AsyncOS 11.5.x for Cisco Web Security Appliances リリース ノート

発行日:2019 年 7 月 31 日

改訂:2021 年 2 月 2 日

目次

Cisco Systems, Inc.
www.cisco.com

最新情報

AsyncOS 11.5.3-016 の新機能：MD（メンテナンス導入）

このリリースには複数のバグ修正が含まれています。詳細については、「既知および修正済みの問題（22 ページ）」を参照してください。

AsyncOS 11.5.2-020 の新機能：MD（メンテナンス導入）

機能	説明
差分更新の有効化または無効化	CLI コマンド `updateconfig > setup` を使用して、Web レピュテーション サービスからの差分更新を有効または無効にできます。差分更新を無効にすると、アプライアンスはシスコのサーバから更新全体をダウンロードし続けます。 **（注）** 差分更新を無効にすると、アプライアンスで更新された Web レピュテーション情報の受信に遅延が発生します。 詳細については、ユーザ ガイドの「Web Security Appliance CLI Commands」の章を参照してください。
管理ポートでのアウトバウンド ACL のサポート	管理ポート上の IP アドレスを制限する新しいサブコマンド OUTBOUNDACL が CLI コマンド `fipsconfig` に追加されています。 このサブコマンドを使用して、アプライアンスがアウトバウンド接続を行わないように制限する IP アドレスを設定できます。このサブコマンドは、FIPS モードでのみ使用できます。 サブコマンド OUTBOUNDACL を使用して、次のアクションを実行できます。 • 新規追加 • 編集 • 削除 • クリア

機能	説明
ログイン履歴の設定のサポート	ログイン履歴を保持する日数を設定するため、新しいサブコマンド LOGINHISTORY が CLI コマンド `adminaccessconfig` に追加されています。デフォルト値は 1 日です。 これは FIPS モードと非 FIPS モードの両方で使用可能です。
最大同時ログイン セッションをサポートするためのサポート	コマンドライン インターフェイスや Web インターフェイスを使用したアプライアンスの同時セッションの最大数を設定するため、新しいサブコマンド `maxsessions` が CLI コマンド `adminaccessconfig` に追加されます。 FIPS モードのデフォルト値は 3 で、非 FIPS モードの場合は 10 です。 これは FIPS モードと非 FIPS モードの両方で使用可能です。
WBRS の機能拡張	現在、WBRS の更新が失敗すると、工場出荷時のデフォルト設定に戻ります。 新しい WBRS の機能拡張により、更新プロセス中に WBRS の更新に失敗した場合、またはファイルのダウンロードに失敗した場合、WBRS は以前のバージョンに戻ります。工場出荷時のデフォルト設定に戻ることはありません。

このリリースには複数のバグ修正が含まれています。詳細については、「既知および修正済みの問題（22 ページ）」を参照してください。

AsyncOS 11.5.1-125 の新機能：GD（一般導入）更新

このリリースには複数のバグ修正が含まれています。詳細については、「既知および修正済みの問題（22 ページ）」を参照してください。

AsyncOS 11.5.1-124 の新機能：GD（一般導入）更新

機能	説明
Office 365 Web サービスの外部 URL カテゴリ	URL と IP を提供する Microsoft Office 365 Web サービスの外部ライブ フィードを使用してアプライアンスを設定できます。Web サービス URL には *ClientRequestId* が含まれていてはならず、JSON 形式である必要があります。 ユーザ ガイドの「Classify URLs for Policy Application」の章を参照してください。

