Cisco Secure Email Gateway スタートアップガイド

この章は、次の項で構成されています。

AsyncOS 14.0 の新機能

表 *1 : AsyncOS 14.0* の新機能

機能	説明
Cisco Secure Email Gateway と Cisco Secure Awareness クラウドサービスの統合	Cisco Secure Awareness クラウドサービスを使用すると、フィッシング シミュレーション、意識向上トレーニング、またはその両方を効果的に展開して、結果を測定およびレポートできます。これにより、セキュリティ運用チームは、エンドユーザの状況緩和ではなく、リアルタイムの脅威に集中できます。 Cisco Secure Awareness クラウドサービスは、リピートクリッカー（任意の URL または電子メールで送信された添付ファイルを繰り返しクリックするユーザ）のレポートを提供します。これらのユーザは、Cisco Secure Awareness クラウドサービスによって定義されたフィッシング シミュレーション キャンペーンによって識別されます。 電子メールゲートウェイを Cisco Secure Awareness クラウドサービスと統合することで、組織は次のことが可能になります。 • 実際のフィッシング攻撃に対するユーザの認識が向上します。 • メール管理者は、Cisco Secure Awareness クラウドサービスによって「リピートクリッカー」として識別された一連のユーザに対して厳格なポリシーを設定できます。 詳細については、電子メールゲートウェイと Cisco Secure Awareness クラウドサービスの統合を参照してください。

機能	説明
電子メールゲートウェイのフィッシング検出の改善	電子メールゲートウェイのフィッシング検出を改善するために行われた拡張は次のとおりです。 • 送信者ドメイン レピュテーション フィルタリングの機能拡張 • メッセージ添付ファイルのURLのデフォルトスキャン **送信者ドメイン レピュテーション フィルタリングの拡張**：SMTPカンバセーションレベルでSDR（送信者ドメインレピュテーション）の判定に基づいてメッセージをブロックするように電子メールゲートウェイを設定できます。 メールフローポリシー構成の設定を使用して、SDR 検証を有効または無効にできます。 （注） デフォルトでは、SDR検証は受信メールフローポリシーの場合は有効で、発信メールフローポリシーの場合は無効です。 **メッセージ添付ファイルのURLのデフォルトスキャン**：デフォルトでは、電子メールゲートウェイは、電子メールパイプラインの初期（アンチスパムエンジンの前）に悪意のあるコンテンツがないか、メッセージ添付ファイルの URL をスキャンします。 SMTPカンバセーションレベルでのSDR判定とメッセージ添付ファイルの URL のデフォルトスキャンに基づいてメッセージをブロックする機能は、組織が次のことを行うのに役立ちます。 • フィッシングおよびドメインスプーフィングにおける有効性の検出が向上します。 • SDR レピュテーション判定で実行されたデフォルトアクションに基づいて、電子メールパイプラインで早期にフィッシング攻撃を検出します。 詳細については、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ホスト アクセス テーブルを使用した接続を許可するホストの定義を参照してください。

機能	説明
メッセージ内のパスワードで保護された添付ファイルのスキャン	

機能	説明
	電子メールゲートウェイのコンテンツスキャナを設定して、着信メッセージまたは発信メッセージ内のパスワードで保護された添付ファイルの内容をスキャンできます。 電子メールゲートウェイでパスワードで保護されたメッセージの添付ファイルをスキャンする機能は、組織が次のことを行うのに役立ちます。 • 限られたサイバー攻撃をターゲットとするパスワード保護されたメッセージ内の添付ファイルとしてマルウェアを使用するフィッシングキャンペーンを検出します。 • 悪意のあるアクティビティやデータのプライバシーについてパスワードで保護された添付ファイルを含むメッセージを分析します。 この機能では、英語、イタリア語、ポルトガル語、スペイン語、ドイツ語、およびフランス語がサポートされています。 ユーザ定義のパスフレーズを作成して、次のいずれかの方法で、着信メッセージまたは発信メッセージ内のパスワードで保護された添付ファイルを開くことができます。 • Web インターフェイスの [セキュリティサービス（Security Services）] > [スキャン動作（Scan Behavior）] ページ。 • CLI の `scanconfig` > `protectedattachmentconfig` サブコマンド。 このリリースでは、コンテンツスキャナは次のファイルタイプのパスワードで保護された添付ファイルの内容のみをスキャンできます。 • Adobe Portable Document Format（PDF）ファイル。 • 次の MS Office ファイルタイプ： • Word：2002 ～ 2004 のバージョンをサポートする .doc ファイル形式および 2007 ー 2016 のバージョンをサポートする .docx ファイル形式。 • Excel：2007 ～ 2016 のバージョンをサポートする .xls および .xlsx ファイル形式。 • PowerPoint：2007 ～ 2016 のバージョンをサポー

