Cisco Web セキュリティアプライアンス向け AsyncOS 14.0 リリースノート

初版：2021 年 5 月 5 日

最終更新：2022 年 9 月 14 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 14.0.3-014 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 14.0.3-014 の既知および修正済みの問題のリスト （26 ページ）」および「AsyncOS 14.0.3-014 MD（メンテナンス導入）の動作の変更 （11 ページ）」を参照してください。

AsyncOS 14.0.2-012 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 14.0.2-012 の既知および修正済みの問題のリスト （26 ページ）」および「AsyncOS 14.0.2-012 MD（メンテナンス導入）の動作の変更 （12 ページ）」を参照してください。

AsyncOS 14.0.1-053 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 14.0.1-053 の既知および修正済みの問題のリスト （26 ページ）」を参照してください。

AsyncOS 14.0.1-040 LD（限定導入）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 14.0.1-040 の既知および修正済みの問題のリスト （26 ページ）」および「AsyncOS 14.0.1-040 LD（限定導入）の動作の変更：更新 （12 ページ）」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
スマート ソフトウェア ライセンシングの機能強化	

機能	説明
	• スマート ソフトウェア ライセンシングを有効にし、Web セキュリティアプライアンスを Cisco Smart Software Manager に登録すると、Cisco Cloud Services（**[ネットワーク（Network）]**>**[クラウドサービスの設定（Cloud Service Settings）]**）は、Cisco Cloud Services ポータルを介して Web セキュリティアプライアンスを自動的に有効にして登録します。 • Cisco Smart Software Manager ポータルで作成されたスマートアカウントの詳細を表示するには、CLI で smartaccountinfo コマンドを使用します。 • Cisco Cloud Services 証明書の有効期限が切れている場合は、CLI で **cloudserviceconfig** > **fetchcertificate** サブコマンドを使用して Cisco Talos Intelligence Services ポータルから新しい証明書をダウンロードできます。 Cisco Cloud Services の証明書の有効期限が切れているか、まもなく期限切れになる場合、AsyncOS 14.0.1-040 へのアップグレード後に、Cisco Cloud Services が証明書を自動更新します。自動更新が失敗した場合は、fetchcertificate サブコマンドを使用して証明書を手動で更新できます。 （注） このコマンドは、スマートライセンスモードでのみサポートされています。 • CLI で **cloudserviceconfig** > **autoregister** サブコマンドを使用して、Web セキュリティアプライアンスを Cisco Cloud Services ポータルに自動登録できます。 （注） • このコマンドは、クラウドサービスポータルへの自動登録が失敗した場合にのみ使用できます。 • スマートライセンスが評価モードの場合、Cisco Cloud Services は自動登録できません。 • CLI で **updateconfig** > **clientcertificate** サブコマンドを使用して、仮想アプライアンスおよびハードウェアアプライアンスの証明書をロードできます。 （注） アプライアンスにスマートライセンスが登録されている場合は、Cisco Cloud Services を無効化または登録解除できません。

機能	説明
	ユーザーガイドの「Smart Software Licensing」セクションおよび「Integrating with Cisco SecureX and Cisco Threat Response」の章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 14.0.1-014 LD（限定導入）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、「AsyncOS 14.0.1-014 LD（限定導入）の新機能 （5 ページ）」および「AsyncOS 14.0.1-014 LD（限定導入）の動作の変更 （13 ページ）」を参照してください。

機能	説明
Cisco SecureX の統合	Cisco Web セキュリティ アプライアンスは、Cisco SecureX との統合をサポートするようになりました。Cisco SecureX は、すべてのシスコセキュリティ製品に組み込まれたセキュリティプラットフォームです。Web セキュリティ アプライアンスと Cisco SecureX を統合させることで、測定可能な分析情報を提供し、目標とする結果とこれまでにないチーム間コラボレーションを実現します。 Cisco SecureX は、セキュリティ インフラストラクチャの可視性を統一し、自動化を実現します。また、インシデント対応ワークフローの加速化と脅威検出の強化を図ります。Cisco SecureX の分散機能は、Cisco SecureX リボンでアプリケーションやツールの形式で利用できます。 ユーザーガイドの「Integrating with Cisco SecureX and Cisco Threat Response」の章を参照してください。

