CHAPTER 1

IronPort 電子メール セキュリティ アプライアンスをご使用の前に

この章は、次の内容で構成されています。

今回のリリースでの変更点

ここでは、AsyncOS for Email 7.3 の新機能および拡張機能について説明します。このリリースの詳細については、製品リリース ノートを参照してください。リリース ノートは、次の URL の IronPort カスタマー サポート ポータルから入手できます。

`http://www.ironport.com/support/login.html`

（注） このサイトにアクセスするには、サポート ポータルのアカウントが必要です。アカウントをお持ちでない場合は、[Support Portal] ログイン ページの [Request an Account] リンクをクリックします。通常、サポート ポータルにアクセスできるのは、IronPort のカスタマー、パートナー、および社員だけです。

以前のリリースのリリース ノートを見直して、これまでに追加された機能や拡張を確認すると役立つこともあります。サポート ポータルでこれらのリリース ノートを表示するには、該当するアプライアンスのマニュアル ページの [Earlier Releases] リンクをクリックします。

新機能：FIPS 準拠

AsyncOS for Email 7.3 では、FIPS 準拠の Hardware Security Module（HSM）カードを備えるセレクト Cisco IronPort 電子メール セキュリティ アプライアンスのサポートを提供します。

Federal Information Processing Standard（FIPS; 連邦情報処理標準）140 は、米国とカナダの連邦政府が共同で開発し、公表された標準です。機密情報であるが機密扱いされていない情報を保護するために、すべての政府機関で使用される暗号化モジュールの要件を規定しています。Cisco IronPort 電子メール セキュリティ アプライアンスとともに提供される HSM は、FIPS 140-2 レベル 2 標準に準拠した CAVIUM Nitrox XL CN15xx-NFBE 暗号化モジュールです。この標準は、秘密キーに不正使用防止のハードウェア キーストロークを使用するなど、暗号化操作で使用される情報の追加的な保護を規定します。

HSM カードでは、秘密キーのストレージの他に、アプライアンス用の暗号化処理を提供します。すべての暗号化操作は、HSM カードのセキュアな環境内で行われます。

電子メール セキュリティ アプライアンスが HSM カードを備え、AsyncOS 7.3 を使用する場合、すべての暗号化操作を FIPS に準拠した方法で動作する HSM カードに移行します。また、AsyncOS for Email 7.3 は、FIPS オフィサが HSM カードを設定して証明書および秘密キーを管理できる FIPS 管理コンソールも提供します。

詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「FIPS Management」の章を参照してください。

電子メール セキュリティ アプライアンスのマニュアル セット

電子メール セキュリティ アプライアンスには、次のマニュアルがあります。

- 『*Cisco IronPort AsyncOS for Email Daily Management Guide*』。このガイドでは、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、システム管理者が IronPort アプライアンスの管理およびモニタに使用する共通の日常タスクの実行につい

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介入する機能についての参考情報も記載します。

- 『*Cisco IronPort AsyncOS for Email Configuration Guide*』。このガイドは、新しく IronPort アプライアンスをセットアップし、電子メール配信機能を習得しようとするシステム管理者に推奨されるものです。既存のネットワーク インフラストラクチャへのアプライアンスの導入や電子メール ゲートウェイ アプライアンスとしてのセットアップについて説明します。また、電子メール パイプライン、ウイルス感染フィルタ、コンテンツ フィルタ、RSA Email DLP、電子メール暗号化、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の参考情報および設定手順についても説明します。
- 『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』。このガイドでは、IronPort アプライアンスの高度な機能を設定する手順について説明します。トピックとして、FIPS、LDAP と連携させるためのアプライアンスの設定、電子メール ポリシーを順守させ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への編成、およびアプライアンスのリスナーのカスタマイズがあります。このガイドでは設定の他に、メッセージ フィルタ ルールとアクション、コンテンツ ディクショナリとメッセージ フィルタ ルールで使用する正規表現、LDAP クエリーの構文と属性など、高度な機能の参考資料を提供します。
- 『*IronPort AsyncOS CLI Reference Guide*』。このガイドでは、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提供します。システム管理者は、IronPort アプライアンスでの CLI の使用時に参照用としてこのガイドを使用できます。

