Cisco Web セキュリティアプライアンス向け AsyncOS 14.5 リリースノート

初版：2022 年 4 月 11 日

最終更新：2024 年 1 月 31 日

Secure Web Appliance について

Cisco Secure Web Appliance はインターネットトラフィックを代行受信してモニターし、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 14.5.2-011 MD（メンテナンス導入）の新機能

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 14.5.2-011 の既知および修正済みの問題 （19 ページ）」を参照してください。

AsyncOS 14.5.1-016 MD（メンテナンス導入） の新機能：更新

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 14.5.1-016 の既知および修正済みの問題 （20 ページ）」を参照してください。

AsyncOS 14.5.1-008 MD（メンテナンス導入）の新機能

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 14.5.1-008 の既知および修正済みの問題 （20 ページ）」を参照してください。

AsyncOS 14.5.0-537 GD（一般導入）の新機能

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 14.5.0-537 の既知および修正済みの問題 （20 ページ）」を参照してください。

AsyncOS 14.5.0-498 LD（限定導入）の新機能

このリリースでは次の機能が導入されました。

<table>
<tr><th>機能</th><th colspan="2">説明</th></tr>
<tr><td>セキュア DNS</td><td colspan="2">Secure Web Appliance で、暗号化署名を使用して DNS サーバーから受信した DNS 応答を検証できるようになりました。
ユーザーガイドの「Editing DNS Settings」のセクションを参照してください。</td></tr>
<tr><td>クライアントあたりの最大接続数</td><td colspan="2">Secure Web Appliance で、クライアントによって開始される同時接続の数を設定した値に制限します。
ユーザーガイドの「Configuring Web Proxy Settings」のセクションを参照してください。</td></tr>
<tr><td rowspan="2">Cisco Web セキュリティアプライアンスから Cisco Secure Web Appliance へのブランド変更</td><td colspan="2">AsyncOS リリース 14.5 以降、Cisco Web セキュリティアプライアンスは、Web インターフェイスとすべてのユーザーマニュアルで Cisco Secure Web Appliance にブランド変更されました。</td></tr>
<tr><td>旧用語</td><td>ブランド変更後の用語</td></tr>
<tr><td>製品のブランド変更</td><td>Web セキュリティアプライアンス</td><td>Cisco Secure Web Appliance</td></tr>
<tr><td rowspan="6">製品のブランド変更</td><td>旧用語</td><td>ブランド変更後の用語</td></tr>
<tr><td>AMP for Endpoints</td><td>Secure Endpoint</td></tr>
<tr><td>Advanced Malware Protection</td><td>Secure Endpoint</td></tr>
<tr><td>AMP</td><td>Secure Endpoint</td></tr>
<tr><td>Thread Grid</td><td>Malware Analytics</td></tr>
<tr><td colspan="2">（注） このドキュメントに記載されているブランド変更された用語のインスタンスは、Web インターフェイスに対応していません。Web インターフェイスでは、AMP for Endpoints、Advance Malware Protection、および AMP は Malware Analytics と呼ばれます。Web インターフェイスは、次のリリースで更新されます。</td></tr>
<tr><td>誤分類要求</td><td colspan="2">誤分類要求はHTTPS経由で送信されるため、セキュリティアラート通知を受信しません。
ユーザーガイドの「Configuring On-Box End-User Notification Pages」セクションを参照してください。</td></tr>
</table>

機能	説明
新しいアクセスログ決定タグ	EUN（エンドユーザー通知）ページがクライアントの Web ブラウザに表示されると、復号化ポリシーグループのアクセスログ決定タグに EUN が付加されます。 ユーザーガイドの「ACL Decision Tags」セクションを参照してください。
ポリシーの複製	ポリシーの複製機能を使用すると、ポリシーの既存の構成をコピーまたは複製して、新しいポリシーを作成できます。 ユーザーガイドの「Policy Configuration」セクションを参照してください。
詳細な帯域幅制御	クォータプロファイルで帯域幅の値を設定し、アクセスポリシー URL カテゴリまたは全体的な Web アクティビティクォータでクォータプロファイルをマッピングすることにより、トラフィックの帯域幅を管理できます。 ユーザーガイドの「Defining Time, Volume, and Bandwidth Quotas」セクションを参照してください。
管理ポリシー、復号化ポリシー、ルーティングポリシー、IP スプーフィングポリシー、マルウェア対策とレピュテーション、認証レルム、Cisco スマート ソフトウェア ライセンス、Cisco Umbrella シームレス ID、ID サービス、およびシステムセットアップを設定するための REST API	設定情報を取得し、変更（既存の情報の変更、新しい情報の追加、エントリの削除など）を、REST API を使用してアプライアンスの設定データで実行できるようになりました。 『AsyncOS API 14.5 for Cisco Secure Web Appliance - Getting Started Guide』を参照してください。
ISE-SXP 統合	ISE-SXP 展開を Cisco Secure Web Appliance と統合して、パッシブ認証に使用できます。これによって、SXP を通じて公開された SGT から IP アドレスへのマッピングを含む、定義済みのすべてのマッピングを取得できます。 ユーザーガイドの「Configure ISE-SXP Integration」セクションを参照してください。

