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 14.1* の新機能

機能	説明
新しい [システム正常性ステータス（System Health Status）] ダッシュボード	AsyncOS 14.0 では、Web セキュリティアプライアンスの現在のステータスと構成を 1 ページで表示できるようになりました。Webセキュリティアプライアンスで、[モニタリング（Monitoring）] > [システムの正常性（System Health）] を選択して、システムステータスをモニタする必要があります。 詳細については、新しい Web インターフェイスの [システムの正常性（System Health）] ダッシュボードを参照してください。

機能	説明
トラッキングデータのエクスポート	AsyncOS 14.1.0 では、トラッキングのエクスポート機能は次のように拡張されています。 • 追加のフィールドを表示して、メッセージの詳細とともに [ファイルのエクスポート（Export file）] オプションを使用して、関連するメールの分析と調査を実行します。 • エクスポートを実行すると、表示できる行の最大数が 50000 に設定されるようになりました。 詳細については、メッセージサービスのエクスポートを参照してください。
検疫カスタムアクセスロール	管理者は、隔離メッセージの読み取り専用オプションを使用してカスタムロールを作成できます。読み取り専用オプションを使用すると、ユーザはメッセージを削除またはリリースできなくなり、隔離への読み取り専用アクセス権のみが付与されます。
スパムの隔離しきい値アラート	AsyncOS 14.1.0 では、指定された期間に一定の数のスパムメッセージが隔離されるとアラートが送信されます。アラートは、生成時に Syslog にも入力されます。さらに、隔離しきい値に達すると、Cisco Secure Email and Web Manager によってアラートがトリガーされます。
一元管理	AsyncOS 14.1.0 を使用すると、複数の Cisco Secure Email and Web Manager で複数のログインを実行する必要がないため、より多くの時間を節約できます。プライマリアプライアンスで、個々の Cisco Secure Email and Web Manager の [レポート（Reporting）]、[追跡（Tracking）]、および [検疫（Quarantine）] のページを表示できます。表示するために、[追跡、レポート、および検疫（Tracking, Reporting, and Quarantine）] ページのドロップダウンリストから必要な Cisco Secure Email and Web Manager を選択できます。 詳細については、一元管理を参照してください。

機能	説明
スマートライセンスの再登録	次のいずれかのシナリオに基づいて、Cisco Secure Email and Web Manager を Cisco Cloud Services ポータルに再登録できます。 • 電子メールゲートウェイを Cisco Cloud Services ポータルに自動的に登録するときに、Cisco Cloud Services ポータルに追加されたデバイスを表示または管理できない場合。 • アプライアンスを Cisco Cloud Services ポータルに自動的に登録するときに、スマートアカウントと Cisco Cloud Services アカウントがリンクされていない場合。 詳細については、Cisco Cloud Service ポータルへの登録を参照してください。
Syslog プッシュの新しいパラメータ：ログ取得方式	Cisco Secure Email and Web Manager で Syslog プッシュログ取得方式を設定するために使用する必要がある新しいパラメータは次のとおりです。 • リモート Syslog サーバのポート番号。 • リモート Syslog サーバーに送信されるログメッセージの最大サイズ。 • （TCP プロトコルの場合のみ）：Cisco Secure Email and Web Manager とリモート Syslog サーバー間の TLS 接続。