機能	説明
ヘッダーの書き換え	HTTP リクエストのカスタム ヘッダー プロファイルを設定し、ヘッダー書き換えプロファイルの下に複数のヘッダーを作成できます。ヘッダー書き換えプロファイル機能を使用すると、認証が成功した後、アプライアンスがユーザとグループの情報を別のアップストリーム デバイスに渡すことができます。アップストリーム プロキシはユーザを認証済みと見なし、追加の認証をバイパスし、定義されたアクセス ポリシーに基づいてユーザにアクセスを提供します。 ユーザーガイドの「Intercepting Web Requests」の章を参照してください。
X 認証ヘッダーの使用	Active Directory のヘッダー ベース認証スキームを設定できるようになりました。クライアントおよび Web セキュリティアプライアンスは、ユーザを認証済みと見なし、認証またはユーザクレデンシャルの再入力を求めません。X-Authenticated 機能は、Web セキュリティアプライアンスがアップストリーム デバイスとして動作する場合に機能します。 ユーザーガイドの「Configuring Global Authentication Settings」および「Classifying Users and Client Software」を参照してください。

機能	説明
新しい Web インターフェイスの [システムステータス（System Status）] ダッシュボード	アプライアンスのシステム ステータス ダッシュボードが拡張されました。 • [容量（Capacity）] タブ：既存の [システムステータス（System Status）] ダッシュボードに追加された新しいタブ。[時間範囲（Time Range）]、[システムCPUとメモリ使用率（System CPU and Memory Usage）]、[帯域幅とRPS（Bandwidth and RPS）]、[機能別CPU使用率（CPU Usage by Function）]、および [クライアントまたはサーバ接続（Client or Server Connections）] の詳細を示します。 • [ステータス（Status）] タブの [プロキシトラフィック特性（Proxy Traffic Characteristics）] には、クライアントとサーバの接続の詳細が示されます。 • [サービス応答時間（Service Response Time）] に、棒グラフの詳細と以前の日付の凡例データが含まれるようになりました。 ユーザーガイドの「System Status Page on the New Web Interface」セクションを参照してください。
管理ポリシー、アクセスポリシー、およびバイパスポリシーを設定するための REST API	設定情報の取得と、アプライアンスの設定データでの変更（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 を使用して実行できるようになりました。 『*AsyncOS API 14.0 for Cisco Web Security Appliances - Getting Started Guide*』を参照してください。

機能	説明
HTTP 2.0 のサポート	

機能	説明
	Cisco AsyncOS 14.0 バージョンは、TLS を介した Web リクエストおよび応答向けに HTTP 2.0 をサポートします。HTTP 2.0 サポートには、TLS 1.2 以降のバージョンでのみ使用可能な TLS ALPN ベースのネゴシエーションが必要です。 このリリースでは、HTTPS 2.0 は次の機能ではサポートされていません。 • Web トラフィック タップ（Web Traffic Tap） • 外部 DLP（External DLP） • 全体の帯域幅とアプリケーションの帯域幅 HTTP 2.0 設定を有効または無効にするために、新しい CLI コマンド <*HTTP2*> が導入されました。 アプライアンスの Web ユーザインターフェイスを使用して HTTP 2.0 を有効または無効にしたり、ドメインを制限したりすることはできません。HTTP 2.0 設定は、Cisco Secure Email and Web Manager（シスコのコンテンツセキュリティ管理アプライアンス）ではサポートされていません。 （注） デフォルトでは、HTTP 2.0 機能は無効になっています。この機能を有効にするには、<*HTTP2*> コマンドを使用します。 Cisco AsyncOS 14.0 バージョンは、次の HTTP 2.0 機能をサポートしていません。 • バイナリフレーミング：プッシュの約束と優先順位付け • プレーンテキスト HTTP2.0（H2C） • NPN ベースのネゴシエーション • HTTPS のセッション Cookie と永続的な Cookie HTTP 2.0 機能では、次をサポートします。 • 最大 4096 の同時セッションと 128 の同時ストリーム。 • ALPN にあるすべての HTTP プロトコルとアドバタイズされた ALPN にある最大 7 つのプロトコル。 • 最大サイズが 16k のヘッダー。

