AsyncOS 14.0.1 for Cisco Secure Email Gateway リリースノート

発行日:2021 年 3 月 22 日
改訂日:2021 年 10 月 28 日

目次

Cisco Systems, Inc.
www.cisco.com

今回のリリースでの変更点

AsyncOS 14.0.1 の新機能

機能	説明
URL フィルタリングの詳細設定	電子メールゲートウェイの Web インターフェイスで、次の高度な URL フィルタリングパラメータを設定できるようになりました。 • URL ルックアップタイムアウト値(URL Lookup Timeout value) • メッセージ本文の URL の最大数(Maximum number of URLs in the message body) • メッセージ添付ファイルの URL の最大数(Maximum number of URLs in message attachments) • メッセージ内の URL テキストと HREF の書き換え(Rewrite URL text and HREF in the message) • メールログおよびメッセージトラッキングの URL の詳細(URL details in Mail Logs and Message Tracking) 詳細については、このリリースに関連するユーザーガイドの「Protecting Against Malicious or Undesirable URLs」の章の「Enable URL Filtering」のセクションを参照してください。
Cisco Cloud Services ポータルへの電子メールゲートウェイの登録	次のいずれかのシナリオに基づいて、電子メールゲートウェイを Cisco Cloud Services ポータルに再登録できます。 • 電子メールゲートウェイを Cisco Cloud Services ポータルに自動的に登録するときに、Cisco Cloud Services ポータルに追加されたデバイスを表示または管理できない場合。 • 電子メールゲートウェイを Cisco Cloud Services ポータルに自動的に登録するときに、スマートアカウントと Cisco Cloud Services アカウントがリンクされていない場合。 次のいずれかの方法を使用して、Cisco Cloud Services ポータルに電子メールゲートウェイを再登録できます。 • Web インターフェイスの [ネットワーク(Network)] > [クラウドサービス設定(Cloud Service Settings)] ページ。 • CLI の `cloudserviceconfig` > `reregister` サブコマンド。 詳細については、以下を参照してください。 • このリリースに関連するユーザーガイドの「Integrating with Cisco SecureX Threat Response」の章の「Reregistering Email Gateway with Cisco Cloud Services Portal」セクション。 • このリリースに関連する CLI リファレンスガイドの「The Commands: Reference Examples」章の「Configuring Cisco Cloud Service Portal Settings and Usage」セクション。

Syslog プッシュの新しいパラメータ - ログ取得方式	電子メールゲートウェイで Syslog プッシュログの取得方法を設定するために使用する必要がある新しいパラメータは次のとおりです。 • リモート Syslog サーバーのポート番号。 • リモート Syslog サーバーに送信されるログメッセージの最大サイズ(バイト単位)。 • (TCPプロトコルの場合のみ):電子メールゲートウェイとリモート Syslog サーバー間の TLS 接続。 次のいずれかの方法を使用して、Syslog プッシュログ取得方式の新しいパラメータを設定できます。 • 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 • CLI での `logconfig` コマンド。 詳細については、以下を参照してください。 • このリリースに関連するユーザーガイドの「Logging」の章の「Log Retrieval Methods」セクション。 • このリリースに関連する CLI リファレンスガイドの「The Commands: Reference Examples」の章の「Logging and Alerts」セクション。
TLS を使用した SMTP コールアヘッド受信者検証の実行	TLS を使用して SMTP コールアヘッド受信者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るようになりました。 SMTP コールアヘッド受信者検証では、電子メールゲートウェイの [SSL 設定(SSL Configuration)] ページの [その他の TLS クライアントサービス(Other TLS Client Services)] オプションで選択したものと同じ TLS バージョンを使用します。 SMTP コールアヘッド受信者検証の TLS サポートをイネーブルにするには、次のいずれかの方法を使用します。 • Web インターフェイスの [ネットワーク(Network)] > [SMTP コールアヘッド(SMTP Call-Ahead)] ページ • CLI での `callaheadconfig` コマンド 詳細については、以下を参照してください。 • このリリースに関連するユーザーガイドの「Validating Recipients Using an SMTP Server」の章の「SMTP Call-Ahead Server Profile Settings」セクション。 • このリリースに関連する CLI リファレンスガイドの「The Commands: Reference Examples」の章の「SMTP Services Configuration」セクション。

電子メールゲートウェイのコンテンツディクショナリの最大数の設定	電子メールゲートウェイで最大 150 のコンテンツディクショナリを設定できるようになりました。 **(注)** デフォルトでは、電子メールゲートウェイに最大 100 のコンテンツディクショナリを設定できます。 デフォルトの制限を変更するには、CLI で `dictionaryconfig > dictionarylimits` サブコマンドを使用します。 **(注)** [メッセージ本文または添付ファイル(Message Body or Attachments)] コンテンツフィルタ条件または [本文のスキャン(Body Scanning)] または [添付ファイルのスキャン(Attachment Scanning)] メッセージフィルタルールでコンテンツディクショナリを広範囲に使用すると、システムパフォーマンスが低下する場合があります。 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「The Commands: Reference Examples」の章の「Policy Enforcement」セクションを参照してください。
Secure Email Gateway での ESXi 7.0 認定	Cisco Secure Email 仮想ゲートウェイを VMware vSphere Hypervisor (ESXi)7.0 に展開できるようになりました。 詳細については、『Cisco Content Security Virtual Appliance Installation Guide』を参照してください。このドキュメントは、https://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html から入手できます。
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、以下を参照してください。 • このリリースに関連するユーザーガイドの「Configuring Email Gateway to Consume External Threat Feeds」の章の「How to Configure Email Gateway to Consume External Threat Feeds」および「Configuring SecureX Threat Response Feeds Source」のセクション。 • このリリースに関連する CLI リファレンスガイドの「The Commands: Reference Examples」の章の「Configuring Email Gateway to Consume External Threat Feeds」のセクション。

AsyncOS 14.0 の新機能

機能	説明
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	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 またはメッセージ内の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と Cisco Secure Awareness クラウドサービスを統合することで、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エンドユーザの認識が向上します。 • 電子メール管理者は、リピートクリッカーと識別されたエンド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、ユーザガイドまたはオンラインヘルプの「Integrating Cisco Email Gateway with Cisco Secure Awareness Cloud Service」の章を参照してください。
Simple Network Management Protocol (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、ユーザガイドまたはオンラインヘルプの「Managing and Monitoring Using the CLI」の章を参照してください。

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 会話レベルで送信者ドメインレピュテーション(SDR)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。 **(注)** デフォルトでは、SDR 判定が「Awful」の場合、電子メールゲートウェイはすべての着信メッセージをブロックします。 **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、ユーザガイドまたはオンラインヘルプの「Sender Domain Reputation Filtering」と「Defining Which Hosts Are Allowed to Connect Using the Host Access Table」の章を参照してください。

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	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 ? 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、ユーザガイドの「Using Message Filters to Enforce Email Policies」の章と『*CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway*』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、ユーザガイドまたはオンラインヘルプの「Using Email Security Monitor」の章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、ユーザガイドまたはオンラインヘルプの「Using Email Security Monitor」の章を参照してください。

[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	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)] に変更されました。 詳細については、ユーザガイドまたはオンラインヘルプの「Using Email Security Monitor」の章を参照してください。

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。
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、ユーザガイドまたはオンラインヘルプの「Remediating Messages in Mailboxes」の章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、ユーザガイドまたはオンラインヘルプの「Integrating with Cisco SecureX Threat Response」の章を参照してください。