トピックの追加情報を得るために、このガイドから他のガイドを参照する場合があります。これらのガイドは、IronPort カスタマー サポート ポータルの他に、IronPort アプライアンスに付属の Documentation CD からも入手できます。詳細については、「シスコ サポート コミュニティ」（P.1-11）を参照してください。

このガイドの使い方

このガイドを情報源として使用し、IronPort アプライアンスの機能について学習します。トピックは論理的な順序で編成されています。本書内のすべての章を読む必要はありません。目次および「本書の構成」（P.1-5）の項を確認し、ご使用のシステムに関連する章を特定します。

また、このガイドを参考書として使用することもできます。ネットワークおよびファイアウォールの構成設定など、アプライアンスの使用期間を通して参照する可能性のある重要な情報が含まれています。

このガイドは、印刷版の他に、PDF ファイルおよび HTML ファイルで電子データとして配布されています。電子版のガイドは、IronPort カスタマー サポート ポータルで入手できます。また、アプライアンスの GUI の右上隅にある [Help and Support] リンクをクリックすると、本書の HTML オンライン ヘルプ バージョンにもアクセスできます。

始める前に

このガイドを読む前に、『*IronPort Quickstart Guide*』およびご使用のアプライアンスの最新の製品リリース ノートを確認します。このガイドでは、アプライアンスを梱包箱から取り出し、物理的にラックに取り付けて電源を投入済みであることを前提としています。

（注） すでにアプライアンスをネットワークに配線済みの場合は、IronPort アプライアンスのデフォルト IP アドレスが、ネットワーク上の他の IP アドレスと競合していないことを確認します。（IronPort X1050/1060、C650/660、および C350/350D/360 アプライアンスの）管理ポートまたは（IronPort C150/160 アプライアンスの）データ 1 ポートで事前に設定される IP アドレスは、`192.168.42.42` です。

本書の構成

第 1 章「IronPort 電子メール セキュリティ アプライアンスをご使用の前に」では、IronPort アプライアンスの概要について説明し、企業ネットワークにおけるその主な機能および役割を定義します。最新リリースの新機能について説明します。

第 2 章「概要」では、IronPort AsyncOS for Email について、および IronPort アプライアンスの GUI および CLI を使用した管理について説明します。CLI を使用するための表記法について説明します。この章では、汎用的な CLI コマンドの概要についても説明します。

第 3 章「セットアップおよび設置」では、IronPort アプライアンスへの接続オプションについて、ネットワーク計画、アプライアンスの初期システム セットアップと設定を含めて説明します。

第 4 章「電子メール パイプラインの理解」では、電子メール パイプラインの概要（IronPort アプライアンスで電子メールが処理されるときのフロー）を説明し、パイプラインを構成する機能について簡単に説明します。この説明には、各機能について詳細に説明しているセクションへの相互参照があります。

第 5 章「電子メールを受信するためのゲートウェイの設定」では、アプライアンスを電子メール ゲートウェイとして設定するプロセスについて説明します。この章では、着信電子メール トラフィックおよびメール フロー モニタをサポートする、インターフェイス、リスナー、および Host Access Table（HAT; ホスト アクセス テーブル）の概念について説明します。

第 6 章「電子メール セキュリティ マネージャ」では、IronPort アプライアンス上のすべての電子メール セキュリティ サービスおよびアプリケーションを管理する、単一で包括的なダッシュボードである電子メール セキュリティ マネージャについて説明します。電子メール セキュリティ マネージャを使用すると、ウイルス感染フィルタ機能、アンチスパム、アンチウイルスおよび電子メール コンテンツ ポリシーを、個別のインバウンドおよびアウトバウンド ポリシーを介して、受信者または送信者単位で管理できます。

