

Cisco Web セキュリティアプライアンス向け AsyncOS 12.0 リリースノート

初版：2020 年 1 月 13 日

最終更新：2021 年 10 月 28 日

Web セキュリティアプライアンスについて

Cisco Web セキュリティアプライアンスはインターネットトラフィックを代行受信してモニタし、ポリシーを適用することによって、マルウェア、機密データの漏洩、生産性の低下などのインターネットベースの脅威から内部ネットワークを保護します。

最新情報

- [AsyncOS 12.0.4-002 の新機能：MD（メンテナンス導入）](#)
- [AsyncOS 12.0.3-007 の新機能：MD（メンテナンス導入）](#)
- [AsyncOS 12.0.3-005 の新機能：MD（メンテナンス導入）](#)
- [AsyncOS 12.0.2-012 MD（メンテナンス導入） の新機能：更新](#)
- [AsyncOS 12.0.2-004 の新機能：MD（メンテナンス導入）](#)
- [AsyncOS 12.0.1-334 GD（一般導入） の新機能](#)
- [AsyncOS 12.0.1-268 LD（限定導入） の新機能](#)

AsyncOS 12.0.4-002 の新機能：MD（メンテナンス導入）

このリリースには複数のバグ修正が含まれています。詳細については、「[リリース 12.0.4-002 の既知および修正済みの問題のリスト（21 ページ）](#)」を参照してください。

AsyncOS 12.0.3-007 の新機能：MD（メンテナンス導入）

このリリースには、多数のバグ修正が含まれています。詳細については、「[リリース 12.0.3-007 の既知および修正済みの問題のリスト](#)」を参照してください。

新しい URL カテゴリの更新通知	新しい URL カテゴリの更新通知 がバナーに導入されました。 ユーザには、今後の URL カテゴリの更新に関する電子メール通知も送信されます。
-------------------	--

AsyncOS 12.0.3-005 の新機能 : MD (メンテナンス導入)

このリリースには、多数のバグ修正が含まれています。詳細については、「[リリース 12.0.3-005 の既知および修正済みの問題のリスト](#)」を参照してください。

AsyncOS 12.0.2-012 MD (メンテナンス導入) の新機能 : 更新

このリリースには、多数のバグ修正が含まれています。詳細については、「[リリース 12.0.2-012 の既知および修正済みの問題のリスト](#)」および「[AsyncOS 12.0.2-012 の動作の変更](#)」を参照してください。

AsyncOS 12.0.2-004 の新機能 : MD (メンテナンス導入)

このリリースには、多数のバグ修正が含まれています。詳細については、「[リリース 12.0.2-004 の既知および修正済みの問題のリスト](#)」を参照してください。

機能	説明
<p>TLS 1.0/1.1 の廃止</p>	<p>アプライアンスを AMP ファイルレピュテーションサーバに接続するには、TLS 1.2以降のバージョンを使用します。南・北・中央アメリカ (レガシー) cloud-sa.amp.sourcefire.com は AMP ファイルレピュテーションサーバリストから削除されるため、南・北・中央アメリカ (レガシー) cloud-sa.amp.sourcefire.com はアプライアンスで設定できません。</p> <p>アプライアンスを 12.0.2 バージョンにアップグレードする前に、以下を推奨します。</p> <ul style="list-style-type: none"> AMP サービスが有効で、ファイルレピュテーションサーバが南・北・中央アメリカ (レガシー) cloud-sa.amp.sourcefire.com として設定されている場合は、ファイルレピュテーションサーバを南・北・中央アメリカ (cloud-sa.amp.cisco.com) に変更します。 アプライアンスをアップグレードした後、ファイルレピュテーションサーバが南・北・中央アメリカ (cloud-sa.amp.cisco.com) として保持されているかどうかを確認します。 <p>(注) アプライアンスをアップグレードする前にヨーロッパまたはアジア太平洋、日本、中国をファイルレピュテーションサーバとして設定した場合、上記の条件は適用されません。</p> <p>詳細については、Cisco Web セキュリティアプライアンスのレガシーファイルレピュテーションサーバの使用停止を参照してください。</p>
機能拡張	

機能	説明
AMP での最大同時スキャン数の設定をサポート	<p>Enter the number of concurrent scans to be supported by AMP オプションが、メインの CLI コマンド <code>advancedproxyconfig > scanners > AMP</code> に新たに追加されました。</p> <p>この新しい CLI オプションを使用すると、AMP でサポートされる同時スキャン数を設定できます。すべてのモデルのデフォルト値は、上限の 250 です。</p>
長時間実行中のスキャン削除時の判定変更をサポート	<p>新しい CLI サブコマンド eviction がメインの CLI コマンド <code>advancedproxyconfig > scanners</code> に追加されました。</p> <p>この新しい CLI サブコマンドを使用すると、長時間実行中のスキャン削除の判定設定をデフォルトの Unscannable から Timeout に、またはその逆に変更できます。</p>

