Cisco Email Security Appliances をご使用の前に

この章は、次の項で構成されています。

AsyncOS 12.5 の新機能

表 *1 : AsyncOS 12.5* の新機能

機能	説明
新しいハードウェア サポート	Cisco Email Security Appliances 向け AsyncOS 12.5 リリースでは、次のハードウェア モデルがサポートされています。 • C195 • C395 • C695 • C695F 詳細については、https://www.cisco.com/c/en/us/products/collateral/security/cloud-email-security/datasheet_c22-739910.htmlを参照してください。

機能	説明
高度なマルウェア防御（AMP）隔離管理の改善	AMP エンジンのスキャン プロセス実行時に、ファイル レピュテーション サービスから不明な判定を受信した添付ファイルが分類前チェックとファイル分析のために送信されます。 分類前チェック フェーズでは、メッセージが電子メール セキュリティ アプライアンスにローカルに保存されてから、完全なファイル分析を行うために添付ファイルが送信された場合にのみ、中央集中型隔離に送信されるようになりました。 これにより、パフォーマンスが向上し、集中型隔離の全体的な負荷が軽減されます。

機能	説明
外部脅威フィードの消費機能	

機能	説明
	Cisco Email Security Appliance で、TAXII プロトコルで通信される STIX フォーマットで外部脅威情報を使用するように設定できます。 Cisco E メール セキュリティ アプライアンスで外部脅威情報を使用する機能によって、組織は以下のことを実施できるようになります。 • マルウェア、ランサムウェア、フィッシング攻撃、標的型攻撃などのサイバー脅威にプロアクティブに対応する。 • 外部脅威フィードまたは TAXII プロトコルで通信する STIX フォーマットで外部脅威フィードを取得可能な組織のネットワーク上の他のデバイスに登録し、アプライアンスで脅威情報を使用する。 • アプライアンスに動的な情報（URL の動的なリストなど）をインポートし、動的な情報に基づいてメール ポリシーの設定やメッセージ アクションの定義を実行する。 • Cisco E メール セキュリティ アプライアンスの機能を向上する。 クラシック ライセンシング モードを使用していて、外部脅威フィードの機能キーをお持ちでない場合は、以下の手順でシスコの Global Licensing Operations（GLO）チームに連絡して機能キーを取得する必要があります。 1. GLO チーム（licensing@cisco.com）に電子メールを送信し、件名を「外部脅威フィード機能キーのリクエスト」とします。その後、電子メールに製品認証キー（PAK）ファイルと発注書（PO）の詳細を記載します。 2. GLO チームが機能キーを手動でプロビジョニングし、アプライアンスにインストール可能なライセンス キーを電子メールで送信します。 （注） アプライアンスでスマート ライセンシング モードに切り替えると、自動

機能	説明
	的に外部脅威フィード機能キーが提供されます。 詳細は、外部脅威フィードを消費する Cisco E メール セキュリティ ゲートウェイの設定および『*CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*』を参照してください。
送信者ドメイン レピュテーションを使用したメッセージのフィルタリング	シスコの送信者ドメイン レピュテーション（SDR）は、送信者のドメインおよびその他の属性に基づいて電子メールメッセージのレピュテーションの判定を提供するクラウドサービスです。 ドメインベースのレピュテーション分析では、共有 IP、ホスティングまたはインフラストラクチャ プロバイダーのレピュテーションよりも詳しい情報を調べることでより高いスパム検出率を達成し、完全修飾ドメイン名（FQDN）やSMTP通信およびメッセージヘッダーのその他の送信者情報に関連する特徴に基づいて判定を取得します。SDR の詳細は、Cisco Talos セキュリティ インテリジェンスおよびリサーチ グループ（Talos）（https://www.talosintelligence.com）までお問い合わせください。 詳細は、送信者ドメイン レピュテーション フィルタリングおよび『*CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*』を参照してください。
脅威名に基づいた悪意のあるメッセージの表示	メッセージ トラッキングで、脅威名に基づいてAMPエンジンに悪意があると検出された着信または発信メッセージを検索できるようになりました。 詳細については、メッセージ トラッキングを参照してください。

