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 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 13.8.1* の新機能

機能	説明
AsyncOS API を使用したログ情報の取得	AsyncOS API を使用して、アプライアンスから次のログ詳細を取得できるようになりました。 • サブスクリプションの詳細を記録します。 • 特定のログサブスクリプションのすべてのログファイル。 • ファイル名または URL を使用したログファイル。 詳細については、『AsyncOS 13.8.1 API for Cisco Content Security Management Appliances - Getting Started Guide』の「Logging APIs」セクションを参照してください。

機能	説明
監査ログを使用した認証、許可、アカウンティングのイベント（AAA：Authentication、Authorization、および Accounting）の記録	Cisco コンテンツセキュリティ管理アプライアンスは、AAA（認証、許可、アカウンティング）のイベントを記録する新しいタイプのログサブスクリプション「監査ログ」をサポートしています。 監査ログの詳細の一部を次に示します。 • ユーザー - ログオン • ユーザー - ログオンに失敗しました、パスワードが正しくありません • ユーザー - ログオンに失敗しました、ユーザー名が不明です • ユーザー - ログオンに失敗しました、アカウントの有効期限が切れています • ユーザー - ログオフ • ユーザー - ロックアウト • ユーザー - アクティブ化済み • ユーザー - パスワードの変更 • ユーザー - パスワードのリセット • ユーザー - セキュリティ設定/プロファイルの変更 • ユーザー - 作成済み • ユーザー - 削除済みまたは変更済み • ユーザー設定 - ユーザーが行った設定変更。 • グループ/ロール - 削除済みまたは変更済み • グループ/ロール - 権限の変更 • 隔離 - 隔離内のメッセージに対して実行されるアクション。 詳細については、監査ログの使用を参照してください。

機能	説明
AsyncOS API のコンテンツセキュリティ管理アプライアンスでの OpenID Connect 1.0 の設定	Cisco コンテンツセキュリティ管理アプライアンスは、OpenID Connect 1.0 認証で ID プロバイダ（IDP）を使用するアプリケーションまたはクライアントとの統合をサポートし、アプライアンスで使用可能な AsyncOS API とシームレスに接続します。現在、お使いのアプライアンスは、Microsoft AD FS のみを使用して OpenID Connectで認定されています。 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。
新しいアクセス権限：委任管理者のログサブスクリプション	新しいアクセス権限オプションである[ログサブスクリプション（Log Subscription）] が、アプライアンスの Web インターフェイスの [システム管理（System Administration）] > [ユーザーロール（User Role）] ページに追加されました。[ログサブスクリプション（Log Subscription）] オプションを使用して、カスタムユーザロールに割り当てられている委任管理者がログサブスクリプションまたはログ API にアクセスしてログファイルを表示またはダウンロードできるかどうかを定義します。 詳細については、管理タスクの分散を参照してください。

表 *2 : AsyncOS 13.8.0* の新機能

機能	説明
メッセージトラッキング機能拡張	新しい Web インターフェイスには、次のユーザーエクスペリエンスの拡張が含まれています。 • [メッセージトラッキングの検索結果（Message Tracking Search Results）] ページが拡張され、ページビューあたりより多くの検索結果が表示されるようになりました。 • [メッセージトラッキングの検索の詳細（Message Tracking Search Details）] ページのレイアウトが拡張され、[エンベロープのヘッダーとサマリー（Envelope Header and Summary）] ペインおよび [ホストサマリーの送信（Sending Host Summary）] ペインが [処理詳細（Processing Details）] ペインの横に表示されるようになりました。この新しいレイアウトでは、すべての重要な情報を同じページビューでスクロールすることなく表示できます。
レポートの機能拡張	お気に入りレポートをスケジュールしてアーカイブできるようになりました。お気に入りレポートのデータを CSV または PDF 形式でエクスポートすることもできます。

機能	説明
スパム通知の機能拡張	• スパム通知でリンクの有効期限を設定できるようになりました。これらのリンクは、指定された期間後に自動的に期限切れになります。 • スパム通知内のすべての隔離メッセージを表示するためにリンクを表示するか非表示にするかを選択できるようになりました。また、スパム通知でリンク表示を選択している場合は、エンドユーザーにスパム隔離へのアクセスの前に認証を強制できるようになりました。 詳細については、『ユーザーガイド』の「隔離されたメッセージに関するエンドユーザへの通知」を参照してください。
セキュリティ機能の拡張	AsyncOS 13.8.0 には、次のセキュリティ機能拡張が含まれています。 • アプライアンスは SSLv2 および SSLv3 方式をサポートしなくなります。下位の AsyncOS バージョンからアップグレードする場合、アプライアンスは自動的に TLS 1.1 および TLS 1.2 を使用します。詳細については、リリースノートの「SSL 設定の変更」のトピックを参照してください。 • アプライアンスは、TLS 経由でシスコテクニカルサポート要求を送信します。SMTP サーバーが TLS を使用していない場合、要求はプレーンテキストとして送信されます。 • TLSを介してアラートを送信するようにアプライアンスを設定できるようになりました。この機能を設定するには、CLI で次のサブコマンドを使用します。**alertconfig > SETUP > Do you want to enable TLS support to send alert messages?**
Cisco SecureX および Cisco Threat Response の機能拡張	アプライアンスを設定してプロキシ経由で Cisco SecureX および Cisco Threat Response に接続できるようになりました。プロキシ経由で接続するには、**[ネットワーク（Network）] > [クラウドサービス設定（Cloud Service Settings）]** ページの [プロキシの使用（Use Proxy）] チェックボックスをオンにします。

