AsyncOS 15.2 for Cisco Secure Web Appliance リリースノート

最終更新：2025 年 3 月 25 日

Secure Web Appliance について

Cisco Secure Web Appliance 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。プロキシサーバーとして機能し、ユーザーからの Web 要求を代行受信して、要求された Web コンテンツをスキャンし、マルウェア、ウイルス、フィッシング攻撃などの潜在的な脅威を検出します。Cisco Secure Web Appliance は URL フィルタリング、ウイルス対策スキャン、レピュテーションベースのフィルタリング、高度なマルウェア防御などのさまざまなセキュリティテクノロジーを使用して、Web トラフィックのセキュリティを確保します。

最新情報

- AsyncOS 15.2.1-011（メンテナンス導入）の新機能 （2 ページ）
- AsyncOS 15.2.0-164 の新機能 （2 ページ）
- 既知の動作 （5 ページ）
- 既知の制限事項 （8 ページ）

AsyncOS 15.2.1-011（メンテナンス導入）の新機能

機能	説明
SecureX から XDR への移行	SecureX は、機能強化され、より堅牢になったプラットフォームである XDR（Extended Detection and Response）に移行しています。この移行の一環として、XDR を Cisco Secure Web Appliance と統合することが不可欠です。Cisco Secure Web Appliance と Cisco XDR 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 XDR 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 Secure Web Appliance を XDR と統合する方法の詳細については、ユーザーガイドの「Integration」の章にある「Integrating with Cisco XDR」のトピックを参照してください。

AsyncOS 15.2.0-164 の新機能

機能	説明
Cisco Secure Web Appliance 向けの M6 ハードウェアの導入	AsyncOS 15.2 リリースでは、Cisco Secure Web Appliance 向けの M6 ハードウェアが導入されています。次のハードウェアモデルがサポートされています。 • S196 • S396 • S696 • S696F 詳細については、『*Cisco Web セキュリティアプライアンス S196、S396、S696、および S696F スタートアップガイド*』および『*Cisco Web セキュリティアプライアンス S196、S396、S696、および S696F ハードウェア設置ガイド*』を参照してください。

機能	説明
Cisco Secure Web Appliance の必須スマートライセンス	AsyncOS 15.2 以降のリリースでは、スマート ソフトウェア ライセンスは必須です。スマートライセンスの導入には、次の機能が含まれます。 • Cisco Secure Web Appliance イメージを Cisco.com からインストールした場合、スマートライセンスはデフォルトで有効になります。 • システム管理者がデバイスのスマート ソフトウェア ライセンスを有効にしていない場合、AsyncOS 15.2 ビルドにアップグレードできません。 • AsyncOS 15.2 以降のリリースでは、従来のライセンスコマンドと UI オプションはサポートされていません。これらのコマンドと UI オプションは、Cisco スマートライセンスポリシーでは無効です。 詳細については、『Smart Software Licensing』を参照してください。

<table>
<tr><th>機能</th><th colspan="2">説明</th></tr>
<tr><td>Cisco Umbrella との Cisco Secure Web Appliance の統合</td><td colspan="2">Cisco Umbrella と Cisco Secure Web Appliance の統合により、Cisco Umbrella から Cisco Secure Web Appliance への共通 Web ポリシーの展開が容易になります。また、Cisco Umbrella ダッシュボードを使用してポリシーを設定したり、ログを表示したりできます。

Cisco Umbrella ダッシュボードで共通 Web ポリシーを設定すると、ポリシーは Cisco Secure Web Appliance にプッシュされます。設定したこれらの Web ポリシーのレポートデータは Cisco Umbrella に送り返され、Cisco Umbrella ダッシュボードで使用できます。レポートデータには、参照された URL、その IP アドレス、URL が許可されたかブロックされたかなどの情報が含まれます。

