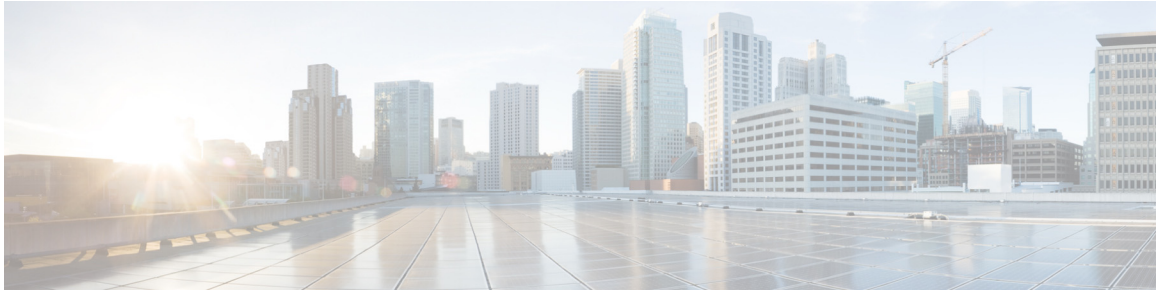

# AsyncOS 15.0 for Cisco Secure Email Gateway リリースノート（一般導入）

**発行日：2023 年 8 月 10 日**

## 目次




**Cisco Systems, Inc.**
www.cisco.com

# 今回のリリースでの変更点

| 機能 | 説明 |
|---|---|
| 脅威検出効果の向上 | 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。<br>• HTML 解析と悪意のあるスクリプト検出の改善<br>• URL 解析とリダイレクト検出の改善<br>この機能を使用するには、次の設定手順を実行します。<br>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。<br>**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)]<br>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。<br>**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]>`」<br>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。<br>a. 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。<br>b. [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。<br>c. [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。<br>d. 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。<br>e. [オプション]:その他必要なスパム対策の設定を行います。<br>f. [送信(Submit)] をクリックし、変更をコミットします。<br>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。<br>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。<br>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。<br>[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。<br>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」の章を参照してください。 |
| 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。<br>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。<br>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。<br>• 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。<br>• CLI での `Threatdefenseconfig` コマンドの使用。<br>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、または CLI リファレンスガイドの「Integrating Secure Email Gateway with Threat Defense」の章を参照してください。 |

| | |
|---|---|
| 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。<br>• バナーの位置<br>• バナーの色<br>• バナーメッセージのテキストの色<br>• バナーメッセージの内容<br>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。<br>（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。<br>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「Managing Spam and Graymail」の章にある「Customizing Graymail Unsubscribe Banner based on Organizational Requirements」の項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。<br>（注） [Cisco Secure Endpoint プライベート クラウド ユーザーのみ]: このリリースにアップグレードする前に、新しいファイル レピュテーション サービスのアクティブ化の前提条件をすべて満たしていることを確認してください。詳細については、このドキュメントの「アップグレード前の注意事項」の項の「暗号化通知テンプレートの削除」サブセクションを参照してください。<br>（注） [Cisco Secure Endpoint プライベート クラウド ユーザーのみ]: アップグレード中にファイル レピュテーション サービスのアクティブ化に関する手順をスキップした場合は、アップグレード後のファイル レピュテーション サービスのアクティブ化方法について、このドキュメントの「アップグレード後の注意事項」の項にある「次期 AsyncOS リリースにおけるシスコ スマート ソフトウェア ライセンシングの必須使用」サブセクションを参照してください。<br>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「File Reputation Filtering and File Analysis」の章を参照してください。 |

| | |
|---|---|
| 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。<br>• 認証 API<br>• URL リスト API<br>• ディクショナリ API<br>• ホストアクセステーブル（HAT）API<br>（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。<br>（注） 構成 API の場合:<br>- 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。<br>- 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。<br>- 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。<br>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。 |

