はじめに

この章は、次の項で構成されています。

今回のリリースでの新機能

ここでは、AsyncOS for Secure Email and Web Manager 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。

表 *1 : AsyncOS 15.0* の新機能

機能	説明
（オンプレミスのみ）FIPS 認定	Cisco Secure Email and Web Manager は FIPS 認定され、FIPS 140-2 認定の暗号化モジュール、Cisco Common Crypto Module を統合しました（FIPS 140-2 認定 #4036）。 （注） Cisco Secure Email and Web Manager の FIPS 認定は、電子メールゲートウェイの統合にのみ適用され、Cisco Secure Web Appliance の統合には適用されません。 （注） Cisco Secure Email and Web manager が FIPS モードの場合、TLS v1.0 方式はサポートされません。 詳細については、FIPS 管理を参照してください。

機能	説明
単一ログライン（SLL）	SLL 機能は、電子メールトラッキングデータを単一ログラインまたはフラット化モデルとして作成、インデックス付け、および保存します。したがって、クエリを実行してすぐに応答を取得できます。この機能は、高速応答、低メモリ、および CPU 使用率により、トラッキングクエリまたは検索のパフォーマンスを向上させます。 この機能は、アップグレード後の電子メールトラッキングデータにのみ適用されます。
CRL ソースの設定	Cisco Secure Email and Web Manager は、ユーザーの証明書が失効していないことを確認するために、証明書検証の一環として証明書失効リスト（CRL）と呼ばれる失効した証明書のリストを確認します。サーバー上でこのリストを最新のバージョンに保つ必要があります。Cisco Secure Email and Web Manager は、ユーザーが作成したスケジュールでこれをダウンロードします。リストは手動で更新することもできます。 次の方法を使用して CRL ソースを設定できます。 • レガシー Web インターフェイスで、[ネットワーク（Network）] > [CRL ソース（CRL Sources）] > [CRL ソースの追加（Add CRL Source）] > [CRL（証明書失効リスト）ソースの追加（Add CRL (Certificate Revocation Lists) Source）] ウィンドウに移動します。 • CLI の `Certconfig` > `CRL` サブコマンドを使用します。 CRL ソースの設定の詳細については、CRL ソースの設定を参照してください。

機能	説明
古い Splunk データの削除	

機能	説明
	Cisco Secure Email and Web Manager 15.0 以降にアップグレードし、電子メールトラッキングデータが Splunk データベースに含まれている場合、アップグレードを続行すると、システムによって Splunk データベースとバイナリが削除されます。 （注） Cisco Secure Email and Web Manager 13.6.2 リリース以降、Splunk データベースは電子メールトラッキングデータの保存に使用されなくなりました。新しい電子メールトラッキングデータはすべて、Lucene データベースに保存されます。Cisco Secure Email and Web Manager 15.0 にアップグレードすると、Cisco Secure Email and Web Manager 13.6.2 へのアップグレード前のすべてのトラッキングデータが削除され、回復できなくなります。 Cisco Secure Email and Web Manager 15.0 以降へのアップグレード中に、システムが Splunk データベースを削除することを示す警告メッセージが、CLI または Cisco Secure Email and Web Manager の Web インターフェイスに表示されます。 **警告メッセージの例** *"From the Secure Email and Web Manager 13.6.2 version onwards, we have moved to a newer storage system for email tracking data. Generally, the old data is replaced with new data in the new storage system automatically. However, in some scenarios (for example, late upgrades, low mail flow and tracking data, and so on), there could be traces of old data still present in the old storage system that is no longer supported.* *In your case, it is 19 MB, which was last updated on 11 Aug 2022.* *You can take a back up of the email tracking data (if required). You can use the backupconfig command in the CLI to perform the backup action. For more information, see the 'Scheduling Single or Recurring Backups' section in the 'Common Administrative Tasks' chapter of the user guide.* *If you proceed with this upgrade process, your Splunk email tracking data will be deleted.* *You can choose to proceed with the upgrade or abort the upgrade.* *Do you agree to proceed with this upgrade? [Y]"* （注） 警告メッセージは、オンプレミスの管理者ユーザーにのみ表示されます。 （注） Splunk データベースのデバッグ情報を収集するために使用される [デバッグ（debug）] サブメニューは、CLI の [診断（Diagnostic）] > [トラッキング