統合が成功すると、次の Web ポリシーが変換され、Cisco Umbrella から Cisco Secure Web Appliance にプッシュされます。
<table>
<tr><th>Cisco Umbrella から</th><th>Cisco Secure Web Appliance へ</th></tr>
<tr><td>ルールセットアイデンティティ</td><td>グローバル識別プロファイル</td></tr>
<tr><td>接続先リスト</td><td>カスタムおよび外部 URL カテゴリ</td></tr>
<tr><td>Web ポリシー（ルール）</td><td>アクセス ポリシー（Access Policies）</td></tr>
<tr><td>HTTPS 検査</td><td>復号ポリシー</td></tr>
<tr><td>Microsoft 365 の互換性</td><td>カスタムおよび外部 URL カテゴリ</td></tr>
<tr><td>ルールセットのブロックされているページの設定</td><td>ユーザ通知（End-User Notification）</td></tr>
<tr><td>アプリケーション設定（CASI）</td><td>アプリケーション アクセス ポリシー</td></tr>
<tr><td colspan="2">詳細については、「Integrate Cisco Secure Web Appliance with Cisco Umbrella」を参照してください。</td></tr>
</table>
</td></tr>
</table>

（注） AsyncOS 15.2 は連邦情報処理標準（FIPS）モードをサポートしていないため、FIPS モードを有効にした状態で AsyncOS 15.2 にアップグレードすることは推奨しません。

AsyncOS 15.2.1-011（メンテナンス導入）の動作の変更

- Cisco Secure Web Appliance は、継続的なアップデートでデータサブスクリプションをサポートするために ISE pxGrid ノードと通信します。セカンダリ ISE pxGrid ノード（サー

バー）の指定はオプションです。CLI で **iseconfig->removeisenodedetails** コマンドを使用すると、セカンダリ ISE pxGrid ノードを削除できるようになりました。

AsyncOS AsyncOS 15.2.0-164（一般導入）の動作の変更

- AsyncOS 15.2.0-164 へのアップグレード時：
  - SWA S396 モデルでは高パフォーマンスモードを有効にできます。
  - SWA S696 モデルのプロキシインスタンスが 3 から 5 に増加します。

  アプライアンスが高パフォーマンスモードになっている場合、次のスキャンエンジンは S396 モデルでは 2 インスタンス、S696 モデルでは 5 インスタンスとして複製されます。
  - Sophos
  - Mcafee
  - Merlin
  - AVC
  - アーカイブスキャン
  - AMP

（注） S396 アプライアンスでは [高パフォーマンス（High Performance）] を有効にすることを推奨します。高パフォーマンスを有効にするには、CLI コマンド **advancedproxyconfig > highperformance** を使用します。

- Cisco SecureX、Cisco Cognitive Threat Analysis（CTA）、および Cisco Cloudlock は、AsyncOS 15.2 で廃止されています。AsyncOS 15.2 にアップグレードすると、これらの機能が無効になり、Cisco Secure Web Appliance GUI から有効にすることはできなくなります。
- Cisco Secure Web Appliance のデータセンター アーキテクチャ（DCA）機能は、AsyncOS 15.0 GD のリリースに伴い無効になりました。今後のリリースではサポートされなくなります。したがって、有効にすることは推奨しません。
- Data 1 および Data 2 インターフェイスはサポートされていません。代わりに、P1 インターフェイス、P2 インターフェイス、またはその両方を使用できます。M2、Data 1、Data 2 インターフェイスのオプションは、**etherconfig** CLI では使用できません。

既知の動作

次に、このリリースの既知の動作を示します。

Cisco Secure Web Appliance AVC または ADC エンジンの既知の制限事項：アプリケーションが ADC/AVC でブロックされるように設定されている場合、アプリケーションのすべてのサブ

カテゴリもブロックされます。特定のサブカテゴリは詳細なゲイン制御機能を使用してブロックできますが、この機能は smugmug、Facebook、LinkedIn などの特定のアプリに限定されます。

