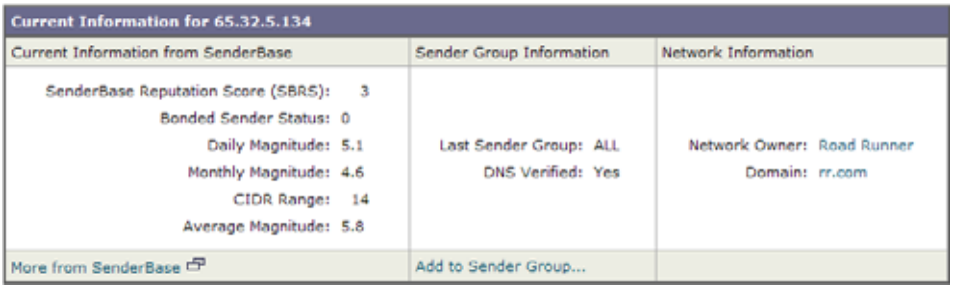


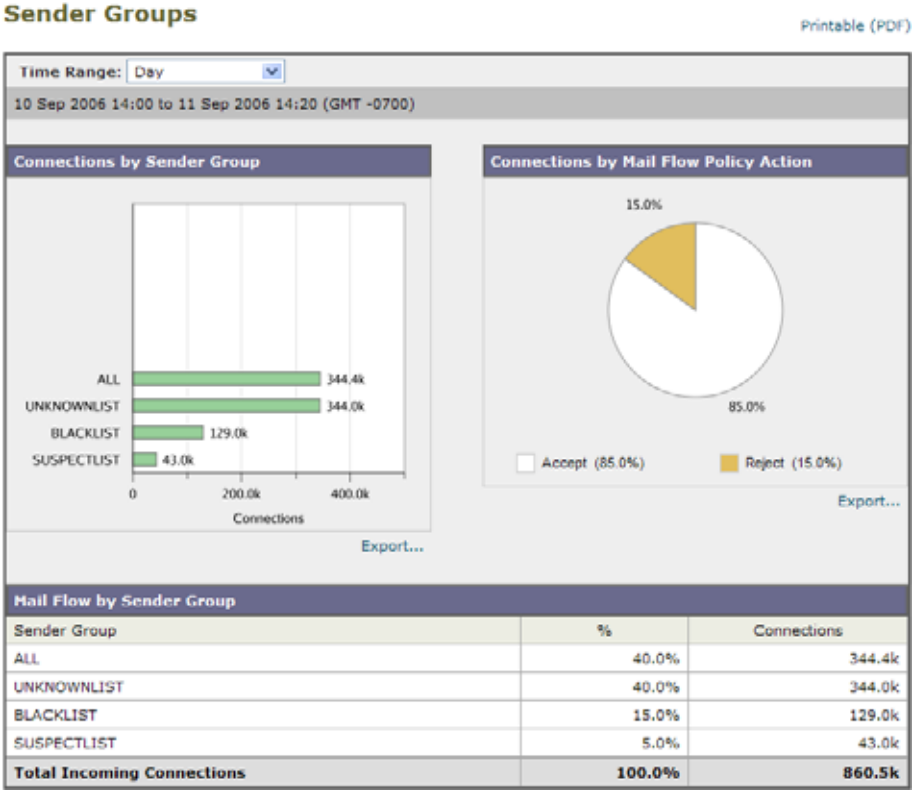
図 2-13　IP アドレス プロファイル ページ（2/2）



送信者グループ レポート

送信者グループ レポートは、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 Configuration Guide*』の「Configuring the Gateway to Receive Email」の章を参照してください。

図 2-14　送信者グループ レポート ページ



Outgoing Destinations

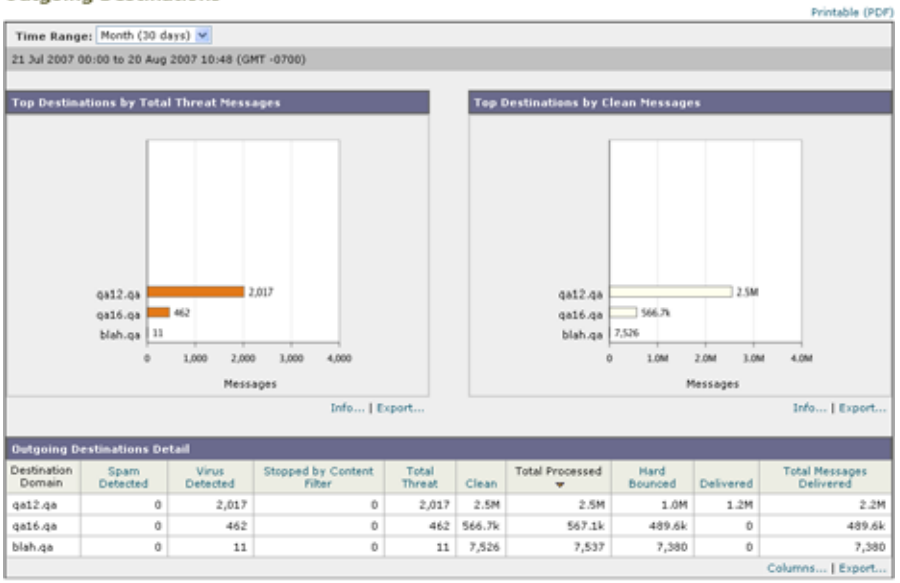
[Outgoing Destinations] ページには、メールの送信先ドメインに関する情報が示されます。このページは、2 つのセクションで構成されます。ページの上部は、発信脅威メッセージ別の上位宛先および発信クリーン メッセージの上位宛先を示すグラフで構成されます。ページの下部には、総受信者数別にソートされた（デフォルト設定）全カラムを示す表が表示されます。

レポート対象の時間範囲（時間や週など）、またはカスタムの範囲を選択できます。グラフまたは詳細リストのデータは、すべてのレポートと同様に [Export] リンクを使用して CSV 形式にエクスポートできます。

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

- Cisco IronPort アプライアンスのメール送信先
- 各ドメインに送信されるメールの量
- クリーン、スパム陽性、またはコンテンツ フィルタによる阻止のメールの割合
- 配信されたメッセージおよび宛先サーバによってハードバウンスされたメッセージの数

図 2-15　[Outgoing Destinations] ページ



Outgoing Senders

[Outgoing Senders] ページでは、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るメールの量および種類に関する情報が示されます。このページを表示すると、ドメイン別または IP アドレス別に結果を表示できます。各ドメインによって送信されたメールの量を確認する場合にはドメイン別の結果、最も多いウイルス メッセージを送信している、または最も多くコンテンツ フィルタをトリガーしている IP アドレスを表示する場合には IP アドレス別の結果を表示することが推奨されます。

このページは、2 つのセクションで構成されます。ページの左側は、総脅威メッセージ別の上位送信者を示すグラフです。総脅威メッセージには、スパムもしくはウイルス陽性のメッセージ、またはコンテンツ フィルタをトリガーしたメッセージが含まれます。ページの上部の右側は、クリーン メッセージ別の上位送信者を表示するグラフです。ページの下部には、総メッセージ数別にソートされた（デフォルト設定）全カラムを示す表が表示されます。

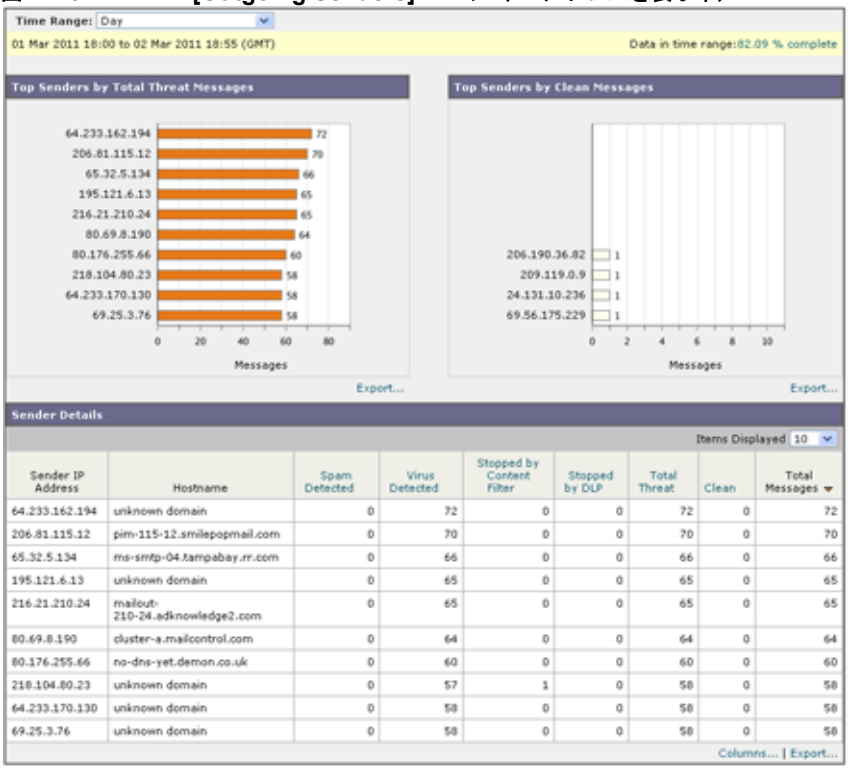
（注）　このページには、メッセージ配信に関する情報は表示されません。特定のドメインからのバウンスされたメッセージの数などの配信情報は、[Delivery Status] ページを使用して追跡できます。

レポート対象の時間範囲（時間や週など）、またはカスタムの範囲を選択できます。グラフまたは詳細リストのデータは、すべてのレポートと同様に [Export] リンクを使用して CSV 形式にエクスポートできます。

[Outgoing Senders] ページを使用すると、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

図 2-16　[Outgoing Senders] ページ（IP アドレスを表示中）



[Delivery Status] ページ

特定の受信者ドメインに対する配信の問題を疑ったり、仮想ゲートウェイ アドレスに関する情報収集を行ったりする場合には、[Monitor] > [Delivery Status Page] をクリックすると、特定の受信者ドメインに関連する電子メール操作に関するモニタリング情報が提供されます。

[Delivery Status] ページには、CLI で `tophosts` コマンドを使用した場合と同じ情報が表示されます（詳細については、第 6 章「CLI による管理およびモニタリング」の「電子メール キューの構成の確認」を参照してください）。

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。

- 特定のドメインを検索するには、[Domain Name:] フィールドにドメイン名を入力し、[Search] をクリックします。
- 表示されているドメインをドリルダウンするには、ドメイン名のリンクをクリックします。

[Delivery Status Details] ページに結果が表示されます。

（注）　受信者ドメインで任意のアクティビティが発生すると、このドメインが「アクティブ」となり、[Overview] ページに表示されます。たとえば、配信の問題があるためにメールが発信キューにとどまると、この受信者ドメインは、引き続き発信メールの概要に表示されます。

配信の再試行

後で配信されるようにスケジュール設定されているメッセージは、[Retry All Delivery] をクリックすると、ただちに再試行できます。[Retry All Delivery] では、キューに含まれるメッセージがただちに配信されるようにスケジュールを変更できます。「ダウン」としてマークされたすべてのドメインおよびスケジュール設定されているか、ソフト バウンスされたメッセージは、ただちに配信されるためにキューに入れられます。

特定の宛先ドメインに向けての配信を再施行するには、ドメイン名のリンクをクリックします。[Delivery Status Details] ページで、[Retry Delivery] をクリックします。

CLI で `delivernow` コマンドを使用して、ただちに配送するようにメッセージのスケジュールを変更することもできます。詳細については、「電子メールの即時配信スケジュール」（P.6-47）を参照してください。

[Delivery Status Details] ページ

特定の受信者ドメインに関する統計情報を検索するには、[Delivery Status Details] ページを使用します。このページには、CLI 内で `hoststatus` コマンドを使用した場合と同じ情報（メール ステータス、カウンタ、およびゲージ）が

表示されます（詳細については、第 6 章「CLI による管理およびモニタリング」の「メール ホストのステータスのモニタリング」を参照してください）。特定のドメインを検索するには、[Domain Name:] フィールドにドメイン名を入力し、[Search] をクリックします。`altsrchost` 機能を使用している場合、仮想ゲートウェイのアドレス情報が表示されます。

図 2-17　[Delivery Status] ページ

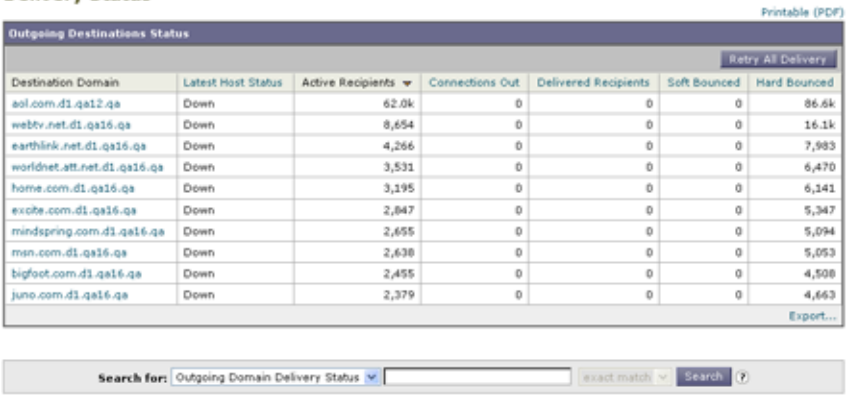
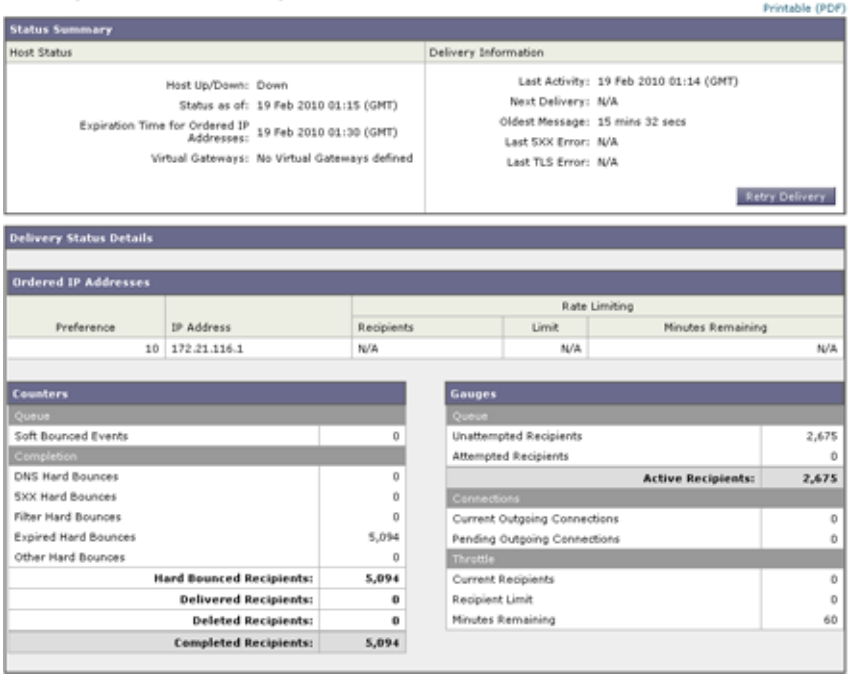


図 2-18　[Delivery Status Details] ページ



[Internal Users] ページ

[Internal Users] ページでは、内部ユーザによって送受信されたメールに関する情報が、*電子メール アドレスごとに表示されます*（単一ユーザの複数の電子メール アドレスが、リストに表示される場合があります。レポートでは、電子メール アドレスはまとめられません）。

このページは、クリーン着信メッセージ別およびクリーン発信メッセージ別の上位ユーザを示すグラフとユーザ メール フローの詳細の 2 つのセクションで構成されます。レポート対象の時間範囲（時間、日、週、または月）を選択できます。グラフまたは詳細リストのデータは、すべてのレポートと同様に [Export] リンクを使用して CSV 形式にエクスポートできます。

[User Mail Flow Details] リストでは、送受信メールが電子メール アドレスごとに [Clean]、[Spam Detected]（着信のみ）、[Virus Detected]、および [Content Filter Matches] に分類されます。このリストは、カラム見出しをクリックしてソートできます。

内部ユーザ レポートを使用すると、次の情報を入手できます。

- 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
- コンテンツ フィルタをトリガーしたユーザとそのコンテンツ フィルタの種類
- 電子メールをコンテンツ フィルタで捕捉されたユーザ

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。

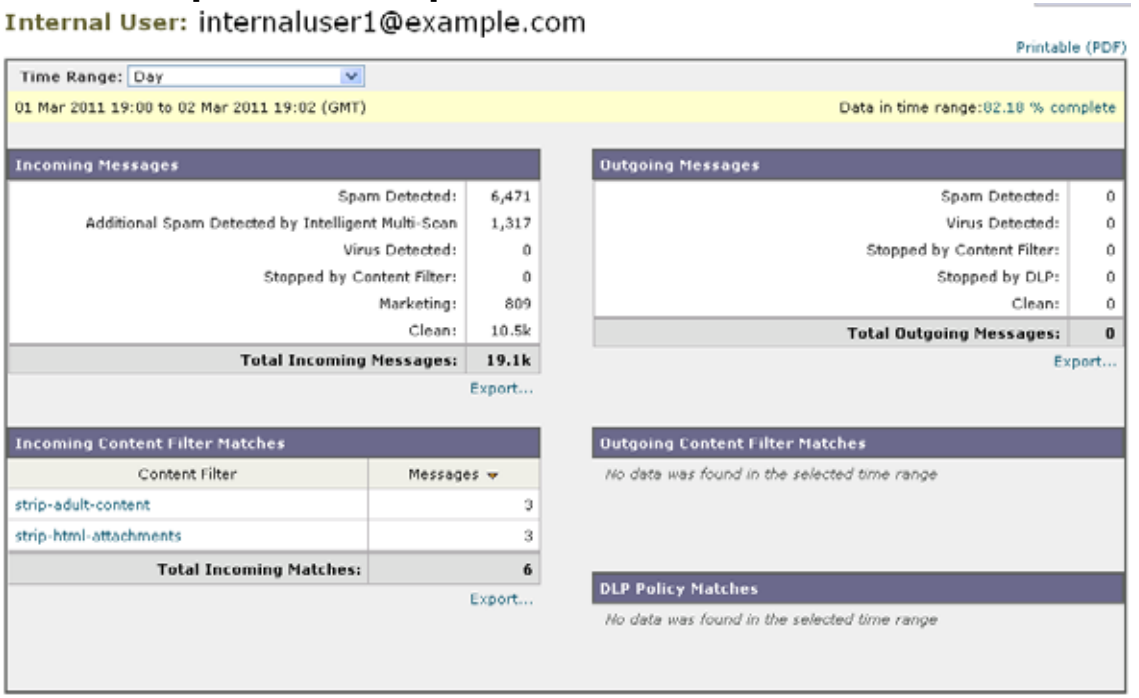
一部の送信メール（バウンスなど）の送信者は、null です。これらの送信者は、送信および「不明」に集計されます。

内部ユーザの [Internal User Details] ページを表示するには、この内部ユーザをクリックします。

[Internal User Details]

[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送受信メッセージの内訳など指定した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 フィルタおよび DLP ポリシーの一致も示されます。

図 2-19　[Internal User Details] ページ

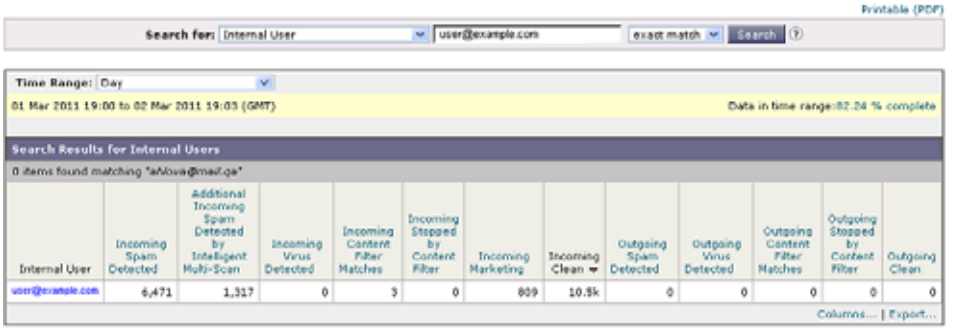


コンテンツ フィルタの詳細情報を対応するコンテンツ フィルタ情報ページに表示するには、そのコンテンツ フィルタ名をクリックします（「[Content Filters] ページ」（P.2-39）を参照）。この方法を使用すると、特定のコンテンツ フィルタに一致したメールを送受信したユーザのリストも取得できます。

特定の内部ユーザの検索

特定の内部ユーザ（電子メール アドレス）は、[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から検索できます。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.com」が一致します）を選択します。

図 2-20　内部ユーザ検索の結果



[DLP Incidents] ページ

[DLP Incidents] 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 インシデント 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 Incidents] ページは、次の 2 つの主なセクションで構成されます。

- 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 Incidents Details] リスト

レポート対象の時間範囲（時間や週など）、またはカスタムの範囲を選択できます。グラフまたは詳細リストのデータは、すべてのレポートと同様に [Export] リンクを使用して CSV 形式にエクスポートするか、[Printable (PDF)] リンクを使用して PDF 形式にエクスポートできます。英語以外の言語での PDF の生成については、「レポートに関する注意事項」（P.68）を参照してください。

図 2-21　DLP インシデント グラフ : [Top Incidents by Severity]、[Incident Summary]、および [Top DLP Policy Matches]

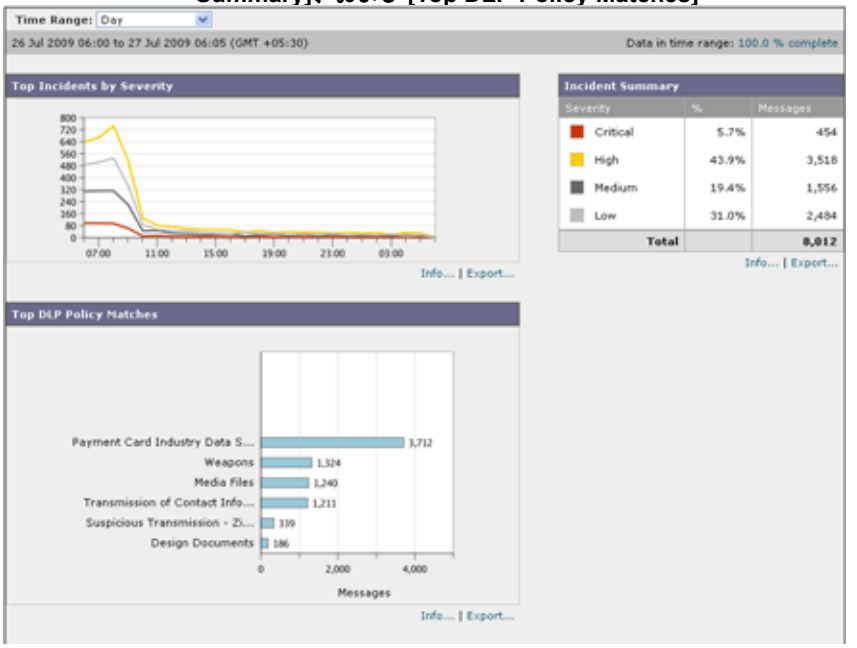


図 2-22　DLP Incident Details

DLP Incident Details

DLP Policy	Low	Medium	High	Critical	Total	Delivered (encrypted)	Delivered (clear)	Dropped
Payment Card Industry Data Security Standard (PCI-DSS)	1,391	906	961	454	3,712	0	0	0
Weapons	902	422	0	0	1,324	0	0	0
Media Files	0	0	1,240	0	1,240	0	0	0
Transmission of Contact Information	191	228	792	0	1,211	0	0	0
Suspicious Transmission - Zip Files	0	0	339	0	339	0	339	0
Design Documents	0	0	186	0	186	0	0	0

Columns... | Export...

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

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の DLP ポリシーは、[DLP Incidents] ページの下部にある [DLP Incidents Details] テーブルに表示されます。詳細情報を表示するには、DLP ポリシーの名前をクリックします。

[DLP Incidents 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、クリアに配信されたメッセージの数、暗号化されて配信されたメッセージの数、ドロップされたメッセージの数が示されます。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。

[DLP Policy Detail] ページ

[DLP Incidents 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] リストも含まれます。このリストには、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] リストを使用すると、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。

図 2-23　DLP ポリシーの詳細グラフ：[Top Incidents by Severity]、[Incident Summary]

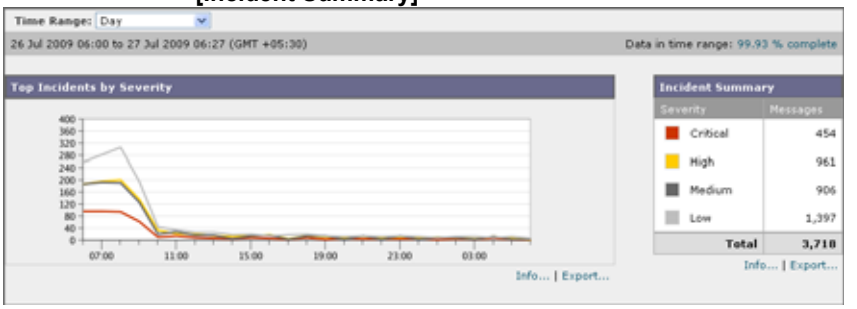


図 2-24　DLP Policy Incidents by Sender

Incidents by Sender

Items Displayed 10

Sender	Low	Medium	High	Critical	Total	Delivered (encrypted)	Delivered (clear)	Dropped
user@test.com	698	453	480	227	1,858	0	0	0
testuserTP1@test.com	171	0	0	57	228	0	0	0
testuseridentities@test.com	114	0	0	0	114	0	0	0
testusertencc@test.com	0	112	0	0	112	0	0	0
testuser200cc@test.com	0	0	0	57	57	0	0	0
testuser25cc@test.com	0	0	57	0	57	0	0	0
testusercontact_IPaddr_visa@test.com	0	0	57	0	57	0	0	0
testusercontact_visa@test.com	0	0	57	0	57	0	0	0
testuserCreditcard__sev_high@test.com	0	0	57	0	57	0	0	0
testuserCritical_violation_DL@test.com	0	57	0	0	57	0	0	0

Columns... | Export...

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.2-33）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 2 種類の形式（棒グラフとリスト）で表示されます。[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

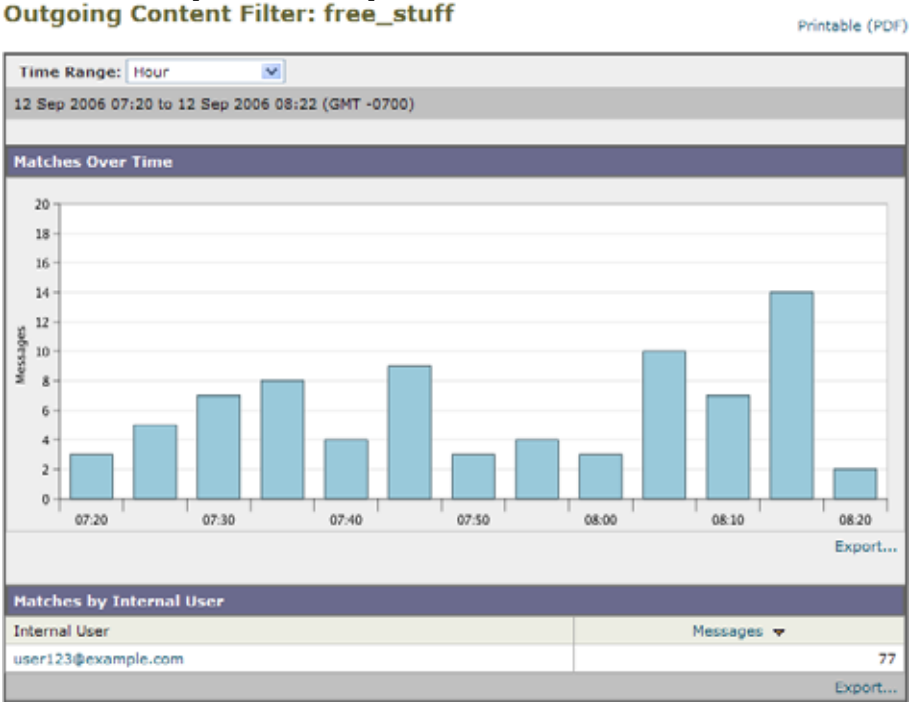
リストのコンテンツ フィルタ名をクリックすると、[Content Filter Details] ページにこのフィルタに関する詳細を表示できます。

Content Filter Details

[Content Filter Details] 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] セクションでは、ユーザ名をクリックして内部ユーザ（電子メール アドレス）の [Internal User Details] ページを表示できます（「[Internal User Details]」（P.2-34）を参照）。

図 2-25　[Content Filters] ページ



[Outbreak Filters] ページ

[Outbreak Filters] ページには、お使いの Cisco IronPort アプライアンスの Outbreak フィルタの現在のステータスおよび設定に加えて、最近の発生状況や Outbreak 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、対象を絞ったウイルス、詐欺、およびフィッシング攻撃に対する防御をモニタできます。

[Threats By Type] セクションには、アプライアンスによって受信された脅威メッセージのさまざまなタイプが示されます。[Threat Summary] セクションには、[Virus]、[Phish]、および [Scam] によるメッセージの内訳が示されます。

[Past Year Outbreak Summary] には、この 1 年間にわたるグローバル発生およびローカル発生が表示されるので、ローカル ネットワークのトレンドとグローバルなトレンドを比較できます。グローバル発生リストは、すべての発生（ウイルスとウイルス以外の両方）の上位集合です。これに対して、ローカル発生は、お

使いの Cisco IronPort アプライアンスに影響を与えたウイルス発生に限定されています。ローカル感染発生データには、ウイルス以外の脅威は含まれません。グローバル感染発生データは、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発生を表します。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発生を表します。[Total Local Protection Time] は、Cisco IronPort Threat Operations Center による各ウイルス発生の検出と、主要ベンダーによるアンチウイルス シグニチャの解放との時間差に常に基づいています。必ずしもすべてのグローバル発生が、お使いの 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、Outbreak フィルタの検疫状況の概要が示されます。これは、Outbreak 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、メッセージはアンチウイルスおよびアンチスパム ルールが使用可能になる前に検疫されます。メッセージが解放されると、アンチウイルスおよびアンチスパム ソフトウェアによってスキャンされ、陽性か、クリーンかを判定されます。発生トラッキングの動的性質により、メッセージが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）、脅威の名前、脅威の説明、識別されたメッセージの数などの、特定の発生に関する情報が表示されます。ウイルス発生の場合は [Past Year Virus Outbreaks] に、発生の名前と ID、ウイルス発生が初めてグローバルに検出された日時、Outbreak フィルタによって提供される保護時間、および検疫されたメッセージの数が含まれます。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。このリストは、カラム見出しをクリックしてソートできます。

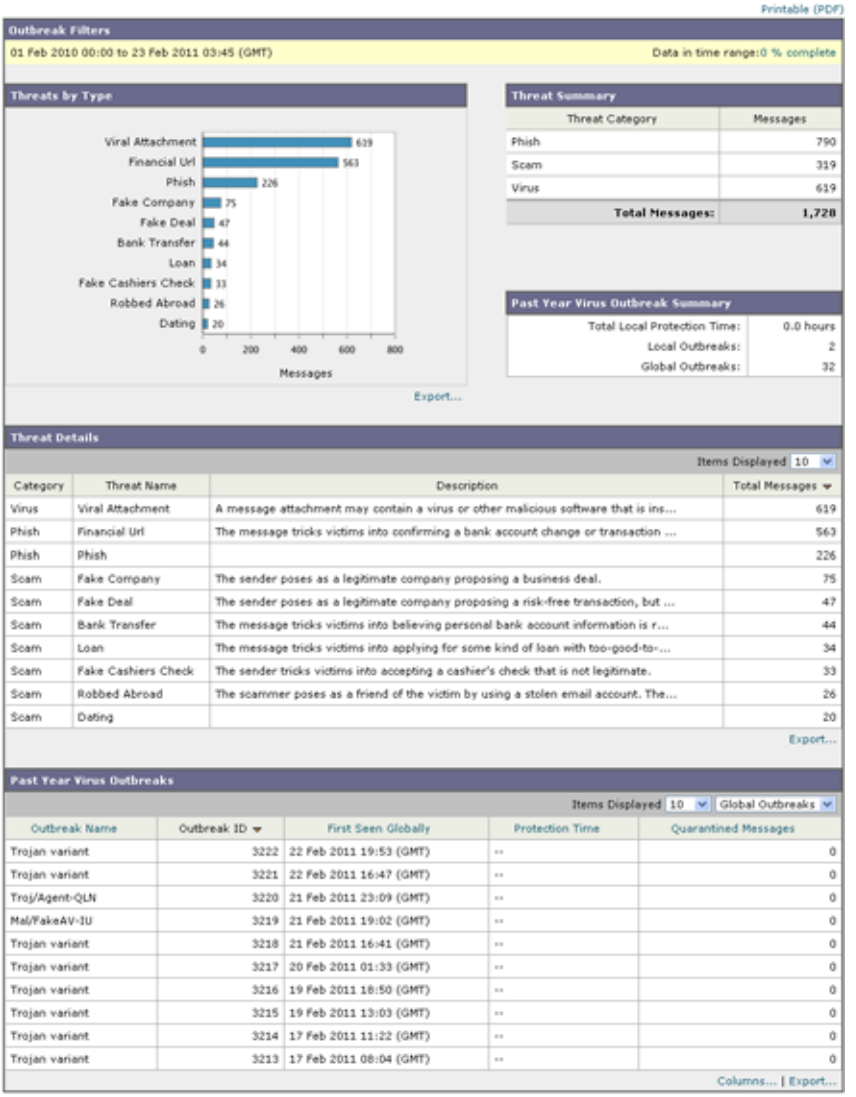
[First Seen Globally] の時間は、世界最大の電子メールおよび Web モニタリング ネットワークである SenderBase のデータに基づいて、Cisco IronPort Threat Operations Center によって決定されます。[Protection Time] は、Cisco IronPort Threat Operations Center による各脅威の検出と、主要ベンダーによるアンチウイルス シグニチャの解放との時間差に基づいています。

「--」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] ページを使用すると、次の情報を取得できます。

- 検疫されているメッセージの数と、それらの脅威のタイプ
- ウイルス発生に対する Outbreak フィルタ機能のリード タイム
- グローバル ウイルス発生と比較したローカル ウイルスの発生状況

図 2-26　[Outbreak Filters] ページ



[Virus Types] ページ

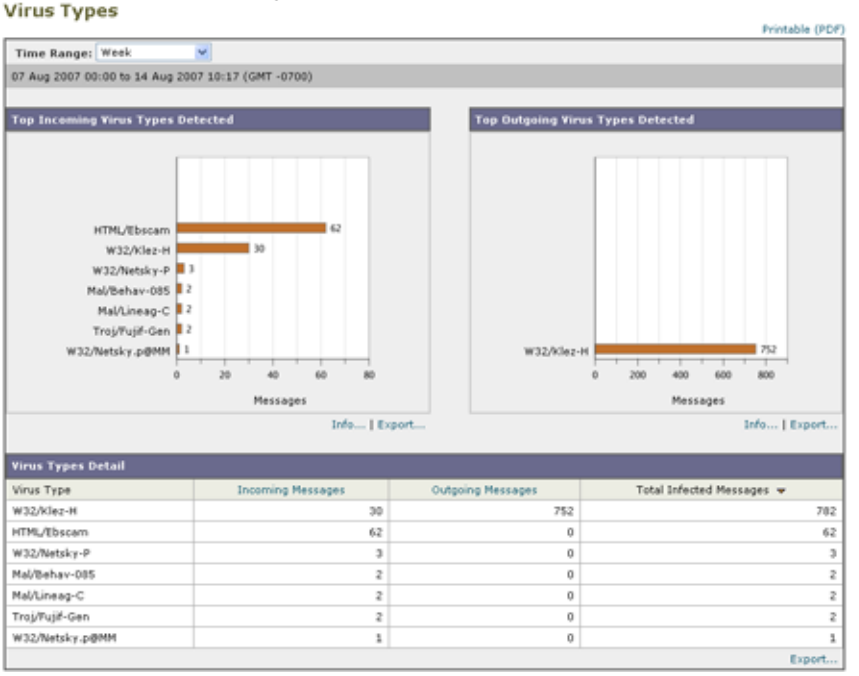
[Virus Types] ページでは、ネットワークに浸入したウイルスおよびネットワークから送信されたウイルスの概要が示されます。[Virus Types] ページには、お使いの Cisco IronPort アプライアンスで稼動するウイルス スキャン エンジンによって検出されたウイルスが表示されます。このレポートを使用して、特定のウイルスに対して特定のアクションを実行することが推奨されます。たとえば、PDF ファイルに組み込まれることが判明しているウイルスを大量に受信している場合、PDF が添付されているメッセージを検疫するフィルタ アクションを作成することが推奨されます。

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。

[Virus Types] ページには、ネットワークに浸入したウイルスおよび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。[Top Incoming Virus Detected] セクションには、ネットワークに送信されたウイルスのチャート ビューが降順で表示されます。[Top Outgoing Virus Detected] セクションには、ネットワークから送信されたウイルスのチャート ビューが降順で表示されます。

（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。

図 2-27　[Virus Types] ページ



[Virus Types Details] リストには、感染した送受信メッセージ、および感染メッセージの総数など特定のウイルスに関する情報が表示されます。感染した受信メッセージの詳細リストには、ウイルスの名前およびこのウイルスに感染した受信メッセージの総数が表示されます。同様に、送信メッセージの詳細リストには、ウイルスの名前およびこのウイルスに感染した送信メッセージの総数が表示されます。ウイルスの種類の詳細は、[Incoming Messages]、[Outgoing Messages]、または [Total Infected Messages] 別にソートできます。

[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] ページは、着信接続に関するセクションと、発信接続に関するセクションに分かれています。各セクションには、詳細情報が含まれたグラフ、サマリー、および表が含まれています。

グラフには、指定した時間範囲にわたる、送受信 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。グラフには、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 TLS 暗号化メッセージの量が表示されます。グラフでは、TLS が必須であった接続と、TLS が単に優先された接続が区別されます。

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。ドメインごとに、成功/失敗した必須の TLS 接続と優先された TLS 接続の数、試行された TLS 接続の総数（成功したか失敗したかにかかわらず）、および暗号化されていない接続の総数を表示できます。また、TLS が試行されたすべての接続の割合、および正常に送信された暗号化メッセージの総数（TLS が優先か必須かにかかわらず）も表示できます。この表の下部にある [Columns] リンクをクリックすることにより、カラムの表示/非表示を切り替えることができます。

図 2-28　TLS 接続レポート：着信接続

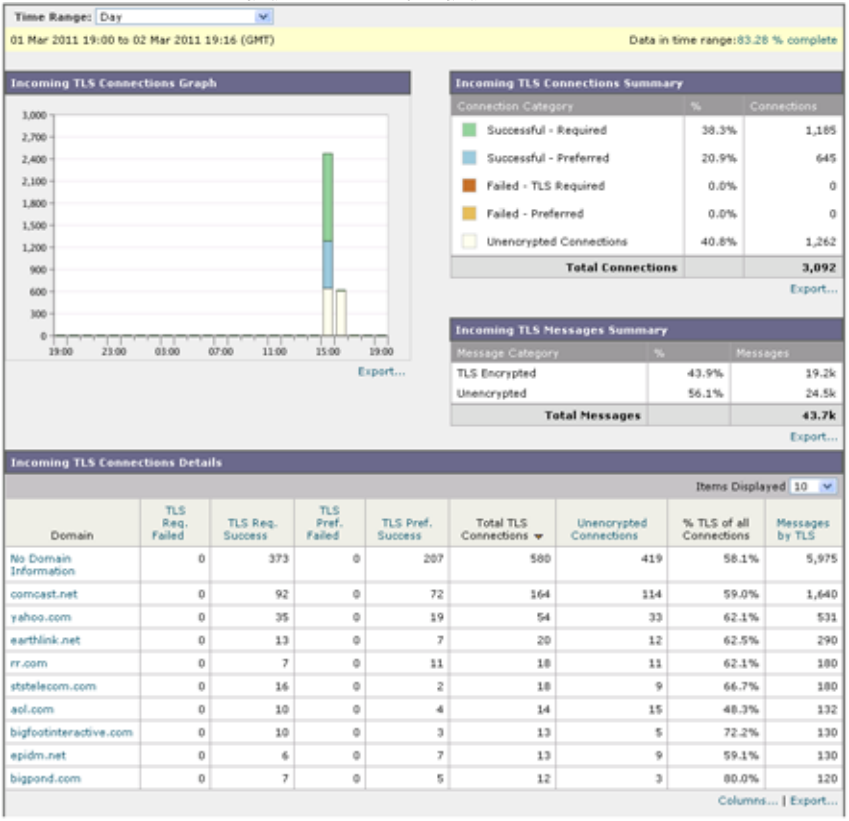
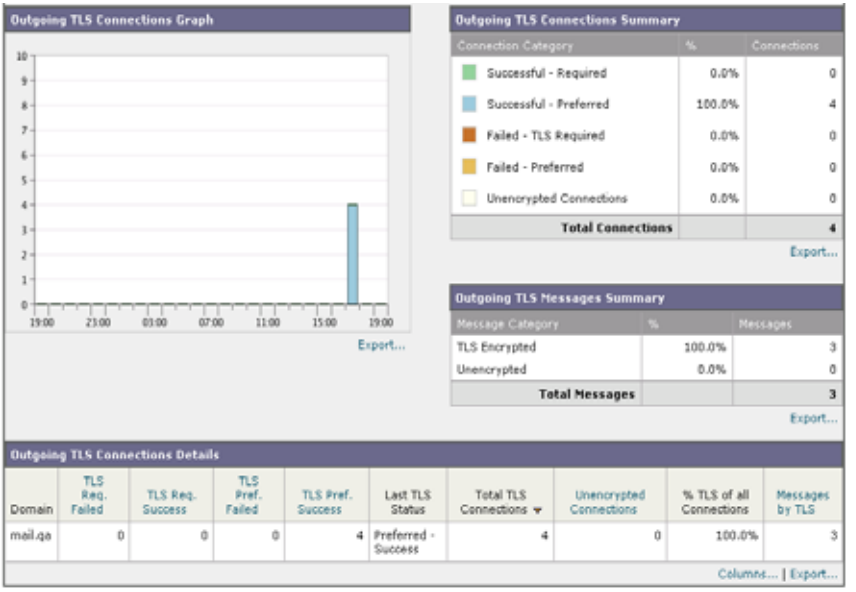


図 2-29　TLS 接続レポート：発信接続



[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、作業キューで費やした平均時間、送受信メッセージ（量、サイズ、件数）、全体的な CPU 使用率、機能別の CPU 使用率、メモリ ページ スワップ情報などシステム負荷の詳細が示されます。

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

- Cisco IronPort アプライアンスが推奨キャパシティを超えて、設定の最適化または追加アプライアンスが必要になった時間
- 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
- 最も多くのリソースを使用したシステムの部分（トラブルシューティングを支援するため）

お使いの Cisco IronPort をモニタして、メッセージの量に対してキャパシティが適切であることを確認することが重要です。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.2-52）および「[System Capacity] : [Outgoing Mail]」（P.2-53）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、有害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。しかし作業キューは、負荷のかかっているシステムを示す最良の指標であり、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。[WorkQueue] ページを使用すると、作業キュー内でメッセージが費やした平均時間および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.2-50）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。リソース節約モードは、[System Capacity] ページでは追跡できません。

[System Capacity] : [Workqueue]

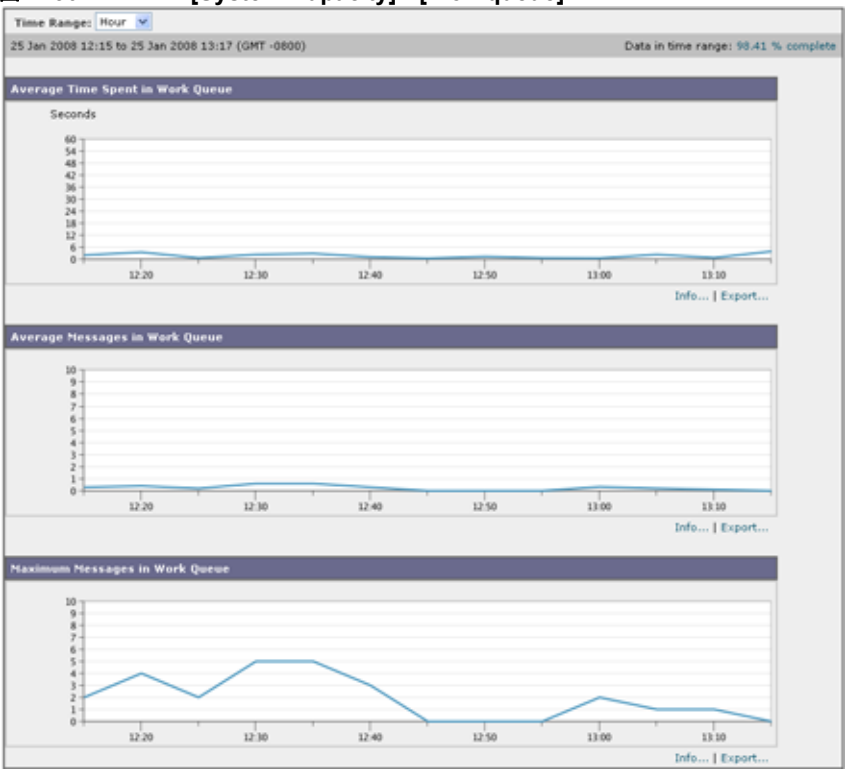
[Workqueue] ページには、作業キュー内でメッセージが費やした平均時間（IronPort スパム検疫またはシステム検疫で費やした時間は除く）が表示されます。1 時間から 1 月までの時間範囲を表示できます。平均は、メール配信を遅延させた短期間のイベントおよびシステム上の負荷の長期トレンドの両方を識別するのに役立ちます。

（注）　検疫から作業キューにメッセージが解放される場合、「作業キュー内の平均時間」メトリックではこの時間が無視されます。これにより、重複集計と検疫で費やされた延長時間による統計の歪みを回避できます。

このレポートでは、指定期間の作業キュー内のメッセージの量および同期間の作業キュー内の最大メッセージ数も示されます。

[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 2-30　[System Capacity] : [Workqueue]



[System Capacity] : [Incoming Mail]

[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。結果を、指定した時間範囲に制限できます。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。[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 2-31　[System Capacity] : [Incoming Mail]（1/2 ページ）

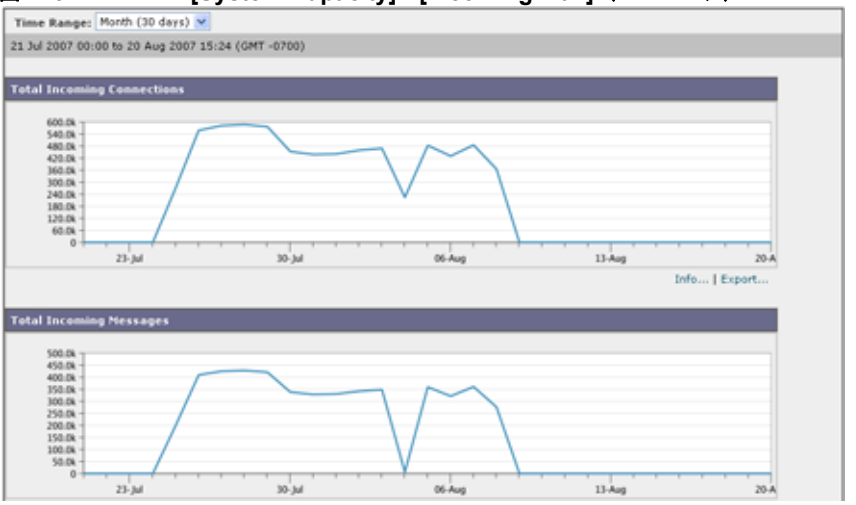
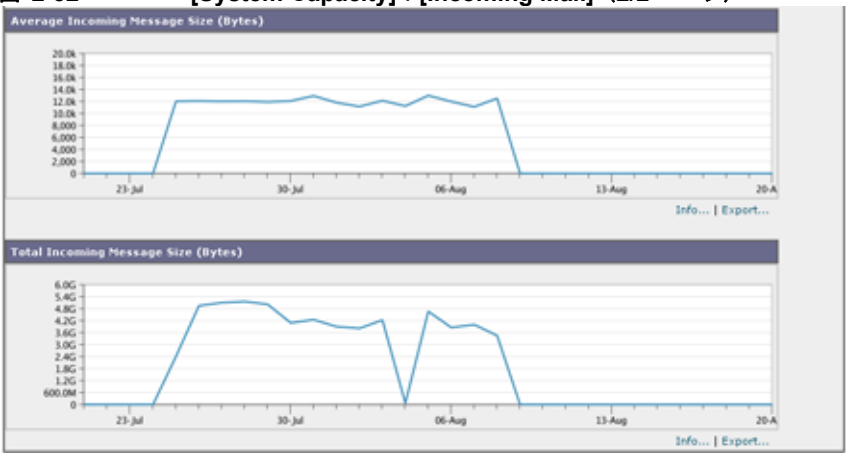


図 2-32　[System Capacity] : [Incoming Mail]（2/2 ページ）



[System Capacity] : [Outgoing Mail]

[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、着信メッセージの総サイズが示されます。結果を、指定した時間範囲に制限できます。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。[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の量のトレンドを表示することも推奨されます。

図 2-33　[System Capacity] : [Outgoing Mail]（1/2 ページ）

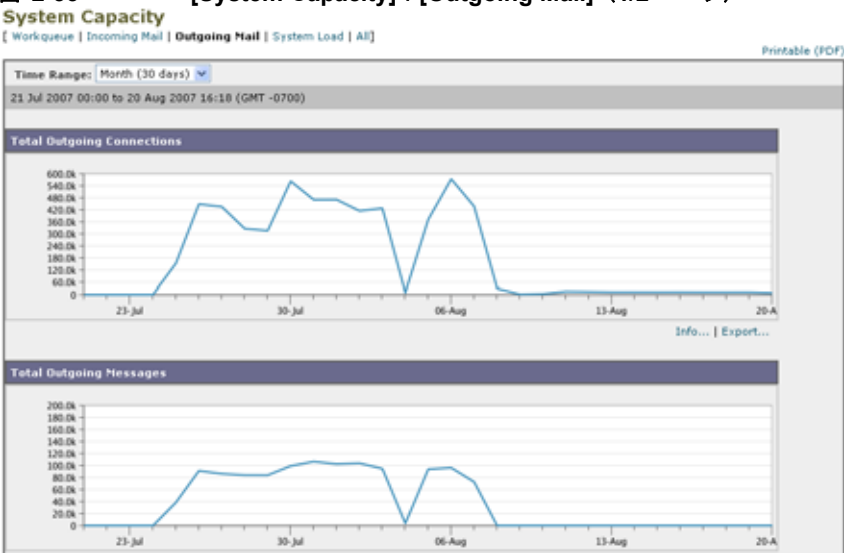
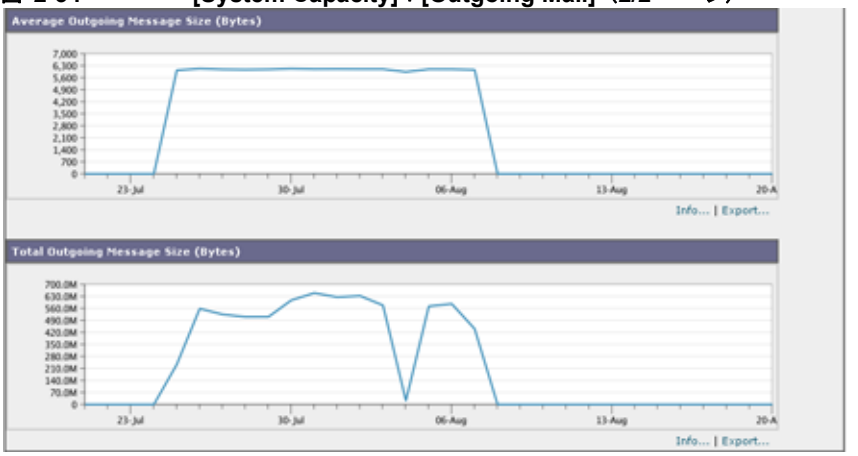


図 2-34　[System Capacity] : [Outgoing Mail]（2/2 ページ）



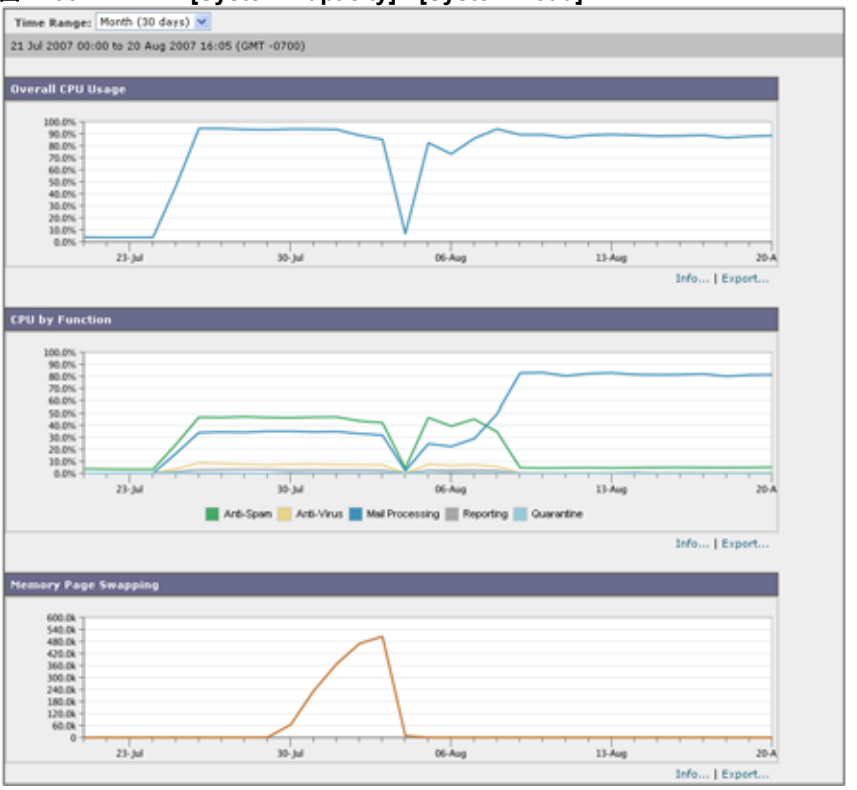
[System Capacity] : [System Load]

システム負荷レポートには、お使いの Cisco IronPort 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良い指標です。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。

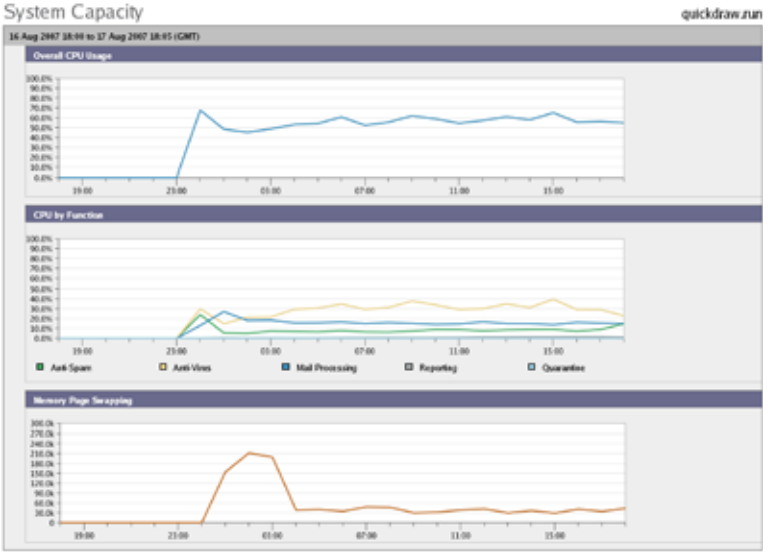
図 2-35　[System Capacity] : [System Load]



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/C160 アプライアンスの場合）。たとえば、図 2-36 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 2-36　[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 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。英語以外の言語での PDF の生成については、「レポートに関する注意事項」（P.68）を参照してください。

[System Status] ページ

[System Status] ページには、システムのすべてのリアルタイム メールおよび DNS アクティビティの詳細が表示されます。表示される情報は、CLI で `status detail` コマンドおよび `dnsstatus` コマンドを使用して入手できる情報と同じです。status detail コマンドの詳細については、第 6 章「CLI による管理およびモ

ニタリング」の「詳細な電子メール ステータスのモニタリング」を参照してください。dnsstatus コマンドの詳細については、同章の「DNS ステータスの確認」を参照してください。

[System Status] ページは、[System Status]、[Gauges]、[Rates]、および [Counters] の 4 つのセクションで構成されます。

System Status

[System Status] セクションには、[Mail System Status] および [Version Information] が示されます。

Mail System Status

[Mail System Status] セクションには、次の情報が含まれます。

- システム ステータス（システム ステータスの詳細については、「Status」（P.2-6）を参照してください）。
- ステータスが報告された最終時刻。
- アプライアンスのアップタイム。
- システム内の最も古いメッセージ（配信用にまだキューに入っていないメッセージも含む）。

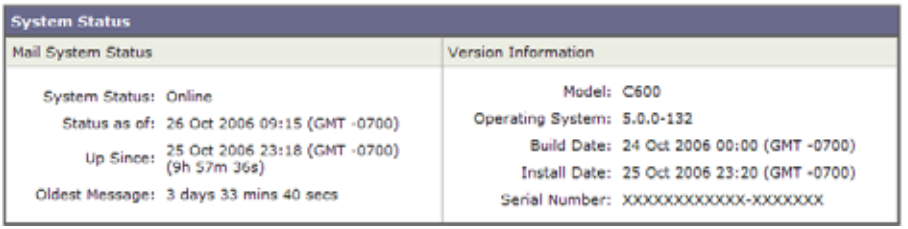
Version Information

[Version Information] セクションには、次の情報が含まれます。

- Cisco IronPort アプライアンスのモデル名。
- インストールされている Cisco IronPort AsyncOS オペレーティング システムのバージョンとビルド日。
- Cisco IronPort AsyncOS オペレーティング システムのインストール日。
- 接続先のシステムのシリアル番号。

この情報は、Cisco IronPort Customer Support に問い合わせる場合に役立ちます（「シスコのテクニカル サポート」（P.1-7）を参照）。

図 2-37　System Status



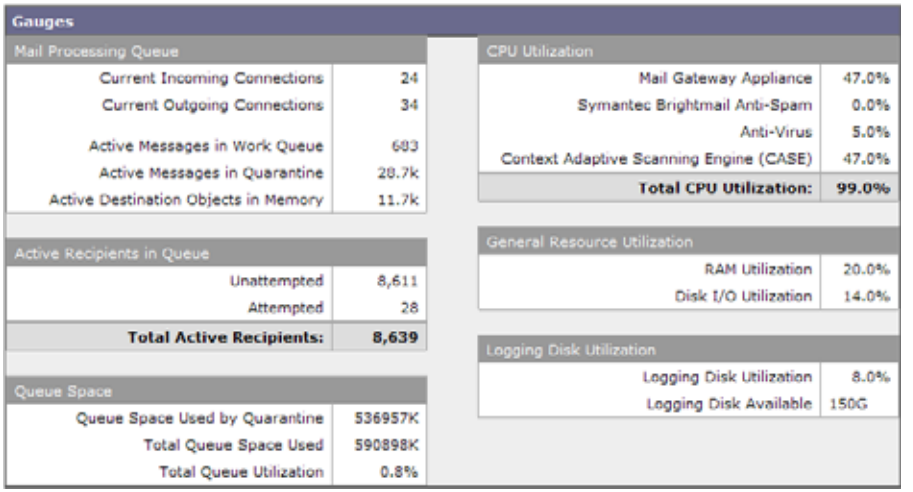
Gauges

[Gauges] には、次のようにキューおよびリソース使用率について示されます。

- Mail Processing Queue
- Active Recipients in Queue
- Queue Space
- CPU Utilization

  メール ゲートウェイ アプライアンスは、AsyncOS プロセスが消費している CPU 率を参照します。CASE は、IronPort アンチスパム スキャン エンジンおよび Outbreak フィルタ プロセスなど複数のアイテムを参照します。
- General Resource Utilization
- Logging Disk Utilization

図 2-38　Gauges

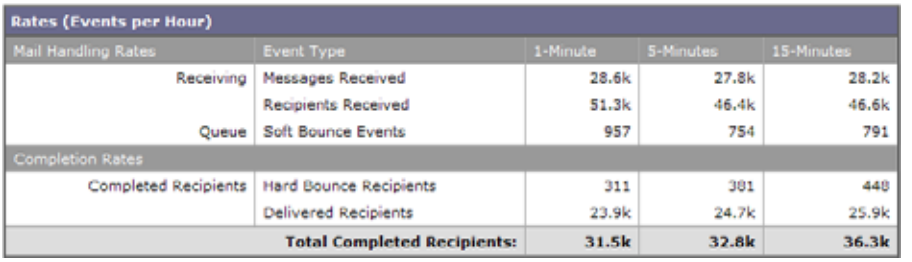


Rates

[Rates] セクションには、次の受信者に関する処理率が示されます。

- Mail Handling Rates
- Completion Rates

図 2-39　Rates



Counters

Cloud Email Security アプライアンスでは、カウンタをリセットしないようにすることを推奨します。

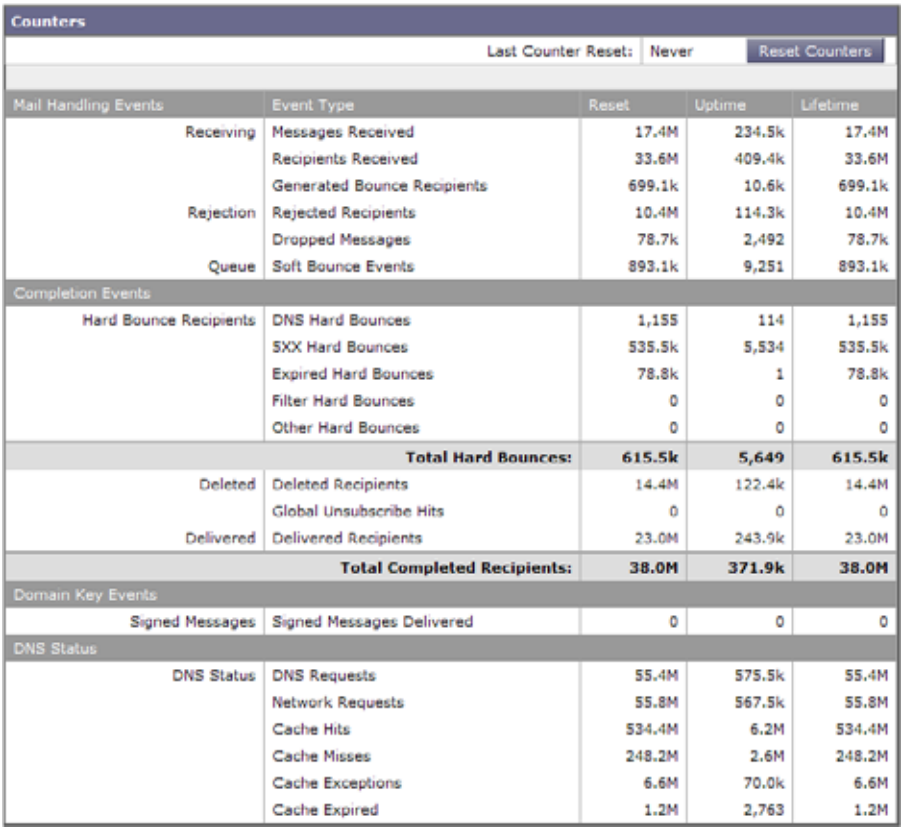
システム統計情報用の累積電子メール モニタリング カウンタをリセットし、カウンタの最終リセット日時を表示することができます。リセットは、システム カウンタおよびドメインごとのカウンタに影響します。リセットは、再試行スケジュールに関連する配信キュー内のメッセージのカウンタには影響しません。

（注）　管理者グループまたはオペレータ グループに属するユーザ アカウントのみが、カウンタをリセットできます。ゲスト グループ内で作成したユーザ アカウントでは、カウンタをリセットできません。詳細については、「ユーザ アカウントを使用する作業」（P.8-18）を参照してください。

