



CHAPTER 1

セキュリティ管理アプライアンスをご使用の前に

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

- [今回のリリースでの変更点](#)
- [はじめる前に](#)
- [セキュリティ管理アプライアンスの概要](#)

今回のリリースでの変更点

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

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

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

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

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

機能	説明
新機能：	
新規の電子メールセキュリティ機能に対するレポーティングおよびメッセージトラッキングのサポート	<p>AsyncOS 7.6 for Email Security の次の新機能が、[Centralized Reporting] または [Centralized Message Tracking]、あるいはその両方でサポートされています。</p> <ul style="list-style-type: none"> レポーティング、トラッキング、および Cisco IronPort Spam Quarantine での IPv6 経由で送品されたメッセージに対するサポート。 (今回のリリースでは、セキュリティ管理アプライアンスのすべてのインターフェイスで引き続き IPv4 が使用されます)。 送信者ごとのレート制限に対するレポーティングおよびメッセージトラッキングのサポート。 これには、新規の中央集中型レート制限レポートが含まれます。このレポートでは、組織で受信された大量の電子メールメッセージの上位送信者を識別できます。 メッセージトラッキングにおける、新規の [Quarantine a copy and deliver] 機能で処理されるメッセージの識別。これにより、メッセージに対する措置を取ることなく、データ消失防止違反をモニタできます。 <p>これらのレポートの基礎をなす機能の一般的な情報については、『Release Notes for Cisco IronPort AsyncOS 7.6 for Email Security』を参照してください。</p> <p>中央集中型電子メールセキュリティレポーティングの使用の章の検索およびインタラクティブ電子メールレポートページと [Rate Limits] ページ、および 電子メールメッセージのトラッキングの章の電子メールメッセージの検索も参照してください。</p>
アップグレードとサービスアップデートに対する異なるサーバ設定	<p>イメージサーバとリストサーバの両方について、アップグレードとアップデートで別個のダウンロードサーバ設定を指定できるようになりました。</p> <p>たとえば、AsyncOS のアップグレード用にローカルサーバ、サービスアップデート用に Cisco IronPort アップデートサーバをそれぞれ指定できます。これにより、サービスアップデートを即時利用できるようにしながら、アップグレードのタイミングを制御することが可能になります。</p> <p>詳細については、一般的な管理タスクの章のアップグレードおよびサービスアップデートの設定を参照してください。</p>
ルートログインを防止する機能	<p>現在、ルートレベルの SSH アクセスはデフォルトでディセーブルになりますが、Cisco IronPort サポート担当者がアクセスできるよう、必要に応じてイネーブルにすることができます。</p>
拡張機能：	
拡張対象： DLP トラッキング権限に対するきめ細かな制御	<p>メッセージトラッキングにおける機密のデータ消失防止情報に対するユーザの役割でのアクセスを制限できるようになりました。</p> <p>詳細については、管理タスクの分散の章のメッセージトラッキングでの DLP 機密情報へのアクセスの制御を参照してください。</p>

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

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

はじめる前に

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

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

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



(注)

すでにアプライアンスをネットワークに配線済みの場合は、IronPort アプライアンスのデフォルト IP アドレスが、ネットワーク上の他の IP アドレスと競合していないことを確認します。各アプライアンスの管理ポートに事前に設定されている IP アドレスは、192.168.42.42 です。

詳細情報の入手先

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

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

ドキュメント セット

マニュアルは、PDF ファイルおよび HTML ファイルとして配布されます。このマニュアルの電子バージョンは、Cisco IronPort カスタマー サポート サイトで入手できます。また、右上の [Help and Support] をクリックすることにより、アプライアンスの GUI からユーザ ガイドの HTML オンライン ヘルプ バージョンに直接アクセスできます。

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

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

このドキュメントおよびその他のドキュメントは、次の場所にあります。

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

トレーニングと認定試験

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

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

ナレッジ ベース

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

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



(注)

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

ナレッジ ベースには、Cisco IronPort 製品に関するトピックについて豊富な情報が用意されています。一般に、項目は次のカテゴリのいずれかに分類されています。

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

シスコ サポート コミュニティ

シスコ サポート コミュニティは、シスコのお客様、パートナー、および従業員のオンライン フォーラムです。電子メールおよび Web セキュリティに関する一般的な問題や、特定のシスコ製品に関する技術情報について話し合う場を提供します。フォーラムにトピックを投稿して質問したり、他のシスコ ユーザや Cisco IronPort ユーザと情報を共有したりできます。

シスコ サポート コミュニティには次の URL からアクセスできます。

<https://supportforums.cisco.com>

シスコのテクニカル サポート

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

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

以下を含むさまざまな作業にこの Web サイトが役立ちます。

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

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

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

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

サードパーティ コントリビュータ

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

契約の全文については、次の URL を参照してください。

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

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

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

マニュアルに関するフィードバック

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

セキュリティ管理アプライアンスの概要

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

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

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

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

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

セキュリティ管理アプライアンスは、電子メール セキュリティ アプライアンスおよび Web セキュリティ アプライアンスから最大のパフォーマンスを確保し、導入の柔軟性を高めることによって企業ネットワークの整合性を保護します。1 台のセキュリティ管理アプライアンスからのセキュリティ操作を調整することも、複数のアプライアンス間に負荷を分散させることもできます。

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



(注)

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

セキュリティ管理アプライアンスでサポートされるサービス

セキュリティ管理アプライアンスは、次のサービスをサポートしています。

- [電子メール セキュリティ管理](#)
- [Web セキュリティ管理](#)
- [追加機能](#)

電子メール セキュリティ管理

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

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

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

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

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

セキュリティ管理アプライアンスにおける電子メールセキュリティアプライアンスの制御は、中央集中型管理機能を介して提供されます。電子メールセキュリティアプライアンスで使用できるこの機能によって、一貫性と結合性のあるポリシーを一元的に管理できます。管理者は、ユーザ、LDAP グループメンバーシップ、またはドメインメンバーシップに応じて、固有のポリシーを設定することによって、モニタリングタスクを振り分けることができます。

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

Web セキュリティ管理

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

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

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

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

追加機能

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

- **外部 Cisco IronPort スパム隔離** : エンドユーザ向けのスパムメッセージおよび陽性と疑わしいスパムメッセージを保持しており、エンドユーザおよび管理者は、スパムとフラグ付けされたメッセージをレビューしてから最終的な決定を下すことができます。
- **中央集中型レポート** : 複数の電子メールおよび Web セキュリティアプライアンスから集約したデータに対してレポートを実行します。
- **中央集中型トラッキング** : 複数の電子メールおよび Web セキュリティアプライアンスを通過する電子メールおよび Web メッセージを追跡します。

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