

はじめに

この章で説明する内容は、次のとおりです。

- Web セキュリティアプライアンス について (2ページ)
- AsyncOS 12.5 の新機能 (2ページ)
- •関連項目 (4ページ)
- •アプライアンス Web インターフェイスの使用 (4ページ)
- サポートされる言語(8ページ)
- Cisco SensorBase ネットワーク (9 ページ)

Web セキュリティアプライアンス について

AsyncOS 12.5 の新機能

表 1: Async 0S 12.5 の新機能

機能	説明
Web プロキシの IP スプーフィング	IP スプーフィングプロファイルを作成し、そ れをルーティングポリシーに追加することに よって、Web プロキシ IP スプーフィングを設 定できるようになりました。IP スプーフィン グプロファイルがルーティングポリシーで使 用されている場合、Web プロキシは送信元 IP アドレスを IP スプーフィングプロファイルで 定義されたカスタム IP アドレスに変更しま す。Web プロキシの IP スプーフィングを参照 してください。
	FTP プロキシ設定で、ネイティブ FTP 要求の クライアント IP スプーフィングを有効または 無効にすることができるようになりました。 FTP プロキシの有効化と設定を参照してくだ さい。
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	新しい Web インターフェイスでは、アプライ アンスに新しいページ([モニターリング (Monitoring)]>[システムステータス(System Status)]) があり、アプライアンスの現在のス テータスと設定が表示されます。新しい Web インターフェイスの[システムステータス (System Status)]ページを参照してください。
ネットワーク、ログサブスクリプション、お よびその他の設定用の 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 12.5 for Cisco Web Security Appliances - Getting Started Guide』を参照して ください。

機能	説明	
YouTube 分類のサポート	セキュアなアクセス制御のため、YouTubeの カスタム URL カテゴリを作成し、YouTube カ スタムカテゴリでポリシーを設定できるよう になりました。YouTubeの分類を参照してく ださい。	
Web セキュリティアプライアンスにおける Cisco Success Network	Cisco Success Network (CSN)機能によって シスコはアプライアンスの機能使用状況情報 のテレメトリを収集できます。シスコはこれ らの詳細情報を使用して、デバイス情報、 料の機能やライセンス供与された機能のリン ト、およびそれらのアクティベーションステ タスを識別します。	
	 (注) デフォルトでは、Cisco Success Network 機能はアプライアンスで 有効になっています。必要に応じ て、Webユーザーインターフェイ ス([システム管理 (System Administration)]>[Cisco Success Network])または CLI コマンド csidconfigを使用することで、こ の機能を無効にできます。 	
	「Cisco Success Network を使用した Cisco Web セキュリティアプライアンスのユーザーエク スペリエンスの向上」を参照してください。	

機能	説明
ハイパフォーマンスのサポート:フェーズ2	Cisco AsyncOS 12.5 リリースでは、プラット フォーム S680、S690、および S695/F 向けの高 いパフォーマンス(HP)を備えた Web セキュ リティアプライアンスが提供されています。 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。
	アプライアンスで次の機能を有効にしている 場合でも、12.5 バージョンにアップグレード し、モデル(S680、S690、S695、S680F、 S690F、S695F)でハイパフォーマンスモード を利用できるようになりました。
	• 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)
	以前のリリースでは、ハイパフォーマンスモー ドを利用するために、上記の機能を無効にす る必要がありました。

関連項目

http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-release-notes-list.html

アプライアンス Web インターフェイスの使用

- •Web インターフェイスのブラウザ要件 (4 ページ)
- 仮想アプライアンスでのWebインターフェイスへのアクセスのイネーブル化(6ページ)
- •アプライアンス Web インターフェイスへのアクセス (6ページ)
- •Web インターフェイスでの変更内容のコミット (8ページ)
- •Web インターフェイスでの変更内容のクリア (8ページ)

Web インターフェイスのブラウザ要件

Webインターフェイスにアクセスするための要件は次のとおりです。

- ・ブラウザで Cookie と JavaScript がサポートされ、有効になっている必要があります。
- また、ブラウザでは Cascading Style Sheet (CSS) を含む HTML ページをレンダリングで きる必要があります。
- Cisco Web セキュリティアプライアンス は YUI (http://yuilibrary.com/yui/environments/) で 設定されたターゲット環境に準拠しています。
- ・セッションは、非アクティブな状態が30分続くと自動的にタイムアウトします。
- Webインターフェイス内の一部のボタンとリンクを使用すると、さらにウィンドウが開きます。そのため、Webインターフェイスを使用するには、ブラウザのポップアップブロックを設定する必要があります。



