Cisco クラウド E メール セキュリティをご使用の前に

この章は、次の項で構成されています。

- AsyncOS 13.5.1 の新機能 （1 ページ）
- 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 （6 ページ）
- 詳細情報の入手先 （10 ページ）
- Cisco Email Security Appliances の概要 （14 ページ）

AsyncOS 13.5.1 の新機能

表 *1 : AsyncOS 13.5.1* の新機能

機能	説明
メールボックス内のメッセージの検索と修復	アプライアンスを設定し、検索および修復機能を使用して、手動でメッセージを修復できるようになりました。この機能により、メッセージ トラッキング フィルタを使用してメッセージを検索し、メッセージに修復アクションを適用できるようになります。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
Cisco Success Network を使用した Cisco E メール セキュリティ ゲートウェイのユーザエクスペリエンスの向上	Cisco Success Network（CSN）機能を使用して、アプライアンスや機能の使用状況の詳細をシスコに送信できます。これらの詳細情報は、アプライアンスのバージョン、およびアプライアンスでアクティブになっているが有効になっていない機能を識別するために使用されます。 アプライアンスや機能の使用状況の詳細をシスコに送信する機能により、組織は次のことを行うことができます。 • 収集されたテレメトリデータの分析を実行し、デジタルキャンペーンを使用してユーザに推奨事項を提示することによって、ユーザネットワークでの製品の有効性を向上させます。 • Cisco E メール セキュリティ ゲートウェイの使用により、ユーザエクスペリエンスが向上します。 詳細については、Cisco Threat Response との統合を参照してください。

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、シスコ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やフィッシング、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、次の URL にある Cisco Talos 電子メールステータスポータルのヘルプページを参照してください。 https://talosintelligence.com/tickets/email_submissions/help 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。
アプライアンスの新しい Web インターフェイスを暗色モードで利用	暗色モードは反転カラースキームであり、暗い色の背景上で明るい色のタイポグラフィ、UI 要素、アイコンが使用されます。 アプライアンスの新しい Web インターフェイスを暗色モードで利用できるようになりました。 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。

機能	説明
プロキシサーバを使用して Cisco Threat Response にアプライアンスを接続する機能	プロキシサーバを使用してアプライアンスを Cisco Threat Response に接続できるようになりました。 次のいずれかの方法でプロキシサーバを設定できます。 • Web インターフェイスの [セキュリティサービス（Security Services）] > [サービスアップデート（Service Updates）] ページ。 • CLI の `updateconfig` > `setup` サブコマンド。 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
Cisco E メール セキュリティ ゲートウェイと Cisco Advanced Phishing Protection クラウドサービスの統合	Cisco E メール セキュリティ ゲートウェイ上の Cisco Advanced Phishing Protection エンジンは、組織に送信された過去の電子メールトラフィックに基づいて、正当なすべての送信者の固有の動作を確認します。Cisco Advanced Phishing Protection のクラウドサービス インターフェイスは、悪意のある可能性があるメッセージを正常なメッセージと区別するためにリスク分析を実行します。 Cisco Advanced Phishing Protection クラウドサービスは、電子メールゲートウェイを組織への着信メッセージのメタデータのコピーを受信するためのセンサーエンジンとして使用します。このセンサーエンジンが、電子メールゲートウェイからのメッセージヘッダーなどのメタデータを収集し、それらを分析するために Cisco Advanced Phishing Protection クラウドサービスへ中継します。分析後に、悪意のある可能性があるメッセージは、Cisco Advanced Phishing Protection クラウドサービス上の事前に設定されたポリシーに基づいて、受信者のメールボックスから自動的に修復されます。 Cisco E メール セキュリティ ゲートウェイをセンサーエンジンとして使用できると、組織が次のことを行うときに役立ちます。 • 受信者のメールボックスからのメッセージヘッダーで確認された脅威を特定し、調査し、修復する。 • 組織内の複数の電子メールゲートウェイからメッセージのメタデータのレポートデータを表示する。 • 悪意のあるメッセージに関して、エンドユーザにリアルタイムのアラートを送信する。 詳細については、Cisco E メール セキュリティ ゲートウェイと Cisco Advanced Phishing Protection の統合を参照してください。
サービスログを使用したフィッシング検知有効性の向上	サービスログは、フィッシング検出を改善するために Cisco Talos クラウドサービスに送信されます。 詳細については、サービスログを使用したフィッシング検知機能の有効性の向上を参照してください。

機能	説明
フィッシングに対する有効性の向上	Cisco E メールセキュリティ アプライアンスでは、フィッシングの検出をより迅速かつ効果的に行うため、IP レピュテーションおよび URL レピュテーションサービスが改善されています。
（注） HTTP プロキシサーバを設定している場合、IP レピュテーション/URL レピュテーションサービス、およびサービスログは、インターネットに直接接続して IP と URL のレピュテーションを取得します。これらのサービスにプロキシを使用する場合は、電子メールゲートウェイで HTTPS プロキシサーバを設定します。 （注） HTTPS プロキシサーバを設定している場合は、E メールゲートウェイから発信される HTTPS トラフィックを復号するようにプロキシサーバを設定しないでください。	

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。

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
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（Montior）] 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。	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。
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。	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。	-
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。

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	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。

- 資料 （10 ページ）
- トレーニング （11 ページ）
- Cisco 通知サービス （12 ページ）
- ナレッジ ベース （12 ページ）
- シスコ サポート コミュニティ （12 ページ）
- シスコ カスタマー サポート （12 ページ）
- サードパーティ コントリビュータ （13 ページ）
- マニュアルに関するフィードバック （13 ページ）
- シスコ アカウントの登録 （13 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、シスコ アカウントの登録 （13 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

クラウド E メール セキュリティ アプライアンス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、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、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 （12 ページ）
- ナレッジ ベース （12 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 （15 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