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 15.0 の新機能

表 *1 : AsyncOS 15.0* の新機能

機能	説明
脅威検出効果の向上	

機能	説明
	以下により、電子メールゲートウェイのセキュリティが向上しました。 • HTML 解析と悪意のあるスクリプト検出の改善。 • URL 解析とリダイレクト検出の改善。 この機能を使用するには、次の設定手順を実行します。 **1.** 次のいずれかの方法で、電子メールゲートウェイで**グレイメール** サービス エンジンをグローバルに有効化します。 **Web インターフェイス**：[セキュリティサービス（Security Services）] > [IMSおよびグレイメール（IMS and Graymail）] ページに移動し、[グレイメールのグローバル設定（Graymail Global Settings）] の下にある [グレイメール検出（Graymail Detection）] チェックボックスをオンにします。 **CLI**：`graymail > setup` サブコマンドを使用し、次のステートメントに対して **yes** と入力します：「`Would you like to use Graymail Detection? [Y]>`」 **2.** 次のように、必要な受信メールポリシーのスパム対策サービスエンジンを有効にします。 **1.** Web インターフェイスで、[メールポリシー（Mail Policies）] > [受信メールポリシー（Incoming Mail Policies）] ページに移動します。 **2.** [ポリシー（Policies）] フィールドの [スパム対策（Anti-Spam）] の下にある [無効（Disabled）] リンクをクリックします。 **3.** [IronPortスパム対策サービスを使用（Use IronPort Anti-Spam service）] または [IronPortインテリジェントマルチスキャンを使用（Use IronPort Intelligent Multi-Scan）] オプションボタンのいずれか該当するほうを選択して、メールポリシーのスパム対策スキャンを有効にします。 **4.** 陽性と判定されたスパムメッセージに適用する必要なアクション（「配信（deliver）」、「ドロップ（drop）」、「スパムの隔離（spam quarantine）」、または「バウンス（bounce）」のいずれか）を選択します。

機能	説明
	5. [オプション]：その他必要なスパム対策の設定を行います。 6. [送信（Submit）] をクリックし、変更をコミットします。 脅威検出の改善によりメッセージが「スパム」に分類されたことを示す新しい判定である**ThreatScanner スパム陽性**が、メッセージトラッキングとメールログに追加されました。**ThreatScanner スパム陽性**判定に対して推奨されるスパム対策ポリシーアクションは、[隔離（Quarantine）] です。 スパム理由データを含む**グレイメール**ログは、**情報**ログレベルで利用できます。
送信者レベルまたは受信者レベルでの発信メッセージに対する TLS の適用	既存の送信先コントロール設定を使用して、ドメインごとに TLS モード（TLS 必須、TLS 推奨など）を上書きできます。 送信者、受信者などの追加の条件に基づいて発信メッセージに TLS を適用する必要がある場合は、`X-ESA-CF-TLS-Mandatory` ヘッダーを使用できるようになりました。 [コンテンツフィルタ–ヘッダーの追加/編集（Content Filter – Add/Edit Header）] アクションを設定して、コンテンツフィルタ条件に基づいて [ヘッダー名：（Header Name:）] フィールドに `X-ESA-CF-TLS-Mandatory` ヘッダーを追加し、コンテンツフィルタを発信メールポリシーにアタッチできます。
URL レトロスペクティブ判定と URL 修復	レピュテーションが不明な URL は常に、ユーザのメールボックスに達した後であっても、悪意のあるファイルに変化する可能性があります。Talos から受信した URL レトロスペクティブ判定に基づいてアラートを送信するように、電子メールゲートウェイで URL フィルタリングを設定できます。URL 判定が不明から悪意ありに変更されたときにユーザのメールボックス内のメッセージに対して自動修復アクションを実行するように電子メールゲートウェイを設定することもできます。 詳細については、悪意のある URL または望ましくない URL からの保護を参照してください。

