Cisco Email Security 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 13.5.2 の新機能

表 *1 : AsyncOS 13.5.2* の新機能

機能	説明
Cisco SecureX の統合	Cisco E メール セキュリティ アプライアンスは、Cisco SecureX との統合をサポートするようになりました。Cisco SecureX は、すべてのシスコセキュリティ製品に組み込まれたセキュリティプラットフォームです。E メール セキュリティ アプライアンスと Cisco SecureX を統合させることで、測定可能な分析情報を提供し、目標とする結果とこれまでにないチーム間コラボレーションを実現します。 Cisco SecureX は、セキュリティ インフラストラクチャの可視性を統一し、自動化を実現します。また、インシデント対応ワークフローの加速化と脅威検出の強化を図ります。Cisco SecureX の分散機能は、Cisco SecureX リボンでアプリケーションやツールの形式で利用できます。 詳細については、Cisco SecureX Threat Response との統合を参照してください。 また、アプライアンスの Web インターフェイスで How-To ウィジェットをクリックして、「Integrate Cisco Email Security Gateway with Cisco SecureX or Cisco Threat Response」ウォークスルーにアクセスすることもできます。
SMTP カンバセーション用のカスタム SMTP Helo の設定	CLI の `interfaceconfig > edit` サブコマンドにカスタム SMTP Helo を設定するための新しいオプションが追加されました。 新しい CLI オプションを使用して、SMTP Helo に使用されるデフォルトのインターフェイスホスト名を変更できます。

機能	説明
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アプライアンス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を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
[ファイル分析保留中のメッセージ（Messages with File Analysis Pending）] 機能の拡張	新しいオプション [ファイル分析判定保留中にメッセージ添付ファイルを削除（Drop Message Attachments while File Analysis Verdict Pending）] が [ファイル分析保留中のメッセージ（Messages with File Analysis Pending）] セクション（[メールポリシー（Mail Policies）]>[受信メールポリシー（Incoming Mail Policies）] で、変更するメールポリシーの [高度なマルウェア防御（Advanced Malware Protection）] 列のリンクをクリック）に追加されました。 アプライアンスからの最終メッセージを配信している間にファイル分析の判定が保留された場合、添付ファイルをドロップするかどうかを選択できるようになりました。デフォルトのオプションは [いいえ（No）] です。 このオプションを [はい（Yes）] に設定した場合、[メッセージトラッキング（Message Tracking）]（[モニタ（Monitor）]>[メッセージトラッキング（Message Tracking）]）の [処理詳細（Processing Details）] セクションに、ファイル分析の判定が保留中のときに削除されたメッセージの添付ファイルに関する詳細が表示されます。 また、メールログには、設定された AMP ポリシーに基づいてファイル分析の判定が保留されている場合に削除されたメッセージの添付ファイルのログの詳細も表示されます。 このオプションは、CLI で `policyconfig` コマンドを使用して有効にすることもできます。 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
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。 設定されたクエリタイムアウト中に、アプライアンスはファイル レピュテーション クエリを AMP サーバに送信します。アプライアンスは 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、アプライアンスが応答を受信できます。
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	アプライアンスにログインすると、[メールフロー概要（Mail Flow Summary）] ページが表示されます。	アプライアンスにログインすると、[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、アプライアンスのレポートを表示できます。	[モニタ（Monitor）] メニューで、アプライアンス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）]	アプライアンスの [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。	アプライアンスでは、[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。	アプライアンスの欠落データ 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、アプライアンス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	アプライアンスでは、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、アプライアンスの [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、アプライアンス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、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。

- サード パーティ コントリビュータ, on page 12
- マニュアルに関するフィードバック, on page 12
- シスコ アカウントの登録 , on page 12

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 E メール セキュリティ アプライアンス 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 E* メール セキュリティ アプライアンス 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	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 , on page 12を参照してください。

ナレッジ ベース

Procedure

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。

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 , on page 11
- ナレッジ ベース, on page 11

Cisco E メール セキュリティ アプライアンス 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、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、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、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, on page 14

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