Secure Web Appliance と Umbrella の統合 - ハイブリッドポリシーの既知の動作

- デフォルトでは、Secure Web Appliance の Umbrella 設定のソースインターフェイスは [管理（Management）] に設定されています。ソースインターフェイスを [データ（Data）] に変更するには、ハイブリッドポリシーを有効にする前に、変更を送信してコミットする必要があります。
- ハイブリッドポリシーは、ルールアクションの [許可（Allow）]、[ブロック（Block）]、および [警告（Warn）] でサポートされています。
- 変換は、コンテンツカテゴリ、接続先リスト、アプリケーションでサポートされています。
- AD ユーザー、AD グループ、およびパブリックネットワークに関連付けられた内部ネットワークの変換がサポートされています。
- Secure Web Appliance では、1 つのグローバルな Umbrella がプッシュした識別プロファイルが常に使用可能です。
- Secure Web Appliance の管理者によって設定されたポリシーは、Umbrella からのポリシープッシュに従って優先されます。
- 登録済みアプライアンスページでポリシープッシュが有効になっている場合、Umbrella で設定されたポリシーは、Umbrella に登録されているすべての Secure Web Appliance にプッシュされます。
- Cisco Umbrella によってプッシュされた復号ポリシーでは、Web ベースのレピュテーションスコア（WBRS）は無効になります。
- Umbrella によってプッシュされた復号ポリシーは、デフォルトでは [複合（Decrypt）] アクションに設定されています。
- [エンドユーザー通知（End-User Notification）] ページは、グローバル設定として Secure Web Appliance で常に有効になります。
- Secure Web Appliance では、[エンドユーザー通知（End-User Notification）] ページは、Umbrella の最初のルールセットで最初に選択されたブロックページにのみ設定されます。
- 最初のルールセットの選択されたブロックページの外観の変更は、3 時間ごとに変換されます。
- Umbrella によってプッシュされた識別プロファイルと顧客カテゴリでは、これらのプロファイルまたはカテゴリが Umbrella から削除されると、管理者が設定したポリシーは Secure Web Appliance 側から無効になります。
- Cisco Umbrella 組織への Cisco Secure Web Appliance 登録は、特定の組織に割り当てられたシート数に制限されています。これは、Cisco Umbrella ユーザーインターフェイスの次の

パスに表示されます。[管理者（Admin）]>[ライセンス（Licensing）]>[シート数（Number of seats）]。

- Umbrella ORG に登録されている場合は、SMA ポリシーを Secure Web Appliance にプッシュできません。
- Umbrella に統合された内部ネットワークと AD がない場合、Umbrella はプロファイル、ポリシー、およびカスタム URL カテゴリを Secure Web Appliance にプッシュできません。
- 登録およびハイブリッドサービスの有効化に使用された API キーが期限切れの場合、Umbrella でハイブリッドポリシーまたは登録された Secure Web Appliance を再度有効にするまで、接続が閉じられません。
- 次の Umbrella ルール設定は、ハイブリッド ポリシー プッシュではサポートされていません：[ルールスケジューリング（Rules Scheduling）]および[保護バイパス（Protected Bypass）]
- Secure Web Appliance が Umbrella によって管理されている場合、Secure Web Appliance にプッシュされた SMA ポリシーは受け入れられません。
- 設定の保存と読み込みの機能が、Umbrella の設定では機能しません。
- 次のルールセット設定では、変換はサポートされていません。
  - ルールセット アイデンティティ - Chromebook、G Suite OU、G Suite ユーザー、トンネル、ローミングコンピュータ、内部ネットワークのすべてのトンネル
  - テナント制御
  - ファイル分析
  - ファイルタイプ制御
  - HTTPS インスペクション - 選択的復号リストのアプリケーションのみ
  - PAC ファイル
  - SafeSearch
  - ルールセットロギング
  - SAML
  - セキュリティ設定
- Secure Web Appliance の HTTPS プロキシまたは AD レルムに加えられた変更は、Umbrella ポリシーには影響しません。
- アプリケーション設定（CASI）変換
  - ルールで選択したアプリケーション設定は、Secure Web Appliance の **[セキュリティサービス（Security Services）]** > **[使用許可コントロール（Acceptable Use Control）]** で ADC が有効になっている場合にのみ変換され、Secure Web Appliance のアクセスポリシーにプッシュされます。