AsyncOS 12.0.1-334 GD (一般導入) の新機能

このリリースには、多数のバグ修正が含まれています。詳細については、「[リリース 12.0.1-334 の既知および修正済みの問題のリスト](#)」を参照してください。

advancedproxyconfig CLI コマンドの下に **scanners** サブコマンドが追加されました。

新しいコマンドラインインターフェイス	説明
AMP エンジンによるスキャンからの MIME タイプの除外が可能	<p>新しいサブコマンド scanners がメインの advanced proxyconfig コマンドの下に追加され、AMP エンジンによるスキャン対象から MIME タイプを除外できるようになりました。scanners サブコマンドを使用するには、「アダプティブスキャン」機能を無効にする必要があります。</p> <p>scanners サブコマンドを使用して、AMP エンジンでスキャンする必要のない MIME タイプを追加し、スキャンのパフォーマンスを向上させることができます。デフォルトの MIME タイプのオプションは、「image/ALL and text/ALL」です。</p> <p>MIME タイプを追加するには、デフォルトのオプションの後に追加する必要があります。たとえば、ビデオと音声の MIME タイプを追加する場合は、次の形式にする必要があります。</p> <p>「image/ALL and text/ALL video/ALL audio/ALL」</p>

AsyncOS 12.0.1-268 LD (限定導入) の新機能

このリリースには、多数のバグ修正が含まれています。詳細については、「[リリース 12.0.1-268 の既知および修正済みの問題のリスト](#)」を参照してください。

このリリースでは次の機能が導入されました。

機能	説明
<p>ハイパフォーマンスのサポート</p>	<p>Cisco AsyncOS 12.0 リリースは、プラットフォーム S680、S690、および S695 向けにハイパフォーマンス (HP) を備えた Web セキュリティアプライアンスを提供します。これにより、既存のハイエンドアプライアンスのトラフィック処理パフォーマンスが向上します。</p> <p>ハイパフォーマンスモードがアプライアンス上で有効になっている場合、次のスキャンエンジンは S680 モデルでは 2 インスタンス、S690/S695 モデルでは 3 インスタンスとして複製されます。</p> <ul style="list-style-type: none"> • Sophos • McAfee • Merlin • Firestone • AVC • アーカイブスキャン • AMP
<p>Web セキュリティアプライアンスと Cisco Threat Response (CTR) ポータルの統合</p>	<p>Cisco Threat Response ポータルにアプライアンスを統合すると、Cisco Threat Response ポータルで次のアクションを実行できます。</p> <ul style="list-style-type: none"> • 組織内の複数のアプライアンスから Web トラッキングデータを表示します。 • Web トラッキングで検出された脅威を特定、調査、修正します。 • 特定した脅威を迅速に解決し、特定した脅威に対して推奨されるアクションを実行します。 • ポータルで脅威をドキュメント化して調査を保存し、ポータル内の他のデバイス間で情報を共有します。 <p>ユーザーガイドの「Intercepting with Cisco Threat Response Portal」の章を参照してください。</p>

機能	説明
TLS バージョン	<p>アプライアンスは TLSv1.3 バージョンをサポートしています。暗号 「TLS_AES_256_GCM_SHA384」 がデフォルトの暗号リストに追加されました。</p> <p>デフォルトでは、TLSv1.3 はアプライアンス上で有効になります。</p> <p>ユーザガイドの「Web 要求の代行受信」の章を参照してください。</p>
拡張機能	
<p>コンフィギュレーションファイルのバックアップのための Web インターフェイスの機能拡張</p>	<p>コンフィギュレーションファイルのバックアップ機能がサブメニューの [ログサブスクリプション (Log Subscriptions)] から [システム管理の (System Administration)] 下にある [コンフィギュレーションファイル (Configuration File)] に移動しました。</p>
ECDSA 証明書のアップロード	<p>アプライアンスが HTTPS プロキシの ECDSA 証明書のアップロードをサポートするようになりました。</p>



(注) 12.0.1-268 にアップグレードする前に次の機能を無効にし、モデル (S680、S690、S695、S680F、S690F、および S695F) でハイパフォーマンスモードを利用できるようにします。

- Web トラフィック タップ (Web Traffic Tap)
- ボリューム クォータと時間クォータ
- 全体の帯域幅の制限 (Overall Bandwidth Limits)

ハイパフォーマンスモードの Web セキュリティアプライアンスは、高レート of トランザクション処理をサポートしています。セキュリティ管理アプライアンスまたは Web セキュリティアプライアンスのハードディスク上のレポートデータとトラッキングデータを保持する期間は、処理容量の増加により、ハイパフォーマンスモードでは短縮されます。



(注) セキュリティ管理アプライアンス (SMA) モデルが 680 の場合は、SMA 12.7 バージョンを使用して Cisco Web セキュリティアプライアンス 12.0 を管理します。

