

# AsyncOS 12.5.x for Cisco Content Security Management Appliances リリースノート

---

発行日: 2019 年 7 月 22 日


改訂日: 2020 年 10 月 8 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 \(3 ページ\)](#)
- [新しい Web インターフェイスとレガシー Web インターフェイスでの Web インターフェイスの比較 \(4 ページ\)](#)
- [アップグレード パス \(9 ページ\)](#)
- [E メールセキュリティおよび Web セキュリティのリリースとの互換性 \(12 ページ\)](#)
- [インストールおよびアップグレードに関する注意事項 \(12 ページ\)](#)
- [このリリースでサポートされているハードウェア \(15 ページ\)](#)
- [既知および修正済みの問題 \(16 ページ\)](#)
- [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
新しいハードウェアモデルのサポート	<p>シスコのコンテンツセキュリティ管理アプライアンス向け AsyncOS 12.5.0 リリースでは、x80 シリーズと x90 シリーズの他に、次のハードウェアモデルをサポートするようになりました。</p> <ul style="list-style-type: none"> <li>• M195</li> <li>• M395</li> <li>• M695</li> </ul> <p>詳細については、<a href="https://www.cisco.com/c/ja_jp/products/collateral/security/content-security-management-appliance/datasheet_C78-721194.html">https://www.cisco.com/c/ja_jp/products/collateral/security/content-security-management-appliance/datasheet_C78-721194.html</a> を参照してください。</p>
設定マスターの複数のサブセットの管理	<p>特定のバージョンの設定マスターのサブセットを設定して、Web セキュリティアプライアンスのさまざまなポリシー設定を一元的に管理できるようになりました。</p> <p>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 Web Security Appliances」の章を参照してください。</p>
ケースブックを使用した脅威分析の実行	<p>Cisco コンテンツセキュリティ管理アプライアンスに、ケースブックとピボットメニューのウィジェットが追加されました。</p> <p> (注) Microsoft Internet Explorer ブラウザを使用してアプライアンスにアクセスしている場合、[ケースブック (Casebook)] ウィジェットを使用することはできません。</p> <hr/> <p>[ケースブック (Casebook)] ウィジェットと [ピボットメニュー (Pivot Menu)] ウィジェットを使用して、アプライアンスで次のアクションを実行できます。</p> <ul style="list-style-type: none"> <li>• 観測対象をケースブックに追加し、脅威分析の調査を実行します。</li> <li>• 新しいケース、既存のケース、または Cisco Threat Response ポータルに登録されているその他のデバイス (エンドポイント向け AMP、Cisco Umbrella、Cisco Talos Intelligence など) の監視対象をピボットし、脅威分析のために調査します。</li> </ul> <p>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 Threat Response Server」の章を参照してください。</p>
Cisco Threat Response ポータルでアプライアンスを登録するときに Cisco Threat Response サーバを選択する機能	<p>アプライアンスを Cisco Threat Response ポータルに登録するときに、Cisco Threat Response ポータルにアプライアンスを接続するための Cisco Threat Response サーバを選択できるようになりました。</p> <p>このリリースでサポートされている Cisco Threat Response サーバは次のとおりです。</p> <ul style="list-style-type: none"> <li>• 米国 (<a href="https://api-sse.cisco.com">api-sse.cisco.com</a>)</li> <li>• 欧州 (<a href="https://api.eu.sse.itd.cisco.com">api.eu.sse.itd.cisco.com</a>)</li> </ul> <p>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 Threat Response Server」の章を参照してください。</p>