- ルールでアプリケーションを選択すると、選択したアプリケーションのドメインを含むカスタム URL カテゴリがそのルールにプッシュされます。これと同じカテゴリのカスタム URL が、アクセスポリシーの [URL フィルタリング（URL Filtering）] セクションで選択され、アクションとして [モニター（Monitor）] が選択されます。
- Secure Web Appliance で使用可能で、Umbrella では使用できないアプリケーションは、グローバル設定アクションを継承します。Umbrella で使用可能で、Secure Web Appliance で使用できないアプリケーションは無視されます。
- Secure Web Appliance では、ルール内で選択されていないアプリケーションはグローバル設定を継承します。

- 選択的ポリシープッシュ
  - Umbrella Web ポリシーは、ハイブリッドポリシーの状態が [アクティブ（Active）] で、ポリシープッシュが有効になっている場合にのみ、登録済みの Secure Web Appliance にプッシュされます。
- Umbrella UI エラーメッセージ
  - 最後のポリシープッシュの失敗に関するエラーメッセージは、[登録済みアプライアンス（Registered Appliance）] ページに表示されます。最大文字数は 1024 文字です。
- Umbrella プッシュポリシーのクリーンアップ
  - Umbrella によってプッシュされたポリシーがクリーンアップされると、管理者が設定したすべてのポリシーが無効になります。

Secure Web Appliance と Umbrella の統合 - ハイブリッドレポートの既知の動作

- Secure Web Appliance のハイブリッドレポート機能は、ハイブリッドポリシーが有効になっている場合にのみ有効にできます。
- Secure Web Appliance は、Umbrella が設定したポリシーレポートデータを Umbrella ダッシュボードに送信します。
- ローカルレポートディスク容量の約 25 % がハイブリッドレポートデータの保存に使用され、Umbrella にプッシュされます。
- Secure Web Appliance がレポートデータを Umbrella にプッシュしない場合、後でデバッグするためにそれらのレポートデータのみをディスクに保存します。
- Secure Web Appliance は、その SWA に対する選択的ポリシープッシュが無効になった後でも、Umbrella ポリシーによって評価されたレポートデータを送信し続けます。ルールが Umbrella ポリシーから削除されている場合、Umbrella ポリシー レポート ダッシュボードには、それらのレコードの削除されたルールが表示されることがあります。

既知の制限事項

このリリースでは、次の既知の制限事項があります。

Cisco Secure Web Appliance と Cisco Umbrella の統合 - ハイブリッドポリシーの既知の制限事項

- 次のシナリオでは、ポリシー変換がトリガーされません。
  - ルールセットの名前の変更。
  - ルールで選択された接続先リストの名前の変更。
  - ルールで選択されたアプリケーションリストの名前の変更。
  - HTTP インスペクション中に選択された選択的復号リストの名前の変更。
  - HTTPS インスペクションに使用される選択的復号リストのカテゴリの追加または削除。
  - HTTPs インスペクションでの、カテゴリのみを含む選択的復号リストの選択。
  - ルールセットまたはルールの AD ユーザーまたはグループの追加または削除。
  - Umbrella ダッシュボードの AD の統合または削除。
- ルールセット アイデンティティが複数のルールセットで同じである場合、同じアイデンティティの最初のルールセットのみが、一貫して HTTPS インスペクション設定を変換します。
- エンドユーザー通知の [カスタム URL へのリダイレクト（Redirect to Custom URL）] テキストボックスの形式で、整形式のホスト名またはIPV4アドレスのみがサポートされます。Umbrella のブロックページで構成された他の URL 形式を Secure Web Appliance にプッシュすると、ポリシープッシュが失敗し、次のエラーメッセージが表示されます。「http/https の URL は適切なホスト名または IPv4 アドレスで構成されていなければなりません。任意でポート番号を含めることはできますが、クエリ文字列（'?...'）は含めないでください。'コード' : '400'、'説明' : '400 = 不正なリクエスト構文またはサポートされていないメソッド'。（An http/https URL must consist of a well-formed hostname or IPv4 address, may optionally include a port, but may not contain a querystring ('?...').'.", 'code': '400', 'explanation': '400 = Bad request syntax or unsupported method.'）」
- ルールセットで AD グループが選択されていて、ルールが一致しない場合、そのルールに対してアクセスポリシーが作成されません。
- Umbrella から Secure Web Appliance にプッシュされる復号ポリシーについて、選択的復号リストで選択されたカテゴリとドメインがパススルーに設定されます。定義済みおよびカスタムの URL カテゴリの場合、Secure Web Appliance でアクセスポリシーは適用されませんが、ルールは Umbrella の同じ設定に適用されます。
- Umbrella で Microsoft 365 互換性が有効になっている場合、Umbrella から Secure Web Appliance にプッシュされる復号ポリシーがパススルーに設定されます。その結果、Microsoft 365 エンドポイントのすべてのカテゴリでパススルーが有効になります。
- 信頼できる AD が Secure Web Appliance で設定されておらず、この AD に対して Umbrella レベルでグループが選択されている場合、Secure Web Appliance レベルで設定する必要があることを示すエラーメッセージが表示されます。