機能	説明
Cisco Secure Email Gateway と脅威防御の統合	Threat Defense Connector クライアントは、Cisco Secure Email Gateway を Cisco Secure Email Threat Defense に接続して、高度なフィッシングとスプーフィングのメッセージをスキャンします。 Threat Defense コネクタを設定すると、Cisco Secure Email Gateway は実際のメッセージのコピーを添付ファイルとして Threat Defense ポータルのメッセージ受信アドレスに送信します。メッセージはユーザーの受信トレイに配信され、Threat Defense ポータルで高度なスキャンが完了します。 次のいずれかの方法で、脅威防御コネクタを有効にできます。 • Web インターフェイスの [セキュリティサービス（Security Services）] > [Threat Defense Connector] ページから。 • CLI での `Threatdefenseconfig` コマンドの使用。 詳細については、Cisco Secure Email Gateway と脅威防御の統合を参照してください。
ファイル レピュテーション サービスの強化	AsyncOS 15.x リリース以降、電子メールゲートウェイは新しいバージョンの AMP エンジンを使用しています。この新しい AMP エンジンは、TCP の代わりに HTTPS（ポート 443）を使用して、電子メールゲートウェイと Cisco Secure Endpoint Cloud 間の安全な通信を保証します。 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
AsyncOS API を使用した設定情報の取得	設定 API を使用して、電子メールゲートウェイでさまざまな操作（作成、取得、更新、削除など）を実行できます。設定の各種 API カテゴリは次のとおりです。 • 認証 API • URL リスト API • ディクショナリ API • ホストアクセステーブル（HAT）API （注） 構成 API の場合、管理者およびクラウド管理者のユーザーロールのみがサポートされています。 （注） 構成 API の場合： • クラスタモードでいずれかの API を変更すると、その変更はクラスタ内の他のすべてのマシンに適用されます。 • グループモードでいずれかの API を変更すると、その変更はグループ内の他のすべてのマシンに適用されます。 • マシンモードでいずれかの API を変更すると、その変更は指定されたマシンにのみ適用されます。 詳細については、『*AsyncOS 15.0 API for Cisco Secure Email Gateway - Getting Started Guide*』の「Configuration APIs」セクションを参照してください。

機能	説明
グレイメール登録解除バナーのカスタマイズ	組織の要件に基づいて、グレイメール登録解除バナーの次の設定をカスタマイズできます。 • バナーの位置 • バナーの色 • バナーメッセージのテキストの色 • バナーメッセージの内容 バナーメッセージは、英語（米国）、イタリア語、中国語、ポルトガル語、スペイン語、ドイツ語、フランス語、ロシア語、日本語、韓国語、中国語（台湾）をサポートしています。 （注） このリリースでは、この機能に対する CLI サポートはありません。 詳細については、組織の要件に基づいたグレイメール配信停止バナーのカスタマイズを参照してください。

機能	説明

電子メールトラッキングデータ用の古い Splunk データベースの削除	[**オンプレミスユーザーのみ**]：Cisco Secure Email Gateway 15.0 以降にアップグレードし、電子メールトラッキングデータが Splunk データベースに含まれている場合、アップグレードを続行すると、システムによって Splunk データベースが削除されます。
	
	アップグレード中に、システムが Splunk データベースを削除することを示す警告メッセージが、CLI または電子メールゲートウェイの Web インターフェイスに表示されます。
	
	次に、アップグレード時に表示される警告メッセージの例を示します。
	
	`"From Secure Email Gateway 12.1.x version onwards, we have moved to a newer storage system for email tracking data.`
	`Generally, the old data is replaced with new data in the new storage system automatically.`
	`However, in some scenarios (for example, 'late upgrades', 'low mail flow' and 'tracking data', and so on),`
	`there could be traces of old data still present in the old storage system that is no longer supported.`
	`In your case it is, 7.1 MB, which was last updated in 01 Jul 2022.`
	`If you proceed with this upgrade process, the data in the old storage will be removed.`
	`You can choose to proceed with the upgrade or abort the upgrade.`
	`Do you want to proceed with the upgrade?[Y]"`
	
	（注） Splunk データベースのデバッグ情報を収集するために使用される `debug` サブメニューは、CLI の `Diagnostic` > `Tracking` サブコマンドから削除されました。
	
	[**クラウドユーザーのみ**]：Cisco Secure Email Gateway 15.0 以降にアップグレードし、電子メールトラッキングデータが Splunk データベースに含まれている場合、アップグレードを続行すると、システムによって Splunk データベースが削除されます。
	
	（注） Splunk データベースのデバッグ情報を収集するために使用される `debug` サブメニューは、CLI の `Diagnostic` > `Tracking` サブコマンドから削除されました。

