



# AsyncOS 15.5.1 for Cisco Secure Email Cloud Gateway リリースノート (一般導入)

---


発行日: 2024 年 4 月 30 日


## 目次

- [今回のリリースでの変更点 \(2 ページ\)](#)
- [動作における変更 \(9 ページ\)](#)
- [アップグレードパス \(10 ページ\)](#)
- [このリリースでサポートされる VM \(10 ページ\)](#)
- [アップグレード前の注意事項 \(10 ページ\)](#)
- [アップグレード後の注意事項 \(13 ページ\)](#)
- [パフォーマンスアドバイザリ \(15 ページ\)](#)
- [既知および修正済みの問題 \(16 ページ\)](#)
- [ソフトウェア ライフサイクル サポート ステートメント \(17 ページ\)](#)
- [関連資料 \(17 ページ\)](#)
- [サービスとサポート \(17 ページ\)](#)



## 今回のリリースでの変更点

機能	説明
Vault サービスのモニタリングとアラートの送信	<p>電子メールゲートウェイは、初期化されているかどうかにかかわらず、Vault サービスをモニターし、そのステータスを追跡するようになりました。また、適切なアラートメッセージを送信し、ステータス情報を <code>error_logs</code> に記録します。</p> <p>アラートログには、次のいずれかの方法でアクセスできます。</p> <ul style="list-style-type: none"> <li>• Web インターフェイスで [システム管理 (System Administration)] &gt; [アラート (Alerts)] ページに移動し、[上位アラートの表示 (View Top Alerts)] ボタンをクリックします。</li> <li>• CLI で <code>displayalerts</code> コマンドを使用します。</li> </ul> <p>何らかの問題によって Vault サービスの初期化に失敗した場合は、Vault サービスがダウンしていることを示すアラートメッセージを (メール、Web インターフェイス、および CLI で) 受信します。Vault サービスを復元するには、Vault Recovery プロセスを実行する必要があります。</p> <hr/> <p> (注) AsyncOS 15.5.1 へのアップグレード中にアップグレードが失敗した場合は、<code>upgrade_logs</code> で Vault サービスエラーを確認する必要があります。Vault サービスエラーがあった場合は、Vault サービスを復元するか、設定を保存せずにアップグレードプロセスを続行する必要があります。</p> <hr/> <p>アラートメッセージは次のようなシナリオで受信します。</p> <ul style="list-style-type: none"> <li>• AsyncOS 15.5.1 へのアップグレード後に Vault サービスの初期化に失敗した場合、メール、Web インターフェイス、および CLI でアラートメッセージを受信します。</li> <li>• 電子メールゲートウェイのいずれかのサービスが初期化に失敗した Vault サービスを使用している場合、メール、Web インターフェイス、および CLI でアラートメッセージを受信します。送信されるアラートメッセージは、暗号化ステータスによって異なります。暗号化ステータスは、<code>fipsconfig &gt; encryptedconfig</code> サブコマンドを使用して確認できます。</li> </ul> <p>Vault モニタリングメカニズムは、75 分ごとに Vault サービスをチェックします。ダウンしている場合は、Vault サービスが復元されるまでアラートメッセージを送信します。</p> <p>成功した Vault 正常性チェックと初期化ログエントリの例については、『<i>User Guide for AsyncOS 15.5.1 for Secure Email Cloud Gateway</i>』の「Logging」の章にある「Successful Vault Health Check and Initialization」セクションを参照してください。</p>