カウンタをリセットするには、[Reset Counters] をクリックします。このボタンは、CLI の `resetcounters` コマンドと同様の機能を提供します。詳細については、「電子メール モニタリング カウンタのリセット」（P.6-32）を参照してください。

- Mail Handling Events
- Completion Events
- Domain Key Events
- DNS Status

図 2-40　Counters



Counters

Last Counter Reset: Never　Reset Counters

Mail Handling Events	Event Type	Reset	Uptime	Lifetime
Receiving	Messages Received	17.4M	234.5k	17.4M
	Recipients Received	33.6M	409.4k	33.6M
	Generated Bounce Recipients	699.1k	10.6k	699.1k
Rejection	Rejected Recipients	10.4M	114.3k	10.4M
	Dropped Messages	78.7k	2,492	78.7k
Queue	Soft Bounce Events	893.1k	9,251	893.1k
Completion Events				
Hard Bounce Recipients	DNS Hard Bounces	1,155	114	1,155
	5XX Hard Bounces	535.5k	5,534	535.5k
	Expired Hard Bounces	78.8k	1	78.8k
	Filter Hard Bounces	0	0	0
	Other Hard Bounces	0	0	0
	Total Hard Bounces:	**615.5k**	**5,649**	**615.5k**
Deleted	Deleted Recipients	14.4M	122.4k	14.4M
	Global Unsubscribe Hits	0	0	0
Delivered	Delivered Recipients	23.0M	243.9k	23.0M
	Total Completed Recipients:	**38.0M**	**371.9k**	**38.0M**
Domain Key Events				
Signed Messages	Signed Messages Delivered	0	0	0
DNS Status				
DNS Status	DNS Requests	55.4M	575.5k	55.4M
	Network Requests	55.8M	567.5k	55.8M
	Cache Hits	534.4M	6.2M	534.4M
	Cache Misses	248.2M	2.6M	248.2M
	Cache Exceptions	6.6M	70.0k	6.6M
	Cache Expired	1.2M	2,763	1.2M

CSV データの取得

電子メール セキュリティ モニタで図やグラフの作成に使用されたデータは、CSV 形式で取得できます。CSV データにアクセスする方法は、次の 2 つです。

- **電子メールによる CSV レポートの配信**。電子メールで配信される、またはアーカイブされる CSV レポートを生成できます。この配信方法は、電子メール セキュリティ モニタ ページに表示される各表に関する個別レポートを必要とする場合、または内部ネットワークにアクセスできないユーザに CSV データを送信する場合に便利です。

Comma-Separated Value（CSV; カンマ区切り）レポート タイプは、スケジュール設定されたレポートの表形式データを含む ASCII テキスト ファイルです。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。単一のレポートの複数の CSV ファイルは、単一の .zip ファイルに圧縮されて、アーカイブ ファイルの保存オプションを提供するか、個別の電子メール メッセージに添付されて電子メールで配信されます。

スケジュール設定されたレポートまたはオンデマンド レポートの詳細については、「レポーティングの概要」（P.2-66）を参照してください。

- **HTTP による CSV ファイルの取得**。電子メール セキュリティ モニタ機能で図やグラフの作成に使用されたデータは、HTTP を使用して取得できます。この配信方法は、他のツールを使用してデータの詳細分析を実行する予定の場合に役立ちます。たとえば、未加工データのダウンロード、処理、および他のシステムでの結果表示を行う自動スクリプトによって、データの取得を自動化できます。

自動プロセスによる CSV データの取得

必要とする HTTP クエリーを最も容易に取得する方法は、必要な種類のデータを表示するように電子メール セキュリティ モニタ ページの 1 つを設定することです。次に、[Export] リンクをコピーできます。これがダウンロード URL です。このようにデータ取得を自動化した場合、ダウンロード URL 内のパラメータを固定し、変更しないことが重要です（下記を参照）。

ダウンロード URL はコード化されるので、（適切な HTTP 認証を使用して）同じクエリーを実行し、同様のデータ セットを取得できる外部スクリプトにコピーできます。このスクリプトでは、Basic HTTP 認証またはクッキー認証を使用できます。自動プロセスで CSV データを取得する場合は、次の事項に注意する必要があります。

- URL の再利用時に関する時間範囲の選択（過去 1 時間、1 日、1 週間など）。URL をコピーして「過去 1 日」の CSV データ セットを取得する場合、この URL を次に使用するときには、URL の再送信時から「過去 1 日」を対象とする新しいデータ セットを取得します。時間範囲の選択は保持され、CSV クエリー文字列（たとえば `date_range=current_day`）に表示されます。
- データ セットのフィルタリングおよび分類の優先順位。フィルタは保持され、クエリー文字列に表示されます。レポートでは、フィルタはほとんど使用されません。1 つの例としては、発生レポートにおける「グローバル/ローカル」発生セレクタが挙げられます。

- CVS ダウンロードでは、選択した時間範囲について表内のデータのすべての行が返されます。
- CSV では、タイムスタンプおよびキーで指示された表内のデータの行が返されます。スプレッドシート アプリケーションを使用するなどして、別個のステップで更にソートできます。
- 最初の行には、レポートに示される表示名に一致するカラム見出しが含まれています。タイムスタンプ（「タイムスタンプ」（P.2-65）を参照）およびキー（「キー」（P.2-66）を参照）も表示されます。

URL のサンプル

http://example.com/monitor/content_filters?format=csv&sort_col_ss_0_0_0=MAIL_CONTENT_FILTER_INCOMING.RECIPIENTS_MATCHED&section=ss_0_0_0&date_range=current_day&sort_order_ss_0_0_0=desc&report_def_id=mga_content_filters

Basic HTTP 認証クレデンシャルの追加

URL に Basic HTTP 認証クレデンシャルを指定する例を次に示します。

```
http://example.com/monitor/
```

次のようになります。

```
http://username:password@example.com/monitor/
```

ファイル形式

ダウンロードされるファイルは CSV 形式であり、ファイル拡張子は .csv です。ファイル見出しは、デフォルトのファイル名であり、レポートの名前に始まり、レポートのセクションが続きます。

タイムスタンプ

データのストリーミングを行うエクスポートには、各行の時間「間隔」について開始タイムスタンプおよび終了タイムスタンプが示されます。2 種類の開始タイムスタンプおよび終了タイムスタンプ（数値形式および人間が読み取れる文字列形式）が提供されます。タイムスタンプは GMT 時間です。これにより、アプライアンスが複数の時間帯にある場合、ログの集約が容易になります。

あまりないことですが、データが他のソースのデータとマージされる場合には、エクスポート ファイルにタイムスタンプは含まれません。たとえば、発生の詳細のエクスポートでは、レポートのデータと Threat Operations Center（TOC）データがマージされ、タイムスタンプが不適切になります。これは、間隔が存在しないためです。

キー

レポートにキーが表示されない場合であっても、エクスポートには、レポート テーブル キーが含まれます。キーが表示される場合、レポートに表示される表示名がカラム見出しとして使用されます。それ以外の場合は、「key0」、「key1」などのカラム見出しが表示されます。

ストリーミング

大部分のエクスポートでは、データをクライアントにストリーミングで戻します。これは、データ量が非常に大きい可能性があるからです。しかし、一部のエクスポートでは、ストリーミング データではなく結果セット全体を返します。通常、レポート データが非レポート データ（発生の詳細など）と集約される場合が該当します。

レポーティングの概要

AsyncOS におけるレポーティングには、次の 3 つの基本動作が含まれます。

- 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できます。
- ただちにレポートを生成できます（「オンデマンド」レポート）。
- 以前実行したレポートのアーカイブ版を表示できます（スケジュール設定されたレポートおよびオンデマンド レポートの両方）。

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、[Monitor] > [Scheduled Reports] ページから設定できます。アーカイブ済みレポートは、[Monitor] > [Archived Reports] ページから表示できます。

Cisco IronPort 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、最大で合計 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 `/saved_reports` ディレクトリに保管されます（詳細については、付録 A「Accessing the Appliance」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種類

次のレポートの種類から選択できます。

- コンテンツ フィルタ
- 配信ステータス
- DLP インシデント サマリー
- 要約
- 着信メール サマリー
- 内部ユーザ サマリー
- 発信先
- 発信メール サマリー
- 発信送信者：ドメイン
- 送信者グループ
- システム キャパシティ
- TLS 接続
- Outbreak フィルタ
- ウイルスの種類

各レポートは、対応する電子メール セキュリティ モニタ ページのサマリーで構成されます。したがって、たとえばコンテンツ フィルタ レポートでは、[Monitor] > [Content Filters] ページに表示される情報のサマリーが示されます。要約レポートは、[Monitor] > [Overview] ページに基づいています。

レポートに関する注意事項

PDF 形式のコンテンツ フィルタ レポートは、最大 40 のコンテンツ フィルタに制限されます。完全なリストは、CSV 形式のレポートで入手できます。

（注） Windows コンピュータ上で中国語、日本語、または韓国語の PDF を生成するには、Adobe.com から該当するフォント パックをダウンロードしてローカル コンピュータにインストールすることも必要です。

レポート用返信アドレスの設定

レポート用返信アドレスを設定するには、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「System Administration」の章を参照してください。CLI から、`addressconfig` コマンドを使用します。

レポートの管理

アーカイブ済みのスケジュール設定されたレポートは、作成、編集、削除、および表示を行うことができます。ただちにレポートを実行することもできます（オンデマンド レポート）。コンテンツ フィルタ、DLP インシデント サマリー、要約、着信メール サマリー、内部ユーザ サマリー、発信メール サマリー、送信者グループ、および Outbreak フィルタの各レポートを使用できます。これらのレポートの管理および表示については、後述します。

（注） クラスタ モードでは、レポートを表示できません。マシン モードの場合、レポートを表示できます。

[Monitor] > [Scheduled Reports] ページには、アプライアンスで生成済みのスケジュール設定されたレポートのリストが示されます。

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は、日単位、週単位、または月単位で実行するようにスケジュール設定できます。レポートを実行する時間を選択できます。レポートを実行する時間には関係なく、指定した期間（たとえば、過去 3 日または前の 1 か月）のデータのみが含まれます。午前 1 時に実行するようにスケジュール設定されている日単位のレポートには、前の日（午前 0 時～午前 0 時）のデータが含まれることに注意してください。

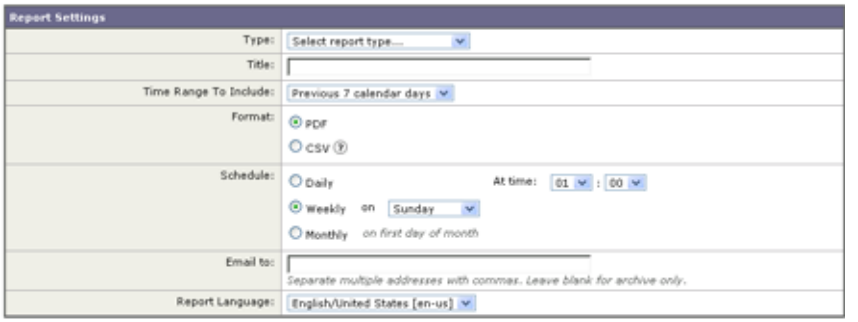
お使いの Cisco IronPort アプライアンスは、デフォルトのレポート セットがスケジュール設定された状態で出荷されています。このレポート セットのいずれかを使用したり、変更や削除を行ったりすることができます。

スケジュール設定されたレポートの作成

スケジュール設定されたレポートを作成するには、次の手順を実行します。

ステップ 1　[Monitor] > [Scheduled Reports] ページで、[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 2-41　スケジュール設定されたレポートの追加



ステップ 2　レポートの種類を選択します。選択したレポートの種類に応じて、異なるオプションを使用できます。

使用可能なスケジュール設定されたレポートの種類の詳細については、「スケジュール設定されたレポートの種類」（P.2-67）を参照してください。

ステップ 3　レポートのわかりやすいタイトルを入力します。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 4　レポート データの時間範囲を選択します（Outbreak フィルタ 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 5　レポートの形式を選択します。

- [PDF]。配信用、アーカイブ用、またはその両方の用途で PDF 形式のドキュメントを作成します。[Preview PDF Report] をクリックすると、ただちに PDF ファイルでレポートを表示できます。

  英語以外の言語での PDF の生成については、「レポートに関する注意事項」（P.68）を参照してください。

- [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 6　使用可能な場合は、レポート オプションを指定します。レポートによっては、レポート オプションはありません。

ステップ 7　スケジュールおよび配信オプションを指定します。電子メール アドレスを指定しない場合、レポートはアーカイブされますが、いずれの受信者にも送信されません。

（注）　外部アカウント（Yahoo または Gmail など）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 8　[Submit] をクリックします。変更を保存します。

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　[Services] > [Centralized Reporting] ページでリストのレポート タイトルをクリックします。

ステップ 2　変更を行います。

ステップ 3　変更を送信し、保存します。

スケジュール設定されたレポートの削除

スケジュール設定されたレポートを削除するには、次の手順を実行します。

ステップ 1　[Services] > [Centralized Reporting] ページで、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。

（注）　スケジュール設定されたレポートをすべて削除するには、[All] チェックボックスをオンにします。

ステップ 2　[Delete] をクリックします。

ステップ 3　削除を確認し、変更内容を確定させます。

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*。

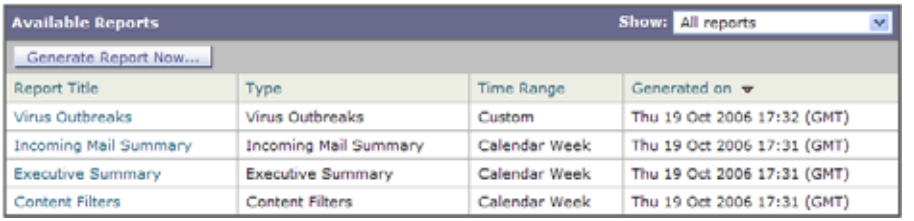
アーカイブ済みのレポート

[Monitor] > [Archived Reports] ページでは、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] カラムの名前をクリックすると、レポートを表示できます。[Generate Report Now] をクリックすると、ただちにレポートを生成できます。

リストに表示されるレポートの種類をフィルタリングするには、[Show] メニューを使用します。リストをソートするには、カラム見出しをクリックします。

アーカイブ済みのレポートは、自動的に削除されます。スケジュール設定された各レポートの最大 12 インスタンス（最大 1000 レポート）が保存され、新たなレポートが追加されると、古いレポートが削除されてレポートの数は 1000 に維持されます。12 インスタンスという制限は、レポートの種類に対してではなく、個別のスケジュール設定された各レポートに対して適用されます。

図 2-42　アーカイブ済みのレポート



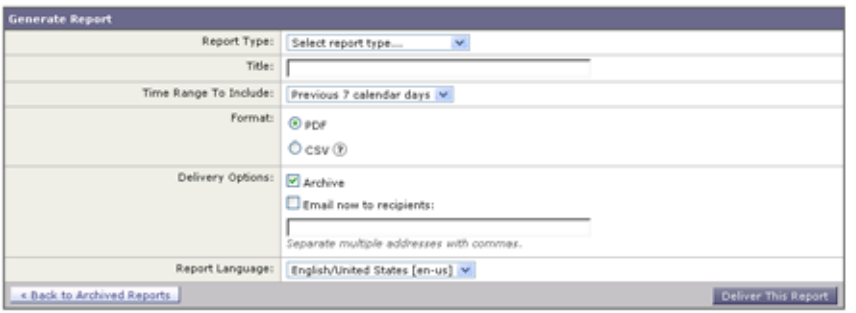
オンデマンド レポート

レポートは、スケジュールを設定しなくても生成できます。これらのオンデマンド レポートも指定したタイム フレームに基づいていますが、ただちに生成できます。

ただちに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　[Archived Reports] ページで [Generate Report Now] をクリックします。

図 2-43　[Generate Report] ダイアログ



ステップ 2　レポートの種類を選択し、必要に応じてタイトルを編集します。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。

使用可能なスケジュール設定されたレポートの種類の詳細については、「スケジュール設定されたレポートの種類」（P.2-67）を参照してください。

ステップ 3　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）。

カスタムの範囲を作成した場合は、その範囲がリンクとして表示されます。範囲を変更するには、そのリンクをクリックします。

ステップ 4　レポートの形式を選択します。

- [PDF]。配信用、アーカイブ用、またはその両方の用途で PDF 形式のドキュメントを作成します。[Preview PDF Report] をクリックすると、ただちに PDF ファイルでレポートを表示できます。

  英語以外の言語での PDF の生成については、「レポートに関する注意事項」（P.68）を参照してください。

- [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。任意のレポート オプションを指定します。

ステップ 5　レポートをアーカイブするかどうかを選択します（アーカイブする場合には、レポートが [Archived Reports] ページに表示されます）。

ステップ 6　レポートを電子メールで送信するかどうか、レポートの送信先の電子メール アドレスを指定します。

ステップ 7　[Deliver this Report] をクリックしてレポートを生成し、受信者に配信するか、このレポートをアーカイブします。

ステップ 8　変更を保存します。

CHAPTER 3

電子メール メッセージのトラッキング

この章は、次の内容で構成されています。

トラッキング サービスの概要

メッセージ トラッキング サービスにより、AsyncOS で処理されるメッセージのステータスを簡単に調べられるようになります。それにより、メッセージの正確な場所を確定して、ヘルプ デスク コールを迅速に解決できます。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ために、メッセージ トラッキングを使用できます。

メッセージ トラッキングは、ローカルの Cisco IronPort 電子メール セキュリティ アプライアンス上でイネーブルにできます。また、M-Series アプライアンス上で集中トラッキングをイネーブルにして、複数の電子メール セキュリティ アプライアンスに対してメッセージをトラッキングすることもできます。集中トラッキングをイネーブルにする手順については、『*Cisco IronPort AsyncOS for*

Security Management User Guide 』を参照してください。ローカル トラッキングをイネーブルにする手順については、「ローカル メッセージ トラッキングのイネーブル化とディセーブル化」（P.3-3）を参照してください。

「grep」などのツールを使用してログ ファイル全体を検索しなくても、柔軟なトラッキング インターフェイスを使用してメッセージの場所を特定できます。さまざまな検索パラメータを組み合わせて使用できます。

トラッキング クエリーには次の条件を含められます。

- **エンベロープ情報：**一致するテキスト 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受信者のメッセージを探します。
- **件名ヘッダー：**件名行のテキスト ストリングと一致します。警告：規制によりそのようなトラッキングが禁止されている環境では、このタイプの検索を使用しないでください。
- **タイム フレーム：**指定された日時の間に送信されたメッセージを探します。
- **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。
- **イベント情報：**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 IronPort メッセージ ID（MID）を識別してメッセージを探します。
- **添付ファイル名：**エンベロープ情報フィールド（エンベロープ送信者またはエンベロープ受信者）内の添付ファイル名に基づいてメッセージを検索できます。名前に対してクエリーが実行された少なくとも 1 つの添付ファイルを含むメッセージが検索結果に表示されます。

  トラッキングできない添付ファイルもあります。パフォーマンス上の理由から、添付ファイル名のスキャンは、メッセージまたはコンテンツ フィルタリング、DLP、免責事項スタンプなどの、他のスキャン操作の一部としてのみ実行されます。添付ファイル名は、添付ファイルがまだ添付されている間に本文スキャンを通過するメッセージに対してのみ使用できます。添付ファイル名が表示されない例をいくつか次に示します（ただし、これに限定されるものではありません）。

  - システムがコンテンツ フィルタのみを使用しているときに、メッセージがドロップされるか、またはその添付ファイルがアンチスパムまたはアンチウイルス フィルタによって削除された場合

– 本文スキャンが実行される前に、メッセージ分裂ポリシーによって一部のメッセージから添付ファイルが削除された場合

ローカル メッセージ トラッキングのイネーブル化とディセーブル化

ローカル メッセージ 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　[Services] > [Message Tracking] をクリックします。

[Message Tracking] ページが表示されます。

図 3-1　ローカル メッセージ トラッキングをイネーブルにした [Message Tracking] ページ

ステップ 2　[Message Tracking] セクション内で、[Enable Message Tracking Service] をクリックします。

システム設定ウィザードを実行してから初めてメッセージ 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。

ステップ 3　必要に応じて、拒絶された接続に関する情報を保存するチェックボックスをオンにします。

ステップ 4　変更を送信し、保存します。

（注）　メッセージ トラッキングで添付ファイル名を検索して表示したり、ログ ファイル内の添付ファイル名を表示したりするには、メッセージ フィルタやコンテンツ フィルタなどの本文スキャン プロセスを少なくとも 1 つ設定してイネーブルにする必要があります。詳細については、『*Cisco IronPort AsyncOS for Email*

Configuration Guide』の「Email Security Manager」の章、および『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の対応する項を参照してください。

ローカル メッセージ トラッキングのディセーブル化

ローカル メッセージ トラッキング サービス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　[Services] > [Message Tracking] で、[Edit Settings] ボタンをクリックします。

ステップ 2　[Enable Message Tracking Service] チェックボックスをオフにします。

ステップ 3　変更を送信し、保存します。

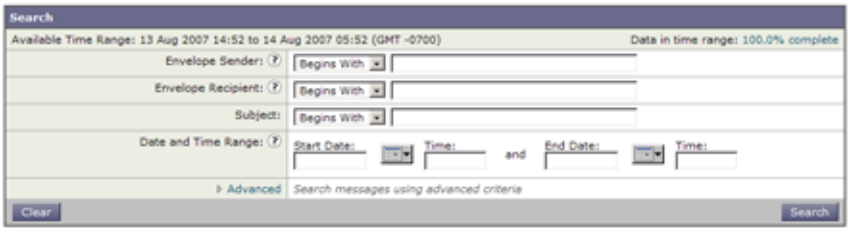
トラッキング クエリーのセットアップについて

メッセージ 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、添付ファイル名、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 トラッキングを使用して、メッセージ フローを詳細に確認できます。また、処理イベントや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。

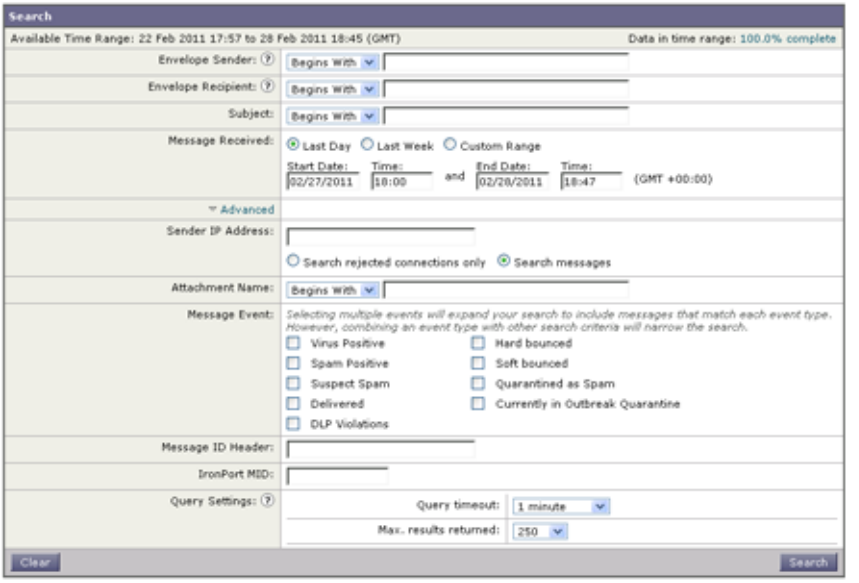
[Monitor] > [Message Tracking] ページを使用して、電子メール メッセージの場所を特定します。

図 3-2　[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 3-3　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。トラッキング検索では、大文字と小文字は区別されません。

メッセージ トラッキング クエリーを実行するとき、次の検索パラメータを使用できます。

- [Envelope Sender] : [Begins With]、[Is]、または [Contains] を選択し、エンベロープ送信者に対して検索するテキスト ストリングを入力します。有効なパラメータ値は、電子メール アドレス、ユーザ名、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に対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、およびドメインです。

  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、この検索では、元のエンベロープ アドレスではなく、拡張後の受信者アドレスが検索されます。それ以外の場合、メッセージ トラッキング クエリーでは、元のエンベロープ受信者アドレスが検索されます。
- [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 ストリングを入力します。

（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。

- [Dates and Times] : クエリーの日付と時間の範囲を指定します。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。

  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に変換されます。

  メッセージは、ロギング済みのものだけが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。詳細については、第 5 章「ロギング」を参照してください。
- [Message Event] : トラッキング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]、[Hard Bounced]、[Soft Bounced]、[Currently in Outbreak Quarantine]、[DLP Violations]、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他の多くの条件とは異なり、イベントは「OR」演算子で追加されます。複数のイベントを選択すると、検索結果は拡大します。

[DLP Violations] を選択すると、AsyncOS によって追加の DLP 関連オプションが表示されます。オプションには、メッセージが違反した DLP ポリシーとその違反の重大度（[Critical]、[High]、[Medium]、および [Low]）があります。

デフォルトでは、DLP 違反の検索を実行している場合、一致した内容を表示できるのは管理者だけです。他のユーザ（委任管理者を含む）がこの内容を表示できるようにするには、**[System Administration] > [Users]** ページを使用して DLP トラッキング権限をイネーブルにします。詳細については、「メッセージ トラッキング内の機密情報へのアクセスのディセーブル化」（P.8-27）を参照してください。

- [Message-ID Header] と MID :「Message-ID:」ヘッダーのテキスト ストリングと IronPort メッセージ ID（MID）のいずれかまたは両方を入力します。
- [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の ASCII または Unicode テキスト ストリングを入力します。

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　[Monitor] > [Message Tracking] ページで、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.3-4）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 2　[Search] をクリックして、クエリーを送信します。クエリーの結果がページの下部に表示されます。各行が 1 つの電子メール メッセージに対応します。

図 3-4　メッセージ トラッキング クエリーの結果

ステップ 3　返された行の数が [Items per page] フィールドに指定された値を上回ると、それらの結果は複数ページにわたって表示されます。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。

ステップ 4　必要に応じて、新しい検索基準を入力することにより検索を精密化し、クエリーを再実行します。あるいは、次の項の説明に従って、結果セットを絞り込むことにより検索を精密化することもできます。

結果セットの絞り込み

クエリーを実行すると、結果セットに必要以上の情報が含まれていることがあります。新しいクエリーを作成しなくても、行内の値をクリックして結果セットを絞り込めます。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できます。

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、検索を精密化できます。

- 日付と時間
- メッセージ ID（MID）
- 送信者のユーザ名
- 送信者のドメイン

- 受信者のユーザ名
- 受信者のドメイン
- メッセージの件名行

ステップ 2　値をクリックして、検索を精密化します。

[Results] セクションに、元のクエリー パラメータと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] ボタンをクリックし、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 クエリーに指定された基準に一致するすべてのメッセージが一覧されます。[Message Event] オプションを除き、各クエリー条件は「AND」演算子で追加されます。結果セット内のメッセージは、これらの「AND」条件をすべて満たす必要があります。たとえば、エンベロープ送信者は j で始まり、件名は t で始まることを指定すると、クエリーは、両方の条件を満たすメッセージだけを返します。

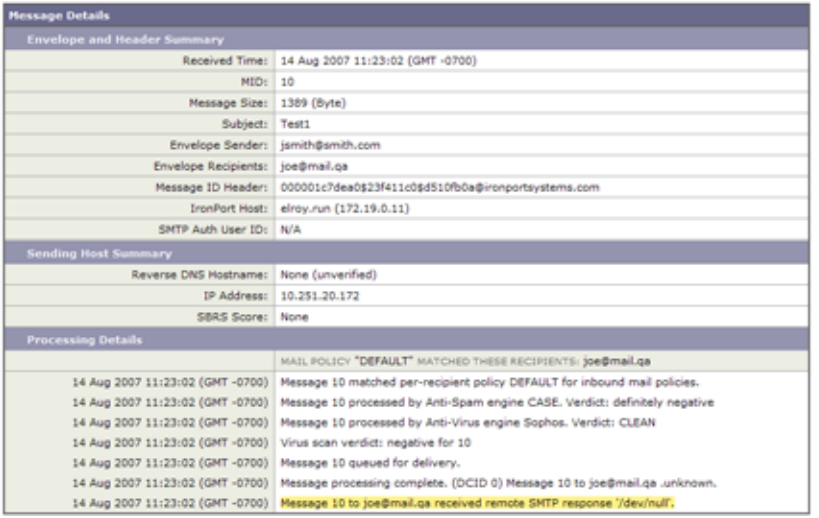
メッセージごとに、日付/時間、送信者、受信者、件名、最終状態、IronPort メッセージ ID（MID）、および添付ファイルの名前が表示されます。メッセージの詳細情報を表示するには、各メッセージの [Show Details] リンクをクリックします。詳細については、「メッセージの詳細」（P.3-9）を参照してください。

（注） セキュリティ管理アプライアンスからは、最初の 10,000 行までのデータが返されます。それ以降のレコードにアクセスするには、クエリーを調整して、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、[Show Details] リンクをクリックします。メッセージの詳細を表示した新しいブラウザ ウィンドウが開きます。

図 3-5　メッセージの詳細



メッセージの詳細には、[Envelope and Header Summary]、[Sending Host Summary] および [Processing Details] のセクションが含まれます。

Envelope and Header Summary

このセクションには、エンベロープ送信者や受信者など、メッセージのエンベロープとヘッダーの情報が表示されます。収集する情報は次のとおりです。

[Received Time]：電子メール セキュリティ アプライアンスがメッセージを受信した時間。

[MID]：IronPort 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 Cisco IronPort 電子メール セキュリティ アプライアンスがログ ファイルに件名行を記録するように設定されていない場合、トラッキング結果内の件名行は「(No Subject)」という値になることがあります。

件名ヘッダーをロギングするように電子メール セキュリティ アプライアンスを設定する方法の詳細については、第 5 章「ロギング」を参照してください。

[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るときに挿入されます。「Message-ID:」ヘッダーは、特定のメッセージを検索する際に役立つ場合があります。

[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、SMTP で認証された送信者のユーザ名。それ以外の場合、この値は [N/A] になります。

[Attachments]：メッセージに添付されたファイルの名前。パフォーマンス上の理由から、添付ファイル内のファイルの名前（たとえば、OLE オブジェクトや、.ZIP ファイルなどのアーカイブ）は検索されません。

Sending Host Summary

[Reverse DNS Hostname]：送信元ホストのホスト名。リバース DNS（PTR）ルックアップで検証されます。

[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ギングされたさまざまなステータス イベントが表示されます。

エントリには、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、およびコンテンツまたはメッセージ フィルタによって追加されるカスタム ログ エントリが含まれます。

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。

CHAPTER 4

検疫

検疫とは、メッセージを保管し、処理するために使用される特別なキューまたはリポジトリです。Cisco IronPort AsyncOS では、着信または発信のメッセージをアプライアンスの検疫（「システム」と「IronPort スパム」）のいずれかに入れることができます。

検疫エリア内のメッセージは、配信または削除ができます。検疫は、作成、変更、および削除できます。検疫にはユーザを関連付けられます。それぞれの検疫の内容を表示したり、検疫エリア内に特定のメッセージがないか検索したり、メッセージのコピーを送信したりできます。

この章は、次の内容で構成されています。

検疫の概要

メッセージが Cisco IronPort アプライアンスによって処理されるとき、さまざまなアクションが適用されます。フィルタがメッセージに適用されたり、スパムまたはウイルスがないかメッセージがスキャンされたり、Outbreak フィルタ機能によって、対象を絞った攻撃がないかメッセージがスキャンされたりします。これらのアクションにより、設定に従ってメッセージを検疫できます。

検疫の種類

IronPort スパム検疫は、エンド ユーザ宛のスパムまたは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 ユーザのことであり、AsyncOS の外部に存在します。IronPort スパム検疫はローカルに設置して、Cisco IronPort アプライアンス上に保管できます。また、メッセージを外部の IronPort スパム検疫に送信して、別の Cisco IronPort アプライアンス上に保管することもできます。IronPort スパム検疫には、AsyncOS 管理者およびエンド ユーザ（AsyncOS ユーザではない）のどちらからもアクセスできます。

システム検疫（前のバージョンから変更なし）は、AsyncOS によって実施されるさまざまなアクション（フィルタリング、アンチウイルス スキャン、Outbreak フィルタなど）に基づいてメッセージを保管するために使用されます。

システム検疫

通常、メッセージはフィルタ アクションによってシステム検疫に入れられます。さらに、Outbreak フィルタ機能により、不審なメッセージは Outbreak 検疫に検疫されます。システム検疫は、メッセージを自動的に処理するように設定されています。つまり、メッセージは、送信先の検疫の設定（詳細については、「システム検疫の設定」（P.4-5）を参照）に基づいて配信または削除されます。自動化されたプロセスの他に、指定されたユーザ（メール管理者、人事担当部門、法務部門など）が検疫された内容を確認し、各メッセージの解放、削除、またはコピーの送信を実行することもできます。解放されたメッセージは、ウイルスに感染されていないかスキャンされます（その特定のメール ポリシーに対してアンチウイルスがイネーブルになっている場合）。

システム検疫は、次の目的に適しています。

- ポリシーの実施：メッセージが配信される前に、人事部門または法務部門がそれらに不快な情報や秘密情報が含まれていないか確認します。
- Virus 検疫：アンチウイルス スキャン エンジンによってスキャン不可能とマークされたメッセージ（または暗号化メッセージや感染メッセージなど）を保管します。

- Outbreak フィルタ機能のための基盤の提供：Outbreak フィルタ機能によってフラグが設定されているメッセージを、アンチウイルスまたはアンチスパム アップデートがリリースされるまで保管します。Outbreak フィルタ機能の詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Outbreak Filters」の章を参照してください。

Cisco IronPort アプライアンスには、ライセンスされている機能に応じていくつかの検疫が事前に設定されます。ただし、Policy 検疫は、ライセンスに関係なくデフォルトで作成されます。

- Outbreak：Outbreak フィルタ機能によって使用される検疫です。Outbreak フィルタ機能ライセンス キーが有効化されている場合に作成されます。
- Virus：アンチウイルス エンジンによって使用される検疫です。アンチウイルス ライセンス キーが有効化されている場合に作成されます。
- Policy：デフォルトの検疫です（たとえば、確認を必要とするメッセージを保管するためにこの検疫を使用します）。

その他の検疫を追加、変更、削除する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（GUI）を使用したシステム検疫の管理」（P.4-4）を参照してください。

システム検疫に対するアクセスおよび操作には、Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）または Command Line Interface（CLI; コマンドライン インターフェイス）の `quarantineconfig` コマンドを使用します。

（注）　システム検疫用の Command Line Interface（CLI; コマンドライン インターフェイス）では、GUI で使用可能な機能の一部が提供されます（『*Cisco IronPort AsyncOS CLI Reference Guide*』を参照）。

IronPort スパム検疫

AsyncOS は、スパムおよびその疑いのあるものを IronPort スパム検疫に送信するように設定できます。また、スパムおよびその疑いのあるメッセージが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、システムを設定することもできます。この通知には、IronPort スパム検疫に現在入っているそのユーザ宛のメッセージの要約が含まれます。ユーザは、メッセージを確認し、それらを自分の受信箱に配信するか、それとも削除するかを決定できます。また、検疫されているメッセージ全体を検索することもできます。ユーザはこの通知を利用

して検疫にアクセスできますが、Web ブラウザから直接アクセスすることもできます（この場合は認証が必要です。「エンド ユーザ検疫へのアクセスの設定」（P.4-36）を参照）。

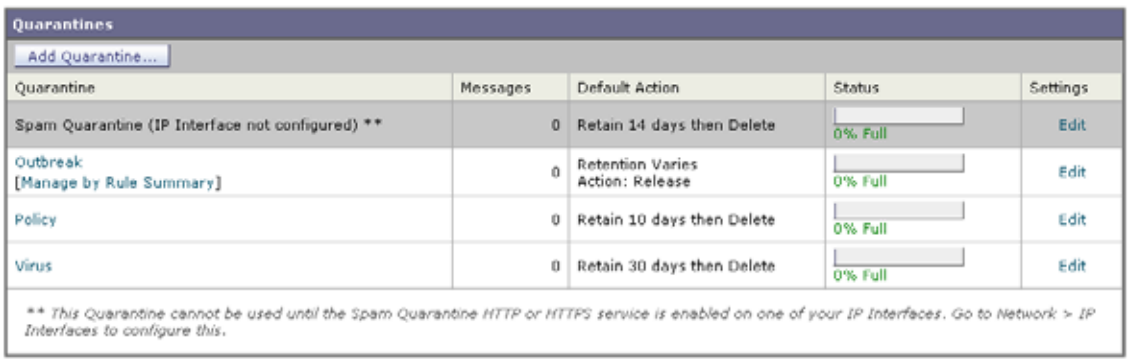
システムは、自己メンテナンスするように設定できます。つまり、検疫のスペースを使い果たすことがないように、定期的に IronPort スパム検疫からメールを自動削除します。IronPort スパム検疫は、エンド ユーザ宛のスパムおよびその疑いのあるメッセージを保管することを目的として使用されます。

IronPort スパム検疫の詳細については、「IronPort スパム検疫内のメッセージの管理」（P.4-52）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（GUI）を使用したシステム検疫の管理

Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）にログインし、[Monitor] タブをクリックします（GUI にアクセスする方法の詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Overview」を参照してください）。左側のメニューの [Quarantines] セクション内にある [Quarantines] リンクをクリックします。

図 4-1　[Quarantines] ページ



[Quarantines] ページには、すべての検疫について、それぞれに保管されているメッセージの数、デフォルト アクション（保存期間、およびその後の削除または解放の最終アクション）、使用率などの情報が表示されます。各設定（サイズ、保存期間、デフォルト アクション、オーバーフロー メッセージの処理方法、お

よび検疫に関連付けられているユーザ）は、[Edit] リンクを使用して編集できます（詳細については、「システム検疫の設定」（P.4-5）を参照してください）。また、関連するセキュリティ サービス（Virus 検疫の場合はアンチウイルス スキャン、Outbreak 検疫の場合は Outbreak フィルタ）がイネーブルにされているかどうか、各検疫の内容が現在使用可能かどうかなど、検疫のステータスも表示されます。

アプライアンス上で IronPort スパム検疫がイネーブルにされている場合は、IronPort スパム検疫も検疫のリストに表示されることに注意してください。この検疫はエンド ユーザ検疫です。エンド ユーザ検疫の使用方法の詳細については、「IronPort スパム検疫機能の設定」（P.4-27）を参照してください。

システム検疫の設定

検疫には、検疫設定に基づいてメッセージを処理する自動化されたプロセスが組み込まれています。検疫の日々の動作を決定するために、複数の設定が使用されます（スペース割り当て、保存期間、デフォルト アクション、オーバーフロー メッセージ、およびユーザ）。設定を変更した場合は、[Submit] ボタンをクリックし、必要に応じて省略可能なコメントを追加し、[Commit Changes] をクリックして変更を保存します。

システム検疫用のスペースの割り当て

システム検疫は Cisco IronPort アプライアンス自体に作成されるので、システム検疫に使用できるスペースは限られます。新しい検疫に使用可能なスペースは、[Manage Quarantines] ページに表示されます。検疫エリアのサイズが割り当てられているスペースに達すると、メッセージは検疫エリアから強制的に削除されます。詳細については、「システム検疫の設定」（P.4-5）を参照してください。

表 4-1　Cisco IronPort アプライアンス上で検疫に使用可能なスペース

Cisco IronPort アプライアンス	記憶域	Outbreak フィルタの記憶域*
X1050/1060/1070	10 GB	3 GB
C650/660/670	10 GB	3 GB
C350/360/370	4 GB	2 GB
C150/160	2.5 GB	1 GB

* Outbreak フィルタ機能をライセンスした場合の追加スペース

1 つの検疫の最小サイズは 250 MB です。

保存期間

保存期間とは、メッセージを検疫エリア内に保持する時間の長さです。検疫エリア内のメッセージは、その保存期間が経過すると、デフォルト アクション（「デフォルト アクション」（P.4-6）を参照）が実行されます。各メッセージには、それぞれ独自の有効期限があり、検疫のリストに表示されます。

メッセージは、メール管理者（または他のユーザ）によって手動で処理されるか、検疫に設定されたサイズ制限に達しない限り、指定された時間が経過するまで保管されます（通常の期限切れ）。サイズ制限に達すると、古いメッセージから処理されます（早期の期限切れ）。検疫エリアのサイズがサイズ制限未満に戻るまで、各メッセージに対してデフォルト アクションが実行されます。このポリシーは、First In First Out（FIFO; 先入れ先出し）です。検疫エリアのサイズ制限の指定方法の詳細については、「システム検疫の作成」（P.4-9）を参照してください。

メッセージの有効期限は、各種検疫のリスト内で [Select Action] メニューを使用して遅らせる（延長させる）ことができます。メッセージの有効期限を遅らせることは、スケジュールされた有効期限を越えて検疫エリア内の特定のメッセージを保持する必要がある場合に役立ちます（たとえば、管理者がメッセージを確認する時間を確保したり、特定のアンチウイルス IDE が公開されるまで延長したりします）。

（注） Outbreak フィルタ検疫でのメッセージの保存期間は、アプライアンスのメール ポリシーで設定されます。

デフォルト アクション

デフォルト アクションとは、次の 2 つの状況のいずれかが起こったときに、検疫エリア内のメッセージに対して実行されるアクションのことです。

- 通常の期限切れ：検疫エリア内のメッセージが保存期間を満了する場合です（「保存期間」（P.4-6）を参照）。
- 早期の期限切れ：検疫エリアのサイズ制限に達してメッセージが検疫エリアから強制的に削除される場合です。検疫エリアのサイズ制限を設定する方法の詳細については、「システム検疫の作成」（P.4-9）を参照してください。

キューが満杯状態のため検疫エリアから解放されるメッセージ（早期の期限切れ）に対しては、他の操作を実行することもできます。詳細については、「[When Allocated Space is Exceeded Send Messages and:]」（P.4-7）を参照してください。

デフォルト アクションは 2 つあります。

- Delete：メッセージが削除されます。
- Release：メッセージが解放されて配信されます。解放時、メッセージは、その特定のメール ポリシーに対してアンチウイルスがイネーブルになっていれば、ウイルスに感染していないか再スキャンされます。ウイルス スキャンおよび検疫エリアから解放されるメッセージの詳細については、「システム検疫とウイルス スキャン」（P.4-24）を参照してください。

（注） 検疫されたメッセージのリスト内では、これら 2 つのデフォルト アクションに加え、第 3 のメッセージ アクション（Delay Exit）を [Select Action] メニューから利用できます。

[When Allocated Space is Exceeded Send Messages and:]

[When Allocated Space is Exceeded Send Messages and:] セクションは、メッセージがオーバーフローによって検疫エリアから解放されるとき、それらをどのように処理するかを指定するために使用します。これらの設定には、件名のタグ付け、X-Header の追加、添付ファイルの削除などがあります。

件名のタグ付け

キューが満杯状態のため検疫エリアから解放または削除されるメッセージには（早期の期限切れのみ）、検疫を編集または作成した際に指定したテキストでそれらの件名にタグを付けられます。

タグは、ユーザ定義の文字列であり、元の件名ヘッダーの前または後ろに追加できます。

（注） 非 ASCII 文字を含む件名を正しく表示するために、件名は RFC 2047 に従って表記されている必要があります。

X-Header の追加

キューが満杯状態のため検疫エリアから解放または削除されるメッセージには（早期の期限切れのみ）、X-Header を追加できます。

X-Header の名前および値を指定します。

添付ファイルの削除

キューが満杯状態のため検疫エリアから解放または削除されるメッセージに対し（早期の期限切れのみ）、それらに付属する添付ファイルを削除できます。これは、ウイルスに感染したファイルが検疫エリアから解放される可能性を低減するために使用できます。

システム検疫のパフォーマンス

システム検疫に保管されているメッセージは、ハード ドライブ領域に加えてシステム メモリを使用します。1 つのアプライアンス上のシステム検疫に数 10 万のメッセージを保管すると、過剰なメモリ使用のために、そのアプライアンスのパフォーマンスが低下することがあります。アプライアンスでのメッセージの検疫、削除、および解放により多くの時間が必要になるため、メッセージ処理の速度が低下し、電子メール パイプラインが渋滞します。

電子メール セキュリティ アプライアンスが通常の速度で電子メールを処理できるようにするために、システム検疫に保管するメッセージの数を平均で 20,000 未満にすることを推奨します。

ユーザおよびユーザ グループ

Administrators グループに属するユーザは、デフォルトで検疫にアクセスできます。Operators、Guests、Read-Only Operators、および Help Desk Users グループに属するユーザのほか、検疫アクセス権限を持つカスタム ユーザ ロールは、検疫に割り当てできますが（それにより、検疫エリア内のメッセージの表示、処理、検索が可能になります）、検疫の設定（サイズ、保存期間など）を変更したり、検疫を作成または削除したりできません。Technicians グループに属するユーザは検疫にアクセスできません。

システム検疫の作成

新しいシステム検疫を作成してメッセージを保管できます。検疫を設定するための基本的なワークフローは次のとおりです。

1. 検疫にアクセスするユーザを作成します。
   a. **ローカル ユーザ。**検疫のユーザ リストには、Administrators 以外のすべてのユーザ グループ内のローカル ユーザが入ります。Administrators グループ内のユーザは、常に検疫に対してすべてのアクセス権限を持ちます。詳細については、「ユーザ アカウントを使用する作業」（P.8-18）を参照してください。
   b. **外部ユーザ。**また、Cisco IronPort アプライアンスが外部ディレクトリを使用してユーザを認証し、検疫にアクセスできるユーザ グループを選択できるようにすることもできます。詳細については、「外部認証」（P.8-35）を参照してください。
   c. **委任管理者。**検疫アクセス権限を持つカスタム ユーザ ロールを作成し、検疫の委任管理者として機能するローカル ユーザをそのグループに割り当てることができます。詳細については、「委任管理のためのカスタム ユーザ ロールの管理」（P.8-44）を参照してください。
2. 後述の手順に従って、検疫を作成します。
3. メッセージを検疫エリアに移動するフィルタを作成します。フィルタの作成方法の詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Email Security Manager」および『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Using Message Filters to Enforce Email Policies」を参照してください。

システム検疫を作成するには、次の手順を実行します。

ステップ 1　[Quarantines] ページで [Add Quarantine] をクリックします。[Add Quarantine] ページが表示されます。

ステップ 2　検疫の名前を入力します。

ステップ 3　検疫に割り当てるスペース（単位は MB）を指定します。詳細については、「システム検疫用のスペースの割り当て」（P.4-5）を参照してください。

ステップ 4　保存期間（メッセージに対してデフォルト アクションが実行される前にメッセージを保持する時間）を選択します。詳細については、「保存期間」（P.4-6）を参照してください。

ステップ 5　デフォルト アクションを選択します（[Delete] または [Release]）。

ステップ 6　検疫によって処理されるメッセージの件名を変更する場合は、追加するテキストを入力し、そのテキストを元のメッセージの件名の前と後ろのどちらに追加するかを選択します。詳細については、「件名のタグ付け」（P.4-7）を参照してください。

ステップ 7　X-Header を追加する場合は、名前と値を入力します。詳細については、「X-Header の追加」（P.4-8）を参照してください。

ステップ 8　オーバーフローのためファイルが検疫エリアから解放されるとき（早期の解放）、そのファイルの添付ファイルを削除する場合は、[On] を選択します。詳細については、「添付ファイルの削除」（P.4-8）を参照してください。

ステップ 9　[Local Users] リンクをクリックし、検疫にアクセスできるようにするユーザのチェックボックスをオンにすることによって、この検疫にアクセスするユーザを選択します。検疫のユーザ リストには、Administrators と Technicians を除く、すべてのユーザ グループ内のローカル ユーザが含まれます。Administrators グループ内のユーザには常に、検疫へのフル アクセスが与えられ、Technicians グループ内のユーザは検疫にアクセスできません。詳細については、「ユーザおよびユーザ グループ」（P.4-8）を参照してください。このリンクは、まだユーザを作成していない場合は使用できません。

ステップ 10　必要に応じて、[Externally Authenticated Users] のリンクをクリックし、この検疫にアクセスする外部認証ユーザのユーザ ロールのチェックボックスをオンにします。外部認証ユーザは、集中管理された認証システムを使用して Cisco IronPort アプライアンスによって認証されます。詳細については、「外部認証」（P.8-35）を参照してください。

ステップ 11　必要に応じて、委任管理者がこの検疫にアクセスできるようにする場合は [Custom User Roles] のリンクをクリックします。検疫アクセス権限を持つカスタム ユーザ ロールのチェックボックスをオンにして、[OK] をクリックします。詳細については、「委任管理のためのカスタム ユーザ ロールの管理」（P.8-44）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。

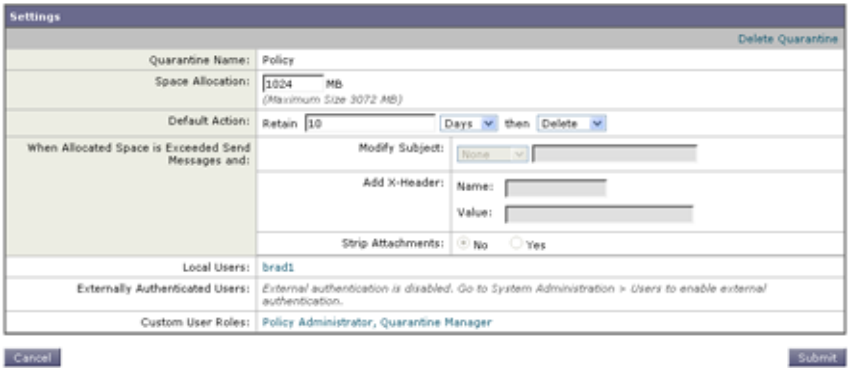
システム検疫の編集

検疫を編集できるのは、Administrators グループに属するユーザだけです。

既存の検疫を編集するには、次の手順を実行します。

ステップ 1　変更する検疫に対して [Settings] カラム内の [Edit] リンクをクリックします。[Edit Quarantine] ページが表示されます。

図 4-2　システム検疫の編集



ステップ 2　検疫の設定を変更します。

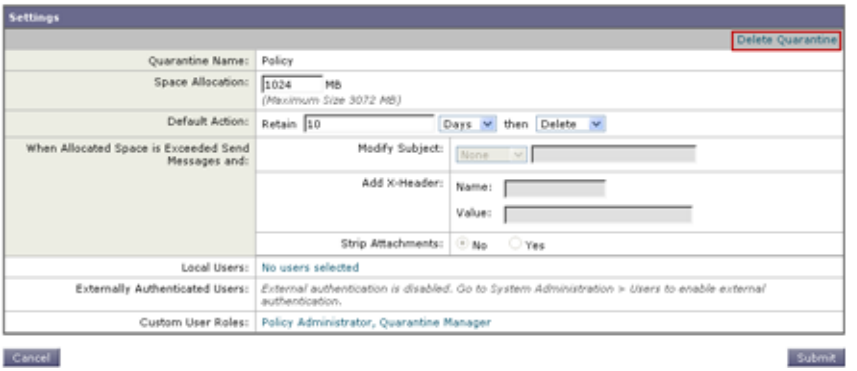
ステップ 3　変更を送信し、保存します。

システム検疫の削除

既存の検疫を削除するには、次の手順を実行します。

ステップ 1　[Edit Quarantine] ページ内の [Delete Quarantine] リンクをクリックします。

図 4-3　システム検疫の削除



ステップ 2　確認メッセージが表示されます。

図 4-4　システム検疫の削除の確認

ステップ 3　[Delete] をクリックします。検疫が削除されます。

ステップ 4　変更を保存します。

システム検疫内のメッセージの操作

[Quarantine Overview] を使用して、検疫エリア内のメッセージを操作します。検疫にアクセスできるユーザの場合、次の作業を実行できます。

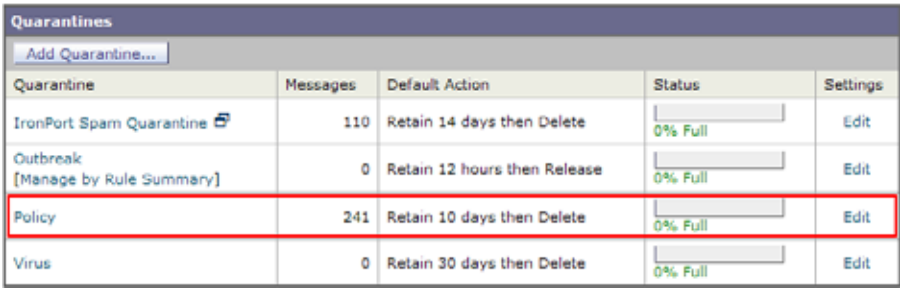
- 検疫エリア内のメッセージの表示
- メッセージに対するメッセージ アクションの実行（メッセージの処理）
- メッセージの添付ファイルのダウンロード
- 検疫エリア内のメッセージの検索

（注）　ここで説明される機能は、GUI にのみ当てはまります。

システム検疫内のメッセージの表示

[Local Quarantine] ページを使用して、検疫エリア内にメッセージが入っているかどうかを確認します。次の例では、Policy 検疫に 241 件のメッセージが入っています。

図 4-5　ローカル検疫



検疫の名前をクリックして、検疫エリア内のメッセージを表示します。このページから、特定のメッセージを表示したり、1 つまたは複数のメッセージを処理したり、メッセージ全体を検索したりできます。

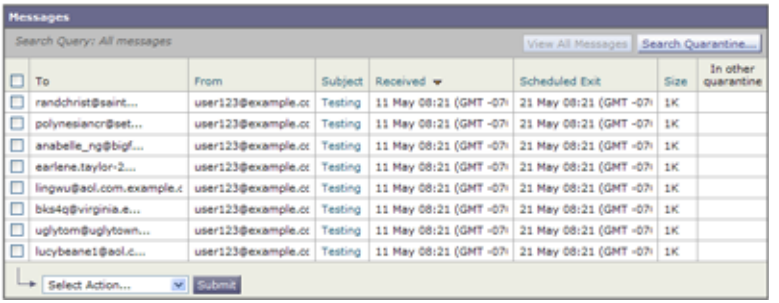
検疫エリア内のメッセージの処理

メッセージは、自動（通常または早期の期限切れ）または手動のいずれかで検疫エリアから除去（配信または削除）できます。

手動でメッセージを処理する場合は、[Message Actions] ページからメッセージのメッセージ アクションを手動で選択します。

[Quarantine Overview] ページで検疫名をクリックして、検疫エリア内のメッセージを表示します。

図 4-6　検疫エリア内のメッセージのリストの表示



検疫エリア内のすべてのメッセージが一覧表示されます。各メッセージには、宛先、差出人、件名、受信日時、スケジュールされた保存期間の終了日時、サイズ、および「他の検疫に含まれるかどうか」が表示されます。[Previous]、[Next]、ページ番号、または二重矢印のリンクを使用して、リストの各ページを移動できます。二重矢印を使用すると、リストの先頭（[<<]）または最後（[>>]）のページに移動します。

あるメッセージが他の 1 つまたは複数の検疫エリア内にも存在している場合、それらの検疫にアクセスできるかどうかに関係なく、そのメッセージの [In other quarantines] カラムに [Yes] が表示されます。詳細については、「マルチユーザアクセスと複数の検疫エリア内のメッセージ」（P.4-22）を参照してください。

カラム見出しをクリックすることにより、そのカラムの内容の昇順または降順に結果をソートします（[In other quarantines] カラムは除く）。

リストの左側にあるチェックボックスの列から対応するチェックボックスをクリックすることにより、メッセージを選択できます。リストに現在表示されているすべてのメッセージを選択するには、見出し内の [All] ボックスをマークします（リストの一番上。先頭メッセージよりも上）。これは、現在表示されているメッセージにだけ適用されることに注意してください。現在のページに表示されていないメッセージは影響を受けません。

リスト内で選択したすべてのメッセージに対してアクション（[Delete]、[Release]、[Delay Scheduled Exit]）を適用できます。リストの下部にあるプルダウン メニューからアクションを選択し、[Submit] をクリックします。選択内容を確認するダイアログボックスが表示されます。[Yes] をクリックして、マークされたすべてのメッセージに対してアクションを実行します。

Outbreak 検疫の [Manage Rule by Summary] リンクをクリックして、Outbreak 検疫エリア内のメッセージをルールに従って処理します。詳細については、「Outbreak フィルタ機能と Outbreak 検疫」（P.4-25）を参照してください。

検疫されたメッセージおよび国際文字セット

メッセージの件名に国際文字セット（2 バイト、可変長、および非 ASCII の符号化）の文字が含まれる場合、[System Quarantine] ページでは、非 ASCII 文字の件名行が復号化された形式で表示されます。

メッセージ アクションおよびメッセージ内容の表示

メッセージの内容を表示したり、[Quarantined Message] ページにアクセスしたりするには、メッセージの件名行をクリックします。

図 4-7　[Quarantined Message] ページ

[Quarantined Message] には、[Quarantine Details] と [Message Details] の 2 つのセクションがあります。

[Quarantined Message] ページから、メッセージを読んだり、メッセージ アクションを選択したり、メッセージのコピーを送信したり、ウイルス検査を実行したりできます。また、メッセージが検疫エリアから解放されるときに Encrypt on Delivery フィルタ アクションによって暗号化されるかどうかを確認することもできます。

[Message Details] セクションには、メッセージ本文、メッセージ ヘッダー、および添付ファイルが表示されます。メッセージ本文は最初の 100 KB だけが表示されます。メッセージがそれよりも長い場合は、最初の 100 KB が表示され、その後に省略記号（...）が続きます。実際のメッセージが切り捨てられることはありません。この処置は表示目的のためだけに行われます。[Message Details] の下部にある [Message Parts] セクション内の [message body] をクリックすることにより、メッセージ本文をダウンロードできます。また、添付ファイルのファイル名をクリックすることにより、メッセージの任意の添付ファイルをダウンロードすることもできます。

ウイルスの含まれるメッセージを表示する場合、ご使用のコンピュータにデスクトップ アンチウイルス ソフトウェアがインストールされていると、そのアンチウイルス ソフトウェアから、ウイルスが検出されたと警告される場合があります。これは、ご使用のコンピュータに対して脅威ではないため、無視しても問題ありません。

（注） 特別な Outbreak 検疫の場合、追加の機能を利用できます。詳細については、「Outbreak フィルタ機能と Outbreak 検疫」（P.4-25）を参照してください。

一致した内容の表示

Attachment Content 条件、Message Body または Attachment 条件、Message 本文条件、または Attachment 内容条件と一致するメッセージに対して検疫アクションを設定した場合、検疫されたメッセージ内の一致した内容を表示できます。メッセージ本文を表示する場合、DLP ポリシー違反の一致を除き、一致した内容が黄色で強調表示されます。また、`$MatchedContent` アクション変数を使用して、メッセージの一致した内容やコンテンツ フィルタの一致をメッセージの件名に含めることもできます。

一致した内容が添付ファイルに含まれる場合は、その判定結果が DLP ポリシー違反、コンテンツ フィルタ条件、メッセージ フィルタ条件、または画像解析のいずれによるものかに関係なく、添付ファイルの内容がその検疫理由とともに表示されます。

メッセージ フィルタまたはコンテンツ フィルタのルールをトリガーしたローカル検疫内のメッセージを表示すると、フィルタ アクションを実際にはトリガーしなかった内容が（フィルタ アクションをトリガーした内容とともに）GUI で表示されることがあります。GUI 表示は、内容の一致箇所を特定する際のガイドラインとして使用されますが、内容の一致リストを正確に反映しているとは限りません。これは、GUI で使用される内容一致ロジックが、フィルタで使用されるものほど厳密ではないため起こります。この問題は、メッセージ本文内での強調表示に対してのみ当てはまります。メッセージの各パート内の一致文字列をそれに対応するフィルタ ルールとともに一覧表示するテーブルは正しく表示されます。

[Message Parts] または [Matched Content] セクション内の添付ファイルのファイル名をクリックすることにより、メッセージの添付ファイルをダウンロードできます。AsyncOS から、未知の送信元からの添付ファイルにはウイルスが含まれる可能性があることを示す警告が表示され、続行するかどうか尋ねられます。[Message Parts] セクション内の [message body] をクリックすることにより、メッセージ本文をダウンロードすることもできます。

図 4-8　Policy 検疫エリア内で表示された一致内容

メッセージ アクションの選択

使用可能なアクションは、メッセージの削除、メッセージの解放、および有効期限の延長の 3 種類あります。詳細については、「デフォルト アクション」（P.4-6）を参照してください。

ステップ 1　対象となるメッセージのボックスをマークします。

ステップ 2　[Select Action] メニューからアクションを選択します。

ステップ 3　[Submit] をクリックします。

（注）　メッセージは、複数の検疫に入れられる場合があります。複数の検疫に属しているメッセージの処理方法の詳細については、「マルチユーザ アクセスと複数の検疫エリア内のメッセージ」（P.4-22）を参照してください。

メッセージのコピーの送信

メッセージのコピーは、Administrators グループに属しているユーザだけが送信できます。

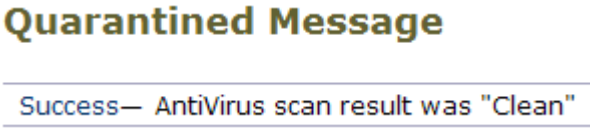
メッセージのコピーを送信するには、[Send Copy To:] フィールドに電子メールアドレスを入力し、[Submit] をクリックします。メッセージのコピーを送信しても、そのメッセージに対してその他のアクションが実行されることはありません。

ウイルスの検査

メッセージがウイルスに感染していないかどうかを検査するには、[Start Test] をクリックします。アンチウイルス シグニチャが最新のものであることを確認できるまで、メッセージの保管に検疫を使用します。

ウイルスの検査では、オリジナルのメッセージではなく、メッセージのコピーがアンチウイルス エンジンに送信されます。アンチウイルス エンジンの判定結果は、[Quarantines] エリアの上に表示されます。

図 4-9　　ウイルス スキャンの結果



添付ファイルのダウンロード

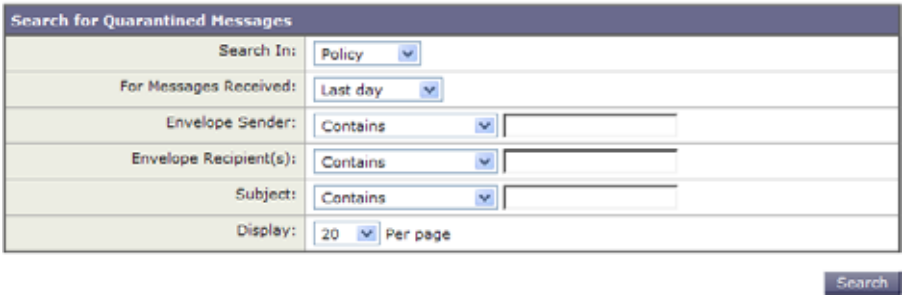
添付ファイルをダウンロードするには、[Matched Content] または [Message Parts] セクション内にある添付ファイルのファイル名をクリックします。AsyncOS から、未知の送信元からの添付ファイルにはウイルスが含まれる可能性があることを示す警告が表示され、続行するかどうか尋ねられます。

システム検疫の検索

1 つまたは複数の特定のメッセージについて検疫を検索するには、次の手順を実行します。

ステップ 1　[Quarantines] ページ内にある検疫の名前をクリックします。[**Search Quarantine**] をクリックします。[Search Quarantine] ページが表示されます。

図 4-10　検疫の検索



ステップ 2　検索基準を入力します。

- [Search in]：検索対象の検疫を選択します。
- [For messages received by]：タイム フレームを選択します。
- [Envelope Sender]：[contains]、[starts with]、[ends with]、[matches exactly]、またはそれらの「does not」版を選択し、テキストを入力します。
- [Envelope Recipient(s)]：[contains]、[starts with]、[ends with]、[matches exactly]、またはそれらの「does not」版を選択し、テキストを入力します。
- [Subject]：[contains]、[starts with]、[ends with]、[matches exactly]、またはそれらの「does not」版を選択し、テキストを入力します。
- [Display]：1 ページに表示する行数を選択します。

（注）　実行される検索は「AND」検索です。検索フィールドに指定されたすべての基準を満たす結果だけが返されます。たとえば、検索フィールドで [Envelope Recipient] と [Subject] を指定すると、[Envelope Recipient] に指定した項目と [Subject] に指定した項目の両方に一致するメッセージだけが返されます。

ステップ 3　[Search] をクリックします。

ステップ 4　結果（指定されたすべての基準に一致するメッセージ）が表示されます。

これらの検索結果は、検疫のリストを使用するのと同様に使用できます。また、検索結果のリストは、スケジュールされた保存期間の終了日時で並べ替えることもできます。詳細については、「検疫エリア内のメッセージの処理」（P.4-13）を参照してください。