機能	説明
	トする .ppt または .pptx ファイル形式。 • アーカイブファイルタイプ：.zip 形式。 詳細については、メッセージ フィルタを使用した電子メール ポリシーの適用を参照してください。
簡易ネットワーク管理プロトコル（SNMP）の機能拡張	SNMP の設定に関する機能拡張は、次のとおりです。 • 追加のモニタリング用に新しい SNMP MIB が追加されました。 • SNMPv3トラップのサポート： • SNMPv3 は、noAuthNoPriv、authNoPriv、authPriv の 3 つのセキュリティレベルをすべてサポートします。 • SNMPv3 と SNMPv2 の両方が有効になっている場合、トラップに必要なバージョンを選択する必要があります。 • `snmpconfig` CLI コマンドに、SNMPv2 と SNMPv3 の両方が有効な場合にトラップバージョンを選択するための新しいオプションが追加されました。 詳細については、CLIによる管理およびモニタリングを参照してください。
メールポリシーの詳細に関する新しいレポート	新しいレポート：[メールポリシーの詳細（Mail Policy Details）] が電子メールゲートウェイの新しい Web インターフェイスに追加されています。このレポートを使用して、設定されたメールポリシーに一致するメッセージの数を表示します。 詳細については、電子メール セキュリティ モニタの使用方法を参照してください。

機能	説明
メールポリシーの詳細に関する新しいメッセージ トラッキング フィルタ	新しいメッセージ トラッキング フィルタ：[メールポリシー（Mail Policy）] が、電子メールゲートウェイの新しい Web インターフェイスの [メッセージトラッキング（Message Tracking）] > [詳細検索（Advanced Search）] > [メッセージイベント（Message Event）] オプションに追加されています。[メールポリシー名（Mail Policy Name）] フィールドに入力された設定済みメールポリシー名と一致する受信メッセージまたは発信メッセージを検索するには、このオプションを使用します。
拡張された [概要（Overview）] および [受信メールサマリー（Incoming Mail Summary）] レポートページ	電子メールゲートウェイのレガシー Web インターフェイスの [概要（Overview）] レポートページと [受信メール（Incoming Mail）] レポートページで行われた機能拡張は次のとおりです。 [概要（Overview）] レポートページ： • [受信メールサマリー（Incoming Mail Summary）] セクションに新しいメッセージカテゴリ [ドメインレピュテーションフィルタによる停止（Stopped by Domain Reputation Filtering）] が追加されました。 • [受信メールの概要（Incoming Mail Summary）] セクションの [レピュテーションフィルタによる停止（Stopped by Reputation Filtering）] メッセージカテゴリ名が [IP レピュテーションフィルタによる停止（Stopped by IP Reputation Filtering）] に変更されました。 [受信メール（Incoming Mail）] レポートページ： • [受信メールの詳細（Incoming Mail Details）] セクションに [ドメインレピュテーションフィルタによる停止（Stopped by Domain Reputation Filtering）] という新しい列が追加されました。 • [受信メールの詳細（Incoming Mail Details）] セクションの [レピュテーションフィルタによる停止（Stopped by Reputation Filtering）] 列の名前が [IP レピュテーションフィルタによる停止（Stopped by IP Reputation Filtering）] に変更されました。 詳細については、電子メール セキュリティ モニタの使用方法を参照してください。