	<p>Vault サービスを復元するには、Vault Recovery プロセスを実行する必要があります。</p> <p> <b>注意</b> 暗号化(CLI&gt; fipsconfig&gt; encryptconfig)が有効になっている場合は、データの損失を防ぐため、電子メールゲートウェイの設定のコピーを常に保存し、維持してください。</p> <p>電子メールゲートウェイの設定を保存する方法の詳細については、<a href="#">電子メールゲートウェイの設定の保存(10 ページ)</a>を参照してください。</p> <p>Vault Recovery プロセスの実行方法については、<a href="#">Vault の問題を解決するための Vault Recovery プロセスの実行(11 ページ)</a>を参照してください。</p>
<p>メッセージ終了 RFC 標準規格に違反しているメッセージの識別</p>	<p>電子メールゲートウェイは、メッセージ終了 RFC 標準規格(つまり &lt;CRLF.CRLF&gt;)に違反しているメッセージを識別してフィルタ処理し、脅威を検出するようになりました。</p> <p>電子メールゲートウェイは、無効なメッセージ終了シーケンスを含むメッセージを受信すると、メッセージ終了 RFC 標準規格に準拠するメッセージを受信するまで、その接続内のすべてのメッセージ ID (MID) に <b>X-Ironport-Invalid-End-Of-Message</b> 拡張ヘッダー (X-Header) を追加します。</p> <p>コンテンツフィルタでポリシーを設定し、これらのメッセージに対して必要なアクションを実行できます。</p> <p>CR および LF 処理フィールドの設定の詳細については、『<i>User Guide for AsyncOS 15.5.1 for Secure Email Gateway</i>』の「Listening for Connection Requests by Creation a Listener Using Web Interface」セクションを参照してください。</p>
<p>CLI による API サーバーの再起動</p>	<p>新しい CLI サブコマンド <code>API_SERVER</code> を使用して API サーバーを再起動できるようになりました。<code>API_SERVER</code> サブコマンドを使用して、API サーバーを再起動しステータスを表示できます。<code>API_SERVER</code> サブコマンドは、<code>diagnostic &gt; SERVICES</code> サブコマンドの下に追加されています。</p> <p><code>diagnostic</code> コマンドとそのサブコマンドの詳細については、『<i>CLI Reference Guide for AsyncOS 15.5.1 for Cisco Secure Email Gateway</i>』の「The Commands: Reference Example」の章の「diagnostic」セクションを参照してください。</p>

脅威検出のための脅威  
スキャナの設定

AsynOS 15.0 リリースでは、着信メッセージの脅威を検出するために脅威スキャナ機能が導入されました。そのリリースでは、脅威スキャナを直接設定して脅威を検出することはできず、設定はバックエンドで行われていました。

このリリース以降、電子メールゲートウェイで着信した脅威を検出するように脅威スキャナを設定できます。脅威スキャナは受信メールポリシーごとに有効または無効にできます。脅威スキャナを有効にすると、着信メッセージがスキャンされ、スパム対策の判定に影響します。

**前提条件:** 脅威スキャナを有効にするには、**グレイメールのグローバル設定**を有効にする必要があります。

脅威スキャナは、次の方法でポリシーごとに設定できます。


- **Web インターフェイス:** [メールポリシー (Mail Policies)] > [受信メールポリシー (Incoming Mail Policies)] の順に選択し、メールポリシーの [スパム対策 (Anti-Spam)] 列の下にあるリンクをクリックして、[メールポリシー: スパム対策 (Mail Policies: Anti-Spam)] ページを開きます。[脅威スキャナの有効化 (Enable Threat Scanner)] チェックボックスをオンまたはオフにすることができます。
- **CLI:** `policyconfig` コマンドを使用します。



#### インストールとアップグレードのシナリオ

電子メールゲートウェイをインストールするか、AsynOS 15.0 以前のバージョンから AsynOS 15.5.1 リリースにアップグレードすると、脅威スキャナはデフォルトで無効になります。




詳細については、『*User Guide for AsynOS 15.5.1 for Secure Email Gateway*』の「Managing Spam and Graymail」の章にある「Defining Anti-Spam Policies」セクションを参照してください。

CLI を使用した脅威スキャナの設定の詳細については、『*CLI Reference Guide for AsynOS 15.5.1 for Cisco Secure Email Gateway*』の「The Commands: Reference Examples」の章にある「Configuring Threat Scanner Per Policy」セクションを参照してください。