マルチユーザ アクセスとシステム検疫

AsyncOS では、検疫管理の委任がサポートされており、Operators、Help Desk Users、および Guests グループのユーザのほか、検疫アクセス権限を持つカスタム ユーザ ロールのユーザが検疫内のメッセージを処理するように指定できます。

次の例を参考にしてください。

- 人事部門のチームによる Policy 検疫の確認と管理
- 法務部門のチームによる Confidential Material 検疫の管理

検疫にアクセスできるこれらのユーザは、その検疫内のメッセージを検索したり、その検疫のメッセージの処理（解放または削除、あるいはその両方）を行ったりすることができます。

マルチユーザ アクセスの設定

検疫にユーザを追加するには、追加するユーザがすでに存在している必要があります。ユーザとユーザ ロールの作成の詳細については、「ユーザ アカウントを使用する作業」（P.8-18）および「Cloud Guest」（P.8-44）を参照してください。

各ユーザは、すべてまたは一部の検疫にアクセスできるようにすることも、まったくアクセスできないようにすることもできます。検疫の閲覧を許可されていないユーザに対しては、GUI または CLI の検疫のリスト表示で、その検疫の存在を示す記録は一切表示されません。

マルチユーザ アクセスと複数の検疫エリア内のメッセージ

複数の検疫エリア内に存在するメッセージは、すべての検疫エリアから解放されなければ検疫からの解放が許可されないという意味で「保守的な」ポリシーで制御されます。

1 つのメッセージが複数の検疫エリア内に存在する場合、検疫エリアからメッセージを解放しても、そのメッセージが配信されるとは限りません。メッセージは先に、自身が存在するすべての検疫エリアから解放される必要があります。

複数の検疫エリア内に存在するメッセージは、特定の検疫エリアから削除されても、他の検疫エリア内には存在したままになります。この時点で他の検疫エリアからメッセージを解放しても、そのメッセージは配信されません。

メッセージは複数の検疫エリアに存在できますが、そのメッセージを解放しようとするユーザはそれらの検疫の一部にしかアクセスできない場合があるため、次のルールが適用されます。

- メッセージは、自身が存在するすべての検疫エリアから解放されるまで、どの検疫エリアからも解放されません。
- メッセージは、いずれかの検疫エリア内で削除済みとマークされると、他の検疫エリアからも配信できなくなります。解放はできますが、配信されません。

したがって、メッセージが複数の検疫エリア内にキューイングされ、ユーザがそのうちの 1 つまたは複数の検疫にアクセスできない場合は、次のことが起こります。

- ユーザは、ユーザがアクセスできる各検疫についてそのメッセージが存在するかどうか通知されます。
- GUI は、ユーザがアクセスできる検疫のスケジュールされた保存期間の終了日時のみを表示します（同じメッセージに対して、検疫ごとに別々の終了日時が存在します）。
- GUI は、そのメッセージが他の検疫にも保管されているかどうかを表示します。

図 4-11　検疫の検索

- ユーザは、そのメッセージを保管している他の検疫の名前を知らされません。
- メッセージの解放は、ユーザがアクセスできるキューにだけ効果があります。

- ユーザがアクセスできない他の検疫エリアにもメッセージがキューイングされている場合、残りの検疫にアクセスできるユーザによって処理されるまで（あるいは早期または通常の期限切れによって「正常に」解放されるまで）、そのメッセージは変更されずに検疫エリア内に残ります。

システム検疫とウイルス スキャン

検疫が行われたすべてのキューから配信に向けて解放されたメッセージは、配信が許可される前に、ウイルスやスパムに感染していないかどうか再スキャンされます（そのメール ポリシーに対してアンチウイルスおよびスパムがイネーブルになっている場合）。

メッセージは、検疫エリアから解放されるとき、アンチウイルスおよびスパム エンジンによってウイルスやスパムに感染していないかどうかスキャンされます（アンチウイルスがイネーブルになっている場合）。判定結果が前回そのメッセージを処理したときの判定結果と一致する場合、そのメッセージは再検疫されません。逆に、判定が異なると、そのメッセージは別の検疫に送信される可能性があります。

原理的に、メッセージの検疫が無限に繰り返されることはないようになっています。たとえば、メッセージが暗号化されていて、その結果、Virus 検疫に送信されるとします。管理者がそのメッセージを解放しても、アンチウイルス エンジンはまだそのメッセージを復号化できません。しかし、そのメッセージは再検疫されない必要があります。再検疫されるとループ状態となり、そのメッセージは検疫エリアからまったく解放されなくなります。2 回とも判定は同じ結果になるので、システムは 2 回めには Virus 検疫を無視します。

システム検疫とアラート

検疫エリアの容量が 75% 以上および 95% 以上になると、アラートが送信されます。このチェックは、メッセージが検疫エリアに入れられたときに実行されます。したがって、メッセージが Policy 検疫に追加されたとき、検疫エリアのサイズが指定容量の 75% 以上に増加すると、次のようなアラートが送信されます。

```
Warning: Quarantine "Policy" is 75% full
```

アラートの詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「System Administration」を参照してください。

システム検疫とロギング

AsyncOS により、検疫されるすべてのメッセージが個別にロギングされます。

```
Info: MID 482 quarantined to "Policy" (message
filter:policy_violation)
```

括弧内には、メッセージを検疫させたメッセージ フィルタまたは Outbreak フィルタ機能のルールが出力されます。メッセージが入れられる検疫ごとに独立したログ エントリが生成されます。

また、AsyncOS により、検疫エリアから除去されるメッセージも個別にロギングされます。

```
Info: MID 483 released from quarantine "Policy" (queue full)
```

```
Info: MID 484 deleted from quarantine "Anti-Virus" (expired)
```

メッセージがすべての検疫エリアから除去され、完全に削除されるか、配信用にスケジュールされると、それらのメッセージはシステムによって次のように個別にロギングされます。

```
Info: MID 483 released from all quarantines
```

```
Info: MID 484 deleted from all quarantines
```

メッセージが再注入されると、新しい MID を持つ新しいメッセージ オブジェクトがシステムによって作成されます。このことは、次のように「署名入り」の新しい MID を伴う既存のログ メッセージを使用してロギングされます。

```
Info: MID 483 rewritten to 513 by System Quarantine
```

Outbreak フィルタ機能と Outbreak 検疫

Outbreak 検疫は、Outbreak フィルタ機能の有効なライセンス キーが入力されている場合に存在します。Outbreak フィルタ機能では、しきい値セットに従ってメッセージが Outbreak 検疫に送信されます。詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Outbreak Filters」の章を参照してください。

Outbreak フィルタ機能のライセンスの有効期限が切れると、メッセージを Outbreak 検疫にそれ以上追加できなくなります。検疫エリア内に現在存在するメッセージの保存期間が終了して Outbreak 検疫が空になると、GUI の検疫リストに Outbreak 検疫は表示されなくなります。

Outbreak 検疫は、他の検疫と同様の機能を持ち、メッセージを検索したり、メッセージを解放または削除したりできます。Outbreak 検疫に入れられたメッセージは、新しく公開されたルールによってもう脅威ではないと見なされると、自動的に解放されます。

Outbreak 検疫には、他の検疫では使用できない追加の機能があります（[Manage by Rule Summary] リンク、メッセージの詳細を表示しているときの IronPort への送信機能、およびスケジュールされた保存期間の終了日時でソート結果内のメッセージを並べ替えるオプション）。

アプライアンス上でアンチスパムおよびアンチウイルスがイネーブルになっている場合、スキャン エンジンは、メッセージに適用されるメール フロー ポリシーに基づいて、Outbreak 検疫から解放されたすべてのメッセージをスキャンします。

[Manage by Rule Summary] リンク

検疫リストで Outbreak 検疫の横にある [Manage by Rule Summary] リンクをクリックして、[Manage by Rule Summary] ページを表示します。検疫エリア内のすべてのメッセージに対し、それらのメッセージを検疫させた感染防止ルールに基づいてメッセージ アクション（Release、Delete、Delay Exit）を実行できます。これは、Outbreak 検疫から大量のメッセージを片付ける場合に適しています。詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Outbreak Filters」の章を参照してください。

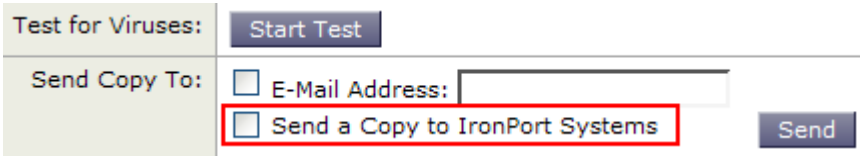
IronPort への送信

Outbreak 検疫内のメッセージについてメッセージの詳細を表示しているとき、そのメッセージを Cisco IronPort に報告することもできます。これは、偽陽性を報告する場合または不審なメッセージを Cisco IronPort に報告する場合に行います。

メッセージのコピーを Cisco IronPort に送信するには、次の手順を実行します。

ステップ 1　[Message Details] ページで、[Send a Copy to IronPort Systems] ボックスをマークします。

図 4-12　検疫の検索



ステップ 2　[Send] をクリックします。メッセージのコピーが IronPort システムに送信されます。

IronPort スパム検疫機能の設定

各 Cisco IronPort アプライアンスでは、IronPort アンチスパムがイネーブルになっている場合、ローカルの IronPort スパム検疫をイネーブルにすることができます。また、各 Cisco IronPort アプライアンスは、外部の IronPort スパム検疫を参照することもできます。この検疫は、別の Cisco IronPort アプライアンス上で設定されます（通常は M-Series アプライアンス。詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「The Cisco IronPort M-Series Security Management Appliance」の章を参照してください）。

なお、ローカルと外部の両方の IronPort スパム検疫がイネーブルになっている場合、*ローカルの IronPort スパム検疫が使用されます。*

スパムまたはその疑いのあるメッセージを IronPort スパム検疫（ローカルまたは外部）に送信するように、Cisco IronPort アプライアンスを設定するには、次の手順に従います。

ステップ 1　外部の IronPort スパム検疫を追加するか（「外部の IronPort スパム検疫の設定」（P.4-40）を参照）、ローカルの IronPort スパム検疫をイネーブルにして設定します（「ローカルの IronPort スパム検疫の設定」（P.4-33）を参照）。ローカルの IronPort スパム検疫を設定する場合、検疫のアクセス / 内容 / 動作、通知、認証、および AsyncOS ユーザ アクセスに関連した設定を指定できます。

ステップ 2　ローカルの IronPort スパム検疫を設定する場合は、IP インターフェイスを編集し、IronPort スパム検疫の HTTP または HTTPS サービスをイネーブルにします（「IP インターフェイス上での IronPort スパム検疫 HTTP/S サービスのイネーブル化」（P.4-42）を参照）。IronPort スパム検疫の HTTP/S サービスをイネーブルにすると、その検疫にアクセスできるようになります。

ステップ 3　ローカルの IronPort スパム検疫から外部の IronPort スパム検疫に移行する場合は、アンチスパム設定を設定し、より短い有効期限を設定し、ローカル検疫内に残っているすべてのメッセージを削除します（「ローカルの IronPort スパム検疫から外部の検疫への移行」（P.4-30）を参照）。

ステップ 4　スパムまたはその疑いのあるメッセージ（または両方）を IronPort スパム検疫に送信するように、ポリシーのアンチスパム スキャン オプションを設定します（「メール ポリシーの IronPort スパム検疫のイネーブル化」（P.4-44）を参照）。この手順は、スパムまたはその疑いのあるメッセージを検疫するように、システムを実際に設定する場合のものです。

ステップ 5　「導入上の考慮事項」（P.4-45）を参照してください。この重要な項には、通知、認証、関連する他の AsyncOS 機能の設定など、IronPort スパム検疫に関する追加のガイダンスと情報が豊富に提供されています。

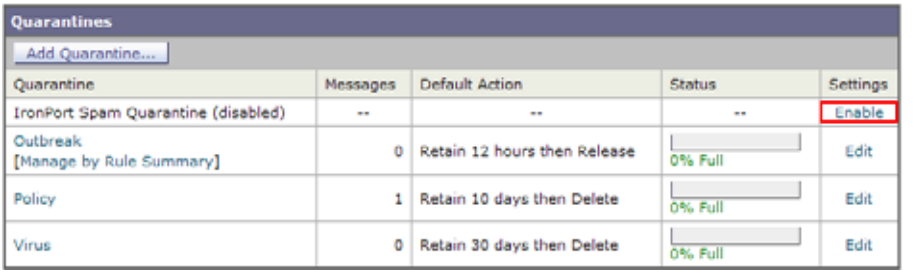
ローカルの IronPort スパム検疫のイネーブル化とディセーブル化

ローカルの IronPort スパム検疫をイネーブルにすると、AsyncOS は、外部の IronPort スパム検疫が設定されても、ローカルの IronPort スパム検疫を使用します。

ローカルの 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　[Monitor] > [Quarantines] ページで、[Enable] をクリックします。

図 4-13　ローカルの IronPort スパム検疫のイネーブル化



ステップ 2　IronPort スパム検疫がイネーブルになります。IronPort スパム検疫が設定されていない場合は、[Edit IronPort Spam Quarantine] ページが表示されます（「ローカルの IronPort スパム検疫の設定」（P.4-33）を参照）。

ステップ 3　変更を送信し、保存します。

ローカルの IronPort スパム検疫のディセーブル化

ローカルの 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（M-Series アプライアンス上では使用できません）。

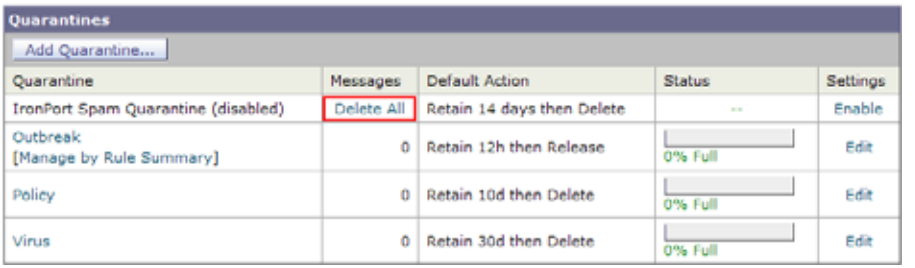
ステップ 1　[Monitor] > [Quarantines] ページで、IronPort スパム検疫の [Settings] カラム内の [Edit] をクリックします。

ステップ 2　[Spam Quarantine Settings] セクション内で、[Enable IronPort Spam Quarantine] のチェックボックスをオフにします。

ステップ 3　変更を送信し、保存します。

ローカルの IronPort スパム検疫がディセーブルになっているとき、その検疫エリア内にメッセージが存在する場合は、[Quarantines] ページの [Delete All] リンクを使用してすべてのメッセージを削除することもできます。

図 4-14　[Quarantines] ページの [Delete All] リンク



（注）　[Delete All] リンクは、Cisco IronPort M-Series アプライアンス上では使用できません。M-Series アプライアンス上の IronPort スパム検疫からすべてのメッセージを取り除くには、その検疫エリアへのスパムの送信を停止し、検疫されているメッセージが期限切れになるのを待ちます。

ディセーブルにされた IronPort スパム検疫とメール ポリシー

IronPort スパム検疫がディセーブルにされると、スパムまたはその疑いのあるメッセージを検疫するように設定されたメール ポリシーは、メッセージを配信するように設定が変更されます。

ローカルの IronPort スパム検疫から外部の検疫への移行

ローカルの Cisco IronPort C- または X-Series アプライアンス上で現在使用中のローカルの IronPort スパム検疫を、そのローカル検疫内のメッセージにアクセスできるようにしたまま、Cisco IronPort M-series アプライアンスをホストとする外部の IronPort スパム検疫に移行する場合は、次の戦略の使用を検討します。

- アンチスパム設定の設定：M-Series アプライアンスを代替ホストとして指定して、メール ポリシーにアンチスパム設定を設定します。この処置により、ローカル検疫にアクセス可能なまま、新しいスパムは外部の検疫に送信されます。
- より短い有効期限の設定：ローカル検疫に対して Schedule Delete After 設定をより短い期間に設定します。

- 残っているすべてのメッセージを削除：ローカル検疫内に残っているすべてのメッセージを削除するには、その検疫をディセーブルにし、ローカル検疫のページで [Delete All] リンクをクリックします（「IronPort スパム検疫からのメッセージの削除」（P.4-55）を参照）。このリンクは、まだメッセージが残っているローカルの IronPort スパム検疫がディセーブルになっているときにだけ使用可能になります。

これで、移行中に新しいメッセージがローカル検疫に入らないようにしながら、ローカル検疫のディセーブル化と外部の検疫のイネーブル化をできるようになります。

IronPort スパム検疫の設定

スパム検疫の設定

検疫サイズ、削除/保存ポリシー、デフォルト言語、および IronPort 通知のイネーブル化またはディセーブル化を設定します。デフォルトでは、ローカルの IronPort スパム検疫は自己管理型になっています。つまり、この検疫がイネーブルになると、設定された期間後にスパムが自動的に削除されます。検疫エリアが満杯になった場合は、古いスパムから削除されます。IronPort スパム検疫の外観および動作は、カスタム ロゴやログイン ページ メッセージの指定も含め、設定およびカスタマイズできます。「ローカルの IronPort スパム検疫用のスパム検疫設定」（P.4-33）を参照してください。

ローカルの IronPort スパム検疫内にあるメッセージを表示したり、操作したりする AsyncOS Operator ユーザを指定します。AsyncOS に作成されたすべての Administrator レベルのユーザ（デフォルトの「admin」ユーザなど）は、IronPort スパム検疫に対して自動的にアクセスおよび変更できるようになります。Operator は、検疫の内容を表示できますが、検疫の設定を変更できない場合があります。「IronPort スパム検疫の管理ユーザの設定」（P.4-35）を参照してください。

IronPort スパム検疫へのアクセス

各エンド ユーザが IronPort スパム検疫内にある自分宛のメッセージを Web ブラウザからじかにアクセスおよび管理することを許可します。アクセスを許可されたユーザは、スパム通知を受信したかどうかに関係なく、検疫エリアからメッセージを表示、検索、解放、および削除できるようになります。メッセージ本文を表示するか、非表示にするかを指定します。使用されるエンド ユーザ認証を

指定できます（LDAP、Active Directory、IMAP/POP、またはなし）。「エンドユーザ検疫へのアクセスの設定」（P.4-36）を参照してください。「なし」を指定すると、エンド ユーザは、通知メッセージに含まれるリンク経由でしか IronPort スパム検疫にアクセスできなくなり、認証は使用されなくなります（ユーザ名とパスワードは必要ありません）。

表 4-2　エンド ユーザの認証とアクセス

認証	ユーザのアクセス方法
LDAP	URL、通知
メールボックス（IMAP/POP）	URL、通知
なし	通知のみ
無効	アクセス不可能（通知がイネーブルになっている場合、[Spam Notifications] セクションで設定された [Deliver Bounce Messages To:] のアドレスに通知が送信されます）

スパム通知

通知とは、IronPort スパム検疫内にある各ユーザ宛の新しいスパム メッセージを要約したものです。スパム通知をイネーブルにし、その内容を設定します。スパム通知の内容には、差出人アドレス、件名、メッセージ本文、メッセージ形式、バウンス アドレス、通知スケジュールなどがあります。IronPort スパム検疫へのアクセスがイネーブルになっている場合、ユーザは、LDAP やメールボックスの認証を使用しなくても、通知によって自分宛の検疫されたメッセージにアクセスできるようになります。通知は、電子メールが検疫されている各エンベロープ受信者（メーリング リストおよびその他のエイリアスを含む）に送信されます。各メーリング リストは、単一の要約を受信します。つまり、各メーリング リストの購読者は、全員が同じ通知を受信することになり、その検疫にログインしてメッセージを解放したり、削除したりできます。この場合、ユーザが検疫にアクセスして、通知に示されたメッセージを表示しようとしても、それらのメッセージは他のユーザによってすでに削除されている可能性もあります。複数のエイリアスに属していたり、複数の電子メール アドレスを使用したりしているユーザは、複数の通知を受信します（「複数の通知の受信」（P.4-49）を参照）。「スパム通知の設定」（P.4-38）を参照してください。

（注）　スパム通知がイネーブルになっていても、IronPort スパム検疫へのアクセスがイネーブルになっていなければ、通知は [Deliver Bounce Messages To:] のアドレスに送信されます。

ローカルの IronPort スパム検疫の設定

ローカルの IronPort スパム検疫がイネーブルになった後（「ローカルの IronPort スパム検疫のイネーブル化とディセーブル化」（P.4-28）を参照）、検疫の設定を編集して、IronPort スパム検疫と、それをユーザがどのように操作するのかを設定できます。

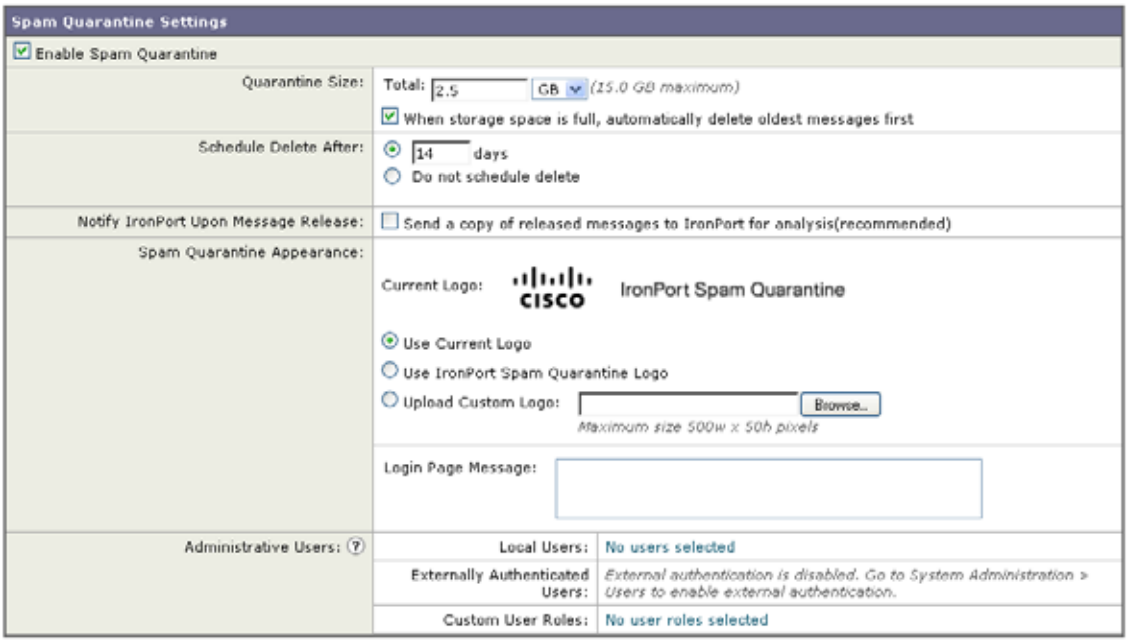
ローカルの IronPort スパム検疫を設定するには、[Monitor] > [Quarantines] ページで IronPort スパム検疫の [Settings] カラム内にある [Edit] をクリックします。[Edit IronPort Spam Quarantine] ページが表示されます。

ローカルの IronPort スパム検疫用のスパム検疫設定

ローカルの Cisco IronPort アプライアンス上の IronPort スパム検疫用に、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　[Monitor] > [Quarantines] ページで IronPort スパム検疫の [Settings] カラム内にある [Edit] をクリックします。[Edit IronPort Spam Quarantine] ページが表示されます。

図 4-15　IronPort スパム検疫設定の編集



ステップ 2　[Spam Quarantine Settings] セクション内で、検疫エリアの最大サイズを指定します。

ステップ 3　検疫エリアが満杯になったら古いメッセージから削除するように検疫を設定できます。チェックボックスをオフにすると、満杯の検疫エリアに新しいメッセージは追加されなくなります。検疫エリアが満杯になることでアプライアンス上にメッセージの待ち行列（渋滞）ができることがないように、この機能をイネーブルにすることを推奨します。

ステップ 4　メッセージを削除する前の保管日数を指定します。あるいは、自動削除をスケジュールしないことを選択することもできます。検疫エリアの容量が満杯になるのを防ぐために、古いメッセージから削除するように検疫を設定することを推奨します。

ステップ 5　デフォルトの言語を指定します。

ステップ 6　解放されたメッセージのコピーを分析用に Cisco IronPort へ送信するように検疫を設定できます。検疫をそのように設定することを推奨します。

ステップ 7　エンド ユーザが検疫を確認するときに表示されるページをカスタマイズします。カスタム ロゴをアップロードします（任意）。このロゴは、ユーザがログインして検疫されたメッセージを確認するときに、IronPort スパム検疫のページの最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 ファイルを指定しなければ、IronPort スパム検疫のデフォルトのロゴが使用されます。

（注）　カスタム ロゴを指定すると、Cisco IronPort ロゴは削除されます。

ステップ 8　ログイン ページ メッセージを指定します。このメッセージは、検疫を表示する前に、エンド ユーザに対してログインを要求するときに表示されます。

ステップ 9　変更を送信し、保存します。

（注）　Cisco IronPort M-Series アプライアンスを設定する場合の詳細については、『*Cisco IronPort AsyncOS for Security Management User Guide*』を参照してください。

IronPort スパム検疫の管理ユーザの設定

IronPort スパム検疫の管理ユーザを指定できます。この場合の「管理」とは、IronPort スパム検疫へのユーザのアクセス権を示します。管理ユーザのリストには、検疫権限を持つカスタム ユーザ ロールに属するオペレータ、ヘルプ デスク ユーザ、読み取り専用オペレータ、および委任管理者を追加できます。管理者レベルのユーザ（デフォルトの admin ユーザを含む）はすべて、自動的に IronPort スパム検疫の管理ユーザであると見なされます。したがって、それらのユーザは、[Available] カラムや [Authorized Users] カラムに表示されません。

IronPort スパム検疫内にあるすべてのメッセージを表示できるユーザのリストに対して AsyncOS オペレータ ユーザを追加または削除するには、次の手順を実行します。

図 4-16　IronPort スパム検疫の管理ユーザの編集

ステップ 1　ローカル、外部認証、またはカスタム ロール（委任管理者）から、適切なユーザのタイプのリンクをクリックします。

ステップ 2　追加するユーザを選択します。

ステップ 3　[Add] をクリックします。

Operator レベルのユーザおよび委任管理者は、IronPort スパム検疫内のメッセージを表示できますが、検疫の設定を編集できないことに注意してください。管理ユーザは、メッセージを表示し、設定を変更できます。

ステップ 4　変更を送信し、保存します。

エンド ユーザ検疫へのアクセスの設定

エンド ユーザが IronPort スパム検疫に直接（通知を必要とせずに）アクセスできるようにするには、[Monitor] -> [Quarantines] ページで IronPort スパム検疫の [Settings] カラム内にある [Edit] をクリックします。[Edit IronPort Spam Quarantine] ページが表示されます。

ステップ 1　[Enable End-User Quarantine Access] と書かれたチェックボックスをオンにします。Administrator ユーザは、このチェックボックスがオンかオフかに関係なく、検疫にアクセスできます。

図 4-17　IronPort スパム検疫へのアクセス設定の編集

ステップ 2　メッセージが解放される前に、メッセージ本文を表示するかどうかを指定します。このチェックボックスをオンにすると、ユーザは、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の本文を表示するには、そのメッセージを解放してから、ユーザのメール

アプリケーション（Outlook など）で表示する必要があります。これは、すべての閲覧された電子メールがアーカイブされなければならない場合のコンプライアンスの問題と特に関係しています。

ステップ 3　エンドユーザが（電子メール通知経由ではなく）Web ブラウザから検疫を直接表示しようとする場合に、それらのエンドユーザを認証するために使用する方式を指定します。メールボックス認証または LDAP 認証を使用できます。

認証をイネーブルにしなくても、IronPort スパム検疫へのエンド ユーザのアクセスを許可できることに注意してください。この場合、ユーザは通知メッセージに含まれるリンク経由で検疫にアクセスでき、システムはユーザの認証を行いません。認証なしのエンド ユーザ アクセスをイネーブルにする場合は、[End-User Authentication] ドロップダウン メニューで [None] を選択します。

LDAP 認証：**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、[System Administration] > [LDAP] リンクをクリックして、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 認証の設定方法の詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「LDAP Queries」を参照してください。

メールボックス認証：認証に LDAP ディレクトリを使用しないサイトの場合、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することもできます。Web UI にログインするとき、ユーザは各自の完全な電子メール アドレスとメールボックス パスワードを入力します。この情報を使用して、メールボックス サーバに検疫のユーザとしてのログインが試行されます。ログインに成功すれば、そのユーザは認証されます。その後、ただちにログアウトするので、ユーザの受信箱に対して行われる変更はありません。メールボックス認証の使用は、LDAP ディレクトリを稼動しないサイトに適していますが、電子メール エイリアス宛に送られてきたメッセージをメールボックス認証でユーザに提示できません。

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（example.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）、Cisco IronPort アプライアンスは APOP のみを使用します。一部またはすべてのユーザに対して APOP がサポートされていない場合は、APOP をアドバタイズしないように POP サーバを設定する必要があります。

ステップ 4　変更を送信し、保存します。

スパム通知の設定

スパム通知とは、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（LDAP によるユーザ認証の場合は、LDAP リポジトリ内でそのユーザに関連付けられている電子メール アドレス宛。「エンド ユーザ検疫へのアクセスの設定」（P.4-36）を参照）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するために使用するリンクも含まれます。通知は、イネーブルにされた後、ここで設定されたスケジュールに従って送信されます。

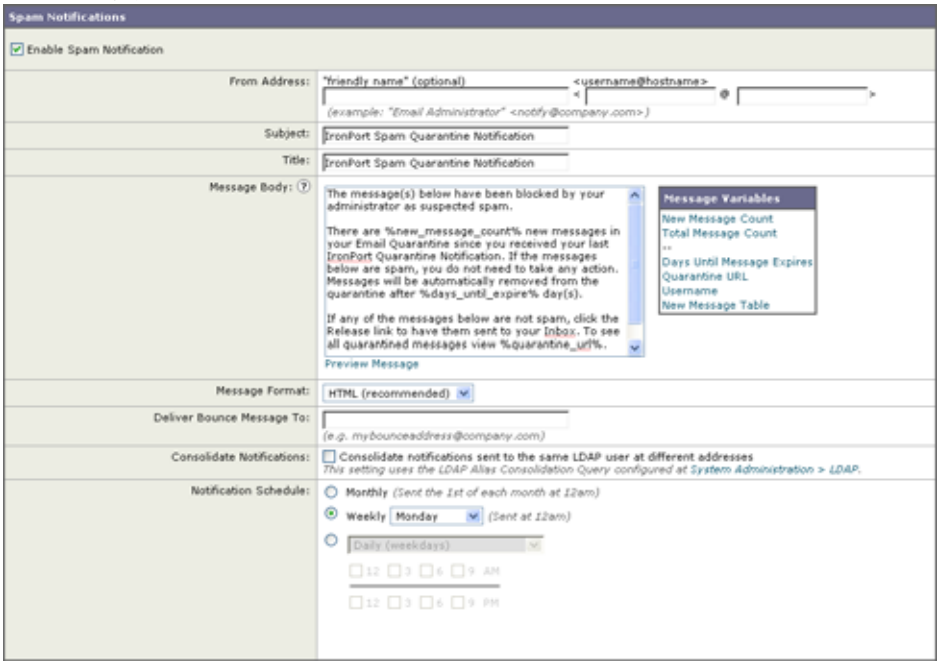
スパム通知により、エンドユーザが検疫にログインするための代替方法が提供されます。ユーザは、受信した電子メール通知を介して検疫にアクセスします（その検疫に対して通知がイネーブルになっている場合）。メッセージの件名をクリックすると、ユーザは、その通知が送信された電子メール アドレスの検疫の UI にログインします。この方法による IronPort スパム検疫へのアクセスには、LDAP 認証もメールボックス認証も必要ありません。この方法によるログインでは、アプライアンスが電子メール通知にスパム検疫エイリアス統合クエリーを使用していない限り、エンドユーザが所有する他のエイリアス宛の検疫対象メッセージは表示されないことに注意してください。Cisco IronPort 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に対する同じ検疫にアクセスできます。

Cisco IronPort アプライアンスによるスパム通知の生成方法では、電子メール エイリアスを所有するユーザや複数の電子メール アドレスを使用するユーザは、複数のスパム通知を受信する可能性があります。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セットアップされていない場合は、[System Administration] > [LDAP] リンクをクリックして、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、このマニュアル内の「導入上の考慮事項」（P.4-45）と「複数の通知の受信」（P.4-49）に加え、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「LDAP Queries」も参照してください。

エンド ユーザに送信される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　[Enable Spam Notifications] と書かれた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 4-18　スパム通知の設定



ステップ 2　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任意の「ホワイトリスト」に追加できます（「導入上の考慮事項」（P.4-45）を参照）。

ステップ 3　通知の件名を入力します。

ステップ 4　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 5　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、ユーザに対して通知が生成されるとき、そのユーザの実際の名前に展開されます。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 6　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 7　バウンス アドレスを指定します（バウンスされた通知がこのアドレスに送信されます）。

ステップ 8　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 9　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、または日に 1 回以上送信するように（週末の有無も含めて）設定できます。

ステップ 10　変更を送信し、保存します。

外部の IronPort スパム検疫の設定

スパムおよびその疑いのあるメッセージを別の Cisco IronPort アプライアンス上に設定された外部の IronPort スパム検疫に送信するように、Cisco IronPort アプライアンスを設定できます。Cisco IronPort M-Series アプライアンスは、特にこの役割を担うように設計されています。Cisco IronPort M-Series アプライアンスの詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「The Cisco IronPort M-Series Security Management Appliance」を参照してください。

外部の IronPort スパム検疫を使用する場合、検疫の設定は、その Cisco IronPort アプライアンス上で行います。Cisco IronPort アプライアンス上でローカルと外部の IronPort スパム検疫を両方ともイネーブルにした場合、ローカルの IronPort スパム検疫がその設定とともに優先されます。

M-Series アプライアンス（外部検疫）から解放されるメッセージは、RAT、ドメイン例外、エイリアシング、着信フィルタ、マスカレード、バウンス検証、および作業キューをスキップします。

外部の IronPort スパム検疫の追加

外部の IronPort スパム検疫を追加するには、次の手順を実行します。

ステップ 1　[Monitor] > [External Spam Quarantine] ページから、[Add Quarantine...] をクリックします。[External Quarantines] ページが表示されます。

図 4-19　外部のエンド ユーザ検疫の追加

ステップ 2　検疫の名前を入力します。この名前に意味はありません。参照目的でのみ使用されます。

ステップ 3　IP アドレスとポート番号を入力します。この IP アドレスとポート番号は、M-Series アプライアンス上で [Spam Quarantines Settings] ページ内に指定されています（詳細については、『*Cisco IronPort AsyncOS for Security Management User Guide* 』を参照してください）。

ステップ 4　変更を送信し、保存します。

外部の IronPort スパム検疫の編集

既存の外部 IronPort スパム検疫を編集するには、次の手順を実行します。

ステップ 1　[Settings] カラム内にある [Edit] をクリックします。[Edit External Quarantine] ページが表示されます。

ステップ 2　設定を変更します。

ステップ 3　変更を送信し、保存します。

外部の IronPort スパム検疫の削除

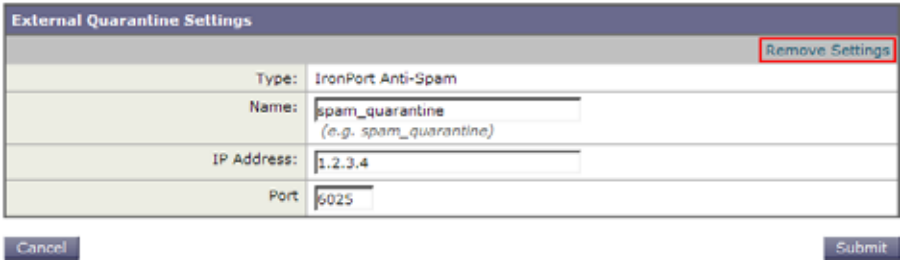
Cisco IronPort アプライアンスには、外部の IronPort スパム検疫を 1 つしか指定できません。外部の IronPort スパム検疫の削除では、その検疫自体が削除されることはなく、その検疫エリア内のデータは少しも変更されないことに注意してください。代わりに、その外部 IronPort スパム検疫に対する参照がローカル マシンから削除されます。

外部の IronPort スパム検疫を削除するには、次の手順を実行します。

ステップ 1　[Settings] カラム内にある [Edit] をクリックします。[Edit External Quarantine] ページが表示されます。

ステップ 2　[Remove Settings] をクリックします。

図 4-20　外部の IronPort スパム検疫の削除



ステップ 3　[Delete] をクリックして、削除を確認するように求められます。

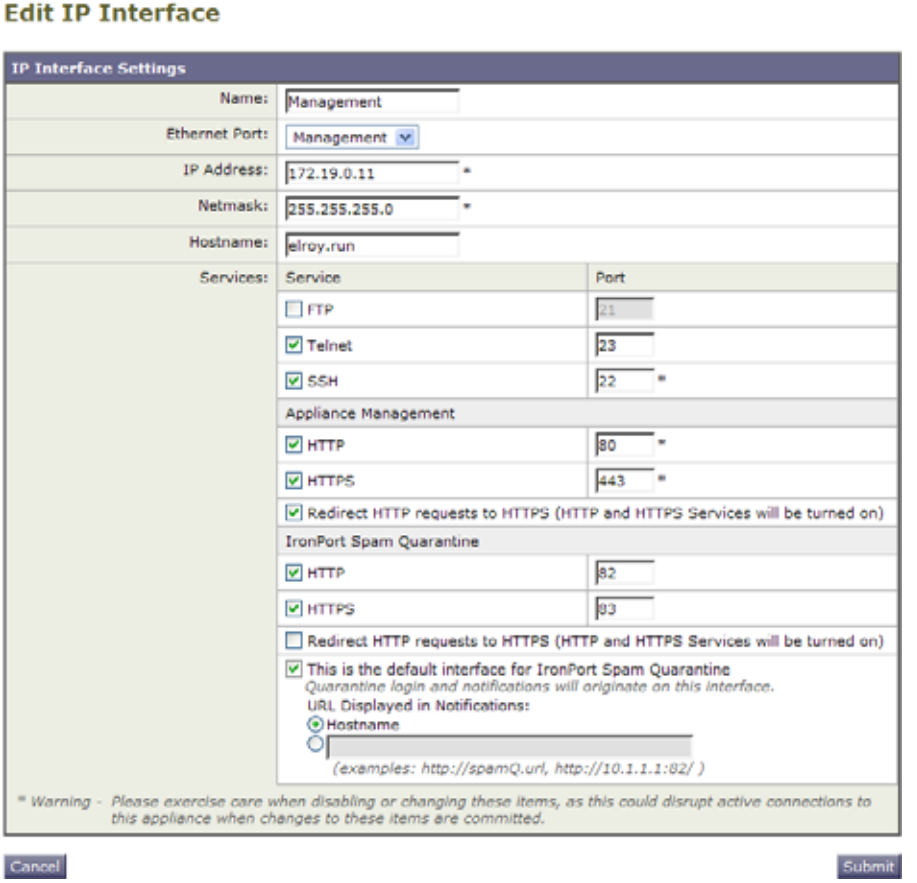
IP インターフェイス上での IronPort スパム検疫 HTTP/S サービスのイネーブル化

ローカルの IronPort スパム検疫をイネーブルにした後、IronPort スパム検疫の HTTP または HTTPS サービスを IP インターフェイス上でイネーブルにします。

IronPort スパム検疫の HTTP または HTTPS サービスを IP インターフェイス上で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　[Network] > [IP Interfaces] ページで、インターフェイス名をクリックします（この例では、Management インターフェイスを使用します）。[Edit IP Interface] ダイアログが表示されます。

図 4-21　Management インターフェイス上での IronPort スパム検疫のイネーブル化



ステップ 2　HTTP や HTTPS を使用するかどうかを、それらに対応するポート番号とともに指定します。

ステップ 3　HTTP 要求を HTTPS にリダイレクトするかどうかを選択します。

ステップ 4　IronPort スパム検疫にアクセスするためのデフォルトのインターフェイス（通知および検疫ログインがこのインターフェイス上で開始されます）にするかどうかを指定します。URL 内のホスト名を使用するか、それともカスタム URL を指定するかを選択します。

ステップ 5　変更を送信し、保存します。

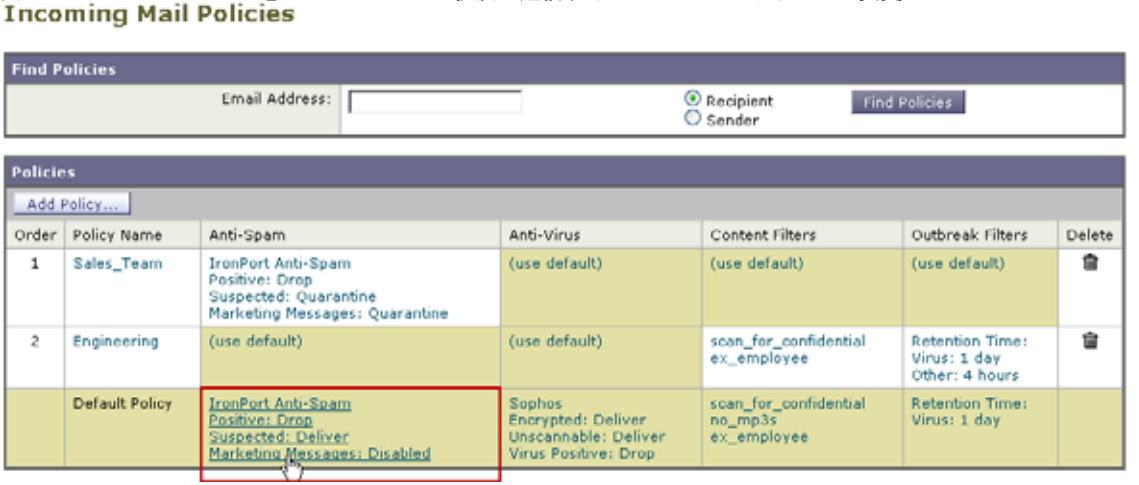
メール ポリシーの IronPort スパム検疫のイネーブル化

ローカルの IronPort スパム検疫をイネーブルにした後（または外部の IronPort スパム検疫を追加した後）、スパムまたはスパムの疑いのあるメッセージをその検疫エリアに送信するように、メール ポリシーを設定できます。メールを IronPort スパム検疫に送信できるようにするために、IronPort アンチスパム スキャンがメール ポリシーでイネーブルにされる必要があることに注意してください。

スパムまたはその疑いのあるメッセージを IronPort スパム検疫に送信するようにメール ポリシーを設定するには、次の手順を実行します。

ステップ 1　[Mail Policies] > [Incoming Mail Policies] ページで、対応するメール ポリシーの [Anti-Spam] カラム内にあるリンクをクリックします。

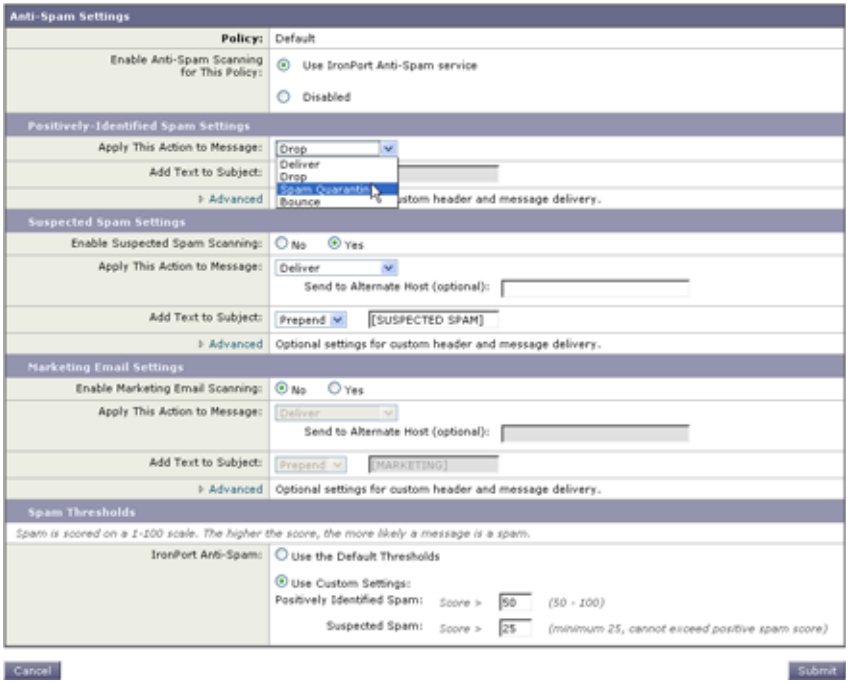
図 4-22　スパムを IronPort スパム検疫に送信するためのメール ポリシーの変更



ステップ 2　[Mail Policies: Anti-Spam] ページが表示されます。

ステップ 3　[Positively-Identified Spam Settings] セクション内で、[Apply This Action to Message] オプションに [IronPort Spam Quarantine] を選択します。

図 4-23　陽性と識別されたスパムの IronPort スパム検疫への送信



ステップ 4　必要に応じて、スパムの疑いのあるメッセージやマーケティング電子メールに対してもこの設定を繰り返します。

ステップ 5　変更を送信し、保存します。

導入上の考慮事項

ここでは、IronPort スパム検疫を導入する際に注意すべき、さまざまなヒントと情報を提供します。

ディスク スペース

表 4-3 に、各アプライアンス上で IronPort スパム検疫に使用可能なディスク スペースを示します。

表 4-3　Cisco IronPort アプライアンスごとに IronPort スパム検疫に使用可能なディスク スペース

モデル	ディスク スペース（単位：GB）
C150/160	5
C350/360/370	15
C650/660/670	30
X1050/1060/1070	30

IronPort スパム検疫にアクセスするエンド ユーザ

エンド ユーザは、受信した通知内のリンク経由で IronPort スパム検疫にアクセスできます。この方法で検疫にアクセスする場合、LDAP 認証や IMAP/POP 認証は必要ありません（エンド ユーザは自分自身を認証する必要がありません）。通知メッセージ内に存在するリンクには有効期限がないことに注意してください。エンド ユーザは、これらのリンクを使用すれば、認証しなくても、自分宛の検疫されたメッセージを表示できます。

ユーザは、自分の Web ブラウザにリンクを直接入力して検疫にアクセスすることもできます。Web ブラウザに入力した URL 経由で検疫にアクセスする場合、ユーザは認証を行う必要があります。認証方式（LDAP または「メールボックス」（IMAP/POP））は、検疫設定の [End User Quarantine Access] セクション内で定義されます（「エンド ユーザ検疫へのアクセスの設定」（P.4-36）を参照）。

LDAP 認証

LDAP の認証プロセスは次のとおりです。

ステップ 1　ユーザが自分のユーザ名とパスワードを Web UI ログイン ページに入力します。

ステップ 2　IronPort スパム検疫は、匿名検索を実行するように、または指定された「サーバ ログイン」DN とパスワードによる認証ユーザとして、指定された LDAP サーバに接続します。Active Directory の場合、一般に「グローバル カタログ ポー

ト」（6000 番台）上でサーバ接続を確立する必要があり、検索を実行するために、IronPort スパム検疫がバインドできる低い特権 LDAP ユーザを作成する必要があります。

ステップ 3　次に、IronPort スパム検疫は、指定された BaseDN とクエリー ストリングを使用してユーザを検索します。ユーザの LDAP レコードが見つかると、IronPort スパム検疫は、そのレコードの DN を抽出し、ユーザ レコードの DN と最初にユーザが入力したパスワードを使用してディレクトリへのバインドを試みます。このパスワード チェックに成功すると、ユーザは正しく認証されます。しかしまだ、IronPort スパム検疫は、そのユーザに対してどのメールボックスの内容を表示するのか決定する必要があります。

ステップ 4　メッセージは、受信者のエンベロープ アドレスを使用して IronPort スパム検疫に保管されます。ユーザのパスワードが LDAP に対して検証された後、IronPort スパム検疫は、「プライマリ電子メール属性」を LDAP レコードから取得して、どのエンベロープ アドレスの検疫されたメッセージを表示する必要があるのか決定します。「プライマリ電子メール属性」には、電子メール アドレスが複数格納されている場合があり、これらのアドレスを使用して、検疫からどのエンベロープ アドレスが認証ユーザに対して表示される必要があるのか決定されます。

IMAP/POP 認証

IMAP/POP の認証プロセスは次のとおりです。

ステップ 1　メール サーバ設定に応じて、ユーザは、自分のユーザ名（`joe`）または電子メール アドレス（`joe@example.com`）と、パスワードを Web UI ログイン ページに入力します。ユーザに電子メール アドレスをフルに入力する必要があるのか、ユーザ名だけを入力すればよいのか知らせるために、ログイン ページ メッセージを変更できます（「エンド ユーザ検疫へのアクセスの設定」（P.4-36）を参照）。

ステップ 2　IronPort スパム検疫は、IMAP サーバまたは POP サーバに接続し、入力されたログイン名（ユーザ名または電子メール アドレス）とパスワードを使用して IMAP/POP サーバへのログインを試みます。パスワードが受け入れられると、そのユーザは認証されたと見なされ、IronPort スパム検疫はただちに IMAP/POP サーバからログアウトします。

ステップ 3　ユーザが認証された後、IronPort スパム検疫は、ユーザの電子メール アドレスに基づいて、そのユーザ宛の電子メールのリストを作成します。

- IronPort スパム検疫の設定において、修飾のないユーザ名（`joe` など）に追加するドメインを指定している場合は、このドメインを後ろに追加してできる完全修飾電子メール アドレスを使用して、検疫エリア内の一致するエンベロープが検索されます。

– それ以外の場合、IronPort スパム検疫は、入力された電子メール アドレスを使用して、一致するエンベロープを検索します。

IronPort スパム検疫にログインするための URL の決定

エンドユーザが IronPort スパム検疫に直接アクセスするために使用できる URL は、マシンのホスト名と、検疫がイネーブルになっている IP インターフェイス上の設定（HTTP/S とポート番号）から作成されます。次の例を参考にしてください。

```
HTTP://mail3.example.com:82
```

設定例

POP/IMAP の設定例：

IMAP および POP の場合（単一ドメイン）：

- サーバ名を入力します。
- サーバで SSL を使用するように設定している場合は、SSL をイネーブルにします。
- [Append Domain to Unqualified Usernames] をイネーブルにし、ユーザのログイン用にエンベロープのドメインをこれに設定します。

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

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

通知のテスト

電子メール セキュリティ マネージャでテスト用のメール ポリシーを設定することにより、通知をテストできます。この場合、単一のユーザに対してだけ、スパムを検疫させます。その後、IronPort スパム検疫の通知設定で、[Enable Spam Notification] チェックボックスをオンにし、[Enable End-User Quarantine Access] チェックボックスをオフにします。これにより、[Deliver Bounced Messages To] フィールドに設定された管理者だけが、検疫内の新しいスパムについて通知されます。

エンド ユーザでの通知の確実な受信

エンド ユーザに対して、IronPort スパム検疫からの通知電子メールの差出人アドレスを各自のメール アプリケーション（Outlook、Thunderbird など）の迷惑メール設定にある「ホワイトリスト」へ追加することを推奨してください。

複数の通知の受信

ユーザは、複数の電子メール エイリアスに属しているか、複数の電子メール アドレスを使用していると、複数の通知を受信します。また、電子メールを受信する LDAP グループに属しているユーザもこれに当てはまります。

表 4-4　アドレス/エイリアスに応じた通知数

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

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

各ユーザに対して存在するメッセージの確認

認証の方式によっては（LDAP または IMAP/POP）、ユーザに対して IronPort スパム検疫内に複数の電子メール アドレス宛のメールが存在する可能性があります。

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

しかし、ユーザが通知経由で検疫に直接アクセスする場合、あるいは認証方式が IMAP/POP の場合、検疫にはそのユーザの電子メール アドレス（または通知が送信されたアドレス）宛のメッセージしか表示されません。エンド ユーザ認証の動作の詳細については、「IronPort スパム検疫にアクセスするエンド ユーザ」（P.4-46）を参照してください。

IronPort スパム検疫内では、電子メール アドレスの大文字と小文字が区別されないことに注意してください。たとえば、Admin@example.com 宛と admin@example.com 宛の電子メールは、両方とも「admin@example.com」に関連付けられたユーザの検疫エリア内に存在します。

検疫対象のメールのアドレスを制限

複数のメール ポリシーを使用して（[Mail Policies] > [Incoming Mail Policy]）、メールの検疫対象から除外する受信者アドレスのリストを指定できます。そのメール ポリシーにアンチスパムを設定する際、検疫の代わりに [Deliver] または [Drop] を選択します。

デフォルト エンコーディング

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

デフォルト エンコーディングの指定

着信電子メールのヘッダーに文字セットのエンコーディングが指定されていない場合、Cisco IronPort アプライアンスを設定して、デフォルト エンコーディングを指定できます。そうすることにより、そのようなメッセージを IronPort スパム検疫内で正しく表示するのに役立ちます。

ただし、デフォルト エンコーディングを指定すると、他の文字セットのメッセージが正しく表示されなくなる可能性があります。これは、メッセージ ヘッダーにエンコーディングが指定されていないメッセージに対してのみ適用されます。一般に、このカテゴリに入るメールの多くが 1 つの特定のエンコーディングになると予測される場合にだけ、デフォルト エンコーディングを設定します。たとえば、検疫されるメールのうち、メッセージ ヘッダーに文字セットのエンコーディングが指定されていないものの多くが日本語（ISO-2022-JP）の場合、（下の `scanconfig->setup` オプションにおいて）「`Configure encoding to use when none is specified for plain body text or anything with MIME type plain/text or plain/html.`」のプロンプトが表示された際に、オプション 12 を選択します。

メッセージ ヘッダーにエンコーディングを指定していないメッセージに対してデフォルト エンコーディングを設定するには、CLI から `scanconfig->setup` コマンドを使用します。次の例では、デフォルトとして UTF-8 が設定されます。

```
mail3.example.com> scanconfig


There are currently 7 attachment type mappings configured to be SKIPPED.


Choose the operation you want to perform:

- NEW - Add a new entry.

- DELETE - Remove an entry.

- SETUP - Configure scanning behavior.

- IMPORT - Load mappings from a file.

- EXPORT - Save mappings to a file.

- PRINT - Display the list.

- CLEAR - Remove all entries.

[]> setup
```

```
[ ... ]

Configure encoding to use when none is specified for plain body text or
anything with MIME type plain/text or plain/html.



1. US-ASCII

2. Unicode (UTF-8)

3. Unicode (UTF-16)

[ ... list of encodings ... ]

13. Japanese (EUC)

[1]> 2



Encoding set to "Unicode (UTF-8)".
```

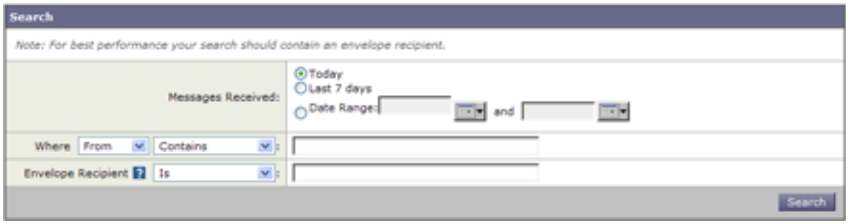
IronPort スパム検疫内のメッセージの管理

ここでは、管理者の視点から、ローカルまたは外部の IronPort スパム検疫内にあるメッセージの操作方法について説明します。管理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。

管理者として、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

図 4-24　IronPort スパム検疫の検索ページ



IronPort スパム検疫内でのメッセージの検索

検索フォームを使用して、IronPort スパム検疫内のすべてのメッセージにわたって検索します。

ステップ 1　エンベロープ受信者を指定します。アドレスは部分的に入力することもできます。入力した受信者に検索結果が厳密に一致する必要があるか、あるいは入力した値が検索結果のアドレスの一部、先頭、または末尾のいずれと一致する必要があるかを選択します。

ステップ 2　検索の対象期間を入力します。カレンダー アイコンをクリックして、日付を選択します。

ステップ 3　差出人アドレスを指定し、入力した値が検索結果のアドレスの一部、全体、先頭、または末尾のいずれと一致する必要があるかを選択します。

ステップ 4　[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

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

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

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、IronPort スパム検疫内のメッセージが表示されます。一度に表示されるメッセージの件数を選択できます。カラム見出しをクリックすることにより、表示をソートできます。同じカラムを再びクリックすると、逆順にソートされます。

メッセージの件名をクリックしてメッセージを表示します。これには、本文とヘッダーが含まれます。メッセージは、[Message Details] ページに表示されます。メッセージの最初の 20 KB が表示されます。メッセージがそれよりも長い場合、表示は 20 KB で打ち切られ、メッセージの最後にあるリンクからメッセージをダウンロードできます。

[Message Details] ページから、メッセージを削除したり（[Delete] を選択）、[Release] を選択してメッセージを解放したりできます。メッセージを解放すると、そのメッセージは配信されます。

添付ファイルを含むメッセージの表示

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

HTML メッセージの表示

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。画像は表示されません。

符号化されたメッセージの表示

Base64 で符号化されたメッセージは、復号化されてから表示されます。

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、解放する 1 つまたは複数のメッセージの隣にあるチェックボックスをクリックし、ドロップダウン メニューから [Release] を選択します。その後、[Submit] をクリックします。

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

解放されたメッセージは、それ以降の電子メール パイプライン内の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。

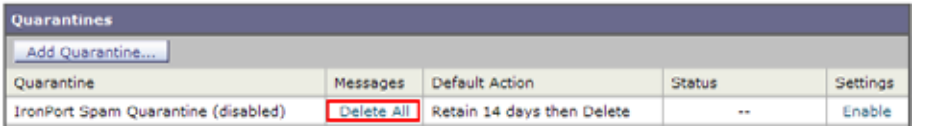
IronPort スパム検疫からのメッセージの削除

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

IronPort スパム検疫内のすべてのメッセージを削除するには、その検疫をディセーブルにし（「ローカルの IronPort スパム検疫のディセーブル化」（P.4-29）を参照）、[Delete All Messages] リンクをクリックします。リンクの末尾にある括弧内の数字は、IronPort スパム検疫内のメッセージの件数です。

図 4-25　すべてのメッセージを削除するリンク



セーフリストとブロックリストの利用

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可能にして、どの電子メールがスパムとして処理されるかをより適切に制御できます。セーフリストにより、ユーザは、特定のユーザまたはドメインがスパムとして処理されないようにできます。それに対してブロックリストでは、特定のユーザまたはドメインが常にスパムとして処理されるようにできます。セーフリストとブロックリストの設定は、IronPort スパム検疫から設定されます。そのため、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）　セーフリストとブロックリストは、メールがスパムとして処理されるのを防止したり、メールがスパムとして処理されることを保証したりします。ただし、セーフリストやブロックリストを設定しても、電子メール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、Cisco IronPort アプライアンスで実行されます。メッセージは、セーフリストに該当しても、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。

セーフリスト/ブロックリスト データベース

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 Cisco IronPort アプライアンス上のデータベースに保管されます。M-Series を使用する場合、このデータベースは、M-Series アプライアンス上に保存され、関連するすべての C-Series アプライアンス上で定期的に更新と同期が行われます。IronPort スパム検疫が C-Series アプライアンス上にホスティングされる場合、セーフリスト/ブロックリスト データベースは、その C-Series アプライアンス上に維持されます。複数の C-Series アプライアンスを M-Series アプライアンスなしで使用する場合、データベースと設定を手動で同期する必要があります。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を異なる C-Series アプライアンス間で同期する方法の詳細については、「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.4-61）を参照してください。

バックアップ .CSV データベースを利用する方法については、「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.4-60）を参照してください。

セーフリストとブロックリストを M-Series アプライアンス上で利用する方法については、『*Cisco IronPort AsyncOS for Security Management User Guide*』を参照してください。

セーフリストとブロックリストの作成およびメンテナンス

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を作成し、メンテナンスするには、管理者とエンドユーザが次の作業を実行します。

- **管理者作業**。管理者は、IronPort スパム検疫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のイネーブル化、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、異なるアプライアンス間でのセーフリスト/ブロックリスト データベースの同期、およびログ、アラート、カスタム ヘッダーによるセーフリストとブロックリストに関する問題のトラブルシューティングを行います。管理者作業の詳細については、「セーフリストとブロックリストの作成およびメンテナンスを行うための管理者作業」（P.4-58）を参照してください。
- **エンドユーザ作業**。エンドユーザは、エンドユーザ スパム検疫によって自分のセーフリストとブロックリストの設定を作成します。エンド ユーザは、自分のセーフリスト/ブロックリスト設定にアクセスするために、（IronPort スパム検疫通知内のリンクをクリックする代わりに）ログイン作業が必要になる場合があります。エンドユーザ スパム検疫から、エンドユーザは、[Options] メニューを使用してセーフリストとブロックリストを作成できます。あるいは、検疫された電子メールのリストから、セーフリスト設定を作成できます。エンドユーザ作業の詳細については、「セーフリストとブロックリストを設定するためのエンド ユーザ作業」（P.4-62）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、Cisco IronPort 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。Cisco IronPort 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、受信者が複数存在すると（および各受信者のセーフリスト/ブロックリスト設定が異なると）、そのメッセージは分裂します。たとえば、受信者 A と受信者 B の両方に送信されるメッセージがあるとします。受信者 A のセーフリストにはこのメッセージの送信者のエントリがありますが、受信者 B にはセーフリストにもブロックリストにもエントリがありません。この場合、メッセージは 2 つのメッセージ ID で 2 つのメッセージに分割されます。受信者 A に送信されるメッセージは、セーフリストに一致していることが *X-SLBL-Result- セーフリスト* ヘッダーによってマークされ、アンチスパム スキャンをスキップします。一方、受信者 B 宛のメッセージは、アンチスパム スキャン エンジンによってスキャンされます。その後、どちらのメッセージもパイプライン（アンチウイルス スキャン、コンテンツ ポリシーなど）を続行し、設定されているすべての設定に従います。

メッセージの送信者またはドメインがブロックリストに含まれる場合、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。ブロックリスト アクションの設定が検疫を実行するようになっている場合、そのメッセージはスキャンされ、最終的に検疫されます。ブロックリスト アクションがドロップに設定されている場合、そのメッセージは、セーフリスト/ブロックリスト スキャンの直後にドロップされます。

セーフリストとブロックリストは IronPort スパム検疫内で管理されているため、配信の動作は、他のアンチスパム設定にも左右されます。たとえば、アンチスパム スキャンをスキップするように 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。

セーフリストとブロックリストの作成およびメンテナンスを行うための管理者作業

セーフリストとブロックリストを使用するために、管理者は次の作業を実行する必要があります。

- **Ironport スパム検疫のイネーブル化と設定**。セーフリストとブロックリストは IronPort スパム検疫からアクセスされるため、セーフリストとブロックリストを使用するにはこの機能をイネーブルにする必要があります。詳細については、「IronPort スパム検疫機能の設定」（P.4-27）を参照してください。
- **セーフリスト/ブロックリスト機能のイネーブル化と設定**。IronPort スパム検疫をイネーブルにした後、セーフリスト/ブロックリスト機能をイネーブルにし、設定します。ブロックリストの電子メールに対するブロックリスト アクション（検疫または削除）も設定する必要があります。詳細については、「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」（P.4-59）を参照してください。

- **セーフリスト/ブロックリスト データベースのバックアップと復元**。アップグレードするとき、セーフリスト/ブロックリスト データベースをバックアップし、復元する作業が必要になります。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.4-60）を参照してください。
- **セーフリスト/ブロックリスト データベースの同期**。エンド ユーザがセーフリストまたはブロックリストのエントリを入力すると、それらの設定はデータベースに保存されます。このデータベースは、AsyncOS が電子メールを処理する際に使用するデータベースと定期的に同期されます。IronPort スパム検疫が M-Series アプライアンス上に維持されている場合、管理者は、C-Series アプライアンスと同期するようにセーフリスト/ブロックリスト データベースを設定する必要があります。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.4-61）を参照してください。
- **セーフリストとブロックリストのトラブルシューティング**。セーフリストとブロックリストをトラブルシューティングするために、ログ、アラートを確認できます。詳細については、「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」（P.4-62）を参照してください。