機能	説明
[メールフロー概要（Mail Flow Summary）]および[メールフローの詳細（Mail Flow Details）] レポートページの拡張	

機能	説明
	電子メールゲートウェイの新しい Web インターフェイスの [メールフロー概要（Mail Flow Summary）] レポートページと [メールフローの詳細（Mail Flow Details）] レポートページで行われた機能拡張は次のとおりです。 [メールフロー概要（Mail Flow Summary）] レポートページ • [脅威メッセージ（Threat Messages）] グラフセクションに新しいカテゴリ [ドメインレピュテーションフィルタによる停止（Stopped by Domain Reputation Filtering ）] が追加されました。 • [脅威メッセージ（Threat Messages）] グラフセクションの [レピュテーションフィルタによる停止（Stopped by Reputation Filtering）] カテゴリ名が [IP レピュテーションフィルタよる停止（Stopped by IP Reputation Filtering）] に変更されました。 • [脅威検出のサマリー（Threat Detection Summary）] セクションに [ドメインレピュテーションフィルタによる停止（Stopped by Domain Reputation Filtering）] という新しい列が追加されました。 • [脅威検出のサマリー（Threat Detection Summary）] セクションの [レピュテーションフィルタによる停止（Stopped by Reputation Filtering）] 列の名前が [IP レピュテーションフィルタによる停止（Stopped by IP Reputation Filtering）] に変更されました。 [メールフローの詳細（Mail Flow Details）] レポートページ： • [IPアドレス（IP Addresses）]、[ドメイン（Domains）]、および [ネットワーク所有者（Network Owners）] の [受信メール（Incoming Mails）] セクションに [ドメインレピュテーションフィルタによる停止（Stopped by Domain Reputation Filtering）] という新しい列が追加されました。 • [IPアドレス（IP Addresses）]、[ドメイン（Domains）]、および [ネットワーク所有者（Network Owners）] の [受信メール（Incoming Mails）] セクションで [レピュテーションフィルタによる停止（Stopped by Reputation Filtering）] 列の名前が [IPレピュテーションフィルタによる停止（Stopped by IP Reputation Filtering）] に変更されま

機能	説明
	した。
国際化ドメイン名（IDN）のサポート	Cisco Secure Email Gateway 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、電子メール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。 詳細については、システム管理を参照してください。
セキュリティ機能の拡張	AsyncOS 14.0 には、次のセキュリティ機能拡張が含まれています。 • 電子メールゲートウェイは TLS を介してシスコテクニカルサポート要求を送信するようになりました。SMTP サーバが 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電子メールゲートウェイを設定できるようになりました。CLI で次のサブコマンドを使用してこの機能を設定します。 `alertconfig > SETUP > Do you want to enable TLS support to send alert messages?` 詳細については、このリリースに関連する『CLI Reference Guide』を参照してください。

機能	説明
新しい修復レポートステータスウィジェット	電子メールゲートウェイの新しい Web インターフェイスの [メッセージトラッキング（Message Tracking）] ページでメッセージを検索および修復すると、新しいウィジェットの [修復レポートステータス（Remediation Report Status）] が追加されます。 このウィジェットを使用して修復レポートの生成ステータスを確認します。詳細については、メールボックスでのメッセージの修復を参照してください。

機能	説明
新しいコンテンツ照合分類子のサポート：東南アジア各国の国民識別番号	次の新しいコンテンツ照合分類子のいずれかを使用してDLPポリシーを作成できます。 • インドネシア KTP • マレーシア MyKad • タイ ID • フィリピン UMID • シンガポール NRIC 電子メールゲートウェイの Web インターフェイスの次のページで、新しいコンテンツ照合分類子を選択できます。 • [メールポリシー（Mail Policies）] > [DLP Policy Manager] > [カスタムポリシーの追加（Add Custom Policy）] ページ > [定義済みカスタム分類子（Predefined Custom Classifiers）] > **[ポリシー照合の詳細（Policy Matching Details）]** オプションに移動します。 • [メールポリシー（Mail Policies）] > [DLP Policy Manager] > [カスタムポリシーの追加（Add Custom Policy）] ページ > [カスタム分類子の作成（Create Custom Classifier）] > **[エンティティルール（Entity rule）]** オプションに移動します。 • [メールポリシー（Mail Policies）] > [DLP Policy Manager] > [DLPポリシーの追加（Add DLP Policy）] ページ > **[プライバシー保護（Privacy Protection）] テンプレート**オプションに移動します。 • [メールポリシー（Mail Policies）] > [DLPポリシーのカスタマイズ（DLP Policy Customizations）] > [カスタム分類子の追加（Add Custom Classifier）] ページ > **[エンティティルール（Entity rule）]** オプションに移動します。