<p>SDR サービスの有効性を向上させるための追加属性の追加</p>	<p>送信者ドメインのレピュテーション (SDR) サービスの有効性を向上させるため、電子メールゲートウェイには、レピュテーション分析のために Cisco TAC に送信されるテレメトリデータの一部として、デフォルトで追加属性 (名前と完全な電子メールアドレス: ユーザー名とドメインを表示) が含まれるようになりました。</p> <p>管理者が電子メールゲートウェイにログインすると、テレメトリデータに個人データの処理を含めるために、SDR の [追加属性を含める (Include Additional Attributes)] オプションがデフォルトで有効になっていることを通知する警告メッセージが表示されます。</p>  <p><b>(注)</b> [追加属性を含める (Include Additional Attributes)] オプションは、送信者ドメインレピュテーションのフィルタ処理を有効にした場合にのみデフォルトで有効になります。</p> <p>[追加属性を含める (Include Additional Attributes)] オプションを無効にする場合は、次の手順を実行します。</p> <ol style="list-style-type: none"> <li>1. [セキュリティサービス (Security Services)] &gt; [ドメインレピュテーション (Domain Reputation)] に移動します。</li> <li>2. [グローバル設定を編集 (Edit Global Settings)] をクリックし、[追加属性を含める (Include Additional Attributes)] チェックボックスをオフにします。</li> </ol> <p>詳細については、『<i>User Guide for AsyncOS 15.5.1 for Secure Email Cloud Gateway</i>』の「Sender Domain Reputation Filtering」の章にある「Enabling Sender Domain Reputation Filtering on Email Gateway」セクションを参照してください。</p>
<p>個々の受信メールポリシーに Threat Defense Connector を設定します。</p>	<p>受信メールポリシーごとに Threat Defense Connector を設定できるようになりました。この機能を使用するには、Cisco Secure Email Gateway で Threat Defense Connector を設定して有効にしておく必要があります。</p> <p>[メールポリシー (Mail Policies)] &gt; [受信メールポリシー (Incoming Mail Policies)] に移動して、個々のメールポリシーに対して Threat Defense Connector を有効または無効にします。</p> <p>詳細については、『<i>User Guide for AsyncOS 15.5.1 for Cisco Secure Email Cloud Gateway</i>』の「Integrating Secure Email Gateway with Threat Defense」の章を参照してください。</p>


<p>DKIM 検証での大きなキーサイズ値のサポート</p>	<p>電子メールゲートウェイの DKIM 検証には、次の大きなキーサイズ値を使用できます。</p> <ul style="list-style-type: none"> <li>• 3072 キービットサイズ</li> <li>• 4096 キービットサイズ</li> </ul> <p>次の方法で、DKIM 検証に新しい大きなキーサイズ値を選択できます。</p> <ul style="list-style-type: none"> <li>• <b>Web インターフェイス:</b> [メールポリシー (Mail Policies)] &gt; [検証プロファイル (Verification Profiles)] &gt; [プロファイルの追加 (Add Profile)] または [デフォルト (Default)] に移動し、[許容最小キー: (Smallest Key to be Accepted:)] または [許容最大キー: (Largest Key to be Accepted:)] ドロップダウン リスト フィールドから <b>3072</b> または <b>4096</b> を選択します。</li> <li>• <b>CLI:</b> domainkeysconfig &gt; keys &gt; new または edit &gt; Enter the smallest key to be accepted または Enter the largest key to be accepted オプションを使用し、特定の DKIM 検証プロファイルに 3072 または 4096 に対応する必要な値を入力します。</li> </ul>
<p>新しい DKIM 検証プロファイルでの 512 および 768 キーサイズ値の非サポート</p>	<p>このリリース以降、新しい DKIM 検証プロファイルを作成する際、512 および 768 のキービットサイズ値はサポートされなくなりました。</p> <p></p> <p><b>(注)</b> 512 および 768 のキーサイズ値で作成された既存の DKIM 検証プロファイルは、このリリースへのアップグレードでも引き続きサポートされます。</p>
<p>SSL サービスの TLS 1.3 のサポート</p>	<p>電子メールゲートウェイで次の TLS サービスに対して TLS 1.3 を設定できるようになりました。</p> <ul style="list-style-type: none"> <li>• GUI HTTPS</li> <li>• インバウンド SMTP</li> <li>• アウトバウンド SMTP</li> </ul> <p>「GUI HTTPS」、「インバウンド SMTP」、および「アウトバウンド SMTP」の TLS サービスに TLS 1.3 を設定する場合、電子メールゲートウェイは次の TLS 暗号のみをサポートします。</p> <ul style="list-style-type: none"> <li>• TLS_AES_128_GCM_SHA256</li> <li>• TLS_AES_256_GCM_SHA384</li> <li>• TLS_CHACHA20_POLY1305_SHA256</li> </ul> <p></p> <p><b>(注)</b> 電子メールゲートウェイでは、TLS 1.3 に使用される暗号を変更できません。</p> <p>TLS 1.3 を設定すると、電子メールゲートウェイと API サービスのレガシーまたは新しい Web インターフェイス全体で TLS 通信に使用できます。</p>