機能	説明
How-To ウィジェットを使用したユーザ エクスペリエンスの強化	How-To は、アプライアンスで複雑なタスクを実行するためにウォークスルー形式でユーザにアプリ内アシスタンスを提供する、コンテキスト型ウィジェットです。 （注） ウォークスルーのリストは更新可能なクラウドです。ハウツー ウィジェットの更新バージョンとポップアップ ウィンドウを表示するには、ブラウザのキャッシュをクリアします。 詳細は、アプライアンスへのアクセスおよび『*CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*』を参照してください。
ファイル分析に向けた Cisco AMP Threat Grid クラスタリングのサポート	以下のいずれかの方法で、ファイル分析に向けてスタンドアロンまたはクラスタの Cisco AMP Threat Grid アプライアンスを追加できるようになりました。 • Web インターフェイスの [セキュリティ サービス（Security Services）] > [ファイル レピュテーションと分析（File Reputation and Analysis）] ページ。ファイル レピュテーション フィルタリングとファイル分析を参照してください。 • CLI での `ampconfig` コマンド。『*CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*』を参照してください。
ファイル分析に向けたしきい値の設定	許容されるファイル分析スコアのしきい値の上限を設定できるようになりました。 しきい値設定に基づいてブロックされるファイルは、詳細マルウェア保護レポートの [着信マルウェア脅威ファイル（Incoming Malware Threat Files）] セクションで、[カスタムしきい値（Custom Threshold）] として表示されます。 詳細については、ファイル レピュテーション フィルタリングとファイル分析を参照してください。

機能	説明
脅威名に基づいた悪意のあるメッセージの表示	メッセージ トラッキングで、脅威名に基づいてAMPエンジンに悪意があると検出された着信または発信メッセージを検索できるようになりました。 詳細については、メッセージ トラッキングを参照してください。
発信 TLS 接続に向けた、名前付きエンティティの DNS ベースの認証（DANE）サポート	アプライアンスの発信 TLS 接続に向けた名前付きエンティティの DNS ベースの認証（DANE）を有効にすることで、有効な受信者のドメインに安全にメッセージを送信できるようになりました。 有効な受信者のドメインに安全にメッセージを送信する機能によって、宛先のドメインで DANE がサポートされていれば、組織はビジネス クリティカルな機密情報を意図した受信者に確実に送信できます。 詳細については、他の MTA との暗号化通信を参照してください。

機能	説明
スマート ソフトウェア ライセンシングのサポート	スマート ソフトウェア ライセンシングを使用すると、Cisco Email Security Appliance のライセンスをシームレスに管理およびモニタできます。スマート ソフトウェア ライセンシングをアクティブ化するには、Cisco Smart Software Manager（CSSM）でアプライアンスを登録する必要があります。CSSM は、購入して使用するすべてのシスコ製品についてライセンスの詳細を管理する一元化されたデータベースです。 以下は、アプライアンスでクラシック ライセンシング モードからスマート ライセンシング モードに切り替える利点です。 • クラシック ライセンス モードでは困難だった、物理アプライアンスと仮想アプライアンス間の製品認証キー（PAK）ライセンスの管理が簡単に行えます。 • 組織内のデバイスまたはアカウント間で、ソフトウェア ライセンスを簡単に移行できます。 • アプライアンスで PAK ファイルを管理したり、コピーを維持する必要がありません。 • スマート ライセンシング アカウントでは、ユーザのアクセスを制限できます。 **注意** アプライアンスでスマート ライセンシング機能を有効にすると、スマート ライセンシングからクラシック ラインセンシング モードにロールバックすることができなくなります。 詳細は、 システム管理 および『 *CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*』を参照してください。

機能	説明
偽装メールの検出	[メールポリシー（Mail Policies）] > [アドレスリスト（Address Lists）] を選択して、完全な電子メール アドレスのみで構成された例外リストを作成することで、[偽装電子メール検出（Forged Email Detection）] コンテンツ フィルタをバイパスできるようになりました。アプライアンスで、設定済みのコンテンツ フィルタから電子メール アドレスをスキップする場合、偽装電子メール検出ルールでこの例外リストを使用できます。詳細は、ユーザ ガイドの「Content Filters」の章を参照してください。
ログ サブスクリプションの強化	レート制限オプションを使用して、指定した時間範囲（秒単位）内での、ログ ファイルにログ記録されるイベントの最大数を設定することができます。デフォルトの時間範囲の値は 10 秒です。Web インターフェイスの [システム管理（System Administration）] > [ログサブスクリプション（Log Subscriptions）] ページを使用するか、CLI の logconfig コマンドを使用して、レート制限を設定します。詳細は、ユーザ ガイドの「Logging」の章を参照してください。