機能	説明
新しい Web インターフェイスでのお気に入りのレポートの管理	<p>カスタムレポート ページを作成するには、アプライアンスの新しい Web インターフェイスにある既存のすべての電子メール セキュリティ レポートからチャート (グラフ) とテーブルを構成します。</p> <p>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「Working with Reports on the New Web Interface」の章を参照してください。</p>
新しい Web インターフェイスでのポリシー、ウイルス、およびアウトブレイク隔離の設定	<p>アプライアンスの新しい Web インターフェイスから、ポリシー、ウイルス、またはアウトブレイク隔離を設定できるようになりました。</p> <p>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「Centralized Policy, Virus, and Outbreak Quarantines」の章を参照してください。</p>
Swagger UI を使用した API の管理	<p>Swagger は、OpenAPI 仕様に基づいて構築された一連のオープンソースのツールです。</p> <p>Swagger UI を使用すると、Web インターフェイスでの AsyncOS API リソースの設計と管理が容易になります。</p> <p>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「Setup, Installation and Basic Configuration」の章を参照してください。</p>
機能の使用状況の統計情報を収集することによるユーザエクスペリエンスの向上	<p>Cisco コンテンツ セキュリティ管理アプライアンスで、アプライアンスの新しい Web インターフェイスで機能およびインターフェイスまたはその一方の使用状況の統計情報が収集されるようになりました。これにより、全体的なユーザエクスペリエンスを向上させることができます。収集されたすべてのデータは匿名化されます。この機能の選択を解除する場合は、Web インターフェイスで [管理アプライアンス (Management Appliance)] &gt; [システム管理 (System Administration)] &gt; [一般設定 (General Settings)] &gt; [使用状況分析 (Usage Analytics)] ページに移動して無効にします。</p> <p>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「Monitoring Web Usage Analytics」の項を参照してください。</p>
アプライアンスの Web インターフェイス使用状況の統計情報を収集することによるユーザエクスペリエンスの向上	<p>Cisco コンテンツ セキュリティ管理アプライアンスで、使用状況分析機能を使用して、アプライアンスの Web インターフェイス使用状況の統計情報を収集できるようになりました。この機能は、Web インターフェイスの使用状況データを収集して分析し、アプライアンスのユーザエクスペリエンスを向上させるための洞察を提供するために使用されます。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「Monitoring Web Usage Analytics」を参照してください。</p>

## 動作における変更

パスフレーズの生成における変更	このリリースにアップグレードした後は、アプライアンスでのシステムパスフレーズの生成を選択できません。
ポリシー、ウイルス、およびアウトブレイク隔離のメッセージ添付ファイルのダウンロード	<p>これより前のリリースでは、ポリシー、ウイルス、およびアウトブレイクの隔離エンジンによって検出され、隔離されたメッセージ添付ファイルは新しいブラウザ ウィンドウに表示されました。</p> <p>このリリースへのアップグレード後は、ポリシー、ウイルス、およびアウトブレイクの隔離エンジンによって検出され、隔離されたメッセージ添付ファイルはダウンロードできます。</p>

## 新しい Web インターフェイスとレガシー Web インターフェイスでの Web インターフェイスの比較

Web インターフェイス ページまたは要素	新しい Web インターフェイス	レガシー Web インターフェイス
ランディングページ	セキュリティ管理アプライアンスにログインすると、[メールフロー概要 (Mail Flow Summary)] ページが表示されます。	アプライアンスにログインすると、[システムステータス (System Status)] ページが表示されます。
製品ドロップダウン	[製品 (Product)] ドロップダウンで、E メール セキュリティ アプライアンスと Web セキュリティアプライアンスを切り替えることができます。	[電子メール (Email)] または [ウェブ (Web)] タブを使用して、E メール セキュリティアプライアンスと Web セキュリティアプライアンスを切り替えることができます。
レポートドロップダウン	[レポート (Reports)] ドロップダウンで、E メール セキュリティアプライアンスと Web セキュリティアプライアンスのレポートを表示できます。	[レポート (Reporting)] ドロップダウンメニューで、E メール セキュリティアプライアンスと Web セキュリティアプライアンスのレポートを表示できます。
管理アプライアンスタブ	セキュリティ管理アプライアンスで  をクリックして、[管理アプライアンス (Management Appliance)] タブにアクセスします。	レポート、メッセージトラッキング、隔離の有効化と設定、ネットワークアクセスの設定、およびシステムステータスの監視を実行できます。
マイレポートページ	[製品 (Product)] ドロップダウンから [メール (Email)] を選択し、[レポート (Reports)] ドロップダウンから [マイレポート (My Reports)] を選択します。	[マイレポート (My Reports)] ページは、[メール (Email)] > [レポート (Reporting)] > [マイレポート (My Reports)] から表示できます。
有効なレポートデータページ	セキュリティ管理アプライアンスで  をクリックして、[メール (Email)] > [レポート (Reporting)] > [有効なレポートデータ (Reporting Data Availability)] を選択し、[有効なレポートデータ (Reporting Data Availability)] ページにアクセスします。	データを表示、更新およびソートして、リソース使用率と電子メールトラフィックの問題点に対するリアルタイムの可視性を提供できます。