第 7 章「評価フィルタリング」では、SenderBase 評価サービスのスコアを使用し、メッセージの送信者の評価に基づいて着信メールを制御する方法の概要を説明します。

第 8 章「アンチスパム」では、IronPort アプライアンスに統合された SenderBase 評価フィルタ、IronPort Anti-Spam、および IronPort Intelligent Multi-Scan の機能を使用して、スパムに対抗する独自のアプローチについて説明します。

第 9 章「アンチウイルス」では、IronPort アプライアンスに統合された Sophos および McAfee のアンチウイルス スキャン機能について説明します。

第 10 章「ウイルス感染フィルタ」では、ウイルス感染フィルタが新たな拡散に対して重要な最初のレイヤによる防御をプロアクティブに提供する方法を説明します。リアルタイムに新たな拡散を検出し、疑わしいトラフィックがネットワークに侵入するのを阻止するために動的に対処することにより、新しいシグニチャアップデートがデプロイされるまでの間、ウイルス感染フィルタによる保護が提供されます。

第 11 章「データ消失防止」では、RSA Security 社のデータ消失防止機能を使用して、組織の情報および知的財産を保護する方法、およびユーザが気付かずに機密データを電子メールで送信することを防ぐことによって、規制上および組織的なコンプライアンスを順守させる方法について説明します。

第 12 章「IronPort 電子メール暗号化」では、IronPort 暗号化アプライアンスまたはホステッド キー サービスを使用して、電子メールの暗号化に使用するプロセスについて説明します。

第 13 章「SenderBase Network Participation」では、SenderBase ネットワークを使用してアプライアンスからのデータを共有する方法について説明します。

第 14 章「テキスト リソース」では、AsyncOS のさまざまなコンポーネントで使用するコンテンツ ディクショナリ、通知テンプレート、免責事項などのテキスト リソースの作成について説明します。

第 15 章「システム管理」では、機能キーによる操作、AsyncOS のアップグレード、AsyncOS の復帰、日常のシステム メンテナンスの実行など、IronPort アプライアンスを管理およびモニタするための代表的な管理コマンドについて説明します。メンテナンス タスクには、システム時刻の設定、管理者パスワードの変更、およびシステムのオフライン化があります。この章では、DNS、インターフェイス、ルーティング、ホスト名の設定など、IronPort アプライアンスのネットワーク動作の設定方法についても説明します。

第 16 章「C300D/C350D/C360D アプライアンスのイネーブル化」では、IronPort C300D、C350D、および C360D のアプライアンスについて説明します。

第 17 章「IronPort M-Series セキュリティ管理アプライアンス」では、IronPort M-Series アプライアンスについて説明します。このアプライアンスは、重要なポリシーおよびランタイム データを集中管理および統合するために設計されており、管理者やエンドユーザにレポート作成の管理および情報の監査のための単一のインターフェイスを提供します。

付録 A「アプライアンスへのアクセス」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 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。

付録 B「ネットワーク アドレスと IP アドレスの割り当て」では、ネットワークおよび IP アドレスの割り当て関する全般的なルールについて説明し、企業ネットワーク インフラストラクチャ内で IronPort アプライアンスに接続する手段を示します。

付録 C「ファイアウォール情報」では、セキュリティ ファイアウォールの背後にある IronPort アプライアンスを適切に動作させるために、開く必要性が生じることがあるポートについて説明します。

付録 D「Cisco IronPort Systems, LLC ソフトウェア使用許諾契約書」には、IronPort 電子メール セキュリティ アプライアンスのソフトウェア使用許諾契約が含まれています。

『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』で説明されているトピック

『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』では、次のトピックについて説明しています。

第 1 章「FIPS Management」では、FIPS 準拠の C370 アプライアンスを暗号化動作用にセットアップするプロセスについて説明します。

第 2 章「Customizing Listeners」では、企業の電子メール ゲートウェイの設定を調整するためのプロセスについて説明します。この章では、ゲートウェイを通って受信する電子メールを処理するために、インターフェイスおよびリスナーを設定する際に使用できる高度な機能を詳細に説明します。

