CHAPTER 1

スタートアップ ガイド

今回のリリースでの変更点

ここでは、AsyncOS for Cisco Content Security Management のこ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

アップグレードする場合、以前のリリースとこのリリースの間の他のリリースのリリース ノートも確認する必要があります。これは、これらのリリースで追加された機能および拡張機能を確認するためです。

機能	説明
リリース 8.1.1 の新機能：	
新しいハードウェアのサポート	このリリースでは、新しい M380 および M680 ハードウェアをサポートします。
リモート電源管理	この機能は M380 および M680 ハードウェアでのみ使用可能です。 アプライアンス シャーシの電源をリモートからリセットできるようになりました。 必要なときにこの機能を使用できるようにするには、事前にこの機能を設定する必要があります。「リモート電源管理のイネーブル化」（P.14-6）および「リモートからのアプライアンス電源のリセット」（P.16-6）を参照してください。
リリース 8.1.0 の新機能：	

機能	説明
集約ポリシー、ウイルス、およびアウトブレイク隔離	次の隔離がシスコのコンテンツ セキュリティ管理アプライアンスにまとめて集約されます。 • ウイルス対策 • アウトブレイク • 以下によって捕らえられるメッセージに使用されるポリシー隔離 – メッセージ フィルタ – コンテンツ フィルタ – データ漏洩防止ポリシー これらの隔離の集約には次の利点があります。 • 管理者は 1 か所で複数の電子メール セキュリティ アプライアンスからの隔離済みメッセージを管理できます。 • 隔離されたメッセージは、DMZ 内ではなくファイアウォールの背後に保存され、セキュリティ リスクを減らします。 • 集約隔離は、シスコのコンテンツ セキュリティ管理アプライアンスの標準バックアップ機能の一部としてバックアップされることができます。 詳細については、第 8 章「集約ポリシー、ウイルス、およびアウトブレイク隔離」を参照してください。
[お気に入り（My Favorites）] リスト	頻繁に使用するページをお気に入りページのクイック アクセス メニューに追加します。 詳細については、「お気に入りページの使用」（P.14-57）を参照してください。
バックグラウンドでのアップグレードのダウンロード	バックグラウンドでアップグレードをダウンロードしておき、後でインストールすることができ、サービスの中断を最小限に抑えることができます。 詳細については、「AsyncOS のアップグレード」（P.14-18）を参照してください。
以前のコンフィギュレーションへのロールバック	現在のコンフィギュレーションを以前のコンフィギュレーションに設定して、そのコンフィギュレーション以降のすべてのコンフィギュレーション変更をロールバックできます。 詳細については、「以前コミットしたコンフィギュレーションへのロールバック」（P.14-52）を参照してください。
最近のアラートの表示	アラート電子メールが配信されていなかったりまたは削除されていてもアプリケーションの最近のアラートのリストを表示できます。 詳細については、「最新アラートの表示」（P.14-35）を参照してください。

機能	説明
レポート作成機能の拡張	レポート作成機能の拡張により、以下が可能になります。 • 頻繁に参照するグラフやテーブルを使用したカスタム ページを作成します。詳細については、「カスタム レポート」（P.3-7）を参照してください。 • データ漏洩防止またはコンテンツ フィルタリング ポリシーに違反するメッセージのメッセージ トラッキング データを表示するためにレポート内のリンクをクリックします。この機能拡張により、こうした違反の調査パターンと根本原因を簡素化します。 さらに、Common Access Card（CAC）を使用している組織用に、クライアント証明書のある SMTP セッション認証を使用して受信したメッセージのデータの概要を新しい受信 SMTP 認証レポートに示します。
メッセージ トラッキング機能拡張	• 現在、次に対するメッセージ トラッキングを検索できます。 – UTF-8 符号化された件名のメッセージ – なんらかの隔離状態にあるメッセージ – コンテンツ フィルタで検出されたメッセージ • メッセージ トラッキングの検索結果およびメッセージの詳細にはメッセージが保存されている隔離のメッセージ詳細ページへのリンクが含まれるようになりました。 • メッセージ トラッキング クエリーから 1000 件以上のメッセージが返された場合、他のツールを使用した分析のためにカンマ区切り値ファイルとしてクエリーに一致する最大 50,000 件のメッセージをエクスポートできます。 • メッセージ トラッキングには、Common Access Card（CAC）を使用している組織用に、クライアント証明書のある SMTP セッション認証を使用して受信したメッセージのデータを含みます。
より柔軟なパスワードの長さのサポート	文字数ゼロも含め任意の長さのアプライアンスのパスワードがサポートされるようになりました。 詳細については、「パスワードの設定およびログインの要件」（P.13-13）を参照してください。
SNMP トラップの向上	linkUp および linkDown の SNMP トラップは、標準 RFC 実装（RFC-3418）に置き換えられました。
スパム隔離の向上	スパム隔離の検索結果の表示が、より簡単になりました。