機能	説明
製品および関連資料でのバイアスフリー用語の使用方法	製品および関連資料のバイアス用語を削除しました。 次に、新しいバイアスフリー用語に置き換えられたバイアス用語のリストを示します。 • 「ホワイトリスト」を「許可リスト」に置き換え • 「ブラックリスト」を「ブロックリスト」に置き換え • 「マスター」を「プライマリ」に置き換え • 「スレーブ」を「セカンダリ」に置き換え • 「ブラックホール」を「シンクホール」に置き換え
ブランド変更後の製品と関連資料	製品と関連資料のブランドを次のように変更しました。 • Cisco E メール セキュリティ アプライアンスを *Cisco Secure Email Gateway* に変更 • Cisco クラウド E メール セキュリティ アプライアンスを *Cisco Secure Email Cloud Gateway* に変更 • Cisco コンテンツ セキュリティ管理アプライアンスを *Cisco Secure Email and Web Manager* に変更
ファイル分析用の AMP アップストリームのプロキシ設定	ファイル分析用のアップストリームのプロキシを設定できるようになりました。 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。
Cisco SecureX Threat Response 内のメッセージに対する修復アクションの実行	Cisco SecureX Threat Response では、電子メールゲートウェイで処理されたメッセージに対して次の修復アクションを調査して適用できるようになりました。 • 削除（Delete） • 転送（Forward） • 転送と削除（Forward and Delete） 詳細については、Cisco SecureX Threat Response との統合を参照してください。

機能	説明
コンテンツフィルタ：添付ファイル情報の条件と添付ファイル情報による削除アクションの機能強化	新しいオプション：**ファイルハッシュリスト**がコンテンツフィルタの[添付ファイル情報（Attachment File Info）]の条件と[添付ファイル情報による削除（Strip by Attachment File Info）]アクションに追加されました。 このオプションを使用して、選択したファイルハッシュリスト内の特定のファイル SHA-256 値に一致するメッセージ添付ファイルに対してアクションを実行するようにコンテンツフィルタを設定します。 （注） メッセージフィルタを使用してこの機能を設定することもできます。 詳細については、コンテンツ フィルタおよびメッセージ フィルタを使用した電子メール ポリシーの適用を参照してください。
スマート ソフトウェア ライセンシングの機能強化	AsyncOS 14.0 には、次のスマート ソフトウェア ライセンシングの拡張機能が含まれています。 • クラスタ構成では、スマート ソフトウェア ライセンシングを有効にして、すべてのマシンを同時に Cisco Smart Software Manager に登録できるようになりました。 • スマート ソフトウェア ライセンシングを有効にし、電子メールゲートウェイを Cisco Smart Software Manager に登録すると、Cisco Cloud Services ポータルが自動的に有効になり、電子メールゲートウェイに登録されます。 • Cisco Cloud Services 証明書の有効期限が切れている場合は、CLI で `cloudserviceconfig > fetchcertificate` サブコマンドを使用して Cisco Talos Intelligence Services ポータルから新しい証明書をダウンロードできます。 • Cisco Smart Software Manager ポータルで作成されたスマートアカウントの詳細を表示するには、CLI で `smartaccountinfo` コマンドを使用します。 詳細については、システム管理およびCisco SecureX Threat Response との統合を参照してください。

機能	説明
AsyncOS 14.0 リリース後の送信者ドメインの経過時間機能のサポートなし	AsyncOS 14.0 リリース以降、送信者ドメインの経過時間機能はサポートされません。送信者ドメインの経過時間機能は、送信者の成熟度機能に置き換えられます。 [送信者の成熟度（Sender Maturity）] は、電子メール送信者としてのドメインの成熟度に関する Cisco Talos の見解を表します。成熟度の値は、電子メールに関する脅威の検出を有効にするように調整されており、通常は「Whois-based domain age」で表されるドメインの経過時間は反映されません。[送信者の成熟度（Sender Maturity）] は 90 日の制限に設定されており、この制限を超えるとドメインは電子メール送信者として成熟していると見なされてそれ以上の詳細は提供されません。 送信者の成熟度は送信者のレピュテーションの計算に使用されます。未熟なドメインには低いレピュテーションが割り当てられます。Cisco Talos では、ポリシーアクションの決定にのみ送信者のレピュテーションを使用することを推奨しています。送信者の成熟度は、特定の標準外シナリオに合わせてフィルタを微調整するために使用されます。 （注） Cisco Talos ではドメインの成熟度を手動で調整しませんが、最適な値を決定するために自動システムとセンサーに依存します。
サポート終了（EOL）またはサービス終了（EOS）の AsyncOS バージョンまたはハードウェアモデルに対するアラートまたは通知バナー	電子メールゲートウェイがサポート終了（EOL）またはサービス終了（EOS）の AsyncOS バージョンまたはハードウェアモデルで実行されている場合、電子メールゲートウェイの Web インターフェイスまたは CLI で、アラートまたは通知バナーメッセージが送信されるようになりました。
Office 365 または Hybrid（Graph API）修復アカウントプロファイル設定の機能拡張	Azure 管理ポータルで生成されたアプリケーションのクライアントシークレット値を使用して、Office 365 または Hybrid（Graph API）修復アカウントプロファイルのクライアントクレデンシャルを検証できるようになりました。 詳細については、メールボックスでのメッセージの修復を参照してください。 .