第 3 章「Configuring Routing and Delivery Features」では、電子メールのルーティングおよび IronPort アプライアンスを通過する電子メールの配信に作用する機能について説明します。

第 4 章「LDAP Queries」では、IronPort アプライアンスが社内の Lightweight Directory Access Protocol（LDAP）サーバに接続し、承認する受信者の確認（グループ メンバーシップなど）を目的としたクエリーの実行方法、メールのルーティングとアドレスの書き換え、ヘッダーのマスカレード、および SMTP 認証のサポートについて説明します。

第 5 章「Email Authentication」では、IronPort アプライアンスで電子メール認証を設定およびイネーブルにするプロセスについて説明します。IronPort AsyncOS は、発信メールに対する DomainKeys および DomainKeys Identified Mail（DKIM）の署名の他に、着信メールに対する Sender Policy Framework（SPF）、Sender ID Framework（SIDF）、DKIM の検証など、複数種類の電子メール認証をサポートします。

第 6 章「Using Message Filters to Enforce Email Policies」では、メッセージ フィルタを使用して、電子メールを処理するためのルールを定義する方法について説明します。添付ファイル フィルタリング、イメージ分析、およびコンテンツ ディクショナリの機能を使用してメッセージの内容を修正する機能についても説明します。

第 7 章「Advanced Network Configuration」には、NIC ペアリング、仮想 LAN などの情報が含まれています。

第 8 章「Centralized Management」では、複数のアプライアンスの管理および設定が可能な集中管理機能について説明します。集中管理機能により、ネットワーク内における信頼性、柔軟性、およびスケーラビリティが向上し、ローカル ポリシーに準拠しながら、グローバルに管理できるようになります。

付録 A「AsyncOS Quick Reference Guide」では、CLI のほとんどのコマンドのクイック リファレンスを提供します。

付録 B「Accessing the Appliance」では、IronPort アプライアンスからファイルを送信および取得するために 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。

『*Cisco IronPort AsyncOS for Email Daily Management Guide*』では、次のトピックが説明されています。

第 1 章「Managing the IronPort Email Appliance」では、IronPort アプライアンスの概要について説明し、企業ネットワークにおけるその主な機能および役割を定義します。

第 2 章「Using Email Security Monitor」では、企業のすべてのインバウンド電子メール トラフィックを全体的に確認できる高性能な 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「Tracking Email Messages」では、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して、特定のメッセージについて、配信、ウイルスの検出、またはスパム検疫が行われたかどうかを識別できます。

第 4 章「Quarantines」では、メッセージの保留および処理に使用される特別なキューまたはリポジトリについて説明します。検疫されたメッセージは、検疫の設定方法に基づいて配信したり削除したりできます。これには IronPort スパム検疫が含まれます。

第 5 章「Logging」では、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「Managing and Monitoring via the CLI」では、ゲートウェイを通過するメール フローのモニタ時に使用できる CLI のコマンドについて説明します。

第 7 章「Other Tasks in the GUI」では、GUI を使用して IronPort アプライアンスを管理およびモニタするための代表的な管理タスクについて説明します。

第 8 章「Common Administrative Tasks」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、IronPort アプライアンスの管理およびモニタのための代表的な管理コマンドについて説明します。この章は、テクニカル サポートの依頼方法、IronPort カスタマー サポートによるご使用の IronPort へのリモート アクセスの許可方法、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「Testing and Troubleshooting」では、システム パフォーマンスのテストおよび設定上の問題のトラブルシューティング用のいわゆる *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 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。画面上のコンピュータ出力。	`Please choose an IP interface for this Listener.` `sethostname` コマンドは、IronPort アプライアンスの名前を設定します。

AaBbCc123	ユーザ入力。画面上のコンピュータ出力と対比。	`mail3.example.com> commit`
		`Please enter some comments describing your changes:`
		`[]> Changed the system hostname`

AaBbCc123	マニュアル タイトル、新規用語、強調語句、およびコマンド ラインの変数。コマンド ラインの変数の場合、斜体のテキストが実際の名前や値のプレースホルダです。	『*IronPort Quickstart Guide*』をお読みください。
		