| | |
|---|---|
| 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 | 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。<br><br>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。<br><br>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。<br><br>`"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.`<br><br>`In your case it is, 7.1 MB, which was last updated in 01 Jul 2022.`<br><br>`If you proceed with this upgrade process, the data in the old storage will be removed.`<br><br>`You can choose to proceed with the upgrade or abort the upgrade.`<br><br>`Do you want to proceed with the upgrade?[Y]"`<br><br>**（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。 |
| 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。<br><br>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。<br><br>**（注）** 電子メールゲートウェイがクラスタ内にある場合、`deletelogfile` サブコマンドはマシンレベルのオプションです。<br><br>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。 |
| 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）。<br><br>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「FIPS Management」の章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。<br>(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。<br>(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。<br>詳細については、https://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html から『Cisco Content Security Virtual Appliance Installation Guide』を参照してください。 |
| 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。<br>詳細については、https://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html から『Cisco Content Security Virtual Appliance Installation Guide』を参照してください。 |
| 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。<br>詳細については、https://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html から『Cisco Content Security Virtual Appliances on AWS EC2 Installation Guide』を参照してください。 |
| 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。<br>(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。<br>(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。<br>詳細については、https://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html から『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。 |

| | |
|---|---|
| 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。<br>• C100V<br>• C300V<br>• C600V<br>各仮想アプライアンスモデルに該当する新しい 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。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。 |
| 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。 |

| | |
|---|---|
| 事前定義された DLP ポリシーの新しい分類子 | 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。<br>• 銀行口座番号（オーストリア IBAN）<br>• 銀行口座番号（ベルギー IBAN）<br>• 銀行口座番号（ブルガリア IBAN）<br>• 銀行口座番号（クロアチア IBAN）<br>• 銀行口座番号（キプロス IBAN）<br>• 銀行口座番号（チェコ共和国 IBAN）<br>• 銀行口座番号（デンマーク IBAN）<br>• 銀行口座番号（エストニア IBAN）<br>• 銀行口座番号（フィンランド IBAN）<br>• 銀行口座番号（ギリシャ IBAN）<br>• 銀行口座番号（ハンガリー IBAN）<br>• 銀行口座番号（アイルランド IBAN）<br>• 銀行口座番号（ラトビア IBAN）<br>• 銀行口座番号（リトアニア IBAN）<br>• 銀行口座番号（ルクセンブルク IBAN）<br>• 銀行口座番号（マルタ IBAN）<br>• 銀行口座番号（ポーランド IBAN）<br>• 銀行口座番号（ポルトガル IBAN）<br>• 銀行口座番号（ルーマニア IBAN）<br>• 銀行口座番号（スロバキア IBAN）<br>• 銀行口座番号（スロベニア IBAN）<br>• 銀行口座番号（スペイン IBAN）<br>• カンボジア国民 ID<br>• キプロス国民 ID<br>• フィンランド国民 ID<br>• マルタ国民 ID<br>• ミャンマー国民 ID<br>• ポルトガル国民 ID<br>• ベトナム国民 ID |
| 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。<br>• GUI HTTPS<br>• インバウンド SMTP |

# 動作における変更

| | |
|---|---|
| 送信者ドメイン レピュテーション フィルタリング:ドメイン例外リストの変更 | [このリリースの前]:[Envelope From:のドメインに基づいてドメイン例外リストを照合(Match Domain Exception List based on Domain in Envelope From:)] オプションを無効にすると、メッセージの「Envelope From:」、「From:」、および「Reply-To:」ヘッダーのドメインが同じであり、ドメイン例外リストにある場合にのみ、メッセージがドメイン例外リストと照合されます。<br>[このリリース以降]:[Envelope From:のドメインに基づいてドメイン例外リストを照合(Match Domain Exception List based on Domain in Envelope From:)] オプションを無効にすると、メッセージの「Envelope From:」、「From:」、および「Reply-To:」ヘッダーのドメインが異なり、「HELO:」、「RDNS:」、「Envelope From:」、「From:」、および「Reply-To:」のいずれかのドメインがドメイン例外リストにある場合でも、メッセージがドメイン例外リストと照合されます。 |
| RFC 違反のため、メッセージをスキャン不可(Unscannable)として分類する新しい条件 | [このリリース前]: メッセージの MIME 部分に複数の「Content-Transfer-Encoding」ヘッダーが含まれている場合、コンテンツスキャナは RFC 違反によりメッセージを「スキャン不可(Unscannable)」として分類しませんでした。<br>[このリリース以降]:MIME 部分に複数の「Content-Transfer-Encoding」ヘッダーが含まれている場合、コンテンツスキャナは RFC 違反のため、メッセージを「スキャン不可(Unscannable)」として分類します。「セキュリティサービス(Security Services) > スキャン動作(Scan Behavior) > RFC 違反が原因でメッセージをスキャンできない場合のアクション(Action when a message is unscannable due to RFC violations)」で設定されたアクションがメッセージに適用されます。 |
| Syslog メッセージの変更 | [このリリースの前]:Syslog メッセージには、電子メールゲートウェイの設定済み IP アドレスが表示されていました。<br>[このリリース以降]:Syslog メッセージに IP アドレスは表示されませんが、電子メールゲートウェイの設定された FQDN またはホスト名が表示されるようになりました。 |