機能	説明
Amazon Web Services（AWS）向けの仮想電子メールゲートウェイのサポート	Amazon Web Services（AWS）の Amazon Elastic Compute Cloud（EC2）に Cisco Secure Email 仮想ゲートウェイを展開できます。 AMI イメージをプロビジョニングするには、AWS アカウントの詳細（ユーザ名とリージョン）をシスコの営業担当者にお問い合わせください。
統合イベントログの機能拡張	[統合イベントログ（Consolidated Event Logs）] ログタイプに加えられた機能拡張は次のとおりです。 • 新しいログフィールドの [メッセージサイズ（Message Size）] が [統合イベントログ（Consolidated Event Logs）] のログタイプに追加され、単一のログ行出力にメッセージサイズが表示されます。 • メッセージの添付ファイルのサイズを 1 つのログ行の出力に表示できるようになりました **手順**： **1.** 統合イベントログのログサブスクリプションを設定する場合は、[ファイルの詳細（File(s) Details）] ログフィールドを選択します。 **2.** メッセージフィルタルールを次のように設定します。 `Custom_ Log_Entry: if (true) { log-entry("$filesizes"); }` または カスタマイズされたテキストを「`$ filesizes`」として追加して、**[ログエントリの追加（Add Log Entry）]** コンテンツ フィルタ アクションを設定します。
クラウドコネクタロギングのサポート	電子メールゲートウェイが新しいタイプのログサブスクリプションである**クラウドコネクタログ**をサポートするようになりました。このログサブスクリプションを使用して、Cisco Aggregator Server からの Web インタラクション トラッキング データに関する情報を表示します。ほとんどの情報は、[情報（Info）] または [警告（Warning）] レベルです

機能	説明
ファイル レピュテーション サービスの要求再試行方式の拡張：	ファイルレピュテーションおよび分析サービスの設定時に、レピュテーションクエリのタイムアウト値を 20 ー 30 秒の範囲で設定できるようになりました（[セキュリティサービス（Security Services）] > [ファイルレピュテーションおよび分析（File Reputation and Analysis）]）。デフォルト値は 20（最小値）です。 設定したクエリタイムアウト中に、電子メールゲートウェイはファイル レピュテーション クエリを AMP サーバに送信します。電子メールゲートウェイは AMP サーバからの応答の受信に失敗すると、AMP サーバにクエリをもう一度送信して再試行します。クエリタイムアウトには、最初のクエリ要求と再試行要求にかかった時間が含まれます。 再試行方式を使用すると、ネットワークの遅延や AMP サーバに関連する問題などがある場合に、電子メールゲートウェイが応答を受信できます。
新しい Cisco Talos 電子メールステータスポータル	Cisco Talos 電子メールステータスポータルは、従来のシスコ電子メール送信およびトラッキングポータルに変わるものです。 Cisco Talos 電子メールステータスポータルは、エンドユーザからの電子メール送信のステータスをモニタリングするための Web ベースツールです。 **重要** • 従来のポータルのユーザは、新しいポータルで以前の送信に引き続きアクセスできます。 • 新しいポータルでは電子メールゲートウェイによって誤って識別された可能性のあるスパム、フィッシング、ハム、マーケティングまたは非マーケティング電子メールのサンプル送信することはできません。電子メールサンプルの送信方法の詳細については、https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/214133-how-to-submit-email-messages-to-cisco.html にある『How to Submit Email Messages to Cisco』を参照してください。 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
認証ログの機能拡張	ログインしたユーザのユーザ権限ロールの詳細（たとえば、「admin」、「operator」など）を認証ログに表示できるようになりました。
ログインパスフレーズを定義するための新しいパスフレーズルール	新しいパスフレーズルールが電子メールゲートウェイに追加され、ログインパスフレーズが定義されます。 3 つ以上の反復文字または連続文字を含むパスフレーズ（たとえば、「AAA @ 124」、「Abc @ 123」など）は使用しないでください。 このパスフレーズルールは、次のいずれかの方法で設定できます。 • Web インターフェイスで、[システム（System）] > [管理（Administration）] > [ユーザ（Users）] > [ローカルユーザアカウントとパスフレーズの設定（Local User Account & Passphrase Settings）] > [パスフレーズに3つ以上の繰り返し文字または連続した文字を拒否する（Reject three or more repetitive or sequential characters in passphrases）] チェックボックスをオンにします。 • CLI の `userconfig` > `POLICY` > `PASSWORDSTRENGTH` > `Reject passphrases that contain three or more repetitive or sequential characters? [Y]>` コマンド