機能	説明
Cisco Umbrella シームレス ID	Cisco Umbrella シームレス ID 機能を使用すると、正常に認証された後に、アプライアンスからユーザ識別情報を Cisco Umbrella セキュア Web ゲートウェイ（SWG）にパスすることができます。Cisco Umbrella SWG は、Secure Web Appliance から受信した認証済み識別情報に基づいて、Active Directory のユーザー情報をチェックします。Cisco Umbrella SWG は、ユーザーを認証済みと見なし、定義されたセキュリティポリシーに基づいてユーザにアクセスを提供します。 Secure Web Appliance は、X-USWG-PKH、X-USWG-SK、および X-USWG-Data を含む HTTP ヘッダーを使用して Cisco Umbrella SWG にユーザー識別情報をパスします。 （注） Cisco Umbrella シームレス ID ヘッダーは、Secure Web Appliance 上の同じ名前のヘッダーを上書きします。 Cisco Umbrella シームレス ID 機能は、Active Directory でのみ認証方式をサポートします。この機能は、LDAP、Cisco Identity Services Engine（ISE）、および Cisco Context Directory Agent（CDA）をサポートしていません。 Cisco Umbrella SWG は FTP および SOCKS トラフィックをサポートしていません。 ユーザーガイドの「Cisco Umbrella Seamless ID」セクションを参照してください。
拡張機能	
Samba のアップグレード	Samba のバージョンは、バージョン 4.11.15 にアップグレードされています。 smbprotoconfig コマンドを使用して、Samba バージョン 4.11.15 の SMB1 プロトコルサポートを有効または無効にすることができます。デフォルトでは、このサポートは無効になっており、認証レルム構成に基づいて有効にすることができます。 ユーザーガイドの「Secure Web Appliance CLI Commands」セクションを参照してください。

（注） （TAC のみ）

CLI の復帰が小さいため、HTTPS プロキシポートは仮想 Secure Web Appliance では無効になっています。interfaceconfig コマンドを使用して、インターフェイスで HTTPS を有効にします。

動作における変更

AsyncOS 14.5.0-537 GD（一般導入）の動作の変更

ポリシーの複製	Cisco Secure Web Appliance のクローンオプションを含む次のポリシーは、Cisco Secure Email and Web Manager（SMA）でも管理できます。 • アクセス • 識別プロファイル • 復号化 • ルーティング

AsyncOS 14.5.0-498 LD（限定導入）の動作の変更

SSL の設定	TLSv1.2 は、Chrome ブラウザのバージョン 98.0.4758.80 以降をサポートするために、[システム管理者（Test Interface）] > [SSL設定（SSL Configuration）] の下のアプライアンス管理 Web ユーザーインターフェイスに対してデフォルトで有効になっています。
セッション再開	アップグレード後、セッションの再開はデフォルトで無効になります。
Context Directory Agent（CDA）	Context Directory Agent（CDA）はサポートされなくなりました。同じ機能を実現するために、透過的なユーザー識別のために ISE/ISE-PIC を設定することをお勧めします。 将来のリリースでは CDA を設定するオプションは使用できなくなります。 詳細については、「End-of-Sale and End-of-Life Announcement for the Cisco Context Directory Agent (CDA)」を参照してください。