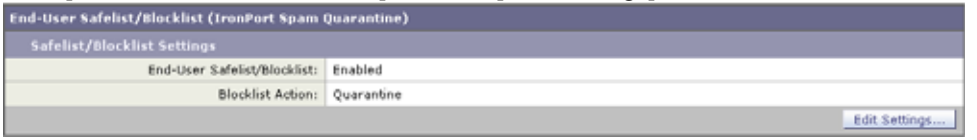
セーフリスト/ブロックリスト設定のイネーブル化と設定

[Quarantines] ページからセーフリストとブロックリストの設定をイネーブルにし、設定できます。

ステップ 1　C-Series アプライアンス上でセーフリストとブロックリストをイネーブルにするには、[Monitor] > [Quarantines] に移動します。

（注）　セーフリストとブロックリストを設定する前に、IronPort スパム検疫をイネーブルにし、設定しておく必要があります。

ステップ 2　[End-User Safelist/Blocklist] 設定で、[Edit Settings] を選択します。



ステップ 3　[Enable Safelist/Blocklist Feature] を選択します。

ステップ 4　[Blocklist Action] に [Quarantine] または [Delete] を選択します。

ステップ 5　[Maximum List Items Per User] を指定します。この値は、ユーザが各セーフリストとブロックリストに載せることのできるアドレスまたはドメインの最大数を表します。

ステップ 6　[Submit] をクリックします。

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

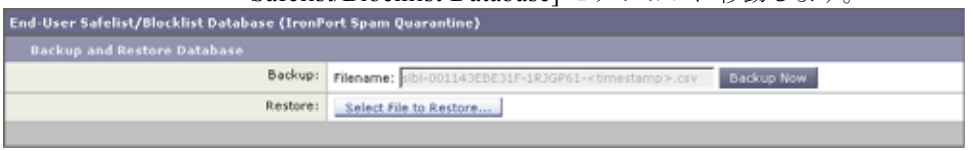
セーフリスト/ブロックリスト データベースのバックアップを保存するには、Cisco IronPort アプライアンスでデータベースを .CSV ファイルとして保存します。.CSV ファイルは、Cisco IronPort アプライアンスの設定が格納される XML コンフィギュレーション ファイルとは別に保管されます。Cisco IronPort アプライアンスをアップグレードする場合、またはインストール ウィザードを実行する場合、セーフリスト/ブロックリスト データベースを .CSV ファイルにバックアップする必要があります。

ファイルをバックアップすると、Cisco IronPort アプライアンスによって、.CSV ファイルが次の命名規約に従って `/configuration` ディレクトリに保存されます。

slbl<timestamp><serial number>.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　[System Administration] > [Configuration File] から、[End-User Safelist/Blocklist Database] セクションに移動します。



ステップ 2　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 3　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。

Cisco IronPort アプライアンスにより、コンフィギュレーション 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 4　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

エンド ユーザがセーフリストまたはブロックリストを作成すると、その設定はデータベースに保存されます。IronPort スパム検疫が M-Series アプライアンス上に存在する場合、セーフリスト/ブロックリスト設定が着信メールに適用される前に、このデータベースを C-Series アプライアンス上のデータベースと同期する必要があります。IronPort スパム検疫が C-Series アプライアンス上に存在する場合は、このデータベースを、メール キューを処理するときに使用される読み取り専用データベースと同期する必要があります。これらのデータベースを自動で同期するのにかかる時間は、アプライアンスのモデルによって異なります。次の表に、セーフリストとブロックリストの更新についてのデフォルトの設定を示します。

表 4-5　セーフリストとブロックリストの設定の同期

アプライアンス	同期時間
C150/C160	10 分
C350/C360/C370	15 分
C650/C660/C670	30 分
X1050/X1060/X1070	60 分
M600/M660	120 分
M1000/M1050/M1060	240 分

C-Series アプライアンスのグループを M-Series アプライアンスなしで使用する場合、セーフリスト/ブロックリストの設定とデータベースはマシン間で同期する必要があります。

集中管理機能を使用して複数の Cisco IronPort 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、『*Cisco IronPort AsyncOS for Email Configuration Guide*』または『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』のいずれかに記載された「Accessing the Appliance」を参照してください。

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

各エンド ユーザは、それぞれ独自のセーフリストとブロックリストを維持します。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した場合にのみ、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。セーフリストとブロックリストに関する問題をトラブルシューティングするために、ログ ファイルまたはシステム アラートを表示できます。

電子メールがセーフリスト/ブロックリスト設定によってブロックされると、そのアクションが ISQ_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。セーフリストに含まれる電子メールは、セーフリストに一致していることが *X-SLBL-Result- セーフリスト* ヘッダーによってマークされます。ブロックリストに含まれる電子メールは、ブロックリストに一致していることが *X-SLBL-Result- ブロックリスト* ヘッダーによってマークされます。

アラートは、データベースが作成または更新されたり、データベースの変更またはセーフリスト/ブロックリスト プロセスの実行においてエラーが発生したりすると送信されます。

アラートの詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「System Administration」を参照してください。

ログ ファイルの詳細については、第 5 章「ロギング」を参照してください。

セーフリストとブロックリストを設定するためのエンド ユーザ作業

エンド ユーザは、特定の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、特定の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、もう興味のないメーリング リストから電子メールを受信している場合があります。そのようなユーザは、このメーリング リストからの電子メールが自分の受信箱に送信されないように、その送信者を自分のブロックリストに追加できます。また他方で、エンド ユーザは、スパムではない特定の送信者からの電子メールが自分の IronPort スパム検疫に送信されていることに気づくこともあります。これらの送信者からの電子メールが検疫されないようにするために、エンド ユーザはそれらの送信者を自分のセーフリストに追加できます。

（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。

セーフリストとブロックリストを利用するために、エンド ユーザは次の作業を実行する必要があります。

- **セーフリストとブロックリストにアクセスします**。認証の設定によっては、エンド ユーザは自分の IronPort スパム検疫アカウントにログインする必要があります。詳細については、「セーフリストとブロックリストへのアクセス」（P.4-63）を参照してください。
- **セーフリスト エントリを追加します**。ユーザは、IronPort スパム検疫内の [Options] メニューまたは検疫されたメッセージのリストからセーフリスト エントリを追加します。詳細については、「セーフリストへのエントリの追加」（P.4-64）を参照してください。
- **ブロックリスト エントリを追加します**。ユーザは、IronPort スパム検疫内の [Options] メニューからブロックリスト エントリを追加します。詳細については、「ブロックリストへのエントリの追加」（P.4-67）を参照してください。

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/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、IronPort スパム検疫に対して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自分の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 エントリとブロックリスト エントリの構文

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、エンド ユーザが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の電子メール アドレスをブロックリストに追加した場合、Cisco IronPort アプライアンスは両方のルールを適用します（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、Cisco IronPort 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。

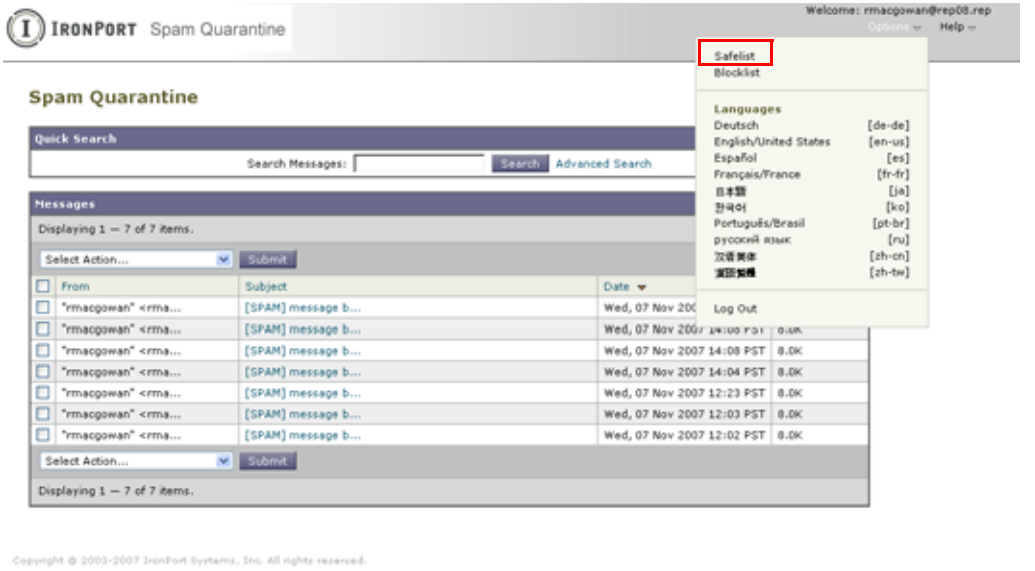
セーフリストへのエントリの追加

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。

方法 1

ステップ 1　IronPort スパム検疫から、[Options] ドロップダウン メニューを選択します。

図 4-26　エンドユーザ検疫内のセーフリスト オプション



ステップ 2　[Safelist] を選択します。

ステップ 3　[Safelist] ダイアログボックスから、電子メール アドレスまたはドメインを入力します。ドメインと電子メール アドレスは、コンマで区切って複数入力できます。

ステップ 4　[Add to List] をクリックします。

図 4-27　エンドユーザ検疫内のセーフリスト

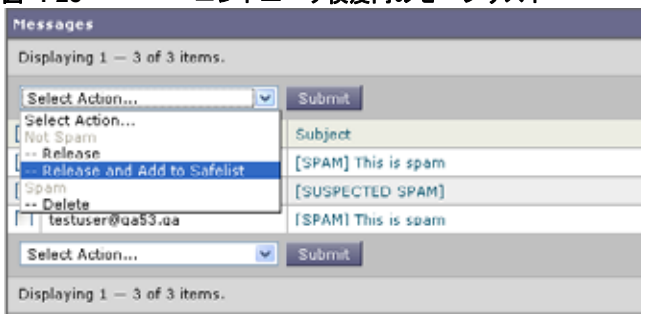
方法 2

エンド ユーザは、メッセージがエンド ユーザ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。

ステップ 1　エンドユーザ検疫から、メッセージの横にあるチェックボックスをオンにします。

ステップ 2　ドロップダウン メニューから [Release and Add to Safelist] を選択します。

図 4-28　エンドユーザ検疫内のセーフリスト



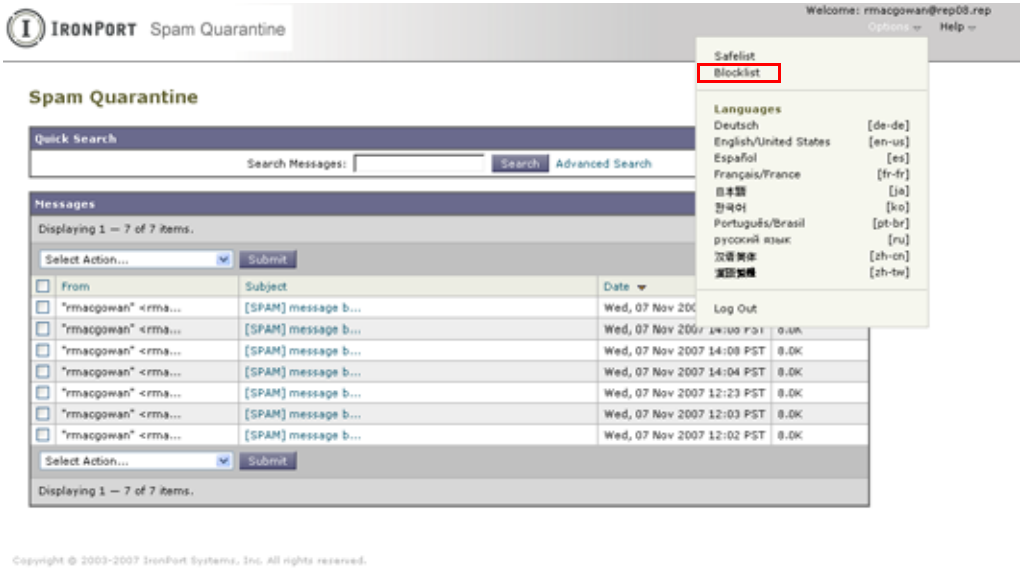
指定したメールのエンベロープ送信者と差出人ヘッダーが両方ともセーフリストに追加されます。解放されたメッセージは、それ以降の電子メール パイプライン内の作業キューの処理をスキップして、宛先キューへ直接進みます。

ブロックリストへのエントリの追加

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を受信しないようにできます。

ステップ 1　エンドユーザ検疫から、[Options] ドロップダウン メニューを選択します。

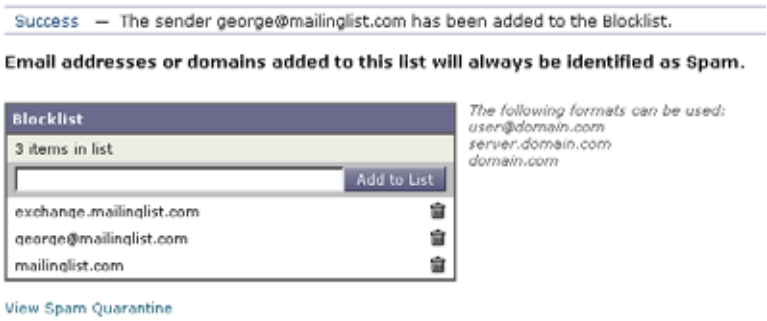
図 4-29　エンドユーザ検疫内のブロックリスト オプション



ステップ 2　ブロックリストに追加するドメインまたは電子メール アドレスを入力します。ドメインと電子メール アドレスは、コンマで区切って複数入力できます。

ステップ 3　[Add to List] をクリックします。

図 4-30　ブロックリストへの送信者の追加



Cisco IronPort 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。このメールは、セーフリスト/ブロックリスト アクション設定に応じて、拒否されるか、検疫されます。

（注）　セーフリスト エントリとは異なり、ブロックリスト エントリは、エンドユーザ検疫内の [Options] メニューからだけ追加できます。

CHAPTER 5

ロギング

Cisco IronPort 電子メール セキュリティ 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 は多くのログ タイプを生成し、さまざまなタイプの情報を記録できます。ログ ファイルには、システムの各種コンポーネントによる通常のアクティビティとエラーの記録が保持されます。この情報は、Cisco IronPort アプライアンスをモニタするときや、パフォーマンスのトラブルシューティングまたはチェックを行うときに役立つ場合があります。

この章は、次の内容で構成されています。

概要

ここでは、次の項目について説明します。

ログ ファイルおよびログ サブスクリプションについて

ログは、AsyncOS の電子メール動作に関する重要な情報を収集する、簡潔で効率的な方法です。これらのログには、Cisco IronPort アプライアンスでのアクティビティに関する情報が記録されます。情報は、バウンス ログや配信ログなど、表示するログによって異なります。

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、配信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 エディタで読み取ることができます。

IronPort は、複数の Cisco IronPort アプライアンスからのログに対応するオフボックスの集中化レポーティングおよびトラッキング ツールを提供しています。詳細については、Cisco IronPort の担当者にお問い合わせください。

ログ サブスクリプションでは、ログ タイプに名前、ロギング レベル、およびその他の制約事項（サイズや宛先情報など）を関連付けます。同じログ タイプに対して複数のサブスクリプションが許可されます。

ログ タイプ

ログ タイプは、メッセージ データ、システム統計情報、バイナリまたはテキスト データなど、生成されたログにどの情報が記録されるかを示します。ログ タイプは、ログ サブスクリプションを作成するときに選択します。詳細については、「ログ サブスクリプション」（P.5-59）を参照してください。

Cisco IronPort AsyncOS for Email では、次のログ タイプが生成されます。

表 5-1　　ログ タイプ

ログ	説明
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 システムの動作に関する情報が記録されます。たとえば、メッセージの受信、メッセージの配信試行、接続のオープンとクローズ、バウンス、TLS 接続などです。
qmail 形式メール ログ	qmail 形式の配信ログには、次の配信ログと同じく電子メール システムの動作に関する情報が記録されますが、保存は qmail 形式です。

表 5-1　ログ タイプ（続き）

ログ	説明
配信ログ	配信ログには、Cisco IronPort アプライアンスの電子メール配信動作に関する重要な情報が記録されます。たとえば、配信試行時の各受信者の配信やバウンスに関する情報などです。ログ メッセージは「ステートレス」です。つまり、関連付けられたすべての情報が各ログ メッセージに記録されるので、ユーザは、現在の配信試行に関する情報について前のログ メッセージを参照する必要がありません。配信ログは、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。配信ログ ファイルを XML または Comma-Separated Values（CSV）形式に変換するには、提供されるユーティリティを使用して事後処理する必要があります。変換ツールは、次の場所にあります。`http://support.ironport.com`
バウンス ログ	バウンス ログには、バウンスされた受信者の情報が記録されます。バウンスされた受信者ごとに記録される情報には、メッセージ ID、受信者 ID、Envelope From アドレス、Envelope To アドレス、その受信者のバウンスの理由、および受信者ホストからの応答コードなどが含まれます。また、バウンスされた各受信者メッセージの一定量を記録するように選択することもできます。この量はバイトで定義され、デフォルトはゼロです。
ステータス ログ	このログ ファイルには、`status detail` および `dnsstatus` などの CLI ステータス コマンドで検出されたシステムの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 ログに報告される各カウンタまたはレートは、カウンタが最後にリセットされてからの値です。
ドメイン デバッグ ログ	ドメイン デバッグ ログには、Cisco IronPort アプライアンスと指定の受信者ホスト間の SMTP 会話でのクライアントとサーバの通信が記録されます。このログ タイプは、特定の受信者ホストに関する問題のデバッグに使用できます。ログ ファイルに記録する SMTP セッションの合計数を指定する必要があります。セッションが記録されるにつれ、この数は減少していきます。ログ サブスクリプションを削除または編集することによって、すべてのセッションが記録される前にドメイン デバッグを停止できます。

表 5-1　ログ タイプ（続き）

ログ	説明
インジェクション デバッグ ログ	インジェクション デバッグ ログには、Cisco IronPort アプライアンスと、システムに接続している指定のホスト間の SMTP 会話が記録されます。インジェクション デバッグ ログは、インターネット上の Cisco IronPort アプライアンスとホスト間の通信に関する問題をトラブルシューティングするのに役立ちます。
システム ログ	システム ログには、ブート情報、DNS ステータス情報、および `commit` コマンドを使用してユーザが入力したコメントが記録されます。システム ログは、アプライアンスの基本的な状態をトラブルシューティングするのに役立ちます。
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、セキュア HTTP サービス、またはその両方のサービスに関する情報が記録されます。Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）には HTTP を介してアクセスするので、HTTP ログは表面上 CLI 監査ログと同等の GUI です。GUI でアクセスされたセッション データ（新規セッション、期限切れセッション）およびページが記録されます。
NTP ログ	NTP ログには、設定されている任意の Network Time Protocol（NTP; ネットワーク タイム プロトコル）サーバとアプライアンス間の会話が記録されます。詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「System Administration」の章の「Editing the Network Time Protocol (NTP) Configuration (Time Keeping Method)」を参照してください。

表 5-1　ログ タイプ（続き）

ログ	説明
LDAP デバッグ ログ	LDAP デバッグ ログは、LDAP インストールのデバッグを目的としています（『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「LDAP Queries」の章を参照してください）。ここには、Cisco IronPort アプライアンスが LDAP サーバに送信しているクエリーについての有益な情報が記録されます。
アンチスパム ログ	アンチスパム ログには、最新のアンチスパム ルールのアップデート受信に関するステータスなど、システムのアンチスパム スキャン機能のステータスが記録されます。また、Context Adaptive Scanning Engine に関するすべてのログもここに記録されます。
アンチスパム アーカイブ	アンチスパム スキャン機能をイネーブルにすると、スキャンされ、「メッセージのアーカイブ」アクションに関連付けられたメッセージがここにアーカイブされます。これは、mbox 形式のログファイルとなります。アンチスパム エンジンの詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Anti-Spam」の章を参照してください。
アンチウイルス ログ	アンチウイルス ログには、最新のアンチウイルス アイデンティティ ファイルのアップデート受信に関するステータスなど、システムのアンチウイルス スキャン機能のステータスが記録されます。
アンチウイルス アーカイブ	アンチウイルス エンジンをイネーブルにすると、スキャンされ、「メッセージのアーカイブ」アクションに関連付けられたメッセージがここにアーカイブされます。これは、mbox 形式のログファイルとなります。詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Anti-Virus」の章を参照してください。

表 5-1　ログ タイプ（続き）

ログ	説明
スキャン ログ	スキャン ログには、スキャン エンジンに関するすべての LOG および COMMON メッセージが保持されます（『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「System Administration」の章の「Alerts」を参照してください）。これは一般に、アプリケーションの障害、送信されたアラート、失敗したアラート、およびログ エラー メッセージになります。このログは、システム全体のアラートには適用されません。
IronPort スパム検疫ログ	IronPort スパム検疫ログには、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。
IronPort スパム検疫 GUI ログ	IronPort スパム検疫ログには、GUI を介した設定、エンド ユーザ認証、およびエンド ユーザ アクション（電子メールの解放など）を含む、IronPort スパム検疫に関連付けられたアクションが記録されます。
SMTP 会話ログ	SMTP 会話ログには、着信および発信 SMTP 会話のすべての部分が記録されます。
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に関するデータとデータベースが記録されます。
レポーティング ログ	レポーティング ログには、集中化レポーティング サービスのプロセスに関連付けられたアクションが記録されます。
レポーティング クエリー ログ	レポーティング クエリー ログには、アプライアンスで実行されるレポーティング クエリーに関連付けられたアクションが記録されます。
アップデータ ログ	アップデータ ログには、McAfee アンチウイルス定義のアップデートなど、システム サービスのアップデートに関するイベントが記録されます。
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 ログのサブセットです。

表 5-1　ログ タイプ（続き）

ログ	説明
認証ログ	認証ログには、成功したユーザ ログインと失敗したログイン試行が記録されます。
設定履歴ログ	設定履歴ログには、電子メール セキュリティ アプライアンス上でどのような変更が、いつ行われたかに関する情報が記録されます。ユーザが変更をコミットするたびに、新しい設定履歴ログが作成されます。

ログ タイプの特徴

表 5-2 に、各ログ タイプの特徴をまとめます。

表 5-2　ログ タイプの比較

	記載内容													
	トランザクション	ステータス	テキストとして記録	mboxファイルとして記録	バイナリとして記録	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	インジェクションSMTP会話	ヘッダーロギング	配信SMTP会話	設定情報
IronPort メール ログ	•		•			•	•	•	•	•		•		
qmail 形式配信ログ		•			•		•	•	•			•		
配信ログ		•			•		•	•	•			•		
バウンス ログ	•		•						•	•		•		
ステータス ログ		•	•			•								

表 5-2　ログ タイプの比較（続き）

	記載内容													
	トランザクション	ステータス	テキストとして記録	mboxファイルとして記録	バイナリとして記録	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	インジェクションSMTP会話	ヘッダーロギング	配信SMTP会話	設定情報
ドメイン デバッグ ログ	•		•					•	•	•			•	
インジェクション デバッグ ログ	•		•				•				•			
システム ログ	•		•			•								
CLI 監査ログ	•		•			•								
FTP サーバ ログ	•		•			•								
HTTP ログ	•		•			•								
NTP ログ	•		•			•								
LDAP ログ	•		•											
アンチスパム ログ	•		•			•								
アンチスパム アーカイブ ログ				•										
アンチウイルス ログ	•		•			•								

表 5-2　ログ タイプの比較（続き）

	記載内容													
	トランザクション	ステータス	テキストとして記録	mboxファイルとして記録	バイナリとして記録	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	インジェクションSMTP会話	ヘッダーロギング	配信SMTP会話	設定情報
アンチウイルス アーカイブ				•										
スキャン ログ	•		•			•								•
IronPort スパム検疫	•		•			•								
IronPort スパム検疫 GUI	•		•			•								
セーフリスト/ブロックリスト ログ	•		•			•								
レポーティング ログ	•		•		•									
レポーティング クエリー ログ	•		•		•									
アップデータ ログ			•											
トラッキング ログ	•				•	•	•	•	•	•		•		

表 5-2　ログ タイプの比較（続き）

	記載内容													
	トランザクション	ステータス	テキストとして記録	mboxファイルとして記録	バイナリとして記録	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	インジェクションSMTP会話	ヘッダーロギング	配信SMTP会話	設定情報
認証ログ	•		•											
設定履歴ログ	•		•											•

ログ取得方法

ログ ファイルは、次のいずれかのファイル転送プロトコルに基づいて取得できます。ログ サブスクリプション プロセス中に GUI または `logconfig` コマンドを使用して、ログ サブスクリプションの作成や編集を行いながらプロトコルを設定します。

表 5-3　ログ転送プロトコル

手動でのダウンロード	この方法では、[Log Subscriptions] ページにあるログ ディレクトリへのリンクをクリックし、アクセスするログ ファイルをクリックすることによって、いつでもログ ファイルにアクセスできます。使用しているブラウザに応じて、そのファイルをブラウザ ウィンドウに表示するか、またはテキスト ファイルとして開いたり、保存したりすることできます。この方法は HTTP（S）プロトコルを使用し、デフォルトの取得方法になっています。 **（注）** この方法を使用すると、この方法を CLI で指定した場合でも、レベル（マシン、グループ、またはクラスタ）には関係なく、クラスタ内のどのコンピュータのログも取得できません。
FTP プッシュ	この方法では、リモート コンピュータ上の FTP サーバに定期的にログ ファイルをプッシュします。サブスクリプションには、リモート コンピュータ上のユーザ名、パスワード、および宛先ディレクトリが必要です。ログ ファイルは、ユーザが設定したロールオーバー スケジュールに基づいて転送されます。「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.8-65）も参照してください。

表 5-3　ログ転送プロトコル（続き）

SCP プッシュ	この方法では、リモート コンピュータ上の SCP サーバに定期的にログ ファイルをプッシュします。この方法には、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、リモート コンピュータ上のユーザ名、SSH キー、および宛先ディレクトリが必要です。ログ ファイルは、ユーザが設定したロールオーバー スケジュールに基づいて転送されます。
syslog プッシュ	この方法では、ログ メッセージをリモートの syslog サーバに送信します。この方法は、RFC 3164 に準拠しています。syslog サーバのホスト名を送信し、ログの転送に UDP または TCP を使用するように選択する必要があります。使用するポートは 514 です。ログのファシリティは選択できますが、ログ タイプのデフォルトはドロップダウン メニューであらかじめ選択されています。syslog プッシュを使用して転送できるのは、テキストベースのログだけです。

ログ ファイル名とディレクトリ構造

Cisco IronPort AsyncOS は、ログ サブスクリプション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。ディレクトリ内の実際のログ ファイル名は、ユーザが指定したログ ファイル名、ログ ファイルが開始されたときのタイムスタンプ、および単一文字のステータス コードで構成されます。ログのファイル名は、次の形式で作成されます。

```
/LogSubscriptionName/LogFilename.@timestamp.statuscode
```

ステータス コードは、`.current` または `.s`（保存済みを示す）になります。saved（保存済み）ステータスのログ ファイルだけを転送または削除するようにしてください。

ログのロールオーバーおよび転送スケジュール

ログ ファイルはログ サブスクリプションによって作成され、到達したユーザ指定の最初の条件（最大ファイル サイズまたはスケジュール設定されたロールオーバー）に基づいて、ロールオーバー（および、プッシュ ベースの取得オプションが選択されている場合は転送）されます。最大ファイル サイズとスケジュール設定されたロールオーバーの時間間隔の両方を設定するには、CLI で、または GUI の [Log Subscriptions] ページで `logconfig` コマンドを使用します。また、GUI の [**Rollover Now**] ボタン、または CLI の `rollovernow` コマンドを

使用して、選択したログ サブスクリプションをロールオーバーすることもできます。ロールオーバーのスケジュール設定の詳細については、「ログ サブスクリプションのロール オーバー」（P.5-69）を参照してください。

手動のダウンロードを使用して取得されたログは、指定した最大数（デフォルトは 10 ファイル）に達するか、またはシステムでログ ファイル用にさらにスペースが必要になるまで保存されます。

デフォルトでイネーブルになるログ

Cisco IronPort アプライアンスは、次のログ サブスクリプションがデフォルトでイネーブルになった状態で事前に設定されています（適用したライセンス キーによって、その他のログが設定される場合があります）。デフォルトでは、取得方法は「手動でのダウンロード」です。

表 5-4　事前に設定されるログ サブスクリプション

ログ番号	ログ サブスクリプション名	ログ タイプ
1	antispam	アンチスパム ログ
2	antivirus	アンチウイルス ログ
3	asarchive	アンチスパム アーカイブ
4	authentication	認証ログ
5	avarchive	アンチウイルス アーカイブ
6	bounces	バウンス ログ
7	cli_logs	CLI 監査ログ
8	encryption	暗号化
9	error_logs	IronPort テキスト メール ログ
10	euq_logs	IronPort スパム検疫ログ
11	euqgui_logs	IronPort スパム検疫 GUI ログ
12	ftpd_logs	FTP サーバ ログ
13	gui_logs	HTTP ログ
14	mail_logs	IronPort テキスト メール ログ

表 5-4　事前に設定されるログ サブスクリプション（続き）

ログ番号	ログ サブスクリプション名	ログ タイプ
15	reportd_logs	レポーティング ログ
16	reportingqueryd_logs	レポーティング クエリー ログ
17	scanning	スキャン ログ
18	slbld_logs	セーフリスト/ブロックリスト ログ
19	sntpd_logs	NTP ログ
20	status	ステータス ログ
21	system_logs	システム ログ
22	trackerd_logs	トラッキング ログ
23	updater_logs	アップデータ ログ

エラーだけが含まれるように 1 に設定された error_logs を除き、事前に設定されるすべてのログ サブスクリプションのログ レベルは 3 になります。詳細については、「ログ レベル」（P.5-61）を参照してください。新規のログ サブスクリプションの作成、または既存のログ サブスクリプションの変更については、「ログ サブスクリプション」（P.5-59）を参照してください。

ログ タイプ

ここでは、次の内容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（秒単位でログの始まりにのみ表示）が含まれます。

- アンチウイルス ログ
- LDAP ログ
- システム ログ
- メール ログ

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、システムを正しく設定する必要があります。また、添付ファイル名が必ずしもログに記録されるとは限りません。詳細については、「ローカル メッセージ トラッキングのイネーブル化とディセーブル化」（P.3-3）および「トラッキング サービスの概要」（P.3-1）を参照してください。

表 5-5 に、テキスト メール ログに表示される情報を示します。

表 5-5　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 であり、この接続で 1 個から数千個のメッセージが送信されます。
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）。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、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	Message ID（メッセージ ID）：この ID を使用して、ログを通過するメッセージを追跡します。
RID	Recipient ID（受信者 ID）：各メッセージ受信者に 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。

IronPort テキスト メール ログの解釈

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 5-6　テキスト メール ログの詳細

1	`Mon Apr 17 19:56:22 2003 Info: New SMTP ICID 5 interface Management (10.1.1.1) address 10.1.1.209 reverse dns host remotehost.com verified yes`
2	`Mon Apr 17 19:57:20 2003 Info: Start MID 6 ICID 5`
3	`Mon Apr 17 19:57:20 2003 Info: MID 6 ICID 5 From: <sender@remotehost.com>`
4	`Mon Apr 17 19:58:06 2003 Info: MID 6 ICID 5 RID 0 To: <mary@yourdomain.com>`
5	`Mon Apr 17 19:59:52 2003 Info: MID 6 ready 100 bytes from <sender@remotehost.com>`
6	`Mon Apr 17 19:59:59 2003 Info: ICID 5 close`
7	`Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 8 interface 192.168.42.42 address 10.5.3.25`
8	`Mon Mar 31 20:10:58 2003 Info: Delivery start DCID 8 MID 6 to RID [0]`
9	`Mon Mar 31 20:10:58 2003 Info: Message done DCID 8 MID 6 to RID [0]`
10	`Mon Mar 31 20:11:03 2003 Info: DCID 8 close`

前述のログ ファイルを読み取るためのガイドとして、表 5-7 を使用してください。

表 5-7　テキスト メール ログの例の詳細

行番号	説明
1.	システムへの新しい接続が開始され、Injection ID（ICID; インジェクション ID）「5」が割り当てられます。この接続は、管理 IP インターフェイスで受信され、リモート ホスト 10.1.1.209 から開始されました。
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」が割り当てられます。
5.	MID 5 が受け入れられ、ディスクに書き込まれ、承認されます。
6.	受信に成功し、受信接続がクローズします。
7.	次に、メッセージ配信プロセスが開始されます。192.168.42.42 から 10.5.3.25 への配信に、Delivery Connection ID（DCID; 配信接続 ID）「8」が割り当てられます。
8.	RID「0」へのメッセージ配信が開始されます。
9.	MID 6 から RID「0」への配信に成功します。
10.	配信接続がクローズします。

テキスト メール ログ エントリの例

次に、さまざまな状況に基づいたいくつかのサンプル ログ エントリを示します。

メッセージのインジェクションおよび配信

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

```
Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 5 interface 172.19.0.11
address 63.251.108.110

Mon Mar 31 20:10:58 2003 Info: Delivery start DCID 5 MID 4 to RID [0]

Mon Mar 31 20:10:58 2003 Info: Message done DCID 5 MID 4 to RID [0]

Mon Mar 31 20:11:03 2003 Info: DCID 5 close
```

失敗したメッセージ配信（ハード バウンス）

2 人の受信者が指定されたメッセージが Cisco IronPort アプライアンスにインジェクトされます。配信時に、宛先ホストが 5*XX* エラーを返します。このエラーは、メッセージをいずれの受信者にも配信できないことを示します。Cisco IronPort アプライアンスは、送信者に通知して、キューからそれらの受信者を削除します。

```
Mon Mar 31 20:00:23 2003 Info: New SMTP DCID 3 interface 172.19.0.11
address 64.81.204.225

Mon Mar 31 20:00:23 2003 Info: Delivery start DCID 3 MID 4 to RID [0,
1]

Mon Mar 31 20:00:27 2003 Info: Bounced: DCID 3 MID 4 to RID 0 - 5.1.0
- Unknown address error ('550', ['<george@yourdomain.com>... Relaying
denied']) []

Mon Mar 31 20:00:27 2003 Info: Bounced: DCID 3 MID 4 to RID 1 - 5.1.0
- Unknown address error ('550', ['<jane@yourdomain.com>... Relaying
denied']) []

Mon Mar 31 20:00:32 2003 Info: DCID 3 close
```

ソフト バウンスの後の正常な配信

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
```

scanconfig コマンドのメッセージ スキャン結果

`scanconfig` コマンドを使用して、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）のシステムの動作を決定できます。オプションは、`Deliver`、`Bounce`、または `Drop` です。

次に、scanconfig を Deliver に設定した IronPort テキスト メール ログの例を示します。

```
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
```

次に、scanconfig を drop に設定した IronPort テキスト メール ログの例を示します。

```
Tue Aug 3 16:38:53 2004 Info: Start MID 257 ICID 44785

Tue Aug 3 16:38:53 2004 Info: MID 257 ICID 44785 From: test@virus.org

Tue Aug 3 16:38:53 2004 Info: MID 257 ICID 44785 RID 0 To:
<joe@example.com>

Tue Aug 3 16:38:53 2004 Info: MID 257 Message-ID
'<392912.@virus.org>'
```

```
Tue Aug 3 16:38:53 2004 Info: MID 25781 Subject 'Virus Scanner Test
#22'

Tue Aug 3 16:38:53 2004 Info: MID 257 ready 1627 bytes from
<test@virus.org>

Tue Aug 3 16:38:53 2004 Warning: MID 257, Message Scanning Problem:
Continuation line seen before first header

Tue Aug 3 16:38:53 2004 Info: Message aborted MID 25781 Dropped by
filter 'drop_zip_c'

Tue Aug 3 16:38:53 2004 Info: Message finished MID 257 done

Tue Aug 3 16:38:53 2004 Info: ICID 44785 close
```

添付ファイルを含むメッセージ

次の例では、添付ファイル名の識別を可能にするために、「Message Body Contains」という条件のコンテンツ 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 つ目が 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、これらの添付ファイルは Quoted-Printable 形式で表されます。

生成またはリライトされたメッセージに対するログ エントリ

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'
```

「rewritten」エントリについては、ログ内で新しい MID の使用を示す行の後に表示される点に注目してください。

IronPort スパム検疫エリアに送信されたメッセージ

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 Connection ID（RCID; RPC 接続 ID）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、スパムとしてタグが付けられたメッセージが 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 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
```

IronPort 配信ログの使用

配信ログには、AsyncOS の電子メール配信動作に関する重要な情報が記録されます。ログ メッセージは「ステートレス」です。つまり、関連するすべての情報が各ログ メッセージに記録されるので、ユーザは、現在の配信試行に関する情報について前のログ メッセージを参照する必要がありません。

配信ログには、受信者ごとの電子メール配信動作に関連するすべての情報が記録されます。すべての情報は、論理的にレイアウトされ、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、次の場所にあります。

`http://support.ironport.com`

配信ログは、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。次の表に、配信ログに記録される情報を示します。

表 5-8　配信ログの統計情報

統計	説明
Delivery status	success（メッセージは正常に配信されました）または bounce（メッセージはハード バウンスされました）
Del_time	配信時間。
Inj_time	インジェクション時間。`del_time` - `inj_time` = 受信者メッセージがキューに留まっていた時間。
Bytes	メッセージ サイズ

表 5-8　配信ログの統計情報（続き）

統計	説明
Mid	メッセージ ID
Ip	受信者ホスト IP 受信者メッセージを受信またはバウンスしたホストの IP アドレス
From	Envelope From（Envelope Sender または MAIL FROM としても知られます）
Source_ip	送信元ホスト IP 着信メッセージのホストの IP アドレス
Code	受信者ホストからの SMTP 応答コード
Reply	受信者ホストからの SMTP 応答メッセージ
Rcpt Rid	受信者 ID。受信者 ID は <0> から始まります。複数の受信者が指定されたメッセージには、複数の受信者 ID が付きます。
To	Envelope To
Attempts	配信試行回数

配信ステータスが bounce であった場合は、次の追加情報が配信ログに表示されます。

表 5-9　配信ログのバウンス情報

統計	説明
Reason	配信時の SMTP 応答に対する RFC 1893 Enhanced Mail Status Code の解釈
Code	受信者ホストからの SMTP 応答コード
Error	受信者ホストからの SMTP 応答メッセージ

ログヘッダーを設定している場合（「メッセージ ヘッダーのロギング」（P.5-66）を参照）、ヘッダー情報は配信情報の後に表示されます。

表 5-10　配信ログのヘッダー情報

統計	説明
Customer_data	ログに記録されるヘッダーの始まりを示す XML タグ

表 5-10　配信ログのヘッダー情報（続き）

統計	説明
Header Name	ヘッダーの名前
Value	ログに記録されるヘッダーの内容

配信ログ エントリの例

ここでは、さまざまな配信ログ エントリの例を示します。

正常なメッセージ配信

```
<success del_time="Fri Jan 09 15:34:20.234 2004" inj_time="Fri Jan 09
15:33:38.623 2004" bytes="202" mid="45949" ip="10.1.1.1"
from="campaign1@yourdomain.com" source_ip="192.168.102.1" code="250"
reply="sent">

<rcpt rid="0" to="alsdfj.ajsdfl@alsdfj.d2.qa25.qa" attempts="1" />

</success>
```

配信ステータス バウンス

```
<bounce del_time="Sun Jan 05 08:28:33.073 2003" inj_time="Mon Jan 05
08:28:32.929 2003" bytes="4074" mid="94157762" ip="0.0.0.0"
from="campaign1@yourdomain.com" source_ip="192.168.102.1 "reason="5.1.0 -
Unknown address error" code="550" error="["Requested action not taken:
mailbox unavailable"]">

<rcpt rid="0" to="user@sampledomain.com" attempts="1" />

</bounce>
```

ログヘッダー付きの配信ログ エントリ

```
<success del_time="Tue Jan 28 15:56:13.123 2003" inj_time="Tue Jan 28
15:55:17.696 2003" bytes="139" mid="202" ip="10.1.1.13"
from="campaign1@yourdomain.com" source_ip="192.168.102.1" code="250"
reply="sent">

<rcpt rid="0" to="user@sampledomain.com" attempts="1" />

<customer_data>

<header name="xname" value="sh"/>

</customer_data>

</success>
```

IronPort バウンス ログの使用

バウンス ログには、バウンスされた各受信者に関するすべての情報が記録されます。表 5-11 に、バウンス ログに記録される情報を示します。

表 5-11　バウンス ログの統計情報

統計	説明
Timestamp	バウンス イベントの時刻
Log level	このバウンス ログの詳細レベル
Bounce type	Bounced または Delayed（ハードバウンスまたはソフトバウンスなど）
MID/RID	メッセージ ID および受信者 ID
From	Envelope From
To	Envelope To
Reason	配信時の SMTP 応答に対する RFC 1893 Enhanced Mail Status Code の解釈
Response	受信者ホストからの SMTP 応答コードおよびメッセージ

また、ログに記録するメッセージ サイズを指定しているか、ログヘッダーを設定している（「メッセージ ヘッダーのロギング」（P.5-66）を参照）場合、メッセージおよびヘッダー情報はバウンス情報の後に表示されます。

表 5-12　バウンス ログのヘッダー情報

Header	ヘッダー名およびヘッダーのコンテンツ。
Message	ログに記録されるメッセージのコンテンツ。

バウンス ログ エントリの例

ソフトバウンスされた受信者（バウンス タイプ = Delayed）

```
Thu Dec 26 18:37:00 2003 Info: Delayed: 44451135:0
From:<campaign1@yourdomain.com> To:<user@sampledomain.com>



Reason: "4.1.0 - Unknown address error" Response: "('451',
['<user@sampledomain.com> Automated block triggered by suspicious
activity from your IP address (10.1.1.1). Have your system administrator
send e-mail to postmaster@sampledomain.com if you believe this block is
in error'])"
```

ハードバウンスされた受信者（バウンス タイプ = Bounced）

```
Thu Dec 26 18:36:59 2003 Info: Bounced: 45346670:0
From:<campaign1@yourdomain.com> To:<user2@sampledomain.com>



Reason: "5.1.0 - Unknown address error" Response: "('550', ['There is no
such active account.'])"
```

メッセージ本文およびログヘッダー付きのバウンス ログ

```
Wed Jan 29 00:06:30 2003 Info: Bounced: 203:0
From:<campaign1@yourdomain.com> To:<user@sampledomain.com>

Reason:"5.1.2 - Bad destination host" Response: "('000', [])" Headers:
['xname: userID2333']' Message: Message-Id:



<1u5jak$6b@yourdomain.com>¥015¥012xname: userID2333¥015¥012subject:
Greetings.¥015¥012¥015¥012Hi Tom:'
```

（注）　テキスト文字列 ¥015¥012 は、改行を表します（CRLF など）。

IronPort 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 ログに報告される各カウンタまたはレートは、カウンタが最後にリセットされてからの値です。

ステータス ログの読み取り

表 5-13 に、ステータス ログ ラベルと、一致するシステム統計情報を示します。

表 5-13　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

表 5-13　ステータス ログの統計情報（続き）

統計	説明
HrdBncRcp	ハード バウンスされた受信者
DnsHrdBnc	DNS ハード バウンス
5XXHrdBnc	5XX ハード バウンス
FltrHrdBnc	フィルタ ハード バウンス
ExpHrdBnc	期限切れハード バウンス
OtrHrdBnc	その他のハード バウンス
DlvRcp	配信された受信者
DelRcp	削除された受信者
GlbUnsbHt	グローバル配信停止リストとの一致数
ActvRcp	アクティブ受信者
UnatmptRcp	未試行受信者
AtmptRcp	試行受信者
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

表 5-13　ステータス ログの統計情報（続き）

統計	説明
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るキロバイト
LogUsd	使用されるログ パーティションの割合
AVLd	アンチウイルス スキャンで使用される CPU の割合
CmrkLd	Cloudmark アンチスパム スキャンで使用される CPU の割合
SophLd	Sophos アンチスパム スキャンで使用される CPU の割合
McafLd	McAfee アンチウイルス スキャンで使用される CPU の割合
CASELd	CASE スキャンで使用される 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 スペース
EuQ	IronPort スパム検疫内の推定メッセージ数
EuqRls	IronPort スパム検疫解放キュー内の推定メッセージ数

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
```

IronPort ドメイン デバッグ ログの使用

ドメイン デバッグ ログには、Cisco IronPort アプライアンスと指定の受信者ホスト間の SMTP 会話でのクライアントとサーバの通信が記録されます。このログ タイプは主に、特定の受信者ホストに関する問題のデバッグに使用されます。

表 5-14　ドメイン デバッグ ログの統計情報

統計	説明
Timestamp	バウンス イベントの時刻
Log level	このバウンス ログの詳細レベル
From	Envelope From
To	Envelope To
Reason	配信時の SMTP 応答に対する RFC 1893 Enhanced Mail Status Code の解釈
Response	受信者ホストからの SMTP 応答コードおよびメッセージ

ドメイン デバッグ ログの例

```
Sat Dec 21 02:37:22 2003 Info: 102503993 Sent: 'MAIL
FROM:<daily@dailyf-y-i.net>'

Sat Dec 21 02:37:23 2003 Info: 102503993 Rcvd: '250 OK'

Sat Dec 21 02:37:23 2003 Info: 102503993 Sent: 'RCPT
TO:<LLLSMILE@aol.com>'

Sat Dec 21 02:37:23 2003 Info: 102503993 Rcvd: '250 OK'

Sat Dec 21 02:37:23 2003 Info: 102503993 Sent: 'DATA'

Sat Dec 21 02:37:24 2003 Info: 102503993 Rcvd: '354 START MAIL INPUT, END
WITH "." ON A LINE BY ITSELF'

Sat Dec 21 02:37:24 2003 Info: 102503993 Rcvd: '250 OK'
```

IronPort インジェクション デバッグ ログの使用

インジェクション デバッグ ログには、Cisco IronPort アプライアンスと、システムに接続している指定のホスト間の SMTP 会話が記録されます。インジェクション デバッグ ログは、インターネットから接続を開始するクライアントと Cisco IronPort アプライアンス間の通信に関する問題をトラブルシューティングするのに役立ちます。このログでは、2 つのシステム間で伝送されたすべてのバイトが記録され、[Sent to]（接続ホストに送信）または [Rcvd from]（接続ホストから受信）に分類されます。

記録するホストの会話を指定するには、IP アドレス、IP 範囲、ホスト名、または部分ホスト名を指定する必要があります。IP 範囲内で接続している IP アドレスがすべて記録されます。部分ドメイン内のホストがすべて記録されます。システムは、接続している IP アドレスに対してリバース DNS ルックアップを実行して、ホスト名に変換します。DNS に対応する PTR レコードがない IP アドレスは、ホスト名に一致しません。

記録するセッション数も指定する必要があります。

インジェクション デバッグ ログ内の各行には、表 5-15 に示す情報が含まれます。

表 5-15　インジェクション デバッグ ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻
ICID	インジェクション接続 ID は、別のログ サブスクリプションで同じ接続に関連付けることができる固有識別子です。
Sent/Received	「Sent to」と記された行は、接続ホストに送信された実際のバイトです。「Rcvd from」と記された行は、接続ホストから受信した実際のバイトです。
IP Address	接続ホストの IP アドレス。

インジェクション デバッグ ログの例

```
Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '220
postman.example.com ESMTP¥015¥012'

Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'HELO
mail.remotehost.com¥015¥012'

Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '250
postman.example.com¥015¥012'

Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'MAIL
FROM:<sender@remotehost.com>¥015¥012'

Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '250 sender
<sender@remotehost.com> ok¥015¥012'

Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'RCPT
TO:<recipient@example.com>¥015¥012'

Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '250 recipient
<recipient@example.com> ok¥015¥012'

Wed Apr 2 14:30:04 Info: 6216 Rcvd from '172.16.0.22': 'DATA¥015¥012'

Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '354 go
ahead¥015¥012'

Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'To:
recipient@example.com¥015¥012Date: Apr 02 2003 10:09:44¥015¥012Subject:
Test Subject¥015¥012From: Sender <sender@remotehost.com>¥015¥012'

Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'This is the
content of the message'

Wed Apr 2 14:30:04 Info: 6216 Sent to '172.16.0.22': '250 ok¥015¥012'

Wed Apr 2 14:30:04 Info: 6216 Rcvd from '172.16.0.22': 'QUIT¥015¥012'

Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '221
postman.example.com¥015¥012'
```

IronPort システム ログの使用

表 5-16　システム ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻
Message	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: 4.0.0-206 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.
```

IronPort CLI 監査ログの使用

表 5-17　CLI 監査ログの統計情報

統計	説明
Timestamp	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。
Message	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[]> '
```

IronPort FTP サーバ ログの使用

表 5-18　FTP サーバ ログの統計情報

統計	説明
Timestamp	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。
Message	ログ エントリのメッセージ セクションは、ログファイル 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
```

IronPort HTTP ログの使用

表 5-19　HTTP ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻
ID	セッション ID
req	接続マシンの IP アドレス
user	接続ユーザのユーザ名
Message	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 GUI の対話（システム設定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
```

IronPort NTP ログの使用

表 5-20　NTP ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻
Message	メッセージは、サーバへの Simple Network Time Protocol (SNTP; 簡易ネットワーク タイム プロトコル) 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
```

スキャン ログの使用

スキャン ログには、アプライアンスのスキャン エンジンのすべての LOG および COMMON メッセージが含まれています。使用可能な COMMON および LOG アラート メッセージのリストについては、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「System Administration」の章の「Alerts」を参照してください。

表 5-21　スキャン 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
Message	メッセージは、いずれかのスキャン エンジンのアプリケーションの障害、送信されたアラート、失敗したアラート、またはログ エラー メッセージで構成されています。

スキャン ログの例

次のログの例は、Sophos アンチウイルスに関する警告アラートを送信しているアプライアンスの履歴を示しています。

```
Wed Feb 23 22:05:48 2011 Info: Internal SMTP system attempting to
send a message to alerts@example.com with subject 'Warning
<Anti-Virus> mail3.example.com: sophos antivirus - The Anti-Virus
database on this system is...' (attempt #0).

Wed Feb 23 22:05:48 2011 Info: Internal SMTP system successfully sent
a message to alerts@example.com with subject 'Warning <Anti-Virus>
mail3.example.com: sophos antivirus - The Anti-Virus database on this
system is...'.

Wed Feb 23 22:05:48 2011 Info: A Anti-Virus/Warning alert was sent to
alerts@example.com with subject "Warning <Anti-Virus>
mail3.example.com: sophos antivirus - The Anti-Virus database on this
system is...".
```

IronPort アンチスパムの使用

表 5-22　アンチスパム ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻
Message	メッセージは、アンチスパム アップデートの確認と結果（エンジンまたはアンチスパム ルールのアップデートが必要であったかどうかなど）で構成されます。

アンチスパム ログの例

次のアンチスパム ログの例は、アンチスパム エンジンによる、スパム定義のアップデートおよび CASE アップデートの確認を示しています。

```
Fri Apr 13 18:59:47 2007 Info: case antispam - engine (19103) :
case-daemon: server successfully spawned child process, pid 19111

Fri Apr 13 18:59:47 2007 Info: case antispam - engine (19111) :
startup: Region profile: Using profile global

Fri Apr 13 18:59:59 2007 Info: case antispam - engine (19111) : fuzzy:
Fuzzy plugin v7 successfully loaded, ready to roll

Fri Apr 13 19:00:01 2007 Info: case antispam - engine (19110) :
uribllocal: running URI blocklist local

Fri Apr 13 19:00:04 2007 Info: case antispam - engine (19111) : config:
Finished loading configuration
```

IronPort アンチウイルス ログの使用

表 5-23　アンチウイルス ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻
Message	メッセージは、アンチウイルス アップデートの確認と結果（エンジンまたはウイルス定義のアップデートが必要であったかどうかなど）で構成されます。

アンチウイルス ログの例

次のアンチウイルス ログの例は、Sophos アンチウイルス エンジンによる、ウイルス定義（IDE）とエンジン自体のアップデートの確認を示しています。

```
Thu Sep  9 14:18:04 2004 Info: Checking for Sophos Update

Thu Sep  9 14:18:04 2004 Info: Current SAV engine ver=3.84. No engine
update needed

Thu Sep  9 14:18:04 2004 Info: Current IDE serial=2004090902. No update
needed.
```

このログを一時的に DEBUG レベルに設定すると、アンチウイルス エンジンが所定のメッセージについて特定の結果を返した理由を診断するのに役立ちます。DEBUG ロギング情報は冗長です。使用の際は注意してください。

IronPort スパム検疫ログの使用

表 5-24　IronPort スパム ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻
Message	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。

IronPort スパム検疫ログの例

次のログの例は、検疫から admin@example.com にメッセージ（MID 8298624）が解放されている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
```

IronPort スパム検疫 GUI ログの使用

表 5-25　IronPort スパム GUI ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻
Message	メッセージは、ユーザ認証などの実行されたアクションで構成されます。

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。

```
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
```

IronPort LDAP デバッグ ログの使用

表 5-26　LDAP デバッグ ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻
Message	LDAP デバッグ メッセージ。

LDAP デバッグ ログの例

（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。

```
1    Thu Sep  9 12:24:56 2004 Begin Logfile

2    Thu Sep  9 12:25:02 2004 LDAP: Masquerade query sun.masquerade
     address employee@routing.qa to employee@mail.qa

3    Thu Sep  9 12:25:02 2004 LDAP: Masquerade query sun.masquerade
     address employee@routing.qa to employee@mail.qa

4    Thu Sep  9 12:25:02 2004 LDAP: Masquerade query sun.masquerade
     address employee@routing.qa to employee@mail.qa

5    Thu Sep  9 12:28:08 2004 LDAP: Clearing LDAP cache

6    Thu Sep  9 13:00:09 2004 LDAP: Query
     '(&(ObjectClass={g})(mailLocalAddress={a}))' to server sun
     (sun.qa:389)

7    Thu Sep  9 13:00:09 2004 LDAP: After substitute, query is
     '(&(ObjectClass=inetLocalMailRecipient)(mailLocalAddress=rroute.d000
     02b.loc@ldap.route.local.add00002.qa))'

8    Thu Sep  9 13:00:09 2004 LDAP: connecting to server

9    Thu Sep  9 13:00:09 2004 LDAP: connected
```

```
10   Thu Sep  9 13:00:09 2004 LDAP: Query
     (&(ObjectClass=inetLocalMailRecipient)(mailLocalAddress=rroute.d0000
     2b.loc@ldap.route.local.add00002.qa)) returned 1 results

11   Thu Sep  9 13:00:09 2004 LDAP: returning: [<LDAP:>]
```

前述のログ ファイルを読み取るためのガイドとして使用してください。

表 5-27　LDAP デバッグ ログの例の詳細

行番号	説明
1.	ログ ファイルが開始されます。
2. **3.** **4.**	リスナーは、明確に「sun.masquerade」という LDAP クエリーによって、マスカレードに LDAP を使用するように設定されています。 アドレス employee@routing.qa が LDAP サーバで検索され、一致が検出されます。その結果のマスカレード アドレスは employee@mail.qa であり、マスカレードの設定によってこのアドレスがメッセージ ヘッダー、エンベロープ送信者、またはその両方に書き込まれます。
5.	ユーザは手動で `ldapflush` を実行しています。
6.	クエリーは、sun.qa、ポート 389 に送信されます。クエリー テンプレートは (&(ObjectClass={g})(mailLocalAddress={a})) です。 {g} は、発信側フィルタ（rcpt-to-group または mail-from-group ルール）で指定されたグループ名に置換されます。 {a} は、当該のアドレスに置換されます。
7. **8.**	ここで代入（前述のとおり）が実行されます。LDAP サーバに送信される前のクエリーはこのようになります。
9.	サーバへの接続がまだ確立されていないので、接続します。

表 5-27　LDAP デバッグ ログの例の詳細（続き）

行番号	説明
10.	サーバに送信されるデータです。
11.	結果は、確実に空になります。つまり、1 つのレコードが返されますが、クエリーはフィールドを要求していないので、データは報告されません。これらは、データベースに一致があるかどうかをクエリーでチェックするときに、グループ クエリーと許可クエリーの両方に使用されます。

セーフリスト/ブロックリスト ログの使用

表 5-28 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 5-28　セーフリスト/ブロックリスト ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻。
Message	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.
```

レポーティング ログの使用

表 5-29 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 5-29　レポーティング ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻。
Message	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 5-30 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 5-30　レポーティング クエリー ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻。
Message	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.
```

アップデータ ログの使用

表 5-31　アップデータ ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻。
Message	メッセージは、システム サービス アップデート情報のほか、AsyncOS によるアップデートの確認と、スケジュールされている次回アップデートの日時で構成されます。

アップデータ ログの例

次のログの例は、アプライアンスが新規の McAfee アンチウイルス定義でアップデートされていることを示しています。

```
Fri Sep 19 11:07:51 2008 Info: Starting scheduled update

Fri Sep 19 11:07:52 2008 Info: Acquired server manifest, starting update
11

Fri Sep 19 11:07:52 2008 Info: Server manifest specified an update for
mcafee
```

```
Fri Sep 19 11:07:52 2008 Info: mcafee was signalled to start a new update

Fri Sep 19 11:07:52 2008 Info: mcafee processing files from the server
manifest

Fri Sep 19 11:07:52 2008 Info: mcafee started downloading files

Fri Sep 19 11:07:52 2008 Info: mcafee downloading remote file
"http://stage-updates.ironport.com/mcafee/dat/5388"

Fri Sep 19 11:07:52 2008 Info: Scheduled next update to occur at Fri Sep
19 11:12:52 2008

Fri Sep 19 11:08:12 2008 Info: mcafee started decrypting files

Fri Sep 19 11:08:12 2008 Info: mcafee decrypting file
"mcafee/dat/5388" with method "des3_cbc"

Fri Sep 19 11:08:17 2008 Info: mcafee started decompressing files

Fri Sep 19 11:08:17 2008 Info: mcafee started applying files

Fri Sep 19 11:08:17 2008 Info: mcafee applying file "mcafee/dat/5388"

Fri Sep 19 11:08:18 2008 Info: mcafee verifying applied files

Fri Sep 19 11:08:18 2008 Info: mcafee updating the client manifest

Fri Sep 19 11:08:18 2008 Info: mcafee update completed

Fri Sep 19 11:08:18 2008 Info: mcafee waiting for new updates

Fri Sep 19 11:12:52 2008 Info: Starting scheduled update

Fri Sep 19 11:12:52 2008 Info: Scheduled next update to occur at Fri Sep
19 11:17:52 2008

Fri Sep 19 11:17:52 2008 Info: Starting scheduled update

Fri Sep 19 11:17:52 2008 Info: Scheduled next update to occur at Fri Sep
19 11:22:52 2008
```

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、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`

認証ログの使用

認証ログには、成功したユーザ ログインと失敗したログイン試行が記録されます。

表 5-32　認証ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻。
Message	メッセージは、アプライアンスにログインしようとしたユーザのユーザ名と、そのユーザが正常に認証されたかどうかという情報で構成されます。

認証ログの例

次のログの例は、「admin」、「joe」、および「dan」というユーザによるログイン試行を示しています。

```
Wed Sep 17 15:16:25 2008 Info: Begin Logfile

Wed Sep 17 15:16:25 2008 Info: Version: 6.5.0-262 SN: XXXXXXX-XXXXX
```

```
Wed Sep 17 15:16:25 2008 Info: Time offset from UTC: 0 seconds

Wed Sep 17 15:18:21 2008 Info: User admin was authenticated successfully.

Wed Sep 17 16:26:17 2008 Info: User joe failed authentication.

Wed Sep 17 16:28:28 2008 Info: User joe was authenticated successfully.

Wed Sep 17 20:59:30 2008 Info: User admin was authenticated successfully.

Wed Sep 17 21:37:09 2008 Info: User dan failed authentication.
```

設定履歴ログの使用

設定履歴ログは、ユーザの名前が一覧表示された追加のセクションを含むコンフィギュレーション ファイル、ユーザが設定内のどこで変更を行ったかの説明、およびユーザがその変更をコミットするときに入力したコメント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。

設定履歴ログの例

次の設定履歴ログの例は、システムへのログインを許可されているローカル 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>
```

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。

- 「ロギングに対するグローバル設定」（P.5-64）
- 「ログ サブスクリプションのロール オーバー」（P.5-69）
- 「ホスト キーの設定」（P.5-77）

ログ サブスクリプションの設定

シスコの電子メール セキュリティ アプライアンスでは、既存のログ サブスクリプションを削除しないようにすることを推奨します。

[System Administration] の [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 サブスクリプションによって、エラーを含む AsyncOS アクティビティの情報を保存するログ ファイルが作成されます。ログ サブスクリプションは、取得されるか、または別のコンピュータに配信（プッシュ）されるかのどちらかです。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 5-33　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、表 5-1「ログ タイプ」（P.2）を参照してください。
Name	今後の参照に使用するログ サブスクリプションのニックネーム。
Rollover by File Size	ファイルの最大サイズ。このサイズに到達すると、ローリング オーバーされます。
Rollover by Time	ファイルのロールオーバーの時間間隔を設定します。
Log level	ログ サブスクリプションごとに詳細のレベルを設定します。
Retrieval method	ログ サブスクリプションが Cisco IronPort アプライアンスから取得される方法を定義します。
Log filename	ディスクに書き込むときのファイルの物理名に使用されます。複数の Cisco IronPort アプライアンスを使用している場合、ログ ファイルを生成したシステムを識別するため、ログ ファイル名を固有にする必要があります。

ログ レベル

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。詳細レベルを高くするほど大きいログ ファイルが作成され、システムのパフォーマンスが低下します。詳細レベルの高い設定には、詳細レベルの低い設定に保持されるすべてのメッセージと、その他のメッセージも含まれます。詳細レベルを上げるほど、システムのパフォーマンスは低下します。

（注） ログ レベルは、すべてのメール ログ タイプに対して選択できます。

表 5-34　ログ レベル

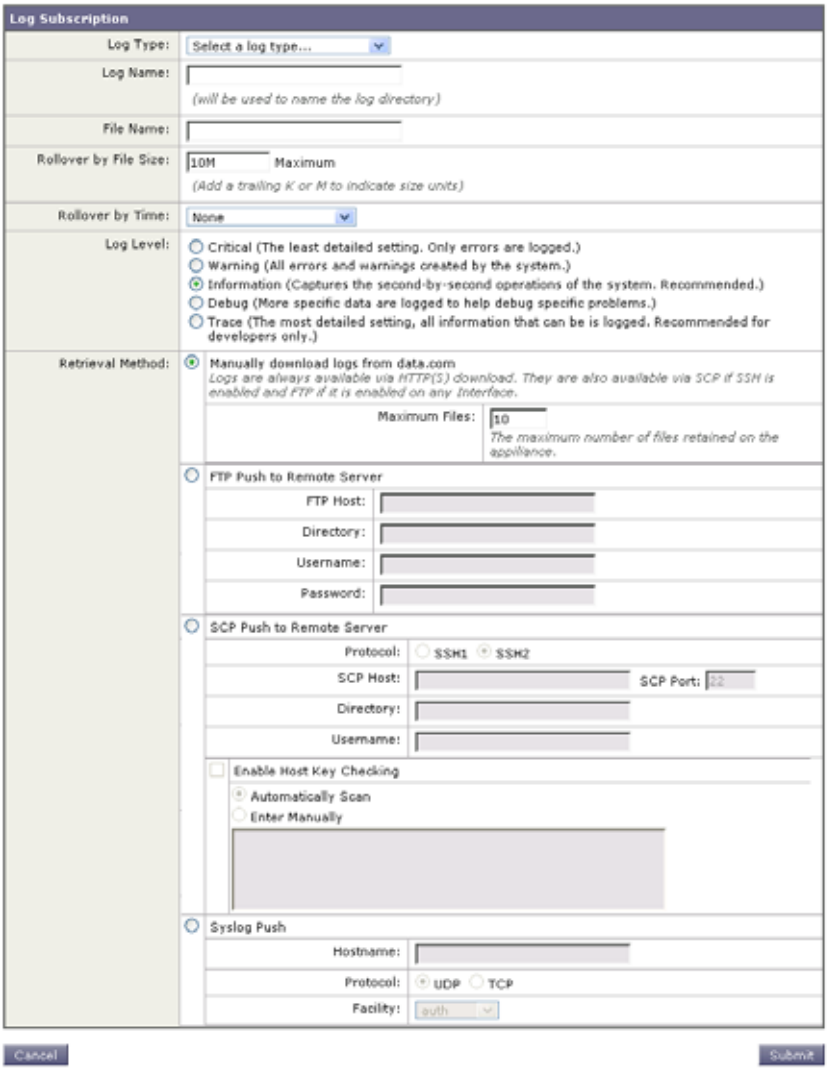
ログ レベル	説明
Critical	詳細レベルの最も低い設定。エラーだけがログに記録されます。この設定にすると、パフォーマンスやその他の重要なアクティビティをモニタできませんが、ログ ファイルがすぐには最大サイズに達しなくなります。このログ レベルは、syslog レベル「Alert」と同等です。
Warning	システムによって作成されたすべてのエラーと警告。この設定にすると、パフォーマンスやその他の重要なアクティビティをモニタできません。このログ レベルは、syslog レベル「Warning」と同等です。
Information	情報設定では、システムの秒単位の動作がキャプチャされます。たとえば、接続のオープンや配信試行などです。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	エラーの原因を調べるときは、Debug ログ レベルを使用します。この設定は一時的に使用し、後でデフォルト レベルに戻します。このログ レベルは、syslog レベル「Debug」と同等です。
Trace	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　[Log Subscription] ページで [Add Log Subscription] をクリックします。次の [New Log Subscription] ページが表示されます。

図 5-1　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　AsyncOS がログ ファイルをロールオーバーする前の最大ファイル サイズ、およびロールオーバー間の時間間隔を指定します。ファイルのロールオーバーの詳細については、「ログ サブスクリプションのロール オーバー」（P.5-69）を参照してください。

ステップ 4　ログ レベルを選択します。使用可能なオプションは、[Critical]、[Warning]、[Information]、[Debug]、または [Trace] です。

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 Settings] カラムにあるログの名前をクリックします。[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変更します。

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、IronPort テキスト メール ログおよび IronPort ステータス ログ内にシステムの測定を定期的に記録します。[System Administration] > [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。

- システムの測定頻度。これは、システムが測定を記録するまで待機する時間（秒単位）です。
- 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のリスト。

すべての IronPort ログには、次の 3 つのデータを任意で記録できます。

1. 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 自体で生成される場合があります。次の例を参考にしてください。