<p>AsyncOS API を使用したファイルハッシュリスト、RAT、SMTP ルート、保存と読み込みの設定、アドレス一覧、および受信メールポリシーユーザー情報の取得</p>	<p>AsyncOS API を使用して、電子メールゲートウェイのファイルハッシュリスト、受信者アクセステーブル (RAT) エントリ、SMTP ルート、保存と読み込みの設定、アドレス一覧、および受信メールポリシーユーザーに関する情報を取得できるようになりました。</p> <p>詳細については、『<i>AsyncOS 15.5.1 API for Cisco Secure Email Cloud Gateway - Getting Started Guide</i>』の「Configuration APIs」セクションを参照してください。</p>
<p>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</p>	<p>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の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。</p> <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> </ul> <p>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、フランス語、日本語、および韓国語がサポートされています。</p> <p>詳細については、『<i>User Guide for AsyncOS 15.5.1 for Secure Email Cloud Gateway</i>』の「Using Message Filters to Enforce Email Policies」を参照してください。</p>
<p>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</p>	<p>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。</p> <p>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。</p> <p>[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。</p>

<p>異なるクラスタのマシン間で設定変更を同時に同期する</p>	<p>あるクラスタのログインマシンに加えられた設定変更を、リモートクラスタのすべてのマシンに同時に同期できます。同期プロセスは、両方のクラスタが同じ領域の同じ、または異なるデータセンターにある場合にのみ発生します。</p> <p> (注) 設定の変更は、グループまたはマシンレベルではなく、クラスタレベルでのみマシン間で同期できます。</p> <p> (注) クラスタ間でスパムの隔離の IP 設定が同期されないようにするには、マシンをグループレベルに移動する必要があります。</p> <p>この機能を有効にするには、シスコのアカウントマネージャに連絡してください。</p> <p><b>前提条件:</b>シスコのアカウントマネージャにこの機能を有効にするよう依頼する前に、クラスタ全体のすべてのマシンで設定が同じであることを確認してください。</p> <p>同期プロセスが完了した後、1 つのマシンで設定を変更すると、同じ設定がクラスタ全体のすべてのマシンに自動的に複製されます。同じであることは、[システムログ (System Logs)] で確認できます。詳細については、『<i>User Guide for AsyncOS 15.5.1 for Secure Email Cloud Gateway</i>』の「Logging」の章を参照してください。</p> <p> (注) クラスタ間接続プロセスが完了した後、クラスタ名を変更してはなりません。クラスタには一意の名前を付けてください。</p>
<p>URL レトロスペクティブサービスのリージョンベースのポーリング</p>	<p>Cisco Secure Email Gateway が判定の更新のために接続する URL レトロスペクティブサービスのリージョンを設定できます。Cisco Secure Email Gateway ESA は、レトロスペクティブサービスのリージョンおよび関連するエンドポイントの URL を更新できます。</p> <p>詳細については、『<i>User Guide for AsyncOS 15.5.1 for Secure Email Cloud Gateway</i>』の「Setting Up URL Filtering」セクションを参照してください。</p>