- ルールセットとルールで異なるマスクを持つネットワークが選択されている場合、変換はサポートされません。
- ルール全体で多数のアプリケーションが選択されている場合、Secure Web Appliance のパフォーマンスが影響を受けます。
- 冗長な設定を避けるために、ルールで個々のアプリケーションを選択するのではなく、アプリケーションリストを使用することをお勧めします。

Cisco Secure Web Appliance と Cisco Umbrella の統合 - ハイブリッドレポートの既知の制限事項

- 次のイベントが発生した場合、AD ユーザーを Cisco Umbrella 発信元 ID にマッピングできないことがあります。
  - 新しい AD ユーザーが最後のポリシープッシュ後に Cisco Umbrella ポリシーで明示的に設定されていない場合。
  - UPN DB の作成がまだ進行中の場合。UPN DB の作成は、Cisco Umbrella 組織で使用可能なユーザーの数によって異なります。たとえば、10000 ユーザーには 30 秒必要です。
  - AD ユーザー名に括弧が含まれている場合、実際の AD ユーザーがダッシュボードに表示されないことがあります。

（注） このタイプのイベントは、Secure Web Appliance の発信元 ID によって識別されます。

- フィルタリングのサポート
  - Secure Web Appliance ベースのフィルタリングでは、外部 IP アドレスのみがサポートされます。
  - 同じ管理 IP アドレスを持つ同じ組織（異なる場所）の Secure Web Appliance は、結合されたレポートデータになります。
  - LDAP/ISE/ゲストベースのアイデンティティの場合、Secure Web Appliance AD のユーザーベースのアイデンティティはサポートされていません。
- 場合によっては、レポートエントリが重複または失われることがあります。
- ハイブリッドレポートを有効または無効にすると、レポートされたヘルパーでアプリケーション障害が発生します。

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、[Secure Web Appliance をクリックして新しい外観を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 1440 x 900 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。

- Sx95/F
- Sx96/F

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
- S1000v

（注）
- アプライアンスに付属の Cisco SFP を使用します。
- AsyncOS バージョン 15.0 は、Sx90/F モデルでサポートされる最後のリリースになります。

アップグレードパス

- AsyncOS 15.2.1-011 へのアップグレード （13 ページ）
- AsyncOS 15.2.0-164 へのアップグレード （13 ページ）

AsyncOS 15.2.1-011 へのアップグレード

（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。

次のバージョンから AsyncOS 15.2.1-011 バージョンにアップグレードできます。

- 12.5.1-011
- 12.5.1-043
- 12.5.2-011
- 12.5.3-006
- 12.5.4-005
- 12.5.4-011
- 12.5.5-004
- 12.5.5-008
- 12.5.6-008
- 12.7.0-033
- 14.0.1-053
- 14.0.2-012
- 14.0.3-014
- 14.0.4-005
- 14.0.5-007
- 14.1.0-041
- 14.1.0-047
- 14.5.0-498
- 14.5.0-537
- 14.5.0-673
- 14.5.1-016
- 14.5.2-011
- 14.5.3-033
- 14.6.0-108
- 15.0.0-302
- 15.0.0-322
- 15.0.0-355
- 15.0.0-608
- 15.0.0-612
- 15.0.1-004
- 15.1.0-287
- 15.2.0-116
- 15.2.0-164