```
Tue Apr 6 14:38:34 2004 Info: MID 1 Message-ID Message-ID-Content
```

2. Remote Response

   このオプションを設定すると、可能な場合はすべてのメッセージのリモート応答ステータス コードがログに記録されます。次の例を参考にしてください。

```
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 応答の場合は 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、文字列「Message MID accepted」がログに記録されます。

3. 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）に、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 IronPort テキスト メール ログ、IronPort 配信ログ、および IronPort バウンス 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 5-35　ログ ヘッダー

Header name	ヘッダーの名前
Value	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。

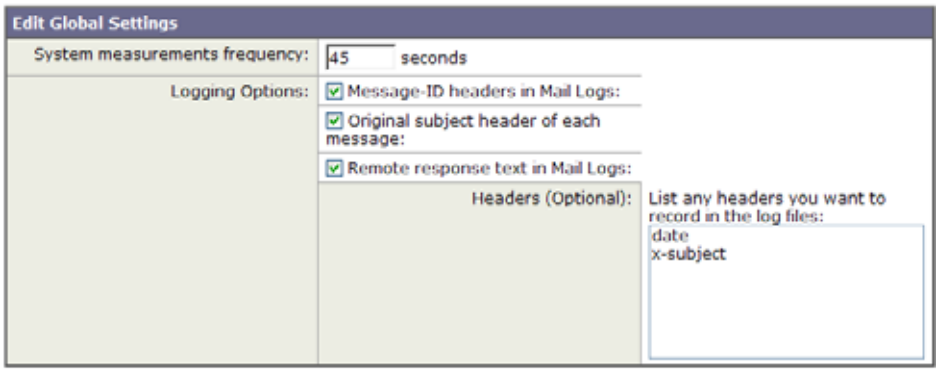
```
Tue May 31 10:14:12 2005 Info: Message done DCID 0 MID 3 to RID [0]
[('date', 'Tue, 31 May 2005 10:13:18 -0700'), ('x-subject', 'Logging this
header')]
```

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 5-2　ログ サブスクリプションのグローバル設定



ステップ 2　システム測定頻度、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

アプライアンス上のログ ファイルが大きくなりすぎないようにするために、ログ ファイルがユーザ指定の最大ファイル サイズまたは時間間隔に達すると、AsyncOS は「ロールオーバー」を実行してログ ファイルをアーカイブし、着信するログ データのための新しいファイルを作成します。ログ サブスクリプション用に定義された取得方法に基づいて、古いログ ファイルは取得のためにアプライアンス上に保管されるか、または外部のコンピュータに配信されます。アプライアンスからログ ファイルを取得する方法の詳細については、「ログ取得方法」（P.5-11）を参照してください。

AsyncOS は、ログ ファイルをロールオーバーするときに次のアクションを実行します。

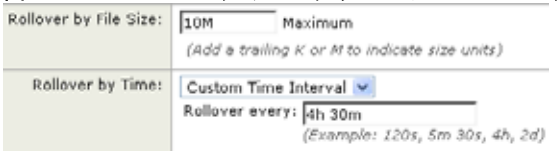
- 現在のログ ファイルの名前をロールオーバーのタイムスタンプと、保存済みを示す文字「**s**」の拡張子を使用して変更します。
- 新しいログ ファイルを作成し、「**current**」の拡張子を使用して、そのファイルを最新として指定します。
- 新しく保存されたログ ファイルをリモート ホストに転送します（プッシュ ベースの取得方法を使用している場合）。
- 同じサブスクリプションから、以前に失敗したログ ファイルをすべて転送します（プッシュ ベースの取得方法を使用している場合）。
- 保存すべきファイルの総数を超えた場合は、ログ サブスクリプション内の最も古いファイルを削除します（ポーリング ベースの取得方法を使用している場合）。

ログ サブスクリプションのロールオーバーの設定は、GUI の [System Administration] > [Log Subscriptions] ページ、または CLI の `logconfig` コマンドを使用してサブスクリプションを作成または編集するときに定義します。ログ ファイルのロールオーバーをトリガーするために使用できる 2 つの設定は次のとおりです。

- 最大ファイル サイズ。
- 時間間隔。

図 5-3 に、GUI でログ サブスクリプションに使用できるロールオーバーの設定を示します。

図 5-3　ログ サブスクリプションのためのログ ファイルのロールオーバーの設定



ファイル サイズによるロールオーバー

AsyncOS は、ログ ファイルで使用されるディスク領域が多くなりすぎないようにするために、最大ファイル サイズに達したログ ファイルをロールオーバーします。ロールオーバーのための最大ファイル サイズを定義する場合は、メガバイトを示す `m` とキロバイトを示す `k` のサフィックスを使用します。たとえば、ログ ファイルが 10 MB に達したら AsyncOS によってロールオーバーされるようにする場合は、「`10m`」と入力します。

時間によるロールオーバー

ロールオーバーを定期的に実行されるようにスケジュールする場合は、次のいずれかの時間間隔を選択できます。

- [None]。AsyncOS は、ログ ファイルが最大ファイル サイズに達した場合にのみロールオーバーを実行します。
- [Custom Time Interval]。AsyncOS は、以前のロールオーバーから指定された時間が経過した後にロールオーバーを実行します。スケジュール設定されたロールオーバーのためのカスタムの時間間隔を作成するには、`d`、`h`、および `m` をサフィックスとして使用して、ロールオーバー間の日数、時間数、および分数を入力します。
- [Daily Rollover]。AsyncOS は、毎日指定された時刻にロールオーバーを実行します。日単位のロールオーバーを選択した場合は、24 時間形式（HH:MM）を使用して、AsyncOS がロールオーバーを実行する時刻を入力します。

  GUI では、[Daily Rollover] オプションのみが提供されます。CLI の `logconfig` コマンドを使用して日単位のロールオーバーを設定する場合は、[Weekly Rollover] オプションを選択し、アスタリスク（*）を使用して AsyncOS がすべての曜日にロールオーバーを実行することを指定します。

- [Weekly Rollover]。AsyncOS は、1 つ以上の曜日の指定された時刻にロールオーバーを実行します。たとえば、毎週水曜日と金曜日の午前 0：00 にログ ファイルをロールオーバーするように AsyncOS を設定できます。週単位のロールオーバーを設定するには、ロールオーバーを実行する曜日と 24 時間形式（HH:MM）の時刻を選択します。

  CLI を使用している場合は、ダッシュ（-）を使用して日の範囲を指定するか、アスタリスク（*）を使用してすべての曜日を指定するか、またはカンマ（,）を使用して複数の日と時刻を区切ることができます。

図 5-4 に、GUI で [Weekly Rollover] オプションに使用できる設定を示します。

図 5-4　GUI での週単位のログ ロールオーバーの設定

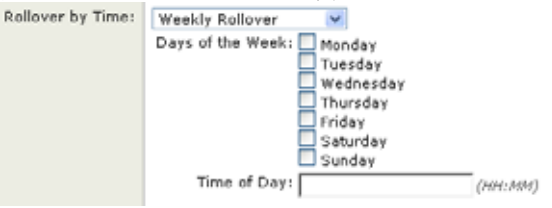


表 5-36 に、CLI を使用して、水曜日と金曜日の午前 0:00（00:00）にログ サブスクリプションのファイルをロールオーバーする方法を示します。

表 5-36　CLI での週単位のログ ロールオーバーの設定

```
Do you want to configure time-based log files rollover? [N]> y



Configure log rollover settings:

1. Custom time interval.

2. Weekly rollover.

[1]> 2



1. Monday

2. Tuesday

3. Wednesday

4. Thursday

5. Friday

6. Saturday

7. Sunday

Choose the day of week to roll over the log files.  Separate multiple
days with comma, or use "*" to specify every day of a week.  Also you
can use dash to specify a range like "1-5":

[]> 3, 5



Enter the time of day to rollover log files in 24-hour format
(HH:MM).  You can specify hour as "*" to match every hour, the same
for minutes.  Separate multiple times of day with comma:

[]> 00:00
```

オンデマンドでのログ サブスクリプションのロールオーバー

GUI を使用してログ サブスクリプションをただちに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　[System Administration] > [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。

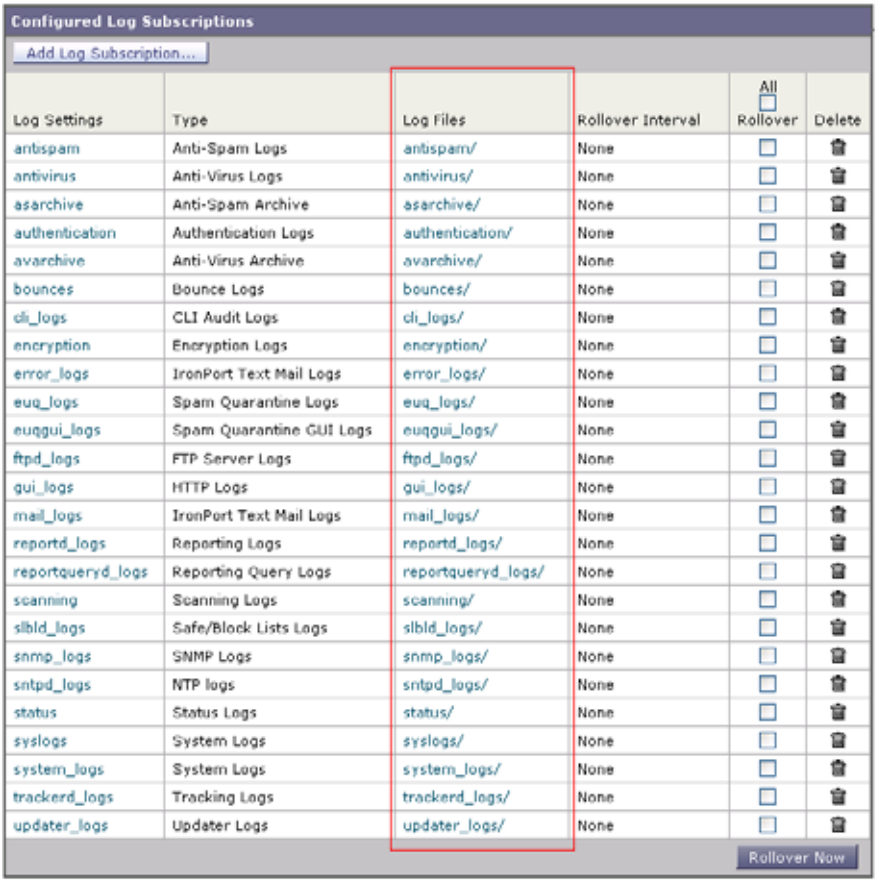
ステップ 2　任意で、[All] チェックボックスをオンにして、すべてのログをロールオーバー対象として選択できます。

ステップ 3　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。[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。

GUI 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、パスワードの入力を求められてから、そのサブスクリプションに対するログ ファイルの一覧が表示されます。次に、いずれかのログ ファイルをクリックして、ブラウザに表示したり、ディスクに保存したりすることができます。GUI を介してログを表示するには、管理インターフェイスで HTTP または HTTPS サービスをイネーブルにしておく必要があります。

図 5-5　ログ サブスクリプションのグローバル設定



CLI での最近のログ 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+ C を押して、`tail` コマンドを終了します。

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（このログは、特に commit コマンドによるユーザのコメントを追跡します）。また、tail コマンドでは、パラメータとして表示するログの名前 tail mail_logs が受け入れられています。

```
mail3.example.com> tail


Currently configured logs:

1. "antispam" Type: "Anti-Spam Logs" Retrieval: Manual Download

2. "antivirus" Type: "Anti-Virus Logs" Retrieval: Manual Download

3. "asarchive" Type: "Anti-Spam Archive" Retrieval: Manual Download

4. "authentication" Type: "Authentication Logs" Retrieval: Manual
Download

5. "avarchive" Type: "Anti-Virus Archive" Retrieval: Manual Download

6. "bounces" Type: "Bounce Logs" Retrieval: Manual Download

7. "cli_logs" Type: "CLI Audit Logs" Retrieval: Manual Download

8. "encryption" Type: "Encryption Logs" Retrieval: Manual Download

9. "error_logs" Type: "IronPort Text Mail Logs" Retrieval: Manual
Download

10. "euq_logs" Type: "IronPort Spam Quarantine Logs" Retrieval: Manual
Download

11. "euqgui_logs" Type: "IronPort Spam Quarantine GUI Logs" Retrieval:
Manual Download

12. "ftpd_logs" Type: "FTP Server Logs" Retrieval: Manual Download

13. "gui_logs" Type: "HTTP Logs" Retrieval: Manual Download
```

```
14. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: Manual
Download

15. "reportd_logs" Type: "Reporting Logs" Retrieval: Manual Download

16. "reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: Manual
Download

17. "scanning" Type: "Scanning Logs" Retrieval: Manual Download

18. "slbld_logs" Type: "Safe/Block Lists Logs" Retrieval: Manual
Download

19. "sntpd_logs" Type: "NTP logs" Retrieval: Manual Download

20. "status" Type: "Status Logs" Retrieval: Manual Download

21. "system_logs" Type: "System Logs" Retrieval: Manual Download

22. "trackerd_logs" Type: "Tracking Logs" Retrieval: Manual Download

23. "updater_logs" Type: "Updater Logs" Retrieval: Manual Download



Enter the number of the log you wish to tail.

[]> 19



Press Ctrl-C to stop.

Mon Feb 21 12:25:10 2011 Info: PID 274: User system commit changes:
Automated Update for Quarantine Delivery Host

Mon Feb 21 23:18:10 2011 Info: PID 19626: User admin commit changes:

Mon Feb 21 23:18:10 2011 Info: PID 274: User system commit changes:
Updated filter logs config
```

```
Mon Feb 21 23:46:06 2011 Info: PID 25696: User admin commit changes:
Receiving suspended.

^Cmail3.example.com>
```

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 キーを管理するには、「セキュア シェル（SSH）キーの管理」（P.8-71）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 5-37　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、AsyncOS によってホスト キーがスキャンされ、ホスト用に追加されます。

```
mail3.example.com> logconfig


Currently configured logs:

[ list of logs ]


Choose the operation you want to perform:

- NEW - Create a new log.

- EDIT - Modify a log subscription.

- DELETE - Remove a log subscription.

- SETUP - General settings.

- LOGHEADERS - Configure headers to log.

- HOSTKEYCONFIG - Configure SSH host keys.

[]> hostkeyconfig


Currently installed host keys:

1. mail3.example.com ssh-dss [ key displayed ]


Choose the operation you want to perform:

- NEW - Add a new key.

- EDIT - Modify a key.
```

```
- DELETE - Remove a key.

- SCAN - Automatically download a host key.

- PRINT - Display a key.

- HOST - Display system host keys.

- FINGERPRINT - Display system host key fingerprints.

- USER - Display system user keys.

[]> scan


Please enter the host or IP address to lookup.

[]> mail3.example.com


Choose the ssh protocol type:

1. SSH1:rsa

2. SSH2:rsa

3. SSH2:dsa

4. All

[4]>


SSH2:dsa

mail3.example.com ssh-dss

[ key displayed ]
```

```
SSH2:rsa

mail3.example.com ssh-rsa

[ key displayed ]


SSH1:rsa

mail3.example.com 1024 35

[ key displayed ]


Add the preceding host key(s) for mail3.example.com? [Y]>


Currently installed host keys:

1. mail3.example.com ssh-dss [ key displayed ]

2. mail3.example.com ssh-rsa [ key displayed ]

3. mail3.example.com 1024 35 [ key displayed ]


Choose the operation you want to perform:

- NEW - Add a new key.

- EDIT - Modify a key.

- DELETE - Remove a key.

- SCAN - Automatically download a host key.

- PRINT - Display a key.

- HOST - Display system host keys.
```

```
- FINGERPRINT - Display system host key fingerprints.

- USER - Display system user keys.

[]>


Currently configured logs:

[ list of configured logs ]


Choose the operation you want to perform:

- NEW - Create a new log.

- EDIT - Modify a log subscription.

- DELETE - Remove a log subscription.

- SETUP - General settings.

- LOGHEADERS - Configure headers to log.

- HOSTKEYCONFIG - Configure SSH host keys.

[]>


mail3.example.com> commit
```

CHAPTER 6

CLI による管理およびモニタリング

Cisco IronPort アプライアンスには、ログを解析せずに電子メール動作をモニタするためのコマンドが用意されています。Cisco IronPort アプライアンスのモニタには、コマンドライン インターフェイス（CLI）とグラフィカル ユーザ インターフェイス（GUI）のいずれかを使用できます。この章では、モニタリングおよび管理コマンドについて、また CLI を使ってそれらのコマンドにアクセスする方法について説明します。コンポーネントの多くは GUI から使用することもできます。GUI については、第 7 章「GUI でのその他の作業」を参照してください。

この章は、次の内容で構成されています。

使用可能なモニタリング コンポーネントの読み取り

システムのモニタリングには、次の 3 つの主要コンポーネントがあります。

- カウンタ
- ゲージ
- レート

カウンタの読み取り

カウンタは、システム内の各種イベントの現在までの合計を示します。カウンタごとに、そのカウンタのリセット以降、最後のシステム リブート以降、およびシステムの存続期間に発生したイベントの合計数を表示できます。

カウンタは、イベントが発生するごとに増加し、次の 3 つのバージョンで表示されます。

Reset	`resetcounters` コマンドによる最後のカウンタ リセット以降
Uptime	最後のシステム リブート以降
Lifetime	Cisco IronPort アプライアンスの存続期間中の合計

表 6-1 に、Cisco IronPort アプライアンスをモニタするときに使用できるカウンタとその説明を示します。

（注） これは、全体的なリストです。表示されるカウンタは、選択した表示オプションまたはコマンドによって異なります。このリストは参照用として使用してください。

表 6-1　カウンタ

統計	説明
Receiving	
Messages Received	配信キューに受信されたメッセージ。
Recipients Received	受信されたすべてのメッセージの受信者。
Generated Bounce Recipients	システムによってバウンスが生成され、配信キューに挿入された対象の受信者。

表 6-1　カウンタ（続き）

統計	説明
Rejection	
Rejected Recipients	Recipient Access Table（RAT; 受信者アクセス テーブル）によって、または早期接続終了などの予期しないプロトコル ネゴシエーションによって配信キューへの受信を拒否された受信者。
Dropped Messages	フィルタ ドロップ アクションの一致によって配信キューへの受信を拒否されたメッセージ、またはブラック ホール キューイング リスナーによって受信されたメッセージ。エイリアス テーブル内の `/dev/null` エントリ宛てのメッセージは、ドロップされたメッセージと見なされます。アンチスパム フィルタリング（システムでイネーブルになっている場合）によってドロップされたメッセージも、このカウンタに計上されます。
Queue	
Soft Bounced Events	ソフト バウンス イベントの数。複数回ソフト バウンスしたメッセージには、複数のソフト バウンス イベントが設定されます。
Completion	
Completed Recipients	ハード バウンスされた受信者、配信された受信者、および削除された受信者の総合計。配信キューから削除されたすべての受信者。
Hard Bounced Recipients	DNS ハード バウンス、5XX ハード バウンス、フィルタ ハード バウンス、期限切れハード バウンス、およびその他のハード バウンスの総合計。受信者へのメッセージの配信に失敗し、配信がただちに終了となったものを表します。
DNS Hard Bounces	受信者へのメッセージの配信試行中に検出された DNS エラー。
5XX Hard Bounces	受信者へのメッセージの配信試行中に、宛先メール サーバから「5XX」応答コードが返されたものを表します。
Expired Hard Bounces	配信キューに許容されている最大時間、または最大接続試行回数を超えているメッセージ受信者。

表 6-1　カウンタ（続き）

統計	説明
Filter Hard Bounces	一致フィルタの bounce アクションによってプリエンプトされた受信者の配信。アンチスパム フィルタリング（システムでイネーブルになっている場合）によってドロップされたメッセージも、このカウンタに計上されます。
Other Hard Bounces	メッセージ配信中の予期しないエラー。または、メッセージ受信者が bouncerecipients コマンドによって明示的にバウンスされたものを表します。
Delivered Recipients	メッセージが正常に配信された受信者。
Deleted Recipients	deleterecipients コマンドによって明示的に削除されたメッセージ受信者、またはグローバル配信停止リストに合致するメッセージ受信者の合計。
Global Unsubscribe Hits	グローバル配信停止設定との一致により削除されたメッセージ受信者。
Current IDs	
Message ID (MID)	配信キューに挿入されたメッセージに割り当てられた最後のメッセージ ID。MID は、Cisco IronPort アプライアンスによって受信されたすべてのメッセージに関連付けられており、メール ログで追跡できます。MID は、2^{31} でゼロにリセットされます。
Injection Connection ID (ICID)	リスナー インターフェイスへの接続に割り当てられた最後のインジェクション接続 ID。ICID は 2^{31} でロール オーバー（ゼロにリセット）されます。
Delivery Connection ID (DCID)	宛先メール サーバへの接続に割り当てられた最後の配信接続 ID。DCID は 2^{31} でロール オーバー（ゼロにリセット）されます。

ゲージの読み取り

ゲージは、メモリ、ディスク スペース、またはアクティブ接続などのシステム リソースの現在の使用率を示します。

表 6-2 に、Cisco IronPort アプライアンスをモニタするときに使用できるゲージとその説明を示します。

（注）　これは、全体的なリストです。表示されるゲージは、選択した表示オプションまたはコマンドによって異なります。このリストは参照用として使用してください。

表 6-2　　ゲージ

統計	説明
System Gauges	
RAM Utilization	システムによる物理 Random Access Memory（RAM; ランダム アクセス メモリ）の使用率。
CPU Utilization	CPU 使用率。
Disk I/O Utilization	ディスク I/O の使用率。 （注）　Disk I/O Utilization ゲージには、既知の値の測定は表示されません。このゲージには、これまでにシステムで確認され、最後のリブート以降の最大値に対して測定された I/O 使用率が表示されます。したがって、ゲージに 100 % と表示されている場合、システムでは起動後最も高いレベルの I/O 使用率が発生しています（必ずしも、システム全体の 100 % の物理ディスク I/O を表すものではありません）。
Resource Conservation	0 ～ 60 または 999 の値。0 ～ 60 の数値は、重要なシステム リソースの急速な消耗を防止するために、システムがメッセージの受け入れを減らしている度合いを表しています。数値が大きいほど、受け入れを減らす度合いが大きくなります。ゼロは、受け入れの減少がないことを示します。このゲージに 999 と表示されている場合、システムは「リソース節約モード」になっており、メッセージは受け入れられません。システムがリソース節約モードかどうかに関係なく、アラート メッセージは送信されます。
Disk Utilization: Logs	ログに使用されているディスクの割合。ステータス ログには LogUsd、XML ステータスには log_used として表示されます。

表 6-2　ゲージ（続き）

統計	説明
Connections Gauges	
Current Inbound Connections	リスナー インターフェイスへの現在の着信接続。
Current Outbound Connections	宛先メール サーバへの現在の発信接続。
Queue Gauges	
Active Recipients	配信キュー内のメッセージ受信者。Unattempted Recipients と Attempted Recipients の合計。
Unattempted Recipients	Active Recipients のサブカテゴリ。配信がまだ試行されていない、キュー内のメッセージ受信者。
Attempted Recipients	Active Recipients のサブカテゴリ。試行されたものの、ソフト バウンス イベントによって失敗した配信の対象となっている、キュー内のメッセージ受信者。
Messages in Work Queue	キューに入る前に、エイリアス テーブル拡張、マスカレード、アンチスパム、アンチウイルス スキャン、メッセージ フィルタ、および LDAP クエリーによる処理を待つメッセージの数。
Messages in Quarantine	検疫エリア内にあるメッセージに、解放または削除されたが実際の処理がまだ行われていないメッセージを足した一意の数。たとえば、Outbreak からすべての検疫対象メッセージを解放すると、Outbreak の合計メッセージ数はただちにゼロになりますが、このフィールドでは、完全に配信されるまでの検疫対象メッセージが反映されます。

表 6-2　ゲージ（続き）

統計	説明
Destinations in Memory	メモリ内の宛先ドメインの数。メッセージの配信先となる各ドメインに対して、宛先オブジェクトがメモリ内に作成されます。そのドメインに対するすべてのメールが配信された後、宛先オブジェクトは 3 時間保持されます。3 時間のうちに、そのドメインに対して新しいメッセージがバインドされなければ、オブジェクトは期限切れとなり、宛先は（`tophosts` コマンドなどで）報告されなくなります。1 つのドメインだけにメールを配信する場合、このカウンタは「1」になります。メッセージを送信したことがない（または、長い時間アプライアンスによってメッセージが処理されていない）場合、カウンタは「0」になります。 仮想ゲートウェイを使用している場合、各仮想ゲートウェイの宛先ドメインには別個の宛先オブジェクトが作成されます（たとえば、3 つの異なる仮想ゲートウェイから yahoo.com に配信している場合、yahoo.com が 3 つの宛先オブジェクトとしてカウントされます）。
Kilobytes Used	使用されるキュー ストレージ（キロバイト単位）。
Kilobytes in Quarantine	検疫対象メッセージに使用されるキュー ストレージ。メッセージ サイズと、上記の Messages in Quarantine にカウントされている受信者ごとに 30 バイトを足した値になります。この計算では通常、使用されるスペースが*過大に見積もられます*。
Kilobytes Free	残りのキュー ストレージ（キロバイト単位）。

レートの読み取り

すべてのレートは、クエリーが作成された特定の時点における、1 時間あたりの平均イベント発生レートを示します。レートには、過去 1 分間、5 分間、および 15 分間という 3 つの間隔で 1 時間あたりの平均レートが計算されます。

たとえば、Cisco IronPort アプライアンスが 1 分で 100 の受信者を受信すると、1 分間隔に対するレートは 1 時間あたり 6,000 となります。5 分間隔に対するレートは 1 時間あたり 1,200 となり、15 分間隔に対するレートは 1 時間あたり 400 となります。レートは、1 分間のレートが継続した場合の 1 時間あたりの平均レートを示すように計算されます。したがって、1 分で 100 件のメッセージのほうが 15 分で 100 件のメッセージよりもレートは高くなります。

表 6-3 に、Cisco IronPort アプライアンスをモニタするときに使用できるレートとその説明を示します。

（注） これは、全体的なリストです。表示されるレートは、選択した表示オプションまたはコマンドによって異なります。このリストは参照用として使用してください。

表 6-3　レート

統計	説明
Messages Received	1 時間あたりに配信キューに挿入されるメッセージのレート。
Recipients Received	1 時間あたりに配信キューに挿入されるすべてのメッセージに対する受信者数のレート。
Soft Bounced Events	1 時間あたりのソフト バウンス イベント数のレート（複数回ソフト バウンスしたメッセージには、複数のソフト バウンス イベントが設定されます）。
Completed Recipients	ハード バウンスされた受信者、配信された受信者、および削除された受信者の総合計のレート。配信キューから削除された受信者は、完了済みと見なされます。
Hard Bounced Recipients	1 時間あたりの DNS ハード バウンス、5XX ハード バウンス、フィルタ ハード バウンス、期限切れハード バウンス、およびその他のハード バウンスの総合計のレート。ハード バウンスとは、受信者へのメッセージの配信試行に失敗し、その配信がただちに終了されることをいいます。
Delivered Recipients	受信者に正常に配信された 1 時間あたりのメッセージ数のレート。

CLI によるモニタリング

ここでは、次の内容について説明します。

電子メール ステータスのモニタリング

Cisco IronPort アプライアンスにおける電子メール動作のステータスをモニタすることが必要になることがあります。`status` コマンドは、電子メール動作についてモニタされる情報のサブセットを返します。返された統計情報は、カウンタとゲージのいずれかの形式で表示されます。カウンタは、システム内の各種イベントの現在までの合計を示します。カウンタごとに、そのカウンタのリセット以降、最後のシステム リブート以降、およびシステムの存続期間に発生したイベントの合計数を表示できます。ゲージは、メモリ、ディスク スペース、またはアクティブ接続などのシステム リソースの現在の使用率を示します。

各項目の説明については、「使用可能なモニタリング コンポーネントの読み取り」（P.6-1）を参照してください。

表 6-4　メール ステータス

統計	説明
Status as of	現在のシステム日時を表示します。
Last counter reset	カウンタが最後にリセットされた時刻を表示します。

表 6-4　メール ステータス（続き）

統計	説明
System status	online、offline、receiving suspended、または delivery suspended。ステータスが receiving suspended になるのは、すべてのリスナーが一時停止した場合のみです。すべてのリスナーに対する受信と配信が一時停止されると、ステータスは offline になります。
Oldest Message	システムによる配信を待つ、最も古いメッセージを表示します。
Features	`featurekey` コマンドによってシステムにインストールされた特別な機能を表示します。

例

```
mail3.example.com> status


Status as of:              Thu Oct 21 14:33:27 2004 PDT
Up since:                    Wed Oct 20 15:47:58 2004 PDT (22h 45m 29s)
Last counter reset:        Never
System status:             Online
Oldest Message:             4 weeks 46 mins 53 secs


Counters:                     Reset          Uptime        Lifetime
  Receiving
    Messages Received      62,049,822         290,920      62,049,822
    Recipients Received    62,049,823         290,920      62,049,823
  Rejection
    Rejected Recipients     3,949,663          11,921       3,949,663
    Dropped Messages       11,606,037             219      11,606,037
  Queue
    Soft Bounced Events     2,334,552          13,598       2,334,552
  Completion
    Completed Recipients   50,441,741         332,625      50,441,741
  Current IDs
    Message ID (MID)                                      99524480
```

```
    Injection Conn. ID (ICID)                              51180368
    Delivery Conn. ID (DCID)                               17550674


Gauges:                                  Current
  Connections
    Current Inbound Conn.                      0
    Current Outbound Conn.                    14
  Queue
    Active Recipients                      7,166
    Messages In Work Queue                     0
    Messages In Quarantine                16,248
    Kilobytes Used                       387,143
      Kilobytes In Quarantine            338,206
    Kilobytes Free                    39,458,745


mail3.example.com>
```

詳細な電子メール ステータスのモニタリング

`status detail` コマンドは、電子メール動作についてモニタされた詳細な情報を返します。返された統計情報は、カウンタ、レート、およびゲージのいずれかのカテゴリで表示されます。カウンタは、システム内の各種イベントの現在までの合計を示します。カウンタごとに、そのカウンタのリセット以降、最後のシステム リブート以降、およびシステムの存続期間に発生したイベントの合計数を表示できます。ゲージは、メモリ、ディスク スペース、またはアクティブ接続などのシステム リソースの現在の使用率を示します。すべてのレートは、クエ

リーが作成された特定の時点における、1 時間あたりの平均イベント発生レートを示します。レートには、過去 1 分間、5 分間、および 15 分間という 3 つの間隔で 1 時間あたりの平均レートが計算されます。各項目の説明については、「使用可能なモニタリング コンポーネントの読み取り」（P.6-1）を参照してください。

例

```
mail3.example.com> status detail


Status as of:           Thu Jun 30 13:09:18 2005 PDT
Up since:                Thu Jun 23 22:21:14 2005 PDT (6d 14h 48m 4s)
Last counter reset:            Tue Jun 29 19:30:42 2004 PDT
System status:                 Online
Oldest Message:                No Messages
Feature - IronPort Anti-Spam:  17 days
Feature - Sophos:              Dormant/Perpetual
Feature - Outbreak Filters: Dormant/Perpetual
Feature - Central Mgmt:        Dormant/Perpetual


Counters:                         Reset          Uptime        Lifetime
  Receiving
    Messages Received       2,571,967          24,760       3,113,176
    Recipients Received     2,914,875          25,450       3,468,024
    Gen. Bounce Recipients      2,165               0           7,451
  Rejection
    Rejected Recipients     1,019,453             792       1,740,603
    Dropped Messages        1,209,001              66       1,209,028
  Queue
```

```
  Soft Bounced Events          11,236               0          11,405
Completion
  Completed Recipients      2,591,740          49,095       3,145,002
    Hard Bounced Recipients     2,469               0           7,875
      DNS Hard Bounces            199               0           3,235
      5XX Hard Bounces          2,151               0           4,520
      Expired Hard Bounces        119               0             120
      Filter Hard Bounces           0               0               0
      Other Hard Bounces            0               0               0
    Delivered Recipients      2,589,270          49,095       3,137,126
    Deleted Recipients              1               0               1
      Global Unsub. Hits            0               0               0
  DomainKeys Signed Msgs           10               9              10

Current IDs
  Message ID (MID)                                               7615199
  Injection Conn. ID (ICID)                                      3263654
  Delivery Conn. ID (DCID)                                       1988479

Rates (Events Per Hour):       1-Minute       5-Minutes      15-Minutes
  Receiving
    Messages Received               180             300             188
```

```
  Recipients Received          180            300            188
Queue
  Soft Bounced Events            0              0              0
Completion
  Completed Recipients         360            600            368
    Hard Bounced Recipients      0              0              0
    Delivered Recipients       360            600            368


Gauges:                                   Current
  System
    RAM Utilization                            1%
    CPU Utilization
      MGA                                      0%
      AntiSpam                                 0%
      AntiVirus                                0%
    Disk I/O Utilization                       0%
    Resource Conservation                       0
  Connections
    Current Inbound Conn.                       0
    Current Outbound Conn.                      0
  Queue
    Active Recipients                           0
```

```
  Unattempted Recipients                0
  Attempted Recipients                  0
Messages In Work Queue                  0
Messages In Quarantine                 19
Destinations In Memory                  3
Kilobytes Used                        473
  Kilobytes In Quarantine             473
Kilobytes Free                 39,845,415
```

（注）　新たにインストールされたアプライアンスでは、最も古いメッセージ カウンタにメッセージが示される場合がありますが、実際にはカウンタに示される受信者はありません。リモート ホストが接続されており、メッセージの受信が非常に遅い（つまり、メッセージを受信するまでに数分かかる）場合には、受信された受信者カウンタに「0」と表示され、最も古いメッセージ カウンタに「1」と表示されることがあります。これは、最も古いメッセージ カウンタに進行中のメッセージが表示されるためです。接続が最終的にドロップされると、カウンタはリセットされます。

メール ホストのステータスのモニタリング

特定の受信者ホストへの配信に問題があると思われる場合や、仮想ゲートウェイ アドレスに関する情報を収集する場合には、hoststatus コマンドを実行するとそれらの情報を表示できます。hoststatus コマンドは、特定の受信者ホストに関する電子メール動作のモニタリング情報を返します。コマンドには、取得するホスト情報のドメインを入力する必要があります。AsyncOS キャッシュに格納されている DNS 情報と、受信者ホストから最後に返されたエラーも表示されます。返されるデータは、最後に実行した resetcounters コマンドからの累積です。返される統計情報は、カウンタとゲージの 2 つのカテゴリに表示されます。各項目の説明については、「使用可能なモニタリング コンポーネントの読み取り」（P.6-1）を参照してください。

また、hoststatus コマンドに固有のその他のデータも返されます。

表 6-5　hoststatus コマンドのその他のデータ

統計	説明
Pending Outbound Connections	開いている接続や作業中の接続とは対照的な、宛先メール ホストへの保留中、または「初期」接続。Pending Outbound Connections は、プロトコルのグリーティングの段階にまだ達していない接続です。
Oldest Message	このドメインに対する配信キュー内で最も古いアクティブ受信者の経過時間。このカウンタは、ソフト バウンス イベントやホストの停止によって配信できない、キュー内のメッセージの経過時間を判断するのに役立ちます。
Last Activity	このフィールドは、そのホストにメッセージ配信が試みられるたびに更新されます。
Ordered IP Addresses	このフィールドには、IP アドレスの Time To Live（TTL; 存続可能時間）、MX レコードに応じた IP アドレスの優先順位、および実際のアドレスが表示されます。MX レコードは、ドメインに対するメール サーバの IP アドレスを指定します。1 つのドメインが複数の MX レコードを持つことができます。各 MX レコードのメール サーバには優先順位が割り当てられます。優先順位の数値が最も小さい MX レコードが優先されます。
Last 5XX error	このフィールドには、ホストから返された最新の「5XX」ステータス コードと説明が表示されます。このフィールドが表示されるのは、5XX エラーが存在する場合のみです。
MX Records	MX レコードは、ドメインに対するメール サーバの IP アドレスを指定します。1 つのドメインが複数の MX レコードを持つことができます。各 MX レコードのメール サーバには優先順位が割り当てられます。優先順位の数値が最も小さい MX レコードが優先されます。
SMTP Routes for this host	このドメインに対して SMTP ルートが定義されている場合は、ここに表示されます。
Last TLS Error	このフィールドには、最新の発信 TLS 接続エラーの説明と、アプライアンスが確立を試みた TLS 接続のタイプが表示されます。このフィールドが表示されるのは、TLS エラーが存在する場合のみです。

仮想ゲートウェイ

次に示す仮想ゲートウェイ情報は、仮想ゲートウェイ アドレスを設定している場合のみ表示されます（『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Configuring the Gateway to Receive Email」を参照してください）。

表 6-6　hoststatus コマンドのその他の仮想ゲートウェイ データ

統計	説明
Host up/down	同じ名前のグローバル `hoststatus` フィールドと同じ定義。仮想ゲートウェイ アドレスごとに追跡されます。
Last Activity	同じ名前のグローバル `hoststatus` フィールドと同じ定義。仮想ゲートウェイ アドレスごとに追跡されます。
Recipients	このフィールドも、グローバル `hoststatus` コマンドの定義に対応します。Active Recipients フィールド：仮想ゲートウェイ アドレスごとに追跡されます。
Last 5XX error	このフィールドには、ホストから返された最新の 5XX ステータス コードと説明が表示されます。このフィールドが表示されるのは、5XX エラーが存在する場合のみです。

例

```
mail3.example.com> hoststatus

Recipient host:
[]> aol.com

Host mail status for: 'aol.com'
Status as of:          Tue Mar 02 15:17:32 2010
Host up/down:         up

Counters:
  Queue
    Soft Bounced Events                        0
  Completion
    Completed Recipients                       1
      Hard Bounced Recipients                  1
        DNS Hard Bounces                       0
        5XX Hard Bounces                       1
        Filter Hard Bounces                    0
        Expired Hard Bounces                   0
        Other Hard Bounces                     0
      Delivered Recipients                     0
```

```
      Deleted Recipients                        0


Gauges:

  Queue

    Active Recipients                           0

      Unattempted Recipients                    0

      Attempted Recipients                      0

    Connections

      Current Outbound Connections              0

      Pending Outbound Connections              0


Oldest Message        No Messages

Last Activity         Tue Mar 02 15:17:32 2010

Ordered IP addresses: (expiring at Tue Mar 02 16:17:32 2010)

    Preference   IPs

    15           64.12.137.121    64.12.138.89     64.12.138.120

    15           64.12.137.89     64.12.138.152    152.163.224.122

    15           64.12.137.184    64.12.137.89     64.12.136.57

    15           64.12.138.57     64.12.136.153    205.188.156.122

    15           64.12.138.57     64.12.137.152    64.12.136.89

    15           64.12.138.89     205.188.156.154  64.12.138.152

    15           64.12.136.121    152.163.224.26   64.12.137.184
```

```
    15          64.12.138.120    64.12.137.152    64.12.137.121


MX Records:
    Preference   TTL        Hostname
    15           52m24s     mailin-01.mx.aol.com
    15           52m24s     mailin-02.mx.aol.com
    15           52m24s     mailin-03.mx.aol.com
    15           52m24s     mailin-04.mx.aol.com


    Last 5XX Error:
    ----------
    550 REQUESTED ACTION NOT TAKEN: DNS FAILURE
 (at Tue Mar 02 15:17:32 2010 GMT) IP: 10.10.10.10
    ----------


   Last TLS Error:             Required - Verify
       ----------
       TLS required, STARTTLS unavailable
       (at Tue Mar 02 15:17:32 2010 GMT) IP: 10.10.10.10


Virtual gateway information:
============================================================
```

```
example.com (PublicNet_017):

    Host up/down:          up

    Last Activity          Wed June 22 13:47:02 2005

    Recipients             0
```

（注）　仮想ゲートウェイ アドレス情報は、altsrchost 機能を使用している場合のみ表示されます。

電子メール キューの構成の確認

電子メール キューに関する現在の情報を取得し、特定の受信者ホストに配信の問題（キューの増大など）があるかどうかを判断するには、tophosts コマンドを使用します。tophosts コマンドは、キュー内の上位 20 の受信者のリストを返します。リストは、アクティブ受信者、発信接続、配信済み受信者、ソフト バウンス イベント、およびハード バウンスされた受信者など、さまざまな統計情報別にソートできます。各項目の説明については、「使用可能なモニタリング コンポーネントの読み取り」（P.6-1）を参照してください。

例

```
mail3.example.com> tophosts


Sort results by:


1. Active Recipients

2. Connections Out

3. Delivered Recipients

4. Soft Bounced Events

5. Hard Bounced Recipients

[1]> 1


Status as of:         Mon Nov 18 22:22:23 2003

                    Active    Conn.   Deliv.   Soft      Hard

#  Recipient Host   Recip     Out     Recip.   Bounced   Bounced

1  aol.com          365       10      255      21         8

2  hotmail.com      290        7      198      28        13

3  yahoo.com        134        6      123      11        19

4  excite.com        98        3       84       9         4

5  msn.com           84        2       76      33        29

mail3.example.com>
```

リアルタイム アクティビティの表示

Cisco IronPort アプライアンスではリアルタイム モニタリングが可能であり、システムにおける電子メール アクティビティの進捗状況を確認できます。`rate` コマンドは、電子メール動作に関するリアルタイム モニタリング情報を返します。この情報は、ユーザが指定した間隔で定期的に更新されます。`rate` コマンドを停止するには、Ctrl+C を使用します。

表 6-7 に、表示されるデータを示します。

表 6-7　rate コマンドのデータ

統計	説明
Connections In	着信接続の数。
Connections Out	発信接続の数。
Recipients Received	システムに受信された受信者の合計数。
Recipients Completed	完了した受信者の合計数。
Delta	最後のデータ アップデート以降変化した、Received 受信者数および Completed 受信者数の差異。
Queue Used	メッセージ キューのサイズ（キロバイト単位）。

例

```
mail3.example.com> rate

Enter the number of seconds between displays.
[10]> 1

Hit Ctrl-C to return to the main prompt.

Time     Connections Recipients          Recipients              Queue
             In    Out   Received    Delta  Completed    Delta     K-Used
23:37:13    10     2   41708833        0   40842686        0         64
23:37:14     8     2   41708841        8   40842692        6        105
23:37:15     9     2   41708848        7   40842700        8         76
23:37:16     7     3   41708852        4   40842705        5         64
23:37:17     5     3   41708858        6   40842711        6         64
23:37:18     9     3   41708871       13   40842722       11         67
23:37:19     7     3   41708881       10   40842734       12         64
23:37:21    11     3   41708893       12   40842744       10         79
^C
```

hostrate コマンドは、特定のメール ホストに関するリアルタイムのモニタリング情報を返します。この情報は、status detail コマンドのサブセットです（「詳細な電子メール ステータスのモニタリング」（P.6-12）を参照）。

表 6-8　hostrate コマンドのデータ

統計	説明
Host Status	特定のホストの現在のステータス（up、down、または unknown）。
Current Connections Out	ホストに対する現在の発信接続数。
Active Recipients in Queue	キュー内の特定のホストに対するアクティブ受信者の合計数。
Active Recipients in Queue Delta	最後の既知のホスト ステータス以降変化した、キュー内の特定のホストに対するアクティブ受信者の合計数の差異。
Delivered Recipients Delta	最後の既知のホスト ステータス以降変化した、キュー内の特定のホストに対する配信済み受信者の合計数の差異。
Hard Bounced Recipients Delta	最後の既知のホスト ステータス以降変化した、キュー内の特定のホストに対するハード バウンスされた受信者の合計数の差異。
Soft Bounce Events Delta	最後の既知のホスト ステータス以降変化した、キュー内の特定のホストに対するソフト バウンスされた受信者の合計数の差異。

`hostrate` コマンドを停止するには、Ctrl+C を使用します。

例

```
mail3.example.com> hostrate


Recipient host:

[]> aol.com


Enter the number of seconds between displays.

[10]> 1


    Time   Host  CrtCncOut  ActvRcp ActvRcp  DlvRcp HrdBncRcp SftBncEvt

           Status                        Delta   Delta     Delta     Delta

23:38:23        up          1         0       0       4         0
0

23:38:24        up          1         0       0       4         0
0

23:38:25        up          1         0       0      12         0
0

^C
```

着信電子メール接続のモニタリング

大量の送信者を識別するため、またはシステムへの着信接続をトラブルシューティングするために、Cisco IronPort アプライアンスに接続しているホストのモニタが必要になる場合があります。topin コマンドは、システムに接続しているリモート ホストのスナップショットを示します。このスナップショットには、特定のリスナーに接続しているリモート IP アドレスごとに 1 つの行を持つテー

ブルが表示されます。同じ IP アドレスから異なるリスナーへの 2 つの接続に対しては、テーブルに 2 つの行が作成されます。表 6-9 に、topin コマンドを使用したときに表示されるフィールドの説明を示します。

表 6-9　topin コマンドのデータ

統計	説明
Remote Hostname	リモート ホストのホスト名。リバース DNS ルックアップによって取得されます。
Remote IP Address	リモート ホストの IP アドレス。
listener	接続を受信している、Cisco IronPort アプライアンス上のリスナーのニックネーム。
Connections In	コマンドが実行されたときに開いていた、指定の IP アドレスを持つリモート ホストからの同時接続数。

システムは、リバース DNS ルックアップによってリモート ホスト名を検索してから、フォワード DNS ルックアップによってその名前を検証します。フォワード ルックアップで元の IP アドレスにならない場合、またはリバース DNS ルックアップに失敗した場合、テーブルのホスト名カラムには IP アドレスが表示されます。送信者検証プロセスの詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Sender Verification」を参照してください。

例

```
mail3.example.com> topin

Status as of:                  Sat Aug 23 21:50:54 2003

#  Remote hostname            Remote IP addr.   listener        Conn. In
1  mail.remotedomain01.com    172.16.0.2        Incoming01            10
```

```
2  mail.remotedomain01.com    172.16.0.2        Incoming02          10

3  mail.remotedomain03.com    172.16.0.4        Incoming01           5

4  mail.remotedomain04.com    172.16.0.5        Incoming02           4

5  mail.remotedomain05.com    172.16.0.6        Incoming01           3


6  mail.remotedomain06.com    172.16.0.7        Incoming02           3

7  mail.remotedomain07.com    172.16.0.8        Incoming01           3

8  mail.remotedomain08.com    172.16.0.9        Incoming01           3

9  mail.remotedomain09.com    172.16.0.10       Incoming01           3

10 mail.remotedomain10.com    172.16.0.11       Incoming01           2


11 mail.remotedomain11.com    172.16.0.12       Incoming01           2

12 mail.remotedomain12.com    172.16.0.13       Incoming02           2

13 mail.remotedomain13.com    172.16.0.14       Incoming01           2

14 mail.remotedomain14.com    172.16.0.15       Incoming01           2

15 mail.remotedomain15.com    172.16.0.16       Incoming01           2


16 mail.remotedomain16.com    172.16.0.17       Incoming01           2

17 mail.remotedomain17.com    172.16.0.18       Incoming01           1

18 mail.remotedomain18.com    172.16.0.19       Incoming02           1

19 mail.remotedomain19.com    172.16.0.20       Incoming01           1

20 mail.remotedomain20.com    172.16.0.21       Incoming01           1
```

DNS ステータスの確認

dnsstatus コマンドは、DNS ルックアップおよびキャッシュ情報の統計を表示するカウンタを返します。カウンタごとに、そのカウンタの最後のリセット以降、最後のシステム リブート以降、およびシステムの存続期間中に発生したイベントの合計数を表示できます。

表 6-10 に、使用可能なカウンタを示します。

表 6-10　dnsstatus コマンドのデータ

統計	説明
DNS Requests	ドメイン名を解決するためのシステム DNS キャッシュに対する上位レベルの非反復要求。
Network Requests	DNS 情報を取得するためのネットワーク（非ローカル）への要求。
Cache Hits	レコードが検出されて返された、DNS キャッシュへの要求。
Cache Misses	レコードが検出されなかった、DNS キャッシュへの要求。
Cache Exceptions	レコードが検出されたものの、ドメインが不明である、DNS キャッシュへの要求。
Cache Expired	レコードが検出された、DNS キャッシュへの要求。 キャッシュでは、使用状況が考慮され、古すぎるレコードは破棄されます。 Time To Live（TTL; 存続可能時間）を超えていても、多くのエントリがキャッシュに存在する場合があります。これらのエントリは使用されない限り、期限切れカウンタには含まれません。キャッシュがフラッシュされると、有効なエントリと無効（古すぎる）エントリの両方が削除されます。フラッシュ動作によって、期限切れカウンタが変更されることはありません。

例

```
mail3.example.com> dnsstatus

Status as of: Sat Aug 23 21:57:28 2003

Counters:                    Reset          Uptime        Lifetime
  DNS Requests         211,735,710       8,269,306     252,177,342
  Network Requests     182,026,818       6,858,332     206,963,542
  Cache Hits           474,675,247      17,934,227     541,605,545
  Cache Misses         624,023,089      24,072,819     704,767,877
  Cache Exceptions      35,246,211       1,568,005      51,445,744
  Cache Expired            418,369           7,800         429,015

mail3.example.com>
```

電子メール モニタリング カウンタのリセット

Cloud Email Security アプライアンスでは、電子メール モニタリング カウンタをリセットしないようにすることを推奨します。

resetcounters コマンドは、累積する電子メール モニタリング カウンタをリセットします。リセットは、グローバル カウンタとホスト単位のカウンタに影響します。リセットは、再試行スケジュールに関連する配信キュー内のメッセージのカウンタには影響しません。

（注）　GUI で、カウンタをリセットすることもできます。「[System Status] ページ」（P.2-58）を参照してください。

例

```
mail3.example.com> resetcounters


Counters reset: Mon Jan 01 12:00:01 2003
```

電子メール キューの管理

Cisco IronPort AsyncOS では、電子メール キュー内のメッセージに対する動作を実行できます。電子メール キュー内のメッセージは、削除、バウンス、一時停止、またはリダイレクトすることができます。また、キュー内の古いメッセージを検索、削除、およびアーカイブすることもできます。

キュー内の受信者の削除

特定の受信者が配信されていない場合や、電子メール キューをクリアする場合には、deleterecipients コマンドを使用します。deleterecipients コマンドでは、配信を待つ特定の受信者を削除することによって、電子メール配信キューを管理できます。削除される受信者は、受信者の宛先である受信者ホストによって、または、メッセージ エンベロープの Envelope From 行に指定された特定のアドレスで識別されるメッセージ送信者によって識別されます。または、配信キュー内のすべてのメッセージ（すべてのアクティブ受信者）を一度に削除することもできます。

（注）　deleterecipients 機能を実行するには、Cisco IronPort アプライアンスをオフラインまたは配信一時停止の状態にすることを推奨します（「Cisco IronPort アプライアンスをメンテナンス状態にする」（P.8-3）を参照）。

（注）　この機能はどの状態でも使用できますが、機能の実行中に一部のメッセージが配信される可能性があります。

受信者ホストおよび送信者の一致は、同一文字列の一致である必要があります。ワイルド カードは使用できません。deleterecipients コマンドは、削除されるメッセージの合計数を返します。また、メール ログ サブスクリプション（IronPort テキスト形式のみ）が設定されている場合、メッセージの削除は別個の行としてログに記録されます。

例

```
mail3.example.com> deleterecipients


Please select how you would like to delete messages:

1. By recipient host.

2. By Envelope From address.

3. All.

[1]>
```

Cisco IronPort アプライアンスには、必要に応じて受信者を削除するための各種のオプションが用意されています。次に、受信者ホスト別の受信者の削除、Envelope From アドレスによる削除、およびキュー内のすべての受信者の削除の例を示します。

受信者ドメインによる削除

```
Please enter the hostname for the messages you wish to delete.

[]> example.com



Are you sure you want to delete all messages being delivered to
"example.com"? [N]> Y



Deleting messages, please wait.

100 messages deleted.
```

Envelope From アドレスによる削除

```
Please enter the Envelope From address for the messages you wish to
delete.

[]> mailadmin@example.com



Are you sure you want to delete all messages with the Envelope From
address of "mailadmin@example.com"? [N]> Y



Deleting messages, please wait.

100 messages deleted.
```

すべて削除

```
Are you sure you want to delete all messages in the delivery queue (all
active recipients)? [N]> Y


Deleting messages, please wait.

1000 messages deleted.
```

キュー内の受信者のバウンス

deleterecipients コマンドと同様に、bouncerecipients コマンドでは、配信を待つ特定の受信者をハード バウンスすることによって、電子メール配信キューを管理できます。メッセージのバウンスは、bounceconfig コマンドに指定された通常のバウンス メッセージ設定に従います。

（注）　bouncerecipients 機能を実行するには、Cisco IronPort アプライアンスをオフラインまたは配信一時停止の状態にすることを推奨します（「Cisco IronPort アプライアンスをメンテナンス状態にする」（P.8-3）を参照）。

（注）　この機能はどの状態でも使用できますが、機能の実行中に一部のメッセージが配信される可能性があります。

受信者ホストおよび送信者の一致は、同一文字列の一致である必要があります。ワイルド カードは使用できません。bouncerecipients コマンドは、バウンスされたメッセージの合計数を返します。

（注）　bouncerecipients 機能ではリソースが集中的に使用され、完了までに数分かかる場合があります。オフラインまたは配信一時停止の状態の場合は、バウンス メッセージの実際の送信（ハード バウンス生成がオンの場合）は、resume コマンドを使用して Cisco IronPort AsyncOS をオンライン状態にした後でのみ開始されます。

例

```
mail3.example.com> bouncerecipients


Please select how you would like to bounce messages:

1. By recipient host.

2. By Envelope From address.

3. All.

[1]>
```

バウンスされる受信者は、宛先受信者ホストによって、またはメッセージ エンベロープの Envelope From 行に指定された特定のアドレスで識別されるメッセージ送信者によって識別されます。または、配信キュー内のすべてのメッセージを一度にバウンスすることもできます。

受信者ホストによるバウンス

```
Please enter the hostname for the messages you wish to bounce.

[]> example.com



Are you sure you want to bounce all messages being delivered to
"example.com"? [N]> Y



Bouncing messages, please wait.

100 messages bounced.
```

Envelope From アドレスによるバウンス

```
Please enter the Envelope From address for the messages you wish to
bounce.

[]> mailadmin@example.com



Are you sure you want to bounce all messages with the Envelope From
address of "mailadmin@example.com"? [N]> Y



Bouncing messages, please wait.

100 messages bounced.
```

すべてバウンス

```
Are you sure you want to bounce all messages in the queue? [N]> Y
```

```
Bouncing messages, please wait.

1000 messages bounced.
```

キュー内のメッセージのリダイレクト

redirectrecipients コマンドを使用すると、電子メール配信キュー内のすべてのメッセージを別のリレー ホストにリダイレクトできます。受信者を、このホストから大量の SMTP メールを受け入れる準備ができていないホストまたは IP アドレスにリダイレクトすると、メッセージがバウンスするだけでなく、メールが失われる可能性もあることに注意してください。

警告　メッセージを、/dev/null を宛先とする受信側ドメインにリダイレクトすると、メッセージが失われます。メールをこのようなドメインにリダイレクトしても、CLI に警告は表示されません。メッセージをリダイレクトする前に、受信側ドメインがあるかどうか SMTP ルートを確認してください。

例

次に、すべてのメールを example2.com ホストにリダイレクトする例を示します。

```
mail3.example.com> redirectrecipients


Please enter the hostname or IP address of the machine you want to
send all mail to.

[]> example2.com


WARNING: redirecting recipients to a host or IP address that is not
prepared to accept large volumes of SMTP mail from this host will
cause messages to bounce and possibly result in the loss of mail.
```

```
Are you sure you want to redirect all mail in the queue to
"example2.com"? [N]> y


Redirecting messages, please wait.

246 recipients redirected.
```

キュー内の受信者に基づいたメッセージの表示

showrecipients コマンドを使用すると、電子メール配信キューからのメッセージが受信者ホストまたは Envelope From アドレスごとに表示されます。また、キュー内のすべてのメッセージを表示することもできます。

例

次に、すべての受信者ホストへのキュー内のメッセージの例を示します。

```
mail3.example.com> showrecipients


Please select how you would like to show messages:

1. By recipient host.

2. By Envelope From address.

3. All.

[1]> 3


Showing messages, please wait.
```

```
MID/     Bytes/    Sender/                  Subject
[RID]    [Atmps]   Recipient
1527     1230      user123456@ironport.com Testing
[0]      [0]       9554@example.com

1522     1230      user123456@ironport.com Testing
[0]      [0]       3059@example.com

1529     1230      user123456@ironport.com Testing
[0]      [0]       7284@example.com

1530     1230      user123456@ironport.com Testing
[0]      [0]       8243@example.com

1532     1230      user123456@ironport.com Testing
[0]      [0]       1820@example.com

1531     1230      user123456@ironport.com Testing
[0]      [0]       9595@example.com

1518     1230      user123456@ironport.com Testing
[0]      [0]       8778@example.com
```

```
1535      1230      user123456@ironport.com Testing
[0]       [0]       1703@example.com

1533      1230      user123456@ironport.com Testing
[0]       [0]       3052@example.com

1536      1230      user123456@ironport.com Testing
[0]       [0]       511@example.com
```

電子メール配信の一時停止

アプライアンスでは、電子メール配信を一時停止したり、再開したりしないようにすることを推奨します。

メンテナンスやトラブルシューティングのために電子メールの配信を一時的に停止するには、suspenddel コマンドを使用します。suspenddel コマンドは、Cisco IronPort AsyncOS を配信一時停止の状態にします。この状態には、次のような特徴があります。

- 発信電子メール配信は停止されます。
- 着信電子メール接続は受け入れられます。
- ログ転送は続行します。
- CLI はアクセス可能のままになります。

suspenddel コマンドを実行すると、開いていた発信接続が閉じられ、新規の接続は開かれません。suspenddel コマンドはただちに開始され、確立しているすべての接続を正常に閉じることができます。配信一時停止の状態から通常の動作に戻すには、resumedel コマンドを使用します。

（注）「delivery suspend」状態は、システムをリブートしても保持されます。suspenddel コマンドを使用してからアプライアンスをリブートする場合は、resumedel コマンドを使用してリブートしてから配信を再開する必要があります。

例

```
mail3.example.com> suspenddel


Enter the number of seconds to wait before abruptly closing connections.

[30]>


Waiting for outgoing deliveries to finish...

Mail delivery suspended.
```

電子メール配信の再開

Cloud Email Security アプライアンスでは、電子メール配信を一時停止したり、再開したりしないようにすることを推奨します。

resumedel コマンドは、suspenddel コマンドの使用後に Cisco IronPort AsyncOS を通常の動作状態に戻します。

構文

```
        resumedel
```

```
mail3.example.com> resumedel
```

```
Mail delivery resumed.
```

受信の一時停止

Cloud Email Security アプライアンスでは、リスナーを一時停止したり、再開したりしないようにすることを推奨します。

すべてのリスナーに対して 電子メールの受信を一時停止するには、`suspendlistener` コマンドを使用します。受信が一時停止されている間、システムはリスナーの特定のポートへの接続を受け入れません。

これは、このリリースの AsyncOS で変更された動作です。以前のリリースでは、システムは接続を受け入れ、次のように応答してから接続解除していました。

- SMTP: `421` *hostname* `Service not available, closing transaction channel`
- QMQP: `ZService not available`

（注） 「receiving suspend」状態は、システムをリブートしても保持されます。`suspendlistener` コマンドを使用してからアプライアンスをリブートする場合、リスナーでメッセージの受信を再開するには、`resumelistener` コマンドを使用する必要があります。

構文

```
        suspendlistener

mail3.example.com> suspendlistener



Choose the listener(s) you wish to suspend.

Separate multiple entries with commas.

1. All
```

```
2. InboundMail

3. OutboundMail

[1]> 1


Enter the number of seconds to wait before abruptly closing connections.

[30]>


Waiting for listeners to exit...

Receiving suspended.

mail3.example.com>
```

受信の再開

Cloud Email Security アプライアンスでは、リスナーを一時停止したり、再開したりしないようにすることを推奨します。

`resumelistener` コマンドは、`suspendlistener` コマンドの使用後に Cisco IronPort AsyncOS を通常の動作状態に戻します。

構文

```
        resumelistener

mail3.example.com> resumelistener


Choose the listener(s) you wish to resume.

Separate multiple entries with commas.
```

```
1. All

2. InboundMail

3. OutboundMail

[1]> 1


Receiving resumed.

mail3.example.com>
```

配信および受信の再開

resume コマンドは、配信と受信の両方を再開します。

構文

```
        resume
mail3.example.com> resume


Receiving resumed.

Mail delivery resumed.

mail3.example.com>
```

電子メールの即時配信スケジュール

delivernow コマンドを使用すると、後で配信するようにスケジュールされた受信とホストをただちに再試行できます。delivernow コマンドでは、キュー内の電子メールに即時配信を再スケジュールすることができます。down のマークが付いたすべてのドメインと、スケジュールされたメッセージまたはソフト バウンスされたメッセージが、即時配信のキューに入れられます。

delivernow コマンドは、キュー内の（スケジュールされた、およびアクティブな）すべての受信者または特定の受信者に対して呼び出すことができます。特定の受信を選択する際は、即時配信をスケジュールする受信者のドメイン名を入力する必要があります。システムは、文字列全体の文字と長さを照合します。

構文

```
       delivernow

mail3.example.com> delivernow



Please choose an option for scheduling immediate delivery.

1. By recipient host

2. All messages

[1]> 1



Please enter the domain to schedule for immediate delivery.

[]> recipient.example.com



Rescheduling all messages to recipient.example.com for immediate
delivery.

mail3.example.com>
```

作業キューの休止

Cloud Email Security アプライアンスでは、作業キューを休止しないようにすることを推奨します。

LDAP 受信者アクセス、マスカレード、LDAP 再ルーティング、メッセージ フィルタ、アンチスパム、およびアンチウイルス スキャン エンジンの処理は、すべて「作業キュー」で実行されます。処理フローについては『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Delivery Features」、および「Messages in Work Queue」ゲージの説明については表 6-2（P.5）を参照してください。`workqueue` コマンドを使用して、作業キュー部分のメッセージ処理を手動で休止することができます。

たとえば、多くのメッセージが作業キュー内にあるときに、LDAP サーバの設定を変更する必要があるとします。おそらく、LDAP 受信者アクセス クエリーに基づいて、メッセージをバウンスからドロップに切り替えようとします。または、キューを休止して、最新のアンチウイルス スキャン エンジンの定義ファイルを手動で確認（`antivirusupdate` コマンドを使用）する可能性もあります。`workqueue` コマンドを使用すると、作業キューを休止してから再開することで、処理を停止した状態で他の設定変更を行うことができます。

作業キューを休止してから再開すると、そのイベントがログに記録されます。次に例を示します。

```
Sun Aug 17 20:01:36 2003 Info: work queue paused, 1900 msgs S

Sun Aug 17 20:01:39 2003 Info: work queue resumed, 1900 msgs
```