(注) アプライアンスの設定を編集する場合は、一度に1つのブラウザウィンドウまたはタブを使用します。また、WebインターフェイスおよびCLIを同時に使用してアプライアンスを編集しないでください。複数の場所からアプライアンスを編集すると、予期しない動作が発生するので、サポートされません。

GUI にアクセスするには、ブラウザが JavaScript および Cookie をサポートし、受け入れるよう 設定されている必要があり、さらに、Cascading Style Sheet (CSS) を含む HTML ページを描画 できる必要があります。

表 2:サポー	トされ	るブラウ	ウザおよ	びリ	リース
---------	-----	------	------	----	-----

ブラウザ	Windows 10	MacOS 10.6
Safari		7.0 以降
Google Chrome	最新の安定バージョ ン	最新の安定バージョ ン
Microsoft Internet Explorer	11.0	—
Mozilla Firefox	最新の安定バージョ ン	最新の安定バージョ ン
Microsoft Edge	最新の安定バージョ ン	最新の安定バージョ ン

ブラウザは、そのブラウザの公式なサポート対象オペレーティングシステムに対してのみサ ポートされます。

インターフェイスの一部のボタンまたはリンクからは追加のウィンドウがオープンされるため、GUIを使用するには、ブラウザのポップアップブロックの設定が必要な場合があります。 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。



(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。

仮想アプライアンスでのWebインターフェイスへのアクセスのイネー ブル化

デフォルトでは、HTTP および HTTPS インターフェイスは仮想アプライアンスで有効化され ません。これらのプロトコルを有効にするには、コマンドラインインターフェイスを使用する 必要があります。

- **ステップ1** コマンドラインインターフェイスにアクセスします。コマンドラインインターフェイスへのアクセスを参 照してください。
- ステップ2 interfaceconfig コマンドを実行します。

プロンプトで Enter を押すと、デフォルト値が受け入れられます。

HTTP および HTTPS のプロンプトを検索し、使用するプロトコルをイネーブルにします。

HTTP および HTTPS の AsyncOS API (モニターリング)のプロンプトを探し、使用するプロトコルをイ ネーブルにします。

アプライアンス Web インターフェイスへのアクセス

仮想アプライアンスを使用している場合は、仮想アプライアンスでの Web インターフェイス へのアクセスのイネーブル化 (6ページ) を参照してください。

ステップ1 ブラウザを開き、Web セキュリティアプライアンスの IP アドレス(またはホスト名)を入力します。ア プライアンスが事前に設定されていない場合は、デフォルト設定を使用します。

https://192.168.42.42:8443

または

http://192.168.42.42:8080

ここで、192.168.42.42 はデフォルト IP アドレス、8080 は HTTP のデフォルトの管理ポートの設定、8443 は HTTPS のデフォルトの管理ポートです。

アプライアンスが現在設定されている場合は、M1ポートのIPアドレス(またはホスト名)を使用します。

- (注) アプライアンスに接続するときはポート番号を使用する必要があります(デフォルトはポート 8080)。Webインターフェイスにアクセスするときにポート番号を指定しないと、デフォルト ポート 80 になり、[ライセンスなしプロキシ(Proxy Unlicensed)]エラーページが表示されま す。
- ステップ2 (新しい Web インターフェイスのみ)レガシー Web インターフェイスにログインし、[Web セキュリティ アプライアンスのデザインが新しくなりました。お試しください!リンクで新しい Web インターフェイス にアクセスできます。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://wsa_appliance.com:<trailblazer-https-port>/ng-login に移動します。ここで、wsa_appliance.com はアプライアンスのホスト名で、<trailblazer-https-port> はアプライアンスに設定されている TRAILBLAZER HTTPS ポートです。
 - (注) ・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。
 - 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、trailerblazerconfigCLIコマンドを使用してカスタマイズできます。trailblazerconfigCLIコマンドの詳細については、WebセキュリティアプライアンスCLIコマンド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 (モニターリング) ポートは、interfaceconfig CLI コマンドで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、Web セキュリティアプライ アンス CLI コマンドを参照してください。
 - (注) ポートはデフォルトで有効になっていますが、これらのポートを無効にすると、 アップグレード後に再び有効になります。
 - 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もエンタープライズファイアウォールでブロックされないことを確認してください。
- **ステップ3** アプライアンスのログイン画面が表示されたら、アプライアンスにアクセスするためのユーザー名とパス フレーズを入力します。