Web インターフェイス ページまたは要素	新しい Web インターフェイス	レガシー Web インターフェイス
レポートのスケジュール 設定とアーカイブ	<p>セキュリティ管理アプライアンスで  をクリックして、[メール (Email)] &gt; [レポート (Reporting)] &gt; [スケジュール設定されたレポート (Scheduled Reports)] を選択し、レポートをスケジュールします。</p> <p>セキュリティ管理アプライアンスで  をクリックして、[メール (Email)] &gt; [レポート (Reporting)] &gt; [アーカイブレポート (Archive Reports)] を選択し、レポートをアーカイブします。</p>	<p>セキュリティ管理アプライアンスで、[メール (Email)] &gt; [レポート (Reporting)] &gt; [スケジュールされたレポート (Scheduled Reports)] ページを使用してレポートをスケジュールすることができ、[メール (Email)] &gt; [レポート (Reporting)] &gt; [アーカイブレポート (Archived Report)] ページを使用してレポートをアーカイブすることができます。</p>
レポートの概要ページ	<p>セキュリティ管理アプライアンスの [メール レポートの概要 (Email Reporting Overview)] ページの新しい Web インターフェイスが、[メールフロー概要 (Mail Flow Summary)] ページとして設計し直されました。[メールフロー概要 (Mail Flow Summary)] レポートページには、受信および送信メッセージに関する傾向グラフや要約テーブルが表示されます。</p>	<p>セキュリティ管理アプライアンスの [メール レポートの概要 (Email Reporting Overview)] ページに、お使いの E メールセキュリティ アプライアンスからのメール メッセージアクティビティの概要が表示されます。[概要 (Overview)] ページには、グラフや、着信および発信メッセージの要約テーブルが表示されます。</p>
高度なマルウェア防御レ ポートページ	<p>[レポート (Reports)] メニューの [高度なマルウェア防御 (Advanced Malware Protection)] レポートページでは、次のセクションを使用できます。</p> <ul style="list-style-type: none"> <li>• [概要 (Overview)]</li> <li>• [AMP ファイル レピュテーション (AMP File Reputation)]</li> <li>• [ファイル分析 (File Analysis)]</li> <li>• [ファイル レトロスペクション (File Retrospection)]</li> <li>• [メールボックスの自動修復 (Mailbox Auto Remediation)]</li> </ul>	<p>セキュリティ管理アプライアンスの [メール (Email)] &gt; [レポート (Reporting)] ドロップダウンメニューには次の [高度なマルウェア防御 (Advanced Malware Protection)] レポートページがあります。</p> <ul style="list-style-type: none"> <li>• [高度なマルウェア防御 (Advanced Malware Protection)]</li> <li>• [AMP ファイル分析 (AMP File Analysis)]</li> <li>• [AMP 判定のアップデート (AMP Verdict Updates)]</li> <li>• [メールボックスの自動修復 (Mailbox Auto Remediation)]</li> </ul>