このリリースでは、コマンドラインインターフェイスに次の変更が加えられています。

コマンドラインインターフェイス	説明
highperformance	ハイパフォーマンスモードを有効または無効にするために、新しいサブコマンドの highperformance が advancedproxyconfig メインコマンドに追加されました。
proxyscannermap	新しい診断 CLI サブコマンド proxyscannermap が、 <i>diagnostic > proxy</i> に追加されました。 proxyscannermap サブコマンドは、各プロキシと対応するスキャナプロセス間の PID マッピングを表示します。
CLI コマンドの authcache に新しいオプションが追加されました。	新しいオプションの searchdetails が CLI コマンドの authcache に追加されました。 この CLI は、すべてのアプライアンスに適用されます。
CLI コマンド reportingconfig の新しいサブコマンド CTROBSERVABLE	CLI コマンド reportingconfig に新しいサブコマンド CTROBSERVABLE が追加されました。 サブコマンド CTROBSERVABLE を使用して、CTR の監視対象に基づくインデックス作成を有効または無効にすることができます。これを有効にすると、ユーザがアクセスした URL のインデックスを作成できます。また、アプライアンストラッキングデータベース内の URL を検索する粒度も提供されます。

このリリースでは、次の新しいログが導入されました。

- プロキシインスタンスごとに *trackstat* ログファイルを分類
- *replicatord* ログ

動作における変更

- [AsyncOS 12.0.2-012 の動作の変更](#)

AsyncOS 12.0.2-012 の動作の変更

<p>プロキシ malloc メモリ使用率に関する警告メッセージ</p>	<p>アプライアンスの Web ユーザーインターフェイスに次のアラートメッセージがトリガーされます ([システム管理 (System Administration)] > [アラート (Alerts)] > [上位アラートの表示 (View Top Alerts)])。</p> <ul style="list-style-type: none"> • プロキシ malloc メモリがプロキシ malloc メモリ制限の 90% を超えた場合 <i>Proxy malloc memory reached to 90%, proxy will restart whenever max limit exceed</i> (プロキシ malloc メモリが 90% に達しました。プロキシは最大上限を超えるたびに再起動します) • プロキシが malloc メモリの 100% に達し、再起動する場合 <i>Proxy malloc memory exceed the max limit, restarting proxy</i> (プロキシ malloc メモリが上限を超えたため、プロキシを再起動します) <p>いずれの場合も、「Web プロキシ」の重要なアラートを受信するように設定されたすべての「アラート受信者」に、電子メール通知が送信されます。</p> <p>重要なログメッセージにプロキシログが含まれるようになりました。</p>
--------------------------------------	--

新しい Web インターフェイスへのアクセス

新しい Web インターフェイスは、モニタリング レポートとトラッキング Web サービスの新しい外観を提供します。新しい Web インターフェイスには次の方法でアクセスできます。

- レガシー Web インターフェイスにログインし、**をクリックすると、Cisco Web セキュリティアプライアンスが新しい外観になります。** [試してみてください (Try it!!)] リンク。このリンクをクリックすると、Web ブラウザの新しいタブが開き、
`https://wsa01-enterprise.com:<trailblazer-https-port>/ng-login` に移動します。ここでは、`wsa01-enterprise.com` はアプライアンスのホスト名で、`<trailblazer-https-port>` は、新しい Web インターフェイスにアクセスするためにアプライアンスに設定されている TRAILBLAZER HTTPS ポートです。

重要

- アプライアンスのレガシー Web インターフェイスにログインする必要があります。
- 指定したアプライアンスのホスト名を DNS サーバが解決できることを確認します。
- デフォルトでは、新しい Web インターフェイスでは、TCP ポート 6080、6443、および 4431 が動作可能である必要があります。これらのポートがエンタープライズファイアウォールでブロックされていないことを確認します。

- 新しい Web インターフェイスにアクセスするためのデフォルトポートは4431です。これは、**trailblazerconfig** CLI コマンドを使用してカスタマイズできます。**trailblazerconfig** CLI コマンドの詳細については、ユーザガイドの「コマンドラインインターフェイス」の章を参照してください。
- 新しい Web インターフェイスでは、HTTP および HTTPS の AsyncOS API (モニタリング) ポートも必要です。デフォルトでは、これらのポートは 6080 および 6443 です。AsyncOS API (モニタリング) ポートは、**interfaceconfig** CLI コマンドを使用してカスタマイズすることもできます。**Interfaceconfig** CLI コマンドの詳細については、ユーザガイドの「コマンドラインインターフェイス」の章を参照してください。

これらのデフォルトポートを変更した場合は、新しい Web インターフェイスのカスタマイズされたポートがエンタープライズ ファイアウォールでブロックされていないことを確認します。

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 11.8 以降) にアクセスすることをお勧めします。

- Google Chrome
- Mozilla Firefox

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 11.8 以降) でサポートされている解像度は、1280x800 ~ 1680x1050 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。

リリースの分類

各リリースは、リリースのタイプ (ED : 初期導入、GD : 一般導入など) によって識別されています。これらの用語の説明については、<http://www.cisco.com/c/dam/en/us/products/collateral/security/web-security-appliance/content-security-release-terminology.pdf>を参照してください。

このリリースでサポートされているハードウェア

このビルドは、サポートされている既存のすべてのプラットフォーム上でのアップグレードに使用できますが、拡張パフォーマンスのサポートは次のハードウェアモデルでのみ使用できません。