		IronPort アプライアンスは、発信パケットを送信するインターフェイスを一意的に選択できる*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`

その他の情報の入手先

Cisco IronPort では、IronPort 電子メール セキュリティ アプライアンスについて、より深く学ぶための次のリソースを提供しています。

シスコ サポート コミュニティ

シスコ サポート コミュニティは、シスコのカスタマー、パートナー、社員のためのオンライン フォーラムです。特定のシスコ製品に関する技術情報の他に、全般的な電子メールや Web セキュリティの話題をディスカッションする場を提供しています。フォーラムにトピックを投稿して質問したり、他のシスコ ユーザや Cisco IronPort ユーザと情報を共有したりできます。

シスコ サポート コミュニティには次の URL でアクセスします。

`https://supportforums.cisco.com`

Cisco IronPort 技術トレーニング

Cisco IronPort システム技術トレーニング サービスは、IronPort セキュリティ製品およびソリューションの評価、統合、デプロイ、保守、およびサポートを問題なく進めるうえで必要な知識と技術の習得を支援します。

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

トレーニング。登録およびトレーニング全般に関するご質問の場合：

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

認定。認定および認定試験に関するご質問の場合：

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

ナレッジ ベース

Cisco IronPort カスタマー サポート ページ上の IronPort ナレッジ ベースには、次の URL でアクセスできます。

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

（注） サイトにアクセスするには、シスコ サポート アカウントが必要です。アカウントをお持ちでない場合は、[Support] ページの [Register] リンクをクリックします。通常、[Support] ページ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。

ナレッジ ベースには、IronPort 製品関連トピックの情報が豊富に含まれています。

記事は通常、次のいずれかのカテゴリに分類されます。

- **手順。**この記事では、IronPort 製品で何かの処理を実行する方法を説明します。手順の記事では、たとえば、アプライアンスのデータベースのバックアップや復元の手順などを説明します。
- **問題とソリューション。**問題とソリューションの記事では、IronPort 製品の使用中に発生する可能性のある具体的なエラーや問題を扱います。問題とソリューションの記事では、たとえば、製品の新しい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に行うことなどを説明します。
- **参考情報。**参考情報の記事では通常、特定のハードウェアに関連するエラーコードなどの情報のリストを提供します。
- **トラブルシューティング。**トラブルシューティングの記事では、IronPort 製品に関する共通の問題を分析および解決する方法を説明します。トラブルシューティングの記事では、たとえば、DNS の問題が発生した場合に従う手順などを提供します。

ナレッジ ベースの各記事は、固有の回答 ID 番号が付いています。

Cisco IronPort カスタマー サポート

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

カスタマー サポート受付時間：月曜日から金曜日の 24 時間体制（米国の祝日を除く）。ご依頼から 1 時間以内にエンジニアから連絡を差し上げます。

カスタマー サポートの受付時間外で緊急対応が必要なクリティカルな問題を報告する場合は、次のいずれかの方法で IronPort までご連絡ください。

米国フリーダイヤル：1（877）641-4766

海外：`http://cisco.com/web/ironport/contacts.html`

サポート ページ：`http://cisco.com/web/ironport/index.html`

リセラーまたはその他の販売店を通してサポートを購入した場合、製品サポートに関するお問い合わせは購入先に直接ご連絡ください。

サード パーティ コントリビュータ

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

これらの契約内容の全文は次の URL を参照してください。

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

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

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

IronPort 電子メール セキュリティ アプライアンスの概要

IronPort 電子メール セキュリティ アプライアンスは、要求水準が最も高い企業ネットワークの電子メール インフラストラクチャのニーズを満たすために設計された高性能機器です。電子メール セキュリティ アプライアンスは、スパムおよびウイルスを排除し、社内ポリシーを順守させます。また、ネットワーク境界をセキュアに保ち、企業の電子メール インフラストラクチャの Total Cost of Ownership（TCO; 総所有コスト）を削減します。

