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変更点

ここでは、AsyncOS for Cisco コンテンツ セキュリティ管理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*：今回のリリースでの新機能

機能	説明
TLS v1.2 のサポート	Cisco コンテンツ セキュリティ管理アプライアンスは、追加の SSL 方式である TLS v1.2 をサポートするようになりました。 アップグレード前に TLS v1 を使用していなかった場合、アップグレード後に、SSL 方式は自動的に TLS v1.2 に設定されることはありません。 CLI で `sslconfig` コマンドを使用して、既存の SSL 構成を表示または変更できます。 （注） ネゴシエーション時には、クライアント アドバタイズメントで最上位のサポートされる TLS または SSL 方式が常に選択されます。

機能	説明
二要素認証のサポート	Cisco コンテンツ セキュリティ管理アプライアンスは、アプライアンスにログインするときにセキュリティで保護されたアクセスを保証する二要素認証をサポートするようになりました。 標準の RFC に準拠している任意の標準 RADIUS サーバを介してアプライアンスの二要素認証を設定できます。 次のいずれかの方法で、二要素認証を有効化できます。 • Web インターフェイスの [システム管理（System Administration）] > [ユーザ（Users）] ページ。管理タスクの分散を参照してください。 • CLI の `userconfig > twofactorauth` コマンド。

機能	説明
AsyncOS 11.0 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	AsyncOS 11.0 for Cisco E メール セキュリティ アプライアンスの新機能である次の機能のレポート サポート： • 地理的分散。このレポートのページを使用して次のような詳細を表示します。 • 発信国別の受信メール接続数の上位（グラフィカルな形式）。 • 発信国別の受信メール接続の合計数（表形式）。 メッセージ トラッキングを使用すると、コンテンツまたはメッセージ フィルタによって検出される特定の位置情報から着信したメッセージを検索することができます。メッセージ トラッキングの [詳細設定（Advanced）] セクションで [メッセージ イベント（Message Event）] オプションに **位置情報**フィルタを使用します。 詳細については、オンライン ヘルプまたはユーザ ガイドのメール レポートの章で、該当する用語を検索してください。 AMP エンジンによってスキャンされた発信メッセージの詳細を表示する、次のレポートが拡張されました。 • 高度なマルウェア防御（Advanced Malware Protection） • AMP ファイル分析（AMP File Analysis） • [AMP判定のアップデート（AMP Verdict Updates）] • [概要（Overview）] ページ • 送信先（Outgoing Destinations） • 送信者（Outgoing Senders） • 内部ユーザ（Internal Users） 詳細については、ユーザ ガイドのメール レポートの章で、該当する用語を検索してください。

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。 また、セキュリティ管理アプライアンスでのみ使用できる、Web セキュリティの拡張レポートがいくつかあります。
- 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、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って処理された電子メール メッセージおよび 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。

- 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。