- S680
- S690
- S695
- S680F
- S690F
- S695F

このビルドは、次のハードウェアと仮想モデルのアップグレードに使用できます。

ハードウェアモデル：

- x80
- x90
- x95

仮想モデル：

- S100v
- S300v
- S600v

一部のハードウェアモデルでは、この AsyncOS リリースをインストールまたはアップグレードする前に、メモリをアップグレードする必要があります。詳細については、<http://www.cisco.com/c/en/us/support/docs/field-notices/638/fn63931.html>を参照してください。

アップグレードパス

- [AsyncOS 12.0.4-002 へのアップグレード](#)
- [AsyncOS 12.0.3-007 へのアップグレード](#)
- [AsyncOS 12.0.3-005 へのアップグレード](#)
- [AsyncOS 12.0.2-012 へのアップグレード](#)
- [AsyncOS 12.0.2-004 へのアップグレード](#)
- [AsyncOS 12.0.1-334 へのアップグレード](#)
- [AsyncOS 12.0.1-268 へのアップグレード](#)

AsyncOS 12.0.4-002 へのアップグレード



- (注) アップグレード中は、デバイス（キーボード、マウス、管理デバイス（Raritan）など）をアプライアンスの USB ポートに接続しないでください。

次のバージョンから AsyncOS for Cisco Web Security Appliances リリース 12.0.4-002 にアップグレードできます。

- | | | | |
|--------------|--------------|--------------|--------------|
| • 10.6.0-240 | • 11.7.0-418 | • 11.8.0-414 | • 12.0.1-268 |
| • 10.6.0-244 | • 11.7.0-704 | • 11.8.0-453 | • 12.0.1-334 |
| | • 11.7.1-006 | • 11.8.0-603 | • 12.0.2-004 |
| | • 11.7.1-020 | • 11.8.1-023 | • 12.0.2-012 |
| | • 11.7.1-043 | • 11.8.1-028 | • 12.0.3-005 |
| | • 11.7.1-045 | • 11.8.1-604 | • 12.0.3-007 |
| | • 11.7.1-049 | • 11.8.1-702 | |
| | • 11.7.1-501 | • 11.8.2-009 | |
| | • 11.7.2-011 | • 11.8.2-702 | |
| | • 11.7.3-025 | • 11.8.3-018 | |
| | | • 11.8.3-021 | |
| | | • 11.8.3-501 | |
| | | • 11.8.4-004 | |

AsyncOS 12.0.3-007 へのアップグレード



- (注) アップグレード中は、デバイス（キーボード、マウス、管理デバイス（Raritan）など）をアプライアンスの USB ポートに接続しないでください。

次のバージョンから AsyncOS for Cisco Web Security Appliances リリース 12.0.3-007 にアップグレードできます。

- | | | | |
|--------------|--------------|--------------|--------------|
| • 10.1.5-037 | • 11.7.0-418 | • 11.8.0-414 | • 12.0.1-268 |
| • 10.5.6-024 | • 11.7.0-704 | • 11.8.0-453 | • 12.0.1-334 |
| • 10.6.0-240 | • 11.7.1-006 | • 11.8.0-603 | • 12.0.1-004 |
| • 10.6.0-244 | • 11.7.1-020 | • 11.8.1-023 | • 12.0.2-012 |
| | • 11.7.1-043 | • 11.8.1-028 | • 12.0.3-005 |
| | • 11.7.1-045 | • 11.8.1-604 | |
| | • 11.7.1-049 | • 11.8.1-702 | |
| | • 11.7.1-501 | • 11.8.2-009 | |
| | • 11.7.2-011 | • 11.8.2-702 | |
| | • 11.7.3-025 | • 11.8.3-018 | |
| | | • 11.8.3-021 | |
| | | • 11.8.3-501 | |

AsyncOS 12.0.3-005 へのアップグレード



- (注) アップグレード中は、デバイス（キーボード、マウス、管理デバイス（Raritan）など）をアプライアンスの USB ポートに接続しないでください。

次のバージョンから AsyncOS for Cisco Web Security Appliances リリース 12.0.3-005 にアップグレードできます。

- | | | | |
|--------------|--------------|--------------|--------------|
| • 10.1.5-037 | • 11.7.0-418 | • 11.8.0-414 | • 12.0.1-268 |
| • 10.5.6-024 | • 11.7.0-704 | • 11.8.0-453 | • 12.0.1-334 |
| • 10.6.0-240 | • 11.7.1-006 | • 11.8.0-603 | • 12.0.1-004 |
| • 10.6.0-244 | • 11.7.1-020 | • 11.8.1-023 | • 12.0.2-012 |
| | • 11.7.1-043 | • 11.8.1-028 | |
| | • 11.7.1-045 | • 11.8.1-604 | |
| | • 11.7.1-049 | • 11.8.1-702 | |
| | • 11-7-1-501 | • 11.8.2-009 | |
| | • 11.7.2-011 | • 11.8.2-702 | |
| | • 11.7.3-025 | • 11.8.3-018 | |
| | | • 11.8.3-021 | |
| | | • 11.8.3-501 | |