| | |
|---|---|
| [アップグレードのシナリオ]: SSH サーバーとクライアントの設定の変更 | 電子メールゲートウェイを下位の AsyncOS バージョンから AsyncOS 15.0 バージョン以降にアップグレードする場合は、次の SSH サーバーとクライアントの設定の変更が適用されます。<br>[**非 FIPS モードのみ**]: 電子メールゲートウェイが FIPS モードでない場合に適用される、SSH サーバーおよびクライアントの設定の変更は次のとおりです。<br>[**SSH サーバーの設定の変更**]:<br>• 次の暗号アルゴリズム、MAC メソッド、KEX アルゴリズム、およびホストキーアルゴリズムは、デフォルトで電子メールゲートウェイから削除されます。<br>– **暗号アルゴリズム**: `3des-cbc` および `rijndael-cbc@lysator.liu.se`<br>– **MAC メソッド**: `hmac-md5`、`umac-64@openssh.com`、`hmac-ripemd160`、`hmac-ripemd160@openssh.com`、`hmac-sha1-96`、および `hmac-md5-96`<br>– **KEX アルゴリズム**: `diffie-hellman-group-exchange-sha256` および `diffie-hellman-group-exchange-sha1`<br>– **ホストキーアルゴリズム**: `rsa1`<br>• [最小サーバーキー（Minimum Server Key）] オプションは、デフォルトで電子メールゲートウェイの CLI から削除されます。<br>• ホストキーアルゴリズム - `rsa-sha2-256` は、デフォルトで電子メールゲートウェイに追加されます。<br>[**SSH クライアント設定の変更**]:<br>• 暗号アルゴリズム - `arcfour256` および `arcfour128` は、デフォルトで電子メールゲートウェイから削除されます。<br>• ホストキーアルゴリズム - `rsa-sha2-256` は、デフォルトで電子メールゲートウェイに追加されます。 |

| | |
|---|---|
| [アップグレードのシナリオ]: SSH サーバーとクライアントの設定の変更（続き） | [**FIPS モードのみ**]: 電子メールゲートウェイが FIPS モードである場合に適用される、SSH サーバーおよびクライアントの設定の変更は次のとおりです。<br>[**SSH サーバーの設定の変更**]:<br>• 次の暗号アルゴリズム、KEX アルゴリズム、およびホストキーアルゴリズムは FIPS 非準拠であり、電子メールゲートウェイから削除されます。<br>– **暗号アルゴリズム**: `3des-cbc`<br>– **KEX アルゴリズム**: `diffie-hellman-group-exchange-sha256` および `diffie-hellman-group-exchange-sha1`<br>– **ホストキーアルゴリズム**: `ssh-rsa`<br>• [最小サーバーキーサイズ（Minimum Server Key Size）] オプションは、FIPS 非準拠であるため、電子メールゲートウェイの CLI から削除されます。<br>• ホストキーアルゴリズム - `rsa-sha2-256` は、デフォルトで電子メールゲートウェイに追加されます。<br>• ホスト キー アルゴリズム - `ssh-dss` は、デフォルトで電子メール ゲートウェイから削除されます（CLI で `logconfig` > `hostkeyconfig` サブコマンドを使用して設定されている場合）。<br>[**SSH クライアント設定の変更**]:<br>• 暗号アルゴリズム - `3des-cbc` は FIPS 非準拠であるため、電子メールゲートウェイから削除されます。<br>• ホストキーアルゴリズム - `rsa-sha2-256` は、デフォルトで電子メールゲートウェイに追加されます。 |