機能	説明
DMARC 検証をスキップしたメッセージを処理するためにコンテンツ フィルタとメッセージ フィルタを設定	DMARC 検証をスキップしたメッセージに対してアクションを実行するようにアプライアンスを設定できます。 Other Header コンテンツ フィルタで次の設定を使用して、DMARC検証をスキップしたメッセージを分類します。 • ヘッダー名を「X-Ironport-Dmarc-Check-Result」として追加します。 • [Header Value] を選択して、[Equals] を選択し、validskip、invalidskip、temperror、permerror のいずれかの値を追加します。 DMARC 検証をスキップしたメッセージの分類に使用するメッセージフィルタ ルールの構文の例を次に示します。 Quarantine_messages_DMARC_skip: if(header("X-Ironport-Dmarc-Check-Result") == "^validskip$") { quarantine("Policy"); } コンテンツ フィルタとメッセージフィルタで使用されるヘッダー値の詳細については、Cisco TAC にお問い合わせください。
シスコのコンテンツ セキュリティ管理アプライアンス接続パラメータとホスト キーを表示または削除する機能	`smaconfig` CLI コマンドを使用して、アプライアンスでシスコのコンテンツ セキュリティ管理アプライアンス接続パラメータとホストキーを表示または削除できるようになりました。

機能	説明
インテリジェント マルチスキャンの強化	インテリジェントマルチスキャン（IMS）は、パフォーマンスの高いマルチレイヤ スパム対策ソリューションです。Eメールセキュリティアプライアンスの本リリースは、最新の IMS エンジンを提供します。このエンジンは、スパム対策エンジンの様々に組み合わせることによってスパム検出率を向上します。 最新の IMS エンジンを使用するには、IMS 機能キーを追加し、アプライアンスでライセンスを承認する必要があります。既存のIMSユーザの場合は、IMS のすべてのメール ポリシーが移行され、最新の IMS エンジンでシームレスに機能します。 詳細については、スパムおよびグレイメールの管理を参照してください。

機能	説明
カスタム DLP ポリシーに向けたエンティティベースのカスタム分類子ルールの最小スコア	カスタム DLP ポリシーに向けてカスタム分類子を作成する際に、推奨される最小スコアを使用するか、エンティティ ベースのルールの最小スコアを上書きすることを選択できるようになりました。 設定されたルールの重みに代わって、エンティティ ベースのルールの最小スコアを使用できます。最小スコアは部分的一致と完全一致を区別し、それに従ってスコアを計算します。これにより、誤検出と検出漏れの数を削減できます。 以下の方法で最小スコアを設定します。 1. [メールポリシー（Mail Policies）] > [DLP ポリシーカスタマイズ（DLP Policy Customizations）] > [カスタム分類子設定（Custom Classifiers Settings）] セクションで、[エンティティベースのルールで推奨される最小スコアを使用（Use recommended minimum scores for entity-based rules）] チェックボックスを選択します。 2. [メールポリシー（Mail Policies）] > [DLP ポリシーカスタマイズ（DLP Policy Customizations）] > [カスタム分類子の追加（Add Custom Classifier）] に移動し（または既存のカスタム分類子を確認し）、最小スコアを入力します。 詳細については、データ損失の防止を参照してください。

詳細情報の入手先

シスコでは、アプライアンスに関する理解を深めて頂くために次の資料を提供しています。

- 資料 （13 ページ）
- トレーニング （14 ページ）
- Cisco 通知サービス （14 ページ）
- ナレッジ ベース （14 ページ）
- シスコ サポート コミュニティ （14 ページ）
- シスコ カスタマー サポート （15 ページ）

• サード パーティ コントリビュータ （15 ページ）
• マニュアルに関するフィードバック （15 ページ）
• Cisco アカウントの登録 （15 ページ）

資料

アプライアンスの GUI で右上の [ヘルプとサポート（Help and Support）] をクリックすることにより、ユーザ ガイドのオンライン ヘルプ バージョンに直接アクセスできます。

Cisco Email Security Appliances のマニュアル セットには次のマニュアルおよびマニュアルが含まれます。

- リリース ノート
- ご使用の Cisco Email Security Appliances モデルのクイック スタート ガイド
- ご使用のモデルまたはシリーズのハードウェア インストール ガイドまたはハードウェア インストールおよびメンテナンス ガイド
- 『*Cisco Content Security Virtual Appliance Installation Guide*』
- 『Cisco Cisco Email Security Appliances 向け AsyncOS ユーザ ガイド』（本書）
- 『*CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*』
- 『AsyncOS API for Cisco Email Security Appliances - Getting Started Guide』

Cisco Content Security 製品のすべてに関する資料が以下で入手できます。

Cisco コンテンツ セキュリティ製品のマニュアル	**参照先**
ハードウェアおよび仮想アプライアンス	この表で該当する製品を参照してください。
Cisco E メール セキュリティ	http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html
Cisco Web セキュリティ	http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html
Cisco コンテンツ セキュリティ管理	http://www.cisco.com/c/en/us/support/security/content-security-management- appliance/tsd-products-support-series-home.html
Cisco コンテンツ セキュリティ アプライアンスの CLI リファレンス ガイド	http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-command-reference-list.html
Cisco IronPort 暗号化	http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-command-reference-list.html