デフォルトで、アプライアンスには以下のユーザー名とパスフレーズが付属します。

- ユーザー名: admin
- パスフレーズ: ironport

admin のユーザー名でログインするのが初めての場合は、パスフレーズをすぐに変更するよう求められます。

ステップ4 自分のユーザー名での最近のアプライアンスへのアクセス試行(成功、失敗を含む)を表示するには、ア プリケーション ウィンドウの右上の [ログイン(Logged in as)] エントリの前にある [最近のアクティビ ティ(recent-activity)] アイコン(成功は i、失敗は !) をクリックします。

Web インターフェイスでの変更内容のコミット

- ステップ1 [変更を確定 (Commit Changes)]をクリックします。
- ステップ2 選択する場合、[コメント (Comment)]フィールドにコメントを入力します。
- ステップ3 [変更を確定 (Commit Changes)]をクリックします。
 - (注) すべてをコミットする前に、複数の設定変更を行うことができます。

Web インターフェイスでの変更内容のクリア

- ステップ1 [変更を確定 (Commit Changes)] をクリックします。
- ステップ2 [変更を破棄(Abandon Changes)] をクリックします。

サポートされる言語

AsyncOS は次の言語のいずれかで GUI および CLI を表示できます。

- ・ドイツ語
- 英語
- •スペイン語
- •フランス語
- •イタリア語
- 日本語
- 韓国語
- •ポルトガル語
- •ロシア語
- 中国語
- 台湾語

Cisco SensorBase ネットワーク

Cisco SensorBase ネットワークは、世界中の何百万ものドメインを追跡し、インターネットトラフィックのグローバルウォッチリストを維持する脅威の管理データベースです。SensorBase は、既知のインターネットドメインの信頼性の評価をシスコに提供します。Cisco Web セキュリティアプライアンスは、SensorBase データフィードを使用して、Web レピュテーションスコアを向上させます。

SensorBase の利点とプライバシー

Cisco SensorBase ネットワークへの参加は、シスコがデータを収集して、SensorBase 脅威管理 データベースとそのデータを共有することを意味します。このデータには要求属性に関する情 報およびアプライアンスが要求を処理する方法が含まれます。

シスコはプライバシーを維持する重要性を理解しており、ユーザー名やパスフレーズなどの個 人情報または機密情報も収集または使用しません。また、ファイル名とホスト名に続く URL 属性は、機密性を保証するために難読化されます。復号されたHTTPSトランザクションでは、 SensorBaseネットワークはIPアドレス、Webレピュテーションスコア、および証明書内のサー バー名の URL カテゴリのみを受信します。

SensorBase ネットワークへの参加に同意する場合、アプライアンスから送信されたデータは HTTPSを使用して安全に転送されます。データを共有すると、Webベースの脅威に対応して、 悪意のあるアクティビティから企業環境を保護するシスコの機能が向上します。

Cisco SensorBase ネットワークへの参加の有効化



(注) システムの設定時にデフォルトで[標準 SensorBase ネットワークに参加(Standard SensorBase Network Participation)]がイネーブルにされています。

ステップ1 [セキュリティ サービス (Security Services)]>[SensorBase (SensorBase)]を選択します。

ステップ2 [SensorBase ネットワークに参加 (SensorBase Network Participation)] がイネーブルであることを確認します。

ディセーブルの場合、アプライアンスが収集するデータは SensorBase ネットワーク サーバーには戻されません。

ステップ3 [加入レベル (Participation Level)] セクションで、以下のレベルのいずれかを選択します。

• [制限(Limited)]。基本的な参加はサーバー名情報をまとめ、SensorBase ネットワーク サーバーに MD5 ハッシュ パス セグメントを送信します。

- [標準 (Standard)]。拡張された参加は、unobfuscated パスセグメントを使用した URL 全体を SensorBase ネットワーク サーバーに送信します。このオプションは、より強力なデータベースの提供を支援し、 継続的に Web レピュテーション スコアの整合性を向上させます。
- ステップ4 [AnyConnectネットワークへの参加(AnyConnect Network Participation)] フィールドで、Cisco AnyConnect クライアントを使用して Cisco Web セキュリティアプライアンス に接続するクライアントから収集された 情報を含めるかどうかを選択します。

AnyConnect クライアントは、Secure Mobility 機能を使用してアプライアンスに Web トラフィックを送信します。

- **ステップ5** [除外されたドメインと IP アドレス(Excluded Domains and IP Addresses)] フィールドで、任意でドメイン または IP アドレスを入力して、SensorBase サーバーに送信されたトラフィックを除外します。
- ステップ6 変更を送信し、保存します。

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。