次の例では、作業キューが中止されます。

```
mail3.example.com> workqueue


Status as of:  Sun Aug 17 20:02:30 2003 GMT

Status:   Operational

Messages: 1243
```

```
Choose the operation you want to perform:

- STATUS - Display work queue status

- PAUSE - Pause the work queue

- RATE - Display work queue statistics over time

[]> pause


Manually pause work queue?  This will only affect unprocessed messages.
[N]> y


Reason for pausing work queue:

[]> checking LDAP server


Status as of:  Sun Aug 17 20:04:21 2003 GMT

Status:   Paused by admin: checking LDAP server

Messages: 1243
```

（注）　理由の入力は任意です。理由を入力しないと、その理由は [Manually paused by user] としてログに記録されます。

次の例では、作業キューが再開されます。

```
mail3.example.com> workqueue


Status as of:  Sun Aug 17 20:42:10 2003 GMT
```

```
Status:   Paused by admin: checking LDAP server

Messages: 1243


Choose the operation you want to perform:

- STATUS - Display work queue status

- RESUME - Resume the work queue

- RATE - Display work queue statistics over time

[]> resume


Status:   Operational

Messages: 1243
```

古いメッセージの検索およびアーカイブ

時折、古くなったメッセージが配信できずに、キューに留まっていることがあります。これらのメッセージは削除したり、アーカイブしたりすることができます。これには、`showmessage` CLI コマンドを使用して、所定のメッセージ ID に対応するメッセージを表示します。`oldmessage` CLI コマンドを使用すると、システム上の最も古い非検疫メッセージが表示されます。その後は、任意で `removemessage` を使用して、所定のメッセージ ID に対応するメッセージを安全に削除できます。このコマンドでは、作業キュー、再試行キュー、または宛先キュー内のメッセージのみを削除できます。メッセージがこれらのキューのいずれにもない場合は、削除できません。

また、`archivemessage[mid]` CLI コマンドを使用して、所定のメッセージ ID に対応するメッセージをコンフィギュレーション ディレクトリ内の mbox ファイルにアーカイブすることもできます。

oldmessage コマンドを使用して、システム検疫内のメッセージのメッセージ ID を取得することはできません。ただし、メッセージ ID がわかっている場合は、指定のメッセージを表示したり、アーカイブしたりすることができます。メッセージが作業キュー、再試行キュー、または宛先キューにないと、removemessage コマンドでメッセージを削除することはできません。

（注）　IronPort スパム検疫内のメッセージに対しては、これらのキュー管理コマンドを実行できません。

構文

```
        archivemessage

example.com> archivemessage



Enter the MID to archive and remove.

[0]> 47

 MID 47 has been saved in file oldmessage_47.mbox in the configuration
directory

example.com>
```

構文

```
        oldmessage

example.com> oldmessage



MID 9: 1 hour 5 mins 35 secs old

Received: from example.com ([172.16.0.102])

  by example.com with SMTP; 14 Feb 2007 22:11:37 -0800
```

```
From: user123@example.com

To: 4031@test.example2.com

Subject: Testing

Message-Id: <20070215061136.68297.16346@example.com>
```

システム内のメッセージのトラッキング

findevent CLI コマンドは、オンボックスのメール ログ ファイルを使用して、システム内のメッセージのトラッキング（追跡）プロセスを容易にします。findevent CLI コマンドを使用すると、メッセージ ID の検索、またはサブジェクト ヘッダー、エンベロープ送信者、またはエンベロープ受信者に対する正規表現の一致検索によって、メール ログから特定のメッセージを検索できます。現在のログ ファイルやすべてのログ ファイルの結果を表示することも、ログ ファイルを日付別で表示することもできます。ログ ファイルを日付別で表示する場合は、特定の日付か、日付の範囲を指定できます。

ログを表示するメッセージを識別した後は、findevent コマンドによって、分裂情報（分裂したログ メッセージ、バウンス、およびシステム生成メッセージ）を含む、そのメッセージ ID に対するログ情報を表示できます。次に、findevent CLI コマンドで、サブジェクト ヘッダーに「confidential」とあるメッセージの受信と配信を追跡する例を示します。

```
example.com> findevent

Please choose which type of search you want to perform:

1. Search by envelope FROM

2. Search by Message ID

3. Search by Subject

4. Search by envelope TO

[1]> 3
```

```
Enter the regular expression to search for.

[]> confidential

Currently configured logs:

1. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll

Enter the number of the log you wish to use for message tracking.

[]> 1

Please choose which set of logs to search:

1. All available log files

2. Select log files by date list

3. Current log file
```

```
[3]> 3

The following matching message IDs were found. Please choose one to
show additional log information:
1. MID 4 (Tue Jul 31 17:37:35 2007) sales: confidential
[1]> 1
Tue Jul 31 17:37:32 2007 Info: New SMTP ICID 2 interface Data 1
(172.19.1.86) address 10.251.20.180 reverse dns host unknown verified no
Tue Jul 31 17:37:32 2007 Info: ICID 2 ACCEPT SG None match ALL SBRS None
Tue Jul 31 17:37:35 2007 Info: Start MID 4 ICID 2
Tue Jul 31 17:37:35 2007 Info: MID 4 ICID 2 From: <user@example.com>
Tue Jul 31 17:37:35 2007 Info: MID 4 ICID 2 RID 0 To:
<ljohnson@example02.com>
Tue Jul 31 17:37:35 2007 Info: MID 4 Subject 'sales: confidential'
Tue Jul 31 17:37:35 2007 Info: MID 4 ready 4086 bytes from
<user@example.com>
Tue Jul 31 17:37:35 2007 Info: MID 4 matched all recipients for
per-recipient policy DEFAULT in the inbound table
Tue Jul 31 17:37:35 2007 Info: ICID 2 close
Tue Jul 31 17:37:37 2007 Info: MID 4 interim verdict using engine: CASE
spam negative
Tue Jul 31 17:37:37 2007 Info: MID 4 using engine: CASE spam negative
Tue Jul 31 17:37:37 2007 Info: MID 4 interim AV verdict using Sophos
CLEAN
Tue Jul 31 17:37:37 2007 Info: MID 4 antivirus negative
Tue Jul 31 17:37:37 2007 Info: MID 4 queued for delivery
Tue Jul 31 17:37:37 2007 Info: Delivery start DCID 0 MID 4 to RID [0]
Tue Jul 31 17:37:37 2007 Info: Message done DCID 0 MID 4 to RID [0]
Tue Jul 31 17:37:37 2007 Info: MID 4 RID [0] Response '/null'
Tue Jul 31 17:37:37 2007 Info: Message finished MID 4 done
```

SNMP モニタリング

Cloud Email Security アプライアンスでは、SNMP を設定しないようにすることを推奨します。

Cisco IronPort AsyncOS オペレーティング システムは、SNMP（簡易ネットワーク管理プロトコル）を使用したシステム ステータスのモニタリングをサポートしています。これには、IronPort のエンタープライズ MIB、ASYNCOS-MAIL-MIB が含まれます。ASYNCOS-MAIL-MIB を使用すること

で、管理者は、システムの状態をモニタしやすくなります。また、このリリースには、RFC 1213 および 1907 に規定されている MIB-II の読み取り専用のサブセットが実装されています（SNMP の詳細については、RFC 1065、1066、および 1067 を参照してください）。次の点に注意してください。

- SNMP は、デフォルトで**オフ**になります。
- SNMP SET 動作（コンフィギュレーション）は実装されません。
- AsyncOS は SNMPv1、v2、および v3 をサポートしています。
- このサービスをイネーブルにするには、パスワード認証と DES 暗号化を伴う SNMPv3 の使用が必須です（SNMPv3 の詳細については、RFC 2571 ～ 2575 を参照してください）。SNMP システム ステータスのモニタリングをイネーブルにするには、少なくとも 8 文字の SNMPv3 パスフレーズを設定する必要があります。最初に SNMPv3 パスフレーズを入力するときは、確認のためにそのパスフレーズを再入力する必要があります。次に `snmpconfig` コマンドを実行するときは、コマンドにこのフレーズが「記憶」されています。
- SNMPv3 ユーザ名は v3get です。

```
> snmpwalk -v 3 -l AuthNoPriv -u v3get -a MD5 ironport mail.example.com
```

- SNMPv1 または SNMPv2 のみを使用する場合は、コミュニティ ストリングを設定する必要があります。コミュニティ ストリングは、`public` にデフォルト設定されません。
- SNMPv1 および SNMPv2 の場合、どのネットワークからの SNMP GET 要求を受け入れるかを指定する必要があります。
- トラップを使用するには、SNMP マネージャ（AsyncOS には含まれていません）が実行中であり、その IP アドレスがトラップ ターゲットとして入力されている必要があります（ホスト名を使用できますが、その場合、トラップは DNS が動作しているときに限り機能します）。

`snmpconfig` コマンドを使用して、アプライアンスの SNMP システム ステータスを設定します。インターフェイスの値を選択し、設定し終えると、アプライアンスは SNMPv3 GET 要求に応答します。これらのバージョン 3 要求には、一致するパスワードが含まれている必要があります。デフォルトでは、バージョン 1 および 2 要求は拒否されます。イネーブルにする場合は、バージョン 1 および 2 要求に一致するコミュニティ ストリングが含まれている必要があります。

MIB ファイル

Cisco IronPort システムには、「Structure of Management Information」（SMI）ファイルだけでなく、次の「エンタープライズ」MIB が用意されています。

- ASYNCOS-MAIL-MIB.txt：Cisco IronPort アプライアンス用のエンタープライズ MIB の SNMPv2 互換の説明。
- IRONPORT-SMI.txt：IronPort の SNMP 管理対象製品における ASYNCOS-MAIL-MIB の役割を定義します。

これらのファイルは、Cisco IronPort アプライアンスに付属のドキュメンテーション CD に収録されています。また、Cisco IronPort カスタマー サポートを通じてこれらのファイルを要求することもできます。

ハードウェア オブジェクト

Intelligent Platform Management Interface Specification（IPMI）準拠のハードウェア センサーが温度、ファン スピード、および電源モジュール ステータスを報告します。

表 6-11 に、どのモデルでどのハードウェア派生オブジェクトをモニタリングに使用できるかを示します。表示されている数字は、モニタできるオブジェクトのインスタンスの数です。たとえば、C10 アプライアンスの 3 つのファン、および C300/C600/X1000 アプライアンスの 6 つのファンについてクエリーを送信できます。

表 6-11　Cisco IronPort アプライアンスごとのハードウェア オブジェクトの数

モデル	CPU 温度	周囲温度	バックプレーン温度	ライザー温度	ファン	電源ステータス	ディスクステータス	NIC リンク
C10/100	1	1	0	0	3	0	2	2
C30/C60	0	0	0	0	0	0	2（C60 は 4）	3

表 6-11　Cisco IronPort アプライアンスごとのハードウェア オブジェクトの数（続き）

モデル	CPU 温度	周囲温度	バックプレーン温度	ライザー温度	ファン	電源ステータス	ディスクステータス	NIC リンク
C300/C600/X1000	2	1	1	1	6	2	4（C300 は 2）	3（*ファイバーインターフェイス搭載の C600 と X1000 の場合は 5*）
C350/C650/X1050	2	1	0	0	4	2	4（C350 は 2）	3（*ファイバーインターフェイス搭載の C650 と x1050 の場合は 5*）

いずれのモデルでも、SNMP を使用してディスク ドライブの状態とネットワーク インターフェイスのリンク ステータスをモニタできます。

ハードウェア トラップ

表 6-12 に、ハードウェア トラップが送信される温度およびハードウェアの条件を示します。

表 6-12　ハードウェア トラップ：温度およびハードウェアの条件

モデル	高温（CPU）	高温（周囲）	高温（バックプレーン）	高温（ライザー）	ファン障害	電源モジュール	RAID	リンク
C10/C100	90C	47C	NA	NA	0 RPM	ステータス変更	ステータス変更	ステータス変更
C30/C60	NA	NA	NA	NA	NA	NA	ステータス変更	ステータス変更

表 6-12　ハードウェア トラップ：温度およびハードウェアの条件（続き）

モデル	高温（CPU）	高温（周囲）	高温（バックプレーン）	高温（ライザー）	ファン障害	電源モジュール	RAID	リンク
C300/C600/X1000	90C	47C	72C	62C	0 RPM	ステータス変更	ステータス変更	ステータス変更
C350/C650/X1050	90C	47C	NA	NA	0 RPM	ステータス変更	ステータス変更	ステータス変更

ステータス変更トラップは、ステータスが変更されると送信されます。ファン障害および高温トラップは、5 秒ごとに送信されます。その他のトラップは、障害条件アラーム トラップです。これらのトラップは、ステータスが（良好から障害へ）変更されたときに一度だけ送信されます。ハードウェア ステータス テーブルにポーリングを送信して、致命的な状況になる前に潜在的なハードウェア障害を識別することを推奨します。重大値の 10 % 以内の温度を不安原因と考えることができます。

障害条件アラーム トラップは、個々のコンポーネントの致命的な障害を示しますが、システム全体の障害の原因になるとは限りません。たとえば、C600 アプライアンスで 1 つのファンまたは電源モジュールに障害が発生しても、アプライアンスは動作し続けます。

SNMP トラップ

SNMP には、1 つまたは複数の条件が満たされたときに管理アプリケーション（通常は、SNMP 管理コンソール）に知らせるためのトラップ（または通知）を送信する機能が備わっています。トラップとは、トラップを送信するシステムのコンポーネントに関するデータを含むネットワーク パケットです。トラップは、SNMP エージェント（この場合は Cisco IronPort アプライアンス）である条件が満たされた場合に生成されます。条件が満たされると、SNMP エージェントは SNMP パケットを形成し、標準の SNMP トラップ ポートであるポート 162 経由で送信します。次の例では、トラップ ターゲット `snmp-monitor.example.com` およびトラップ コミュニティ ストリングが入力されています。これは、Cisco IronPort アプライアンスから SNMP トラップを受信する SNMP 管理コンソール ソフトウェアを実行しているホストです。

インターフェイスに対して SNMP をイネーブルにするときに、SNMP トラップを設定（特定のトラップをイネーブルまたはディセーブルに）できます。トラップ ターゲットの入力を求められたときに、複数のトラップ ターゲットを指定するには、カンマで区切った IP アドレスを 10 個まで入力できます。

CLI の例

次の例では、snmpconfig コマンドを使用して、ポート 161 の「PublicNet」インターフェイスで SNMP をイネーブルにしています。バージョン 3 のパスフレーズが入力され、確認のために再入力されています。システムは、バージョン 1 および 2 要求を処理するように設定されており、これらのバージョン 1 および 2 からの GET 要求に対してコミュニティ ストリング public が入力されています。トラップ ターゲット snmp-monitor.example.com が入力されています。最後に、システムの場所と連絡先情報が入力されています。

```
mail3.example.com> snmpconfig


Current SNMP settings:

SNMP Disabled.


Choose the operation you want to perform:

- SETUP - Configure SNMP.

[]> setup


Do you want to enable SNMP? [N]> y


Please choose an IP interface for SNMP requests.

1. Data 1 (192.168.1.1/24: mail3.example.com)
```

```
2. Data 2 (192.168.2.1/24: mail3.example.com)

3. Management (192.168.44.44/24: mail3.example.com)

[1]>


Enter the SNMPv3 passphrase.

>

Please enter the SNMPv3 passphrase again to confirm.

>

Which port shall the SNMP daemon listen on?

[161]>


Service SNMP V1/V2c requests? [N]> y


Enter the SNMP V1/V2c community string.

[]> public


From which network shall SNMP V1/V2c requests be allowed?

[192.168.2.0/24]>


Enter the Trap target (IP address recommended). Enter "None" to disable
traps.

[None]> 10.1.1.29
```

```
Enter the Trap Community string.

[]> tcomm


Enterprise Trap Status

1. RAIDStatusChange             Enabled

2. fanFailure                   Enabled

3. highTemperature              Enabled

4. keyExpiration                Enabled

5. linkDown                     Enabled

6. linkUp                       Enabled

7. powerSupplyStatusChange      Enabled

8. resourceConservationMode     Enabled

9. updateFailure                Enabled

Do you want to change any of these settings? [N]> y


Do you want to disable any of these traps? [Y]>


Enter number or numbers of traps to disable. Separate multiple numbers
with commas.

[]> 1,8
```

```
Enterprise Trap Status

1. RAIDStatusChange             Disabled

2. fanFailure                   Enabled

3. highTemperature              Enabled

4. keyExpiration                Enabled

5. linkDown                     Enabled

6. linkUp                       Enabled

7. powerSupplyStatusChange      Enabled

8. resourceConservationMode     Disabled

9. updateFailure                Enabled

Do you want to change any of these settings? [N]>


Enter the System Location string.

[Unknown: Not Yet Configured]> Network Operations Center - west; rack
#31, position 2


Enter the System Contact string.

[snmp@localhost]> Joe Administrator, x8888


Current SNMP settings:

Listening on interface "Data 1" 192.168.2.1/24 port 161.

SNMP v3: Enabled.
```

```
SNMP v1/v2: Enabled, accepting requests from subnet 192.168.2.0/24.

SNMP v1/v2 Community String: public

Trap target: 10.1.1.29

Location: Network Operations Center - west; rack #31, position 2

System Contact: Joe Administrator, x8888


mail3.example.com>
```

CHAPTER 7

GUI でのその他の作業

Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）は、システムのモニタリングおよび設定用の一部の Command Line Interface（CLI; コマンドライン インターフェイス）コマンドに代わる Web ベースのインターフェイスです。GUI を使用することにより、Cisco IronPort AsyncOS コマンド構文を知らなくても、単純な Web ベース インターフェイスを使用してシステムをモニタできます。

この章は、次の内容で構成されています。

Cisco IronPort グラフィカル ユーザ インターフェイス（GUI）

インターフェイスに対して HTTP、HTTPS、またはその両方のサービスをイネーブルにすると、GUI にアクセスし、ログインできるようになります。詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Overview」の章を参照してください。

インターフェイスでの GUI のイネーブル化

システムはデフォルトで、管理インターフェイス（Cisco IronPort C10/100 アプライアンスの Data 1）に対して HTTP がイネーブルになった状態で出荷されます。

GUI をイネーブルにするには、コマンドライン インターフェイスで `interfaceconfig` コマンドを実行し、接続するインターフェイスを編集してから、HTTP サービスまたはセキュア HTTP サービス、あるいはその両方をイネーブルにします。

（注） また、いずれかのインターフェイスで GUI をイネーブルにした後は、[Network] > [IP Interfaces] ページを使用して、別のインターフェイスに対して GUI をイネーブルまたはディセーブルにすることもできます。詳細については、294 ページの「IP Interfaces」を参照してください。

（注） インターフェイスでセキュア HTTP をイネーブルにするには、証明書をインストールする必要があります。詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Enabling a Certificate for HTTPS」を参照してください。

いずれかのサービスに対し、そのサービスをイネーブルにするポートを指定します。デフォルトでは、HTTP はポート 80、HTTPS はポート 443 でイネーブルになります。1 つのインターフェイスで両方のサービスをイネーブルにすると、HTTP 要求をセキュア サービスに自動的にリダイレクトできます。

さらに、このインターフェイスの GUI に（`HTTP` または `HTTPS` 経由で）アクセスしようとするすべてのユーザ（「ユーザ アカウントを使用する作業」（P.8-18）を参照）は、ユーザ名とパスワードを入力する標準のログイン ページで認証を受ける必要があります。

（注） GUI にアクセスするには、まず、`commit` コマンドを使用して変更を保存する必要があります。

次に、Data 1 インターフェイスに対して GUI をイネーブルにする例を示します。`interfaceconfig` コマンドを使用して、ポート 80 で HTTP、およびポート 443 で HTTPS をイネーブルにします（`certconfig` コマンドが実行可能になるまで、

HTTP に対して一時的にデモ用の証明書が使用されます。詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Installing Certificates on the Cisco IronPort Appliance」を参照してください)。Data1 インターフェイスについては、ポート 80 への HTTP 要求がポート 443 に自動的にリダイレクトされるように設定されます。

例

```
mail3.example.com> interfaceconfig

Currently configured interfaces:
1. Data 1 (192.168.1.1/24 on Data1: mail3.example.com)
2. Data 2 (192.168.2.1/24 on Data2: mail3.example.com)
3. Management (192.168.42.42/24 on Management: mail3.example.com)

Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- GROUPS - Define interface groups.
- DELETE - Remove an interface.
[]> edit

Enter the number of the interface you wish to edit.
[]> 1

IP interface name (Ex: "InternalNet"):
[Data 1]>

IP Address (Ex: 192.168.1.2):
```

```
[192.168.1.1]>


Ethernet interface:

1. Data 1

2. Data 2

3. Management

[1]>


Netmask (Ex: "255.255.255.0" or "0xffffff00"):

[255.255.255.0]>


Hostname:

[mail3.example.com]>


Do you want to enable FTP on this interface?  [N]>


Do you want to enable Telnet on this interface?  [N]>


Do you want to enable SSH on this interface?  [N]>


Do you want to enable HTTP on this interface?  [N]> y
```

```
Which port do you want to use for HTTP?

[80]> 80


Do you want to enable HTTPS on this interface?  [N]> y


Which port do you want to use for HTTPS?

[443]> 443


You have not entered a certificate. To assure privacy, run

'certconfig' first.  You may use the demo certificate

to test HTTPS, but this will not be secure.

Do you really wish to use a demo certificate?  [N]> y


Both HTTP and HTTPS are enabled for this interface, should HTTP
requests

redirect to the secure service?  [Y]> y


Currently configured interfaces:

1. Data 1 (192.168.1.1/24 on Data 1: mail3.example.com)

2. Data 2 (192.168.2.1/24 on Data 2: mail3.example.com)

3. Management (192.168.42.42/24 on Management: mail3.example.com)
```

```
Choose the operation you want to perform:

- NEW - Create a new interface.

- EDIT - Modify an interface.

- GROUPS - Define interface groups.

- DELETE - Remove an interface.

[]>

mail3.example.com> commit


Please enter some comments describing your changes:

[]> enabled HTTP, HTTPS for Data 1


Changes committed: Mon Jul  7 13:21:23 2003

mail3.example.com>
```

GUI で使用できるその他の作業の概要

- [System Overview] ページでは、次のことができます。
  - 主要システムのステータスとパフォーマンスの一部の情報を示す履歴グラフおよびテーブルを表示する。
  - アプライアンスにインストールされている Cisco IronPort AsyncOS オペレーティング システムのバージョンを表示する。
  - 主要統計情報のサブセットを表示する。
- [System Status] ページには、システムのすべてのリアルタイム メールおよび DNS アクティビティの詳細が表示されます。また、システム統計情報のカウンタをリセットしたり、カウンタが最後にリセットされた時刻を表示したりすることもできます。

- [System Trace] ページでは、テスト メッセージの送信をエミュレートすることによって、システムを介したメッセージ フローをデバッグできます。リスナーに受け入れられているようにメッセージをエミュレートして、現在のシステム設定によって「トリガー」される、または影響を受ける機能の概要を出力できます。

テスト メッセージを使用したメール フローのデバッグ：トレース

[System Administration] > [Trace] ページを使用して（CLI の `trace` コマンドと同等）、テスト メッセージの送信をエミュレートすることにより、システムを介したメッセージ フローをデバッグできます。[Trace] ページ（および `trace` CLI コマンド）では、リスナーに受け入れられているようにメッセージをエミュレートし、現在のシステム設定（*コミットしていない変更を含む*）によって「トリガー」される、または影響を受ける機能の概要を出力できます。テスト メッセージは実際には送信されません。特に、Cisco IronPort アプライアンスで使用できる多数の高度な機能を組み合わせると、[Trace] ページ（および `trace` CLI コマンド）は、強力なトラブルシューティングまたはデバッグ ツールとなります。

[Trace] ページ（および trace CLI コマンド）では、表 7-1 に示されている入力パラメータのプロンプトが表示されます。

表 7-1　[Trace] ページの入力

値	説明	例
Source IP address	リモート ドメインの送信元を模倣するため、リモート クライアントの IP アドレスを入力します。 **注：**trace コマンドを実行すると、IP アドレスと完全修飾ドメイン名の入力が求められます。完全修飾ドメイン名が一致するかどうかを確認するための IP アドレスの逆引きは*行われません*。trace コマンドでは、完全修飾ドメイン名フィールドをブランクにすることができないので、DNS で適切に逆引きできない場合にはテストできません。	`203.45.98.109`
Fully Qualified Domain Name of the Source IP	模倣する完全修飾リモート ドメイン名を入力します。ヌルのままにすると、送信元 IP アドレスに対してリバース DNS ルックアップが実行されます。	`smtp.example.com`
Listener to Trace Behavior on	テスト メッセージの送信をエミュレートするため、システムに設定されているリスナーのリストから選択します。	`InboundMail`
SenderBase Network Owner Organization ID	SenderBase ネットワーク オーナーに固有の ID 番号を入力するか、送信元 IP アドレスに関連付けられたネットワーク オーナー ID の検索を指示します。GUI を介して送信者グループにネットワーク オーナーを追加した場合は、この情報を表示できます。	`34`

表 7-1　[Trace] ページの入力（続き）

値	説明	例
SenderBase Reputation Score (SBRS scores)	スプーフィング ドメインに与える SBRS スコアを入力するか、送信元 IP アドレスに関連付けられた SBRS スコアの検索を指示します。このパラメータは、SBRS スコアを使用するポリシーをテストするときに役立ちます。手動で入力した SBRS スコアは、Context Adaptive Scanning Engine（CASE）に渡されないことに注意してください。詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Reputation Filtering」を参照してください。	`-7.5`
Envelope Sender	テスト メッセージのエンベロープ送信者を入力します。	`admin@example.net`
Envelope Recipients	テスト メッセージの受信者のリストを入力します。複数のエントリを指定する場合は、カンマで区切ります。	`joe` `frank@example.com`

Message Body	ヘッダーを含む、テスト メッセージの本文を入力します。メッセージ本文の入力を終了するには、別の行にピリオドを入力します。「ヘッダー」は（空白行で区切られた）メッセージ本文の一部と見なされます。ヘッダーを省略したり、ヘッダーの形式に誤りがあったりすると、予期しないトレース結果を招くことがあります。	`To: 1@example.com`
		From: ralph
		Subject: Test
		
		`A test message`
		.

値を入力したら、[Start Trace] をクリックします。メッセージに影響する、システムに設定されたすべての機能の概要が出力されます。

メッセージ本文は、ローカル ファイル システムからアップロードできます（CLI では、`/configuration` ディレクトリにアップロードしたメッセージ本文を使用してテストできます。Cisco IronPort アプライアンスへのインポート用ファイルの準備に関する詳細については、付録 A「Accessing the Appliance」を参照してください）。

概要が出力されると、生成されたメッセージの確認とテスト メッセージの再実行を求められます。別のテスト メッセージを入力する場合、[Trace] ページおよび trace コマンドで、前に入力した表 7-1 の値が使用されます。

（注）　表 7-2 に示す、trace コマンドによってテストされる設定の各セクションは、*順番どおりに*実行されます。この順番は、ある機能の設定が他の機能にどのように影響するかを理解するうえで非常に役立ちます。たとえば、ドメイン マップ機能によって変換される受信者アドレスは、RAT によって評価されるアドレスに影響します。また、RAT の影響を受ける受信者は、エイリアス テーブルによって評価されるアドレスに影響する、というようになります。

表 7-2　トレースを実行した後の出力の表示

trace コマンド セクション	出力
Host Access Table (HAT) and Mail Flow Policy Processing	指定したリスナーに対する Host Access Table の設定が処理されます。システムからは、入力したリモート IP アドレスおよびリモート ドメイン名と一致した HAT 内のエントリが報告されます。デフォルトのメール フロー ポリシーと送信者グループ、およびどちらが所定のエントリに一致したかを確認できます。 Cisco IronPort アプライアンスが（REJECT または TCPREFUSE アクセス ルールを介して）接続を拒否するように設定された場合、処理中の trace コマンドはその時点で終了します。 HAT パラメータの設定の詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Configuring the Gateway to Receive Email」を参照してください。

表 7-2　トレースを実行した後の出力の表示（続き）

trace コマンド セクション	出力
Envelope Sender Address Processing	
これらのセクションには、指定したエンベロープ送信者に対してアプライアンスの設定がどのように影響するかが要約されます（つまり、MAIL FROM コマンドがアプライアンスの設定によってどのように解釈されるかがわかります）。`trace` コマンドは、このセクションの前に「`Processing MAIL FROM:`」を出力します。	
Default Domain	リスナーで、受信するメッセージのデフォルトの送信者ドメインを変更するように指定した場合は、エンベロープ送信者に対するすべての変更がこのセクションに出力されます。 詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「SMTP Address Parsing Options」を参照してください。
Masquerading	メッセージのエンベロープ送信者を変換するように指定した場合は、ここに変更が表示されます。`listenerconfig -> edit -> masquerade -> config` サブコマンドを使用して、プライベート リスナーに対するエンベロープ送信者のマスカレードをイネーブルにします。 詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Masquerading」を参照してください。
Envelope Recipient Processing	
これらのセクションでは、指定したエンベロープ受信者に対してアプライアンスがどのように影響するかの要約を示します（つまり、RCPT TO コマンドがアプライアンスの設定によってどのように解釈されるかがわかります）。`trace` コマンドは、このセクションの前に「`Processing Recipient List:`」を出力します。	

表 7-2　トレースを実行した後の出力の表示（続き）

trace コマンド セクション	出力
Default Domain	リスナーで、受信するメッセージのデフォルトの送信者ドメインを変更するように指定した場合は、エンベロープ受信者に対するすべての変更がこのセクションに出力されます。 詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Customizing Listeners」の章の「SMTP Address Parsing Options」を参照してください。
Domain Map Translation	ドメイン マップ機能によって、受信者アドレスが代替アドレスに変換されます。ドメイン マップの変更を指定しており、指定した受信者アドレスが一致した場合は、このセクションに変換が出力されます。 詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「The Domain Map Feature」を参照してください。
Recipient Access Table (RAT)	ポリシーとパラメータのほか、このセクションには、RAT 内のエントリに一致する各エンベロープ受信者が出力されます（たとえば、リスナーの RAT の制限をバイパスするように、受信者を指定した場合）。 受け入れる受信者の指定の詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Accepting Email for Local Domains or Specific Users on Public listeners (RAT)」を参照してください。

表 7-2　トレースを実行した後の出力の表示（続き）

trace コマンド セクション	出力
Alias Table	このセクションには、アプライアンスで設定されたエイリアス テーブル内のエントリに一致する各エンベロープ受信者（および 1 つまたは複数の受信者アドレスへの後続の変換）が出力されます。 詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Creating Alias Tables」を参照してください。

Pre-Queue Message Operations

ここでは、メッセージのコンテンツを受信してから、メッセージを作業キューに入れるまでに、アプライアンスが各メッセージにどのような影響を及ぼすかを説明します。この処理は、最後の `250 ok` コマンドがリモート MTA に返される前に実行されます。

`trace` コマンドは、このセクションの前に「Message Processing:」を出力します。

Virtual Gateways	`altsrchost` コマンドを実行すると、エンベロープ送信者の完全アドレス、ドメイン、または名前、あるいは IP アドレスの一致に基づいて、特定のインターフェイスにメッセージが割り当てられます。エンベロープ送信者が `altsrchost` コマンドのエントリに一致すると、その情報がこのセクションに出力されます。 ここで割り当てられた仮想ゲートウェイ アドレスは、後述のメッセージ フィルタ処理によって上書きされる場合があります。 詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Using Virtual Gateway™ Technology」を参照してください。

表 7-2　トレースを実行した後の出力の表示（続き）

trace コマンド セクション	出力
Bounce Profiles	バウンス プロファイルは、処理中の 3 つの時点で適用されます。ここが最初のポイントです。リスナーにバウンス プロファイルが割り当てられる場合は、プロセス内のこの時点で割り当てられます。その情報がこのセクションに出力されます。 詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Handling Undeliverable Email」を参照してください。

表 7-2　トレースを実行した後の出力の表示（続き）

trace コマンド セクション	出力
Work Queue Operations	
次の一連の機能は、作業キュー内のメッセージに対して実行されます。機能が実行されるのは、クライアントからのメッセージが受け入れられた後、そのメッセージが配信用として宛先キューに入れられる前です。`status` コマンドおよび `status detail` コマンドによって「Messages in Work Queue」が報告されます。	
Masquerading	メッセージの [To:]、[From:]、および [CC:] ヘッダーが（リスナーから入力されたスタティック テーブルまたは LDAP クエリーを通じて）マスクされるように指定した場合は、ここに変更が表示されます。`listenerconfig -> edit -> masquerade -> config` サブコマンドを使用して、プライベート リスナーに対してメッセージ ヘッダーのマスカレードをイネーブルにします。 詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Masquerading」を参照してください。
LDAP Routing	リスナーに対して LDAP クエリーがイネーブルになっている場合は、このセクションに LDAP 許可、再ルーティング、マスカレード、およびグループ クエリーの結果が出力されます。 詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「LDAP Queries」を参照してください。

表 7-2　トレースを実行した後の出力の表示（続き）

trace コマンド セクション	出力
Message Filters Processing	システムでイネーブルになっているすべてのメッセージ フィルタは、この時点でテスト メッセージによって評価されます。フィルタごとにルールが評価され、最後の結果が「true」であれば、そのフィルタの各アクションが順次実行されます。フィルタには他のフィルタがアクションとして含まれている場合があり、フィルタは無制限にネスティングされます。ルールが「false」と評価された場合、アクションのリストが `else` 句に関連付けられていれば、それらのアクションが代わりに評価されます。このセクションには、順番に処理されたメッセージ フィルタの結果が出力されます。 『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Using Message Filters to Enforce Email Policies」を参照してください。
Mail Policy Processing	メール ポリシーの処理セクションには、アンチスパム、アンチウイルス、Outbreak フィルタ機能と、指定されたすべての受信者に対する免責事項のスタンプが表示されます。複数の受信者が電子メール セキュリティ マネージャの複数のポリシーに一致する場合は、一致する各ポリシーが次の各セクションに繰り返し表示されます。「Message going to」というストリングは、どの受信者がどのポリシーに一致したかを定義します。

表 7-2　トレースを実行した後の出力の表示（続き）

trace コマンド セクション	出力
Anti-Spam	このセクションには、アンチスパム スキャンの処理対象としてフラグが設定されていないメッセージが示されます。メッセージがリスナーに対するアンチスパム スキャンによって処理されることになっている場合、メッセージは処理され、返された判定が出力されます。Cisco IronPort アプライアンスが、その判定に基づいてメッセージをバウンスまたはドロップするように設定されている場合は、その情報が出力され、trace コマンドの処理は停止します。 注：システムでアンチスパム スキャンが使用できない場合、この手順は省略されます。アンチスパム スキャンを使用できても、機能キーによってイネーブルになっていない場合は、その情報もこのセクションに出力されます。 詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Anti-Spam」を参照してください。

表 7-2　トレースを実行した後の出力の表示（続き）

trace コマンド セクション	出力
Anti-Virus	このセクションには、アンチウイルス スキャンの処理対象としてフラグが設定されていないメッセージが示されます。メッセージがリスナーに対するアンチウイルス スキャンによって処理されることになっている場合、メッセージは処理され、返された判定が出力されます。Cisco IronPort アプライアンスが、感染メッセージを「クリーニング」するように設定されている場合は、その情報が表示されます。その判定に基づいてメッセージをバウンスまたはドロップするように設定されている場合は、その情報が出力され、`trace` コマンドの処理は停止します。 注：システムでアンチウイルス スキャンが使用できない場合、この手順は省略されます。アンチウイルス スキャンを使用できても、機能キーによってイネーブルになっていない場合は、その情報もこのセクションに出力されます。 詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Anti-Virus」を参照してください。
Outbreak Filters Processing	このセクションには、Outbreak フィルタ機能をバイパスする添付ファイルを含むメッセージが示されます。メッセージが受信者に対する Outbreak フィルタ機能によって処理されることになっている場合、メッセージは処理され、その評価が出力されます。アプライアンスが、判定に基づいてメッセージを検疫、バウンス、またはドロップするように設定されている場合、その情報が出力されて、処理が停止します。 詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Outbreak Filters」を参照してください。

表 7-2　トレースを実行した後の出力の表示（続き）

trace コマンド セクション	出力
Footer Stamping	このセクションには、メッセージに免責事項テキスト リソースが付加されたかどうかが示されます。テキスト リソースの名前が表示されます。『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Message Disclaimer Stamping」を参照してください。

表 7-2　トレースを実行した後の出力の表示（続き）

trace コマンド セクション	出力
Delivery Operations	
次の各セクションには、メッセージが配信されるときに発生する動作が示されます。`trace` コマンドは、このセクションの前に「`Message Enqueued for Delivery`」を出力します。	
Global Unsubscribe per Domain and per User	`trace` コマンドの入力として指定した受信者が、グローバル配信停止機能に示されている受信者、受信者ドメイン、または IP アドレスに一致すると、未登録の受信者アドレスがこのセクションに出力されます。 『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Using Global Unsubscribe」を参照してください。
Final Result	
すべての処理が出力されると、最終結果が表示されます。CLI では、「Would you like to see the resulting message?」という問いに対して **`y`** を入力します。	

[Trace] ページの GUI の例

図 7-1　[Trace] ページの入力

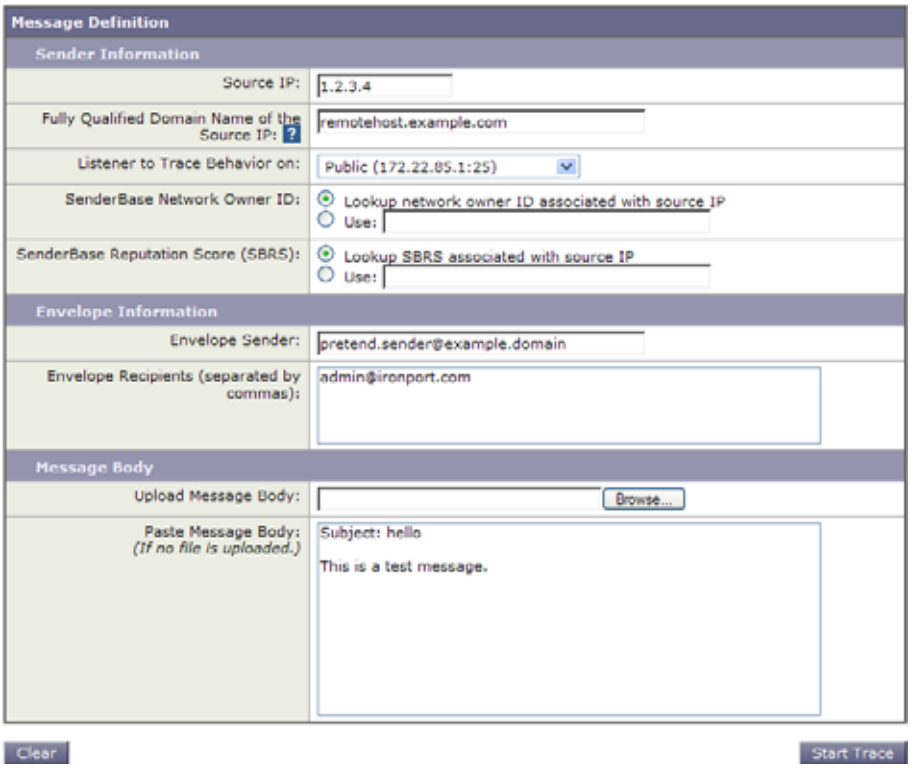
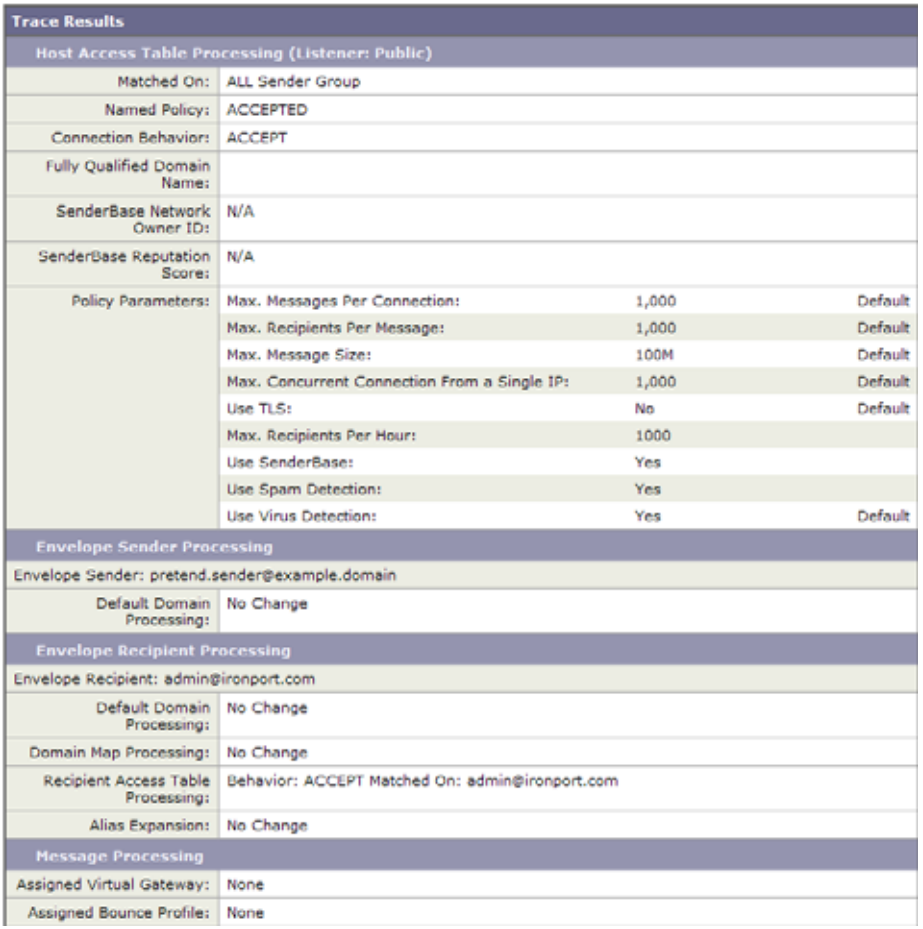


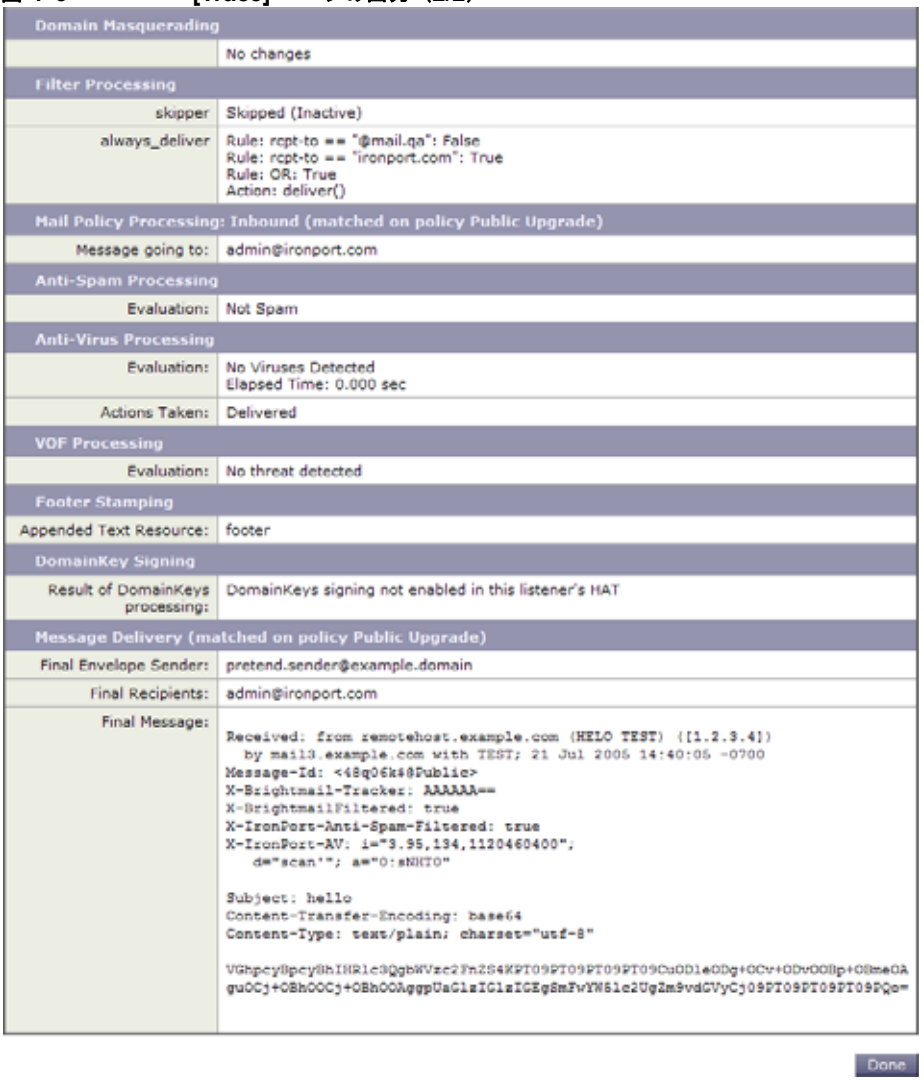
図 7-2　[Trace] ページの出力（1/2）



Trace

Trace Results			
Host Access Table Processing (Listener: Public)			
Matched On:	ALL Sender Group		
Named Policy:	ACCEPTED		
Connection Behavior:	ACCEPT		
Fully Qualified Domain Name:			
SenderBase Network Owner ID:	N/A		
SenderBase Reputation Score:	N/A		
Policy Parameters:	Max. Messages Per Connection:	1,000	Default
	Max. Recipients Per Message:	1,000	Default
	Max. Message Size:	100M	Default
	Max. Concurrent Connection From a Single IP:	1,000	Default
	Use TLS:	No	Default
	Max. Recipients Per Hour:	1000	
	Use SenderBase:	Yes	
	Use Spam Detection:	Yes	
	Use Virus Detection:	Yes	Default
Envelope Sender Processing			
Envelope Sender: pretend.sender@example.domain			
Default Domain Processing:	No Change		
Envelope Recipient Processing			
Envelope Recipient: admin@ironport.com			
Default Domain Processing:	No Change		
Domain Map Processing:	No Change		
Recipient Access Table Processing:	Behavior: ACCEPT Matched On: admin@ironport.com		
Alias Expansion:	No Change		
Message Processing			
Assigned Virtual Gateway:	None		
Assigned Bounce Profile:	None		

図 7-3　[Trace] ページの出力（2/2）



Domain Masquerading	
	No changes
Filter Processing	
skipper	Skipped (Inactive)
always_deliver	Rule: rcpt-to == "@mail.qa": False Rule: rcpt-to == "ironport.com": True Rule: OR: True Action: deliver()
Mail Policy Processing: Inbound (matched on policy Public Upgrade)	
Message going to:	admin@ironport.com
Anti-Spam Processing	
Evaluation:	Not Spam
Anti-Virus Processing	
Evaluation:	No Viruses Detected Elapsed Time: 0.000 sec
Actions Taken:	Delivered
VOF Processing	
Evaluation:	No threat detected
Footer Stamping	
Appended Text Resource:	footer
DomainKey Signing	
Result of DomainKeys processing:	DomainKeys signing not enabled in this listener's HAT
Message Delivery (matched on policy Public Upgrade)	
Final Envelope Sender:	pretend.sender@example.domain
Final Recipients:	admin@ironport.com
Final Message:	Received: from remotehost.example.com (HELO TEST) ([1.2.3.4]) by mail3.example.com with TEST; 21 Jul 2005 14:40:05 -0700 Message-Id: <48q06k4@Public> X-Brightmail-Tracker: AAAAAA== X-BrightmailFiltered: true X-IronPort-Anti-Spam-Filtered: true X-IronPort-AV: i="3.95,134,1120460400", d="scan'"; a="0:sNHT0" Subject: hello Content-Transfer-Encoding: base64 Content-Type: text/plain; charset="utf-8" VGhpcyBpcyBhIHRlc3QgbWVzc2FnZS4KPT09PT09PT09PT09CuODleODg+ODv+ODvOOBp+OBmeOA guOCj+OBhOOCj+OBhOOAggpUaGlzIGlzIGEgSmFwYW5lc2UgZm9vdGVyCj09PT09PT09PT09Cg==

Done

GUI からの XML ステータスの収集

- XML ページを通じてステータスを表示するか、XML ステータス情報にプ

ログラムでアクセスします。

XML ステータス機能は、電子メールのモニタリング統計情報にプログラムでアクセスする方法を提供します。最新のブラウザによっては、XML データを直接表示できるものもあります。

次の表に示す GUI の各ページの情報は、対応する URL にアクセスすることにより、動的な XML 出力としても使用できます。

GUI のページ名	対応する XML ステータス URL
Mail Status	`http://`*hostname*`/xml/status`
Host Mail Status for a Specified Host	`http://`*hostname*`/xml/hoststatus?hostname=`*host*
DNS Status	`http://`*hostname*`/xml/dnsstatus`
Top Incoming Domains	`http://`*hostname*`/xml/topin`
Top Outgoing Domains[a]	`http://`*hostname*`/xml/tophosts`

[a] このページはデフォルトで、アクティブ受信者の番号順にソートされます。この順番を変更するには、URL に「?sort=**order**」を付加します。ここで、**order** は conn_out、deliv_recip、soft_bounced、または hard_bounced です。

CHAPTER 8

一般的な管理タスク

Framemaker テンプレートの内容は次のとおりです。

Cisco IronPort アプライアンスの管理

以下のタスクでは、Cisco IronPort アプライアンス内の一般的な機能を簡単に管理できます。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`
- `updateconfig`

- `upgrade`

Cisco IronPort アプライアンスのシャットダウン

Cisco IronPort アプライアンスをシャットダウンするには、GUI の [System Administration] メニューで利用可能な [Shutdown/Suspend] ページを使用するか、CLI で `shutdown` コマンドを使用します。図 8-1 に、[Shutdown/Suspend] ページを使用してアプライアンスをシャットダウンする方法を示します。

アプライアンスをシャットダウンすると、Cisco IronPort 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。デフォルトの遅延値は 30 秒です。Cisco IronPort AsyncOS では、その遅延値の間にオープンな接続が完了します。その遅延値を超えると、オープンな接続は強制的に閉じられます。

図 8-1　GUI によるアプライアンスのシャットダウン

Cisco IronPort アプライアンスのリブート

Cisco IronPort 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/Suspend] ページを使用するか、CLI で `reboot` コマンドを使用します。図 8-2 に、[Shutdown/Suspend] ページを使用してアプライアンスをリブートする方法を示します。

アプライアンスをリブートすると、Cisco IronPort AsyncOS が再起動され、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。デフォルトの遅延値は 30 秒です。Cisco IronPort AsyncOS では、その遅延値の間にオープンな接続が完了します。その遅延値を超えると、オープンな接続は強制的に閉じられます。アプライアンスは、配信キュー内のメッセージを失わずに再起動できます。

図 8-2　GUI を使用したアプライアンスのリブート

Cisco IronPort アプライアンスをメンテナンス状態にする

システム メンテナンスを実行する場合は、Cisco IronPort アプライアンスをオフライン状態にする必要があります。suspend コマンドと offline コマンドを実行すると、Cisco IronPort AsyncOS オペレーティング システムがオフライン状態になります。オフライン状態の特徴は次のとおりです。

- 着信電子メール接続が許可されません。
- 発信電子メール配信は停止されます。
- ログ転送が停止されます。
- CLI はアクセス可能のままになります。

アプライアンスがオフライン状態になる遅延値を入力する必要があります。デフォルトの遅延値は 30 秒です。Cisco IronPort AsyncOS では、その遅延値の間にオープンな接続が完了します。その遅延値を超えると、オープンな接続は強制的に閉じられます。オープンな接続がない場合は、すぐにオフライン状態になります。

（注）　suspend コマンドと offline コマンドの違いは、suspend コマンドはマシンのリブート後でもその状態を保持することです。suspend コマンドを発行し、アプライアンスをリブートする場合は、resume コマンドを使用してシステムをオンライン状態に戻す必要があります。

GUI で [System Administration] > [Shutdown/Suspend] ページを使用して、アプライアンスでの電子メールの送受信を中断できます。アプライアンスに複数のリスナーが存在する場合は、個々のリスナーに対して電子メールの受信を中断および再開できます。電子メールの送受信を中断するために、[Commit] をクリックします。

図 8-3 に、電子メールの送受信が中断された電子メール セキュリティ アプライアンスの例を示します。

図 8-3　アプライアンスで中断された電子メールの処理

suspend コマンドと 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

AsyncOS CLI で resume コマンドを実行すると、Cisco IronPort AsyncOS オペレーティング システム（suspenddel または suspend コマンドの使用後）が通常の動作状態に戻ります。

また、GUI で [System Administration] > [Shutdown/Suspend] ページを使用して、アプライアンスでの電子メールの送受信を再開できます。アプライアンスに複数のリスナーが存在する場合は、個々のリスナーに対して電子メールの受信を再開できます。電子メールの送受信を再開するために、[Commit] をクリックします。

resume コマンド

```
mail3.example.com> resume


Receiving resumed.

Mail delivery resumed.

mail3.example.com>
```

出荷時デフォルト値へのリセット

物理的にアプライアンスを移動したときに、出荷時デフォルト値に戻したい場合があります。[System Administration] > [Configuration File] ページの [Reset Configuration] セクションまたは resetconfig コマンドを使用すると、すべての

Cisco IronPort AsyncOS の設定値が出荷時デフォルト値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。設定のリセット後にシステム設定ウィザードまたは systemsetup コマンドを実行することが推奨されます。

（注）　resetconfig コマンドは、アプライアンスがオフライン状態にあるときにのみ動作します。resetconfig コマンドが完了すると、systemsetup コマンドを再び実行する前であってもアプライアンスがオフ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 のバージョンを確認するには、GUI の [Monitor] メニューから [System Overview] ページを使用するか（「System Status」（P.2-59）を参照）、CLI で `version` コマンドを使用します。

サポート コマンド

アプライアンスをアップグレードする場合やサポート プロバイダーに連絡する場合に役に立つコマンドと機能は次のとおりです。

- テクニカル サポート（[Support Request] ページと [Remote Access] ページ）
- 機能キー

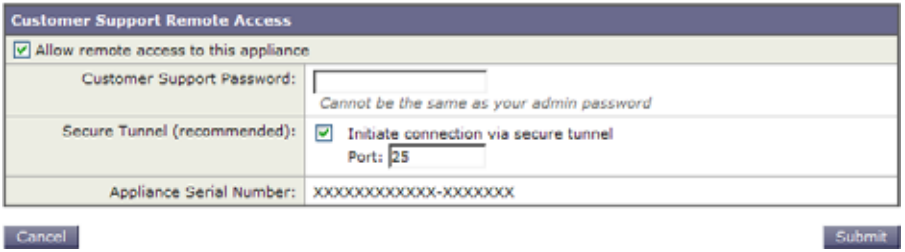
テクニカル サポート

[System Administration] メニューの [Technical Support] セクションには、[Support Request] と [Remote Access] の 2 つのページが含まれます。

Remote Access

Cisco IronPort 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。

図 8-4　[Remote Access] ページ



リモート アクセスをイネーブルにすると、デバッグとシステムへの一般的なアクセスのための、Cisco IronPort カスタマー サポートにより使用される特別なアカウントが有効になります。これは、Cisco IronPort カスタマー サポートにより、顧客がシステムを設定したり、設定を理解したり、障害レポートを調査したりするのを支援するために使用されます。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、アプライアンスにより指定済みポートを介してサーバ `upgrades.ironport.com` への SSH トンネルが作成されます。デフォルトでは、この接続はポート 25 を介します（システムでは電

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が必要になるため、このポートの使用はほとんどの環境で問題ありません）。upgrades.ironport.com への接続が確立されたら、Cisco IronPort カスタマー サポートは SSH トンネルを使用してアプライアンスへのアクセスを取得できます。ポート 25 を介した接続が許可される限り、ほとんどのファイアウォールの制限は適用されません。また、CLI で techsupport tunnel コマンドを使用することもできます。

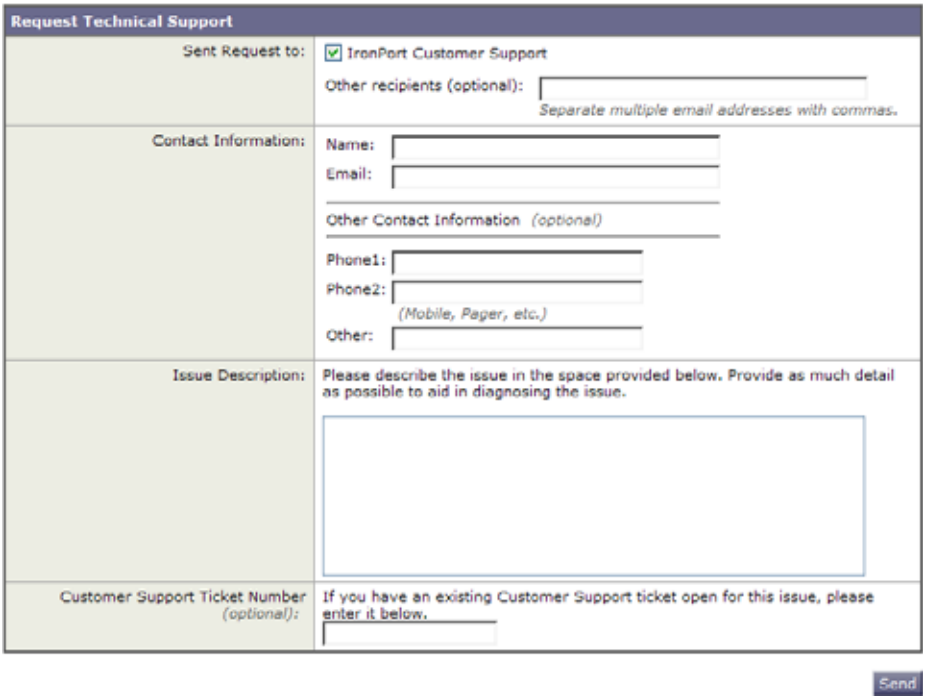
「リモート アクセス」と「トンネル」の両方のモードでは、パスワードが必要です。これはシステムにアクセスするために使用されるパスワード *ではない* ことを理解することが重要です。パスワードとシステムのシリアル番号がカスタマー サポート担当者に提供された後で、アプライアンスにアクセスするために使用されるパスワードが生成されます。

techsupport トンネルがイネーブルになると、upgrades.ironport.com に 7 日間接続されたままになります。7 日間後に、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はアクティブです。

Support Request

[Help] > [Support Request] ページまたは supportrequest コマンド（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）を使用すると、アプライアンスの設定を Cisco IronPort カスタマー サポート チームや追加ユーザに電子メールで送信したり、サポートが必要な問題に関するコメントを入力したりできます。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電子メールを送信できる必要があります。

図 8-5　[Support Request] ページ



ステップ 1　連絡先情報（名前、電子メール アドレス、電話番号など）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　デフォルトでは、サポート要求（コンフィギュレーション ファイルを含む）は Cisco IronPort カスタマー サポートに送信されます（フォーム上部のチェックボックスを使用）。また、他の電子メール アドレス（複数のアドレスはカンマで区切ります）にコンフィギュレーション ファイルを電子メールで送信することもできます。

ステップ 4　この問題に関するカスタマー サポート チケットをすでに持っている場合は、それを入力してください。

ステップ 5　[Send] をクリックします。

ステップ 6　トラブル チケットが作成されます。詳細については、「シスコのテクニカル サポート」（P.1-7）を参照してください。

パケット キャプチャ

場合によっては、問題発生時に Cisco IronPort カスタマー サポートに問い合わせたときに、電子メール セキュリティ アプライアンスとのネットワーク状況について尋ねられることがあります。アプライアンスでは、アプライアンスが接続されたネットワークで送受信されている TCP/IP と他のパケットを傍受および表示できます。

パケット キャプチャを実行すると、ネットワーク設定をデバッグしたり、アプライアンスに到達しているネットワーク トラフィックやアプライアンスから送信されているネットワーク トラフィックを確認したりできます。

アプライアンスはキャプチャされたパケットの状態をファイルに保存し、ファイルをローカルで保持します。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。

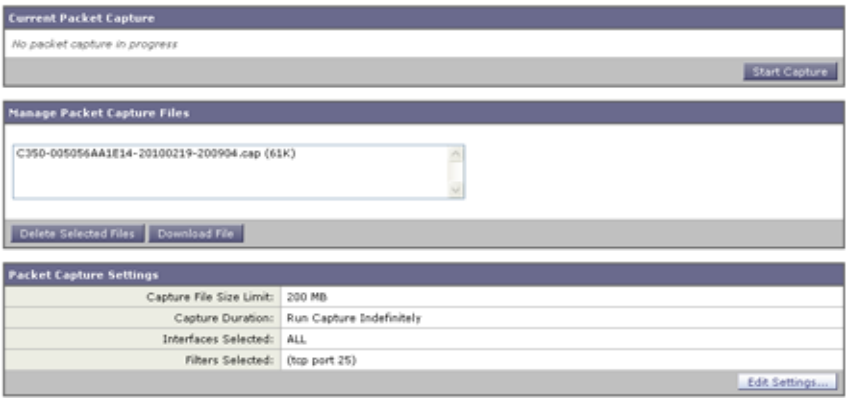
GUI の [Support and Help] > [Packet Capture] ページには、ハード ドライブに格納された完全なパケット キャプチャ ファイルの一覧が表示されます。パケット キャプチャが実行されている場合、[Packet Capture] ページには、実行中のキャプチャのステータス（ファイル サイズや経過時間などの現在の統計情報）が表示されます。

パケット キャプチャ ファイルは [Download File] ボタンを使用してダウンロードし、デバッグやトラブルシューティングのために Cisco IronPort カスタマー サポートに電子メールで送信できます。また、1 つまたは複数のファイルを選択し、[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。

CLI で、`packetcapture` コマンドを使用します。

図 8-6 に、GUI の [Packet Capture] ページを示します。

図 8-6　[Packet Capture] ページ



（注）　パケット キャプチャ機能は UNIX の tcpdump コマンドに似ています。

パケット キャプチャの開始

CLI でパケット キャプチャを開始するには、`packetcapture` > `start` コマンドを実行します。実行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。アプライアンスで、セッション終了時にパケット キャプチャが停止します。

GUI でパケット キャプチャを開始するには、[Support and Help] メニューの [Packet Capture] オプションを選択し、[Start Capture] をクリックします。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。GUI で開始されたキャプチャはセッション間で維持されます。

（注）　GUI に表示されるのは GUI で開始されたパケット キャプチャだけで、CLI で開始されたパケット キャプチャは表示されません。同様に、CLI には CLI で開始された現在のパケット キャプチャのステータスだけが表示されます。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

CLI でパケット キャプチャ設定を編集するには、`packetcapture` > `setup` コマンドを実行します。

GUI でパケット キャプチャ設定を編集するには、[Support and Help] メニューの [Packet Capture] オプションを選択し、[Edit Settings] をクリックします。

表 8-1 に、設定可能なパケット キャプチャの項目を示します。

表 8-1　パケット キャプチャ設定オプション

オプション	説明
Capture file size limit	すべてのパケット キャプチャ ファイルの最大ファイル サイズ（メガバイト単位）。
Capture Duration	パケット キャプチャの実行時間を選択します。 • [Run Capture Until File Size Limit Reached]。パケット キャプチャは、ファイル サイズ制限に到達するまで実行されます。 • [Run Capture Until Time Elapsed Reaches]。パケット キャプチャは、設定された時間が経過するまで実行されます。時間は秒単位（s）、分単位（m）、または時間単位（h）で入力できます。単位を指定せずに時間を入力すると、AsyncOS ではデフォルトで秒単位が使用されます。このオプションは GUI でのみ使用できます。 パケット キャプチャ ファイルは 10 個の部分に分割されます。全体の時間が経過する前にパケット キャプチャ ファイルが最大サイズ制限に到達した場合は、そのファイルの最も古い部分が削除され（データが破棄されます）、現在のパケット キャプチャ データで新しい部分が開始されます。パケット キャプチャ ファイルは一度に 1/10 だけ破棄されます。 • [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。

