製品およびリリースの概要

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 の概要

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。

AsyncOS 11.8 の新機能

機能	説明
ISE/ISE-PIC 統合の機能拡張	• セキュリティ グループ タグと Active Directory グループを使用してアクセス ポリシーを作成できます。 • ISE/ISE-PIC による透過的な識別に失敗したユーザーの場合、Active Directory ベースのレルムを使用してフォールバック認証を設定できます。 • 仮想デスクトップ環境（Citrix、Microsoft 共有/リモートデスクトップ サービス）でユーザーの認証を設定できます。 （注） 仮想デスクトップ環境（VDI）ユーザーのフォールバック認証はサポートされていません。 詳細については、Identity Services Engine（ISE）/ ISE パッシブ ID コントローラ（ISE-PIC）サービスの概要を参照してください。
ドメイン マップ	アプライアンスを設定し、クライアント要求と宛先サーバーの証明書チェックを変更せずに特定の HTTPS トラフィックのパススルーを許可できるようになりました。 詳細については、ドメイン マップを参照してください。 ドメインマップ機能に関して、アクセスログと W3C ログのオプションのフォーマット指定子が導入されました。詳細については、アクセス ログのフォーマット指定子と W3C ログ ファイルのフィールドを参照してください。
アプライアンスの設定のロールバック	新しい CLI コマンド `rollbackconfig` が追加されました。このコマンドを使用して、以前に確定された 10 の設定のいずれかにロールバックします。ロールバック設定機能は、デフォルトで有効になっています。 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。
アプライアンス設定の自動バックアップ	新しいログ タイプ「設定履歴ログ」が追加されます。このログ タイプを使用して、コンフィギュレーション ファイルをサブスクライブし、FTP または SCP を介してリモートに配置されたバックアップ サーバーに送信します。 詳細については、ログファイルのタイプおよびコンフィギュレーション履歴ログの使用を参照してください。

機能	説明
外部フィードおよびO365フィードの例外リストのサポート	[カスタムおよび外部URLカテゴリ（Custom and External URL Categories）] のフィード ファイルからサイトと正規表現を除外できます。これは、[外部ライブフィードカテゴリ（External Live Feed Category）] にのみ適用されます。 詳細については、カスタム URL カテゴリの作成および編集を参照してください。
O365 Web サービスフィードのプロキシバイパス設定	プロキシ バイパス リストには、カスタム URL カテゴリ（O365 URL）のドメイン名または IP アドレスを追加できます。カスタム URL カテゴリのドメイン名または IP アドレスを手動で追加する必要はありません。 詳細については、Web プロキシのバイパス設定（Web 要求の場合）を参照してください。
ファイル分析に向けた Cisco AMP Threat Grid クラスタリングのサポート	以下の方法で、ファイル分析に向けてスタンドアロンまたはクラスタの Cisco AMP Threat Grid アプライアンスを追加できるようになりました。 Web インターフェイスの [セキュリティサービス（Security Services）] > [ファイル レピュテーションとファイル分析（File Reputation and Analysis）] ページ。 詳細については、次を参照してください。ファイル レピュテーションと分析サービスの有効化と設定
ファイル分析に向けたしきい値の設定	許容されるファイル分析スコアのしきい値の上限を設定できるようになりました。 しきい値設定に基づいてブロックされるファイルは、詳細マルウェア保護レポートの [悪意のある受信脅威ファイル（Incoming Malicious Threat Files）] セクションで、[カスタムしきい値（Custom Threshold）] として表示されます。 詳細については、ファイル レピュテーションと分析サービスの有効化と設定を参照してください。
複数の Web カテゴリを使用した URL フィルタリングの設定	複数の URL カテゴリを使用して URL フィルタリング エンジンを設定できるようになりました。複数の URL カテゴリ機能は、アクセス ポリシーのみに適用されます。 詳細については、URL フィルタリング エンジンの設定を参照してください。

機能	説明
新しい脅威カテゴリのサポート	現在、アプライアンスには新しい 22 の脅威カテゴリがあります。新しい脅威カテゴリのリストは、新しいカテゴリが使用可能になるたびに、アプライアンスの新しい Web インターフェイスで自動的に更新されます。 詳細については、「Cisco Web Security Appliances/Cisco Email Security Appliances の URL カテゴリおよび脅威カテゴリの更新に関するリリースノート」を参照してください。

機能	説明
モニターリングおよびトラッキングのための新しい Web インターフェイス	

機能	説明
	アプライアンスには、レポートをモニターリングおよびトラッキングするための新しい Web インターフェイスが追加されました。 [モニターリング（Monitoring）] ページでは、一般的なレポートおよび脅威レポートに分類されたレポートを表示できます。 [トラッキング（Tracking）]ページでは、メッセージまたはメッセージのグループに関して、検索条件に応じて Web インターフェイスの [トラッキング（Tracking）] > [検索（Search）] ページから検索できます。ユーザー ガイドの「メッセージトラッキング」の章を参照してください。 （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。 • 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、`trailerblazerconfig` 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、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。 • 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

機能	説明
	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。 詳細については、新しい Web インターフェイスでのセキュア アプライアンス レポートを参照してください。 新しい Web インターフェイスにアクセスする方法については、次を参照してください：アプライアンス Web インターフェイスへのアクセス （9 ページ）
`trailblazerconfig` CLI コマンド	`trailblazerconfig` コマンドを使用すると、新しい Web インターフェイスで HTTP と HTTPS のポートを介して受信接続と送信接続をルーティングできます。 （注） デフォルトで、`trailblazerconfig` のCLI コマンドはアプライアンスで有効になっています。`help trailblazerconfig` コマンドを入力すると、インライン ヘルプを参照できます。 詳細については、コマンドライン インターフェイスを参照してください。

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

Web インターフェイス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、受け入れがイネーブルになっている必要があります。また、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 *1:* サポートされるブラ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

- Internet Explorer 11.0（Windows 10 のみ）
- Safari 7 以降
- Firefox（最新の安定バージョン）
- Google Chrome（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。

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。

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 キーを押すと、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 （9 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、trailerblazerconfig 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、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。
- 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）] ボタンをクリックします。

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）] ボタンをクリックします。

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。復号化された 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。