AsyncOS 12.0.2-012 へのアップグレード



- (注) アップグレード中は、デバイス（キーボード、マウス、管理デバイス（Raritan）など）をアプライアンスの USB ポートに接続しないでください。

次のバージョンから AsyncOS for Cisco Web Security Appliances リリース 12.0.2-012 にアップグレードできます。

• 10.1.4-017	• 11.5.1-125	• 11.7.0-407	• 11.8.0-414	• 12.0.1-268
• 10.1.5-004	• 11.5.1-504	• 11.7.0-418	• 11.8.0-453	• 12.0.1-334
• 10.1.5-034	• 11.5.1-603	• 11.7.0-704	• 11.8.0-603	• 12.0.1-004
• 10.1.5-037	• 11.5.1-706	• 11.7.1-006	• 11.8.1-023	
• 10.5.2-072	• 11.5.2-020	• 11.7.1-020	• 11.8.1-028	
• 10.5.3-025	• 11.5.3-007	• 11.7.1-043	• 11.8.1-604	
• 10.5.4-018	• 11.5.3-016	• 11.7.1-045	• 11.8.1-702	
• 10.5.5-005	• 11.5.3-504	• 11.7.1-049	• 11.8.2-009	
• 10.5.6-022		• 11.7.1-501	• 11.8.2-702	
• 10.5.6-024		• 11.7.2-011		
• 10.6.0-240				
• 10.6.0-244				

AsyncOS 12.0.2-004 へのアップグレード



- (注) アップグレード中は、デバイス（キーボード、マウス、管理デバイス（Raritan）など）をアプライアンスの USB ポートに接続しないでください。

次のバージョンから AsyncOS for Cisco Web Security Appliances リリース 12.0.2-004 にアップグレードできます。

- 10.1.4-017 • 11.5.1-125 • 11.7.0-334 • 11.8.0-348 • 12.0.1-005
- 10.1.5-004 • 11.5.1-504 • 11.7.0-406 • 11.8.0-414 • 12.0.1-161
- 10.5.2-072 • 11.5.1-603 • 11.7.0-407 • 11.8.0-429
- 10.5.3-025 • 11.5.2-020 • 11.7.0-418 • 11.8.0-440
- 10.5.4-018 • 11.5.3-007 • 11.7.0-704 • 11.8.0-446
- 10.5.5-005 • 11.5.3-016 • 11.7.1-006 • 11.8.0-450
- 10.6.0-240 • 11.5.3-504 • 11.7.1-020 • 11.8.0-453
- 10.6.0-244

アップグレード後の要件

アプライアンスを Cisco Threat Response に登録していない場合は、12.0.4-002 にアップグレードした後、次の手順を実行する必要があります。

手順

ステップ 1 管理者アクセス権を使用して、Cisco Threat Response ポータルでユーザアカウントを作成します。

新しいアカウントを作成するには、URL <https://visibility.amp.cisco.com> を使用して Cisco Threat Response ポータルにログインし、[Cisco セキュリティアカウントの作成 (Create a Cisco Security Account)] をクリックします。新しいユーザアカウントを作成できない場合は、Cisco TAC に連絡してサポートを受けてください。

ステップ 2 アプライアンスを Security Services Exchange (SSE) クラウドポータルに登録するには、自身の地域に対応する SSE ポータルからトークンを生成します。

(注) SSE クラウドポータルへの登録時に、アプライアンスの Web ユーザーインターフェイスから、地域に基づいて次の FQDN を選択します。

- 米国 (api-sse.cisco.com)
- 欧州 (api.eu.sse.itd.cisco.com)
- APJC (api.apj.sse.itd.cisco.com)

ステップ 3 Security Services Exchange ポータルのクラウドサービスにある Cisco Threat Response が有効になっていることを確認します。アプライアンスを Security Services Exchange ポータルに登録するには、FQDN api-sse.cisco.com (米国) のファイアウォールの HTTPS (インとアウト) 443 ポートが開いていることを確認します。

仮想アプライアンスの展開については、『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、

<http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html> から入手できます。

互換性の詳細

- セキュリティ管理のための Cisco AsyncOS との互換性
- クラウドコネクタモードでの IPv6 と Kerberos は使用不可
- IPv6 アドレスの機能サポート
- アップグレード後の要件

セキュリティ管理のための Cisco AsyncOS との互換性

Cisco コンテンツセキュリティ管理リリース向け AsyncOS とこのリリースとの互換性については、
<http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html> にある互換性のマトリックスを参照してください。



(注) このリリースは、現在使用可能なセキュリティ管理リリースと互換性がなく、使用することはできません。互換性のあるセキュリティ管理リリースは間もなく利用可能になります。

クラウドコネクタモードでの IPv6 と Kerberos は使用不可

アプライアンスがクラウドコネクタモードで設定されている場合、Web インターフェイスのページに「IPv6 アドレスと Kerberos 認証用のオプションは使用できません (unavailable options for IPv6 addresses and Kerberos authentication)」と表示されます。使用できるように見えても、それらのオプションはクラウドコネクタモードではサポートされていません。クラウドコネクタモードでは、IPv6 アドレスまたは Kerberos 認証を使用するようにアプライアンスを設定しようとししないでください。