IronPort システムは、ハードウェア、セキュリティの強化されたオペレーティング システム、アプリケーション、およびサポート サービスを組み合わせ、目的に合わせて構築された、企業のメッセージング専用のラックマウント サーバ アプライアンスを提供します。

IronPort AsyncOS™ オペレーティング システムは、複数のインテリジェントな機能を IronPort アプライアンスに統合します。

- SenderBase 評価フィルタと IronPort Anti-Spam を統合した独自のマルチレイヤ アプローチによるゲートウェイでの**アンチスパム**。

- Sophos および McAfee のアンチウイルス スキャン エンジンによるゲートウェイでの**アンチウイルス**。
- 新たなウイルスの拡散に対して IronPort 独自の予防的な保護機能である**ウイルス感染フィルタ** TM。新しいアンチウイルスのアップデートが適用されるまでの間、危険なメッセージを検疫でき、新たなウイルス拡散を招く脆弱性の露出を抑えます。
- 検疫されたスパムおよび陽性と疑わしいスパムへのエンドユーザ アクセスを提供する、オンボックスまたはオフボックスの**スパム検疫**。
- **電子メール認証**。IronPort AsyncOS は、発信メールに対する DomainKeys および DomainKeys Identified Mail（DKIM）の署名の他に、着信メールに対する Sender Policy Framework（SPF）、Sender ID Framework（SIDF）、DKIM の検証など、さまざまな形式の電子メール認証をサポートします。
- **IronPort 電子メール暗号化**。HIPAA、GLBA、および同様の規制要求に対応するために発信メールを暗号化できます。これを行うには、電子メール セキュリティ アプライアンスで暗号化ポリシーを設定し、ローカル キー サーバまたはホステッド キー サービスを使用してメッセージを暗号化します。
- アプライアンス上のすべての電子メール セキュリティ サービスおよびアプリケーションを管理する、単一で包括的なダッシュボードである**電子メール セキュリティ マネージャ**。電子メール セキュリティ マネージャは、ユーザ グループに基づいて電子メール セキュリティを実施でき、インバウンドとアウトバウンドの独立したポリシーを使用して、IronPort 評価フィルタ、ウイルス感染フィルタ、アンチスパム、アンチウイルス、および電子メール コンテンツ ポリシーを管理できます。
- 電子メール ポリシーに違反したメッセージを保持する**オンボックス検疫エリア**。検疫とウイルス感染フィルタ機能は、シームレスに相互作用します。
- **オンボックスのメッセージ トラッキング**。AsyncOS for Email には、電子メール セキュリティ アプライアンスが処理するメッセージのステータスの検索が容易にできる、オンボックスのメッセージ トラッキング機能があります。
- 企業のすべての電子メール トラフィックを全体的に確認できる、すべてのインバウンドおよびアウトバウンドの電子メールに対する**メール フロー モニタ機能**。
- 送信者の IP アドレス、IP アドレス範囲、またはドメインに基づいた、インバウンドの送信者の**アクセス コントロール**。

- 広範な**メッセージ フィルタリング** テクノロジーを使用して、社内ポリシーを順守させ、企業のインフラストラクチャを出入りする特定のメッセージに作用させることができます。フィルタ ルールでは、メッセージまたは添付ファイルの内容、ネットワークに関する情報、メッセージ エンベロープ、メッセージ ヘッダー、またはメッセージ本文に基づいてメッセージを識別します。フィルタ アクションでは、メッセージをドロップ、バウンス、アーカイブ、ブラインド カーボン コピー、または変更したり、通知を生成したりできます。
- **セキュアな SMTP over Transport Layer Security 経由のメッセージの暗号化**により、企業のインフラストラクチャとその他の信頼できるホストとの間でやりとりされるメッセージが暗号化されるようなります。
- **Virtual Gateway™** テクノロジーにより、IronPort アプライアンスは、単一サーバ内で複数の電子メール ゲートウェイとして機能できるため、さまざまな送信元またはキャンペーンの電子メールを、それぞれ独立した IP アドレスを通して送信するように分配できます。これにより、1 つの IP アドレスに影響する配信可能量の問題が、他の IP アドレスに及ばないようにします。