AsyncOS 15.2.0-164 へのアップグレード

（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。

次のバージョンから AsyncOS 15.2.0-164 バージョンにアップグレードできます。

- 11.8.4-004

- 12.0.1-334
- 12.0.2-004
- 12.0.2-012
- 12.0.3-005
- 12.0.3-007
- 12.0.3-503
- 12.0.4-002
- 12.0.5-011
- 12.5.1-011
- 12.5.1-043
- 12.5.2-011
- 12.5.3-006
- 12.5.4-005
- 12.5.4-011
- 12.5.5-004
- 12.5.5-008
- 12.5.6-008
- 12.7.0-033

- 14.0.1-053
- 14.0.2-012
- 14.0.3-014
- 14.0.4-005
- 14.0.5-007
- 14.1.0-041
- 14.1.0-047
- 14.5.0-498
- 14.5.0-537
- 14.5.0-673
- 14.5.1-016
- 14.5.2-011
- 14.6.0-108

- 15.0.0-302
- 15.0.0-322
- 15.0.0-355
- 15.1.0-287
- 15.2.0-116

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 『*Cisco Content Security Virtual Appliance Installation Guide*』[英語] に記載されている手順に従って仮想アプライアンスを設定します。

（注）
セキュリティサービスの更新が正常にインストールされ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バージョンの AsyncOS 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の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。

仮想アプライアンスとハードウェアの 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

- 管理者としてログインします。
- 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。

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、Secure Web Appliance 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）] のいずれかを選択します。

ステップ 4 利用可能なリストから、アップグレードを選択します。

ステップ 5 [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 6 [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 Secure Web Appliance 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。

アップグレード後に必要な重要アクション

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
```

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。新しいキーが作成されたら、ssh 経由でアプライアンスに接続し、接続を承認します。
- 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、「File Reputation Filtering and File Analysis」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、「File Reputation Filtering and File Analysis」を参照してください。

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、その影響についてのアラートがユーザーに送信されます。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 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 （19 ページ）」に示す 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

既知および修正済みの問題のリスト

- リリース 15.2.1-011 の既知および修正済みの問題 （18 ページ）
- リリース 15.2.0-164 の既知および修正済みの問題 （18 ページ）

リリース 15.2.1-011 の既知および修正済みの問題

- 修正済みの問題
- 既知の問題

リリース 15.2.0-164 の既知および修正済みの問題

- 修正済みの問題
- 既知の問題

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 Secure Web Appliance ユーザーガイド	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
Secure Web Appliance のリリースノート、ISE 互換性マトリックス、および暗号	https://www.cisco.com/c/en/us/support/security/web-security-appliance/products-release-notes-list.html
Cisco Secure Email and Web Manager と Cisco Secure Web Appliance の互換性マトリックス	https://www.cisco.com/c/dam/en/us/td/docs/security/security_management/sma/sma_all/web-compatibility/index.html
API ガイド	https://www.cisco.com/c/en/us/support/security/web-security-appliance/products-programming-reference-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、他のシスコユーザー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、Cisco TAC にお問い合わせください。TAC に連絡する前に、仮想ライセンス番号（VLN）番号を準備してください。

Cisco TAC：

http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html。

従来の IronPort のサポート サイト：

http://www.cisco.com/web/services/acquisitions/ironport.html。

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、『Cisco Secure Web Appliance User Guide』の「Troubleshooting」セクションを参照してください。

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

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。

© 2024 Cisco Systems, Inc. All rights reserved.

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。