詳細情報の入手先

- 「Cisco 通知サービス」（P.1-4）
- 「マニュアル」（P.1-4）
- 「トレーニングと認定試験」（P.1-5）
- 「ナレッジ ベース」（P.1-5）
- 「シスコ サポート コミュニティ」（P.1-6）
- 「シスコのテクニカル サポート」（P.1-6）

- 「サード パーティ コントリビュータ」（P.1-5）
- 「シスコ アカウントの登録」（P.1-6）

Cisco 通知サービス

セキュリティ アドバイザリ、フィールド ノーティス、販売終了とサポート終了の通知、およびソフトウェア アップデートと既知の問題に関する情報などのシスコのコンテンツ セキュリティ アプライアンスに関連する通知が配信されるように署名して参加します。

受信する情報通知の頻度やタイプなどのオプションを指定できます。使用する製品ごとの通知に個別に参加する必要があります。

参加するには、次に移動します。http://www.cisco.com/cisco/support/notifications.html

Cisco.com アカウントが必要です。ない場合は、「シスコ アカウントの登録」（P.1-6）を参照してください。

マニュアル

この製品および関連製品のマニュアルは、次の Web サイトで入手可能です。

シスコのコンテンツ セキュリティ製品のマニュアル	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
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
電子メール セキュリティ アプライアンス	http://www.cisco.com/en/US/products/ps10154/tsd_products_support_series_home.html
コンテンツ セキュリティ製品用コマンドライン リファレンス ガイド	http://www.cisco.com/en/US/products/ps10154/prod_command_reference_list.html
Cisco IronPort 暗号化	http://www.cisco.com/en/US/partner/products/ps10602/tsd_products_support_series_home.html

また、右上の [ヘルプとサポート（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。

シスコ コンテンツ セキュリティ 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
- 『The *Quick Start Guide* for the Cisco Content Security Management appliance』
- *AsyncOS 8.1 for Cisco Content Security Management ユーザ ガイド*（このマニュアル）
- *『Cisco IronPort AsyncOS for Web Security User Guide』*
- Cisco AsyncOS for Email Security のドキュメント：

  Email Security リリース 8.0 以降：

  - 『*Cisco AsyncOS for Email User Guide*』

  Email Security リリース 8.0 より前：

  - 『*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 AsyncOS CLI Reference Guide*』

サード パーティ コントリビュータ

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、シスコのライセンス契約に含まれています。

サードパーティのライセンスに関する情報は、次の場所にあるライセンシング ドキュメントで利用できます。http://www.cisco.com/en/US/products/ps10155/prod_release_notes_list.html および https://support.ironport.com/3rdparty/AsyncOS_User_Guide-1-1.html

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。

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

シスコ コンテンツ セキュリティ製品に関する情報についてのナレッジ ベースにアクセスするには、以下の場所を参照してください。

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 ユーザ ID がない場合は、「シスコ アカウントの登録」（P.1-6）を参照してください。

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。コンテンツ 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。このフォーラムにトピックを投稿して質問したり、他の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。

- 電子メール セキュリティと関連管理：
  https://supportforums.cisco.com/community/netpro/security/email
- Web セキュリティと関連管理：
  https://supportforums.cisco.com/community/netpro/security/web

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

シスコ アカウントの登録

Cisco.com の多数のリソースへアクセスするには、シスコのアカウントが必要です。

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。

関連項目

- 「Cisco 通知サービス」（P.1-4）
- 「ナレッジ ベース」（P.1-5）

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。

シスコのコンテンツ セキュリティ管理の概要

AsyncOS for Cisco Content Security Management には次の機能が統合されています。

- **外部スパム隔離**：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。
- **集約ポリシー、ウイルス、アウトブレイク隔離**：これらの隔離および複数の電子メール セキュリティ アプライアンスから隔離内に隔離されたメッセージを管理するための単一のインタフェースを提供します。隔離されたメッセージをファイアウォールの背後に保存できます。
- **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集約したデータに対してレポートを実行します。個別アプライアンスで使用できる同じレポーティング機能を、セキュリティ管理アプライアンスでも使用できます。また、セキュリティ管理アプライアンスでのみ使用できる、Web セキュリティの拡張レポートがいくつかあります。
- **中央集中型トラッキング**：単一のインターフェイスを使用して、電子メール メッセージを追跡すること、および複数の電子メールおよび Web セキュリティ アプライアンスにより処理された Web トランザクションを追跡することができます。
- **中央集中型コンフィギュレーション管理**：簡易性および一貫性のために、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展開を管理できます。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 バージョンを実行するアプライアンスにプッシュできます。
- **データのバックアップ**：レポーティング データ、トラッキング データ、隔離されたメッセージ、安全な送信者とブロックされた送信者のリストなど、セキュリティ管理アプライアンスのデータをバックアップできます。

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。

（注） セキュリティ管理アプライアンスは、集約電子メール管理または電子メール セキュリティ アプライアンスの「クラスタリング」には関係ありません。