機能	説明
	（Tracking）] サブコマンドから削除されます。
最初の製造元の値にネットワーク設定をリセット	`Diagnostic` > `Reload` サブコマンドを使用して、ネットワーク設定を最初の製造元の値にリセットできるようになりました。 `Diagnostic` > `Reload` サブコマンドは、工場出荷時の設定を復元し、ユーザー設定を消去します。このサブコマンドは、既存のユーザーおよび設定データを完全に消去します。このため、これらのデバイスには、新しいデバイスと同じインストールおよび設定方法を使用できます。 最後の Reload サブコマンドの実行ステータスを表示する新しいサブコマンド Reload Status が Diagnostic コマンドに追加されました。 これらのサブコマンドの詳細については、Diagnostic - Reload サブコマンドおよびDiagnostic - Reload Status コマンドを参照してください。
TLS 通信中のピア証明書の X.509 検証の実行	ピア証明書の X.509 検証を実行するように Cisco Secure Email and Web Manager を設定できます。X.509 検証は、次のサービスに適用されます。 • アウトバウンド SMTP • LDAP • アップデータ • TLS を介したアラート • Syslog サーバー（Syslog Server） • スマート ライセンシング サーバー • SSE コネクタ • SSE サーバー 詳細については、X.509 証明書を参照してください。

機能	説明
Secure Email and Web Manager 仮想アプライアンスモデルの新しい RAM 値	AsyncOS 15.0 リリース以降では、KVM または VMWare ESXi を介して展開された M600v Cisco Secure Email and Web Manager 仮想アプライアンスモデルに新しい RAM 値があります。 仮想アプライアンスに適用可能な新しい RAM 値の詳細については、『Cisco Content Security Virtual Appliance Installation Guide』を参照してください（https://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-installation-guides-list.htmlから入手可能）。
（オンプレミスのみ）Azure プラットフォームの第 2 世代展開のサポート	AsyncOS 15.0 リリース以降では、Cisco Secure Email and Web Manager で Azure の第 2 世代展開がサポートされます。 （注） Azure 第 2 世代展開でサポートされるモデルは、**M600V** のみです。 （注） 第 2 世代のイメージは、Azure プラットフォームに展開した後に起動しません。第 2 世代のイメージが展開された後、仮想マシンを再起動する必要があります。 Azure プラットフォームでの第 2 世代展開の詳細については、『Cisco Secure Email Virtual Gateway and Cisco Secure Email and Web Manager Virtual on Microsoft on Azure Deployment Guide』を参照してください（https://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-installation-guides-list.htmlから入手可能）。
（オンプレミスのみ）Microsoft Hyper-V Server 2019 のサポート	Cisco Secure Email and Web Manager 15.0 は、Microsoft Hyper-V Server 2019 をサポートします。
（オンプレミスのみ）Hyper-V の第 2 世代展開のサポート	AsyncOS 15.0 リリース以降では、Cisco Secure Email and Web Manager で Hyper-V の第 2 世代展開のみがサポートされます。 （注） Hyper-V 第 2 世代展開でサポートされるモデルは、**M600V** のみです。 Hyper-V の第 2 世代展開のサポートの詳細については、『Cisco Content Security Virtual Appliance Installation Guide』を参照してください（https://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-installation-guides-list.htmlから入手可能）。

機能	説明
（オンプレミスのみ）AWS 展開でサポートされるモデル	AsyncOS 15.0 リリース以降、AWS 展開でサポートされるモデルは **M600V** のみです。 詳細については、『Deploying Cisco Secure Email Gateway, Secure Web, and Secure Email and Web Manager Virtual Appliances on Amazon Elastic Compute Cloud on Amazon Web Services Guide』を参照してください（https://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-installation-guides-list.htmlから入手可能）。