AsyncOS for Email は、インターネット メッセージングのタスク用に高度に最適化された専用のオペレーティング システムです。AsyncOS は、「セキュリティの強化された」オペレーティング システムです。不要なすべてのサービスは取り除かれ、セキュリティの向上とシステム パフォーマンスの最適化が図れています。IronPort のスタックレスなスレッディング テクノロジーにより、各タスクに対する専用メモリ スタックの割り当ては行われず、MTA の同時並行性と安定性が向上します。従来のオペレーティング システムでの CPU の割り込み型タイム スライシングと比べ、カスタム I/O 駆動型スケジューラは、電子メール ゲートウェイで要求される大量の並列 I/O イベントに対して最適化されています。AsyncOS の基礎となるファイル システムの AsyncFS は、何百万もの小さいファイルを扱うために最適化され、システム障害が発生した場合のデータの復元性を確保します。

AsyncOS for Email は、メッセージを受け入れて配信するために、RFC 2821 準拠の Simple Mail Transfer Protocol（SMTP; シンプル メール転送プロトコル）をサポートします。IronPort アプライアンスは、設定と管理を簡易化するように設計されています。レポート作成コマンド、モニタリング コマンド、およびコンフィギュレーション コマンドのほとんどは、HTTP 経由でも HTTPS 経由でも Web ベースの GUI から使用できます。さらに、Secure Shell（SSH; セキュア シェル）、Telnet、または直接シリアル接続でアクセスするインタラクティブな Command Line Interface（CLI; コマンド ライン インターフェイス）がシステムに用意されています。IronPort アプライアンスには、確実なロギング機能もあり、システム全体の機能にわたるログ サブスクリプションを設定して、必要な

情報を見つけるために費やす時間を削減します。

メール フローおよび IronPort M-Series アプライアンス

M-Series アプライアンスが構成に含まれている場合、他の IronPort（C-Series および X-Series）アプライアンスから IronPort M-Series アプライアンスにメールが送信されます。IronPort M-Series アプライアンスにメールを送信するように設定された IronPort アプライアンスは、その M-Series アプライアンスからリリースされるメールの受信を自動的に予測し、このようなメッセージを逆戻りして受信した場合は再処理を行いません。メッセージは、HAT などのポリシーやスキャン設定をバイパスして配信されます。これを機能させるために、IronPort M-Series アプライアンスの IP アドレスが変わらないようにしてください。IronPort M-Series アプライアンスの IP アドレスが変わると、受信側の C-Series または X-Series のアプライアンスは、メッセージを他の着信メッセージであるものとして処理します。IronPort M-Series アプライアンスでの受信および配信には、常に同じ IP アドレスを使用します。

IronPort M-Series アプライアンスでは、IronPort スパム検疫設定で指定されている IP アドレスから検疫対象のメールを受け入れます。IronPort M-Series アプライアンスでローカル検疫を設定するには、『*IronPort AsyncOS for Security Management User Guide*』を参照してください。IronPort M-Series アプライアンスのローカル検疫エリアは、そこにメールを送信する他の IronPort アプライアンスからは、*外部*検疫エリアとして参照されることに注意してください。

IronPort M-Series アプライアンスによって解放されたメールは、スパム検疫設定の定義に従って、プライマリ ホストおよびセカンダリ ホスト（IronPort アプライアンスまたは他のグループウェア ホスト）に配信されます（『*IronPort AsyncOS for Security Management User Guide*』を参照）。したがって、IronPort M-Series アプライアンスにメールを配信する IronPort アプライアンスの数に関係なく、解放されるすべてのメール、通知、およびアラートが単一のホスト（グループウェアまたは IronPort アプライアンス）に送信されます。IronPort M-Series アプライアンスからの配信によってプライマリ ホストが過負荷にならないように注意してください。