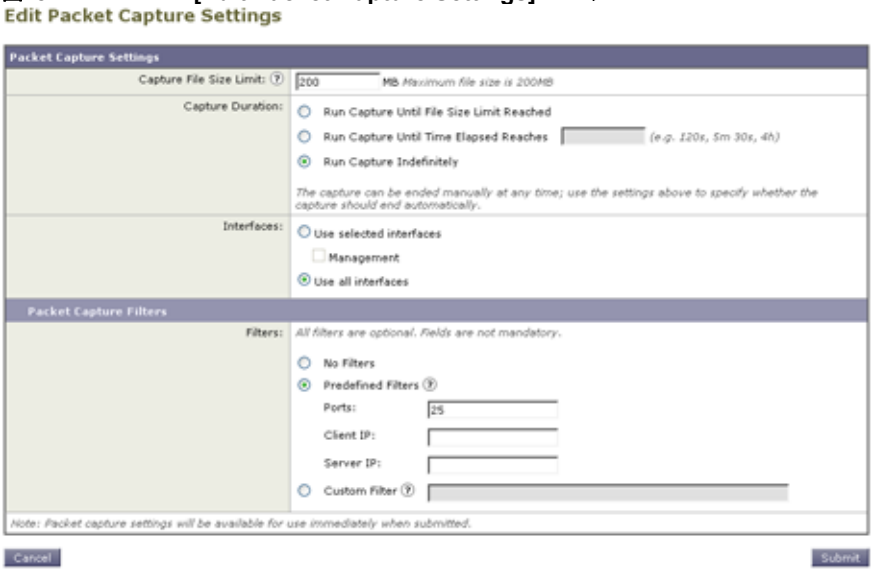
表 8-1　パケット キャプチャ設定オプション（続き）

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 でフィルタリングしたり（GUI のみ）、UNIX の tcpdump コマンドでサポートされた構文（`host 10.10.10.10 && port 80` など）を使用してカスタム フィルタを作成したりできます。 クライアント IP は、電子メール セキュリティ アプライアンスを介してメッセージを送信するメール クライアントなどのアプライアンスに接続しているマシンの IP アドレスです。 サーバ IP は、アプライアンスがメッセージを配信する Exchange サーバなどのアプライアンスが接続しているマシンの IP アドレスです。 クライアントとサーバの IP アドレスを使用して、中間に電子メール セキュリティ アプライアンスがある特定のクライアントと特定のサーバ間のトラフィックを追跡できます。

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）。変更を保存する必要はありません。

図 8-7 に、GUI でパケット キャプチャ設定を編集する例を示します。

図 8-7　[Edit Packet Capture Settings] ページ



機能キーの使用

Cloud Email Security アプライアンスの機能キーの設定は変更しないことを推奨します。

場合によっては、サポート チームが、システムで特定の機能をイネーブルにするキーを提供することがあります。GUI で [System Administration] > [Feature Keys] ページ（または CLI で `featurekey` コマンド）を使用し、キーを入力して、関連付けられた機能をイネーブルにします。

キーはアプライアンスのシリアル番号とイネーブルにされる機能に固有です（あるシステムのキーを別のシステムで再使用することはできません）。キーを間違って入力した場合は、エラー メッセージが生成されます。

機能キーの機能は [Feature Keys] と [Feature Key Settings] の 2 つのページに分割されます。

[Feature Keys] ページ

GUI にログインし、[System Administration] タブをクリックします（GUI へのアクセス方法については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Overview」の章を参照してください）。左側のメニューの [Feature Keys] リンクをクリックします。[Feature Keys] ページの内容は次のとおりです。

- アプライアンスのすべてのアクティブな機能キーが表示されます。
- アクティベーション待ちのすべての機能キーが表示されます。
- 発行された新しいキーを検索できます（これは任意であり、キーをインストールすることもできます）。

現在イネーブルな機能の一覧が表示されます。[Pending Activation] セクションは、アプライアンスに対して発行され、まだアクティベートされていない機能キーの一覧です。設定に応じてアプライアンスが新しいキーを定期的に確認することがあります。[Check for New Keys] ボタンをクリックすると、待機状態のキーの一覧が更新されます。

機能キーの設定

[Feature Key Settings] ページは、新しい機能キーを確認およびダウンロードするかどうかや、これらのキーを自動的にアクティベートするかどうかを制御するために使用します。

図 8-8　[Feature Key Settings] ページ

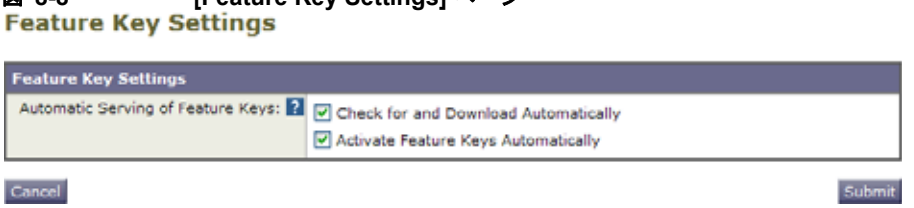
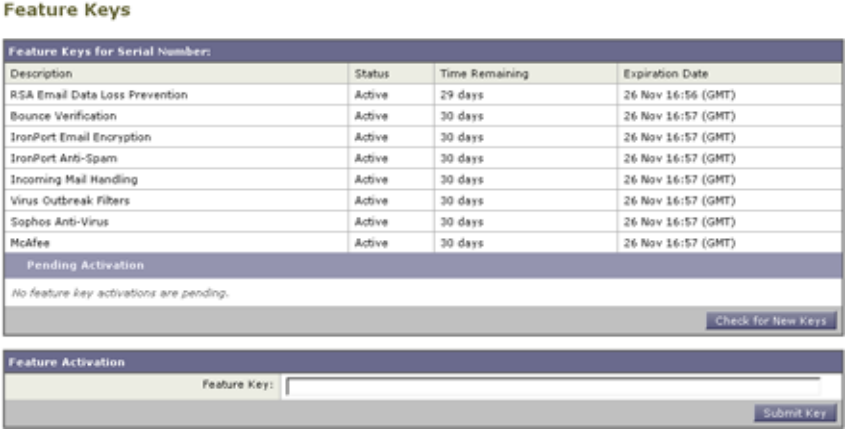


図 8-9　[Feature Keys] ページ



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（キーが正しくない場合など）。それ以外の場合は、機能キーが画面に追加されます。

[Pending Activation] 一覧の新しい機能キーをアクティベートするには、そのキーを選択し（[Select] チェックボックスをオンにします）、[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 Cisco IronPort アプライアンスを設定できます。この場合、[Pending Activation] 一覧は常に空白になります。[Feature Key Settings] ページで自動確認をディセーブルにした場合であっても、[Check for New Keys] ボタンをクリックすることにより、新しいキーを検索するよう AsyncOS にいつでも指示できます。

期限切れ機能キー

（GUI から）アクセスしようとしている機能の機能キーの有効期限が切れている場合は、Cisco IronPort 担当者またはサポート組織までご連絡ください。

ユーザ アカウントを使用する作業

Cisco IronPort アプライアンスには、ユーザ アカウントを追加する 2 つの方法があります。Cisco IronPort アプライアンス自体でユーザ アカウントを作成する方法と、LDAP または RADIUS ディレクトリなどの独自の中央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。ユーザと外部認証ソースへの接続を管理するには、[System Administration] > [Users] ページを使用します（または、CLI で `userconfig` コマンドを使用します）。ユーザを認証するために外部ディレクトリを使用することについては、「外部認証」（P.8-35）を参照してください。

システムのデフォルトのユーザ アカウントである admin はすべての管理権限を持っています。admin ユーザ アカウントは削除できませんが、パスワードを変更してアカウントをロックすることはできます。

新しいユーザ アカウントを作成する場合は、そのユーザを定義済みのユーザ ロールまたはカスタム ユーザ ロールに割り当てます。各ロールには、システム内での異なるレベルの権限が含まれます。

アプライアンスで作成できるユーザ アカウントの数には制限がありませんが、システムにより予約された名前ではユーザ アカウントを作成できません。たとえば、「operator」や「root」などの名前のユーザ アカウントは作成できません。

表 8-2 は、ユーザ アカウントで使用可能なロールを示しています。

表 8-2　ユーザ ロールの一覧

ユーザ ロール	説明
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。ただし、`resetconfig` コマンドと `revert` コマンドにアクセスできるのは admin ユーザだけです。 **（注）** AsyncOS は、GUI から電子メール セキュリティ アプライアンスを同時に設定する複数の管理者をサポートしません。
Technician	Technician ロールを持つユーザ アカウントはシステムのアップグレード、アプライアンスのリブート、機能キーの管理を実行できます。Technician は、アプライアンスをアップグレードするために以下の処理も実行できます。 • 電子メールの配信および受信の一時停止。 • 作業キューとリスナーのステータスの表示。 • コンフィギュレーション ファイルの保存および電子メール送信。 • セーフリストとブロックリストのバックアップ。Technician はこれらのリストを復元できません。 • クラスタからのアプライアンスの接続解除。 • Cisco IronPort テクニカル サポートへのリモート サービス アクセスのイネーブル化またはディセーブル化。 • サポート要求の申請。

表 8-2　ユーザ ロールの一覧（続き）

ユーザ ロール	説明
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。 • `systemsetup` コマンドの発行またはシステム設定ウィザードの実行。 • `adminaccessconfig` コマンドの発行。 • 一部検疫機能の実行（検疫の作成および削除を含む）。 • ユーザ名とパスワード以外の LDAP サーバ プロファイル設定の変更（LDAP が外部認証に対してイネーブルになっている場合）。 これら以外は、Administrator ロールと同じ権限を持ちます。
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 IronPort スパム検疫とシステ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。
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 IronPort スパム検疫とシステ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。

表 8-2　ユーザ ロールの一覧（続き）

ユーザ ロール	説明
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。 • IronPort スパム検疫およびシステム検疫の管理。 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 IronPort スパム検疫とシステム検疫を管理できるようにするには、これらへのアクセスをイネーブルにする必要があります。
カスタム ユーザ ロール	カスタム ユーザ ロールを持つユーザ アカウントはそのロールに割り当てられている電子メール セキュリティ機能にのみアクセスできます。アクセスできる機能は、DLP ポリシー、電子メール ポリシー、レポート、検疫、ローカル メッセージ トラッキング、暗号化プロファイル、およびトレース デバッグ ツールの任意の組み合わせになります。このユーザはシステム設定機能にはアクセスできません。カスタム ユーザ ロールを定義できるのは管理者だけです。詳細については、「委任管理のためのカスタム ユーザ ロールの管理」（P.8-44）を参照してください。 **（注）**　カスタム ロールに割り当てられているユーザは、CLI にはアクセスできません。
Cloud ロール	Cloud Email Security アプライアンスは、Cloud 環境専用に設計されている一連のユーザ ロールを使用します。Cloud ユーザ用に定義されているロールの詳細については、「Cisco IronPort Cloud Email Security の管理」（P.8-39）を参照してください。

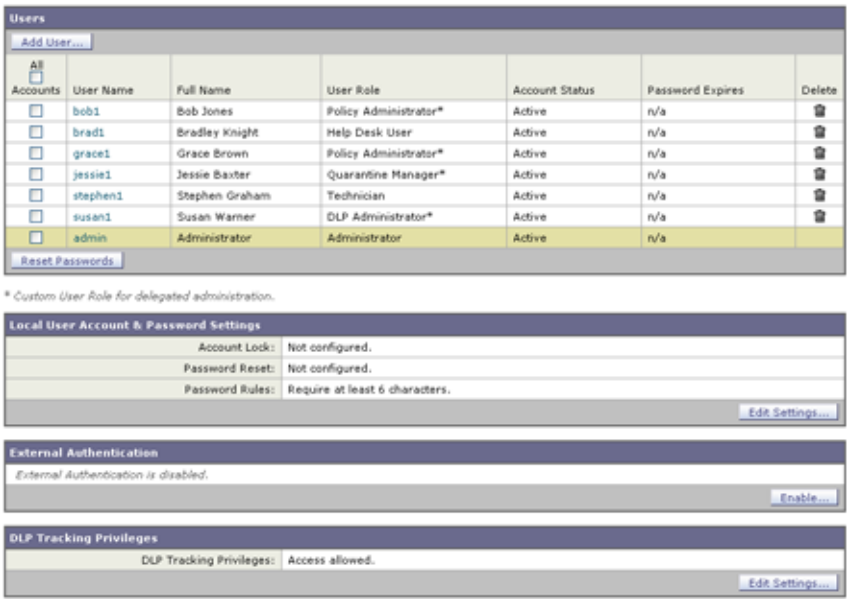
表 8-2 に定義されているロールはすべて GUI と CLI の両方にアクセスできます。ただし、Help Desk User ロールとカスタム ユーザ ロールは GUI にのみアクセスできます。

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.8-35）を参照してください。

ユーザの管理

[System Administration] > [Users] ページで、ユーザを管理できます。

図 8-10　[Users] ページ



[Users] ページには、システムの既存のユーザが一覧（ユーザ名、氏名、およびユーザ タイプまたはグループを含む）で表示されます。

[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。詳細については、「ユーザの追加」（P.8-23）を参照してください。

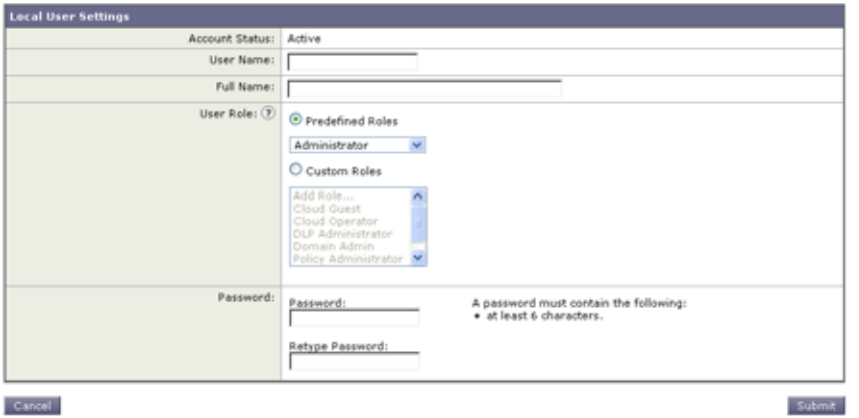
- ユーザの削除。詳細については、「ユーザの削除」（P.8-26）を参照してください。
- ユーザの編集。ユーザのパスワードの変更、ユーザのアカウントのロックおよびロック解除など。詳細については、「ユーザの編集」（P.8-24）を参照してください。
- ローカル アカウント用のユーザ アカウントとパスワード設定値の設定。詳細については、「制限的なユーザ アカウントとパスワードの設定値の設定」（P.8-30）を参照してください。
- ユーザを認証するために LDAP または RADIUS ディレクトリを使用するようアプライアンスをイネーブルにする。詳細については、「外部認証」（P.8-35）を参照してください。
- メッセージ トラッキング内の DLP Matched Content への管理者以外のアクセスをイネーブルにする。

ユーザの追加

ユーザを追加するには、次の手順を実行します。

ステップ 1　[System Administration] > [Users] ページで、[Add User] をクリックします。[Add User] ページが表示されます。

図 8-11　ユーザの追加



ステップ 2　ユーザのログイン名を入力します。一部の単語（「operator」や「root」など）は予約されています。

ステップ 3　ユーザの氏名を入力します。

ステップ 4　定義済みのユーザ ロールまたはカスタム ユーザ ロールを選択します。（ユーザ ロールの詳細については、表 8-2 を参照してください）。

（注）　新しいユーザ ロールを作成して、このユーザ アカウントに適用することができます。詳細については、「委任管理のためのカスタム ユーザ ロールの管理」（P.8-44）を参照してください。

ステップ 5　パスワードを入力し、パスワードを再入力します。パスワードは、[Local User Account & Password Settings] セクションで定義されているルールに準拠している必要があります。詳細については、「制限的なユーザ アカウントとパスワードの設定値の設定」（P.8-30）を参照してください。

ステップ 6　変更を送信し、保存します。

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 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　変更を送信し、保存します。

ユーザ アカウントのロックおよびロック解除

ユーザ アカウントをロックすると、ローカル ユーザがアプライアンスにログインするのを防ぐことができます。ユーザ アカウントは、次のいずれかの方法でロックできます。

- AsyncOS は、ユーザが [Local User Account & Password Settings] セクションで定義されている失敗ログイン試行の最大回数を超えた場合にユーザ アカウントをロックします。
- 管理者は、[System Administration] > [Users] ページを使用して、セキュリティ目的でユーザ アカウントを手動でロックできます。

[Edit User] ページでユーザ アカウントを確認すると、ユーザ アカウントがロックされている理由が AsyncOS によって表示されます。

図 8-12　ロックされているユーザ アカウント

ユーザ アカウントのロックを解除するには、[Users] 一覧でユーザ名をクリックしてユーザ アカウントを開き、[Unlock Account] をクリックします。

ローカル ユーザ アカウントを手動でロックするには、[Users] 一覧でユーザ名をクリックしてユーザ アカウントを開き、[Lock Account] をクリックします。AsyncOS から、ユーザがアプライアンスにログインできなくなるというメッセージが表示され、続行するかどうか尋ねられます。

ユーザが設定した試行回数を超えた後でログインに失敗した場合、すべてのローカル ユーザ アカウントをロックするように設定することもできます。詳細については、「制限的なユーザ アカウントとパスワードの設定値の設定」（P.8-30）を参照してください。

（注） admin アカウントをロックする場合、シリアル コンソール ポートへのシリアル通信接続を介して admin としてログインしてのみロックを解除できます。admin ユーザは、admin アカウントがロックされている場合でも、シリアル コンソール ポートを使用してアプライアンスにいつでもアクセスできます。シリアル コンソール ポートを使用したアプライアンスへのアクセスの詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Setup and Installation」の章を参照してください。

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　変更を保存します。

メッセージ トラッキング内の機密情報へのアクセスのディセーブル化

Data Loss Prevention（DLP）ポリシーに違反するメッセージには、一般的に企業の秘密情報、またはカード番号や健康の記録を含む個人情報などの機密情報が含まれています。デフォルトでは、この内容はメッセージ トラッキングの結果に一覧表示されるメッセージに対する [Message Details] ページの [DLP Matched Content] タブに表示されます。

メッセージ トラッキングにアクセスできる管理者以外のユーザに、このタブとその内容を表示しないように選択することもできます。管理者ユーザは常にこの内容を確認できます。

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　[System Administration] > [Users] ページに移動します。

ステップ 2　[DLP Tracking Privileges] で、[Edit Settings] をクリックします。

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、[Security Services] で以下の機能がイネーブルになっている必要があります。

- Message Tracking
- RSA Email DLP
- [RSA Email DLP] > [Matched Content Logging]

DLP ポリシーの詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Data Loss Prevention」の章を参照してください。

メッセージ トラッキング内の DLP 違反の検索の詳細については、「検索クエリーの実行」（P.3-7）を参照してください。

パスワードの変更

ユーザは GUI の上部にある [Options] > [Change Password] リンクを使用して自分のパスワードを変更できます。

古いパスワードを入力し、次に新しいパスワードを入力して確認のためにそのパスワードを再入力します。[Submit] をクリックします。ログアウトされ、画面にログが表示されます。

CLI で、password コマンドまたは passwd コマンドを使用してパスワードを変更します。admin ユーザ アカウントのパスワードを忘れた場合は、パスワードをリセットするためにカスタマー サポート プロバイダーにご連絡ください。

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ていたユーザを表示します。また、リモート ホストの IP アドレス、ログイン時間、ログアウト時間、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
```

制限的なユーザ アカウントとパスワードの設定値の設定

組織のパスワード ポリシーを実施するために、ユーザ アカウントとパスワードの制限を定義できます。ユーザ アカウントとパスワードの制限は、Cisco IronPort アプライアンスで定義されているローカル ユーザに適用されます。次の設定値を設定できます。

- **ユーザ アカウントのロック。**ユーザのアカウントがロックアウトされる失敗ログインの試行回数を定義できます。
- **パスワード存続期間のルール。**ログイン後にパスワードの変更が必要になるまでのパスワードの存続期間を定義できます。
- **パスワードのルール。**任意指定の文字や必須の文字など、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 アカウントとパスワードの制限は、[System Administration] > [Users] ページの [Local User Account and Password Settings] セクションで定義します。

Cloud ユーザ アカウント

Cloud ユーザ アカウントには、Cloud Administrator が変更できない事前設定済みのパスワード設定があります。Cloud ユーザには以下のパスワード設定が設定されています。

- ユーザは初回ログイン時にパスワードを変更する必要があります。
- ユーザは 6 か月ごとにパスワードを変更する必要があります。
- パスワードは最低 8 文字で指定し、大文字（A ～ Z）を 1 文字、小文字（a ～ z）を 1 文字、数値（1 ～ 9）を 1 文字、特殊文字（@#$% など）を 1 文字含める必要があります。

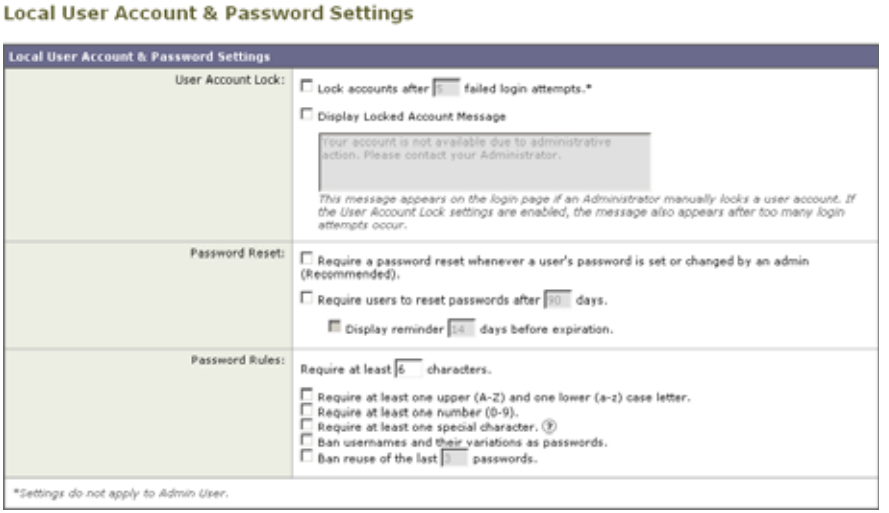
図 8-13 は、[Users] ページの [Local User Account and Password Settings] セクションを示しています。

図 8-13　[Users] ページ、[Local User Account and 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　[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 8-14　　ユーザ アカウントとパスワードの制限の設定



ステップ 2　表 8-3 で説明されている設定を設定します。

表 8-3　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	ユーザがログインに失敗した後でそのユーザ アカウントをロックするかどうかを選択します。アカウントをロックすることになる失敗ログイン試行の回数を指定します。1 から 60 までの任意の数を入力できます。デフォルトは 5 です。 アカウントのロックを設定する場合は、ログインを試みているユーザに表示するメッセージを入力します。テキストは 7 ビット ASCII 文字を使用して入力します。このメッセージは、ユーザがロックされているアカウントの正しいパスワードを入力した場合のみ表示されます。 ユーザ アカウントがロックされた場合、管理者は GUI で [Edit User] ページを使用するか、`userconfig` CLI コマンドを使用してロックを解除できます。 失敗したログインの試行は、ユーザが接続しているマシンや、接続のタイプ（SSH または HTTP など）に関係なく、ユーザ別に追跡されます。ユーザがログインに成功すると、失敗ログイン試行の回数は 0 にリセットされます。 失敗ログイン試行の最大回数に達したためにユーザ アカウントがロックアウトされると、管理者にアラートが送信されます。このアラートは、「Info」重大度レベルに設定されます。 **（注）** 個々のユーザ アカウントを手動でロックすることもできます。詳細については、「ユーザ アカウントのロックおよびロック解除」（P.8-25）を参照してください。

表 8-3　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した後で、ユーザにパスワードを強制的に変更させるかどうかを選択します。 パスワードが期限切れになった後で、ユーザにパスワードを強制的に変更させるかどうかを選択することもできます。ユーザがパスワードを変更するまでのパスワードの存続日数を入力します。1 から 366 までの任意の数を入力できます。デフォルトは 90 です。 期限切れ後にユーザにパスワードを強制的に変更させる場合は、次回のパスワード期限に関する通知を表示できます。ユーザに通知する期限切れ前の日数を選択します。 パスワードが期限切れになると、ユーザは次回ログイン時にアカウント パスワードを強制的に変更させられます。 **（注）** ユーザ アカウントがパスワード チャレンジの代わりに SSH キーを使用している場合でも、Password Reset ルールが適用されます。SSH キーを使用しているユーザ アカウントが期限切れになった場合、ユーザは古いパスワードを入力するか、アカウントに関連付けられているキーを変更するためにパスワードを手動で変更するように管理者に依頼する必要があります。詳細については、「セキュア シェル（SSH）キーの管理」（P.8-71）を参照してください。
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 から 128 までの任意の数を入力できます。デフォルトは 6 です。
Password Rules: Require at least one number (0-9).	パスワードに数字を少なくとも 1 文字含める必要があるかどうかを選択します。

表 8-3　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.	パスワードに特殊文字を少なくとも 1 文字含める必要があるかどうかを選択します。パスワードには次の特殊文字を含めることができます。 ~ ?!@ # $ % ^ & * - _ + = ¥ | / [ ] ( ) < > { } ` ' " ; : , .
Password Rules: Ban usernames and their variations as passwords.	関連付けられているユーザ名またはユーザ名のバリエーションと同じパスワードが認められるかどうかを選択します。ユーザ名のバリエーションが禁止されている場合、以下のルールがパスワードに適用されます。 • パスワードは、大文字と小文字の違いがあってもユーザ名とは同じにできません。 • パスワードは、大文字と小文字の違いがあってもユーザ名を反転したものとは同じにできません。 • パスワードは、以下の文字を置き換えた、ユーザ名または反転したユーザ名とは同じにできません。 – 「a」を「@」または「4」に置換 – 「e」を「3」に置換 – 「i」を「|」、「!」、または「1」に置換 – 「o」を「0」に置換 – 「s」を「$」または「5」に置換 – 「t」を「+」または「7」に置換
Password Rules: Ban reuse of the last <number> passwords.	パスワードを強制的に変更させられる場合に、ユーザに最近使用したパスワードの選択を認めるかどうかを選択します。最近のパスワードの再使用を認めない場合は、再使用を禁止する最近のパスワードの数を入力します。 1 から 15 までの任意の数を入力できます。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。

外部認証

ネットワークの LDAP または RADIUS ディレクトリにユーザ情報を保存する場合は、外部ディレクトリを使用してアプライアンスにログインするユーザを認証するよう Cisco IronPort アプライアンスを設定できます。認証のために外部ディレクトリを使用するようアプライアンスを設定するには、GUI で [System Administration] > [Users] ページを使用するか、CLI で `userconfig` コマンドと `external` サブコマンドを使用します。

外部認証がイネーブルであり、ユーザが電子メール セキュリティ アプライアンスにログインすると、アプライアンスは最初に、ユーザがシステム定義の「admin」アカウントであるかどうかを確認します。ユーザがシステム定義の「admin」アカウントでない場合、アプライアンスは最初に設定された外部サーバをチェックしてユーザがそこで定義されたかどうかを確認します。アプライアンスが最初の外部サーバに接続できなければ、アプライアンスは一覧の次の外部サーバをチェックします。

LDAP サーバの場合は、ユーザが外部サーバで認証に失敗すると、アプライアンスは電子メール セキュリティ アプライアンスで定義されたローカル ユーザとしてユーザを認証しようとします。そのユーザが外部サーバまたはアプライアンスに存在しない場合、またはユーザが間違ったパスワードを入力した場合は、アプライアンスへのアクセスが拒否されます。

外部 RADIUS サーバに接続できなければ、一覧の次のサーバが試行されます。すべてのサーバに接続できない場合、アプライアンスは電子メール セキュリティ アプライアンスで定義されたローカル ユーザとしてユーザを認証しようとします。ただし、外部 RADIUS サーバが何らかの理由（パスワード間違いやユーザ未登録など）でユーザを拒否すると、アプライアンスへのアクセスは拒否されます。

図 8-15　外部認証の確立

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 グループのユーザを Administrator ユーザ ロールに割り当てたり、Support グループのユーザを Help Desk User ロールに割り当てたりできます。1 人のユーザが複数の LDAP グループに属しており、それぞれユーザ ロールが異なる場合は、最も限定的なロールのアクセス許可が AsyncOS によってそのユーザに付与されます。たとえば、ユーザが Operator 権限を持つグループと Help Desk User 権限を持つグループに属する場合、AsyncOS はユーザに Help Desk User ロールの権限を割り当てます。

（注）　外部ユーザが LDAP 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。

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。詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「LDAP Queries」の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　[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 LDAP を選択します。

図 8-16　LDAP を使用した外部認証のイネーブル化

ステップ 4　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 5　ユーザを認証する LDAP 外部認証クエリーを選択します。

ステップ 6　タイムアウトするまでアプライアンスがサーバからの応答を待つ時間を秒単位で入力します。

ステップ 7　アプライアンスで認証する LDAP ディレクトリからのグループ名を入力し、グループのユーザに対するロールを選択します。

ステップ 8　また、[Add Row] をクリックして別のディレクトリ グループを追加することもできます。アプライアンスが認証する各ディレクトリ グループに対してステップ 7 とステップ 8 を繰り返します。

ステップ 9　変更を送信し、保存します。

RADIUS 認証のイネーブル化

ユーザを認証するために 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。

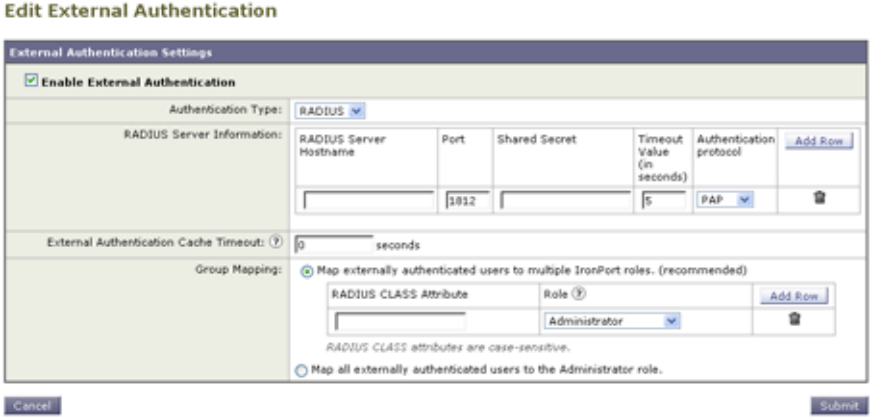
RADIUS を使用して外部認証をイネーブルにするには、次の手順を実行します。

ステップ 1　[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 8-17　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。

Cisco IronPort Cloud Email Security の管理

Cisco IronPort Cloud Email Security サービスを管理する場合、シスコのセキュリティ エキスパートによって実行される一定の管理タスク、およびユーザ組織のメンバーが実行できる管理タスクがあります。組織内の Cloud Email Security ユーザのニーズを満たすために、Cloud Email Security サービスには以下のクラウドベースのロールが含まれています。

表 8-4　Cloud ユーザ ロールの一覧

Cloud ユーザ ロール	説明
Cloud Administrator	Cloud Administrator ロールは、Cloud Email Security 用に作成された特別な管理者ロールです。Cloud 管理者のロールに固有の特定の管理タスクにアクセスできるように設計されています。このロールには、オンプレミスの Administrator と同じ多くの権限が付与されていますが、デバイスのシャットダウン、インストールの実行、またはデバイスのアップデートなど、Cloud Email Security サービスの適切な実行を妨げる可能性があるアクティビティは制限されています。 複数のユーザを Cloud Administrator ロールに割り当てることができます。デフォルトでは、プロビジョニング時に少なくとも 1 人のユーザがこのロールに割り当てられます。 （注）　Cloud Administrator は、CLI にアクセスできる唯一の Cloud ユーザです。他の Cloud ユーザは GUI にのみアクセスできます。 詳細については、「Cloud Administrator」（P.8-42）を参照してください。
Cloud Operator	Cloud Operator のユーザ アカウントには限定された管理権限があります。このユーザは、メール ポリシー、DLP ポリシー、レポート、メッセージ トラッキング、デバッグ トレース機能、およびスパム検疫とシステム検疫に対するすべてのアクセス権限を持ちます。 IronPort スパム検疫とシステム検疫へのアクセス権限は、このロールを持つユーザがそれらの検疫を管理する前にイネーブルにする必要があります。 詳細については、「Cloud Operator」（P.8-43）を参照してください。

表 8-4　Cloud ユーザ ロールの一覧（続き）

Cloud ユーザ ロール	説明
Cloud DLP Admin	その機能が DLP ポリシーを管理することである Cloud ユーザのユーザ アカウントです。このユーザは、DLP ポリシーの管理に対するすべてのアクセス権限を持ちます。 詳細については、「Cloud DLP Admin」（P.8-43）を参照してください。
Cloud Help Desk	Cloud Help Desk ユーザ用のユーザ アカウントです。このユーザは、メッセージ トラッキング、およびスパム検疫とシステム検疫に対するすべてのアクセス権限を持ちます。 IronPort スパム検疫とシステム検疫へのアクセス権限は、このロールを持つユーザがそれらの検疫を管理する前にイネーブルにする必要があります。 詳細については、「Cloud Help Desk」（P.8-44）を参照してください。
Cloud Guest	レポートを実行する、または IronPort スパム検疫およびシステム検疫にアクセスすることがある Cloud ゲスト用のユーザ アカウントです。このユーザは、レポーティングと検疫に対するすべてのアクセス権限を持ちます。 IronPort スパム検疫とシステム検疫へのアクセス権限は、このロールを持つユーザがそれらの検疫を管理する前にイネーブルにする必要があります。 詳細については、「Cloud Guest」（P.8-44）を参照してください。
カスタム ユーザ ロール	カスタム ユーザ ロールを持つユーザ アカウントはそのロールに割り当てられている電子メール セキュリティ機能にのみアクセスできます。アクセスできる機能は、DLP ポリシー、電子メール ポリシー、レポート、検疫、ローカル メッセージ トラッキング、暗号化プロファイル、およびトレース デバッグ ツールの任意の組み合わせになります。このユーザはシステム設定機能にはアクセスできません。カスタム ユーザ ロールを定義できるのは Cloud Administrator だけです。詳細については、「委任管理のためのカスタム ユーザ ロールの管理」（P.8-44）を参照してください。

Cloud Administrator

Cloud Administrator ロールは、組織のメンバーが Cloud Email Security サービスの一部の管理機能を実行できるように設計されていますが、シスコ電子メール セキュリティ エキスパートによって処理されるタスクを妨げないように管理権限は制限されています。

シスコ電子メール セキュリティ エキスパートは、ネットワーク インターフェイスの変更の実施、セキュリティ サービス アップデート設定の変更、デバイスの起動とシャットダウン、クラスタの管理、および設定のメンテナンスとアップデートに対する責任を負います。

Cloud Administrator ロールが付与されているユーザ アカウントは、以下の管理タスクを実行できます。

- Cloud Administrator ロールに属するユーザの作成または変更
- 権限が限定されているカスタム ユーザ ロールの作成および変更
- パスワードの作成およびリセット（パスワード ポリシーの変更はしない）
- ユーザ管理（新規ユーザの作成やアカウントのロックとロック解除など）
- レポートへのアクセスとレポートの実行、およびメッセージの追跡
- メール ポリシーとコンテンツ フィルタの作成
- DLP ポリシーの作成および変更
- トレース デバッグ ツールの実行
- 暗号化プロファイルの設定および変更
- システム検疫および IronPort スパム検疫へのアクセス
- セーフリスト/ブロックリスト ファイルの保存、変更、およびロード

Cloud Administrator ロールは、以下の選択された管理タスクのグループの実行は制限されています。

- ネットワーク インターフェイス設定（ルートと証明書を含む）の変更
- デバイスのシャットダウンおよび再起動
- デバイスへのソフトウェア アップグレードの適用
- クラスタリングのディセーブル、クラスタに対するデバイスの追加または削除
- Administrator の作成または削除

- セキュリティ サービス アップデート設定の変更
- コンフィギュレーション ファイルのロードまたはコンフィギュレーションのリセット
- 外部認証設定の変更
- スケジュール設定されたレポート設定の変更
- アラート設定の変更
- パスワード強度の設定などのパスワード アカウント ポリシーの変更
- システム設定ウィザードの実行

外部認証を使用している場合に、ユーザのグループが Cloud Administrator ロールにマップされている場合、ユーザは Cloud Administrator の権限に割り当てられます。

Cloud Operator

Cloud Operator ロールは、メール ポリシー、DLP ポリシー、レポート、メッセージ トラッキング、デバッグ トレース機能、およびスパム検疫とシステム検疫に対するすべてのアクセス権限を持ちます。

Operator ロールは Cloud Administrator ロールと同じ多くの権限を持つように設計されていますが、以下のアクティビティは制限されています。

- ユーザ アカウントの作成または編集。
- 一部検疫機能の実行（検疫の作成および削除を含む）。

Cloud DLP Admin

Cloud DLP Admin ロールは、RSA DLP ポリシーに対するすべてのアクセス権限をユーザに付与するように設計されています。このユーザは、アプライアンスのすべての DLP ポリシーに対するすべてのアクセス権限を持ちます（新規ポリシーの作成能力を含む）。DLP マネージャは DLP Policy Manager 内の DLP ポリシーの順序を変更することもできます。

データ消失防止の詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Data Loss Prevention」の章を参照してください。

Cloud Help Desk

Cloud Help Desk ロールは、エンドユーザをサポートするために、メッセージ トラッキング、およびスパム検疫とシステム検疫に対するすべてのアクセス権限をユーザに付与するように設計されています。Cloud Help Desk ユーザは、割り当てられた検疫に対するアクション（メッセージの解放または削除など）を表示および実行できますが、検疫のサイズ、保存期間などの検疫の設定は変更できません。また、検疫の作成や削除もできません。

Cloud Guest

このアカウントは、情報を追跡したいが、必ずしもインフラストラクチャの設定を変更する必要はないユーザ向けに設計されています。Cloud Guest アカウントは、レポーティング、およびシステム検疫とスパム検疫に対するすべてのアクセス権限を持ちます。Cloud Guest ユーザは、割り当てられた検疫に対するアクション（メッセージの解放または削除など）を表示および実行できますが、検疫のサイズ、保存期間などの検疫の設定は変更できません。また、検疫の作成や削除もできません。

IronPort スパム検疫とシステム検疫へのアクセス権限は、このロールを持つユーザがそれらの検疫を管理する前にイネーブルにする必要があります。

委任管理のためのカスタム ユーザ ロールの管理

カスタム ユーザ ロールを設計し、組織内でのそれぞれのロールに一致した特定の責任をユーザに委任することができます。*委任管理者*は、それぞれが責任を負う電子メール セキュリティ機能にのみアクセスでき、それぞれのロールに関連しないシステム設定機能にはアクセスできません。委任管理を行うことで、アプライアンスの電子メール セキュリティ機能に対するユーザのアクセスを、定義済みの Administrator、Operator、および Help Desk User ロールより柔軟に制御できるようになります。

たとえば、電子メール セキュリティ アプライアンスの特定ドメインの電子メール ポリシーの管理に関与しているユーザがいる場合に、それらのユーザに、定義済みの Administrator および Operator ロールで付与されるシステム管理やセキュリティ サービスの設定機能にはアクセスさせたくないことがあります。それぞれのユーザに管理するメール ポリシーへのアクセス権限、およびそれらの

ポリシーで処理されるメッセージを管理するために使用できる他の電子メール セキュリティ機能（メッセージ トラッキングやポリシー検疫など）を付与できるメール ポリシー管理者用のカスタム ユーザ ロールを作成できます。

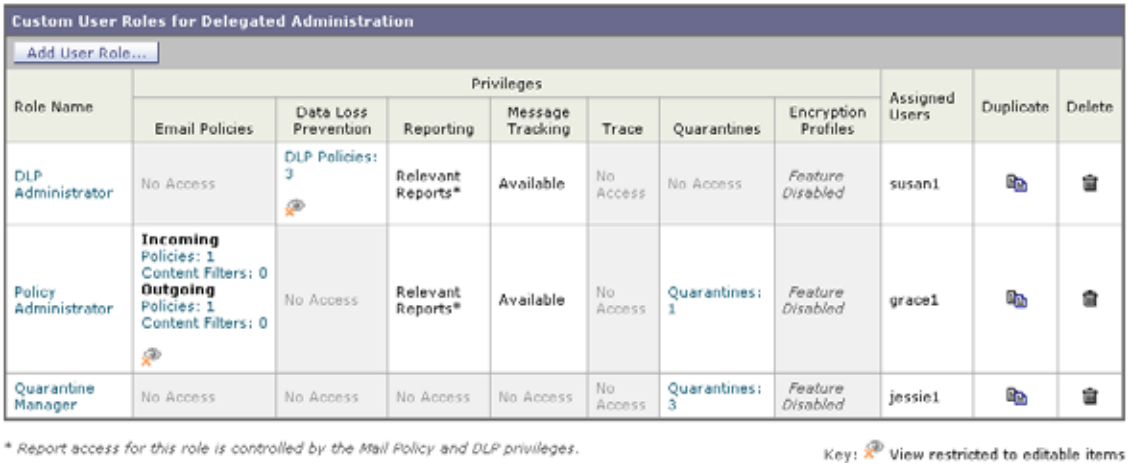
GUI で [System Administration] > [User Roles] ページを使用して（または、CLI で `userconfig -> role` コマンドを使用して）、カスタム ユーザ ロールを定義し、それぞれが責任を負う電子メール セキュリティ機能（メール ポリシー、RSA Email DLP ポリシー、電子メール レポート、および検疫など）を管理します。委任管理者が管理できる電子メール セキュリティ機能の一覧については、「アクセス権限の割り当て」（P.8-47）を参照してください。カスタム ロールは、[System Administration] > [Users] ページを使用して、ローカル ユーザ アカウントを追加または編集するときにも作成できます。詳細については、「ユーザ アカウント追加時のカスタム ユーザ ロールの定義」（P.8-55）を参照してください。

カスタム ユーザ ロールを作成する際には、そのロールの責任が他の委任管理者の責任と重複しすぎないようにする必要があります。たとえば、複数の委任管理者が同じコンテンツ フィルタに対する責任を持ち、そのコンテンツ フィルタを異なるメール ポリシーで使用する場合、1 人の委任管理者がそのフィルタに加えた変更により、他の委任管理者が管理しているメール ポリシーに意図せぬ悪影響を及ぼすことがあります。

カスタム ユーザ ロールを作成すると、他のユーザ ロールと同様にローカル ユーザと外部認証グループをそのカスタム ユーザ ロールに割り当てることができます。詳細については、「ユーザ アカウントを使用する作業」（P.8-18）を参照してください。カスタム ロールに割り当てられているユーザは CLI にアクセスできないことに注意してください。

図 8-18 は、電子メール セキュリティ アプライアンスに定義されているカスタム ユーザ ロールの一覧と各ロールに割り当てられているアクセス権限を示しています。

図 8-18　カスタム ユーザ ロールの一覧



[Account Privileges] ページ

委任管理者がアプライアンスにログインすると、[Account Privileges] ページに委任管理者が責任を持つセキュリティ機能へのリンク、およびそれぞれのアクセス権限についての簡単な説明が表示されます。委任管理者は、[Options] メニューで [Account Privileges] を選択することでこのページに戻ることができます。委任管理者は、Web ページの上部にあるメニューを使用して、管理する機能にアクセスすることもできます。

図 8-19 は、メール ポリシー、電子メール レポーティング、メッセージ トラッキング、および検疫にアクセスできる委任管理者の [Account Privileges] ページを示しています。

図 8-19　委任管理者の [Account Privileges] ページ

アクセス権限の割り当て

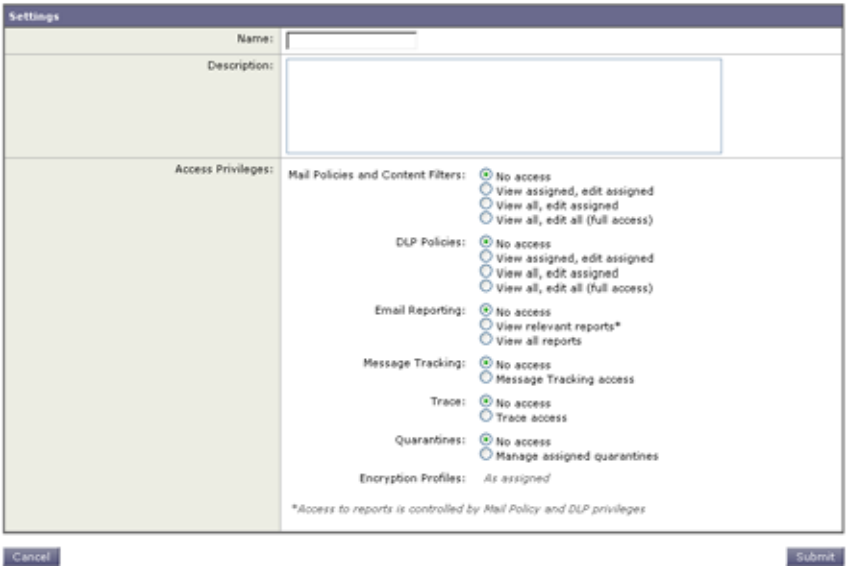
カスタム ユーザ ロールを作成する場合、委任管理者が責任を負うセキュリティ機能へのアクセス レベルを定義します。

委任管理者が管理できるセキュリティ機能は以下のとおりです。

- 送受信のメール ポリシーとコンテンツ フィルタ。
- データ消失防止（DLP）ポリシー。
- 電子メール レポーティング。
- メッセージ トラッキング。
- トレース デバッグ ツール。
- スパム、ポリシー、ウイルス、および Outbreak 検疫。
- Cisco IronPort 電子メール暗号化プロファイル。

図 8-20 は、カスタム ユーザ ロールの作成時に各機能で使用可能なさまざまなアクセス権限を示しています。

図 8-20　カスタム ユーザ ロールで使用可能なアクセス権限



カスタム ユーザ ロールのアクセス レベルを定義したら、委任管理者が責任を負うことになる具体的なメール ポリシー、コンテンツ フィルタ、DLP ポリシー、検疫、または暗号化プロファイルを割り当てる必要があります。

たとえば、異なる RSA Email DLP ポリシーに対して責任を負う 2 つの異なる DLP ポリシー管理者ロールを作成できます。1 つのロールは企業の秘密保持や許容範囲での使用に関する DLP 違反にのみ責任を負い、他のロールはプライバシー保護に関する DLP 違反に責任を負うようにできます。DLP ポリシーへのアクセスに加えて、これらのカスタム ユーザ ロールにはメッセージ データのトラッキング、検疫とレポートの表示に対する権限を割り当てることもできます。それらのロールは、メッセージ トラッキングの使用において責任を負うポリシーに関連する DLP 違反を検索できます。

カスタム ユーザ ロールに割り当てることができる責任については、[User Roles] ページの [Custom User Roles for Delegated Administration] テーブル内の割り当て済み権限のリンクをクリックして確認できます。「カスタム ユーザ ロールの責任のアップデート」（P.8-56）を参照してください。

メール ポリシーとコンテンツ フィルタ

メール ポリシーとコンテンツ フィルタのアクセス権限では、電子メール セキュリティ アプライアンスの送受信メール ポリシーとコンテンツ フィルタへの委任管理者のアクセス レベルを定義します。特定のメール ポリシーとコンテンツ フィルタをカスタム ユーザ ロールに割り当て、そのロールに属する委任管理者、および Operator と Administrator だけがメール ポリシーとコンテンツ フィルタを管理できるようにすることができます。

このアクセス権限を持つすべての委任管理者は、デフォルトの送受信メール ポリシーを表示できますが、すべてのアクセス権限を持っている場合のみそれらのポリシーを編集できます。

アクセス権限を持つすべての委任管理者は、それぞれのメール ポリシーで使用する新しいコンテンツ フィルタを作成できます。委任管理者が作成したコンテンツ フィルタは、そのカスタム ユーザ ロールに割り当てられているの他の委任管理者が使用できます。いずれのカスタム ユーザ ロールにも割り当てられていないコンテンツ フィルタはパブリックであり、メール ポリシーのアクセス権限を持つすべての委任管理者が表示できます。Operator や Administrator が作成したコンテンツ フィルタは、デフォルトで*パブリック*です。委任管理者は、それぞれのカスタム ユーザ ロールに割り当てられているメール ポリシーの既存のコンテンツ フィルタはすべてイネーブルまたはディセーブルにできますが、パブリック コンテンツ フィルタは変更も削除もできません。

委任管理者が自分のポリシー以外のメール ポリシーで使用されているコンテンツ フィルタを削除した場合、またはそのコンテンツ フィルタが他のカスタム ユーザ ロールに割り当てられている場合、AsyncOS はそのコンテンツ フィルタをシステムから削除しません。代わりに、AsyncOS はそのカスタム ユーザ ロールからコンテンツ フィルタのリンクを解除し、委任管理者のメール ポリシーから削除します。そのコンテンツ フィルタは、他のカスタム ユーザ ロールとメール ポリシーでは引き続き使用可能です。

委任管理者は、それぞれのコンテンツ フィルタで任意のテキスト リソースやディクショナリを使用できますが、GUI で [Text Resources] ページや [Dictionaries] ページにアクセスして、それらを表示または変更することはできません。委任管理者は、新しいテキスト リソースやディクショナリを作成することもできません。

送信メール ポリシーの場合、委任管理者は DLP ポリシーをイネーブルまたはディセーブルできますが、DLP ポリシーの権限も持っている場合を除き、DLP の設定をカスタマイズすることはできません。

メール ポリシーとコンテンツ フィルタ用の以下のアクセス レベルのいずれかをカスタム ユーザ ロールに割り当てることができます。

- **No access**：委任管理者は電子メール セキュリティ アプライアンスのメール ポリシーとコンテンツ フィルタを表示も編集もできません。
- **View assigned, edit assigned**：委任管理者はカスタム ユーザ ロールに割り当てられているメール ポリシーとコンテンツ フィルタを表示および編集でき、新しいコンテンツ フィルタを作成できます。委任管理者は、ポリシーのアンチスパム、アンチウイルス、および Outbreak フィルタの設定を編集できます。委任管理者はポリシーに対してそれぞれのコンテンツ フィルタをイネーブルにでき、責任があるものかどうかに関係なく、そのポリシーに割り当てられている既存のコンテンツ フィルタをディセーブルにできます。委任管理者はメール ポリシーの名前、その送信者、受信者、またはグループを変更することはできません。委任管理者は、それぞれのカスタム ユーザ ロールに割り当てられているメール ポリシーのコンテンツ フィルタの順序を変更できます。
- **View all, edit assigned**：委任管理者は、アプライアンスのすべてのメール ポリシーとコンテンツ フィルタを表示できますが、そのカスタム ユーザ ロールに割り当てられているもののみ編集できます。
- **View all, edit all (full access)**：委任管理者は、アプライアンスのすべてのメール ポリシーとコンテンツ フィルタ（デフォルトのメール ポリシーを含む）に対するすべてのアクセス権限を持ち、新しいメール ポリシーを作成できます。委任管理者は、すべてのメール ポリシーの送信者、受信者、およびグループを変更できます。メール ポリシーの順序を変更することもできます。

[User Roles] ページの [Email Security Manager] または [Custom User Roles for Delegated Administration] テーブルを使用して、個々のメール ポリシーとコンテンツ フィルタをカスタム ユーザ ロールに割り当てることができます。

メール ポリシーとコンテンツ フィルタに対する Email Security Manager の使用方法の詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Email Security Manager」の章を参照してください。

[Custom User Roles for Delegated Administration] テーブルを使用したメール ポリシーとコンテンツ フィルタの割り当ての詳細については、「カスタム ユーザ ロールの責任のアップデート」（P.8-56）を参照してください。

DLP ポリシー

DLP ポリシーのアクセス権限では、電子メール セキュリティ アプライアンスの DLP Policy Manager を介した RSA Email DLP ポリシーへの委任管理者のアクセス レベルを定義します。RSA Email DLP ポリシーを特定のカスタム ユーザ ロールに割り当て、Operator と Administrator に加えて、委任管理者にそれらのポリシーを管理させることができます。

委任管理者がメール ポリシー権限も保持している場合は、RSA Email DLP ポリシーをカスタマイズできます。委任管理者は、それぞれの RSA Email DLP ポリシーの任意のカスタム DLP ディクショナリを使用できますが、カスタム DLP ディクショナリは表示も変更もできません。

RSA Email DLP ポリシー用の以下のアクセス レベルのいずれかをカスタム ユーザ ロールに割り当てることができます。

- **No access**：委任管理者は電子メール セキュリティ アプライアンスの RSA Email DLP ポリシーを表示も編集もできません。
- **View assigned, edit assigned**：委任管理者は DLP Policy Manager を使用して、カスタム ユーザ ロールに割り当てられている DLP Policy Manager ポリシーを表示および編集できます。委任管理者は、DLP Policy Manager 内の DLP ポリシーの名前変更も順序変更もできません。
- **View all, edit assigned**：委任管理者はカスタム ユーザ ロールに割り当てられている RSA Email DLP ポリシーを表示および編集できます。委任管理者は、そのカスタム ユーザ ロールに割り当てられていない RSA Email DLP ポリシーをすべて表示できますが、編集することはできません。委任管理者は、DLP Policy Manager 内の DLP ポリシーの順序変更やポリシー名の変更はできません。
- **View all, edit all (full access)**：委任管理者は、アプライアンスのすべての RSA Email DLP ポリシーに対するすべてのアクセス権限を持ち、新しいポリシーを作成することもできます。委任管理者は、DLP Policy Manager 内の DLP ポリシーの順序を変更できます。

[User Roles] ページの [DLP Policy Manager] または [Custom User Roles for Delegated Administration] テーブルを使用して、個々の RSA Email DLP ポリシーをカスタム ユーザ ロールに割り当てることができます。

RSA Email DLP ポリシーと DLP Policy Manager の詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Data Loss Prevention」を参照してください。

[Custom User Roles for Delegated Administration] の一覧を使用して RSA Email DLP ポリシーを割り当てる方法の詳細については、「カスタム ユーザ ロールの責任のアップデート」（P.8-56）を参照してください。

電子メール レポーティング

電子メール レポーティングのアクセス権限では、カスタム ユーザ ロールのメール ポリシー、コンテンツ フィルタ、および RSA Email DLP ポリシーへのアクセス権限に従い、委任管理者が表示できるレポートと [Email Security Monitor] ページを定義します。それらのレポートは割り当てられているポリシーに対してフィルタリングされていません。委任管理者は、自分が責任を負っていないメールと DLP ポリシーのレポートを表示できます。

電子メール レポーティング用の以下のアクセス レベルのいずれかをカスタム ユーザ ロールに割り当てることができます。

- **No access**：委任管理者は、電子メール セキュリティ アプライアンスのレポートを表示できません。
- **View relevant reports**：委任管理者は、[Email Security Monitor] ページにあるそれぞれのメール ポリシー、コンテンツ フィルタ、および DLP ポリシーのアクセス権限に関連するレポートを表示できます。メール ポリシーとコンテンツ フィルタのアクセス権限がある委任管理者は、以下の [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 Outbreaks
  - Virus Types
  - Archived Reports

  DLP ポリシーのアクセス権限がある委任管理者は、以下の [Email Security Monitor] ページを表示できます。
  - Overview

  - DLP Incidents
  - Archived Reports

- **View all reports**：委任管理者は、電子メール セキュリティ アプライアンスのすべてのレポートと [Email Security Monitor] ページを表示できます。

電子メール レポーティングと [Email Security Monitor] の詳細については、第 2 章「電子メール セキュリティ モニタの使用方法」（P.1）の章を参照してください。

メッセージ トラッキング

メッセージ トラッキングのアクセス権限では、カスタム ユーザ ロールに割り当てられている委任管理者がメッセージ トラッキングへのアクセス権限を持つかどうかを定義します。メッセージ トラッキングには、[System Administration] > [Users] ページで [DLP Tracking Policies] オプションがイネーブルになっていて、カスタム ユーザ ロールに DLP ポリシーのアクセス権限もある場合に、組織の DLP ポリシー違反となる可能性があるメッセージの内容も含まれます。

委任管理者はそれぞれに割り当てられている RSA Email DLP ポリシーに対する DLP 違反のみ検索できます。

メッセージ トラッキングの詳細については、第 3 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。

委任管理者に、メッセージ トラッキング内の一致した DLP の内容を表示するためのアクセスを許可する方法の詳細については、「メッセージ トラッキング内の機密情報へのアクセスのディセーブル化」（P.8-27）を参照してください。

トレース

トレースのアクセス権限では、カスタム ユーザ ロールに割り当てられている委任管理者がトレースを使用して、システムを介したメッセージ フローをデバッグできるかどうかを定義します。アクセス権限がある委任管理者は、トレースを実行して、生成されるすべての出力を表示できます。トレース結果は、委任管理者のメールまたは DLP ポリシー権限に基づきフィルタリングはされません。

トレースの使用方法の詳細については、「テスト メッセージを使用したメール フローのデバッグ：トレース」（P.9-2）を参照してください。

検疫

検疫のアクセス権限では、委任管理者が割り当てられた検疫を管理できるかどうかを定義します。委任管理者は、割り当てられた検疫内の任意のメッセージを表示して、メッセージの解放や削除などのアクションを実行できますが、検疫の設定（サイズ、保存期間など）の変更、検疫の作成や削除はできません。

[Monitor] > [Quarantines] ページまたは [User Roles] ページの [Custom User Roles for Delegated Administration] テーブルを使用して、任意の検疫をカスタム ユーザ ロールに割り当てることができます。

検疫の詳細については、第 4 章「検疫」（P.1）を参照してください。

[Custom User Roles for Delegated Administration] 一覧を使用して検疫を割り当てる方法の詳細については、「カスタム ユーザ ロールの責任のアップデート」（P.8-56）を参照してください。

暗号化プロファイル

暗号化プロファイルのアクセス権限では、委任管理者がコンテンツ フィルタまたは DLP ポリシーの編集時に、それぞれのカスタム ユーザ ロールに割り当てられている暗号化プロファイルを使用できるかどうかを定義します。暗号化プロファイルは、メールまたは DLP ポリシーのアクセス権限があるカスタム ユーザ ロールにのみ割り当てることができます。カスタム ロールに割り当てられていない暗号化プロファイルは、メールまたは DLP ポリシーの権限を持つすべての委任管理者が使用可能です。委任管理者はいずれの暗号化プロファイルも表示または変更できません。

暗号化プロファイルは、[Security Services] > [IronPort Email Encryption] ページを使用して暗号化プロファイルを作成または編集するときに割り当てることができます。

詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Cisco IronPort Email Encryption」の章を参照してください。

カスタム ユーザ ロールの定義

GUI で [User Roles] ページを使用して（または CLI で `userconfig -> role` コマンドを使用して）、新しいユーザ ロールを定義し、そのロールのアクセス権限を割り当てます。[User Roles] ページには、アプライアンスの既存のすべてのカスタム ユーザ ロールと各ロールのアクセス権限が表示されます。

[User Roles] ページを使用してカスタム 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　[System Administration] > [User Roles] ページに移動します。

ステップ 2　[Add User Role] をクリックします。[Add User Role] ページが表示されます。

ステップ 3　ユーザ ロールの名前を入力します。

ステップ 4　ユーザ ロールの説明とその権限を入力します。

ステップ 5　ユーザ ロールのアクセス権限を選択します。（各タイプのアクセス権限の詳細については、「アクセス権限の割り当て」（P.8-47）を参照してください）。

ステップ 6　変更を送信し、保存します。

ユーザ アカウント追加時のカスタム ユーザ ロールの定義

電子メール セキュリティ アプライアンスに対してローカル ユーザ アカウントの追加または編集を行う際に、新しいカスタム ユーザ ロールを作成できます。図 8-21 は、[Add Local User] ページでカスタム ユーザ ロールを追加するときに使用可能なオプションを示しています。

図 8-21　ユーザ アカウント追加時のカスタム ロール追加用のオプション

ユーザ アカウントの追加の詳細については、「ユーザの管理」（P.8-22）を参照してください。

ユーザ アカウント作成時にカスタム 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　[System Administration] > [Users] ページに移動します。

ステップ 2　[Add User] をクリックします。

ステップ 3　ユーザ アカウント作成時には、[Custom Roles] を選択します。

ステップ 4　[Add Role] を選択します。

ステップ 5　新しいロールの名前を入力します。

ステップ 6　新しいユーザ アカウントを送信します。

AsyncOS により、新しいユーザ アカウントとカスタム ユーザ ロールが追加されたという通知が表示されます。

ステップ 7　[System Administration] > [User Roles] ページに移動します。

ステップ 8　[Custom User Roles for Delegated Administration] テーブルでカスタム ユーザ ロールの名前をクリックします。[Edit User Role] ページが表示されます。

ステップ 9　ユーザ ロールの説明とその権限を入力します。

ステップ 10　ユーザ ロールのアクセス権限を選択します。（各タイプのアクセス権限の詳細については、「アクセス権限の割り当て」（P.8-47）を参照してください）。

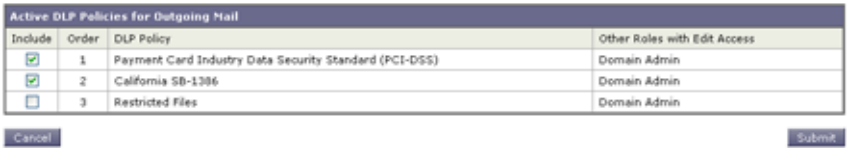
ステップ 11　変更を送信し、保存します。

カスタム ユーザ ロールの責任のアップデート

GUI の上部にあるメニューを使用して個々のセキュリティ機能をブラウズしてカスタム ユーザ ロールに責任を割り当てることができる一方、[User Roles] ページの [Custom User Roles for Delegated Administration] テーブルでは、委任管理者が 1 つの場所で管理できるすべてのセキュリティ機能（暗号化プロファイルを除く）へのリンクを統合できます。テーブルでカスタム ユーザ グループのアクセス権限の名前をクリックすると、アプライアンスのすべてのメール ポリシー、コンテンツ フィルタ、アクティブな RSA Email DLP ポリシー、または検疫の一覧が表示され、それらにアクセスできるその他すべてのカスタム ユーザ ロールの名前が表示されます。

たとえば、図 8-22 は、電子メール セキュリティ アプライアンスで使用可能なアクティブな RSA Email DLP ポリシーの一覧を示しています。また、DLP ポリシーへのアクセス権限がある他のカスタム ユーザ グループも表示されています。この一覧から、管理者は、委任管理者が DLP Policy Manager で使用する DLP ポリシーを選択できます。

図 8-22　委任管理者が使用可能な DLP ポリシー



カスタム ユーザ ロールの責任をアップデートするには、次の手順を実行します。

ステップ 1　[System Administration] > [User Roles] ページに移動します。

ステップ 2　アップデートするカスタム ユーザ ロールのアクセス権限の名前をクリックします。

AsyncOS により、アプライアンスで使用可能なすべてのメール ポリシー、コンテンツ フィルタ、DLP ポリシー、または検疫の一覧、およびその他すべての割り当て済みカスタム ユーザ ロールの名前が表示されます。

ステップ 3　委任管理者に責任を割り当てるメール ポリシー、コンテンツ フィルタ、DLP ポリシー、または検疫を選択します。

ステップ 4　変更を送信し、保存します。

カスタム ユーザ ロールの編集

カスタム ユーザ ロールを編集（アクセス権限を含む）には、次の手順を実行します。

ステップ 1　[System Administration] > [User Roles] ページに移動します。

ステップ 2　[Custom User Roles for Delegated Administration] 一覧でユーザ ロールの名前をクリックします。

[Edit User Role] ページが表示されます。

ステップ 3　ユーザ ロールに変更を加えます。

ステップ 4　変更を送信し、保存します。

カスタム ユーザ ロールの複製

同様のアクセス権限がある複数のカスタム ユーザ ロールを作成し、異なるユーザのセットに異なる責任を割り当てたいことがあります。たとえば、電子メール セキュリティ アプライアンスが複数ドメインのメッセージを処理する場合、同様のアクセス権限だが、ドメインに基づく異なるメール ポリシーに対する権限であるカスタム ユーザ ロールを作成することができます。こうすることで、委任管理者は、他の委任管理者の責任を妨げることなくそれぞれのドメインのメール ポリシーを管理できます。

カスタム ユーザ ロールを複製するには、次の手順を実行します。

ステップ 1　[System Administration] > [User Roles] ページに移動します。

ステップ 2　[Custom User Roles for Delegated Administration] 一覧で、複製するユーザ ロールに対応する複製アイコンをクリックします。

すでに割り当て済みのアクセス権限が表示されている [Add User Role] ページが表示されます。

ステップ 3　カスタム ユーザ ロールの名前を変更します。

ステップ 4　新しいカスタム ユーザ ロールに必要なすべてのアクセス権限の変更を行います。

ステップ 5　変更を送信し、保存します。

カスタム ユーザ ロールの削除

カスタム ロールが削除されると、ユーザは未割り当て状態になり、アプライアンスにアクセスできなくなります。削除したカスタム ユーザ ロールに割り当てられていたすべてのユーザを再割り当てする必要があります。

カスタム ユーザ ロールを削除するには、次の手順を実行します。

ステップ 1　[System Administration] > [User Roles] ページに移動します。

ステップ 2　[Custom User Roles for Delegated Administration] 一覧で、削除するユーザ ロールに対応するゴミ箱のアイコンをクリックします。[Add User Role] ページが表示されます。

ステップ 3　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 4　変更を保存します。

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すべての設定は、1 つのコンフィギュレーション ファイルで管理できます。このファイルは Extensible Markup Language（XML）形式で保持されます。

このファイルは次の複数の方法で使用できます。

- 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を誤った場合は、保存され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（多くの新しいブラウザは XML ファイルを直接レンダリングできます）。これにより、現在の設定に存在する可能性がある小さなエラー（タイピング エラーなど）のトラブルシューティングを行えるようになります。
- 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、変更を行い、そのファイルを同じアプライアンスにアップロードできます。この場合は、実質的に設定の変更を行うために CLI と GUI の両方が「バイパス」されます。
- FTP アクセスを使用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 ファイルの一部または全体を CLI に貼り付けたりできます。
- ファイルは XML 形式であるため、コンフィギュレーション ファイルのすべての XML エンティティを定義する、関連付けられた Document Type Definition（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

- 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を簡単に管理できるようになります。現時点では、コンフィギュレーション ファイルを C/X-Series アプライアンスから M-Series アプライアンスにロードできません。
- ある Cisco IronPort 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

GUI を使用して Cisco IronPort アプライアンスのコンフィギュレーション ファイルを管理するには、[System Administration] タブの [Configuration File] リンクをクリックします。

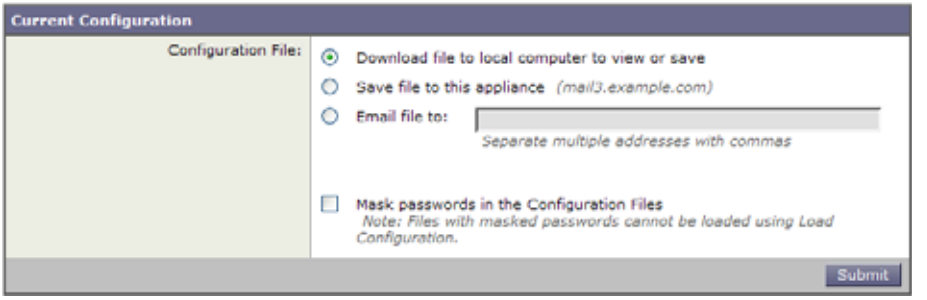
[Configuration File] ページには次の 3 つのセクションがあります。

- [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。
- [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

[System Administration] > [Configuration File] ページの [Current Configuration] の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 8-23　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クリックすることにより、ユーザのパスワードをマスクできます。パスワードをマスクすると、元の暗号化されたパスワードが、エクスポートまたは保存されたファイルで「*****」に置き換えられます。ただし、パスワードがマスクされたコンフィギュレーション ファイルを AsyncOS に再びロードすることはできないことに注意してください。

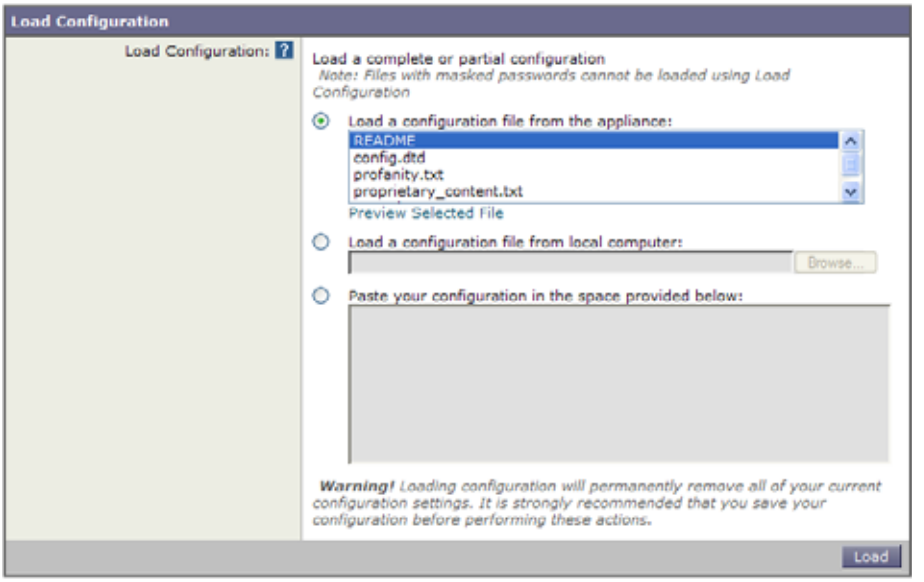
コンフィギュレーション ファイルのロード

[System Administration] > [Configuration File] ページの [Load Configuration] のセクションを使用して新しい設定情報を Cisco IronPort アプライアンスにロードします。情報は次の 3 つのいずれかの方法でロードできます。

- `configuration` ディレクトリに情報を格納し、アップロードする。
- コンフィギュレーション ファイルをローカル マシンから直接アップロードする。
- GUI に設定情報を直接貼り付ける。

パスワードがマスクされたコンフィギュレーション ファイルはロードできません。

図 8-24　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（Document Type Definition）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、次の内容をアップロードまたは解析します。

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE config SYSTEM "config.dtd">

<config>

  <autosupport_enabled>0</autosu

</config>
```

この場合は、アップロード中に検証エラーが発生します。ただし、

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE config SYSTEM "config.dtd">

<config>

  <autosupport_enabled>0</autosupport_enabled>

</config>
```

この場合は、検証エラーが発生しません。

「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つことができないため、次の内容（宣言と <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>
```

ただし、システムでは複数のリスナーを定義できるため（リスナーごとに異なる受信者アクセス テーブルが定義されます）、

```
<rat>
   <rat_entry>
     <rat_address>ALL</rat_address>
     <access>RELAY</access>
   </rat_entry>
 </rat>
```

上記の内容だけをアップロードすることは多義的と見なされ、「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解析する場合は、待機中の可能性がある、保存されていない変更が破棄されることがあります。

空白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解析す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、

```
<listeners></listeners>
```

上記の内容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。

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 ファイルをアップロードする前に、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ることに注意してください。

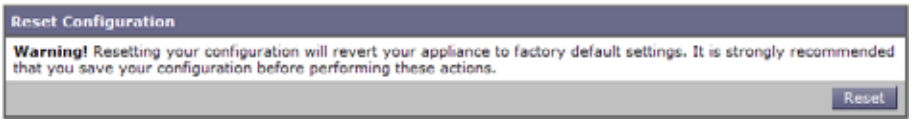
```
<?xml version="1.0" encoding="ISO-8859-1"?>
```

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する必要があります。GUI でこのボタンを使用して設定をリセットすることは、クラスタリング環境ではサポートされていません。

図 8-25　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.8-5）を参照してください。

コンフィギュレーション ファイル用の CLI コマンド

次のコマンドを使用すると、コンフィギュレーション ファイルを操作できます。

- `showconfig`
- `mailconfig`
- `saveconfig`
- `loadconfig`
- `resetconfig`（「出荷時デフォルト値へのリセット」（P.8-5）を参照）

showconfig、mailconfig、および saveconfig コマンド

コンフィギュレーション コマンドの `showconfig`、`mailconfig`、および `saveconfig` の場合は、電子メールで送信されるファイルまたは表示されるファイルにパスワードを含めるかどうか選択することを求められます。パスワードを含めないことを選択すると、パスワード フィールドが空白のままになります。セキュリティの問題を心配する場合は、パスワードを含めないことを選択できます。ただし、`loadconfig` コマンドを使用してロードされた場合、パスワードがないコンフィギュレーション ファイルは失敗します。「ログ サブスクリプションのパスワードのロードについての注意事項」（P.8-65）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ない PEM 形式で含められます。

Showconfig コマンドは現在の設定を画面に出力します。

```
mail3.example.com> showconfig



Do you want to include passwords? Please be aware that a
configuration without passwords will fail when reloaded with
loadconfig.



<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE config SYSTEM "config.dtd">



<!--

  Product: 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.
```

Saveconfig コマンドは、一意のファイル名を使用してコンフィギュレーション ファイルを configuration ディレクトリに保存します。

```
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 C60-00065B8FCEAB-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 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.8-61）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「Accessing the Appliance」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+D を押すと貼り付けコマンドが終了します）。次に、システム設定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、およびデフォルトのゲートウェイ情報を変更します（詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Setup and Installation」を参照してください）。最後に、変更を保存します。

```
mail3.example.com> loadconfig



1. Paste via CLI

2. Load from file

[1]> 1



Paste the configuration file now. Press CTRL-D on a blank line when
done.