IPv6 アドレスの機能サポート

IPv6 アドレスをサポートする特性と機能は次のとおりです。

- コマンドラインと Web インターフェイス。アプライアンスにアクセスするには、[http://\[2001:2:2::8\]:8080](http://[2001:2:2::8]:8080) または [https://\[2001:2:2::8\]:8443](https://[2001:2:2::8]:8443) を使用します。
- IPv6 データトラフィックでのプロキシアクションの実行 (HTTP/HTTPS/SOCKS/FTP)
- IPv6 DNS サーバ
- WCCP 2.01 (Cat6K スイッチ) とレイヤ 4 透過リダイレクション
- アップストリームプロキシ
- 認証サービス

- Active Directory (NTLMSSP、Basic、および Kerberos)
- LDAP
- SaaS SSO
- CDA による透過的ユーザ識別 (CDA との通信は IPv4 のみ)
- クレデンシャルの暗号化

- Web レポートと Web トラッキング
- 外部 DLP サーバ (アプライアンスと DLP サーバ間の通信は IPv4 のみ)
- PAC ファイル ホスティング
- プロトコル : 管理サーバを介した NTP、RADIUS、SNMP、および syslog

IPv4 アドレスを必要とする特性と機能は次のとおりです。

- 内部 SMTP リレー
- 外部認証
- ログ サブスクリプションのプッシュ方式 : FTP、SCP、および syslog
- NTP サーバ
- ローカル アップデート サーバ (アップデート用のプロキシ サーバを含む)
- 認証サービス
- AnyConnect セキュア モビリティ
- Novell eDirectory 認証サーバ
- エンドユーザ 通知のカスタム ログのページ
- Web セキュリティ アプライアンスとセキュリティ管理アプライアンス間の通信
- 2.01 より前の WCCP バージョン
- SNMP

オペレーティング システムとブラウザの Kerberos 認証の可用性

Kerberos 認証は、次のオペレーティング システムとブラウザで使用できます。

- Windows サーバ 2003、2008、2008R2、および 2012
- Mac での Safari および Firefox ブラウザの最新リリース (OSX バージョン10.5 以降)
- IE (バージョン7以降) と Windows 7以降の Firefox および Chrome ブラウザの最新リリース

Kerberos 認証は、次のオペレーティング システムとブラウザでは使用できません。

- 上記に記載されていない Windows オペレーティング システム
- 上記で説明していないブラウザ
- iOS と Android

仮想アプライアンスの展開

仮想アプライアンスの展開については、『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、<http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html> から入手できます。

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

手順

ステップ 1 「アップグレード後の要件」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。

(注) セキュリティサービスの更新が成功したことを確認します。

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。

ハードウェアと仮想アプライアンスの IP アドレスが異なる場合は、設定ファイルをロードする前に、[ネットワーク設定のロード (Load Network Settings)] を選択解除します。

ステップ 5 変更を保存します。

ステップ 6 [ネットワーク (Network)] > [認証 (Authentication)] に移動し、ドメインに再度参加します。そうしないと、アイデンティティは機能しません。

AsyncOS for Web のアップグレード

始める前に

- RAID コントローラ ファームウェアの更新を含むアップグレード前の要件を実行します。
- 管理者としてログインします。

手順

-
- ステップ 1** [システム管理 (System Administration)] > [設定ファイル (Configuration File)] ページで、Web セキュリティアプライアンスから XML 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 2** [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、[アップグレードオプション (Upgrade Options)] をクリックします。
- ステップ 3** [ダウンロードとインストール (Download and install)] または [ダウンロードのみ (Download only)] のいずれかを選択できます。
使用可能なアップグレードのリストから選択します。
- ステップ 4** [続行 (Proceed)] をクリックします。
[ダウンロードのみ (Download only)] を選択した場合は、アップグレードがアプライアンスにダウンロードされます。
- ステップ 5** ([ダウンロードとインストール (Download and install)] を選択した場合) アップグレードが完了したら、[今すぐリブート (Reboot Now)] をクリックして、Web セキュリティアプライアンスをリブートします。
- (注) ブラウザがアップグレードしたバージョンの AsyncOS に新しいオンラインヘルプのコンテンツをロードすることを確認するには、ブラウザを終了してから開いてオンラインヘルプを表示します。これにより、期限切れのコンテンツのブラウザキャッシュがクリアされます。
- (注) Nexus 56128P スイッチインターフェイスを使用して Cisco Web セキュリティアプライアンス S690F をアップグレードまたは再起動すると、10G ファイバインターフェイスのリンクステータスに「down」と表示されます。この問題を解決するには、次の手順を実行します。
1. CLI コマンド `etherconfig > media` を使用して、アプライアンス インターフェイスの「media」を **10Gbase-SR** に設定します。
 2. コミットしてアプライアンスを再起動します。
- (注) ファイバインターフェイス上で、1G SFP から 10G SFP (またはその逆) へのすべての SFP スワップを行った後、S695F Cisco Web セキュリティアプライアンスをリブートします。これにより、目的の帯域幅の変更に合わせてドライババッファの設定が適切に調整されます。
-