トレーニング

シスコでは、技術者、パートナー、学生など、それぞれのニーズに合わせた、さまざまなトレーニング プログラムおよびトレーニング コースを用意しています。

- http://www.cisco.com/c/en/us/training-events/training-certifications/supplemental-training/email-and-web-security.html
- http://www.cisco.com/c/en/us/training-events/training-certifications/overview.html

Cisco 通知サービス

セキュリティ アドバイザリ、フィールド ノーティス、販売終了とサポート終了の通知、およびソフトウェア アップデートと既知の問題に関する情報などの Cisco コンテンツ セキュリティ アプライアンスに関連する通知が配信されるように署名して参加します。

受信する情報通知の頻度やタイプなどのオプションを指定できます。使用する製品ごとの通知に個別に参加する必要があります。

参加するには、http://www.cisco.com/cisco/support/notifications.html に移動します。

Cisco.com アカウントが必要です。ない場合は、Cisco アカウントの登録 （15 ページ）を参照してください。

ナレッジ ベース

手順

ステップ 1 製品のメイン ページ（http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html）にアクセスします。

ステップ 2 名前に **TechNotes** が付くリンクを探します。

シスコ サポート コミュニティ

シスコ サポート コミュニティは、シスコのお客様、パートナー、および従業員のオンライン フォーラムです。電子メールおよび Web セキュリティに関する一般的な問題や、特定のシスコ製品に関する技術情報について話し合う場を提供します。このフォーラムにトピックを投稿して質問したり、他のシスコ ユーザと情報を共有したりできます。

Customer Support Portal のシスコ サポート コミュニティには、次の URL からアクセスします。

- 電子メール セキュリティと関連管理:

  https://supportforums.cisco.com/community/5756/email-security

- Web セキュリティと関連管理：

https://supportforums.cisco.com/community/5786/web-security

シスコ カスタマー サポート

シスコ TAC：http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

従来の IronPort のサポート サイト：http://www.cisco.com/c/en/us/services/acquisitions/ironport.html

重大ではない問題の場合は、アプライアンスからカスタマーサポートにアクセスすることもできます。手順については、ユーザ ガイドまたはオンライン ヘルプを参照してください。

サードパーティ コントリビュータ

次のページにある、ご使用のリリースのオープン ソース ライセンス情報を参照してください。http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-release-notes-list.html
.

Cisco AsyncOS 内に付属の一部のソフトウェアは、FreeBSD、Stichting Mathematisch Centrum、Corporation for National Research Initiatives などのサードパーティ コントリビュータのソフトウェア使用許諾契約の条項、通知、条件の下に配布されています。これらすべての契約条件は、Cisco ライセンス契約に含まれています。

これらの契約内容の全文は次の URL を参照してください。

https://support.ironport.com/3rdparty/AsyncOS_User_Guide-1-1.html.

Cisco AsyncOS 内の一部のソフトウェアは、Tobi Oetiker の書面による同意を得て、RRDtool を基にしています。

このマニュアルには、Dell Computer Corporation の許可を得て複製された内容が一部含まれています。このマニュアルには、McAfee の許可を得て複製された内容が一部含まれています。このマニュアルには、Sophos の許可を得て複製された内容が一部含まれています。

マニュアルに関するフィードバック

シスコのテクニカル マニュアル チームは、製品ドキュメントの向上に努めています。コメントおよびご提案をお待ちしています。ぜひ以下の電子メールまでお知らせください。

contentsecuritydocs@cisco.com

メッセージの件名には、製品名、リリース番号、このマニュアルの発行日をご記入ください。

Cisco アカウントの登録

Cisco.com の多数のリソースへアクセスするには、シスコのアカウントが必要です。

Cisco.com のユーザ ID をお持ちでない場合は、https://tools.cisco.com/RPF/register/register.do%20 で登録できます。