| | |
|---|---|
| [新規インストールのシナリオ]:SSH サーバの設定変更 | 次の SSH サーバー設定の変更は、Cisco Secure Email Gateway 用の AsyncOS 15.0 を初めてインストールする場合にのみ適用されます。<br>[**非 FIPS モードのみ**]:電子メールゲートウェイでは、次の暗号アルゴリズム、MAC メソッド、KEX アルゴリズム、およびホストキーアルゴリズムがサポートされています。<br>• **暗号アルゴリズム**:`aes128-ctr`、`aes192-ctr`、`aes256-ctr`、`aes128-cbc`、`aes192-cbc`、および `aes256-cbc`<br>• **MAC メソッド**:`hmac-sha1`<br>• **KEX アルゴリズム**:`diffie-hellman-group14-sha1`、`ecdh-sha2-nistp256`、`ecdh- sha2-nistp384`、および `ecdh-sha2-nistp521`<br>• **ホストキーアルゴリズム**:`rsa-sha2-256`、`ssh-rsa`、および `ssh-dss`(デフォルトでは無効)<br>(注) CLI で `shconfig > sshd > setup` サブコマンドを使用して、「`ssh-dss`」暗号アルゴリズムを手動で有効にする必要があります。<br>---<br>[**FIPS モードのみ**]:FIPS モードを有効にするには、まず CLI で `sshconfig > sshd > setup` サブコマンドを使用して、FIPS 非準拠の次の暗号アルゴリズムおよびホストキーアルゴリズムを無効にします。<br>• **暗号アルゴリズム**:`aes192-ctr`<br>• **ホストキーアルゴリズム**:`ssh-rsa`<br>(注) ホストキーアルゴリズム - `rsa-sha2-256` が新しく追加され、デフォルトで電子メールゲートウェイで有効になっています。 |
| SPF 電子メール検証の変更 | [このリリースの前]:電子メールゲートウェイは、RFC 4408(セクション 4.4)標準に従って、SPF および TXT レコードに基づいて Sender Policy Framework(SPF)電子メール検証プロセスを実行します。<br>[このリリース以降]:電子メールゲートウェイは、新しい RFC 7208(セクション 4.4)標準に従って、TXT レコードのみに基づいて SPF 電子メール検証プロセスを実行します。 |
| 統合イベントログの CEF フィールド名の変更 | このリリース以降、統合イベントログの次の Common Event Format(CEF)フィールド名が変更されました。<br>• 「`endTime`」から「`end`」<br>• 「`startTime`」から「`start`」<br>• 「`sourceAddress`」から「`src`」<br>• 「`sourceHostName`」から「`shost`」 |

| | |
|---|---|
| ファイル分析のための HTML および Octet-stream ファイルのアップロードにおける変更 | [このリリースの前]:ファイル分析用のファイル拡張子が選択されている場合、電子メールゲートウェイは、HTML および Octet-stream ファイル(MIME タイプ:application/octet-stream および text/html)のみをファイル分析サーバーにアップロードできました。<br>[このリリース以降]:電子メールゲートウェイは、ファイル分析用のファイル拡張子が選択されていない場合でも、ファイル分析のために HTML および Octet-stream ファイルをファイル分析サーバーにアップロードできるようになりました。<br>(注) ファイル分析サーバーにアップロードされるファイルの数が増えると、電子メールゲートウェイがすぐにファイル分析サーバーのファイルアップロード制限に達する可能性があります。 |
| ファイル分析のためのアーカイブファイルのアップロードにおける変更 | [このリリースの前]:AMP エンジンがメッセージからアーカイブファイル(パスワードで保護されアーカイブされた添付ファイルを含む)の抽出に失敗すると、添付ファイルはファイル分析サーバーにアップロードされませんでした。<br>[このリリース以降]:AMP エンジンがメッセージからアーカイブファイル(パスワードで保護されアーカイブされた添付ファイルを含む)の抽出に失敗した場合に、添付ファイルはファイル分析のためにファイル分析サーバーにアップロードされるようになりました。<br>(注) ファイル分析サーバーにアップロードされるファイルの数が増えると、電子メールゲートウェイがすぐにファイル分析サーバーのファイルアップロード制限に達する可能性があります。 |
| メッセージスキャンのデフォルトしきい値の変更 | [このリリースの前]: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エンジンがメッセージをスキャンしないデフォルトのしきい値は、1 M に設定されていました。<br>[このリリース以降]: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エンジンがメッセージをスキャンしないデフォルトのしきい値は、2 M に設定されます。 |
| ECDSA および EDDSA 証明書のインポートのサポート | このリリース以降、ECDSA および EDDSA アルゴリズムを使用した x509 証明書のサポートが導入されました。 |
| 暗号設定の変更 | 非準拠/脆弱な TLS 暗号スイートは、インバウンド SMTP、アウトバウンド SMTP、GUI、LDAP、およびアップデータでデフォルトで無効になりました。<br>`ssh-dss` などの非準拠 CSDL キー SSH アルゴリズムは、デフォルトで SSH サーバーで無効になりましたが、設定することはできます。 |
| 自己署名証明書の作成時に署名アルゴリズムを選択するためのサポート | このリリース以降、CLI と GUI の両方で自己署名/自己署名 SMIME 証明書を生成する際に、署名アルゴリズム(sha256withRSAEncryption、sha384withRSAEncryption、または sha512withRSAEncryption)を選択できます。 |