Web インターフェイス ページまたは要素	新しい Web インターフェイス	レガシー Web インターフェイス
アウトブレイク フィルタ ページ	新しい Web インターフェイスの [アウトブレイク フィルタリング (Outbreak Filtering)] レポート ページでは、[過去 1 年間のウイルスアウトブレイク (Past Year Virus Outbreaks)] および [過去 1 年間のウイルスアウトブレイクの概要 (Past Year Virus Outbreak Summary)] を使用できません。	[メール (Email)] > [レポート (Reporting)] > [アウトブレイク フィルタ (Outbreak Filters)] ページには、[過去 1 年間のウイルスアウトブレイク (Past Year Virus Outbreaks)] および [過去 1 年間のウイルスアウトブレイクの概要 (Past Year Virus Outbreak Summary)] が表示されます。
スパム隔離 (管理者およびエンドユーザ)	新しい Web インターフェイスで [隔離 (Quarantine)] > [スパム隔離 (Spam Quarantine)] > [検索 (Search)] をクリックして [スパム隔離 (Spam Quarantine)] ページにアクセスします。  新しい Web インターフェイスでのスパム隔離ポータルへのエンドユーザのアクセスの詳細については、 <a href="#">新しい Web インターフェイスへのアクセス (8 ページ)</a> を参照してください。	-
ポリシー、ウイルスおよびアウトブレイク隔離	新しい Web インターフェイスで [隔離 (Quarantine)] > [その他の隔離 (Other Quarantine)] をクリックします。  セキュリティ管理アプライアンス上でポリシー、ウイルス、およびアウトブレイク隔離のみを表示できます。	アプライアンスでは、ポリシー、ウイルス、およびアウトブレイク隔離を表示、設定、および変更できます。
隔離内のメッセージに対するすべてのアクションの選択	隔離で複数 (またはすべて) のメッセージを選択し、削除、遅延、リリース、移動などのメッセージアクションを実行できます。	隔離で複数のメッセージを選択して、メッセージアクションを実行することはできません。
添付ファイルの最大ダウンロード制限	隔離されたメッセージの添付ファイルのダウンロードの上限は 25 MB に制限されています。	-
拒否された接続	拒否された接続を検索するには、セキュリティ管理アプライアンスで、[トラッキング (Tracking)] > [検索 (Search)] > [拒否された接続 (Rejected Connection)] タブをクリックします。	-

Web インターフェイス ページまたは要素	新しい Web インターフェイス	レガシー Web インターフェイス
クエリ設定	セキュリティ管理アプライアンスでは、メッセージトラッキング機能の [クエリ設定 (Query Settings)] フィールドは使用できません。	メッセージトラッキング機能の [クエリ設定 (Query Settings)] フィールドで、クエリのタイムアウトを設定できます。
有効なメッセージトラッキング データ	セキュリティ管理アプライアンスで  をクリックして、[メール (Email)] > [メッセージトラッキング (Message Tracking)] > [有効なメッセージトラッキングデータ (Message Tracking Data Availability)] を選択し、[有効なメッセージトラッキングデータ (Message Tracking Data Availability)] ページにアクセスします。	アプライアンスの欠落データインターバルを表示することができます。
判定チャートと最後の状態の判定	判定チャートに、アプライアンス内の各エンジンによってトリガーされる可能性のあるさまざまな判定の情報が表示されます。  メッセージの最後の状態によって、エンジンのすべての可能な判定の後に、トリガーされる最終判定が決まります。	メッセージの判定チャートと最後の状態の判定は、使用できません。
メッセージの詳細におけるメッセージ添付ファイルとホスト名	メッセージの添付ファイルとホスト名は、セキュリティ管理アプライアンスのメッセージの [メッセージの詳細 (Message Details)] セクションに表示されません。	メッセージの添付ファイルとホスト名は、メッセージの [メッセージの詳細 (Message Details)] セクションに表示されます。
メッセージの詳細における送信者グループ、送信者 IP、SBRs スコア、およびポリシー一致	メッセージの送信者グループ、送信者 IP、SBRs スコア、およびポリシー一致の詳細は、セキュリティ管理アプライアンスでメッセージの [メッセージの詳細 (Message Details)] セクションに表示されます。	メッセージの送信者グループ、送信者 IP、SBRs スコア、およびポリシー一致の詳細は、メッセージの [メッセージの詳細 (Message Details)] セクションには表示されません。
メッセージの方向 (受信または送信)	メッセージの方向 (受信または送信) は、セキュリティ管理アプライアンスのメッセージトラッキング結果ページに表示されます。	メッセージの方向 (受信または送信) は、メッセージトラッキング結果ページに表示されません。

## 新しい Web インターフェイスへのアクセス

新しい Web インターフェイスでは、新しいレポートのモニタリング、隔離、およびメッセージの検索が可能です。



(注)

アプライアンスの新しい Web インターフェイスは、AsyncOS API HTTP/HTTPS ポート (6080/6443) および trailblazer HTTPS ポート (4431) を使用します。CLI で `trailblazerconfig` コマンドを使用して、trailblazer HTTPS ポートを設定できます。trailblazer HTTPS ポートがファイアウォールで開かれていることを確認します。