スマートライセンス登録のインターフェイス選択	[テストインターフェイス（Test Interface）] ドロップダウンリストから、データインターフェイスまたは管理インターフェイスのいずれかを選択できるようになりました。 （注） データインターフェイスと管理インターフェイスの両方が構成されていることを確認します。 アップグレード後、分割ルーティングが有効になっている場合、Webインターフェイスのスマートライセンスの[テストインターフェイス（Test Interface）] は [データインターフェイス（Data Interface）] として表示されます。分割ルーティングが無効になっている場合は、[管理インターフェイス（Management Interface）] が表示されます。
HTTPS プロキシ – 無効な証明書の処理	AsyncOS 14.5 の新規インストールでは、HTTPS プロキシページの [期限切れ（Expired）] および [一致しないホスト名（Mismatched Hostname）] 証明書設定値は、デフォルトで [モニター（Monitor）] ではなく [ドロップ（Drop）] として選択されます。 （注） これは、新規インストールにのみ適用され、アップグレードには適用されません。 アプライアンスをアップグレードすると、以前のバージョンと同じ構成が保持されます。
networktuning	Cisco AsyncOS 14.5 へのアップグレード後、初めて networktuning コマンドを実行すると、プロキシプロセスを再起動するように求めるプロンプトが表示されます。 （注） 14.5 より前の AsyncOS バージョンでは、プロキシプロセスを再起動するためのこのプロンプトは使用できません。 アップグレード前に以前のバージョンのいずれかでコマンドが実行された場合、プロンプトはトリガーされません。

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、[Secure Web Appliance をクリックして新しい外観を試してみてください（Secure Web Appliance is getting a new look. Try it!!）] のリンクをクリックします。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 1440 x 900 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：全面導入など）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す。

- Sx90/F
- Sx95/F

（注） AsyncOS バージョン 14.5 は、Sx90/F モデルでサポートされる最後のリリースになります。

仮想モデル：

- S100v
- S300v

  システムの CPU およびメモリ要件は、12.5 リリース以降で変更されています。詳細については、『Cisco Content Security Virtual Appliance Installation Guide』を参照してください。
- S600v
- S1000v

（注） アプライアンスに付属の Cisco SFP を使用します。

アップグレードパス

- AsyncOS 14.5.2-011 へのアップグレード （9 ページ）
- AsyncOS 14.5.1-016 へのアップグレード （10 ページ）
- AsyncOS 14.5.1-008 へのアップグレード （10 ページ）

AsyncOS 14.5.2-011 へのアップグレード

（注） このリリースにアップグレードする前に、アプライアンスの設定ファイルのコピーをアプライアンス以外の場所に保存してください。

次のバージョンから AsyncOS for Cisco Secure Web Appliance リリース 14.5.2-011 にアップグレードできます。

- 11.8.0-453
- 11.8.1-023
- 11.8.1-028
- 11.8.1-511
- 11.8.1-604
- 11.8.1-702
- 11.8.3-021
- 11.8.3-501
- 11.8.4-004
- 12.0.1-334
- 12.0.2-004
- 12.0.2-012
- 12.0.3-005
- 12.0.3-007
- 12.0.3-503
- 12.0.4-002
- 12.0.5-011
- 12.5.1-011
- 12.5.1-035
- 12.5.1-043
- 12.5.2-011
- 12.5.3-002
- 12.5.3-006
- 12.5.4-005
- 12.5.4-011
- 12.5.5-004
- 12.5.5-005
- 12.5.5-008
- 12.5.5-501
- 12.5.6-008
- 12.7.0-033
- 14.0.0-467
- 14-0-1-014
- 14.0.1-040
- 14.0.1-053
- 14.0.2-012
- 14.0.3-007
- 14.0.3-014
- 14.0.4-005
- 14.1.0-032
- 14.1.0-041
- 14.1.0-047
- 14.5.0-388
- 14.5.0-455
- 14.5.0-498
- 14.5.0-537
- 14.5.0-673
- 14.5.1-008
- 14.5.1-016

AsyncOS 14.5.1-016 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 Secure Web Appliance リリース 14.5.1-016 にアップグレードできます。

11.8.0-453	12.0.1-334	14.0.0-467
11.8.1-023	12.0.2-004	14-0-1-014
11.8.1-028	12.0.2-012	14.0.1-040
11.8.1-511	12.0.3-005	14.0.1-053
11.8.1-604	12.0.3-007	14.0.2-012
11.8.1-702	12.0.4-002	14.0.3-007
11.8.2-702	12.0.5-011	14.0.3-014
11.8.3-021	12.5.1-011	14.0.4-005
11.8.3-501	12.5.1-035	14.1.0-032
11.8.4-004	12.5.1-043	14.1.0-041
	12.5.2-011	14.1.0-047
	12.5.3-002	14.5.0-388
	12.5.3-006	14.5.0-455
	12.5.4-005	14.5.0-498
	12.5.4-011	14.5.0-537
	12.5.5-004	14.5.0-673
	12.5.5-005	14.5.1-008
	12.5.5-008	
	12.7.0-033	

AsyncOS 14.5.1-008 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 Secure Web Appliance リリース 14.5.1-008 にアップグレードできます。

