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 14.2* の新機能

機能	説明
新しい送信者ドメインのレピュテーション判定	このリリースでは、送信者ドメインのレピュテーションの判定は、意図する意味と推奨される使用法を正確に反映するように更新されています。 次のレガシー SDR 判定は、新しい SDR 判定にマッピングされます。 • 「Awful」から「Untrusted」へ • 「Poor」から「Questionable」へ • 「Tainted」または「Weak」から「Neutral」へ • 「Neutral」から「Favorable」へ • 「Good」から「Trusted」へ • 「Unknown」から「Unknown」へ SDR レポートとメッセージトラッキングの結果は、アップグレード時に新しい判定で更新されます。電子メールゲートウェイも、新しい SDR 判定を含む最新の 14.2 バージョンにアップグレードしてください。 （注） SDR レポーティングおよびトラッキング AsyncOS API は、新しい SDR 脅威レベルとカテゴリ構造を反映するように更新されています。 （注） SDR トラッキングログが更新され、新しい SDR 脅威レベルと送信者の成熟度の詳細が反映されます。

機能	説明
中央集中型電子メールトラッキングサービスのデータストレージ時間の管理	

機能	説明
	日数に基づいて中央集中型電子メール トラッキング データベースにメッセージ（データ）を保存するように Cisco Secure Email and Web Manager を設定できるようになりました。 この機能は、次のいずれかの方法で設定できます。 • レガシー Web インターフェイスの [システム管理（System Administration）]>[ディスク管理（Disk Management）] > [データ ディスク管理の編集（Edit Data Disk Management）]ページで、[データストレージ時間の適用（Apply Data Storage Time）] オプションを使用する。 • CLI の `diskquotaconfig` > `edit` > `Centralized Email Tracking` サブコマンドで `Manage data based on the storage time` ステートメントを使用する。 **重要**：Cisco Secure Email and Web Manager 13.6.2 バージョン以降、Splunk データベースは電子メールトラッキングデータ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。この機能を使用すると、電子メールトラッキングデータを含む Splunk データベースが自動的に削除されます。 **アクション**：電子メールトラッキングデータのバックアップを作成します（必要な場合）。CLI の `backupconfig` コマンドを使用して、バックアップアクションを実行できます。詳細については、「単一または定期バックアップのスケジュール設定」を参照してください。 （注） 組織のネットワークにある Cisco Secure Email and Web Manager が 1 つだけの場合は、ネットワークに新しい仮想マシン（VM）を展開する必要があります。仮想 Cisco Secure Email and Web Manager の展開方法の詳細については、『Cisco Secure Email and Web 仮想アプライアンス設置ガイド』を参照してください。

機能	説明
	https://www.cisco.com/c/dam/en/us/td/docs/security/content_security/virtual_appliances/Cisco_Content_Security_Virtual_Appliance_Install_Guide.pdf 詳細については、「データストレージ時間」を参照してください。
PVO 検疫しきい値アラート	Cisco Secure Email and Web Manager では、PVO 検疫メッセージの数が、特定の期間と PVO 検疫に対して設定されたユーザー定義のしきい値を超えると、受信者にアラートが送信されます。 Cisco Secure Email and Web Manager を使用すると、電子メールとして設定したアラートを受信できます。 次の方法を使用して、PVO検疫しきい値アラートを設定できます。 • Web インターフェイスの [電子メール（Email）] > [メッセージ検疫（Message Quarantine）] > [ポリシー、ウイルス、およびアウトブレイク検疫（Policy, Virus, and Outbreak Quarantines）] ページ • CLI の `quarantineconfig` コマンド 詳細については、ユーザーガイドの「Centralized Policy, Virus, and Outbreak Quarantines」の章の「PVO Quarantine Threshold Alert」セクションを参照してください。

機能	説明
共有メールボックス用のエンドユーザー検疫の設定	

機能	説明
	管理者がシングルサインオンによるEUQへのアクセスを有効にしていて、共有メールボックスへの委任アクセス権を持っている場合、その共有メールボックスのエンドユーザー検疫（EUQ）にアクセスして、スパム検疫済みメッセージに対して任意のアクションを実行できるようになりました。そのため、管理者のワークロードが軽減され、検疫済みメッセージのタイムリーな配信が可能になります。 SAML 2.0 認証を使用して EUQ にログインできる場合、EUQ にアクセスして共有メールボックスのスパム検疫メッセージを検索できます。プライマリメールボックスのスパム検疫済みメッセージを表示したり、アクセスできる共有メールボックスを追加して、その共有メールボックスのスパム検疫済みメッセージを表示したりできます。 EUQ を使用すると、複数の共有メールボックスを追加でき、スパム検疫済みメッセージを表示、検索、リリース、リリースしてセーフリストに追加、および削除するオプションが使用可能になります。 共有メールボックスには、次の方法でアクセスできます。 • スパム隔離通知メールに含まれている [メールの隔離（email quarantine）] または [すべての隔離済みメッセージを表示（View All Quarantined Messages）] リンクをクリックします。 • スパム検疫ポータルを使用して、Cisco Secure Email and Web Manager EUQ にログインします。 詳細については、ユーザーガイドの「Spam Quarantine」の章の「Configuring End-User Quarantine for Shared Mailbox」セクションを参照してください。 **注**：Office 365 ユーザーは、この機能を使用できます。この機能では、Microsoft Azure Active Directory API を使用して、共有メールボックスに関連付けられたエンドユーザー検疫への