機能	説明
FIPS 認定	Cisco Secure Email Gateway は FIPS 認定され、FIPS 140-2 認定の暗号化モジュール、Cisco Common Crypto Module を統合しました（FIPS 140-2 認定 #4036）。 詳細については、FIPS 管理を参照してください。
電子メールゲートウェイからのログファイルの削除	電子メールゲートウェイの /data/pub/directories パスに保存されているログファイルを削除できるようになりました。 CLI の `logconfig > deletelogfile` サブコマンドを使用してログファイルを削除できます。 （注） 電子メールゲートウェイがスタンドアロンマシンの場合にのみ、ログファイルを削除できます。 詳細については、このリリースに関連する CLI リファレンスガイドの「Example - Deleting Log Files」の項を参照してください。
Hyper-V モデルの第 2 世代展開のサポート	AsyncOS 15.0 リリース以降では、Cisco Secure Email Gateway で Hyper-V モデルの第 2 世代展開がサポートされます。 （注） Hyper-V 第 2 世代展開でサポートされるモデルは、**C600V** のみです。 （注） 現在、第 2 世代の展開の「セキュアブート」および「トラステッドプラットフォームモジュール（TPM）」テクノロジーはサポートされていません。 詳細については、『*Cisco Content Security Virtual Appliance Installation Guide*』を参照してください（https://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html から入手可能）。

機能	説明
Azure の第 2 世代展開のサポート	AsyncOS 15.0 リリース以降では、Cisco Secure Email Gateway で Azure の第 2 世代展開がサポートされます。 （注） Azure 第 2 世代展開でサポートされるモデルは、**C600V** のみです。 （注） 第 2 世代のイメージは、Azure プラットフォームに展開した後に起動しません。第 2 世代のイメージを展開した後、仮想マシンを再起動する必要があります。 詳細については、『*Cisco Secure Email Virtual Gateway and Secure Email and Web Manager Virtual on Azure Deployment Guide*』を参照してください（https://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html から入手可能）。
Microsoft Hyper-V Server 2019 のサポート	Cisco Secure Email Gateway 15.0 は、Microsoft Hyper-V Server 2019 をサポートします。 詳細については、『*Cisco Content Security Virtual Appliance Installation Guide*』を参照してください（https://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html から入手可能）。
AWS 展開でサポートされるモデル	AsyncOS 15.0 リリース以降、AWS 展開でサポートされるモデルは **C600V** のみです。 詳細については、『*Cisco Content Security Virtual Appliances on AWS EC2 Installation Guide*』を参照してください（https://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html から入手可能）。

機能	説明
Cisco Secure Email Gateway 仮想アプライアンスモデルの新しい RAM 値	AsyncOS 15.0 リリース以降では、KVM または VMWare ESXi を介して展開された次の Cisco Secure Email Gateway 仮想アプライアンスモデルに新しい RAM 値があります。 • C100V • C300V • C600V 各仮想アプライアンスモデルに適用可能な新しい RAM 値の詳細については、『*Cisco Content Security Virtual Appliance Installation Guide*』を参照してください（https://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html から入手可能）。

機能	説明
事前定義された DLP ポリシーの新しい分類子	

機能	説明
	次の事前定義された DLP ポリシーの新しい分類子が、Web インターフェイスの [メールポリシー（Mail Policies）] > [DLPポリシーマネージャ（DLP Policy Manager）] > [DLPポリシーの追加（Add DLP Policy）] > [カスタムポリシー（Custom Policy）] > [追加（Add）] > [ポリシー一致の詳細（Policy Matching Details）] ページに追加されます。 • 銀行口座番号（オーストリア IBAN） • 銀行口座番号（ベルギー IBAN） • 銀行口座番号（ブルガリア IBAN） • 銀行口座番号（クロアチア IBAN） • 銀行口座番号（キプロス IBAN） • 銀行口座番号（チェコ共和国 IBAN） • 銀行口座番号（デンマーク IBAN） • 銀行口座番号（エストニア IBAN） • 銀行口座番号（フィンランド IBAN） • 銀行口座番号（ギリシャ IBAN） • 銀行口座番号（ハンガリー IBAN） • 銀行口座番号（アイルランド IBAN） • 銀行口座番号（ラトビア IBAN） • 銀行口座番号（リトアニア IBAN） • 銀行口座番号（ルクセンブルク IBAN） • 銀行口座番号（マルタ IBAN） • 銀行口座番号（ポーランド IBAN） • 銀行口座番号（ポルトガル IBAN） • 銀行口座番号（ルーマニア IBAN） • 銀行口座番号（スロバキア IBAN） • 銀行口座番号（スロベニア IBAN） • 銀行口座番号（スペイン IBAN） • カンボジア国民 ID