Cisco Secure Email and Web Manager の概要

AsyncOS for Cisco Secure Email and Web Manager には、次の機能が統合されています。

- **外部スパム隔離**：エンドユーザー向けのスパム メッセージおよび疑わしいスパム メッセージを保持しており、エンドユーザーおよび管理者は、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（Centralized Policy）、ウイルス（Virus）、アウトブレイク隔離（Outbreak Quarantines）：これらの隔離および隔離内に隔離されたメッセージを複数の E メールゲートウェイから管理するための単一のインターフェイスを提供します。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（Centralized reporting）**：複数の E 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関する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、 Secure Email and Web Manager アプライアンスでも使用できます。
- **中央集中型トラッキング（Centralized tracking）**：単一のインターフェイスを使用して、メール メッセージを追跡すること、および複数の E 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。
- **Web セキュリティ アプライアンスの中央集中型構成管理（Centralized Configuration Management for Web Security appliances）**：簡易性および一貫性のため、複数の Web セキュリティ アプライアンスを対象にポリシー定義とポリシー導入を管理します。

（注） 中央集中型の電子メール管理、または E メールゲートウェイの「クラスタリング」に Secure Email and Web Manager アプライアンスは含まれません。

- **中央集中型アップグレード管理（Centralized Upgrade Management）**：単一の Secure Email and Web Manager アプライアンス（SMA）を使用して、複数の Web セキュリティアプライアンス（WSA）を同時にアップグレードできます。

- **データのバックアップ（Backup of data）**：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、 Secure Email and Web Manager アプライアンスのデータをバックアップします。
- **国際化ドメイン名（IDN）のサポート（Support for Internationalized Domain Name (IDN)）**：AsyncOS 14.0 は、IDN ドメインを含む電子メールアドレスを持つメッセージを受信および配信できるようになりました。現在、コンテンツ セキュリティ ゲートウェイは次の言語の IDN ドメインのみをサポートしています。
  - インドの地域言語：ヒンディー語、タミル語、テルグ語、カンナダ語、マラーティ語、パンジャブ語、マラヤラム語、ベンガル語、グジャラート語、ウルドゥー語、アッサム語、ネパール語、バングラ語、ボド語、ドグリ語、カシミール語、コンカニ語、マイティリ語、マニプリ語、オリヤ語、サンスクリット語、サンタル語、シンド語、トゥル語。
  - ヨーロッパおよびアジアの言語：フランス語、ロシア語、日本語、ドイツ語、ウクライナ語、韓国語、スペイン語、イタリア語、中国語、オランダ語、タイ語、アラビア語、カザフ語。

このリリースでは、コンテンツ セキュリティ ゲートウェイで IDN ドメインを使用して設定できる機能はほとんどありません。

- SMTP ルートの設定：IDN ドメインの追加または編集、IDN ドメインを使用した SMTP ルートのエクスポートまたはインポート。
- レポートの設定：IDN データ（ユーザ名、電子メールアドレス、ドメイン）をレポートに表示します。
- メッセージトラッキングの設定：メッセージトラッキングに IDN データ（ユーザ名、電子メールアドレス、およびドメイン）を表示します。
- ポリシー、ウイルス、およびアウトブレイク隔離の設定：アンチウイルスエンジンによって、マルウェアを送信している可能性があると判定された IDN ドメインを含むメッセージ、アウトブレイクフィルタによってスパムまたはマルウェアの可能性があると判定された IDN ドメインを含むメッセージ、メッセージフィルタ、コンテンツフィルタ、および DLP メッセージアクションによって捕捉された IDN ドメインを含むメッセージを表示します。
- スパム隔離の設定：スパムまたは疑わしいスパムとして検出された IDN ドメインを含むメッセージを表示し、IDN ドメインの電子メールアドレスをセーフリストおよびブロックリストカテゴリに追加します。

1 台の Secure Email and Web Manager アプライアンスからのセキュリティ操作の調整も、複数のアプライアンスへの負荷の分散もできます。

翻訳について
このドキュメントは、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。