機能	説明
	アクセスが提供されます。
Cisco Secure Email Cloud Gateway 用 AsyncOS 14.2 の新機能のサポート	[URLレトロスペクションレポート（URL Retrospection Report）] ページ：このレポートページには、URL レトロスペクティブサービスによって処理されたURLが表示されます。また、悪意のあるURL、URL レトロスペクティブサービスから判定を受け取った日時、影響を受けたメッセージの修復ステータスが一覧表示されます。 （注） URL レトロスペクション レポートデータは、クラウド管理者ユーザーのみが利用できます。 詳細については、「URL レトロスペクション レポート ページ」を参照してください。

機能	説明
電子メールトラッキングデータ用の Splunk データベースは未サポート	Web インターフェイスまたは CLI を使用して Cisco Secure Email and Web Manager にログインすると、電子メールトラッキングデータに Splunk データベースを使用している場合、次のメッセージが表示されることがあります。 「*Splunk* データベースに *x GB* の電子メールトラッキングデータがあります。*Cisco Secure Email and Web Manager 13.6.2* バージョン以降、*Splunk* データベースは電子メールトラッキングデータ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* の今後の一般提供（*GA*）リリースでは、電子メールトラッキングデータ用の *Splunk* データベースのサポートはありません。 **アクション**：電子メールトラッキングデータのバックアップを作成します（必要な場合）。CLI の `backupconfig` コマンドを使用して、バックアップアクションを実行できます。詳細については、「単一または定期バックアップのスケジュール設定」を参照してください。 （注） 組織のネットワークにある Cisco Secure Email and Web Manager が 1 つだけの場合は、ネットワークに新しい仮想マシン（VM）を展開する必要があります。仮想 Cisco Secure Email and Web Manager の展開方法の詳細については、『Cisco Secure Email and Web 仮想アプライアンス設置ガイド』を参照してください。https://www.cisco.com/c/dam/en/us/td/docs/security/content_security/virtual_appliances/Cisco_Content_Security_Virtual_Appliance_Install_Guide.pdf

機能	説明
ファイル分析レポート用のアプライアンスのグループ化に対する強化	Cisco Secure Email and Web Manager は、スマートアカウントIDを使用して、組織内のアプライアンスをグループ化し、すべてのアプライアンスのファイル分析結果を表示するようになりました。 Cisco Secure Email and Web Manager でスマートライセンスが有効になっている場合、ファイル分析レポート用にアプライアンスグループを設定すると、システムによりスマートアカウント ID がアプライアンスグループ ID として自動的に登録されます。アプライアンスグループIDはいつでも変更でき、変更はコミットアクションなしですぐに有効になります。 詳細については、（クラウド ファイル分析）詳細なファイル分析結果が表示されるように管理アプライアンスを設定するを参照してください。 **注**：この機能はオンプレミスの管理者ユーザーのみが使用できます。

機能	説明
スマート ソフトウェア ライセンシングの機能強化	スマート ソフトウェア ライセンシング機能に加えられた拡張機能は次のとおりです。 • **ライセンス予約**：Cisco Smart Software Manager（CSSM）ポータルに接続せずに、Cisco Secure Email and Web Manager で有効になっている機能のライセンスを予約できます。これは主に、インターネットや外部デバイスとの通信がない高度にセキュリティ保護されたネットワーク環境に Cisco Secure Email and Web Manager を展開するユーザーにとって有益です。 詳細については、概要および機能ライセンスの予約を参照してください。 • **Device Led Conversion（DLC）**：Cisco Secure Email and Web Manager をスマートライセンスに登録すると、既存の有効なクラシックライセンスはすべて、Device Led Conversion（DLC）プロセスを使用して自動的にスマートライセンスに変換されます。これらの変換されたライセンスは、CSSM ポータルのバーチャルアカウントで更新されます。 詳細については、概要を参照してください。 **注**：この機能はオンプレミスの管理者ユーザーのみが使用できます。
クラシックライセンスの変更：Web インターフェイスおよび CLI の期限日	このリリース以降、クラシックライセンスの Web インターフェイスおよび CLI の既存の [期限日（Expiration Date）] 列ヘッダーが [期限日（猶予期間を含む）（Expiration Date (including grace period)）] に変更されます。これは、期限日に猶予期間が含まれることを示しています。 **注**：すべてのアラートメッセージとメールログは、機能キーの猶予期間を含む期限日を表示するように変更されます。

機能	説明
設定可能なサイズで Syslog ディスクバッファを有効にする	[TCP プロトコルのみに適用可能（Applicable for TCP protocol only）]：Syslog プッシュ ログ サブスクリプションのローカルディスクバッファを設定するには、このチェックボックスをオンにします。これにより、リモート Syslog サーバーが使用できないときに、Secure Email and Web Manager でログイベントをキャッシュできるようになります。Syslog サーバーが使用可能になると、Cisco Secure Email and Web Manager は、そのログサブスクリプションのバッファにあるすべてのデータを Syslog サーバーに送信し始めます。 詳細については、ログの取得を参照してください。

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。