## 動作における変更

アプリケーション SSH クライアントアルゴリズムのサポート	<p>クラスタに電子メールゲートウェイを追加すると、次のアプリケーション SSH クライアントアルゴリズムがサポートされます。</p> <p><b>[非 FIPS モード]</b></p> <p>既存のアルゴリズムに加え、次の暗号アルゴリズム、MAC メソッド、および KEX アルゴリズムがデフォルトで Cisco Secure Email and Web Manager に追加されます。</p> <ul style="list-style-type: none"> <li>• 暗号アルゴリズム: aes128-ctr</li> <li>• MAC メソッド: hmac-sha2-256</li> <li>• KEX アルゴリズム: diffie-hellman-group14-sha256</li> </ul> <p><b>[FIPS モード]</b></p> <p>既存のアルゴリズムに加えて、次の暗号アルゴリズムと MAC メソッドがデフォルトで Cisco Secure Email and Web Manager に追加されます。</p> <ul style="list-style-type: none"> <li>• 暗号アルゴリズム: aes128-ctr</li> <li>• MAC メソッド: hmac-sha2-256</li> </ul>
Cisco Advanced Malware Protection エンジンによるアーカイブまたは圧縮ファイルの処理	<p>このリリース以降、1 つ以上の構成ファイルがファイル分析の対象となる場合、Cisco Secure Email Gateway はアーカイブファイル全体を Cisco Secure Malware Analytics に送信します。構成ファイルに悪意のあるものが見つかった場合、アーカイブファイル全体がマルウェアとしてマークされます。</p> <p>Cisco Secure Email Gateway が圧縮ファイルまたはアーカイブファイルの抽出に失敗した場合、ファイルは分析のために Cisco Secure Malware Analytics にアップロードされます。</p>
FIPS モードでの aes192-cbc 暗号の非サポート	<p>このリリース以降、aes192-cbc 暗号は、FIPS モードの SSH サーバーと SSH クライアントの両方でサポートされなくなります。AsynOS 15.5.1 で FIPS モードを有効にする場合は、CLI で <code>sshconfig -&gt; SSHD</code> サブコマンドを使用して aes192-cbc 暗号を削除する必要があります。</p> <p> <b>(注)</b> 電子メールゲートウェイが FIPS モードで、AsynOS 15.5.1 リリースにアップグレードされている場合、aes192-cbc 暗号はデフォルトで削除されます。</p>

## アップグレードパス

次のバージョンから、リリース 15.5.1-055 にアップグレードできます。

• 15.5.1-001	• 15.5.0-048	• 15.0.1-105
• 15.0.1-030	• 15.0.0-104	• 15.0.0-097
• 14.3.0-209	• 14.3.0-032	• 14.3.0-020
• 14.2.3-102	• 14.2.3-031	• 14.2.3-027
• 14.2.2-004	• 14.2.1-020	• 14.2.0-620

## このリリースでサポートされる VM

このリリースでは、次の VM がサポートされています。

- C100V
- C300V
- C600V

## 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の設定の保存 \(10 ページ\)](#)
- [Vault の問題を解決するための Vault Recovery プロセスの実行 \(11 ページ\)](#)
- [ディスク容量の不足によるシステムアップグレードのブロック \(12 ページ\)](#)
- [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 \(13 ページ\)](#)

## 電子メールゲートウェイの設定の保存

電子メールゲートウェイで暗号化が有効になっている場合は、AsyncOS 15.5.1 にアップグレードする前または後に、電子メールゲートウェイの設定のコピーを保存することをお勧めします。

Vault Recovery プロセスを実行して Vault サービスを復元した後、保存した電子メールゲートウェイの設定をロードして、デバイスの以前の設定を復元できます。

次の方法を使用してデバイスの設定を保存できます。

- [システム管理 (System Administration)] > [設定ファイル (Configuration File)] に移動し、[コンフィギュレーション ファイルでパズフレーズを暗号化する (Encrypt passphrases in the Configuration Files)] を選択します。
- CLI で `saveconfig` コマンドを使用し、**2** をタイプして [パズフレーズを暗号化する (Encrypt passphrases)] オプションを選択します。

