CHAPTER 1

Security Management アプライアンスをご使用の前に

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

ここでは、次の内容について説明します。

Security Management アプライアンスの概要

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

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

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

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

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

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

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

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

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

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

Security Management アプライアンスは、次のサービスをサポートしています。

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

電子メール セキュリティ管理

電子メール管理者にとって、ネットワークを把握することは電子メールの管理に非常に重要であり、レポーティングによって可能になります。電子メール レポートは、電子メール管理者にとって次の 2 つの重要な機能を果たします。

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

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

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

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

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

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

Web セキュリティ管理

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

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

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

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

追加機能

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

- **外部 Cisco IronPort スパム検疫：**エンドユーザ向けのスパム メッセージおよび陽性と疑わしいスパム メッセージを保持しており、エンドユーザおよび管理者は、スパムとフラグ付けされたメッセージをレビューしてから最終的な決定を下すことができます。
- **中央集中型レポーティング：**複数の電子メールおよび Web セキュリティ アプライアンスからの集約データに対してレポートを実行します。
- **中央集中型トラッキング：**複数の電子メールおよび Web セキュリティ アプライアンスを通過する電子メールと Web メッセージを追跡します。
- **Cisco IronPort 中央集中型コンフィギュレーション マネージャ：**複数の Email Security アプライアンスおよび Web セキュリティ アプライアンスに対するポリシー定義とポリシーの展開を管理します。

今回のリリースでの変更点

ここでは、AsyncOS 7.7 for Security Management の新機能および拡張機能について説明します。このリリースの詳細については、次の URL で入手できる製品リリース ノートを参照してください。

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

以前のリリースのリリース ノートで、以前に追加された機能や拡張機能を確認すると役立つ場合もあります。上記のリンクで、すべてのリリースのリリース ノートを入手できます。

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

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

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

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

機能	説明
IP-Based アクセス	AsyncOS 7.7 では、Security Management アプライアンスにアクセスするユーザの IP アドレスを制御できます。ユーザは、定義したアクセス リストの IP アドレスを持つすべてのマシンから、アプライアンスにアクセスできます。組織のネットワークで、リモート ユーザのマシンと Security Management アプライアンスの間で逆プロキシが使用されている場合、AsyncOS 7.7 では、アプライアンスに接続できるプロキシの IP アドレスのアクセス リストを作成できます。 詳細については、「IP ベースのネットワーク アクセスの設定」の項を参照してください。
Web UI セッション タイムアウト	AsyncOS 7.7 では、Security Management アプライアンスの Web UI から AsyncOS が、非アクティブなユーザをログアウトするまでの時間を指定できます。この Web UI セッション タイムアウトは、admin を含めて、すべてのユーザに適用され、また HTTP セッションと HTTPS セッションの両方に使用されます。 詳細については、「Web UI セッション タイムアウトの設定」の項を参照してください。
パケット キャプチャ	AsyncOS 7.7 ではパケット キャプチャ制御が提供されており、アプライアンスが接続されたネットワークで送受信されている TCP/IP と他のパケットを傍受および表示できます。この機能を使用すると、ネットワーク設定をデバッグし、アプライアンスに到達する、またはアプライアンスから送出されるネットワーク トラフィックを検出できます。 詳細については、「パケット キャプチャ」の項を参照してください。
時間帯の更新	AsyncOS 7.7 からは、AsyncOS のアップグレードとは独立して時間帯ファイルを更新できるようになりました。[Management Appliance] > [System Administration] > [Time Settings] ページで、時間帯ファイルの更新を確認し、手動で時間帯を更新できます。 詳細については、「時間帯ファイルの更新」の項を参照してください。
機能拡張：	
ウイルス感染フィルタ レポート	ウイルス感染フィルタ レポートが拡張され、名前が感染フィルタ レポートに変更されました。現在、このレポートには、マルウェアの配布、詐欺、およびフィッシングの試行に関する情報が含まれます。 詳細については、「[Outbreak Filters] ページ」の項を参照してください。