AsyncOS 11.5.1-115 の新機能：GD（一般導入）

機能	説明
Web トラフィック タップ	お使いのアプライアンスを、アプライアンスをパス スルーする HTTP および HTTPS Web トラフィックにタップするように設定でき、リアル タイム データ トラフィックとともに Web セキュリティ アプライアンス インターフェイスにインラインでコピーできます。お客様が定義したポリシー フィルタに基づいてトラフィックにタップできます。選択されたタップ インターフェイスは、分析、調査、およびアーカイブのため、外部のセキュリティ デバイスに接続する必要があります。 ユーザ ガイドの「Perform System Administration Tasks」の章を参照してください。 概要レポートのページには、4 つの新しいセクションが含まれています。セクションは次のとおりです。 • Web トラフィック タップ ステータス • Web トラフィック タップ サマリ • タップされた HTTP/HTTPS トラフィック • タップされたトラフィック サマリ ユーザ ガイドの「Web Security Appliance Reports」の章を参照してください。
AMP キャッシュ消去	クリーンなファイル、悪意のあるファイル、不明なファイルについて、AMP ファイル レピュテーションの判定結果のキャッシュを消去できるようになりました。 ユーザ ガイドの「Configuring Security Services」の章を参照してください。
ファイル分析用の AMP アップストリームのプロキシ設定	ファイル分析用のアップストリームのプロキシを設定できるようになりました。 ユーザ ガイドの「File Reputation Filtering and File Analysis」の章を参照してください。
Cisco Threat Grid 分析用圧縮ファイルの送信サポート	Cisco Threat Grid 分析用の圧縮ファイルを、解凍せずに送信できるようになりました。送信されるファイルの数を削減することにより、効率性が向上します。 ユーザ ガイドの「File Reputation Filtering and File Analysis」の章を参照してください。
ハイ アベイラビリティ クラスタの Kerberos サポート	ハイ アベイラビリティ クラスタ内のすべてのアプライアンスに対して Kerberos 認証を有効にするには、Active Directory レルムを作成または編集する際に、[Kerberos ハイアベイラビリティ（Kerberos High Availability）] セクションの [キータブ認証を使用（Use keytab authentication）] オプションを使用します。 ユーザ ガイドの「Acquire End-User Credentials」の章を参照してください。

機能	説明
HTTP パッチ要求のサポート	Cisco Web セキュリティ アプライアンスに新しい CLI コマンド `httppatchconfig` が追加されました。このコマンドを使用して、発信 HTTP パッチ要求を有効または無効にできます。 ユーザ ガイドの「Command Line Interface」の章を参照してください。
仮想アプライアンスの機能拡張	Cisco Web セキュリティ仮想アプライアンスを VMware vSphere ハイパーバイザ (ESXi) 6.5 に導入できるようになりました。 詳細については、次のリンクから利用できる『*Cisco Content Security Virtual Appliance Installation Guide*』を参照してください。 https://www.cisco.com/c/ja_jp/support/security/web-security-appliance/products-installation-guides-list.html
拡張機能	
Kerberos の認証	BASIC、NTLMSSP、および NEGO の Kerberos 認証ヘルパーを 5 ～ 21 の範囲内の数値で設定する新しい CLI コマンド `modifyauthhelpers` が追加されます。

AsyncOS 11.5.0-614 の新機能：LD（限定導入）

機能	説明
Cisco Cloudlock に固有の W3C ログ	シスコの Cloudlock ポータルに W3C アクセス ログを送信するようお使いのアプライアンスを設定し、分析とレポーティングに役立てることができます。これらのカスタム W3C ログを使用すると、顧客の SaaS 利用状況がさらに把握しやすくなります。Cisco Cloudlock は、クラウド ネイティブ CASB およびサイバー セキュリティ プラットフォームであり、Software-as-a-Service、Platform-as-a-Service、および Infrastructure-as-a-Service の全体にわたってユーザ、データ、およびアプリケーションを保護します。 ユーザガイドまたはオンラインヘルプの「Monitor System Activity Through Logs」の章を参照してください。
Cisco CTA に固有の W3C ログの機能拡張	アプライアンスの Web インターフェイスで新しい [Cisco Cognitive Threat Analytics] ページを使用して CTA に固有のカスタム W3C ログを設定し、分析のために CTA ポータルに送信できるようになりました。 新しいログ フィールド（*r-ip*）が CTA log のデフォルト フィールドとして追加されます。これにより、アップストリーム展開の場合に Web サイトの IP アドレスを含めることができます。 ログのユーザ名、IP アドレス、およびユーザ グループ フィールドの値を非特定化することも選択できます。そうすることにより、ログがプッシュされる CTA のような外部システムでクライアント関連の情報が開示されなくなります。 ユーザガイドまたはオンラインヘルプの「Monitor System Activity Through Logs」の章を参照してください。

機能	説明
スケジュール設定されたポリシーの有効期限	アクセス ポリシーと復号化ポリシーの有効期限を設定できるようになりました。設定期限を越えると、ポリシーは自動的に無効になります。有効期限の 3 日前と、有効期限の当日にアラートを受信します。 ユーザ ガイドまたはオンライン ヘルプの「Create Policies to Control Internet Requests」および「Perform System Administration Tasks (for alerts)」の章を参照してください。
ユーザ数レポート	[ユーザ数（User Count）] ページには、アプライアンスの認証されたユーザと認証されていないユーザの合計に関する情報が表示されます。 ユーザ ガイドまたはオンライン ヘルプの「Web Security Appliance Reports」の章を参照してください。
W3C ログ フィールドの 非特定化と特定化	W3C ログのユーザ名、IP アドレス、およびユーザ グループ フィールドの値を非特定化することも選択できるようになりました。そうすることにより、ログがプッシュされる外部システムで、クライアント関連の情報が開示されなくなります。 非特定化されたログ フィールド値の実際の値を表示するには、特定化機能を使用して、フィールド値を特定する必要があります。 ユーザガイドまたはオンラインヘルプの「Monitor System Activity Through Logs」の章を参照してください。
IPv6 アドレスの機能拡張	Cisco Web セキュリティ アプライアンスは、次のプロトコルの IPv6 アドレスをサポートしています。 • NTP • RADIUS • Syslog • SNMP

