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

AsyncOS 14.0 の新機能

表 *1 : AsyncOS 14.0* の新機能

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 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。 スマート ソフトウェア ライセンシング および「Cisco SecureX および Cisco Threat Response との統合」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。アプライアンスと Cisco SecureX または Cisco Threat Response の統合を参照してください。
X-Authentication ヘッダーの消費	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、ユーザーを認証済みと見なし、認証またはユーザー 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。 「グローバル認証設定の構成」および「ユーザーとクライアント ソフトウェアの分類」を参照してください。
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。ポリシーごとの Web プロキシ カスタム ヘッダー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ー接続（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。 新しい Web インターフェイスに関する [システム ステータス（System Status）] ページ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）] ページ
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 14.0 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 （注） デフォルトでは HTTP 2.0 機能が無効になっているため、CLI コマンド `HTTP2` を使用して機能を有効にします。 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 のセッションおよび永続的な Cookie HTTP 2.0 機能では、次をサポートします。 • 最大 4,096 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。 （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 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。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

機能	説明
	ライアンス）ではサポートされていません。

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 *2:* 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。
- 指定したアプライアンスのインターフェイスホスト名を DNS サーバー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。