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、ユーザガイドまたはオンラインヘルプの「File Reputation Filtering and File Analysis」の章の「Enabling and Configuring File Reputation and Analysis Services」の項を参照してください。
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、ユーザガイドまたはオンラインヘルプの「Content Filters」の章の「Content Filter Conditions」と「Content Filter Actions」の項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 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。 • 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。 詳細については、以下を参照してください。 • ユーザガイドまたはオンラインヘルプの「System Administration」の章の「Smart Licensing in Cluster Mode」と「Registering the Email Gatewaywith Cisco Smart Software Manager」の項。 • 『*CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway*』の「Smart Software Licensing」と「Configuring Cisco Cloud Service Portal Settings and Usage」の項。

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、『*CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway*』の「Example：Sending Alerts over TLS」の項を参照してください。
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。 このリリースでは、電子メールゲートウェイで IDN ドメインを使用して設定できる機能はほとんどありません。詳細については、電子メールゲートウェイで IDN ドメインを使用して設定可能な機能（32 ページ）を参照してください。

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。
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。
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。

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 ? 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、ユーザガイドまたはオンラインヘルプの「スパムおよびグレイメールの管理(Managing Spam and Graymail)」の章を参照してください。
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。
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、ユーザガイドまたはオンラインヘルプの「Remediating Messages in Mailboxes」の章を参照してください。

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
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。
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、ユーザガイドの「S/MIME Security Services」と「Encrypting Communication with Other MTAs」の章を参照してください。

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、ユーザ ガイドの「System Administration」の章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、ユーザ ガイドの「System Administration」の章を参照してください。

<table>
<tr><td>統合イベントログの機能拡張</td><td>[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:

a. 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。
b. メッセージフィルタルールを次のように設定します。

<code>Custom_ Log_Entry: if (true) {
log-entry("$filesizes");</code>

または

カスタマイズされたテキストを「<code>$ filesizes</code>」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。</td></tr>
<tr><td>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</td><td>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、以下を参照してください。
このリリースに関連するユーザーガイドの「Configuring Email Gateway to Consume External Threat Feeds」の章の「How to Configure Email Gateway to Consume External Threat Feeds」および「Configuring SecureX Threat Response Feeds Source」のセクション。
このリリースに関連する CLI リファレンスガイドの「The Commands: Reference Examples」の章の「Configuring Email Gateway to Consume External Threat Feeds」のセクション。</td></tr>
<tr><td>ブランド変更後の製品と関連資料</td><td>製品と関連資料のブランドを次のように変更しました。

★セグメント分割★
<table><tr><th>以前の用語</th><th>ブランド変更後の用語</th></tr><tr><td>Cisco E メール セキュリティ アプライアンス</td><td>Cisco Secure Email ゲートウェイ</td></tr><tr><td>Cisco クラウド E メール セキュリティ アプライアンス</td><td>Cisco Secure Email クラウドゲートウェイ</td></tr><tr><td>Cisco コンテンツセキュリティ管理アプライアンス</td><td>Cisco Secure Email and Web Manager</td></tr></table></td></tr>
</table>

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すべてのバイアス用語を削除しました。 次の表に、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。

バイアス用語	バイアスフリー用語
ホワイトリスト	許可リスト
ブラックリスト	ブロックリスト
マスター	プライマリ
スレーブ	セカンダリ
ブラックホール	シンクホール

動作における変更

AsyncOS 14.0.1 の動作の変更

ファイル分析のためのアプライアンスグループ化の変更	このリリースより前は、電子メールゲートウェイでアプライアンスグループを設定した場合、グループを変更できませんでした。 このリリースにアップグレードした後は、CLI で `ampconfig > setup` サブコマンドを使用してアプライアンスグループを変更できるようになりました。
メールフローポリシーの送信者ドメインのレピュテーション(SDR)の検証の変更	アップグレードの前に、電子メールゲートウェイでパブリックリスナーのリレー接続動作と [送信者ドメインのレピュテーションの検証(Sender Domain Reputation Verification)] オプションがデフォルトでオンになっているメールフローポリシーを設定した場合。アップグレード時に、メールフローポリシーで [送信者ドメインのレピュテーションの検証(Sender Domain Reputation Verification)] オプションが自動的にオフになります。 電子メールゲートウェイの Web インターフェイスで、メールフローポリシーの [送信者ドメインのレピュテーションの検証(Sender Domain Reputation Verification)] オプションを手動で有効にする必要があります。

URL フィルタ処理の変更	このリリースより前は、CLI で `websecurityadvancedconfig` コマンドを使用して、マシンレベルでのみ高度な URL フィルタ処理設定を行うことができました。 このリリースにアップグレードした後は、CLI で `websecurityadvancedconfig` コマンドを使用して、マシンレベルとクラスタレベルで高度な URL フィルタ処理設定を構成できるようになりました。 **(注)** クラスタ内のマシンごとに異なる高度な URL フィルタ処理設定を行ったとします。アップグレード時に、システムはクラスタレベルですべてのマシンのそれぞれの高度な URL フィルタ処理設定の最大値を設定します。
URL ロギングの変更	このリリースより前は、CLI で `outbreakconfig` コマンドを使用して、電子メールゲートウェイで URL 関連情報のロギングのみを有効にすることができました。 このリリースにアップグレードした後は、次のいずれかの方法で電子メールゲートウェイの URL 関連情報のロギングのみを有効にできます。 • CLI での `websecurityadvancedconfig` コマンド • Web インターフェイスの [セキュリティサービス(Security Services)] > [URL フィルタリング(URL Filtering)] ページ。 詳細については、次の資料を参照してください。 • このリリースに関連するユーザーガイドの「Protecting Against Malicious or Undesirable URLs」の章の「Enable URL Filtering」セクション。 • このリリースに関連する CLI リファレンスガイドの「The Commands: Reference Examples」の章の「URL Filtering」セクション。
電子メールゲートウェイでのメール処理の変更	このリリースより前では、[RFC 違反によるスキャン不可メッセージに対するアクション(Action for unscannable messages due to RFC Violations)] オプションを有効にした場合、電子メールゲートウェイは、[送信元(From:)] ヘッダーフィールドを含まないメッセージまたは、RFC 違反のため「スキャン不可」として複数の [送信元(From:)] ヘッダーフィールドを含むメッセージをマークしませんでした。 このリリースにアップグレードした後は、[RFC 違反によるスキャン不可メッセージに対するアクション(Action for unscannable messages due to RFC Violations)] オプションを有効にした場合、電子メールゲートウェイは、[送信元(From:)] ヘッダーフィールドを含まないメッセージまたは、RFC 違反のため「スキャン不可」として複数の [送信元(From:)] ヘッダーフィールドを含むメッセージをマークするようになりました。