機能	説明
AMP for Endpoints コンソールの統合	アプライアンスを AMP for Endpoints コンソールと統合し、独自のファイル SHA をブロックリストまたは許可リストに追加できるようになりました。 統合後に、ファイル SHA がファイル レピュテーション サーバに送信されると、ファイル SHA に対してファイル レピュテーション サーバから得られた判定は、AMP for Endpoints コンソールの同じファイル SHA に対してすでに利用可能な判定により上書きされます。 アプライアンスを AMP for Endpoints コンソールと統合するには、ユーザ ガイドの「Configuring Security Services」の章を参照してください。 [高度なマルウェア防御レポート（Advanced Malware Protection Report）] ページに、AMP for Endpoints コンソールから受信したブロックリストのファイル SHA の割合を表示するための新しいセクション [カテゴリ別受信マルウェア ファイル（Incoming Malware Files by Category）] が含まれるようになりました。ブロックリストのファイル SHA の脅威名は、レポートの [マルウェア脅威ファイル（Malware Threat Files）] セクションに [シンプルカスタム検出（Simple Custom Detection）] として表示されます。 ユーザ ガイドまたはオンライン ヘルプの「File Reputation Filtering and File Analysis」の章を参照してください。
高度な SSL のデバッグ	Cisco Web セキュリティ アプライアンスに OPENSSL コマンド ツール `ssltool` が含まれるようになりました。このコマンドはアプライアンスの CLI から別の OPENSSL コマンドを実行し、SSL 接続のトラブルシューティングを行います。管理者は、このコマンドを使用して HTTPS/SSL/TLS の問題をデバッグすることができます。 ユーザ ガイドまたはオンライン ヘルプで「Command Line Interface」の章を参照してください。
ネットワーク インターフェイス カード（NIC）ペアリングのサポート	新しいサブコマンド `pairig` が、NIC ペアリングを表示および設定するためのメイン CLI コマンド `etherconfig` に追加されます。 NIC ペアリングのサポートは、ハードウェア デバイスでのみ使用できます。
ファイル レピュテーション判定結果値のキャッシュ有効期間	Web インターフェイスの [セキュリティサービス（Security Services）] > [アンチマルウェアおよび評価（Anti-Malware and Reputation）] > [高度なマルウェア防御サービス（Advanced Malware Protection Services）] > [詳細（Advanced）] > [キャッシュの詳細設定（Advanced Settings for Cache）] ページでファイル レピュテーション判定結果値のキャッシュ有効期間を設定できます。

機能	説明
Amazon Web Services（AWS）の仮想アプライアンスのサポート	Amazon Web Services（AWS）の Amazon Elastic Compute Cloud（EC2）に、Cisco Web セキュリティ仮想アプライアンスおよびセキュリティ管理仮想アプライアンスを導入できます。 **（注）** L4 トラフィック モニタ機能はサポートされていません。 Cisco Web セキュリティ仮想アプライアンス（AsyncOS 11.5.0 614）の AMI ID を次に示します。 S100V-coeus-11-5-0-614-S100V-AMI-110518 S300V-coeus-11-5-0-614-S300V-AMI-120518 S600V-coeus-11-5-0-614-S600V-AMI-120518 『Deploying Cisco Web Security and Security Management Virtual Appliances on Amazon Elastic Compute Cloud on Amazon Web Services』ガイドを参照してください。ガイドの場所については、「関連資料（24 ページ）」を参照してください。
AsyncOS 11.5. for Cisco Web Security Appliances の暗号リスト	AsyncOS 11.5. for Cisco Web Security Appliances のサポート対象とサポート対象外の暗号（SSL および SSH）の一覧を示した新しいドキュメントが利用できるようになりました。 https://www.cisco.com/c/en/us/support/security/web-security-appliance/products-release-notes-list.html を参照してください。
拡張機能	
DNS 設定の更新	新しい CLI コマンド `advancedproxyconfig->miscellaneous->Do you want to disable IP address in Host Header?` が、ホストヘッダーの IP アドレスをブロックするために追加されます。
プロキシ要求の URL サイズの設定	CLI コマンド *`maxhttpheadersize`* を使用して、プロキシ要求の最大 URL サイズを設定できます。
SSH の設定	CLI コマンド `sshconfig` には、次のサブコマンドが追加されています。 • `Incomplete SSH session timeout (in secs)` デフォルト値は 60 です。 • `Unsuccessful SSH login attempts allowed` デフォルト値は 3 です。
FIPS モード更新	• FIPS モードで許可されている同時セッションの最大数は 3 です。 • 非 FIPS モードで許可されている同時セッションの最大数は 10 です。