新しい Web インターフェイスには次のいずれかの方法でアクセスできます。

- `trailblazerconfig` CLI コマンドが有効になっている場合は、`https://example.com:<trailblazer-https-port>/ng-login` の URL を使用します。  
ここで、`example.com` はアプライアンスのホスト名で、`<trailblazer-https-port>` はアプライアンスで設定されている trailblazer の HTTPS ポートです。  
デフォルトで、`trailblazerconfig` はアプライアンスで有効になっています。
  - 設定した HTTPS ポートがファイアウォールで開かれていることを確認します。デフォルトの HTTPS ポートは 4431 です。
  - また、アプライアンスにアクセスするために指定したホスト名を DNS サーバが解決できることを確認します。
- `trailblazerconfig` CLI コマンドが無効になっている場合は、`https://example.com:<https-port>/ng-login` の URL を使用します。  
ここで、`example.com` はアプライアンスのホスト名で、`<https-port>` はアプライアンスで設定されている HTTPS ポートです。



(注)

`trailblazerconfig` CLI コマンドが無効になっている場合は、特定のブラウザの API ポートに複数の証明書を追加する必要がある場合があります。

- アプライアンスにログインし、**セキュリティ管理アプライアンスの外観が新しくなりました**ので、お試してください。新しい Web インターフェイスに移動します。

新しい Web インターフェイスは新しいブラウザウィンドウで開きます。それにアクセスするには、再度ログインする必要があります。アプライアンスから完全にログアウトする場合は、アプライアンスの新しい Web インターフェイスとレガシー Web インターフェイスの両方からログアウトする必要があります。

HTML ページのシームレスなナビゲーションとレンダリングのために、次のブラウザを使用してアプライアンスの新しい Web インターフェイス (AsyncOS 12.0 以降) にアクセスすることをお勧めします。

- Google Chrome (最新の安定バージョン)
- Mozilla Firefox (最新の安定バージョン)
- Safari (最新の安定バージョン)

サポートされているブラウザのいずれかで、アプライアンスのレガシー Web インターフェイスにアクセスできます。

アプライアンスの新しい Web インターフェイス (AsyncOS 12.0 以降) でサポートされている解像度は、1280 X 800 ~ 1680 X 1050 です。すべてのブラウザに対して最適に表示される解像度は 1440x900 です。





(注) シスコでは、より高い解像度でアプライアンスの新しい Web インターフェイスを表示することは推奨していません。

エンドユーザは、以下のいずれかの方法で、新しい Web インターフェイスのスパム検疫にアクセスできます。

- trailblazerconfig CLI コマンドが有効になっているときに、  
https://example.com:<trailblazer-https-port>/euq-login の URL を使用します。  
ここで、example.com はアプライアンスのホスト名で、<trailblazer-https-port> はアプライアンスで設定されている先駆者の HTTPS ポートです。
- trailblazerconfig CLI コマンドが無効になっているときに、  
https://example.com:<https-port>/euq-login の URL を使用します。  
ここで、example.com はアプライアンスのホスト名で、<https-port> はアプライアンスで設定されている HTTPS ポートです。



(注) HTTP/HTTPS ポートおよび AsyncOS API ポートがファイアウォールで開かれていることを確認します。

## アップグレードパス

- [リリース 12.5.0-683 へのアップグレード - MD\(メンテナンス導入\) \(9 ページ\)](#)
- [リリース 12.5.0-678 へのアップグレード - MD\(メンテナンス導入\) \(10 ページ\)](#)
- [リリース 12.5.0-670 へのアップグレード - MD\(メンテナンス導入\) \(10 ページ\)](#)
- [リリース 12.5.0-658 へのアップグレード - MD\(メンテナンス導入\) \(10 ページ\)](#)
- [リリース 12.5.0-655 へのアップグレード - MD\(メンテナンス導入\) \(11 ページ\)](#)
- [リリース 12.5.0-643 へのアップグレード - MD\(メンテナンス導入\) \(11 ページ\)](#)
- [リリース 12.5.0-636 へのアップグレード - MD\(メンテナンス導入\) \(11 ページ\)](#)
- [リリース 12.5.0-633 へのアップグレード - GD\(一般導入\) \(12 ページ\)](#)