機能	説明
	（注） 2.0 の明示的なプロキシに対応する CONNECT も HTTP 1.1 で開始します
拡張機能	
コマンドライン インターフェイスの機能強化	新しい警告メッセージがコマンド ライン インターフェイスに追加されました。次のいずれかの機能のデフォルト証明書を使用しようとすると、CLI に新しい警告メッセージが表示されます。 • アプライアンス証明書（Web ユーザインターフェイスで、**[ネットワーク（Network）]** > **[証明書管理（Certificate Management）]** > **[アプライアンス証明書（Appliance Certificate）]** に移動） • ログイン情報暗号化証明書（Web ユーザインターフェイスで、**[ネットワーク（Network）]** > **[認証（Authentication）]** > **[設定の編集（Edit Settings）]** > **[詳細（Advanced）]** セクションに移動） • HTTPS 管理 UI 証明書（コマンド ライン インターフェイスで、**[certconfig]** > **[SETUP]** を使用）
サーバ証明書の OCSP 検証	新しいサブコマンド **OCSPVALIDATION_FOR_SERVER_CERT** が **certconfig** に追加されました。新しいサブコマンドを使用すると、LDAP サーバ証明書およびアップデータサーバ証明書の OCSP 検証を有効にできます。証明書の検証が有効になっている場合、通信に関係する証明書が失効するとアラートが表示されます。 （注） セキュア LDAP は、プロキシ認証中の OCSP 検証をサポートしていません。OCSP検証は、認証レルムの追加中に手動で認証設定をテストする場合にのみサポートされます（**[ネットワーク（Network）]** > **[認証（Authentication）]**）。

（注） Cisco Web セキュリティアプライアンス向け AsyncOS 14.0 は、クライアントとサーバの TLSv1.3 セッション再開をサポートしています。

次の証明書の有効期間が変更されました。

（注） これは、証明書がアプライアンスを介して生成される場合にのみ適用され、証明書をアップロードするときは適用されません。

証明書	最短有効期間		最長有効期間	
	Previous	**[新規（New）]**	**Previous**	**[新規（New）]**
HTTPS	1 カ月	24 カ月	120 カ月	60 カ月
SAAS	1 カ月	1 カ月	120 カ月	48 カ月
ISE	1 カ月	24 カ月	120 カ月	60 カ月
アプライアンス証明書	1 日間	730 日間	1825 日間	1825 日間
デモ/管理証明書	有効期間は 5 年間			

動作における変更

AsyncOS 14.0.3-014 MD（メンテナンス導入）の動作の変更

networktuning	Cisco AsyncOS 14.0 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） 14.0 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。

AsyncOS 14.0.2-012 MD（メンテナンス導入）の動作の変更

SSL の設定	Cisco AsyncOS 14.0.2 バージョンから、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）] にある [アプライアンス管理Webユーザーインターフェイス（Appliance Management Web User Interface）] 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	Cisco AsyncOS 14.0.2 バージョンへのアップグレード後、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）	Cisco AsyncOS 14.0.2 バージョン以降、CDA のサポートの終了を示す次のメッセージが CDA 設定セクションに追加されています。 「*Context Directory Agent*（*CDA*）のサポートが終了しました。*CDA* の代わりに透過的なユーザー認証用に *ISE/ISE-PIC* を設定することをお勧めします」。
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。

AsyncOS 14.0.1-040 LD（限定導入）の動作の変更：更新

スマート ソフトウェア ライセンシングの機能強化	すでに Cisco Smart Software Manager にアプライアンスを登録しており、Cisco Cloud Services を設定していない場合は、AsyncOS 14.0.1-040 にアップグレードすると Cisco Cloud Services が自動的に有効になります。デフォルトでは、リージョンは米国として登録され、必要に応じてリージョン（欧州および APJC）を変更できます。 （注） Cisco Cloud Services がすでに設定されている場合、アプライアンスを Cisco Smart Software Manager に登録する前に、[クラウドサービスの設定（Cloud Service Settings）] は変更されません。 アプライアンスにスマートライセンスが登録されている場合は、Cisco Cloud Services を無効化または登録解除できません。

