Cisco Web セキュリティアプライアンス向け AsyncOS 12.7 リリースノート

初版：2021 年 9 月 15 日

Cisco 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 12.7.0-033 LD（限定導入）の新機能

AsyncOS 12.7.0-033 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 12.7.0-033 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
ISE-SXP 統合	ISE-SXP 展開を Cisco Web セキュリティアプライアンスと統合して、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。 詳細については、『User Guide for AsyncOS 12.7 for Cisco Web Security Appliances』を参照してください。

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：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。

サポート対象ハードウェア

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。

- Sx80
- Sx90/F
- Sx95/F

アプライアンスをアップグレードまたは再起動する前に、接続されているファイバ スイッチ ポート インターフェイスで LLDP を無効にします。これにより、FCoE トラフィックが自動的に無効になります。

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

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 12.7.0-033 へのアップグレード

Cisco Web セキュリティアプライアンス向け AsyncOS 12.5.1-043 から バージョン 12.7.0-033 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。

アップグレード後の要件

12.7.0-033 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。

（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 この AsyncOS リリースで仮想アプライアンスを設定します。「アップグレード後の要件」を参照してください。

（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 変更を確定します。

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、Cisco Web セキュリティアプライアンスから 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 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

- 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 12.7.0-033 の既知および修正済みの問題のリスト

リリース 12.7.0-033 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=12.7.0-033&sb=fr&svr=3nH&bt=custV

既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282941570&rls=12.7.0&sb=afr&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

資料	参照先
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 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。