## リリース 12.5.0-683 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 12.5.0-683 にアップグレードすることができます。

- 12-5-0-678
- 12-0-0-478
- 11-5-1-121
- 12-0-2-007
- 11-5-0-110
- 12-0-1-017
- 11-0-1-161
- 11-0-0-136

## リリース 12.5.0-678 へのアップグレード - MD(メンテナンス導入)

リリース 12.5.0-678 へは、次のバージョンからアップグレードできます。

- 12.5.0-674
- 12.5.0-670
- 12.5.0-658
- 12.5.0-655
- 12-5-0-652
- 12.5.0-648
- 12.5.0-643
- 12.5.0-636
- 12.5.0-633
- 12.5.0-613
- 12.0.2-007
- 12.0.2-005
- 12.0.2-001
- 12.0.1-011
- 12.0.0-478
- 11.5.1-121
- 11.5.1-115
- 11.5.0-115
- 11.5.0-110
- 11.4.0-823
- 11.0.1-161
- 11.0.0-136

## リリース 12.5.0-670 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 12.5.0-670 にアップグレードすることができます。

- 12.5.0-658
- 12.5.0-655
- 12-5-0-652
- 12.5.0-648
- 12.5.0-643
- 12.5.0-636
- 12.5.0-633
- 12.5.0-613
- 12.0.2-007
- 12.0.2-005
- 12.0.2-001
- 12.0.1-011
- 12.0.0-478
- 11.5.1-121
- 11.5.1-115
- 11.5.0-115
- 11.5.0-110
- 11.4.0-823
- 11.0.1-161
- 11.0.0-136

## リリース 12.5.0-658 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 12.5.0-658 にアップグレードできます。

- 11.0.1-161
- 11.4.0-823
- 11.5.1-121
- 12.0.0-478
- 12.0.1-011
- 12.0.2-001
- 12.5.0-613

- 12.5.0-633
- 12.5.0-636
- 12.5.0-655



(注) このリリースは、Cisco E メールセキュリティ アプライアンスの場合は AsyncOS 12.5、Cisco Web セキュリティ アプライアンスの場合は AsyncOS 11.8 と互換性があります。

## リリース 12.5.0-655 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 12.5.0-655 にアップグレードできます。

- 11.1.0-065
- 11.1.0-088
- 12.0.0-478
- 12.5.0-633
- 12.5.0-636
- 12.5.0-648



(注) このリリースは、Cisco E メールセキュリティ アプライアンスの場合は AsyncOS 12.5、Cisco Web セキュリティ アプライアンスの場合は AsyncOS 11.8 と互換性があります。

## リリース 12.5.0-643 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 12.5.0-643 にアップグレードすることができます。

- 11.1.0-088
- 12.0.0-478



(注) このリリースは、Cisco E メールセキュリティ アプライアンスの場合は AsyncOS 12.5、Cisco Web セキュリティ アプライアンスの場合は AsyncOS 11.8 と互換性があります。

## リリース 12.5.0-636 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 12.5.0-636 にアップグレードすることができます。

- 11.4.0-823
- 12.5.0-633



(注) このリリースは、Cisco E メールセキュリティ アプライアンスの場合は AsyncOS 12.5、Cisco Web セキュリティ アプライアンスの場合は AsyncOS 11.8 と互換性があります。

## リリース 12.5.0-633 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 12.5.0-633 にアップグレードすることができます。

- 11.1.0-077
- 11.1.0-083
- 11.4.0-800
- 11.5.1-121
- 12.0.0-457
- 12.0.0-478
- 12.0.1-011
- 12.5.0-604
- 12.5.0-606
- 12.5.0-613



(注) このリリースは、Cisco E メールセキュリティ アプライアンスの場合は AsyncOS 12.5、Cisco Web セキュリティ アプライアンスの場合は AsyncOS 11.8 と互換性があります。