AsyncOS 14.0.1-014 LD（限定導入）の動作の変更

ログ サブスクリプション	ログサブスクリプションの無効なログ名とファイル名が原因でアップグレードに失敗した場合、アプライアンスのコマンド ライン インターフェイスと Web ユーザインターフェイスに次のメッセージが表示されるようになりました。 **「アップグレードに失敗しました（理由：無効なログ サブスクリプション ファイル名/ログ名）。（Failed to upgrade (Reason: Invalid log subscription file names/log names).）」** 無効なファイル名またはログ名に関連する詳細も表示されます。
アプライアンスと認証サーバ間のポーリング機能の設定サポート	アプライアンスと認証サーバの間にポーリング機能を設定するために、新しい CLI コマンド gathererdconfig が追加されました。 gathererdconfig CLI コマンドを使用して、アプライアンスと認証サーバ間で収集されたポーリング機能を有効または無効にできます。デフォルトでは、ポーリング間隔は 24 時間に設定されています。 CLI コマンドは、アプライアンスが Cisco Secure Email and Web Manager（シスコのコンテンツセキュリティ管理アプライアンス）によって管理されている場合にのみ適用されます。
スマート ライセンシングの登録	アプライアンスでスマートライセンス機能を設定する際に、管理インターフェイスとデータ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。 新しいドロップダウンリストである [テストインターフェイス（Test Interface）]（**[システム管理（System Administration）] > [スマート ソフトウェア ライセンシング（Smart Software Licensing）]**）が、[データ（Data）] および [管理（Management）] という 2 つのインターフェイスオプションとともに追加されました。 これは、分割ルーティングを有効にし、スマートライセンス用に登録する場合にのみ適用されます。 （注） 分割ルーティングが有効になっていない場合は、[テストインターフェイス（Test Interface）] ドロップダウンリストで [管理（Management）] インターフェイスオプションのみを使用できます。

LDAP 認証のテスト開始基準	このリリースにアップグレードした後は、[ベースDN（ベース識別名）（Base DN (Base Distinguished Name)）] フィールド（**[ネットワーク（Network）] > [認証（Authentication）] > [レルムの追加（Add Realm）]**）が空の場合、LDAP 認証の [テスト開始（Start Test）] を実行できません。

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、 **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（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 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：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
- Sx95/F モデル

（注） Sx80 モデルは、AsyncOS バージョン 14.0 以降ではサポートされていません。

仮想モデル：

- S100v
- S300v
- S600v

アップグレードパス

AsyncOS 14.0.3-014 へのアップグレード

次のバージョンから Cisco Web セキュリティアプライアンス向け AsyncOS リリース 14.0.3-014 にアップグレードできます。

（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。

- 11.7.3-025
- 11.8.0-453
- 11.8.1-023
- 11.8.1-028
- 11.8.1-511
- 11.8.1-604
- 11.8.1-702
- 11.8.2-009
- 11.8.2-702
- 11.8.3-021
- 11.8.3-501
- 11.8.4-004
- 12.0.1-268
- 12.0.1-334
- 12.0.2-004
- 12.0.2-012
- 12.0.3-005
- 12.0.3-007
- 12.0.4-002
- 12.0.5-011
- 12.5.1-011
- 12.5.1-035
- 12.5.1-043
- 12.5.2-007
- 12.5.2-011
- 12.5.3-002
- 12.5.4-005
- 14.0.0-467
- 14-0-1-014
- 14.0.1-040
- 14.0.1-053
- 14.0.1-503
- 14.0.2-012