表 *2 : AsyncOS 14.0* の新機能

機能	説明
拡張された [概要（Overview）] および [受信メールサマリー（Incoming Mail Summary）] レポートページ	アプライアンスのレガシー Web インターフェイスの [受信メール（Incoming Mail）] レポートページで行われた機能拡張は次のとおりです。 [着信メール（Incoming Mail）] レポートページ： [受信メールの詳細（Incoming Mail Details）] セクションに [ドメインレピュテーションフィルタによる停止（Stopped by Domain Reputation Filtering）] という新しい列が追加されました。 [受信メールの詳細（Incoming Mail Details）] セクションの [レピュテーションフィルタによる停止（Stopped by Reputation Filtering）] 列の名前が [IPレピュテーションフィルタによる停止（Stopped by IP Reputation Filtering）] に変更されました。 詳細については、中央集中型の電子メール セキュリティ レポーティングの使用を参照してください。
新しい [システム正常性ステータス（System Health Status）] ダッシュボード	Web セキュリティアプライアンスの現在のステータスと構成を 1 ページで表示できるようになりました。Web セキュリティアプライアンスで、**[モニターリング（Monitoring）]** > **[システムの正常性（System Health）]**を選択して、システムステータスをモニターする必要があります。 詳細については、新しい Web インターフェイスの [システムの正常性（System Health）] ダッシュボードを参照してください。

機能	説明
証明書の使用	アプライアンスは、保存された信頼できる認証局を使用してリモートドメインからの証明書を検証し、ドメインのクレデンシャルを確立します。次の信頼できる認証局を使用するようにセキュリティ管理アプライアンスを設定できます。 • システムリスト • カスタム リスト 詳細については、一般的な管理タスクを参照してください。
スマート ライセンス	スマートライセンスを有効にして登録すると、クラウドサービスが有効になり、アプライアンスが自動的に登録されます。 • Cisco SecureX と Cisco Threat Response を有効または無効にするために、generalconfig コマンドの下にオプションが導入されました。 • コマンド threstresponseconfig は、「Cisco SecureX/Threat Response の機能を有効/無効にするには、一般的な config コマンドを入力してください（Enter general config command to Enable / Disable of Cisco SecureX / Threat Response feature）」という警告メッセージを表示します。 • スマートアカウント情報を取得するために、smartaccountinfo コマンドが導入されました。 • CloudServices を有効にすると Cisco SecureX は自動的に有効になり、CloudServices を無効にすると Cisco Securex は無効になります。 詳細については、「Cisco SecureX または Cisco Threat Response との統合」を参照してください。

機能	説明
コンテンツ セキュリティ ゲートウェイでの Cisco SecureX または Threat Response の有効化	コンテンツセキュリティ ゲートウェイでCisco SecureX または Threat Response を有効にするには、一般的な設定を使用する必要があります。 詳細については、「Cisco SecureX または Cisco Threat Response との統合」を参照してください。
メールポリシーの詳細に関する新しいレポート	新しいレポート [メールポリシーの詳細（Mail Policy Details）] がアプライアンスの新しい Web インターフェイスに追加されています。このレポートを使用して、設定されたメールポリシーに一致するメッセージの数を表示します。 詳細については、中央集中型の電子メール セキュリティ レポーティングの使用を参照してください。
Cisco Threat Response 内のメッセージに対する修復アクションの実行	Cisco Threat Response では、アプライアンスで処理されたメッセージに対して次の修復アクションを調査して適用できるようになりました。 • 削除（Delete） • 転送（Forward） • 転送と削除（Forward and Delete） 詳細については、「Cisco SecureX または Cisco Threat Response との統合」を参照してください。

機能	説明
国際化ドメイン名（IDN）のサポート	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、電子メール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。 詳細については、はじめに （1 ページ）を参照してください。
スパム通知	[カスタムロゴの位置（Custom Logo Position）] フィールドが新たに追加され、同じロゴをスパム通知メールの特定の位置に追加できるようになりました。
ブランド変更後の製品と関連資料	シスコは、製品と関連資料にブランドを「Cisco Content Security Management」から「Cisco Secure Email and Web Manager」に変更しました。
パスフレーズ	ログインパスフレーズを定義するには、Email and Web Manager に新しいパスフレーズルールを追加します。 詳細については、一般的な管理タスクを参照してください。

機能	説明
[FQDN]	X.509 証明書の場合、FQDN 検証ではその証明書のサブジェクト識別名の共通名フィールド（CN）と dNSName タイプ（SAN：dNSName）の subjectAltName 拡張が検証されます。 詳細については、一般的な管理タスク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。

Note 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。