重要：アップグレード後に必要なアクション

アップグレード後にアプライアンスが正常に機能し続けるようにするには、次の事項に対処する必要があります。

- [シスコが推奨する暗号スイートへのデフォルト プロキシ サービス暗号スイートの変更](#)

- 仮想アプライアンス：SSH セキュリティ脆弱性の修正に必要な変更
- ファイル分析：クラウドで分析結果の詳細を表示するために必要な変更
- ファイル分析：分析対象のファイル タイプの確認
- 正規表現のエスケープされていないドット

シスコが推奨する暗号スイートへのデフォルト プロキシ サービス暗号スイートの変更

AsyncOS 9.1.1 以降では、プロキシ サービスに使用可能なデフォルトの暗号スイートは、セキュアな暗号スイートのみを含むように変更されます。

ただし、AsyncOS 9.x.x 以降のリリースからアップグレードする場合、デフォルトのプロキシ サービスの暗号スイートは変更されません。セキュリティを強化するために、アップグレード後に、デフォルトのプロキシ サービス暗号スイートをシスコが推奨する暗号スイートに変更することをお勧めします。次の手順を実行します。

手順

ステップ 1 Web インターフェイスを使用してアプライアンスにログインします。

ステップ 2 [システム管理 (System Administration)] > [SSL 設定 (SSL Configuration)] をクリックします。

ステップ 3 [設定の編集 (Edit Settings)] をクリックします。

ステップ 4 [プロキシ サービス (Proxy Services)] で、[使用する暗号 (CIPHER(s) to Use)] フィールドを次のフィールドに設定します。

```
ECDH:DH:RSA:NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA:!SRP:!IDEA:!DH-DSS-AES256-GCM:!AES256-GCM:!DH-RSA-AES128-GCM:!TLS_AES_256_GCM_SHA384
```

注意 上記の文字列を改行またはスペースを含まない単一の文字列として貼り付けてください。

ステップ 5 変更を送信し、保存します。

CLI で `sslconfig` コマンドを使用して、上記の手順を実行することもできます。

仮想アプライアンス：SSH セキュリティ脆弱性の修正に必要な変更

このセクションの要件は AsyncOS 8.8 で導入されました。

次のセキュリティ脆弱性は、アプライアンスに存在する場合、アップグレード中に修正されます。

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150625-ironport>



(注) このパッチは、2015年6月25日より前にダウンロードまたはアップグレードされた仮想アプライアンスリリースにのみ必要です。

アップグレード前にこの問題を修正しなかった場合は、修正されたことを示すメッセージがアップグレード中に表示されます。このメッセージが表示された場合、アップグレード後にアプライアンスを完全な動作順序に戻すには次のアクションを実行する必要があります。

- SSH ユーティリティの既知のホストリストから、アプライアンスの既存のエントリを削除します。その後、アプライアンスに SSH 接続し、新しいキーを使用して接続を受け入れます。
- SCP プッシュを使用して、リモートサーバ (Splunk を含む) にログを転送する場合は、リモートサーバからアプライアンスの古い SSH ホストキーをクリアします。
- 展開に Cisco コンテンツセキュリティ管理アプライアンスが含まれている場合は、そのアプライアンスのリリースノートに記載されている重要な手順を参照してください。

ファイル分析：クラウドで分析結果の詳細を表示するために必要な変更

複数のコンテンツセキュリティアプライアンス (Web、電子メール、または管理) を展開しており、組織内の任意のアプライアンスからアップロードされたすべてのファイルについてクラウド内の詳細なファイル分析結果を表示する場合は、アップグレード後に各アプライアンスでアプライアンスグループを設定する必要があります。アプライアンスグループを設定するには、ユーザガイド (PDF) の「File Reputation Filtering and File Analysis」の章を参照してください (この PDF は AsyncOS 8.8 のオンラインヘルプよりも最新です)。

ファイル分析：分析対象のファイルタイプの確認

AsyncOS 8.8 でファイル分析クラウドサーバの URL が変更されました。その結果、分析可能なファイルタイプがアップグレード後に変更された可能性があります。変更がある場合は、アラートが表示されます。分析用に選択したファイルタイプを確認するには、**[セキュリティサービス (Security Services)] > [マルウェア対策およびレピュテーション (Anti-Malware and Reputation)]** を選択し、Advanced Malware Protection の設定を確認します。

正規表現のエスケープされていないドット

正規表現のパターンマッチングエンジンにアップグレードすると、システムの更新後に既存のパターン定義でエスケープされていないドットに関するアラートが表示されることがあります。ドットの後に 64 文字以上を返すパターン内のエスケープされていないドットは、Velocity パターンマッチングエンジンによって無効化されます。その影響についてのアラートがユーザに送信され、パターンを修正または置換するまで、更新のたびにアラートは送信され続けます。一般に、長い正規表現内のエスケープされていないドットは問題を引き起こす可能性があるため、避ける必要があります。