機能	説明
システム生成パスフレーズの作成	ログインパスフレーズを手動で作成することに加えて、電子メールゲートウェイにログインするためのシステム生成パスフレーズも作成できるようになりました。 システム生成のパスフレーズは次のいずれかの方法で設定できます。 • Web インターフェイスの [オプション（Options）] > [パスフレーズの変更（Change Passphrase）] ページ。 • Web インターフェイスの [システム管理（System Administration）] > [システム セットアップ ウィザード（System Setup Wizard）] ページ。 • Web インターフェイスの [システム管理（System Administration）] > [ユーザ（Users）] > [ローカル ユーザの追加（Add Local User）] ページ。 • CLI の `passphrase` コマンドまたは `passwd` コマンド 詳細については、セットアップおよび設置を参照してください。
証明書の FQDN 検証の実行	次に、証明書の FQDN 検証を実行するように電子メールゲートウェイを設定するシナリオを示します。 • カスタム証明書をインポートする。 • 自己署名 S/MIME 証明書を作成する。 • 自己署名証明書を作成する。 • カスタム認証局（CA）のリストをインポートする。 （注） IDN ドメインを含む電子メールゲートウェイ証明書の FQDN 検証も実行できます。 詳細については、S/MIME セキュリティ サービスおよび他の MTA との暗号化通信を参照してください。

機能	説明
SSL 通信中のピア証明書の FQDN 検証の実行	Web インターフェイスの [システム管理（System Administration）] > [SSL設定（SSL Configuration）] ページで、ピア証明書の FQDN 検証を実行するように電子メールゲートウェイを設定できます。 FQDN 検証は、次のサービスに適用されます。 • アウトバウンド SMTP • LDAP • アップデータ • TLS を介したアラート （注） アウトバウンド SMTP サービスに対してのみの IDN ドメインを含むピア証明書の FQDN 検証を実行できます。 詳細については、システム管理を参照してください。
SSL 通信中のピア証明書の x509 検証の実行	Web インターフェイスの [システム管理（System Administration）] > [SSL設定（SSL Configuration）] ページで、ピア証明書の x509 検証を実行するように電子メールゲートウェイを設定できます。 x509 検証は、次のサービスに適用されます。 • アウトバウンド SMTP • LDAP • アップデータ • TLS を介したアラート 詳細については、システム管理を参照してください。

機能	説明
電子メールゲートウェイで SecureX Threat Response フィードの使用を設定	Cisco SecureX Threat Response ポータルから脅威フィードを使用するように電子メールゲートウェイを設定できるようになりました。 Cisco SecureX Threat Response ポータルでは、監視対象を継続的に収集するためのカスタムフィードを作成し、フィード URL を使用して電子メールゲートウェイでそれらを利用できます。フィードは、JSON 形式の監視対象の単純なリストです。フィードは、SecureX Threat Response ポータルの [インテリジェンス（Intelligence）] > [フィード（Feeds）] ページで作成および管理されます。 詳細については、外部脅威フィードを使用する電子メールゲートウェイの設定を参照してください。