機能	説明
	• キプロス国民 ID • フィンランド国民 ID • マルタ国民 ID • ミャンマー国民 ID • ポルトガル国民 ID • ベトナム国民 ID
システムアップグレード中の脆弱なアルゴリズムの削除に関する新しい注記	[FIPS および非 FIPS モードに適用]：AsyncOS 15.0 以降へのシステムアップグレード時、暗号、キー、KEX、および MAC（設定されている場合）のすべての脆弱なアルゴリズムがアップグレードプロセス後にシステムによって削除されることを通知する新しい注意文が追加されました。
SSL 通信の ECDSA 証明書のサポート	楕円曲線デジタル署名アルゴリズム（ECDSA）証明書を使用して、キー交換と ECDSA 認証に楕円曲線 Diffie-Hellman Ephemeral（ECDHE）アルゴリズムを組み合わせ、次の SSL サービスを設定できるようになりました。 • GUI HTTPS • インバウンド SMTP

AsyncOS 14.2.1 の新機能

表 *2 : AsyncOS 14.2.1* の新機能

機能	説明
パスワードで保護された添付ファイルを開くためのユーザー定義のパスフレーズのみを使用	このリリース以降、メールゲートウェイで作成されたユーザー定義のパスフレーズのみを使用して、受信および送信メッセージでパスワードで保護された添付ファイルを開くことを選択できます。 この機能は、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 [セキュリティサービス（Security Services）] > [スキャン動作（Scan Behavior）] > [グローバル設定の編集（Edit Global Settings）] ページで、[ユーザー定義のパスワードのみを適用（Apply User-defined Passwords Only）] チェックボックスを使用します。 • 「ユーザー定義のパスワードのみを適用しますか? y/n」ステートメントは、CLI の `scanconfig` > `protectedattachmentconfig` サブコマンドの下にあります。 詳細については、スキャン動作の設定を参照してください。

AsyncOS 14.2 の新機能

表 *3 : AsyncOS 14.2* の新機能

機能	説明
URL レトロスペクティブ判定と URL 修復	レピュテーションが不明な URL は常に、ユーザのメールボックスに達した後であっても、悪意のあるファイルに変化する可能性があります。Talos から受信した URL レトロスペクティブ判定に基づいてアラートを送信するように、E メールクラウドゲートウェイで URL フィルタリングを設定できます。URL 判定が不明から悪意ありに変更されたときにユーザのメールボックス内のメッセージに対して自動修復アクションを実行するように電子メールゲートウェイを設定することもできます。 詳細については、「悪意のある URL または望ましくない URL からの保護」の章を参照してください。

機能	説明
送信者の成熟度	このリリースでは、従来の送信者ドメインのレピュテーション（SDR）ドメインのエージ機能が、送信者の成熟度に置き換えられます。送信者の成熟度は、送信者のレピュテーションを確立するための重要な機能です。送信者の成熟度は、スパムを分類するために、複数の情報源に基づいて自動的に生成され、「Whois-based domain age」とは異なる場合があります。 [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。 送信者の成熟度は 30 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。 （注） このリリース以降、[SDR ドメインのエージ（SDR Domain Age）] 設定済みフィルタは、[SDR 送信者の成熟度（SDR Sender Maturity）] フィルタに自動的に更新されます。[送信者の成熟度（Sender Maturity）] の値が無効なフィルタは、アップグレード後に「非アクティブ」としてマークされます。メッセージまたはコンテンツフィルタを確認し、適宜変更してください。 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。 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を参照してください。