[その他の TLS クライアントサービス(Other TLS Client Services)] オプションの新しいヘルプテキスト	電子メールゲートウェイの次の Web ページの [その他の TLS クライアントサービス(Other TLS Client Services)] オプションに新しいヘルプテキストが追加されました。 • [システム管理(System Administration)] > [SSL 設定(SSL Configuration)] ページ • [システム管理(System Administration)] > [SSL 設定(SSL Configuration)] > [SSL 設定の編集(Edit SSL Configuration)] ページ ヘルプテキストメッセージには、[その他の TLS クライアントサービス(Other TLS Client Services)] オプションで選択した TLS 方式に使用されるサービスのリストの詳細が表示されます。
証明書の失効アラートの変更	このリリースより前は、デバイス証明書とカスタム CA 証明書の有効期限が近づいており、[ネットワーク(Network)] > [証明書(Certificate)] > [設定の編集(Edit Settings)] ページで [カスタムリスト(Custom List)] オプションが無効になっている場合、電子メールゲートウェイはシステムアラートを送信していました。 このリリースにアップグレードした後は、電子メールゲートウェイは次の場合にシステムアラートを送信します。 • カスタム CA 証明書の有効期限が近づいており、[カスタムリスト(Custom List)] オプションが [ネットワーク(Network)] > [証明書(Certificate)] > [設定の編集(Edit Settings)] ページで有効になっている。 • デバイス証明書の有効期限が近づいている。 カスタム CA 証明書の有効期限が近づいたときに生成されるシステムアラートの例を次に示します。 `Your certificate "Cisco" expires in 3 days, 4:45:20 hour(s). Use the certconfig -> certauthority -> custom -> delete. sub command in the CLI to delete any unused custom CA certificates in the CA list.`
LDAP プロファイルの SSL 暗号の変更	このリリースより前は、LDAP プロファイルに [SSL を使用(Use SSL)] オプションを選択し、非 FIPS モードから FIPS モードに切り替えた場合、非 FIPS モードで使用可能な同じ SSL 暗号が FIPS モードで LDAP プロファイルに表示されていました。 このリリースにアップグレードした後は、LDAP プロファイルで [SSL を使用(Use SSL)] オプションを選択し、非 FIPS モードから FIPS モードに切り替えると、SSL 暗号は LDAP プロファイルで「FIPS」として表示されます。また、LDAP プロファイルに対して [SSL を使用(Use SSL)] オプションがすでに選択されている非 FIPS モードに切り替えると、次のデフォルトの SSL 暗号が LDAP プロファイルに表示されます。 `ECDHE-RSA:ECDHE-ECDSA:DHE-DSS-AES:AES128:AES256:!DHE-RSA-AE256-SHA:!ECDHE-ECDSA-AES256-SHA:!DHE-DSS-AES256-SHA:!DH-RSA-AES128-SHA:!DH-DSS-AES128-SHA:!DH-RSA-AES256-SHA256:!DH-DSS-AES256-SHA256:!DH-RSA-AES256-SHA:!DH-DSS-AES256-SHA:!aNULL`

LDAP プロファイルでサポートされていない SSL 暗号の変更	このリリースより前では、[SSL を使用(Use SSL)] オプションをすでに選択した場合は、LDAP プロファイルにサポートされていない SSL 暗号を設定していました。Secure Email バージョン 14.0.1 にアップグレードすると、サポートされていない SSL 暗号は、次のデフォルトの SSL 暗号で置き換えられます。 `ECDHE-RSA:ECDHE-ECDSA:DHE-DSS-AES:AES128:AES256:!DHE-RSA-AES256-SHA:!ECDHE-ECDSA-AES256-SHA:!DHE-DSS-AES256-SHA:!DH-RSA-AES128-SHA:!DH-DSS-AES128-SHA:!DH-RSA-AES256-SHA256:!DH-DSS-AES256-SHA256:!DH-RSA-AES256-SHA:!DH-DSS-AES256-SHA:!aNULL.`
システム正常性 API の変更	このリリースより前のリリースでは(AsyncOS 13.5.x および 13.7 リリースバージョンのみに適用)、システム正常性 API のサンプル応答に、配信ステータス API とシステムステータス API の詳細が含まれていました。 このリリース以降、配信ステータス API とシステムステータス API の詳細は、システム正常性 API の応答から削除されます。これらの詳細は、配信ステータス API とシステムステータス API の対応する応答で表示できるようになりました。

AsyncOS 14.0 の動作の変更

Cisco Secure Email Gateway での URL レピュテーション判定名の変更	Cisco Talos では、既存の URL レピュテーション判定に新しいカテゴリと新しい名前が導入されています。現在、Cisco Secure Email Gateway の設定やレポートに関する変更はありません。 電子メールゲートウェイの既存の URL レピュテーション判定の新しいカテゴリと新しい名前を表示するには、既存の URL レピュテーション判定の新しいカテゴリと新しい名前(34 ページ)の次の表を参照してください。 詳細については、Cisco Talos のブログ(https://blog.talosintelligence.com/2019/09/new-cisco-talos-web-reputation-verdicts.html)を参照してください。
スパム対策設定の変更	CASE 機械学習システムで使用されるメタデータ分析とその他の言語に依存しない機能により、電子メールゲートウェイのスパム対策設定における中国語の地域とグローバルのスキャンプロファイル間の有効性の違いが最小限に抑えられました。 中国の地域スキャンプロファイルの代わりにグローバルスキャンプロファイルを使用して脅威を迅速に検出できるようになりました。これにより、中国、台湾、および香港に拠点を置く組織の効率が向上します。
`threatresponseconfig` CLI コマンドと `csnconfig` CLI コマンドのサポートなし	AsyncOS 14.0 リリース以降、`threatresponseconfig` CLI コマンドと `csnconfig` CLI コマンドはサポートされなくなりました。 `cloudserviceconfig` CLI コマンドを使用して `threatresponseconfig` CLI コマンドと `csnconfig` CLI コマンドの機能を設定できるようになりました。 詳細については、『CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway』の「Configuring Cisco Cloud Service Portal Settings and Usage」のセクションを参照してください。

電子メールゲートウェイと Cisco SecureX Threat Response の変更の統合	このリリース以前で統合を完了するには、電子メールゲートウェイを有効にし、Cisco SecureX Threat Response に登録する必要がありました。 このリリースにアップグレード後は、電子メールゲートウェイを有効にして Cisco Cloud Services ポータルに登録し、電子メールゲートウェイでCisco SecureX Threat Response を有効にして統合を完了する必要があります。 **(注)** 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。この統合を完了するのに必要なのは、電子メールゲートウェイで Cisco SecureX Threat Response を手動で有効にすることだけです。 詳細については、ユーザガイドの「Integrating with Cisco SecureX Threat Response」の章を参照してください。
ロギングの詳細の変更	このリリース以降は、「パスフレーズ」、「登録トークン」などのすべての機密データが電子メールゲートウェイによって生成される CLI やメールのログに表示されなくなりました。 **(注)** デフォルトでは、すべての機密データが汎用のカスタマイズされたメッセージに置き換えられます。
[Secure Email Gateway Swagger] ページに AsyncOS バージョンの詳細がなし	このリリース以降、[Secure Email Gateway API Swagger] ページに AsyncOS のバージョンの詳細は表示されなくなります。
AMP エンジンログの変更	このリリース以降、SHA-256 値は AMP エンジンログにテキスト形式で表示されます。
FIPS モードまたは FIPS 以外のモードでの電子メールゲートウェイの機密データの暗号化	FIPS モードか FIPS 以外のモードかに関係なく、電子メールゲートウェイ内の機密データを暗号化するために、新しい CLI サブコマンドの `encryptconfig` が `fipsconfig` CLI コマンドの下に追加されました。
電子メールゲートウェイ証明書の変更(FIPS モードのみ)	このリリース以降、中間証明書の有効期限が切れたり、CRL 検証に失敗した場合は、電子メールゲートウェイ証明書をインポート、編集、または貼り付けることができなくなります。
Cisco Talos の電子メールステータスポータルへの電子メールゲートウェイ登録の変更	電子メールゲートウェイを新しいポータルに登録する前に、Cisco Talos の新しい電子メールステータスポータルからの登録 ID の取得が必要になりました。 詳細については、ユーザガイドまたはオンラインヘルプの「スパムおよびグレイメールの管理(Managing Spam and Graymail)」の章を参照してください。
ファイル レピュテーション クエリのタイムアウトの変更	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 プロセス中の合計タイムアウト期間に 2 秒の追加バッファー時間を追加するようになりました。