11.8.0-453	12.0.1-334	14.0.0-467
11.8.1-023	12.0.2-004	14-0-1-014
11.8.1-028	12.0.2-012	14.0.1-040
11.8.1-511	12.0.3-005	14.0.1-053
11.8.1-604	12.0.3-007	14.0.2-012
11.8.1-702	12.0.4-002	14.0.3-007
11.8.2-702	12.0.5-011	14.0.3-014
11.8.3-021	12.5.1-011	14.1.0-032
11.8.3-501	12.5.1-035	14.1.0-041
11.8.4-004	12.5.1-043	14.1.0-047
	12.5.2-011	14.5.0-388
	12.5.3-002	14.5.0-455
	12.5.3-006	14.5.0-498
	12.5.4-005	14.5.0-537
	12.5.4-011	14.5.0-673
	12.5.5-004	
	12.5.5-005	
	12.5.5-008	
	12.7.0-033	

AsyncOS 14.5.0-537 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 Secure Web Appliance リリース 14.5.0-537 にアップグレードできます。

11.8.0-453	12.0.1-268	14.0.0-467
11.8.1-023	12.0.1-334	14-0-1-014
11.8.1-028	12.0.2-004	14.0.1-040

11.8.1-511	12.0.2-012	14.0.1-053
11.8.1-604	12.0.3-005	14.0.1-503
11.8.1-702	12.0.3-007	14.0.2-012
11.8.2-009	12.0.4-002	14.1.0-032
11.8.2-702	12.5.1-011	14.1.0-041
11.8.3-021	12.5.1-035	14.1.0-047
11.8.3-501	12.5.1-043	14.5.0-388
11.8.4-004	12.5.2-007	14.5.0-455
	12.5.2-011	14.5.0-498
	12.5.3-002	
	12.5.4-005	
	12.5.4-011	
	12.7.0-033	

AsyncOS 14.5.0-498 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 Secure Web Appliance リリース 14.5.0-498 にアップグレードできます。

11.8.0-453	12.0.1-268	14.0.0-467
11.8.1-023	12.0.1-334	14-0-1-014
11.8.1-028	12.0.2-004	14.0.1-040
11.8.1-511	12.0.2-012	14.0.1-053
11.8.1-604	12.0.3-005	14.0.2-012
11.8.1-702	12.0.3-007	14.1.0-032
11.8.2-009	12.0.4-002	14.1.0-041
11.8.2-702	12.5.1-011	14.1.0-047
11.8.3-021	12.5.1-035	14.5.0-388
11.8.3-501	12.5.1-043	14.5.0-455

11.8.4-004	12.5.2-007
	12.5.2-011
	12.5.3-002
	12.7.0-033

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、14.5.1-016 にアップグレードした後で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。

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

セキュリティ管理のための Cisco AsyncOS との互換性

このリリースと Cisco Content Security Management 用の AsyncOS のリリースの互換性については、https://www.cisco.com/c/dam/en/us/td/docs/security/security_management/sma/sma_all/web-compatibility/index.htmlで互換性マトリックスを参照してください。

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 または 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 ロゴのページ
- Secure Web Appliance 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 （13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。

（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）]** > **[構成ファイル（Configuration File）]** ページで、Secure Web Applianceから XML構成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）] を選択した場合は、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、Cisco Secure Web Appliance 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。

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。

```
EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA:!SRP:!IDEA:!DHE-
DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA: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。新しいキーが作成されたら、ssh 経由でアプライアンスに接続し、接続を承認します。
- 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、「File Reputation Filtering and File Analysis」を参照してください。

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、その影響についてのアラートがユーザーに送信されます。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 （21 ページ）」に示す URL にアクセスしてください。

既知および修正済みの問題

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 14.5.2-011 の既知および修正済みの問題

シスコのアカウント クレデンシャルを使用して Cisco Bug Search Tool にログインし、修正されたバグのリストを表示します。

- 修正済みの問題
- 既知の問題

リリース 14.5.1-016 の既知および修正済みの問題

- 修正済みの問題
- 既知の問題

リリース 14.5.1-008 の既知および修正済みの問題

- 修正済みの問題
- 既知の問題

リリース 14.5.0-537 の既知および修正済みの問題

- 修正済みの問題
- 既知の問題

リリース 14.5.0-498 の既知および修正済みの問題

- 修正済みの問題
- 既知の問題

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 Secure Web 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 Secure Web Appliance ユーザーガイド	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ーガイド	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、他のシスコユーザー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、Cisco TAC にお問い合わせください。TAC に連絡する前に、仮想ライセンス番号（VLN）番号を準備してください。

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、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、『Cisco Secure Web Appliance User Guide』の「Troubleshooting」セクションを参照してください。

翻訳について
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。