Webインターフェイスの比較、新しいWebインターフェイスとレガシー Web インターフェイス

次の表は、新しい Web インターフェイスの以前のバージョンとの比較を示しています。

表 *2*：新しい *Web* インターフェイスとレガシー *Web* インターフェイスとの比較

Web インターフェイス ページまたは要素	新しい Web インターフェイス	レガシー Web インターフェイス
ランディングページ	電子メールゲートウェイにログインすると、[メールフロー概要（Mail Flow Summary）] ページが表示されます。	電子メールゲートウェイにログインすると、[マイダッシュボード（My Dashboard）] ページが表示されます。
レポートドロップダウン	[レポート（Reports）] ドロップダウンで、電子メールゲートウェイのレポートを表示できます。	[モニタ（Monitor）] メニューで、電子メールゲートウェイのレポートを表示できます。
[マイ レポート（My Reports）] ページ	[レポート（Reports）] ドロップダウンから [マイレポート（My Reports）] を選択します。	[マイレポート（My Reports）] ページは、[モニタ（Monitor）] > [マイダッシュボード（My Dashboard）] から表示できます。

Web インターフェイス ページまたは要素	新しい Web インターフェイス	レガシー Web インターフェイス
[メール フロー概要（Mail Flow Summary）] ページ	[メールフロー概要（Mail Flow Summary）]ページには、着信および送信メッセージに関するトレンド グラフやサマリー テーブルが表示されます。	[受信メール（Incoming Mail）]には、着信および発信メッセージに関するグラフやサマリー テーブルが含まれます。
高度なマルウェア防御レポートページ	[レポート（Reports）] メニューの [高度なマルウェア防御（Advanced Malware Protection）] レポートページでは、次のセクションを使用できます。 • [概要（Overview）] • [AMP ファイル レピュテーション（AMP File Reputation）] • [ファイル分析（File Analysis）] • [ファイル レトロスペクション（File Retrospection）] • [メールボックスの自動修復（Mailbox Auto Remediation）]	電子メールゲートウェイの [モニタ（Monitor）] メニューには、次の [高度なマルウェア防御（Advanced Malware Protection）] レポートページがあります。 • [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）] • [メールボックスの自動修復（Mailbox Auto Remediation）]
アウトブレイク フィルタ ページ	新しい Web インターフェイスの [アウトブレイクフィルタリング（Outbreak Filtering）] レポート ページでは、[過去1年間のウイルスアウトブレイク（Past Year Virus Outbreaks）] および [過去1年間のウイルスアウトブレイクの概要（Past Year Virus Outbreak Summary）] は使用できません。	[モニタ（Monitor）] > [アウトブレイクフィルタ（Outbreak Filters）] ページには、[過去1年間のウイルスアウトブレイク（Past Year Virus Outbreaks）] および [過去1年間のウイルスアウトブレイクの概要（Past Year Virus Outbreak Summary）] が表示されます。

Web インターフェイス ページまたは要素	新しい Web インターフェイス	レガシー Web インターフェイス
スパム隔離（管理ユーザおよびエンド ユーザ）	新しい Web インターフェイスで **[隔離（Quarantine）] > [スパム隔離（Spam Quarantine）] > [検索（Search）]** をクリックします。 エンドユーザは、次の URL を使用してスパム隔離にアクセスできます。 `https://example.com:<https-api-port>/euq-login` `example.com` はアプライアンス ホスト名で、`<https-api-port>` はファイアウォールで開いている AsyncOS API HTTPS ポートです。	スパム隔離は、[モニタ（Monitor）] > [スパム隔離（Spam Quarantine）] から表示できます。
ポリシー、ウイルスおよびアウトブレイク隔離	新しい Web インターフェイスで **[隔離（Quarantine）] > [その他の隔離（Other Quarantine）]** をクリックします。 新しい Web インターフェイスでは、[ポリシー、ウイルス、およびアウトブレイク隔離（Policy, Virus and Outbreak Quarantines）] のみを表示できます。	電子メールゲートウェイでは、[モニタ（Monitor）] > [ポリシー、ウイルス、およびアウトブレイク隔離（Policy, Virus and Outbreak Quarantines）] を使用して、ポリシー、ウイルス、およびアウトブレイク隔離を表示、設定、および変更できます。
隔離内のメッセージに対するすべてのアクションの選択	複数（またはすべて）のメッセージを選択し、削除、遅延、リリース、移動などのメッセージ アクションを実行できます。	複数のメッセージを選択して、メッセージ アクションを実行することはできません。
添付ファイルの最大ダウンロード制限	隔離されたメッセージの添付ファイルのダウンロードの上限は 25 MB に制限されています。	-