メッセージトラッキング: [詳細の表示(Show Details)] ページの変更	このリリース以降、単一の MID のメッセージ処理に関する詳細の最大20,000件 のレコードを [メッセージトラッキング(Message Tracking)] > [検索(Search)] > [詳細の表示(Show Details)] ページに表示できます。
ホストヘッダー設定の変更	このリリース以前では、設定されたベースホスト名のみを使用して、電子メールゲートウェイが HTTP 要求に応答できるようにすることができました。 このリリースにアップグレードした後、`adminaccessconfig` CLI コマンドで `hostheader` オプションを有効にすると、次を使用して HTTP 要求に応答するように電子メールゲートウェイを設定できます。 • 設定されたベースホスト名。 • (任意)許可ホストリストに追加されたホスト。
DLP ポリシー一致の [送信者および受信者のフィルタリング(Filtering by Sender and Recipients)] フィールドの変更	このリリース以降、電子メールゲートウェイで DLP ポリシーを設定する場合、[送信者および受信者のフィルタリング(Filtering by Sender and Recipients)] フィールドのユーザ(送信者または受信者)のエントリは、大文字と小文字が区別されなくなります。 たとえば、ユーザの受信者に Joe@ と入力すると、設定された DLP ポリシーに基づいて、joe@example.com に送信されるメッセージが一致します。
システムヘルスチェックの変更	このリリースより前は、アップグレードプロセス中にシステムヘルスチェックが自動的に行われていました。 このリリースにアップグレード後は、次のいずれかの方法でシステムヘルスチェックを手動で実行できます。 • Web インターフェイスで、[システム管理(System Administration)] > [システムの状態(System Health)] > [ヘルスチェックを実行(Run Health Check)] オプションに移動します。ユーザ ガイドの「System Administration」の章を参照してください。 • CLI で `healthcheck` コマンドを使用します。『CLI Reference Guide for AsyncOS for Cisco Email Security Appliances』*を参照してください。*
復号化エラー中の免責事項の変更	メッセージのフッターまたはヘッダーに追加された免責事項が復号化エラーを生成した場合、免責事項またはメッセージ本文は個別のメッセージ添付ファイルに分割されます。

SSH サーバの設定変更	次の SSH サーバの設定変更は、Cisco Secure Email Gateway 用の AsyncOS 14.0 を初めてインストールする場合にのみ適用されます。 電子メールゲートウェイでは、次の暗号アルゴリズムと MAC 方式がデフォルトで無効になっています。 • **暗号アルゴリズム**：`3des-cbc` • **MAC 方式**: – mac-md5 – umac-64@openssh.com – hmac-ripemd160 – hmac-ripemd160@openssh.com – hmac-sha1-96 – hmac-md5-96 上記の暗号アルゴリズムと MAC方式を有効にするには、CLI で `sshconfig` > `SSHD` > `setup` サブコマンドを使用します。 (**FIPS モードのみ**)電子メールゲートウェイで FIPS モードを有効にする前に、FIPS モードでサポートされていない次の暗号アルゴリズムを必ず削除してください。 • aes192-ctr • `rijndael-cbc@lysator.liu.se` 電子メールゲートウェイで上記の暗号アルゴリズムを削除するには、CLI で `sshconfig` > `SSHD` > `setup` サブコマンドを使用します。
ファイル レピュテーション サービスの設定変更	電子メールゲートウェイでファイル レピュテーション サービスを設定する場合、SSL 通信を有効または無効にするオプションはありません。電子メールゲートウェイは、デフォルトで SSL プロトコルを使用し、ファイアウォールポート 443 のみを使用してファイル レピュテーション サービスと通信します。 電子メールゲートウェイでファイル レピュテーション サービスの SSL 通信設定を設定する次のオプションは削除されました。 • 電子メールゲートウェイの Web インターフェイスの [セキュリティサービス(Security Services)] > [ファイルレピュテーションと分析(File Reputation and Analysis)] ページの [SSL(ポート 443)を使用する(Use SSL (Port 443))] チェックボックス。 • 「ファイルレピュテーション用の `SSL` 通信(ポート `443`)を有効にしますか？`[Y]`>(`Do you want to enable SSL communication (port 443) for file reputation? [Y]>`)」というステートメント(CLI の `ampconfig` > `advanced` サブコマンド)。
外部脅威フィード:ファイルハッシュ設定の変更	電子メールゲートウェイで、外部脅威フィード(ETF)エンジンによって悪意のあるものとして分類されたファイルハッシュを検出し(大文字と小文字は区別しない)、メッセージに対して適切に設定されたアクションを適用するようになりました。

通知メールの変更	このリリースまでは、特定の受信者に通知メールを送信するコンテンツ フィルタ アクションを設定していた場合、元のメッセージのすべての受信者に対して、電子メールゲートウェイは 1 種類の通知メールが送信されていました。 このリリースにアップグレードすると、電子メールゲートウェイはコンテンツ フィルタ アクションで定義された受信者にのみ通知メールが送信されるようになります。
認証局設定の変更	認証局(CA)の設定変更は、次のいずれかのシナリオに適用されます。 • 下位の AsyncOS バージョンから AsyncOS 14.0 以降のバージョンへのアップグレード。 • Cisco Secure Email Gateway 用の AsyncOS 14.0 を初めてインストールする場合。 認証局リストに次の変更が加えられています。 • 電子メールゲートウェイのカスタム CA 証明書とシステム CA 証明書の数と詳細を表示できます。 カスタム CA 証明書またはシステム CA 証明書の詳細を表示するには、[ネットワーク(Network)] > [証明書(Certificates)] ページで [管理対象の信頼できるルート証明書(Managed Trusted Root Certificates)] オプションを使用します。 • 電子メールゲートウェイでカスタム CA 証明書をアップロード、削除、または追加できます。 • 重複するカスタム CA 証明書を電子メールゲートウェイにアップロードすることはできません。 • (**新しい AsyncOS インストールにのみ適用**):既存のシステム CA 証明書バンドルを利用可能な最新バージョンに更新できます。既存のシステム CA 証明書バンドルを更新するには、Web インターフェイスの [ネットワーク(Network)] > [証明書(Certificates)] ページの [今すぐ更新(Update Now)] オプションまたは `updatenow` CLI コマンドを使用します。 • (**AsyncOS アップグレードにのみ適用**): – アップグレード時に、(現在の AsyncOS ビルドの)システム CA バンドルの有効な CA 証明書を、アップグレードされた AsyncOS ビルドのカスタム CA バンドルに追加するように選択できます。 **(注)** 現在のシステム CA バンドルのバックアップは、`/data/pub/systemca.old/trustedca.old.pem` に保存されます。 – アップグレード後、現在の AsyncOS ビルドのシステム CA 証明書バンドルが自動的に最新バージョンに更新されます。

SSL 暗号設定の変更	次の SSL 暗号設定の変更は、Cisco Secure Email Gateway 用の AsyncOS 14.0 を初めてインストールする場合にのみ適用されます。 • TLS_DHE_RSA_WITH_AES_256_CBC_SHA 暗号スイートは、TLS 1.2 クライアントサービスとサーバサービス(HTTPS GUI、SMTP アウトバウンド、および SMTPインバウンド)ではサポートされなくなりました。 • 次の暗号スイートは、TLS 1.2 クライアントサービス(HTTPS GUI、SMTP アウトバウンド、および SMTP インバウンド)ではサポートされなくなりました。 – TLS_DHE_RSA_WITH_AES_256_CBC_SHA – TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA – TLS_DHE_DSS_WITH_AES_256_CBC_SHA – TLS_DH_RSA_WITH_AES_128_CBC_SHA – TLS_DH_DSS_WITH_AES_128_CBC_SHA – TLS_DH_RSA_WITH_AES_256_CBC_SHA256 – TLS_DH_DSS_WITH_AES_256_CBC_SHA256 – TLS_DH_RSA_WITH_AES_256_CBC_SHA – TLS_DH_DSS_WITH_AES_256_CBC_SHA 次の SSL の設定変更は、次のシナリオのいずれかに適用されます。 • 下位の AsyncOS バージョンから AsyncOS 14.0 以降のバージョンへのアップグレード。 • Cisco Secure Email Gateway 用の AsyncOS 14.0 を初めてインストールする場合。 (X509 検証が有効になっている場合のみ)ピア証明書(LDAP、SMTP アウトバウンド、アップデータ、アラートレシーバなど)の次の署名アルゴリズムはサポートされません。 'sha1withrsaencryption'、'sha224withrsaencryption'、'ecdsa-with-sha1'、'ecsda-with-sha224'、'md2withrsaencryption'、'md4withrsaencryption'、'md5withrsaencryption'、'ripemd128withrsaencryption'、'ripemd160withrsaencryption'、'ripemd256withrsaencryption'、'secp224r1'、'secp192r1'、'brainpoolP160r1'、'brainpoolP192r1'、'secp160r1'、'secp160r2'、'secp192k1'、'secp224k1'、'secp256k1'、'sect163k1'、'sect163r2'、'sect193r1'、'sect193r2'、'sect233k1'、'sect233r1'、'sect239k1'、'sect283k1'、'sect283r1'、'sect409k1'、'sect409r1'、'sect571k1'、'sect571r1'