## E メールセキュリティおよび Web セキュリティのリリースとの互換性

AsyncOS for Email Security と AsyncOS for Web Security のリリースの互換性については、[https://www.cisco.com/c/ja\\_jp/support/security/content-security-management-appliance/products-release-notes-list.html](https://www.cisco.com/c/ja_jp/support/security/content-security-management-appliance/products-release-notes-list.html) から入手可能な互換性マトリクスで詳しく説明されています。

## インストールおよびアップグレードに関する注意事項

- [重要な追加資料\(12 ページ\)](#)
- [仮想アプライアンス\(13 ページ\)](#)
- [アップグレード前の要件\(13 ページ\)](#)
- [アップグレード中の IPMI メッセージ\(14 ページ\)](#)
- [このリリースへのアップグレード\(14 ページ\)](#)

## 重要な追加資料

関連する E メールセキュリティおよび Web セキュリティのリリースのリリースノートも確認する必要があります。

この情報へのリンクについては、[関連資料\(17 ページ\)](#)を参照してください。

## 仮想アプライアンス

仮想アプライアンスのセットアップについては、『*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/ja\\_jp/support/security/content-security-management-appliance/products-installation-guides-list.html](https://www.cisco.com/c/ja_jp/support/security/content-security-management-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が 2 TB 以上のディスク領域をサポートしておらず、このリリースで 2 TB 以上のディスク領域を使用する場合は、仮想アプライアンス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。

仮想アプライアンス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 \(13 ページ\)](#) で説明されているマニュアルを使用して、仮想アプライアンスをセットアップします。
  - ステップ 2** 物理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物理アプライアンスからコンフィギュレーション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コンフィギュレーション ファイルをロードします。
- ディスク領域と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。
- 

### 次の作業

ハードウェア アプライアンスをバックアップ アプライアンスとして使用する場合は、ユーザガイドまたはオンラインヘルプでバックアップに関する情報を参照してください。たとえば、バックアップ アプライアンスが管理対象の E メールセキュリティおよび Web セキュリティアプライアンスから直接データを取得しないようにするか、または Web セキュリティアプライアンスに設定を公開する必要があります。

## アップグレード前の要件

次の重要なアップグレード前タスクを実行します。

- [関連する E メールセキュリティおよび Web セキュリティアプライアンスのバージョンの確認 \(14 ページ\)](#)
- [既存の設定のバックアップ \(14 ページ\)](#)

## 関連する E メールセキュリティおよび Web セキュリティアプライアンスのバージョンの確認

アップグレードする前に、管理する E メールセキュリティアプライアンスと Web セキュリティアプライアンスが互換性のあるリリースを実行していることを確認します。[E メールセキュリティおよび Web セキュリティのリリースとの互換性 \(12 ページ\)](#) を参照してください。

## 既存の設定のバックアップ

Cisco コンテンツ セキュリティ管理アプライアンスをアップグレードする前に、既存のセキュリティ管理アプライアンスから XML 設定ファイルを保存します。アプライアンスから任意の場所にこのファイルを保存します。重要な注意事項と手順については、ユーザガイドまたはオンラインヘルプの「Saving and Exporting the Current Configuration File」のセクションを参照してください。

## アップグレード中の IPMI メッセージ

CLI を使用してアプライアンス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: CSCuz33125

## このリリースへのアップグレード

- 
- ステップ 1** [アップグレード前の要件 \(13 ページ\)](#) で説明されているすべてのトピックに対処します。
  - ステップ 2** このリリースのユーザガイド PDF の「Before You Upgrade: Important Steps」セクションに記載されているすべての手順に従ってください。
  - ステップ 3** アップグレードを実行します。

既存のリリースのユーザガイド PDF の「Common Administrative Tasks」の章の「Upgrading AsyncOS」のセクションの手順に従ってください。



**(注)** リポートしてから少なくとも 20 分経過するまで、いかなる理由があっても (アップグレードの問題をトラブルシューティングするためであっても) アプライアンスの電源をオフにしないでください。仮想アプライアンスがある場合は、ハイパーバイザまたはホスト OS ツールを仮想マシンのリセット、サイクル、または電源オフに使用しないでください。

---

- ステップ 4** 約 10 分後、アプライアンスにアクセスしてログインします。
  - ステップ 5** このリリースのユーザガイド PDF の「After Upgrading」のセクションに記載されている手順に従ってください。
  - ステップ 6** 該当する場合は、[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 \(13 ページ\)](#) を参照してください。
-

