



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 14.0.2 の新機能](#) (2 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](#) (3 ページ)
- [詳細情報の入手先](#) (7 ページ)
- [Cisco Secure Email Gateway の概要](#) (11 ページ)

AsyncOS 14.0.2 の新機能

表 1: AsyncOS 14.0.2 の新機能

機能	説明
<p>Syslog プッシュ ログ サブスクリプションのキャッシング</p>	<p>Syslog プッシュ ログ サブスクリプションのローカルディスクバッファを設定できるようになりました。これにより、リモート Syslog サーバーが使用できないときに、セキュアな電子メールゲートウェイがログイベントをキャッシュできます。Syslog サーバーが使用可能になると、電子メールゲートウェイは、そのログサブスクリプションのバッファ内のすべてのデータを Syslog サーバーに送信し始めます。</p> <p>ディスクバッファパラメータは、次の方法で設定できます。</p> <ul style="list-style-type: none"> • 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)] ページ詳細については、ログ取得方法を参照してください。 • CLI での <code>logconfig</code> コマンド。詳細については、CLI リファレンスガイドの「The Commands : Reference Example」の章の「Logging and Alerts」セクションを参照してください。

機能	説明
プレフィックス付きまたはプレフィックスなしのスマート識別子の検出	<p>電子メールゲートウェイは、メッセージコンテンツのプレフィックスとして追加されたキーワード(「credit」、「ssn」、「cusip」、または「aba」)の有無にかかわらず、スマート識別子を検出します。</p> <p>プレフィックスとして追加されたキーワードの有無にかかわらず、スマート識別子を検出するように、コンテンツフィルタ条件またはメッセージフィルタルールを次の方法で設定できます。</p> <ul style="list-style-type: none"> メッセージ本文、メッセージ本文または添付ファイル、および添付ファイルのコンテンツについて、コンテンツフィルタ条件で、[スマート識別子のプレフィックスを含む (Contains smart identifier prefix)] オプションを使用する。詳細については、コンテンツフィルタの条件を参照してください。 メッセージフィルタルールで、プレフィックス構文を使用する。詳細については、スマート ID の構文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。

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
[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。 <ul style="list-style-type: none"> • [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。 <ul style="list-style-type: none"> • [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。 <code>https://example.com:<https-api-port>/eui-login</code> 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 レピュテーションスコア、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 \(8 ページ\)](#)
- [トレーニング \(8 ページ\)](#)
- [Cisco 通知サービス \(9 ページ\)](#)
- [ナレッジベース \(9 ページ\)](#)

- シスコサポートコミュニティ (9 ページ)
- シスコカスタマーサポート (10 ページ)
- サードパーティ コントリビュータ (10 ページ)
- マニュアルに関するフィードバック (10 ページ)
- シスコアカウントの登録 (10 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.html
Cisco IronPort 暗号化	https://www.cisco.com/c/ja_jp/support/security/email-security-appliance/products/command-reference.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 \(10 ページ\)](#) 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、ユーザー 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 \(9 ページ\)](#)

- [ナレッジベース \(9 ページ\)](#)

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査**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になります。
- **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 \(12 ページ\)](#)

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。