| | |
|---|---|
| x509 証明書の署名アルゴリズムの変更 | TLS サービス（インバウンド SMTP、スマート ライセンス トランスポート URL サーバー、登録クライアント、SSE サーバー、Talos クライアント、Syslog サーバー、ECS クライアント、および Cisco Security Awareness クラウドサーバー）のピア証明書に次の署名アルゴリズムはサポートされません。<br>`'sha1withrsaencryption', 'sha224withrsaencryption', 'dsawithsha1', 'ecdsa-with-sha1', 'ecsda-with-sha224', 'md2withrsaencryption', 'md4withrsaencryption', 'md5withrsaencryption', 'ripemd128withrsaencryption', 'ripemd160withrsaencryption', 'ripemd256withrsaencryption', 'ripemd128withrsa', 'ripemd160withrsa', 'ripemd256withrsa'`<br>TLS サービス（インバウンド SMTP、スマート ライセンス トランスポート URL サーバー、登録クライアント、SSE サーバー、Talos クライアント、Syslog サーバー、ECS、および Cisco Security Awareness クラウドサーバー）の ECDSA 署名アルゴリズムを使用したピア証明書の次の曲線はサポートされません。<br>`'secp224r1', 'secp192r1', 'brainpoolP160r1', 'brainpoolP192r1', 'secp160r1', 'secp160r2', 'prime192v1', 'secp192k1', 'secp224k1', 'secp256k1', 'sect163k1', 'sect163r2', 'sect193r1', 'sect193r2', 'sect233k1', 'sect233r1', 'sect239k1', 'sect283k1', 'sect283r1', 'sect409k1', 'sect409r1', 'sect571k1', 'sect571r1'` |
| リモートアクセスアカウントの有効期限 | このリリース以降、`techsupport > sshaccess` コマンドを使用して作成されたリモートアクセスアカウントは、7 日間アクティブのままになります。その後は、リモートアクセスを再度有効にする必要があります。<br>リモートアクセス用のランダムシード文字列を入力するオプションは、Web インターフェイスおよび CLI で削除されました。 |

# アップグレードの方法



## リリース 15.0.0-104 へのアップグレード（一般導入）

次のバージョンからリリース 15.0.0-104 にアップグレードできます。

- 13.0.5-007
- 13.5.4-038
- 14.0.0-698
- 14.0.1-033
- 14.0.2-020
- 14.2.0-616
- 14.2.0-620
- 14.2.1-015

- 14.2.1-020
- 14.2.2-004
- 14.3.0-023
- 14.3.0-032

## リリース 15.0.0-097 へのアップグレード（限定導入）

次のバージョンからリリース 15.0.0-097 にアップグレードできます。

- 13.0.5-007
- 13.5.4-038
- 14.0.0-698
- 14.0.1-033
- 14.0.2-020
- 14.2.0-616
- 14.2.0-620
- 14.2.1-015
- 14.2.1-020
- 14.2.2-004
- 14.3.0-023
- 14.3.0-032
- 15.0.0-012
- 15.0.0-048
- 15.0.0-068
- 15.0.0-085

## リリース 15.0.0-068 へのアップグレード（限定導入）

次のバージョンからリリース 15.0.0-068 にアップグレードできます。

- 13.0.5-007
- 13.5.4-038
- 14.0.0-698
- 14.0.1-033
- 14.0.2-020
- 14.2.0-616
- 14.2.0-620
- 14.2.1-015
- 14.2.1-020
- 14.2.2-004

- 14.3.0-023
- 14.3.0-032
- 15.0.0-012
- 15.0.0-048

# 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 (18 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 (29 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。



## AsynOS 15.0.0-xxx から AsynOS 15.0.0-104 GD への電子メールゲートウェイのアップグレード

電子メールゲートウェイを AsynOS 15.0.0-xxx から AsynOS 15.0.0-104 GD リリースにアップグレードするとき、「Vault エラー（Vault error）」を示すアラートを受信した場合は、Cisco TAC にお問い合わせください。