クライアント証明書の変更	このリリース以降、電子メールゲートウェイで FIPS モードを有効にすると、次のクライアント証明書の変更が適用されます。 • クライアント証明書に署名したルート認証局(CA)の有効期限が切れている場合、電子メールゲートウェイでクライアント証明書をインポートまたは編集することができなくなります。 • クライアント証明書に署名した中間 CA が期限切れまたは失効している場合、電子メールゲートウェイでクライアント証明書をインポートまたは編集することができなくなります。 **解決策**:次のいずれかのアクションを実行して、クライアント証明書を管理します。 • 有効なルート CA でクライアント証明書に署名し、電子メールゲートウェイにアップロードする。 • 有効または失効していない中間 CA でクライアント証明書に署名し、電子メールゲートウェイにアップロードする。
メールログとトラッキングログの変更	このリリース以前は、メールログとトラッキングログの件名の情報は引用符で囲まれていました。 このリリースへのアップグレード後、メールログとトラッキングログの件名の情報は引用符で囲まれなくなりました。
スマート識別子の変更	このリリース以前は、電子メールゲートウェイは、スマート識別子の前に追加されたキーワードに関係なく、メッセージ内のスマート識別子を検出していました。 このリリースへのアップグレード後、電子メールゲートウェイは、スマート識別子の前に追加されたキーワード(「credit」、「ssn」、「cusip」、または「aba」)がメッセージに含まれている場合にのみ、スマート識別子を検出するようになりました。 たとえば、メッセージに社会保障番号(「XXX-XX-XXXX」)が含まれている場合、電子メールゲートウェイは、キーワード、つまり社会保障番号の前に追加された「ssn」(「ssn XXX-XX-XXXX」、「ssn: XXX-XX-XXXX」など)が存在する場合にのみ、スマート識別子として社会保障番号を検出します。
システム正常性 API の変更	このリリースより前のリリースでは(AsyncOS 13.5.x および 13.7 リリースバージョンのみに適用)、システム正常性 API のサンプル応答に、配信ステータス API とシステムステータス API の詳細が含まれていました。 このリリース以降、配信ステータス API とシステムステータス API の詳細は、システム正常性 API の応答から削除されます。これらの詳細は、配信ステータス API とシステムステータス API の対応する応答で表示できるようになりました。

アップグレード パス

- リリース 14.0.1-033 へのアップグレード - MD(メンテナンス導入)(28 ページ)
- リリース 14.0.0-698 へのアップグレード - GD(一般導入)更新(28 ページ)
- リリース 14.0.0-692 へのアップグレード - GD(一般導入)(29 ページ)
- リリース 14.0.0-484 へのアップグレード - LD(限定導入)(29 ページ)

リリース 14.0.1-033 へのアップグレード - MD(メンテナンス導入)

次のバージョンから、リリース 14.0.1-033 にアップグレードすることができます。

- 12.5.3-035
- 12.5.3-107
- 13.0.0-392
- 13.0.1-030
- 13.0.2-030
- 13.5.1-277
- 13.5.2-036
- 13.5.3-010
- 13.5.4-020
- 13.7.0-093
- 14.0.0-698
- 14.0.1-032

リリース 14.0.0-698 へのアップグレード - GD(一般導入)更新

次のバージョンから、リリース 14.0.0-698 にアップグレードすることができます。

- 12.5.1-037
- 12.5.2-011
- 12.5.3-035
- 13.0.0-392
- 13.0.1-030
- 13.0.2-030
- 13.5.1-277
- 13.5.2-036
- 13.5.2-103
- 13.5.2-204
- 13.5.3-010
- 13.7.0-093
- 13.7.0-094
- 14.0.0-484
- 14.0.0-657
- 14.0.0-692

リリース 14.0.0-692 へのアップグレード - GD(一般導入)

次のバージョンから、リリース 14.0.0-692 にアップグレードすることができます。

- 12.5.1-037
- 12.5.2-011
- 12.5.3-035
- 13.0.0-392
- 13.0.1-030
- 13.0.2-030
- 13.5.1-277
- 13.5.2-036
- 13.5.2-103
- 13.5.3-010
- 13.7.0-093
- 14.0.0-484
- 14.0.0-657

リリース 14.0.0-484 へのアップグレード - LD(限定導入)

次のバージョンからリリース 14.0.0-484 にアップグレードできます。

- 12.5.3-035
- 13.0.0-392
- 13.0.2-030
- 13.5.1-277
- 13.5.3-010
- 13.7.0-093
- 14.0.0-450

インストールおよびアップグレードに関する注意事項

このセクションに記載されているインストールとアップグレードの影響を把握および検討してください。

Web インターフェイスまたは CLI(コマンド ライン インターフェイス)から AsyncOS をアップグレードすると、設定は /configuration/upgrade ディレクトリ内のファイルに保存されます。FTP クライアントを使用して、アップグレード ディレクトリにアクセスできます。各設定ファイル名にはバージョン番号が付加され、設定ファイル内のパスワードは人間が判読できないようにマスクされます。

管理者権限を持つユーザとしてログインして、アップグレードする必要があります。また、アップグレード後に電子メールゲートウェイを再起動する必要があります。

このリリースでサポートされているハードウェア

- すべての仮想アプライアンスモデル
- 次のハードウェア モデル
  - C190
  - C195
  - C390
  - C395
  - C690
  - C695
  - C695F

(注) (C695 および C695F モデルの場合のみ):アプライアンスをアップグレードまたは再起動する前に、接続されているファイバ スイッチ ポート インターフェイスで LLDP を無効にします。これにより、FCoE トラフィックが自動的に無効になります。

アプライアンスがサポートされているかどうかを確認し、現在互換性がない場合にその状況を解決するには、http://www.cisco.com/c/en/us/support/docs/field-notices/638/fn63931.html を参照してください。

このリリースでは、次のハードウェアはサポートされていません。

- C160、C360、C660、および X1060
- C170、C370、C370D、C670、および X1070
- C380 および C680 アプライアンス

仮想アプライアンスの展開またはアップグレード

仮想アプライアンスを展開またはアップグレードする場合は、『Cisco コンテンツセキュリティ仮想アプライアンス インストール ガイド』を参照してください。このドキュメントは https://www.cisco.com/c/ja_jp/support/security/email-security-appliance/products-installation-guides-list.html から入手できます。

仮想アプライアンスのアップグレード

現在の仮想アプライアンスのリリースでは 2 TB 超のディスク領域をサポートしていないため、このリリースで 2 TB 超のディスク領域を使用する場合は、仮想電子メールゲートウェイを単にアップグレードすることはできません。

