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 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/c/en/us/support/security/content-security-management-appliance/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。

表 *1 : AsyncOS 12.5* の新機能

機能	説明
新しいハードウェア モデルのサポート	シスコのコンテンツ セキュリティ管理アプライアンス向け AsyncOS 12.5.0 リリースでは、次のハードウェア モデルをサポートしています。 • M195 • M395 • M695 • M695F 詳細については、https://www.cisco.com/c/en/us/products/collateral/security/content-security-m%20anagement-appliance/datasheet_C78-721194.htmlを参照してください。

機能	説明
設定マスターの複数のサブセットの管理	特定のバージョンの設定マスターのサブセットを設定して、Web セキュリティアプライアンスのさまざまなポリシー設定を一元的に管理できるようになりました。 詳細については、Web セキュリティアプライアンスの管理を参照してください。
ケースブックを使用した脅威分析の実行	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は、ケースブックとピボットメニューのウィジェットが含まれるようになりました。 （注） Microsoft Internet Explorer ブラウザを使用してアプライアンスにアクセスしている場合、[ケースブック（Casebook）] ウィジェットを使用することはできません。 [ケースブック（Casebook）] ウィジェットと [ピボット メニュー（Pivot Menu）] ウィジェットを使用して、アプライアンスで次のアクションを実行できます。 • 観測対象をケースブックに追加し、脅威分析の調査を実行します。 • 新しいケース、既存のケース、または Cisco Threat Response ポータルに登録されているその他のデバイス（エンドポイント向け AMP、Cisco Umbrella、Cisco Talos Intelligence など）の監視対象をピボットし、脅威分析のために調査します。 詳細については、Cisco Threat Response ポータルとの統合を参照してください。
Cisco Threat Response ポータルでアプライアンスを登録するときに Cisco Threat Response サーバを選択する機能	アプライアンスを Cisco Threat Response ポータルに登録するときに、Cisco Threat Response ポータルにアプライアンスを接続するための Cisco Threat Response サーバを選択できるようになりました。 このリリースでサポートされている Cisco Threat Response サーバは次のとおりです。 • 米国（api-sse.cisco.com） • 欧州（api.eu.sse.itd.cisco.com） 詳細については、Cisco Threat Response ポータルとの統合を参照してください。

機能	説明
新しい Web インターフェイスの[マイ レポート（My Reports）] ページ	カスタム レポート ページを作成するには、アプライアンスの新しい Web インターフェイスにある既存のすべての電子メール セキュリティ レポートからチャート（グラフ）とテーブルを構成します。 詳細については、新しい Web インターフェイスでのレポートの使用を参照してください。
新しい Web インターフェイスでのポリシー、ウイルス、およびアウトブレイク隔離の設定	アプライアンスの新しい Web インターフェイスから、ポリシー、ウイルス、またはアウトブレイク隔離を設定できるようになりました。 詳細については、集約されたポリシー、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。
Swagger UI を使用した API の管理	Swagger は、OpenAPI 仕様に基づいて構築された一連のオープンソースのツールです。 Swagger UI を使用すると、Web インターフェイスでの AsyncOS API リソースの設計と管理が容易になります。 詳細については、セットアップ、インストール、および基本設定を参照してください。
Web 使用状況分析のモニタリング	統計分析のために Web サイトの使用状況またはアクティビティの送信を有効または無効にすることができます。 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 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（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 セキュリティ アプライアンス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、セキュリティ管理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 セキュリティ アプライアンスの「クラスタリング」にセキュリティ管理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）：単一のセキュリティ管理アプライアンス（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、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します。

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。