これは既知の問題です。不具合 ID：CSCwh15269。

## 暗号化通知テンプレートの削除

電子メールゲートウェイを AsyncOS 15.0.x にアップグレードすると、アップグレード中に「サポートされていない形式」が含まれていることが検出された既存の暗号化通知テンプレート（HTML またはテキスト形式）は自動的に削除されます。

## ファイル レピュテーション サービスのアクティブ化の前提条件 - Cisco Secure Endpoint プライベートクラウド

このリリースにアップグレードする前に、ファイル レピュテーション サービスのアクティブ化に関する次の前提条件を満たしていることを確認してください。

- Cisco Secure Endpoint プライベートクラウドを 3.8.1 以上のバージョンにアップグレードした
- アップグレードプロセス中にプロンプトが表示されたとき、Cisco Secure Endpoint の「コンソールのホスト名」と「アクティベーションコード」の詳細を入力した。

## 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 15.0 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 15.0 リリースは 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）。

## 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 C380 または C680 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、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、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（既知および修正済みの問題（28 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（17 ページ）を確認します。
- 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（18 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(27 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

## 次期 AsyncOS リリースにおけるシスコ スマート ソフトウェア ライセンシングの必須使用

Cisco Secure Email Gateway の次の AsyncOS リリース（AsyncOS 15.0 リリース以降のすべてのリリース）から、シスコ スマート ソフトウェア ライセンシングを使用する必要があります。

（注） 次の AsyncOS リリースから、クラシックライセンスは**サポートされなくなります**。クラシックライセンスモードでは、新しい機能ライセンスを注文したり、既存の機能ライセンスを更新したりすることはできなくなります。

**前提条件**：Cisco Smart Software Manager ポータルでスマートアカウントを作成し、電子メールゲートウェイでシスコ スマート ソフトウェア ライセンシングを有効にしてください。詳細については、ユーザーガイドの「System Administration」の章にある「Smart Software Licensing」の項を参照してください。

**結果**：シスコ スマート ソフトウェア ライセンシングを有効にすると、電子メールゲートウェイを AsyncOS 15.0 から次期 AsyncOS リリースにシームレスにアップグレードし、スマートライセンスモードで既存の機能ライセンスを引き続き使用できます。

## Cisco Secure Endpoint プライベートクラウドのファイル レピュテーション サービスのアクティブ化

ファイル レピュテーション サービスをアクティブにするには、システムセットアップに基づいて次のいずれかの手順に従います。

- [**クラスタモード**]：新しいファイル レピュテーション サービスがすでに設定されている電子メールゲートウェイに接続します。
- [**スタンドアロンモード**]：次の手順を実行します。

  1. Web インターフェイスで、[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）] ページに移動します。

  2. [グローバル設定を編集（Edit Global Settings）] ボタンをクリックします。

  3. [ファイルレピュテーションの詳細設定（Advanced Settings for File Reputation）] パネルをクリックします。

  4. [ファイルレピュテーションサーバー（File Reputation Server）] ドロップダウンリストから [プライベートレピュテーションクラウド（Private reputation cloud）] オプションを選択します。

  5. 所定のフィールドにコンソールのホスト名とアクティベーションコードを入力します。

  6. [送信（Submit）] をクリックし、変更をコミットします。

## DLP サービスステータスチェック

このリリースにアップグレードした後、DLP サービスで問題が発生する可能性があります。

ソリューション：CLI で `diagnostic` > `services` > `DLP` > `status` サブコマンドを使用して、電子メールゲートウェイの DLP サービスのステータスを確認します。DLP サービスが実行されていない場合は、既知の問題リストにある CSCvy08110 の不具合の「回避策」セクションを参照してください。既知の問題を表示する方法の詳細については、既知および修正済みの問題のリスト（28 ページ）を参照してください。

## 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。

## 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 15.0 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(28 ページ)
- 既知および修正済みの問題のリスト(28 ページ)
- 関連資料(29 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

| | |
|---|---|
| 既知の問題 | https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=afr&svr=3nH&rls=15.0.0&prdNam=Cisco%20IronPort%20Email%20Security%20Appliance%20Software |
| 修正済みの問題 | https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&prdNam=Cisco%20IronPort%20Email%20Security%20Appliance%20Software&kw=*&bt=custV&sb=fr&svr=3nH&rls=15.0.0-104 |

## 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** [リリース(release)] フィールドに、リリースのバージョン(たとえば、15.0)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<br>(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。