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。

表 *1 : AsyncOS 13.0* 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 13.0.0 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 詳細については、「https://www.cisco.com/c/en/us/products/collateral/security/content-security-management-appliance/datasheet_C78-721194.html」を参照してください。

機能	説明
ケースブックを使用した脅威分析の実行	Cisco コンテンツ セキュリティ管理アプライアンスに、ケースブックとピボットメニューのウィジェットが追加されました。 （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 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 との統合を参照してください。
お気に入りレポートの管理	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）とテーブルを構成することで、カスタム レポート ページが作成できるようになりました。 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。

機能	説明
ポリシー、ウイルス、および検疫の新しい CA 証明書の作成	`Updatepvocert` CLI コマンドを使用して、ポリシー、ウイルス、および検疫用に 2048 ビットの CA 証明書を作成できます。 詳細については、updatepvocert コマンドを参照してください。

機能	説明
AsyncOS 13.0 for Cisco E メールセキュリティアプライアンスの新機能のサポート	

機能	説明

	• **スケジュール設定されたレポートとアーカイブされたレポート**：アプライアンスの新しい Web インターフェイスで電子メールレポートをスケジュール設定し、アーカイブされたレポートを表示できるようになりました。
	
	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。
	
	• [Safe Print アクション（Safe Print Action）] レポートページ：このレポートページを使用して、次の情報を表示できます。
	
	  • ファイル タイプ別の、Safe Print で出力された添付ファイルの数（グラフ形式）。
	
	  • ファイル タイプ別の、Safe Print で出力された添付ファイルの概要（表形式）。
	
	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。
	
	• [有効なレポートデータ（Reporting Data Availability）] レポートページ：アプライアンスの新しい Web インターフェイスで、[有効なレポートデータ（Reporting Data Availability）] レポートページを表示できるようになりました。
	
	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。
	
	• **ポリシー、ウイルスおよびアウトブレイク隔離**：アプライアンスの新しいWebインターフェイスで、ポリシー、ウイルスおよび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 のサポート**：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。
	
	• **レポートのエクスポート**：アプライアンスの新しいWebインターフェイスで、電子メールのレポーティングページを PDF（ポータブル ドキュメント ファイル）形式でエクスポートできるようになりました。

機能	説明
	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。
機能の使用状況の統計情報を収集することによるユーザエクスペリエンスの向上	Cisco コンテンツ セキュリティ管理アプライアンスで、アプライアンスの新しい Web インターフェイスで機能およびインターフェイスまたはその一方の使用状況の統計情報が収集されるようになりました。これにより、全体的なユーザエクスペリエンスを向上させることができます。収集されたすべてのデータは匿名化されます。この機能の選択を解除する場合は、Web インターフェイスで [管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [一般設定（General Settings]） > [使用状況分析（Usage Analytics）] ページに移動して無効にします。 詳細については、Web 使用状況分析のモニタリングを参照してください。
アプライアンスの Web インターフェイス使用状況の統計情報を収集することによるユーザエクスペリエンスの向上	Cisco コンテンツ セキュリティ管理アプライアンスで、使用状況分析機能を使用して、アプライアンスの Web インターフェイス使用状況の統計情報を収集できるようになりました。この機能は、Web インターフェイスの使用状況データを収集して分析し、アプライアンスのユーザエクスペリエンスを向上させるための洞察を提供するために使用されます。詳細については、Web 使用状況分析のモニタリングを参照してください。
SAML 2.0 を使用したシングルサインオン	シスコのコンテンツ セキュリティ管理アプライアンスは SAML 2.0 SSO をサポートするようになりました。これにより、ユーザは組織内で他の SAML 2.0 SSO 対応サービスへのアクセスに使用しているのと同じクレデンシャルでアプライアンスの Web インターフェイスにログインできます。 詳細については、SAML 2.0 による SSOを参照してください。
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。

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。