[The configuration file is pasted until the end tag </config>.
Control-D is entered on a separate line.]



Values have been loaded.

Be sure to run "commit" to make these settings active.

mail3.example.com> systemsetup
```

```
[The system setup wizard is run.]

mail3.example.com> commit

Please enter some comments describing your changes:
[]> pasted new configuration file and changed default settings via
systemsetup
```

セキュア シェル（SSH）キーの管理

Cloud Email Security アプライアンスに対する SSH キーの追加や削除は行わないことを推奨します。

sshconfig コマンドを使用すると、システムで設定されたユーザ アカウント（admin アカウントを含む）の authorized_keys ファイルに Secure Shell（SSH; セキュア シェル）公開ユーザ キーを追加したり、それらのキーを削除したりできます。これにより、パスワード チャレンジではなく SSH キーを使用してユーザ アカウントを認証できるようになります。RSA ベース認証と DSA キー タイプを持つ SSH プロトコル バージョン 1（SSH1）と SSH プロトコル バージョン 2（SSH2）の両方がサポートされます。SSH1 は setup サブコマンドを使用してディセーブルにできます。

（注）　Cisco IronPort アプライアンスから他のホスト マシンへのログ ファイルの SCP プッシュを実行する場合に使用されるホスト キーを設定するには、logconfig -> hostkeyconfig を使用します。詳細については、第 5 章「ロギング」を参照してください。

hostkeyconfig を使用すると、リモート ホストのキーをスキャンし、Cisco IronPort アプライアンスに追加できます。

（注）　CLI に新しいキーを直接貼り付ける場合は、空白行で Enter または Return を押してキーの入力を終了します。

次の例では、admin アカウントに対して新しい公開キーがインストールされます。

```
mail3.example.com> sshconfig


Currently installed keys for admin:


Choose the operation you want to perform:

- NEW - Add a new key.

- USER - Switch to a different user to edit.

- SETUP -  Configure general settings.

[]> new


Please enter the public SSH key for authorization.

Press enter on a blank line to finish.


[cut and paste public key for user authentication here]


Currently installed keys for admin:

1. ssh-dss AAAAB3NzaC1kc3MAA...CapRrgxcY= (admin@example.com)
```

```
Choose the operation you want to perform:

- NEW - Add a new key.

- EDIT - Modify a key.

- DELETE - Remove a key.

- PRINT - Display a key.

[]>
```

SSH1 のディセーブル化

SSH1 をディセーブル（またはイネーブル）にするには、sshconfig コマンドの setup サブコマンドを使用します。

```
mail3.example.com> sshconfig


Currently installed keys for admin:


Choose the operation you want to perform:

- NEW - Add a new key.

- USER - Switch to a different user to edit.

- SETUP -  Configure general settings.

[]> setup



Choose the operation you want to perform:
```

```
- DISABLE - Disable SSH v1

[]> disable


Currently installed keys for admin:


Choose the operation you want to perform:

- NEW - Add a new key.

- USER - Switch to a different user to edit.

- SETUP - Configure general settings

[]>


mail3.example.com> commit
```

リモート SSH コマンド実行

CLI では、リモート SSH コマンド実行を使用してコマンドを実行できます。コマンドの一覧については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の付録 A「AsyncOS Quick Reference Guide」を参照してください。たとえば、Cisco IronPort アプライアンスで admin アカウントに対して SSH 公開キーが設定されている場合は、チャレンジされないリモート ホストから次のコマンドを実行できます。

```
# ssh admin@mail3.example.com status

Enter "status detail" for more information.

Status as of: Mon Jan 20 17:24:15 2003

Last counter reset: Mon Jan 20 17:08:21 2003
```

```
System status: online

[rest of command deleted]
```

CHAPTER 9

テストとトラブルシューティング

この章は、次の内容で構成されています。

システムに関する問題のトラブルシューティングや解決を行うには、いくつかの基本的な方法があります。しかし、シスコには、複雑な問題に対応するテクニカル サポートがあることを覚えておいてください（「シスコのテクニカル サポート」（P.1-7）を参照）。

（注） ここ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与えるものや、逆に影響を受けるものがあります。詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の付録 B、「Assigning Network and IP Addresses」を参照してください。

テスト メッセージを使用したメール フローのデバッグ：トレース

[System Administration] > [Trace] ページを使用して（CLI の trace コマンドと同等）、テスト メッセージの送信をエミュレートすることにより、システムを介したメッセージ フローをデバッグできます。[Trace] ページ（および CLI コマンドの trace）では、メッセージをリスナーが受け取ったとしてエミュレートし、システムの現在の設定によって「トリガー」または影響を受ける機能の概要を出力します。テスト メッセージは実際には送信されません。特に、Cisco IronPort アプライアンスで使用できる多数の高度な機能を組み合わせると、[Trace] ページ（および trace CLI コマンド）は、強力なトラブルシューティングまたはデバッグ ツールとなります。

[Trace] ページ（および trace CLI コマンド）では、表 9-1 に示されている入力パラメータのプロンプトが表示されます。

表 9-1　[Trace] ページに対する入力

値	説明	例
Source IP address	リモート ドメインの送信元を模倣するため、リモート クライアントの IP アドレスを入力します。 **注：**trace コマンドを実行すると、IP アドレスと完全修飾ドメイン名の入力が求められます。完全修飾ドメイン名が一致するかどうかを確認するための IP アドレスの逆引きは*行われません*。trace コマンドでは、完全修飾ドメイン名フィールドをブランクにすることができないので、DNS で適切に逆引きできない場合にはテストできません。	`203.45.98.109`
Fully Qualified Domain Name of the Source IP	模倣する完全修飾リモート ドメイン名を入力します。	`smtp.example.com`

表 9-1　[Trace] ページに対する入力（続き）

値	説明	例
Listener to Trace Behavior on	テスト メッセージの送信をエミュレートするため、システムに設定されているリスナーのリストから選択します。	`InboundMail`
SenderBase Network Owner Organization ID	SenderBase ネットワーク オーナーに固有の ID 番号を入力するか、送信元 IP アドレスに関連付けられたネットワーク オーナー ID の検索を指示します。 GUI を介して送信者グループにネットワーク オーナーを追加した場合は、この情報を表示できます。	`34`
SenderBase Reputation Score (SBRS scores)	スプーフされたドメインに与える SBRS を入力するか、システムがソース IP アドレスに対応する SBRS を検索するよう指定します。このパラメータは、SBRS スコアを使用するポリシーをテストするときに役立ちます。詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Implementing Reputation Filtering in a Listener's HAT」を参照してください。	`-7.5`
Envelope Sender	テスト メッセージのエンベロープ送信者を入力します。	`admin@example.net`
Envelope Recipients	テスト メッセージの受信者のリストを入力します。複数のエントリを指定する場合は、カンマで区切ります。	`joe` `frank@example.com`

Message Body	テスト メッセージのメッセージ本文を入力します。メッセージ本文の入力を終了するには、別の行にピリオドを入力します。「ヘッダー」は本文の一部と見なされることに注意してください。	`To: 1@example.com`
		From: ralph
		Subject: Test
		
		`this is a test message`
		.

値を入力したら、[Start Trace] をクリックします。メッセージに影響する、システムに設定されたすべての機能の概要が出力されます。

メッセージ本文は、ローカル ファイル システムからアップロードできます（CLI では、`/configuration` ディレクトリにアップロードしたメッセージ本文を使用してテストできます。Cisco IronPort アプライアンスへのインポート用ファイルの準備に関する詳細については、付録 A「Accessing the Appliance」を参照してください）。

概要が出力されると、生成されたメッセージの確認とテスト メッセージの再実行を求められます。別のテスト メッセージを入力する場合、[Trace] ページおよび `trace` コマンドで、前に入力した表 9-1 の値が使用されます。

（注） 表 9-2 に示す、`trace` コマンドによってテストされる設定の各セクションは、*順番どおりに*実行されます。この順番は、ある機能の設定が他の機能にどのように影響するかを理解するうえで非常に役立ちます。たとえば、ドメイン マップ機能によって変換される受信者アドレスは、RAT によって評価されるアドレスに影響します。また、RAT の影響を受ける受信者は、エイリアス テーブルによって評価されるアドレスに影響する、というようになります。

表 9-2　トレースを実行したときの出力の表示

trace コマンド セクション	出力
Host Access Table (HAT) and Mail Flow Policy Processing	指定したリスナーに対する Host Access Table の設定が処理されます。システムからは、入力したリモート IP アドレスおよびリモート ドメイン名と一致した HAT 内のエントリが報告されます。デフォルトのメール フロー ポリシーと送信者グループ、およびどちらが所定のエントリに一致したかを確認できます。 Cisco IronPort アプライアンスが（REJECT または TCPREFUSE アクセス ルールを介して）接続を拒否するように設定された場合、処理中の `trace` コマンドはその時点で終了します。 HAT パラメータの設定についての詳細は、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「The Host Access Table (HAT): Sender Groups and Mail Flow Policies」を参照してください。
Envelope Sender Address Processing これらのセクションには、指定したエンベロープ送信者に対してアプライアンスの設定がどのように影響するかが要約されます（つまり、MAIL FROM コマンドがアプライアンスの設定によってどのように解釈されるかがわかります）。`trace` コマンドは、このセクションの前に「`Processing MAIL FROM:`」を出力します。	
Default Domain	リスナーで、受信するメッセージのデフォルトの送信者ドメインを変更するように指定した場合は、エンベロープ送信者に対するすべての変更がこのセクションに出力されます。 詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Customizing Listeners」の章を参照してください。

表 9-2　トレースを実行したときの出力の表示（続き）

trace コマンド セクション	出力
Masquerading	メッセージのエンベロープ送信者を変換するように指定した場合は、ここに変更が表示されます。`listenerconfig -> edit -> masquerade -> config` サブコマンドを使用して、プライベート リスナーに対するエンベロープ送信者のマスカレードをイネーブルにします。 詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Delivery Features」の章を参照してください。
Envelope Recipient Processing これらのセクションでは、指定したエンベロープ受信者に対してアプライアンスがどのように影響するかの要約を示します（つまり、RCPT TO コマンドがアプライアンスの設定によってどのように解釈されるかがわかります）。`trace` コマンドは、このセクションの前に「`Processing Recipient List:`」を出力します。	
Default Domain	リスナーで、受信するメッセージのデフォルトの送信者ドメインを変更するように指定した場合は、エンベロープ受信者に対するすべての変更がこのセクションに出力されます。 詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Customizing Listeners」の章を参照してください。

表 9-2　トレースを実行したときの出力の表示（続き）

trace コマンド セクション	出力
Domain Map Translation	ドメイン マップ機能によって、受信者アドレスが代替アドレスに変換されます。ドメイン マップの変更を指定しており、指定した受信者アドレスが一致した場合は、このセクションに変換が出力されます。 詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Delivery Features」の章を参照してください。
Recipient Access Table (RAT)	ポリシーとパラメータのほか、このセクションには、RAT 内のエントリに一致する各エンベロープ受信者が出力されます（たとえば、リスナーの RAT の制限をバイパスするように、受信者を指定した場合）。 受け入れる受信者の指定の詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Configuring the Gateway to Receive Email」の章を参照してください。
Alias Table	このセクションには、アプライアンスで設定されたエイリアス テーブル内のエントリに一致する各エンベロープ受信者（および 1 つまたは複数の受信者アドレスへの後続の変換）が出力されます。 詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Delivery Features」の章を参照してください。

表 9-2　トレースを実行したときの出力の表示（続き）

trace コマンド セクション	出力
Pre-Queue Message Operations ここでは、メッセージのコンテンツを受信してから、メッセージを作業キューに入れるまでに、アプライアンスが各メッセージにどのような影響を及ぼすかを説明します。この処理は、最後の `250 ok` コマンドがリモート MTA に返される前に実行されます。 `trace` コマンドは、このセクションの前に「Message Processing:」を出力します。	
Virtual Gateways	`altsrchost` コマンドを実行すると、エンベロープ送信者の完全アドレス、ドメイン、または名前、あるいは IP アドレスの一致に基づいて、特定のインターフェイスにメッセージが割り当てられます。エンベロープ送信者が `altsrchost` コマンドのエントリに一致すると、その情報がこのセクションに出力されます。 ここで割り当てられた仮想ゲートウェイ アドレスは、後述のメッセージ フィルタ処理によって上書きされる場合があります。 詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Delivery Features」の章を参照してください。

表 9-2　トレースを実行したときの出力の表示（続き）

trace コマンド セクション	出力
Bounce Profiles	バウンス プロファイルは、処理中の 3 つの時点で適用されます。ここが最初のポイントです。リスナーにバウンス プロファイルが割り当てられる場合は、プロセス内のこの時点で割り当てられます。その情報がこのセクションに出力されます。 詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Delivery Features」の章を参照してください。

表 9-2　トレースを実行したときの出力の表示（続き）

trace コマンド セクション	出力
Work Queue Operations 次の一連の機能は、作業キュー内のメッセージに対して実行されます。機能が実行されるのは、クライアントからのメッセージが受け入れられた後、そのメッセージが配信用として宛先キューに入れられる前です。`status` コマンドおよび `status detail` コマンドによって「Messages in Work Queue」が報告されます。	
Masquerading	メッセージの [To:]、[From:]、および [CC:] ヘッダーが（リスナーから入力されたスタティック テーブルまたは LDAP クエリーを通じて）マスクされるように指定した場合は、ここに変更が表示されます。`listenerconfig -> edit -> masquerade -> config` サブコマンドを使用して、プライベート リスナーに対してメッセージ ヘッダーのマスカレードをイネーブルにします。 詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Delivery Features」の章を参照してください。
LDAP Routing	リスナーに対して LDAP クエリーがイネーブルになっている場合は、このセクションに LDAP 許可、再ルーティング、マスカレード、およびグループ クエリーの結果が出力されます。 詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「LDAP Queries」の章を参照してください。

表 9-2　トレースを実行したときの出力の表示（続き）

trace コマンド セクション	出力
Message Filters Processing	システムでイネーブルになっているすべてのメッセージ フィルタは、この時点でテスト メッセージによって評価されます。フィルタごとにルールが評価され、最後の結果が「true」であれば、そのフィルタの各アクションが順次実行されます。フィルタには他のフィルタがアクションとして含まれている場合があり、フィルタは無制限にネスティングされます。ルールが「false」と評価された場合、アクションのリストが `else` 句に関連付けられていれば、それらのアクションが代わりに評価されます。このセクションには、順番に処理されたメッセージ フィルタの結果が出力されます。 『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Using Message Filters to Enforce Email Policies」の章を参照してください。
Mail Policy Processing	メール ポリシーの処理セクションには、アンチスパム、アンチウイルス、ウイルス感染フィルタ機能と、指定されたすべての受信者に対するフッター スタンプ機能が表示されます。複数の受信者が電子メール セキュリティ マネージャの複数のポリシーに一致する場合は、一致する各ポリシーが次の各セクションに繰り返し表示されます。「Message going to」というストリングは、どの受信者がどのポリシーに一致したかを定義します。

表 9-2　トレースを実行したときの出力の表示（続き）

trace コマンド セクション	出力
Anti-Spam	このセクションには、アンチスパム スキャンの処理対象としてフラグが設定されていないメッセージが示されます。メッセージがリスナーに対するアンチスパム スキャンによって処理されることになっている場合、メッセージは処理され、返された判定が出力されます。Cisco IronPort アプライアンスが、その判定に基づいてメッセージをバウンスまたはドロップするように設定されている場合は、その情報が出力され、trace コマンドの処理は停止します。 注：システムでアンチスパム スキャンが使用できない場合、この手順は省略されます。アンチスパム スキャンを使用できても、機能キーによってイネーブルになっていない場合は、その情報もこのセクションに出力されます。 詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Anti-Spam」の章を参照してください。

表 9-2　トレースを実行したときの出力の表示（続き）

trace コマンド セクション	出力
Anti-Virus	このセクションには、アンチウイルス スキャンの処理対象としてフラグが設定されていないメッセージが示されます。メッセージがリスナーに対するアンチウイルス スキャンによって処理されることになっている場合、メッセージは処理され、返された判定が出力されます。Cisco IronPort アプライアンスが、感染メッセージを「クリーニング」するように設定されている場合は、その情報が表示されます。その判定に基づいてメッセージをバウンスまたはドロップするように設定されている場合は、その情報が出力され、`trace` コマンドの処理は停止します。 注：システムでアンチウイルス スキャンが使用できない場合、この手順は省略されます。アンチウイルス スキャンを使用できても、機能キーによってイネーブルになっていない場合は、その情報もこのセクションに出力されます。 詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Anti-Virus」の章を参照してください。

表 9-2　トレースを実行したときの出力の表示（続き）

trace コマンド セクション	出力
Content Filters Processing	システムでイネーブルになっているすべてのコンテンツ フィルタは、この時点でテスト メッセージによって評価されます。フィルタごとにルールが評価され、最後の結果が「true」であれば、そのフィルタの各アクションが順次実行されます。フィルタには他のフィルタがアクションとして含まれている場合があり、フィルタは無制限にネスティングされます。このセクションには、順番に処理されたコンテンツ フィルタの結果が出力されます。 『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Email Security Manager」の章を参照してください。
VOF Processing	このセクションには、Outbreak フィルタ機能をバイパスする添付ファイルのあるメッセージが示されます。メッセージが受信者に対する Outbreak フィルタによって処理されることになっている場合、メッセージは処理され、その評価が出力されます。アプライアンスが、判定に基づいてメッセージを検疫、バウンス、またはドロップするように設定されている場合、その情報が出力されて、処理が停止します。 詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Outbreak Filters」の章を参照してください。
Footer Stamping	このセクションには、メッセージにフッター テキスト リソースが付加されたかどうかが示されます。テキスト リソースの名前が表示されます。『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Text Resources」の章にある「Message Footer Stamping」を参照してください。

表 9-2　トレースを実行したときの出力の表示（続き）

trace コマンド セクション	出力
Delivery Operations 次の各セクションには、メッセージが配信されるときに発生する動作が示されます。`trace` コマンドは、このセクションの前に「`Message Enqueued for Delivery`」を出力します。	
Global Unsubscribe per Domain and per User	`trace` コマンドの入力として指定した受信者が、グローバル配信停止機能に示されている受信者、受信者ドメイン、または IP アドレスに一致すると、未登録の受信者アドレスがこのセクションに出力されます。 『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Delivery Features」の章を参照してください。
Final Result すべての処理が出力されると、最終結果が表示されます。CLI では、「Would you like to see the resulting message?」という問いに対して **`y`** と入力して、結果のメッセージを表示します。	

[Trace] ページの GUI の例

図 9-1　[Trace] ページの入力

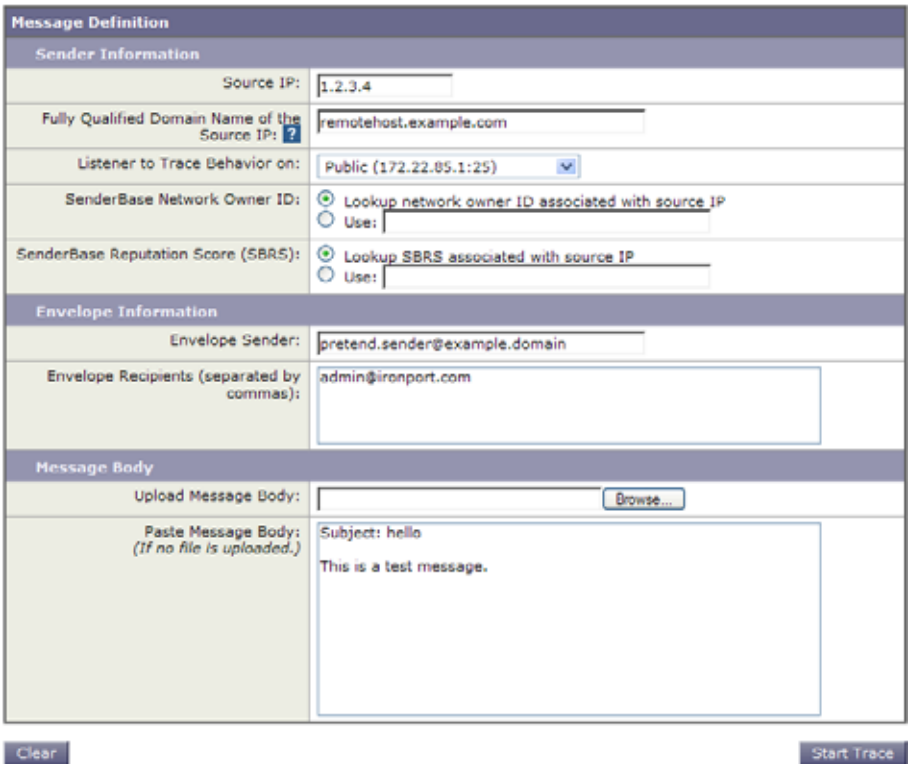
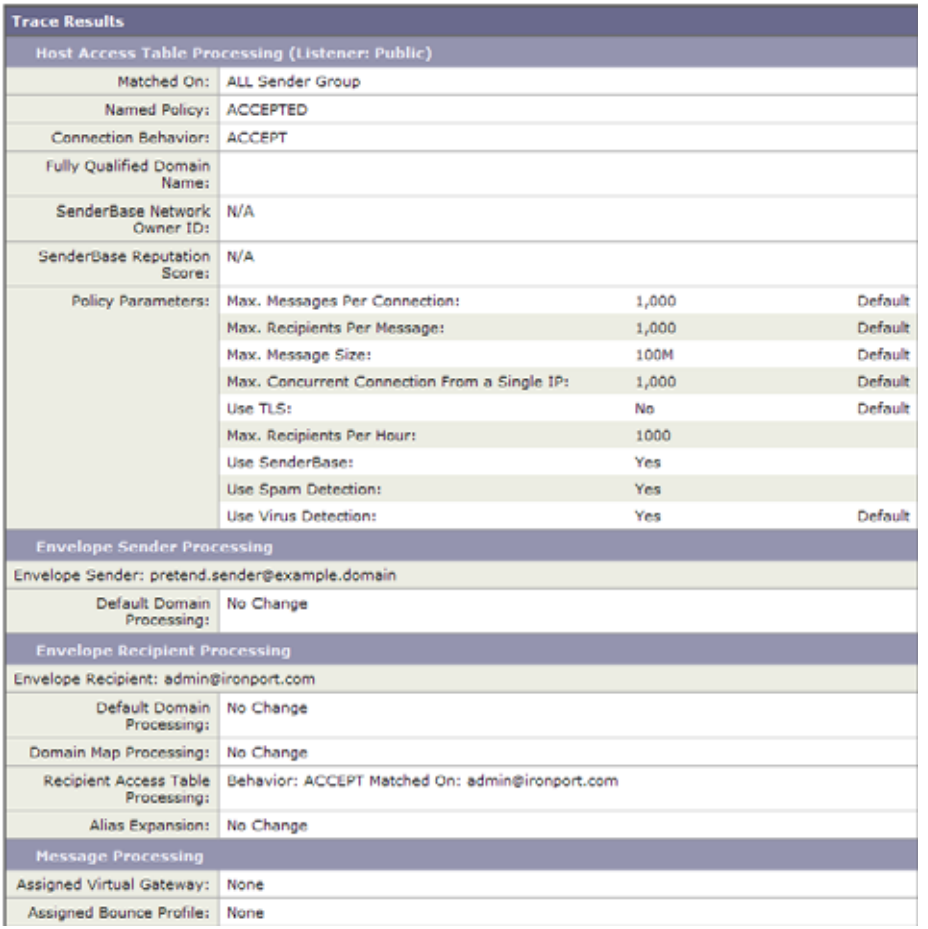


図 9-2　[Trace] ページの出力（1/2）



Trace

Trace Results			
Host Access Table Processing (Listener: Public)			
Matched On:	ALL Sender Group		
Named Policy:	ACCEPTED		
Connection Behavior:	ACCEPT		
Fully Qualified Domain Name:			
SenderBase Network Owner ID:	N/A		
SenderBase Reputation Score:	N/A		
Policy Parameters:	Max. Messages Per Connection:	1,000	Default
	Max. Recipients Per Message:	1,000	Default
	Max. Message Size:	100M	Default
	Max. Concurrent Connection From a Single IP:	1,000	Default
	Use TLS:	No	Default
	Max. Recipients Per Hour:	1000	
	Use SenderBase:	Yes	
	Use Spam Detection:	Yes	
	Use Virus Detection:	Yes	Default
Envelope Sender Processing			
Envelope Sender: pretend.sender@example.domain			
Default Domain Processing:	No Change		
Envelope Recipient Processing			
Envelope Recipient: admin@ironport.com			
Default Domain Processing:	No Change		
Domain Map Processing:	No Change		
Recipient Access Table Processing:	Behavior: ACCEPT Matched On: admin@ironport.com		
Alias Expansion:	No Change		
Message Processing			
Assigned Virtual Gateway:	None		
Assigned Bounce Profile:	None		

図 9-3　[Trace] ページの出力（2/2）

Domain Masquerading	
	No changes
Filter Processing	
skipper	Skipped (Inactive)
always_deliver	Rule: rcpt-to == "@mail.qa": False Rule: rcpt-to == "ironport.com": True Rule: OR: True Action: deliver()
Mail Policy Processing: Inbound (matched on policy Public Upgrade)	
Message going to:	admin@ironport.com
Anti-Spam Processing	
Evaluation:	Not Spam
Anti-Virus Processing	
Evaluation:	No Viruses Detected Elapsed Time: 0.000 sec
Actions Taken:	Delivered
VOF Processing	
Evaluation:	No threat detected
Footer Stamping	
Appended Text Resource:	footer
DomainKey Signing	
Result of DomainKeys processing:	DomainKeys signing not enabled in this listener's HAT
Message Delivery (matched on policy Public Upgrade)	
Final Envelope Sender:	pretend.sender@example.domain
Final Recipients:	admin@ironport.com
Final Message:	Received: from remotehost.example.com (HELO TEST) ([1.2.3.4]) by mail3.example.com with TEST; 21 Jul 2005 14:40:05 -0700 Message-Id: <48q06k4@Public> X-Brightmail-Tracker: AAAAAA== X-BrightmailFiltered: true X-IronPort-Anti-Spam-Filtered: true X-IronPort-AV: i="3.95,134,1120460400", d="scan'"; a="0:sNHT0" Subject: hello Content-Transfer-Encoding: base64 Content-Type: text/plain; charset="utf-8" VGhpcyBpcyBhIHRlc3QgbWVzc2FnZS4KPT09PT09PT09PT09CuODleODg+ODv+ODvOOBp+OBmeOA guOCj+OBhOOCj+OBhOOAggpUaGlzIGlzIGEgSmFwYW5lc2UgZm9vdGVyCj09PT09PT09PQo=

Done

[Trace] ページの CLI の例

```
mail3.example.com> trace


Enter the source IP

[]> 192.168.1.1


Enter the fully qualified domain name of the source IP

[]> example.com


Select the listener to trace behavior on:

1. InboundMail

2. OutboundMail

[1]> 1


Fetching default SenderBase values...

Enter the SenderBase Org ID of the source IP.  The actual ID is N/A.

[N/A]>


Enter the SenderBase Reputation Score of the source IP.  The actual score
is N/A.

[N/A]>
```

```
Enter the Envelope Sender address:

[]> pretend.sender@example.net


Enter the Envelope Recipient addresses.  Separate multiple addresses by
commas.

[]> admin@example.com


Load message from disk?  [Y]> n


Enter or paste the message body here.  Enter '.' on a blank line to end.

This is a test message.

.


HAT matched on unnamed sender group, host ALL

 - Applying $ACCEPTED policy (ACCEPT behavior).

 - Maximum Message Size:  100M (Default)

 - Maximum Number Of Connections From A Single IP:  1000 (Default)

 - Maximum Number Of Messages Per Connection:  1,000 (Default)

 - Maximum Number Of Recipients Per Message:  1,000 (Default)

 - Maximum Recipients Per Hour:  100 (Default)

 - Use SenderBase For Flow Control:  Yes (Default)

 - Spam Detection Enabled:  Yes (Default)
```

```
 - Virus Detection Enabled:  Yes (Default)

 - Allow TLS Connections:  No (Default)


Processing MAIL FROM:

 - Default Domain Processing:  No Change


Processing Recipient List:

Processing admin@ironport.com

 - Default Domain Processing:  No Change

 - Domain Map:  No Change

 - RAT matched on admin@ironport.com, behavior = ACCEPT

 - Alias expansion:  No Change


Message Processing:

 - No Virtual Gateway(tm) Assigned

 - No Bounce Profile Assigned


Domain Masquerading/LDAP Processing:

 - No Changes.


Processing filter 'always_deliver':

Evaluating Rule:   rcpt-to == "@mail.qa"
```

```
    Result = False

Evaluating Rule:   rcpt-to == "ironport.com"

    Result = True

Evaluating Rule:   OR

    Result = True

Executing Action:  deliver()


Footer Stamping:

 - Not Performed


Inbound Recipient Policy Processing: (matched on Management Upgrade
policy)

Message going to:  admin@ironport.com


AntiSpam Evaluation:

 - Not Spam


AntiVirus Evaluation:

 - Message Clean.

 - Elapsed Time = '0.000 sec'


VOF Evaluation:
```

```
 - No threat detected


Message Enqueued for Delivery


Would you like to see the resulting message? [Y]> y




Final text for messages matched on policy Management Upgrade

Final Envelope Sender:  pretend.sender@example.doma

Final Recipients:

 - admin@ironport.com


Final Message Content:


Received: from remotehost.example.com (HELO TEST) (1.2.3.4)

  by stacy.qa with TEST; 19 Oct 2004 00:54:48 -0700

Message-Id: <3i93q9$@Management>

X-IronPort-AV: i="3.86,81,1096873200";

   d="scan'208"; a="0:sNHT0"

Subject: hello
```

```
This is a test message.


Run through another debug session? [N]>
```

アプライアンスのテストにリスナーを使用

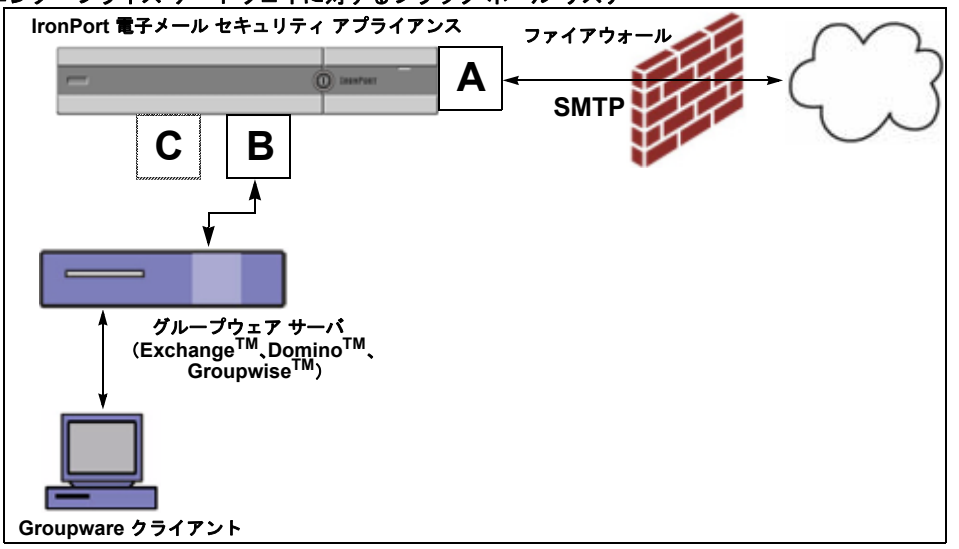
「ブラック ホール」リスナーを使用して、メッセージ生成システムをテストして、受信側のパフォーマンスの大まかな測定を行うことができます。ブラック ホール リスナーには、*キューイング*と*非キューイング*の 2 つのタイプがあります。

キューイング リスナーは、メッセージをキューに保存しますが、その後メッセージをただちに削除します。非キューイング リスナーはメッセージを承認した後、保存しないですぐに削除します。

メッセージ生成システムのインジェクション部分全体のパフォーマンスを測定する場合は、キューイング リスナーを使用します。メッセージ生成システムからアプライアンスまでの接続のトラブルシューティングを行う場合は、非キューイング リスナーを使用します。

たとえば、図 9-4 では、ブラック ホール リスナー「C」を作成して、「B」というプライベート リスナーをミラーリングします。非キューイング版では、グループウェア クライアントからグループウェア サーバを経由してアプライアンスまでのシステムのパフォーマンス パスをテストします。キューイング版では、同じパスと、メッセージをキューイングして SMTP 経由の配信を準備するアプライアンスの能力をテストします。

図 9-4　エンタープライズ ゲートウェイに対するブラック ホール リスナー



次の例では、listenerconfig コマンドを使用して、管理インターフェイスで BlackHole_1 という名前のキューイング タイプのブラック ホール リスナーを作成します。次に、このリスナー用の Host Access Table（HAT）を編集して、次のホストからの接続を受け入れるようにします。

- yoursystem.example.com
- 10.1.2.29
- badmail.tst
- .tst

（注）　最後のエントリである .tst により、.tst ドメイン内にあるすべてのホストから BlackHole_1 という名前のリスナーに電子メールを送信できるようになります。

例

```
mail3.example.com> listenerconfig


Currently configured listeners:
```

```
1. InboundMail (on PublicNet, 192.168.2.1) SMTP Port 25 Public

2. OutboundMail (on PrivateNet, 192.168.1.1) SMTP Port 25 Private


Choose the operation you want to perform:

- NEW - Create a new listener.

- EDIT - Modify a listener.

- DELETE - Remove a listener.

- SETUP - Change global settings.

[]> new


Please select the type of listener you want to create.

1. Private

2. Public

3. Blackhole

[2]> 3


Do you want messages to be queued onto disk?  [N]> y


Please create a name for this listener (Ex: "OutboundMail"):

[]> BlackHole_1


Please choose an IP interface for this Listener.
```

```
1. Management (192.168.42.42/24: mail3.example.com)

2. PrivateNet (192.168.1.1/24: mail3.example.com)

3. PublicNet (192.168.2.1/24: mail3.example.com)

[1]> 1


Choose a protocol.

1. SMTP

2. QMQP

[1]> 1


Please enter the IP port for this listener.

[25]> 25


Please specify the systems allowed to relay email through the IronPort
C60.

Hostnames such as "example.com" are allowed.

Partial hostnames such as ".example.com" are allowed.

IP addresses, IP address ranges, and partial IP addressed are allowed.

Separate multiple entries with commas.

[]> yoursystem.example.com, 10.1.2.29, badmail.tst, .tst


Do you want to enable rate limiting per host? (Rate limiting defines
```

```
the maximum number of recipients per hour you are willing to receive from
a remote domain.) [N]> n


Default Policy Parameters

==========================

Maximum Message Size: 100M

Maximum Number Of Connections From A Single IP: 600

Maximum Number Of Messages Per Connection: 10,000

Maximum Number Of Recipients Per Message: 100,000

Maximum Number Of Recipients Per Hour: Disabled

Use SenderBase for Flow Control:  No

Spam Detection Enabled:  No

Virus Detection Enabled:  Yes

Allow TLS Connections: No

Allow SMTP Authentication: No

Require TLS To Offer SMTP authentication: No

Would you like to change the default host access policy?  [N]> n


Listener BlackHole_1 created.

Defaults have been set for a Black Hole Queuing listener.

Use the listenerconfig->EDIT command to customize the listener.
```

```
Currently configured listeners:

1. BlackHole_1 (on Management, 192.168.42.42) SMTP Port 25 Black Hole
Queuing

2. InboundMail (on PublicNet, 192.1681.1) SMTP Port 25 Public

3. OutboundMail (on PrivateNet, 192.168.1.1) SMTP Port 25 Private


Choose the operation you want to perform:

- NEW - Create a new listener.

- EDIT - Modify a listener.

- DELETE - Remove a listener.

- SETUP - Change global settings.

[]>
```

（commit コマンドを実行して、これらの変更が有効になるようにしてください）

キューイング タイプのブラック ホール リスナーを設定して、HAT でインジェクション システムからの接続を受け入れるよう変更したら、インジェクション システムを使用して、アプライアンスへの電子メールの送信を開始します。status、status detail、および rate コマンドを使用して、システムのパフォーマンスをモニタします。また、Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）でシステムをモニタすることもできます。詳細については、次の資料を参照してください。

- 「CLI によるモニタリング」（P.6-9）
- 「GUI でのその他の作業」（P.7-1）

ネットワークのトラブルシューティング

アプライアンスのネットワーク接続に問題があることが疑われる場合は、まずそのアプライアンスが正常に動作していることを確認してください。

アプライアンスのネットワーク接続のテスト方法

アプライアンスがネットワーク上でアクティブであり、電子メールを送信できることを確認するには、次の手順に従ってください。

ステップ 1　システムに接続し、管理者としてログインします。正常にログインできると、次のメッセージが表示されます。

```
Last login: day month date hh:mm:ss from IP address

Copyright (c) 2001-2003, IronPort Systems, Inc.


AsyncOS x.x for Cisco IronPort


Welcome to the Cisco IronPort Messaging Gateway Appliance(tm)
```

ステップ 2　`status` コマンドまたは `status detail` コマンドを使用します。

```
mail3.example.com> status
```

または

```
mail3.example.com> status detail
```

`status` コマンドは、電子メール動作についてモニタされる情報のサブセットを返します。返される統計情報は、カウンタとゲージの 2 つのカテゴリにグループ化されます。レートなどの電子メールの動作についての全般的なモニタリング情報については、`status detail` コマンドを使用します。カウンタは、システム内の各種イベントの現在までの合計を示します。カウンタごとに、そのカウンタのリセット以降、最後のシステム リブート以降、およびシステムの存続期間に発生したイベントの合計数を表示できます。（詳細は、「CLI によるモニタリング」（P.6-9）を参照してください）。

ステップ 3　`mailconfig` コマンドを使用して、機能している既知のアドレスに電子メールを送信します。

mailconfig コマンドによって、アプライアンスで有効な設定のすべてが含まれる、人が読み取ることのできるファイルが作成されます。このファイルをアプライアンスから機能する既知の電子メール アドレスに送信して、アプライアンスがネットワークで電子メールを送信できることを確認します。

```
mail3.example.com> mailconfig


Please enter the email address to which you want to send the

configuration file.

Separate multiple addresses with commas.


[]> user@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 user@example.com.

mail3.example.com>
```

トラブルシューティング

アプライアンスがネットワーク上でアクティブであることが確認されたら、次のコマンドを使用して、ネットワークの問題をピンポイントで特定します。

- netstat コマンドを使用すると、次のようなネットワーク接続（着信と発信の両方）、ルーティング テーブル、ネットワーク インターフェイスのさまざまな統計情報が表示されます。
  - アクティブなソケットのリスト
  - ネットワーク インターフェイスの状態
  - ルーティング テーブルの内容

  - リッスン キューのサイズ
  - パケット トラフィック情報

- `diagnostic -> network -> flush` コマンドを使用すると、ネットワークに関連するすべてのキャッシュをフラッシュできます。
- `diagnostic -> network -> arpshow` コマンドを使用すると、システムの ARP キャッシュを表示できます。
- `packetcapture` コマンドを使用すると、コンピュータが接続されているネットワーク上で送受信されている TCP/IP や他のパケットを傍受して表示できます。

  `packetcapture` を使用するには、ネットワーク インターフェイスとフィルタを設定します。このフィルタでは、UNIX の `tcpdump` コマンドと同じ形式を使用します。パケットの捕捉を開始するには `start` を、停止するには `stop` を使用します。捕捉を停止した後、SCP または FTP を使用して `/pub/captures` ディレクトリからファイルをダウンロードする必要があります。詳細については、「パケット キャプチャ」（P.8-11）を参照してください。
- アプライアンスでネットワーク上にアクティブな接続があり、ネットワーク上の特定のセグメントに到達できることを確認するには、動作している既知のホストに対して `ping` コマンドを使用します。

  `ping` コマンドを使用すると、アプライアンスからネットワーク ホストへの接続をテストできます。

```
mail3.example.com> ping


Which interface do you want to send the pings from?

1. Auto

2. Management (192.168.42.42/24: mail3.example.com)

3. PrivateNet (192.168.1.1/24: mail3.example.com)

4. PublicNet (192.168.2.1/24: mail3.example.com)

[1]> 1
```

```
Please enter the host you wish to ping.

[]> anotherhost.example.com


Press Ctrl-C to stop.

PING anotherhost.example.com (x.x.x.x): 56 data bytes

64 bytes from 10.19.0.31: icmp_seq=9 ttl=64 time=0.133 ms

64 bytes from 10.19.0.31: icmp_seq=10 ttl=64 time=0.115 ms

^C

--- anotherhost.example.com ping statistics ---

11 packets transmitted, 11 packets received, 0% packet loss

round-trip min/avg/max/stddev = 0.115/0.242/1.421/0.373 ms
```

（注）　ping コマンドを終了するには、Ctrl+C を使用します。

- traceroute コマンドを使用すると、アプライアンスからネットワーク ホストへの接続をテストして、ネットワークのホップに関するルーティングの問題をデバッグできます。

```
mail3.example.com> traceroute


Which interface do you want to trace from?

1. Auto

2. Management (192.168.42.42/24: mail3.example.com)
```

```
3. PrivateNet (192.168.1.1/24: mail3.example.com)

4. PublicNet (192.168.2.1/24: mail3.example.com)

[1]> 1


Please enter the host to which you want to trace the route.

[]> 10.1.1.1


Press Ctrl-C to stop.

traceroute to 10.1.1.1 (10.1.1.1), 64 hops max, 44 byte packets

 1  gateway (192.168.0.1)  0.202 ms  0.173 ms  0.161 ms

 2  hostname (10.1.1.1)  0.298 ms  0.302 ms  0.291 ms

mail3.example.com>
```

- diagnostic -> network -> smtpping コマンドを使用すると、リモートの SMTP サーバをテストできます。
- nslookup コマンドを使用すると、DNS の機能をテストできます。

  nslookup コマンドでは、アプライアンスから動作している Domain Name Service（DNS; ドメイン ネーム サービス）サーバを使用してホスト名や IP アドレスを解決して到達できることを確認できます。

```
mail3.example.com> nslookup


Please enter the host or IP to resolve.

[]> example.com
```

```
Choose the query type:

1. A

2. CNAME

3. MX

4. NS

5. PTR

6. SOA

7. TXT

[1]>


A=192.0.34.166 TTL=2d
```

表 9-3　DNS の機能の確認：クエリーのタイプ

クエリーのタイプ	説明
A	ホストのインターネット アドレス
CNAME	エイリアスの正規の名前
MX	メール エクスチェンジャ
NS	指定したゾーンのネーム サーバ
PTR	クエリーがインターネット アドレスの場合はホスト名、そうでない場合は他の情報に対するポインタ
SOA	ドメインの「start-of-authority（権威の開始）」情報
TXT	テキスト情報

- tophosts コマンドを CLI または GUI から使用して、「Active Recipients」の順にソートします。

  tophosts コマンドからは、キューにある上位 20 の受信者のリストが返されます。このコマンドは、ネットワーク接続の問題が、電子メールを送信しようとしている 1 台のホストまたは 1 つのホスト グループに限定されるかどうかを確認するのに役立ちます（詳細については、49 ページの「メール キューの構成の確認」を参照してください）。

```
mail3.example.com> tophosts


Sort results by:

1. Active Recipients

2. Connections Out

3. Delivered Recipients

4. Soft Bounced Events
```

```
5. Hard Bounced Recipients

[1]> 1


Status as of:         Mon Nov 18 22:22:23 2003

    ActiveConn.Deliv.SoftHard

# Recipient HostRecipOutRecip.BouncedBounced

1  aol.com36510255218

2  hotmail.com29071982813

3  yahoo.com13461231119

4  excite.com9838494

5  msn.com8427633  29

^C
```

- tophosts コマンドの結果として得られたリストの最上位のドメインに対して hoststatus コマンドを実行し、詳しく調べます。

  hoststatus コマンドは、特定の受信者ホストに関する電子メール動作のモニタリング情報を返します。AsyncOS キャッシュに格納されている DNS 情報と、受信者ホストから最後に返されたエラーも表示されます。返されるデータは、最後に実行した resetcounters コマンドからの累積です。（詳細は、「メール ホストのステータスのモニタリング」（P.6-17）を参照してください）。

  最上位のドメインに対して hoststatus コマンドを実行すると、アプライアンスまたはインターネットのいずれかに対する DNS 解決のパフォーマンスの問題を切り分けることができます。たとえば、最上位のアクティブな受信ホストに対して hoststatus コマンドを実行したとき、発信側の多数の接続が保留状態で表示された場合は、特定のホストがダウン状態または到達不能でないかどうか、またアプライアンスがすべてのホストあるいは大半のホストに接続不可能でないかどうかを確認してください。

- ファイアウォールの権限を確認します。

  アプライアンスが正しく機能するためには、ポート 20、21、22、23、25、53、80、123、443、および 628 を開く必要がある場合があります（詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の付録 C、「Firewall Information」を参照してください）。

- ネットワーク上のアプライアンスから、`dnscheck@ironport.com` に対して電子メールを送信します。

  ネットワーク内から `dnscheck@ironport.com` に対して電子メールを送信して、システム上で基本的な DNS の確認を行います。オートレスポンダによる電子メールによって、次の 4 つのテストについての結果と詳細が返されます。

  DNS PTR レコード：Envelope From の IP アドレスがドメインの PTR レコードと一致するか。

  DNS A レコード：ドメインの PTR レコードが Envelope From の IP アドレスと一致するか。

  HELO マッチ：SMTP HELO コマンドにリストされたドメインが、Envelope From の DNS ホスト名と一致するか。

  遅延バウンス メッセージを受け入れるメール サーバ：SMTP HELO コマンドのリストにあるドメインに、そのドメインの IP アドレスを解決する MX レコードがあるか。

リスナーのトラブルシューティング

電子メールのインジェクションに問題があると疑われる場合は、次の方法を使用します。

- インジェクションを行っている IP アドレスを確認し、`listenerconfig` コマンドを使用して許可されているホストを確認します。

  作成したリスナーに接続できるよう IP アドレスが許可されていますか。`listenerconfig` コマンドを使用して、リスナーの Host Access Table（HAT）を確認します。次のコマンドを使用して、リスナーの HAT を出力します。

  `listenerconfig` -> `edit` -> *listener_number* -> `hostaccess` -> `print`

HAT は、IP アドレス、IP アドレスのブロック、ホスト名、ドメインなどを使用して、接続を拒否するよう設定できます。詳細については、「接続が許可されているホストの指定」（P.107）を参照してください。

また、limits サブコマンドを使用して、リスナーに許可されている接続の最大数を確認することもできます。

`listenerconfig -> edit -> listener_number -> limits`

- インジェクションを行っているマシンから、Telnet または FTP を使用して、アプライアンスに手動で接続します。次の例を参考にしてください。

```
injection_machine% telnet appliance_name
```

アプライアンス内で telnet コマンドを使用して、リスナーから実際のアプライアンスに接続することもできます。

```
mail3.example.com> telnet

Please select which interface you want to telnet from.
1. Auto
2. Management (192.168.42.42/24: mail3.example.com)
3. PrivateNet (192.168.1.1/24: mail3.example.com)
4. PublicNet (192.168.2.1/24: mail3.example.com)
[1]> 3

Enter the remote hostname or IP.
[]> 193.168.1.1

Enter the remote port.
```

```
[25]> 25


Trying 193.168.1.1...

Connected to 193.168.1.1.

Escape character is '^]'.
```

あるインターフェイスから他のインターフェイスに接続できない場合は、アプライアンスの Management、Data1、Data2 インターフェイスからネットワークに接続している方法に問題がある可能性があります。telnet を使用して接続を試みている場合は、ターゲットとするインターフェイスで telnet サービスがイネーブルになっていることを確認してください。詳細については、付録 A「Accessing the Appliance」を参照してください。また、リスナーのポート 25 に対して telnet を実行して、SMTP コマンドを手動で入力することもできます（このプロトコルを熟知している場合）。

- IronPort のテキスト メール ログおよびインジェクション デバッグ ログを調べて、受信エラーがあるかどうかを確認します。

  インジェクション デバッグ ログには、アプライアンスとシステムに接続している特定のホストとの間の SMTP カンバセーションが記録されています。インジェクション デバッグ ログは、インターネットから接続を開始するクライアントとアプライアンス間の通信に関する問題をトラブルシューティングするのに役立ちます。このログでは、2 つのシステム間で伝送されたすべてのバイトが記録され、[Sent to]（接続ホストに送信）または [Rcvd from]（接続ホストから受信）に分類されます。

  詳細については、「IronPort テキスト メール ログの使用」（P.5-16）および「IronPort インジェクション デバッグ ログの使用」（P.5-36）を参照してください。

配信のトラブルシューティング

アプライアンスからの電子メールの配信に問題があると疑われる場合は、次の方法を試してください。

- 問題がドメインに限定されたものであるかどうかを判断します。

tophosts コマンドを使用して、電子メール キューに関する直近の情報を入手して、特定の受信者のドメインに配信の問題が生じていないかを確認します。

「Active Recipients」の順にソートすると、問題のあるドメインが返されますか。

「Connections Out」の順にソートしたとき、リスナーに指定されている最大接続数に達しているドメインがありますか。リスナーに対するデフォルトの最大接続数は 600 です。システム全体でのデフォルトの最大接続数は 10,000 です（deliveryconfig コマンドで設定します）。リスナーに対する最大接続数は、次のコマンドで確認できます。

listenerconfig -> edit -> *injector_number* -> limits

リスナーに対する接続が、destconfig コマンドによってさらに制限されていませんか（システムの最大数または仮想ゲートウェイ アドレスによる）。destconfig による接続の制限を確認するには、次のコマンドを使用します。

destconfig -> list

- hoststatus コマンドを使用します。

  tophosts コマンドの結果として得られたリストの最上位のドメインに対して hoststatus コマンドを実行し、詳しく調べます。

  ホストが使用可能で、接続を受け入れていますか。

  指定したホストに対する特定の MX レコードのメール サーバに問題がありませんか。

  hoststatus コマンドでは、特定のホストに対する 5XX エラー（Permanent Negative Completion Reply）がある場合に、ホストから返された直前の「5XX」のステータス コードと説明が表示されます。このホストに対する直前の発信 TLS 接続が失敗した場合は、hoststatus コマンドで失敗した理由が表示されます。

- ドメインのデバッグ、バウンス、およびテキスト メールの各ログを設定および確認して、受信ホストが使用可能かどうかをチェックします。

  ドメイン デバッグ ログには、アプライアンスと指定した受信ホスト間での SMTP カンバセーションの際のクライアントとサーバの接続が記録されます。このタイプのログ ファイルは、特定の受信ホストに関する問題のデバッグに使用できます。

  詳細については、「IronPort ドメイン デバッグ ログの使用」（P.5-35）を参照してください。

バウンス ログには、バウンスされた各受信者に関するすべての情報が記録されます。

詳細については、「IronPort バウンス ログの使用」（P.5-30）を参照してください。

テキスト メール 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。

詳細については、「IronPort テキスト メール ログの使用」（P.5-16）を参照してください。

- `telnet` コマンドを使用して、アプライアンスから問題のあるドメインに接続します。

```
mail3.example.com> telnet


Please select which interface you want to telnet from.

1. Auto

2. Management (192.168.42.42/24: mail3.example.com)

3. PrivateNet (192.168.1.1/24: mail3.example.com)

4. PublicNet (192.168.2.1/24: mail3.example.com)

[1]> 1


Enter the remote hostname or IP.

[]> problemdomain.net


Enter the remote port.

[25]> 25
```

- 必要に応じて tlsverify コマンドを使用して発信 TLS 接続を確立し、宛先ドメインに関する TLS 接続の問題をデバッグすることができます。接続を確立するには、検証するドメインと宛先ホストを指定します。AsyncOS では、必要な（検証）TLS 設定に基づいて TLS 接続を確認します。

```
mail3.example.com> tlsverify


Enter the TLS domain to verify against:

[]> example.com


Enter the destination host to connect to.  Append the port
(example.com:26) if you are not connecting on port 25:

[example.com]> mxe.example.com:25


Connecting to 1.1.1.1 on port 25.

Connected to 1.1.1.1 from interface 10.10.10.10.

Checking TLS connection.

TLS connection established: protocol TLSv1, cipher RC4-SHA.

Verifying peer certificate.

Verifying certificate common name mxe.example.com.

TLS certificate match mxe.example.com

TLS certificate verified.

TLS connection to 1.1.1.1 succeeded.
```

```
TLS successfully connected to mxe.example.com.

TLS verification completed.
```

パフォーマンスのトラブルシューティング

アプライアンスのパフォーマンスに関する問題があると疑われる場合は、次の方法を使用してください。

- `rate` コマンドと `hostrate` コマンドを使用して、現在のシステムのアクティビティを確認します。

  `rate` コマンドは、電子メール動作に関するリアルタイム モニタリング情報を返します。詳細については、「リアルタイム アクティビティの表示」（P.6-25）を参照してください。

  `hostrate` コマンドは、特定のメール ホストに関するリアルタイムのモニタリング情報を返します。

- `status` コマンドを使用して、これまでのレートを比較して、状態の悪化を確認します。
- `status detail` コマンドを使用して、メモリの使用率を確認します。

  `status detail` コマンドを使用すると、システムのメモリ、CPU、ディスク I/O の使用率を、素早く確認できます。

（注） メモリの使用率は、常に 75 % 未満である必要があります。メモリの使用率が 75 % を超えると、アプライアンスは「リソース節約モード」に入ります。これによって「バックオフ」アルゴリズムが起動され、リソースのオーバーサブスクリプションが防止され、電子メールによる次のアラートが送信されます。

```
This system (hostname: hostname) has entered a 'resource conservation'
mode in order to prevent the rapid depletion of critical system
resources.
```

```
RAM utilization for this system has exceeded the resource conservation
threshold of 75%. The allowed injection rate for this system will be
gradually decreased as RAM utilization approaches 85%.
```

この状況は、配信機能が低下していて、大量のインジェクションが行われているときにのみ発生します。メモリの使用率が 75 % を超えたときには、キュー内のメッセージの数を調べて、特定のドメインがダウン状態または配信不可能になっていないかどうかを確認します（hoststatus コマンドまたは hostrate コマンドを使用します）。また、システムのステータスも確認して、配信が中断されないようにします。インジェクションが停止しても、依然としてメモリの使用率が高い場合は、Cisco IronPort カスタマー サポートにご連絡ください。「シスコのテクニカル サポート」（P.1-7）を参照してください。

- 問題が 1 つのドメインに限定されていますか。

  tophosts コマンドを使用して、電子メール キューに関する直近の情報を入手して、特定の受信者のドメインに配信の問題が生じていないかを確認します。

  キューのサイズを確認します。このサイズを制御したり、問題が生じている特定のドメインの受信者に対処するために、電子メール キューにあるメッセージを削除、バウンス、中断、またはリダイレクトすることができます。詳細については、「電子メール キューの管理」（P.6-33）を参照してください。以下のコマンドを使用します。

  - deleterecipients
  - bouncerecipients
  - redirectrecipients
  - suspenddel / resumedel
  - suspendlistener / resumelistener

  tophosts コマンドを使用して、ソフト バウンスおよびハード バウンスの数を確認します。[Soft Bounced Events]（オプション 4）または [Hard Bounced Recipients]（オプション 5）でソートします。特定のドメインに対するパフォーマンスに問題があることが疑われる場合は、上記のコマンドを使用して、そのドメインへの配信を制御します。

INDEX

A

B

C

D

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

X

あ

い

う

え

お

か

き

く

け

こ

さ

し

す

せ

そ

た

つ

て

と

ね

は

ひ

ふ

へ

ほ

む

め

も

ゆ

り

れ

ろ