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

機能	説明
PDF レポートの機能拡張	AsyncOS 7.7 の新機能として、英語以外の言語で PDF レポートを生成できます。また、すべての非 ASCII 文字を PDF レポートに正しく出力できます。現在、複数のレポートを含む PDF レポートに、PDF の先頭へのリンクが含まれるようになりました。 詳細については、「電子メール レポーティング ページの概要」の項を参照してください。
添付ファイルの検索	AsyncOS 7.7 では、[Message Tracking] でメッセージを添付ファイル名によって検索できます。 詳細については、第 6 章「電子メール メッセージのトラッキング」を参照してください。

このマニュアルの使い方

このガイドを情報源として使用し、Cisco IronPort アプライアンスの機能について学習します。項目は、論理的な順序に整理されています。必ずしもマニュアルのすべての章を通読する必要はありません。目次を参照して、お使いのシステムに関連する章を確認してください。

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

このマニュアルは、印刷物として配布されます。また、PDF ファイル、HTML など電子的にも配布されます。このマニュアルの電子バージョンは、Cisco IronPort カスタマー サポート ポータルで入手できます。また、右上の [Help and Support] をクリックすることにより、アプライアンスの GUI からマニュアルの HTML オンライン ヘルプ バージョンに直接アクセスできます。

はじめる前に

このマニュアルを読み始める前に、『*IronPort Quickstart Guide*』およびアプライアンスの最新の製品リリース ノートを確認してください。このマニュアルは、アプライアンスが開梱されてラックに設置され、電源がオンされていることを前提としています。

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

Email Security アプライアンス

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

- X1000T
- C650
- C350

Cisco IronPort X1050、C650、および C350 アプライアンスには、構成（オプションの光ネットワーク インターフェイスがあるかどうか）に応じて最大 4 個のイーサネット インターフェイスがシステムの背面パネルにあります。次のラベルが付いています。

- Management
- Data1
- Data2
- Data3
- Data4

Web セキュリティ アプライアンス

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

- S1050

- S650
- S350

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

- M1
- P1
- P2
- T1
- T2

Security Management アプライアンス

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

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

表記法

コマンドの説明では、次の表記法を使用しています。

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

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

例を挙げて説明する場合は、次の表記法を使用しています。

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

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

詳細情報の入手先

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

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

ドキュメント セット

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

- すべての製品のリリース ノート
- 『Quickstart Guide』と『Getting Started Guide』
- 『*Cisco IronPort AsyncOS for Security Management ユーザ ガイド*』（本書）

- 『*Cisco IronPort AsyncOS for Web Security User Guide*』
- Cisco IronPort AsyncOS for Email Security のユーザ ガイド：
  - 『*Cisco IronPort AsyncOS for Email Security Configuration Guide*』
  - 『*Cisco IronPort AsyncOS for Email Security Advanced Configuration Guide*』
  - 『*Cisco IronPort AsyncOS for Email Security Daily Management Guide*』
- 『*Cisco IronPort AsyncOS CLI Reference Guide*』
- 安全性および準拠性に関する情報
- プラグインおよび API のマニュアル
- ハードウェアおよびファームウェアに関する情報
- ホワイト ペーパー
- ソリューションのマニュアル

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

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

マニュアルの内容	入手場所
Security Management アプライアンス	http://www.cisco.com/en/US/products/ps10155/tsd_products_support_series_home.html
Email Security アプライアンスおよび CLI リファレンス ガイド	http://www.cisco.com/en/US/products/ps10154/tsd_products_support_series_home.html
Web セキュリティ アプライアンス	http://www.cisco.com/en/US/products/ps10164/tsd_products_support_series_home.html

Cisco IronPort 技術トレーニング

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

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

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

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

認定：証明書および認定試験に関するお問い合わせ先は次のとおりです。

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

ナレッジ ベース

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

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

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

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

一般に、項目は次のカテゴリのいずれかに分類されています。

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

- **トラブルシューティング：**トラブルシューティングの項目では、Cisco IronPort 製品に関連する一般的な問題を分析し、解決する方法について説明します。たとえば、DNS で問題が発生した場合に実行する手順を示します。

シスコ サポート コミュニティ

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

シスコ サポート コミュニティには次の URL からアクセスできます。

https://supportforums.cisco.com

Cisco IronPort カスタマー サポート

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

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

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

U.S. フリー ダイヤル：1 (877) 646-4766

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

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

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

サード パーティ コントリビュータ

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

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

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

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

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

Cisco IronPort に対するコメントの送付

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

contentsecuritydocs@cisco.com

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