**重要:**このリリースにアップグレード後、ブラウザの操作をシームレスにするために、以下のいずれかのステップを試行できます。

- Web インターフェイスで使用される証明書を承認し、新しいブラウザウィンドウで `https://hostname.com:<https_api_port>` (例: `https://some.example.com:6443`) の URL 構文を使用して証明書を承認します。ここで、`<https_api_port>` は [ネットワーク (Network)] > [IP インターフェイス (IP Interfaces)] で設定されている AsyncOS API HTTPS ポートです。また、API ポート (HTTP/HTTPS) がファイアウォールで開かれていることを確認します。
- デフォルトで、`trailblazerconfig` の CLI コマンドはアプライアンスで有効になっています。HTTPS ポートがファイアウォールで開かれていることを確認します。また、アプライアンスにアクセスするために指定したホスト名を DNS サーバが解決できることを確認してください。

`trailblazerconfig` の CLI コマンドが無効になっている場合、CLI を使用して `trailblazerconfig > enable` コマンドを実行することにより、以下の問題を回避できます。

- 特定のブラウザで API ポートの複数の証明書を追加する必要がある。
- スпам隔離、セーフリスト、またはブロックリストのページを更新するときに、レガシー Web インターフェイスにリダイレクトされる。
- 高度なマルウェア防御レポート ページのメトリック バーにデータが含まれない。

詳細については、ユーザガイドの「The `trailblazerconfig` Command」のセクションを参照してください。



(注)

Web インターフェイスにアクセスできない場合は、アプライアンスを再起動するか、ブラウザのキャッシュをクリアします。問題が解決しない場合は、シスコカスタマーサポートにご連絡ください。

## 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: M190、M195、M380、M390、M395、M680、M690、および M695。  
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、[https://www.cisco.com/c/ja\\_jp/support/security/content-security-management-appliance/products-field-notices-list.html](https://www.cisco.com/c/ja_jp/support/security/content-security-management-appliance/products-field-notices-list.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。

- M160、M360、M660、および X1060
- M170、M370、M370D、M670、および X1070

## 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 \(16 ページ\)](#)
- [既知および解決済みの問題に関する情報の検索 \(16 ページ\)](#)

## 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/search?kw=*&amp;pf=prdNm&amp;pfVal=282509131&amp;rls=12.5.0&amp;sb=af&amp;sts=open&amp;svr=3nH&amp;bt=custV">https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&amp;pf=prdNm&amp;pfVal=282509131&amp;rls=12.5.0&amp;sb=af&amp;sts=open&amp;svr=3nH&amp;bt=custV</a>
修正済みの問題	<a href="https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&amp;pf=prdNm&amp;pfVal=282509131&amp;rls=12.5.0&amp;sb=fr&amp;svr=3nH&amp;bt=custV">https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&amp;pf=prdNm&amp;pfVal=282509131&amp;rls=12.5.0&amp;sb=fr&amp;svr=3nH&amp;bt=custV</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://bst.cloudapps.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、12.5) 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。
-





(注)

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

次の表の主要なドキュメントに加えて、ナレッジベースおよびシスコサポートコミュニティを含む他のリソースに関する情報は、オンラインヘルプおよびユーザガイド PDF の「More Information」の章に記載されています。

Cisco Content Security 製品の マニュアル:	入手場所
Cisco コンテンツ セキュリティ管理アプライアンス	<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>
Web セキュリティアプライアンス	<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>
E メール セキュリティアプライアンス	<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>
コンテンツ セキュリティ製品用コマンドライン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 Email Encryption	<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、アプライアンスからカスタマーサポートにアクセスすることもできます。手順については、ユーザガイドまたはオンラインヘルプを参照してください。

このマニュアルは、「関連資料」の項に記載されているマニュアルと併せてご利用ください。

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)

このマニュアルで使用している IP アドレスと電話番号は、実際のアドレスと電話番号を示すものではありません。マニュアル内の例、コマンド表示出力、ネットワークボジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2020 Cisco Systems, Inc. All rights reserved.