代わりに、このリリース用に新しい仮想マシンインスタンスを導入する必要があります。

仮想電子メールゲートウェイをアップグレードしても、既存のライセンスは変更されません。

ハードウェアアプライアンスから仮想アプライアンスへの移行

ステップ 1 「仮想アプライアンスの展開またはアップグレード (30 ページ)」で説明されているマニュアルを使用して、この AsyncOS リリースで仮想アプライアンスをセットアップします。

ステップ 2 ハードウェアアプライアンスをこの AsyncOS リリースにアップグレードします。

ステップ 3 アップグレードされたハードウェア アプライアンスから設定ファイルを保存します。

ステップ 4 ハードウェアアプライアンスから仮想アプライアンスに設定ファイルをロードします。

ネットワーク設定に関連する適切なオプションを選択してください。

仮想アプライアンスのテクニカル サポートの取得

仮想アプライアンスのテクニカル サポートを受けるための要件は、http://www.cisco.com/c/ja_jp/support/security/email-security-appliance/products-installation-guides-list.html にある『Cisco コンテンツセキュリティ仮想アプライアンス インストール ガイド』に記載されています。

以下のサービスとサポート (41 ページ)も参照してください。

仮想アプライアンスからの Cisco Registered Envelope Service 管理者のプロビジョニングとアクティブ化

仮想アプライアンスのプロビジョニングに必要な情報については、Cisco TAC にお問い合わせください。

アップグレード前の注意事項

アップグレードする前に、次の事項を確認してください。

電子メールゲートウェイで IDN ドメインを使用して設定可能な機能

前提条件:

国際化ドメイン名(IDN)機能を使用する前に、次の前提条件を満たしていることを確認してください。

- すべての着信メッセージには UTF-8 でエンコードされた IDN が必要です。
  たとえば、電子メールゲートウェイにメッセージを送信する MTA は IDN をサポートし、メッセージ内のドメインが UTF-8 形式であることを確認する必要があります。
- すべての発信メッセージには UTF-8 でエンコードされた IDN が必要であり、宛先サーバはそれに応じて IDN を受け入れ、サポートする必要があります。
  たとえば、電子メールゲートウェイからのメッセージを受け入れる MTA は UTF-8 形式でエンコードされた IDN とドメインをサポートする必要があります。
- 該当するすべての DNS レコードで、Punycode 形式を使用して IDN を設定する必要があります。
  たとえば、IDN に MX レコードを設定する場合、DNS レコードのドメインは Punycode 形式である必要があります。

このリリースでは、電子メールゲートウェイ内で IDN ドメインを使用して設定できるのは次の機能**のみ**です。

- SMTP ルートの設定:
  - IDN ドメインを追加または編集します。
  - IDN ドメインを使用して SMTP ルートをエクスポートまたはインポートします。
- **DNS の設定:**IDN ドメインを使用して DNS サーバを追加または編集します。
- リスナーの設定:
  - インバウンドリスナーまたはアウトバウンドリスナーのデフォルトドメインの IDN ドメインを追加または編集します。
  - HAT テーブルまたは RAT テーブルで IDN ドメインを追加または編集します。
  - IDN ドメインを使用して HAT テーブルまたは RAT テーブルをエクスポートまたはインポートします。
- メールポリシーの設定:
  - [着信メールポリシー(Incoming Mail Policies)] の送信者([送信者を追跡する(Following Senders)] オプションまたは [送信者を追跡しない(Following Senders are)] オプション)と受信者([受信者を追跡する(Following Recipients)]または[受信者を受信しない(Recipients are not)]オプション)の IDN ドメインを使用してドメインを追加または編集します。
  - [発信メールポリシー(Outgoing Mail Policies)] の送信者([送信者を追跡する(Following Senders)] オプションまたは [送信者を追跡しない(Following Senders are)] オプション)と受信者([受信者を追跡する(Following Recipients)]または[受信者を受信しない(Recipients are not)]オプション)の IDN ドメインを使用してドメインを追加または編集します。
  - [着信メールポリシー(Incoming Mail Policies)] または [送信メールポリシー(Outgoing Mail Policies)] で IDN ドメインを使用した送信者または受信者の検索
  - IDN ドメインを使用して送信者判定の例外を定義します。
  - IDN ドメインを使用してアドレスリストを作成します。
  - 宛先の制御に IDN ドメインを使用して宛先ドメインを追加または編集します。

- **バウンスプロファイルの設定:**IDN ドメインを使用して代替電子メールアドレスを追加または編集します。
- **送信者ドメインレピュテーションの設定:**IDN ドメインの送信者ドメイン レピュテーション スコアを定義します。
- **IP レピュテーションの設定:**IDN ドメインの IP レピュテーションスコアを定義します。
- **LDAP の設定:**IDN ドメインを使用して、LDAP グループクエリを作成し、クエリを受け入れ、クエリをルーティングし、クエリをマスカレードします。
- **レポートの設定:**IDN データ(ユーザ名、電子メールアドレス、ドメイン)をレポートに表示します。
- **メッセージトラッキングの設定:**メッセージトラッキングに IDN データ(ユーザ名、電子メールアドレス、およびドメイン)を表示します。
- ポリシー、ウイルス、およびアウトブレイク隔離の設定:
  - ウイルス対策エンジンによる判定に従って、マルウェアを送信する可能性のある IDN ドメインを含むメッセージを表示します。
  - スパムまたはマルウェアの可能性があるとアウトブレイクフィルタによって検出された IDN ドメインを含むメッセージを表示します。
  - メッセージフィルタ、コンテンツフィルタ、および DLP メッセージアクションによって検出された IDN ドメインを含むメッセージを表示します。
- **スパムの隔離の設定:**
  - スパム、または疑いのあるスパムとして検出された IDN ドメインを含むメッセージを表示します。
  - IDN ドメインを含む電子メールアドレスをセーフリストとブロックリストのカテゴリに追加します。

(注) 現在、IDN ドメインを持つ受信者は、[スパムの管理(Spam Quarantine)] 設定ページの [エンドユーザの隔離アクセス(End-User Quarantine Access] セクションでエンドユーザ認証方式が [なし(None)] に設定されている場合にのみ、エンドユーザの隔離にアクセスできます。

- [SPF構成設定(SPF Configuration Settings)]:IDN ドメインを使用してメッセージの SPF 検証を実行します。
- [DKIM構成設定(DKIM Configuration Settings)]:IDN ドメインを使用して DKIM 署名とメッセージの検証を実行します。
- [DMARC構成設定(DMARC Configuration Settings)]:IDNドメインを使用してメッセージの DMARC 検証を実行します。

既存の URL レピュテーション判定の新しいカテゴリと新しい名前

次の表に、電子メールゲートウェイの既存の URL レピュテーション判定の新しいカテゴリと新しい名前を示します。

現在の URL レピュテーション判定名	新しい Cisco Talos URL レピュテーション判定名	スコア範囲	説明
クリーン	信頼できる	+6.0 ~ +10.0	優れた安全性を示す動作を表示します。
ニュートラル	好ましい	+0.1 ~ +5.9	一定のレベルの安全性を示す動作を表示します。
	ニュートラル	-3.0 ~ 0.0	好ましい動作や望ましくない動作は表示されません。ただし、この判定は評価の結果です。
	要検討	-5.9 ~ -3.1	リスクを示す可能性のある動作、または望ましくない動作を表示します。
悪意のある	信頼できない	-10.0 ~ -6.0	非常に悪い、悪意のある、または望ましくない動作を表示します。
スコアなし	不明	スコアなし	この判定は、これまで評価されなかった場合や、脅威レベルの判定をアサートできない場合に表示されます。

Cisco Talos サービスにアクセスするためのファイアウォール設定

電子メールゲートウェイを Cisco Talos サービスに接続するには、次のホスト名または IP アドレス用にファイアウォール上で HTTPS(Out)443 ポートを開く必要があります(以下の表を参照)。