関連項目

- Cisco 通知サービス （14 ページ）
- ナレッジ ベース （14 ページ）

Cisco Email Security Appliances の概要

AsyncOS™ オペレーティング システムには、次の機能が組み込まれています。

- SenderBase レピュテーション フィルタと Cisco Anti-Spam を統合した独自のマルチレイヤ アプローチによるゲートウェイでの**スパム対策**。
- SophosおよびMcAfeeウイルス対策スキャンエンジンによるゲートウェイでの**ウイルス対策**。
- 新しいアップデートが適用されるまで危険なメッセージを隔離し、新しいメッセージ脅威に対する脆弱性を削減する、新しいウイルス、詐欺、およびフィッシングの拡散に対するシスコの独自保護機能である**アウトブレイク フィルタ™**。
- **ポリシー、ウイルス、およびアウトブレイク検疫**は、疑わしいメッセージを保存して管理者が評価するための安全な場所を提供します。
- 隔離されたスパムおよび陽性と疑わしいスパムへのエンドユーザアクセスを提供する、オンボックスまたはオフボックスの**スパム隔離**。
- **電子メール認証**。Cisco AsyncOS は、発信メールに対する DomainKeys および DomainKeys Identified Mail（DKIM）の署名の他に、着信メールに対する Sender Policy Framework（SPF）、Sender ID Framework（SIDF）、DKIM の検証など、さまざまな形式の電子メール認証をサポートします。
- Cisco **電子メール暗号化**。HIPAA、GLBA、および同様の規制要求に対応するために発信メールを暗号化できます。これを行うには、E メール セキュリティ アプライアンスで暗号化ポリシーを設定し、ローカル キー サーバまたはホステッド キー サービスを使用してメッセージを暗号化します。
- アプライアンス上のすべての電子メール セキュリティ サービスおよびアプリケーションを管理する、単一で包括的なダッシュボードである**電子メール セキュリティ マネージャ**。電子メール セキュリティ マネージャは、ユーザ グループに基づいて電子メール セキュリティを実施でき、インバウンドとアウトバウンドの独立したポリシーを使用して、Cisco レピュテーションフィルタ、アウトブレイク フィルタ、アンチスパム、アンチウイルス、および電子メール コンテンツ ポリシーを管理できます。
- **オンボックスのメッセージ トラッキング**。AsyncOS for Email には、電子メール セキュリティアプライアンスが処理するメッセージのステータスの検索が容易にできる、オンボックスのメッセージ トラッキング機能があります。
- 企業のすべての電子メール トラフィックを全体的に確認できる、すべてのインバウンドおよびアウトバウンドの電子メールに対する**メール フロー モニタ機能**。
- 送信者の IP アドレス、IP アドレス範囲、またはドメインに基づいた、インバウンドの送信者の**アクセス制御**。
- 広範な**メッセージおよびコンテンツ フィルタリング** テクノロジーを使用して、社内ポリシーを順守させ、企業のインフラストラクチャを出入りする特定のメッセージに作用させることができます。フィルタ ルールでは、メッセージまたは添付ファイルの内容、ネット

ワークに関する情報、メッセージ エンベロープ、メッセージ ヘッダー、またはメッセージ本文に基づいてメッセージを識別します。フィルタ アクションでは、メッセージをドロップ、バウンス、アーカイブ、ブラインド カーボン コピー、または変更したり、通知を生成したりできます。

- **セキュアな SMTP over Transport Layer Security 経由のメッセージの暗号化**により、企業のインフラストラクチャとその他の信頼できるホストとの間でやりとりされるメッセージが暗号化されるようなります。
- **Virtual Gateway™** テクノロジーにより、E メール セキュリティ アプライアンスは、単一サーバ内で複数の電子メール ゲートウェイとして機能できるため、さまざまな送信元またはキャンペーンの電子メールを、それぞれ独立した IP アドレスを通して送信するように分配できます。これにより、1 つの IP アドレスに影響する配信可能量の問題が、他の IP アドレスに及ばないようにします。
- 複数のサービスによって提供される、電子メール メッセージ内の**悪意のある添付ファイルやリンクからの保護**。
- **データ損失防止**により、組織から出る情報の制御と監視を行います。

AsyncOS は、メッセージを受け入れて配信するために、RFC 2821 準拠の Simple Mail Transfer Protocol（SMTP）をサポートします。

レポート作成コマンド、モニタリング コマンド、およびコンフィギュレーション コマンドのほとんどは、HTTP 経由でも HTTPS 経由でも Web ベースの GUI から使用できます。さらに、セキュア シェル（SSH）または直接シリアル接続でアクセスするインタラクティブなコマンドライン インターフェイス（CLI）がシステムに用意されています。

また、複数の E メール セキュリティ アプライアンスのレポート、トラッキング、および隔離管理を統合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。

関連項目

- サポートされる言語 （17 ページ）

サポートされる言語

AsyncOS は次の言語のいずれかで GUI および CLI を表示できます。

- 英語
- フランス語
- スペイン語
- ドイツ語
- イタリア語
- 韓国語
- 日本語
- ポルトガル語（ブラジル）
- 中国語（繁体字および簡体字）
- ロシア語