## Vault の問題を解決するための Vault Recovery プロセスの実行

AsyncOS 15.5.1 にアップグレードする前または後に、(ハードウェア、オンプレミス、CES、AWS、KVM、Azure、または Hyper-V の) 電子メールゲートウェイで Vault 関連の問題が発生した場合は、その問題を解決するために Vault Recovery プロセスを実行する必要があります。次の手順を使用して Vault Recovery を実行します。

1. 次のログイン情報を使用して、直接 SSH 接続を介して電子メールゲートウェイにログインします。  
 ユーザー名: **enablediag**  
 パスワード: **管理者ユーザーのパスワード**
2. `recovervault` コマンドを実行します。
3. プロンプトが表示されたら、次の一連のサブコマンドを入力します。
  - a. `yes`
  - b. `1 (encryption enabled) or 2 (encryption disabled)`
4. 管理者ユーザーのログイン情報を使用して電子メールゲートウェイにログインし、Vault Recovery プロセスが完了したらデバイスを再起動します。
5. (クラスタセットアップの場合のみ) Vault が回復し、デバイスの再起動が完了したら、電子メールゲートウェイをクラスタに再参加させます。
6. (暗号化が有効になっている場合のみ) 以前に保存したデバイスの設定のコピーをロードして、以前の設定を復元します。
7. Vault サービスのアラートがないか、電子メールゲートウェイを数時間モニターします。

電子メールゲートウェイが回復し、Vault が再初期化されます。これで、問題なくデバイスに接続できます。



(注)

### 暗号化無効

このシナリオでは、すべてのシステム設定が保持されます。

### 暗号化有効

このシナリオでは、次の暗号化された変数がデフォルトの工場出荷時の値にリセットされます。

- 証明書の秘密キー
- RADIUS パスワード
- LDAP バインドのパスワード
- ローカル ユーザのパスワードのハッシュ
- SNMP パスワード
- DK/DKIM 署名キー
- 発信 SMTP 認証パスワード
- PostX 暗号化キー
- PostX 暗号化プロキシ パスワード
- FTP プッシュ ログ サブスクリプションのパスワード
- IPMI LAN パスワード

- アップデータ サーバの URL
- 認証 API のクライアントログイン情報
- Cisco Advanced Malware Protection プロキシパスワード
- SAML 証明書のパスフレーズ

以前の設定を復元する場合は、以前に保存した設定ファイルをロードする必要があります。



(注)

認証 API のクライアントログイン情報は構成ファイルに保存されないため、API を呼び出して新しいクライアントログイン情報を作成する必要があります。

#### ログ (enablediag ユーザーの場合):

Available Commands:

help -- View this text.

quit -- Log out.

service -- Enable or disable access to the service system.

network -- Perform emergency configuration of the diagnostic network interface.

clearnet -- Resets configuration of the diagnostic network interface.

ssh -- Configure emergency SSH daemon on the diagnostic network interface.

clearssh -- Stop emergency SSH daemon on the diagnostic network interface.

tunnel -- Start up tech support tunnel to IronPort.

print -- Print status of the diagnostic network interface.

recovervault -- Recover vault, it will only restore the encrypted variables to factory values, will not touch anything related to configurations if encryption is disabled .

resetappliance -- Reset appliance reverts the appliance to chosen build with factory default settings with default IP. No network configuration would be preserved.

reboot -- Reboot the appliance.

S/N 42189A47B0D50A645948-CEC55115B364

Service Access currently ENABLED (0 current service logins)

esa1.hc303-10.smtpi.com> recovervault

Are you sure you want to recover vault? [N]> y

Encryption is enabled [1]>

Encryption is not enabled [2]>

## ディスク容量の不足によるシステムアップグレードのブロック

マシンにディスク容量が 4GB 未満の次ルートパーティションがあるため、AsyncOS 15.0 バージョンへのシステムアップグレードはブロックされます。ディスク容量が 4 GB ある次ルートパーティションで新しい仮想アプライアンスを展開する必要があります。ディスク容量が 4 GB ある次ルートパーティションで新しい仮想アプライアンスを展開する方法の詳細については、<https://www.cisco.com/c/en/us/support/docs/field-notices/722/fn72230.html> の Field Notice (FN) 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。