(注) HTTPS アップデータプロキシ設定は、Cisco Talos サービスへの接続に使用されます。

ホスト名	IPv4	IPv6
grpc.talos.cisco.com	146.112.62.0/24	2a04:e4c7:ffff::/48
email-sender-ip-rep-grpc.talos.cisco.com	146.112.63.0/24	2a04: e4c7: fffe::/48
serviceconfig.talos.cisco.com	146.112.255.0/24	-
	146.112.59.0/24	-

詳細については、ユーザガイドの「Firewall」の章を参照してください。

Cisco Advanced Phishing Protection クラウドサービスにアクセスするためのファイアウォールの設定

電子メールゲートウェイを Cisco Advanced Phishing Protection クラウドサービスに接続するには、次のホスト名用にファイアウォール上で HTTPS(Out)443 ポートを開く必要があります。

- kinesis.us-west-2.amazonaws.com
- sensor-provisioner.ep.prod.agari.com
- houston.sensor.prod.agari.com

詳細については、ユーザガイドの「Firewall」の章を参照してください。

電子メールゲートウェイでのサービスログの有効化

サービスログは、Cisco E メール セキュリティ アプライアンス データ シートに基づいて個人データを収集するために使用されます。

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。

Cisco Secure Email Gateway は、顧客の電子メールから限定された個人データを収集し、幅広く有用な脅威検出機能を提供します。この機能は、検出された脅威アクティビティを収集し、傾向を提示し、関連付けるための専用分析システムと組み合わせることができます。シスコでは、個人データを使用して、脅威の状況を分析し、悪意のある電子メールに脅威の分類ソリューションを提供し、スパム、ウイルス、ディレクトリ獲得攻撃などの新しい脅威から電子メールゲートウェイを保護するために、電子メールゲートウェイの機能を向上させています。

アップグレードプロセス中に、次のいずれかから電子メールゲートウェイでサービスログを有効にする方法を選択できます。

- Web インターフェイスの [システム管理(System Administration)] > [システムアップグレード(System Upgrade)] ページで、[サービスログ(Service Logs)] に [同意する(I Agree)] オプションを選択します。
- upgrade CLI コマンドの「サービスログをデフォルトで有効にして続行しますか？ [Y] *(Do you agree to proceed with Service Logs being enabled by default? [y])*」に「Yes」と入力します。

詳細については、ユーザガイドの「Improving Phishing Detection Efficacy using Service Logs」の章を参照してください。

クラスタレベルでのインテリジェント マルチスキャンとグレイメール設定のアップグレード

AsyncOS 14.0 にアップグレードする前に、インテリジェント マルチスキャンとグレイメールの設定が同じクラスタレベルに存在していることを確認します。クラスタレベルが異なっている場合は、アップグレード後にインテリジェント マルチスキャンとグレイメールの設定を確認する必要があります。

FIPS の準拠性

AsyncOS 14.0.1 リリースは、FIPS 準拠のリリースではありません。電子メールゲートウェイで FIPS モードを有効にしている場合は AsyncOS 14.0.1 にアップグレードする前に FIPS モードを無効にする必要があります。

AsyncOS の以前のバージョンへの復元

次の AsyncOS バージョンは、内部テストインターフェイスの脆弱性(http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160922-esa)の影響を受けます。

- 9.1.2-023
- 9.1.2-028
- 9.1.2-036
- 9.7.2-046
- 9.7.2-047

- 9.7-2-054
- 10.0.0-124
- 10.0.0-125

集中管理(クラスタ化されたアプライアンス)を使用した展開のアップグレード

クラスタに C160、C360、C660、X1060、C170、C370、C670、C380、C680、または X1070 ハードウェア アプライアンスが含まれている場合は、アップグレードの前に、これらのアプライアンスをクラスタから削除してください。

クラスタ内のすべてのマシンが同じバージョンの AsyncOS を実行している必要があり、x60、x70、および x80 ハードウェアをこのリリースにアップグレードすることはできません。必要に応じて、x60、x70、および x80 アプライアンス用に別のクラスタを作成してください。

直前のリリース以外のリリースからのアップグレード

このリリースの直前のリリース以外のメジャー(AsyncOS X.0)またはマイナー(AsyncOS X.x)リリースからアップグレードする場合は、現在のリリースとこのリリースの間にあるメジャー リリースとマイナー リリースのリリース ノートを確認する必要があります。

メンテナンス リリース(AsyncOS X.x.x)には、バグ修正のみが含まれています。

設定ファイル

通常、シスコは、以前のメジャーリリースに関して、設定ファイルの下位互換性をサポートしていません。マイナーリリースのサポートが提供されています。以前のバージョンの設定ファイルは以降のリリースで動作する可能性がありますが、ロードするために変更が必要になる場合があります。設定ファイルのサポートについて不明な点がある場合は、シスコカスタマーサポートでご確認ください。

アップグレード中の IPMI メッセージ

CLI を使用して電子メールゲートウェイをアップグレードする場合、IPMI に関連するメッセージが表示されることがあります。これらのメッセージは無視しても差し支えありません。これは既知の問題です。

障害 ID:CSCuz28415

このリリースへのアップグレード

はじめる前に

- ワークキュー内のすべてのメッセージをクリアします。ワークキューをクリアせずにアップグレードを実行することはできません。
- 既知の問題(40 ページ) とインストールおよびアップグレードに関する注意事項(29 ページ)を確認してください。
- 仮想電子メールゲートウェイをアップグレードする場合は、仮想アプライアンスのアップグレード(30 ページ)を参照してください。

手順

次の手順を実行して電子メールゲートウェイをアップグレードします。

ステップ 1 電子メールゲートウェイから、XML 構成ファイルを保存します。

ステップ 2 セーフリスト/ブロックリスト機能を使用している場合は、電子メールゲートウェイからセーフリスト/ブロックリストデータベースをエクスポートします。

ステップ 3 すべてのリスナーを一時停止します。

ステップ 4 ワークキューが空になるまで待ちます。

ステップ 5 [システム管理(System Administration)] タブで、[システムアップグレード(System Upgrade)] ページを選択します。

ステップ 6 [利用可能なアップグレード(Available Upgrades)] ボタンをクリックします。ページが更新され、使用可能な AsyncOS アップグレード バージョンのリストが表示されます。

ステップ 7 [アップグレードの開始(Begin Upgrade)] ボタンをクリックすると、アップグレードが開始されます。表示される質問に答えます。

ステップ 8 アップグレードが完了したら、[今すぐリブート(Reboot Now)] ボタンをクリックして電子メールゲートウェイを再起動します。

ステップ 9 すべてのリスナーを再開します。

次の作業

- アップグレード後、SSL の設定を確認し、使用する正しい GUI HTTPS、インバウンド SMTP、およびアウトバウンド SMTP 方式が選択されていることを確認します。[システム管理(System Administration)] > [SSL 構成(SSL Configuration)] ページを使用するか、CLI で `sslconfig` コマンドを使用します。手順については、ユーザガイドまたはオンラインヘルプの「System Administration」の章を参照してください。
- 「パフォーマンスアドバイザリ(39 ページ)」を確認してください。
- SSH キーを変更した場合は、アップグレード後に電子メールゲートウェイと Cisco Secure Email and Web Manager 間の接続を再認証します。

アップグレード後の注意事項

電子メールゲートウェイでのパスワードで保護された添付ファイルのスキャン

パスワード保護された添付ファイルをスキャンするように電子メールゲートウェイのコンテンツスキャナを設定する場合、電子メールトラフィックにパスワード保護された添付ファイルが高い割合で含まれていると、パフォーマンスに影響を与える可能性があります。