マニュアルの更新

Web サイト (www.cisco.com) にあるユーザガイドは、オンライン ヘルプ よりも最新である場合があります。この製品のユーザガイドとその他のドキュメントを入手するには、オンライン ヘルプの [PDF の表示 (View PDF)] ボタンをクリックするか、「[関連資料](#)」に表示される URL にアクセスしてください。

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](#)
- [既知および修正済みの問題のリスト](#)
- [既知および解決済みの問題に関する情報の検索](#)

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

- [リリース 12.0.4-002 の既知および修正済みの問題のリスト](#)
- [リリース 12.0.3-007 の既知および修正済みの問題のリスト](#)
- [リリース 12.0.3-005 の既知および修正済みの問題のリスト](#)
- [リリース 12.0.2-012 の既知および修正済みの問題のリスト](#)
- [リリース 12.0.2-004 の既知および修正済みの問題のリスト](#)
- [リリース 12.0.1-334 の既知および修正済みの問題のリスト](#)
- [リリース 12.0.1-268 の既知および修正済みの問題のリスト](#)

リリース 12.0.4-002 の既知および修正済みの問題のリスト

修正済みの問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=&pf=prdNm&rls=12.0.4-002&sb=fr&svr=3nH&bt=custV&prdNam=Cisco%20IronPort%20Web%20Security%20Appliance%20Software
既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?pf=prdNm&sb=fr&rls=12.0.4&kw=&bt=custV&prdNam=Cisco%20IronPort%20Web%20Security%20Appliance%20Software

リリース 12.0.3-007 の既知および修正済みの問題のリスト

修正済みの問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=&pf=prdNm&pfVal=282941570&rls=12.0.3-007&sb=fr&svr=3nH&bt=custV
---------	---

既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=&pf=prdNm&pfVal=282941570&rls=12.0.3&sb=af&sts=open&svr=3nH&bt=custV
-------	---

リリース 12.0.3-005 の既知および修正済みの問題のリスト

修正済みの問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=&pf=prdNm&pfVal=282941570&rls=12.0.3-005&sb=fr&svr=3nH&bt=custV
既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=&pf=prdNm&pfVal=282941570&rls=12.0&sb=af&sts=open&svr=3nH&bt=custV

リリース 12.0.2-012 の既知および修正済みの問題のリスト

修正済みの問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=&pf=prdNm&pfVal=282941570&rls=12.0.2-012&sb=fr&svr=3nH&bt=custV
既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=&pf=prdNm&pfVal=282941570&rls=12.0&sb=af&sts=open&svr=3nH&bt=custV

リリース 12.0.2-004 の既知および修正済みの問題のリスト

修正済みの問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=&pf=prdNm&pfVal=282941570&rls=12.0.2-004&sb=fr&svr=3nH&bt=custV
既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=&pf=prdNm&pfVal=282941570&rls=12.0&sb=af&sts=open&svr=3nH&bt=custV

リリース 12.0.1-334 の既知および修正済みの問題のリスト

修正済みの問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=&pf=prdNm&pfVal=282521310&rls=12.0.1-334&sb=fr&svr=3nH&bt=custV
既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=&pf=prdNm&pfVal=282521310&rls=12.0.1&sb=af&sts=open&svr=3nH&bt=custV

リリース 12.0.1-268 の既知および修正済みの問題のリスト

修正済みの問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=&pf=prdNm&pfVal=282521310&rls=12.0.1-268&sb=fr&svr=3nH&bt=custV
既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=&pf=prdNm&pfVal=282521310&rls=12.0.1&sb=af&sts=open&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

Cisco Bug Search Tool を使用して、既知および解決済みの不具合に関する現在の情報を検索します。

始める前に

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)] > [Web セキュリティ (Web Security)] > Cisco Web セキュリティアプライアンス (Cisco Web Security Appliance)] をクリックし、[OK] をクリックします。

ステップ 4 [リリース (Releases)] フィールドに、リリースのバージョン (x.x.x 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、[リリース (Releases)] 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、[リリース (Releases)] 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

資料	参照先
『Cisco Web Security Appliance User Guide』	http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html
シスコのコンテンツセキュリティ管理アプライアンスユーザガイド	https://www.cisco.com/c/en/us/support/security/content-security-management-appliance/series.html
仮想アプライアンスインストールガイド	https://www.cisco.com/c/en/us/support/security/email-securityappliance/products-installation-guides-list.html

サポート

シスコ サポート コミュニティ

シスコ サポート コミュニティは、シスコのお客様、パートナー、および従業員向けのオンラインフォーラムです。Web セキュリティに関する一般的な問題や、特定のシスコ製品に関する技術情報について話し合う場を提供します。このフォーラムにトピックを投稿して質問したり、他のシスコ ユーザと情報を共有したりできます。

Web セキュリティと関連管理については、シスコ サポート コミュニティにアクセスしてください。

<https://supportforums.cisco.com/community/5786/web-security>

カスタマー 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 を参照してください。

従来の IronPort のサポート サイト : <http://www.cisco.com/web/services/acquisitions/ironport.html> を参照してください。

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。

【注意】 シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. 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. (1721R)

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。

© 2020–2021 Cisco Systems, Inc. All rights reserved.