## アップグレード後の注意事項

- [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 \(13 ページ\)](#)
- [DLP サービスステータスチェック \(14 ページ\)](#)
- [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 \(14 ページ\)](#)
- [\(スマートライセンスのユーザーのみ\) 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 \(14 ページ\)](#)
- [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 \(14 ページ\)](#)
- [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 \(15 ページ\)](#)

## 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\(16 ページ\)](#)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の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 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ー

### 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を組み合わせて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пам隔離

C シリーズのアプライアンスに対して IronPort スпам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、いっばいに近いときに IronPort スпам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 \(16 ページ\)](#)
- [既知および修正済みの問題のリスト \(16 ページ\)](#)
- [関連資料 \(17 ページ\)](#)

## 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	<a href="https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&amp;kw=*&amp;bt=custV&amp;sb=af&amp;r=3nH&amp;rls=15.5.0,15.5.1&amp;prdNam=Cisco%20Secure%20Email%20Gateway">https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&amp;kw=*&amp;bt=custV&amp;sb=af&amp;r=3nH&amp;rls=15.5.0,15.5.1&amp;prdNam=Cisco%20Secure%20Email%20Gateway</a>
修正済みの問題	<a href="https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&amp;kw=*&amp;bt=custV&amp;sb=fr&amp;svr=3nH&amp;rls=15.5.1-055&amp;prdNam=Cisco%20Secure%20Email%20Gateway">https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&amp;kw=*&amp;bt=custV&amp;sb=fr&amp;svr=3nH&amp;rls=15.5.1-055&amp;prdNam=Cisco%20Secure%20Email%20Gateway</a>

## 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)] > [電子メールセキュリティ (Email Security)] > [Cisco Secure Email Gateway] 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 (15.5.1-055 など) 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。

## ソフトウェアライフサイクルサポート ステートメント

ソフトウェアのタイムベースのリリースモデルおよびソフトウェアリリースのサポートタイムラインについては、「[Software Lifecycle Support Statement](#)」を参照してください。

### 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	<a href="http://www.cisco.com/c/ja_jp/support/security/content-security-management-appliance/tsd-products-support-series-home.html">http://www.cisco.com/c/ja_jp/support/security/content-security-management-appliance/tsd-products-support-series-home.html</a>
Cisco Secure Web Appliance	<a href="http://www.cisco.com/c/ja_jp/support/security/web-security-appliance/tsd-products-support-series-home.html">http://www.cisco.com/c/ja_jp/support/security/web-security-appliance/tsd-products-support-series-home.html</a>
Cisco Secure Email ゲートウェイ	<a href="http://www.cisco.com/c/ja_jp/support/security/email-security-appliance/tsd-products-support-series-home.html">http://www.cisco.com/c/ja_jp/support/security/email-security-appliance/tsd-products-support-series-home.html</a>
Cisco Secure Email クラウドゲートウェイ	<a href="https://www.cisco.com/c/en/us/support/security/cloud-email-security/products-user-guide-list.html">https://www.cisco.com/c/en/us/support/security/cloud-email-security/products-user-guide-list.html</a>
Cisco Secure Email Gateway CLI リファレンスガイド	<a href="http://www.cisco.com/c/ja_jp/support/security/email-security-appliance/products-command-reference-list.html">http://www.cisco.com/c/ja_jp/support/security/email-security-appliance/products-command-reference-list.html</a>
Cisco Secure Email Encryption Service	<a href="http://www.cisco.com/c/ja_jp/support/security/email-encryption/tsd-products-support-series-home.html">http://www.cisco.com/c/ja_jp/support/security/email-encryption/tsd-products-support-series-home.html</a>

### 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: [https://www.cisco.com/c/ja\\_jp/support/web/tsd-cisco-worldwide-contacts.html](https://www.cisco.com/c/ja_jp/support/web/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、ユーザーガイドまたはオンラインヘルプを参照してください。

---

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。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2024 Cisco Systems, Inc. All rights reserved.