Web インターフェイス ページまたは要素	新しい Web インターフェイス	レガシー Web インターフェイス
拒否された接続	拒否された接続を検索するには、 で、[トラッキング（Tracking）] > [検索（Search）]> [拒否された接続（Rejected Connection）] タブをクリックします。	-
クエリ設定	では、メッセージトラッキング機能の [クエリ設定（Query Settings）] フィールドは使用できません。	メッセージ トラッキング機能の [クエリ設定（Query Settings）] フィールドで、クエリのタイムアウトを設定できます。
有効なメッセージ トラッキング データ	[有効なメッセージトラッキングデータ（Message Tracking Data Availability）] ページにアクセスするには、Web インターフェイスのページの右上にある歯車アイコンをクリックします。	電子メールゲートウェイの欠落データインターバルを表示することができます。
メッセージの追加詳細の表示	[判定チャート（Verdict Charts）]、[最後の状態（Last State）]、[送信者グループ（Sender Groups）]、[送信者IP（Sender IP）]、[IP レピュテーションスコア（IP Reputation Score）]、[ポリシー一致（Policy Match）] の詳細など、メッセージの追加詳細を表示できます。	-
判定チャートと最後の状態の判定	判定チャートに、電子メールゲートウェイ内の各エンジンによってトリガーされる可能性のあるさまざまな判定の情報が表示されます。 メッセージの最後の状態によって、エンジンのすべての可能な判定の後に、トリガーされる最終判定が決まります。	メッセージの判定チャートと最後の状態の判定は、使用できません。

Web インターフェイス ページまたは要素	新しい Web インターフェイス	レガシー Web インターフェイス
メッセージの詳細におけるメッセージ添付ファイルとホスト名	電子メールゲートウェイでは、メッセージの添付ファイルとホスト名は、メッセージの [メッセージの詳細（Message Details）] セクションには表示されません。	メッセージの添付ファイルとホスト名は、メッセージの [メッセージの詳細（Message Details）] セクションに表示されます。
メッセージの詳細における送信者グループ、送信者 IP、IP レピュテーションスコア、およびポリシー一致	メッセージの送信者グループ、送信者 IP、IP レピュテーションスコア、およびポリシー一致の詳細は、電子メールゲートウェイの [メッセージの詳細（Message Details）] セクションに表示されます。	メッセージの送信者グループ、送信者 IP、IP レピュテーショスコア、およびポリシー一致は、メッセージの [メッセージの詳細（Message Details）] セクションには表示されません。
メッセージの方向（受信または送信）	メッセージの方向（受信または送信）は、電子メールゲートウェイのメッセージトラッキング結果ページに表示されます。	メッセージの方向（受信または送信）は、メッセージ トラッキング結果ページには表示されません。

詳細情報の入手先

シスコでは、電子メールゲートウェイ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

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 Secure Email Gateway のマニュアルセットには次の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 Secure Email Gateway* 向け *AsyncOS* ユーザーガイド』（本書）
- 『*CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway* 』
- 『AsyncOS API for Cisco Secure Email Gateway - 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	https://www.cisco.com/c/ja_jp/support/security/email-security-appliance/series.html
Cisco Web セキュリティ	https://www.cisco.com/c/ja_jp/support/security/web-security-appliance/series.html
Cisco コンテンツ セキュリティ管理	https://www.cisco.com/c/ja_jp/support/security/content-security-management-appliance/series.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	https://www.cisco.com/c/ja_jp/support/security/email-security-appliance/products-command-reference-list.html
Cisco IronPort 暗号化	https://www.cisco.com/c/ja_jp/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、シスコ アカウントの登録 （28 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、電子メールゲートウェイ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。

シスコ 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次のリンク先で登録できます。
https://idreg.cloudapps.cisco.com/idreg/register.do

関連項目

- Cisco 通知サービス （26 ページ）
- ナレッジ ベース （27 ページ）

Cisco Secure Email Gateway 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、電子メールゲートウェイ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。
- 電子メールゲートウェイ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、電子メールゲートウェイ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、電子メールゲートウェイは、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、複数の電子メールゲートウェイのレポート、トラッキング、および隔離管理を統合するように Cisco Secure Email and Web Manager を設定できます。

関連項目

- サポートされる言語 （30 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