機能	説明
新しい送信者ドメインのレピュテーション判定	このリリース以降、送信者ドメインのレピュテーションの判定は、所期の意味と推奨される使用法を正確に反映するように更新されています。 アップグレード中に、システムは送信者ドメイン レピュテーション メッセージまたはコンテンツフィルタ設定を自動的に更新して、新しい判定を反映します。メッセージまたはコンテンツフィルタを確認し、適宜設定してください。 新しい SDR 判定ごとに実行できる推奨されるアクションの詳細については、「送信者ドメイン レピュテーション フィルタリング」の「SDR 判定」セクションを参照してください。 AsyncOS 14.2.x リリースにアップグレードすると、コンテンツまたはメッセージフィルタ、レポート、およびメッセージトラッキングの従来の SDR 判定は、次のように新しい SDR 判定に置き換えられます。 • 信頼できない • 要検討 • ニュートラル • 好ましい • 信頼できる • 不明 （注） SDR レポーティングおよびトラッキング AsyncOS API は、新しい SDR 脅威レベルとカテゴリ構造を反映するように更新されています。 （注） SDR メールおよびトラッキングログが更新され、新しい SDR 脅威レベルと送信者の成熟度の詳細が反映されます。 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を参照してください。
送信者ドメインのレピュテーション（SDR）フィルタリングの改善	このリリースでは、SDR サービスのユーザーエクスペリエンスおよび全体的な品質が、パフォーマンスの向上、可用性の向上、および SDR の展開によって強化されています。

機能	説明
ファイル分析レポート用のアプライアンスのグループ化に対する強化	電子メールゲートウェイは、スマートアカウント ID を使用して、組織内のアプライアンスをグループ化し、すべてのアプライアンスのファイル分析結果を表示するようになりました。 電子メールゲートウェイでスマートライセンスが有効になっている場合、ファイル分析レポート用にアプライアンスグループを設定すると、システムによりスマートアカウント ID がアプライアンスグループ ID として自動的に登録されます。アプライアンスグループ ID はいつでも変更でき、変更はコミットアクションなしですぐに有効になります。 詳細については、（パブリック クラウド ファイル分析サービスのみ）アプライアンス グループの設定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	スマート ソフトウェア ライセンシング機能に加えられた拡張機能は次のとおりです。 • **ライセンス予約**：Cisco Smart Software Manager（CSSM）ポータルに接続せずに、E メールゲートウェイで有効になっている機能のライセンスを予約できます。これは主に、インターネットや外部デバイスとの通信がない高度にセキュリティ保護されたネットワーク環境に E メールゲートウェイを展開する対象ユーザーにとって有益です。 詳細については、概要および機能ライセンスの予約を参照してください。 • **Device Led Conversion（DLC）**：E メールゲートウェイをスマートライセンスに登録すると、既存のすべての有効なクラシックライセンスは、Device Led Conversion（DLC）プロセスを使用して自動的にスマートライセンスに変換されます。これらの変換されたライセンスは、CSSM ポータルのバーチャルアカウントで更新されます。 詳細については、概要を参照してください。

機能	説明
接続先コントロールのための TLS 証明書の拡張	特定のドメインの「デフォルト」接続先コントロールエントリで設定された証明書以外の別の証明書を選択できるようになりました。 別の証明書は、次のいずれかの方法で選択できます。 • 対応する接続先コントロールエントリを編集し、Web インターフェイスの [TLS 証明書（TLS certificate）] オプションを使用して別の証明書を選択します。 • 接続先コントロールエントリを作成または編集するときに、CLI で `destconfig > new` または `edit` サブコマンドを使用して証明書を選択します。 詳細については、TLS の管理を参照してください。
クラシックライセンスの変更：Web インターフェイスおよびCLI の期限日	このリリース以降、クラシックライセンスの Web インターフェイスおよび CLI の既存の [期限日（Expiration Date）] 列ヘッダーが [期限日（猶予期間を含む）（Expiration Date (including grace period)）] に変更されます。これは、期限日に猶予期間が含まれることを示しています。 （注） すべてのアラートメッセージとメールログは、機能キーの猶予期間を含む期限日を表示するように変更されます。

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 *4:* 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。

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
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。
[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）]

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
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。
スパム隔離（管理ユーザーおよびエンド ユーザー）	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。

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
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。	-
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。	-

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
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。
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 （25 ページ）
- トレーニング （25 ページ）
- Cisco 通知サービス （26 ページ）
- ナレッジ ベース （26 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 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 （27 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

Cisco Secure Email Cloud Gateway に関して支援を必要とする場合、シスコカスタマーサポートには問い合わせないでください。Cloud/Hybrid Email Security アプライアンスのサポートの詳細については、『Cisco IronPort Hosted Email Security / Hybrid Hosted Email Security Overview Guide』を参照してください。

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 （26 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 （29 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

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。