AsyncOS 14.0.2-012 へのアップグレード

次のバージョンから Cisco Web セキュリティアプライアンス向け AsyncOS リリース 14.0.1-012 にアップグレードできます。

（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。

- 11.7.3-025
- 11.8.0-453
- 11.8.1-023
- 11.8.1-028
- 11.8.1-511
- 11.8.1-604
- 11.8.1-702
- 11.8.2-009
- 11.8.2-702
- 11.8.3-021
- 11.8.3-501
- 11.8.4-004
- 12.0.1-268
- 12.0.1-334
- 12.0.2-004
- 12.0.2-012
- 12.0.3-005
- 12.0.3-007
- 12.0.4-002
- 12.5.1-011
- 12.5.1-035
- 12.5.1-043
- 12.5.2-007
- 12.5.3-002
- 14.0.0-467
- 14-0-1-014
- 14.0.1-040
- 14.0.1-053

AsyncOS 14.0.1-053 へのアップグレード

次のバージョンから Cisco Web セキュリティアプライアンス向け AsyncOS リリース 14.0.1-053 にアップグレードできます。

（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。

• 11.7.3-025	• 11.8.0-453	• 12.0.1-268	• 12.5.1-011
	• 11.8.1-023	• 12.0.1-334	• 12.5.1-035
	• 11.8.1-028	• 12.0.2-004	• 12.5.1-043
	• 11.8.1-511	• 12.0.2-012	• 12.5.2-007
	• 11.8.1-604	• 12.0.3-005	• 14.0.0-467
	• 11.8.1-702	• 12.0.3-007	• 14-0-1-014
	• 11.8.2-009		• 14.0.1-040
	• 11.8.2-702		
	• 11.8.3-021		
	• 11.8.3-501		
	• 11.8.4-004		

AsyncOS 14.0.1-040 へのアップグレード

次のバージョンから Cisco Web セキュリティアプライアンス向け AsyncOS リリース 14.0.1-040 にアップグレードできます。

（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。

• 11.7.3-025	• 11.8.0-453	• 12.0.1-268	• 12.5.1-011
	• 11.8.1-023	• 12.0.1-334	• 12.5.1-035
	• 11.8.1-028	• 12.0.2-004	• 12.5.1-043
	• 11.8.1-511	• 12.0.2-012	• 14.0.0-467
	• 11.8.1-604	• 12.0.3-005	• 14-0-1-014
	• 11.8.1-702	• 12.0.3-007	
	• 11.8.2-009		
	• 11.8.2-702		
	• 11.8.3-021		
	• 11.8.3-501		

AsyncOS 14.0.1-014 へのアップグレード

次のバージョンから Cisco Web セキュリティアプライアンス向け AsyncOS リリース 14.0.1-014 にアップグレードできます。

（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。

- 11.7.3-025
- 11.8.0-453
- 11.8.1-023
- 11.8.1-028
- 11.8.1-511
- 11.8.1-604
- 11.8.1-702
- 11.8.2-009
- 11.8.2-702
- 11.8.3-021
- 11.8.3-501
- 12.0.1-268
- 12.0.1-334
- 12.0.2-004
- 12.0.2-012
- 12.5.1-011
- 12.5.1-035
- 12.5.1-043
- 14.0.0-467

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、14.0.3-014 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。

（注） すでに Cisco Threat Response に登録している場合、この手順は適用されません。

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

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

- 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。

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:TLS_AES_128_GCM_SHA256:TLS_CHACHA20_POLY1305_SHA256

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ーに送信され、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。この製品のユーザー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 14.0.3-014 の既知および修正済みの問題のリスト

- 修正済みの問題
- 既知の問題

リリース 14.0.2-012 の既知および修正済みの問題のリスト

- 修正済みの問題
- 既知の問題

リリース 14.0.1-053 の既知および修正済みの問題のリスト

- 修正済みの問題
- 既知の問題

リリース 14.0.1-040 の既知および修正済みの問題のリスト

- 修正済みの問題
- 既知の問題

リリース 14.0.1-014 の既知および修正済みの問題のリスト

- 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 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 [英語] 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 [英語] 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、ユーザーガイドまたはオンライン ヘルプを参照してください。

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product

software, language used based on standards documentation, or language that is used by a referenced third-party product.

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、ネットワークトポロジ図、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。

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。