機能	説明
YouTube レポート（Web）	

機能	説明
	新しい Web インターフェイス（[URLカテゴリ（URL Categories）] レポートページ）で、YouTube の分類機能に関連する次の情報を表示できるようになりました。 • [上位YouTubeカテゴリ（Top Youtube Categories）] : [トランザクションの合計数 （Total Transactions）] サイト上でアクセスされている上位の YouTube カテゴリを表示できます（グラフ形式）。 • [上位YouTubeカテゴリ（Top Youtube Categories）] : [ブロックされたトランザクションと警告されたトランザクション（Blocked and Warned Transactions）] トランザクションごとに発生するブロックアクションまたは警告アクションをトリガーした上位の YouTube URL を表示できます（グラフ形式）。たとえば、ユーザが特定の YouTube URL にリダイレクトされ、特定のポリシーが適用されている場合は、ブロックアクションまたは警告がトリガーされました。この YouTube URL は、ブロックまたは警告されたトランザクションとしてこのグラフに一覧表示されます。 [URLカテゴリ（URL Categories）] レポートページを表示するには、[製品（Product）] ドロップダウンから [Web（Web）] を選択し、[レポート（Reports）] ドロップダウンから [モニターリング（Monitoring）] > [URLカテゴリ（URL Categories）] を選択します。 • [一致したYoutubeカテゴリ（Youtube Categories Matched）] [一致したYoutubeカテゴリ（Youtube Categories Matched）] インタラクティブテーブルには、指定した時間範囲内における Youtube カテゴリ別のトランザクションの処理、使用された帯域幅、各カテゴリで費やされた時間が表示されます。 [一致したYoutubeカテゴリ（Youtube Categories Matched）] インタラクティブテーブルを表示するには、[Web] > [レポート（Reporting）] > [URLカテゴリ（URL Categories）] を選択します。 • Youtube（YT）カテゴリ 新しいフィルタ [YTカテゴリ（YT Category）] が [Web（Web）]>[トラッキング（Tracking）]に追加されました。

機能	説明
	特定の YouTube カテゴリでフィルタ処理するには、[YouTube カテゴリ（YouTube Category）] セクションを展開し、表示する YouTube カテゴリを選択します。
IP スプーフィングプロファイル	IP スプーフィングプロファイルを作成し、それをルーティングポリシーに追加することによって、Web プロキシ IP スプーフィングを設定できるようになりました。IP スプーフィングプロファイルがルーティングポリシーで使用されている場合、Web プロキシは送信元 IP アドレスを IP スプーフィングプロファイルで定義されたカスタム IP アドレスに変更します。 新しい IP スプーフィングプロファイルを作成する、または既存の IP スプーフィングプロファイルを変更するには、[Web（Web）] > [IPスプーフィングプロファイル（IP Spoofing Profiles）] を選択します。 ルーティングポリシーに IP スプーフィングプロファイルを追加するには、[Web（Web）]> [ルーティングポリシー（Routing Policies）]を選択します。 （注） セキュリティ管理アプライアンスの IP スプーフィングプロファイルを Web セキュリティアプライアンスに公開せず、Web セキュリティアプライアンスの既存の IP スプーフィングプロファイルを上書きしない場合は、次の手順を実行します。 1. セキュリティ管理アプライアンスにログインします。 2. **[設定マスター（Configuration Master）] > [IP スプーフィングプロファイル（IP Spoofing Profile）]** に移動します。 3. **[設定の編集（Edit Settings）]** をクリックします。 4. [IPスプーフィングプロファイルをWSAにパブリッシュ（Publish IP Spoofing Profiles to WSA）] を [いいえ（No）]に設定します。 デフォルトで選択されているオプションは [はい（Yes）] です。 詳細については、『*User Guide for AsyncOS 12.5 for Cisco Web Security Appliances*』を参照してください。

Cisco Content Security Management 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 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、Content Security Management 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Security Management 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、Content Security Management 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Content Security Management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。