(スマートライセンスのユーザーのみ)電子メールゲートウェイを Cisco Talos サービスに接続できない

電子メールゲートウェイがスマートライセンスモードで、システム時刻が GMT よりも遅い場合、電子メールゲートウェイで Cisco Talos サービスへの接続に関する問題が発生する可能性があります。

解決策:時刻設定で NTP サーバーを使用するように電子メールゲートウェイを設定していることを確認します。

AsyncOS 13.x へのアップグレード後のクラスタレベルでの DLP 設定の不整合

AsyncOS 13.x にアップグレードした後、電子メールゲートウェイがクラスタモードになっていて、DLP が設定されている場合は、CLI を使用して `clustercheck` コマンドを実行すると DLP 設定の不整合が表示されます。

この不整合を解決するには、クラスタ全体でクラスタ内の他のいずれかのマシンの DLP 設定を使用するように強制します。次のプロンプトを使用します。「この不整合をどのように解決しますか？(How do you want to resolve this inconsistency?)」。次の例に示すように、`clustercheck` コマンドを入力します。

```
(Cluster)> clustercheck
Checking DLP settings...
Inconsistency found!
DLP settings at Cluster test:
mail1.example.com was updated Wed Jan 04 05:52:57 2017 GMT by 'admin' on mail2.example.com
mail2.example.com was updated Wed Jan 04 05:52:57 2017 GMT by 'admin' on mail2.example.com
How do you want to resolve this inconsistency?
1. Force the entire cluster to use the mail1.example.com version.
2. Force the entire cluster to use the mail2.example.com version.
3. Ignore.
[3]>
```

インテリジェント マルチスキャンおよびグレイメールのグローバル設定の変更

AsyncOS 14.0 にアップグレードした後のインテリジェント マルチスキャン(IMS)およびグレイメールのグローバル設定の変更点は次のとおりです。

- IMS およびグレイメールのグローバル設定が異なるクラスタレベルで構成されている場合、電子メールゲートウェイはグローバル設定を最も低い設定レベルにコピーします。たとえば、クラスタレベルで IMS を設定し、マシンレベルでグレイメールを設定すると、電子メールゲートウェイは IMS のグローバル設定をマシンレベルにコピーします。
- スキャンメッセージの最大メッセージサイズとタイムアウト値が異なる場合、電子メールゲートウェイは最大タイムアウトおよび最大メッセージサイズの値を使用して、IMS とグレイメールのグローバル設定を行います。たとえば、IMS およびグレイメールの最大メッセージサイズの値がそれぞれ 1M と 2M である場合、アプライアンスは IMS とグレイメールの両方の最大メッセージサイズ値として 2M を使用します。

パフォーマンスアドバイザリ

アウトブレイクフィルタ

アウトブレイクフィルタは、コンテキスト適応スキャンエンジンを使用してメッセージの脅威レベルを判定し、アダプティブルールとアウトブレイクルールの組み合わせに基づいてメッセージにスコアを付けます。一部の設定では、中程度のパフォーマンス低下が発生する可能性があります。

IronPort スパム隔離

C シリーズのアプライアンスに対して IronPort スパム隔離オンボックスを有効にすると、公称水準の負荷がかかっているアプライアンスでは、システムスループットにわずかな低下が生じます。ピークスループット付近またはピークスループットで実行されている電子メールゲートウェイの場合、アクティブな隔離からの追加の負荷によって、スループットが 10 ~ 20% 低下する可能性があります。システムのキャパシティがいっぱいか、いっぱいに近いときに IronPort スパム隔離を使用する場合は、規模が大きい C シリーズ アプライアンスまたは M シリーズ アプライアンスへの移行を検討してください。

スパム対策ポリシーをスパムのドロップから隔離に変更する場合(オンボックスまたはオフボックス)、ウイルスおよびコンテンツ セキュリティのために追加のスパムメッセージをスキャンする必要があるため、システムの負荷が増大します。インストールのサイジングを適切に行う際にサポートが必要な場合は、認定サポートプロバイダーにお問い合わせください。

既知および修正済みの問題

シスコのバグ検索ツールを使用して、このリリースの既知および修正済みの不具合に関する情報を検索します。

- バグ検索ツールの要件(39 ページ)
- 既知および修正済みの問題のリスト(39 ページ)
- 関連資料(41 ページ)

バグ検索ツールの要件

シスコ アカウントを持っていない場合は、登録します。
https://identity.cisco.com/ui/tenants/global/v1.0/enrollment-ui に移動します。

既知および修正済みの問題のリスト

- 14.0.1 の既知および修正済みの問題(40 ページ)
- 既知および解決済みの問題に関する情報の検索(40 ページ)

14.0.1 の既知および修正済みの問題

既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282941569&rls=14.0.1&sb=afr&sts=open&svr=3nH&bt=custV
修正済みの問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282941569&rls=14.0.1-033&sb=fr&sts=fd&svr=3nH&bt=custV

14.0 の既知および修正済みの問題

既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282941569&rls=14.0.0&sb=afr&sts=open&svr=3nH&bt=custV
修正済みの問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282941569&rls=14.0.0-698&sb=fr&sts=fd&svr=3nH&bt=custV

既知および解決済みの問題に関する情報の検索

シスコのバグ検索ツールを使用して、既知および解決済みの不具合に関する最新情報を検索します。

はじめる前に

シスコ アカウントを持っていない場合は、登録します。
https://identity.cisco.com/ui/tenants/global/v1.0/enrollment-ui に移動します。

手順

ステップ 1 https://tools.cisco.com/bugsearch/ に移動します。

ステップ 2 シスコ アカウントのクレデンシャルでログインします。

ステップ 3 [リストから選択(Select from list)] > [セキュリティ(Security)] > [E メールセキュリティ(Email Security)] > [Cisco E メールセキュリティアプライアンス(Cisco Email Security Appliance)] の順にクリックし、[OK] をクリックします。

ステップ 4 [Releases] フィールドに、リリースのバージョン(たとえば、14.0.1)を入力します。

ステップ 5 要件に応じて、次のいずれかを実行します。

- 解決済みの問題のリストを表示するには、[バグの表示(Show Bugs)] ドロップダウンから、[これらのリリースで修正済み(Fixed in these Releases)] を選択します。
- 既知の問題のリストを表示するには、[バグの表示(Show Bugs)] ドロップダウンから [これらのリリースに影響(Affecting these Releases)] を選択し、[ステータス(Status)] ドロップダウンから [開く(Open)] を選択します。

ご不明な点がある場合は、ツールの右上にある [ヘルプ(Help)] または [フィードバック(Feedback)] リンクをクリックしてください。また、インタラクティブなツアーもあります。これを表示するには、[検索(search)] フィールドの上のオレンジ色のバーにあるリンクをクリックします。

関連資料

マニュアルの内容 （Cisco Content Security 製品）	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 Secure Email and Web Manager	http://www.cisco.com/c/ja_jp/support/security/content-security-management-appliance/tsd-products-support-series-home.html
Cisco Web セキュリティ	http://www.cisco.com/c/ja_jp/support/security/web-security-appliance/tsd-products-support-series-home.html
Cisco Secure Email ゲートウェイ	http://www.cisco.com/c/ja_jp/support/security/email-security-appliance/tsd-products-support-series-home.html
Cisco コンテンツ セキュリティ アプライアンス用 CLI リファレンス ガイド	http://www.cisco.com/c/ja_jp/support/security/email-security-appliance/products-command-reference-list.html
Cisco IronPort Encryption	http://www.cisco.com/c/ja_jp/support/security/email-encryption/tsd-products-support-series-home.html

サービスとサポート

（注） 仮想アプライアンスのサポートを受けるには、仮想ライセンス番号（VLN）をご用意の上 Cisco TAC に連絡してください。

Cisco TAC：http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

従来の IronPort のサポート サイト：http://www.cisco.com/web/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。