動作における変更

AsyncOS 11.5.1 の動作の変更

Microsoft Office 365 フィード形式の外部 URL カテゴリ	Office 365 免除を提供する Microsoft Office 365 フィード形式の外部 URL カテゴリは、XML フィードから Web Representational State Transfer（REST）API ベースの形式への Microsoft 移行が原因で 2018-10-02 以降には更新できない場合があります。Web セキュリティ アプライアンス用 AsyncOS 11.7.0-330 は、Microsoft Office 365 Web サービスをサポートしています。
Web トラフィック タップ範囲の要求	範囲ヘッダーを含む要求があるすべてのトランザクションは、応答ヘッダーが完了するまでタップされます。 応答本文はタップされません。アクセスログには、これを示す TAP_UNSUP_RREQ エラーコードが含まれます。
ログ サブスクリプション名	ログ サブスクリプション名の非 ASCII 文字はサポートされていません。

AsyncOS 11.5.0 の動作の変更

セキュア認証証明書の検証	アップグレードの実行中、セキュア認証の証明書が FIPS 準拠でない場合は、アプライアンスのアップグレードされる最新パスのデフォルトの証明書で置き換えられます。これは、お客様がアップグレードの前にデフォルトの証明書を使用した場合にのみ起こります。
アップグレード中のサポートされていない暗号方式の削除	サポートされていない暗号とホストキーは、10.5 より前のリリースからアップグレードを実行すると削除されます。https://www.cisco.com/c/en/us/support/security/web-security-appliance/products-release-notes-list.html を参照してください。
DNS 設定の更新	CLI でサブコマンド *`advancedproxyconfig->dns->Find web server by`* について、デフォルト値が 1 から 0 に変更されます。
SSH の設定	失敗した SSH ログイン試行回数のデフォルト値が、6 から 3 に変更されます。 CLI コマンド `sshconfig` の次のサブコマンドを使用して、デフォルト値を変更できます。 • `Unsuccessful SSH login attempts allowed`
ユーザ ネットワーク アクセス	アプライアンスの Web インターフェイスで *System Administration* > *Network Access* を介して IP を追加しようとすると、アプライアンスの IP アドレスが自動的にアクセス リストに追加されます。

tail コマンド	ログ ファイルの末尾を表示します。コマンドは、ログ ファイル名をパラメータとして受け入れます。コマンドが変更され、「Press Ctrl-C」でスクロールを停止し、次に「q」で終了するようになります。 例 1 example.com> tail Currently configured logs: 1. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll 2. "amp_logs" Type: "AMP Engine Logs" Retrieval: FTP Poll … … Enter the number of the log you wish to tail. []> 9 Press Ctrl-C to stop scrolling, then `q` to quit. ~ ~ Thu Dec 14 10:03:07 2017 Info: Begin Logfile ~ … "CTRL-C" + "q" 例 2 example.com> tail system_logs Press Ctrl-C to stop scrolling, then `q` to quit. ~ ~ Thu Dec 14 9:59:10 2017 Info: Begin Logfile … … "CTRL-C" + "q"

Cisco Defense Orchestrator モードでの設定の変更と制約

このセクションでは、デバイスを Cisco Defense Orchestrator にオンボードした後に、アプライアンスと Cisco Defense Orchestrator の変更と制約を指定します。

以下に示す制約を除き、アプライアンスの Web インターフェイスでの制約はありません。Cisco Defense Orchestrator からの認証はサポートされていません。

リリース 11.5 では、Cisco Defense Orchestrator は、Web セキュリティ アプライアンスのグローバルおよび非グローバル アクセス ポリシーのポリシー管理のみをサポートしています。その他のすべての設定（認証を含む）にアプライアンスの Web インターフェイスを使用します。

（注） 制約は、アクセス ポリシーとレポートにのみ適用されます。

オンボーディング後の Web セキュリティ アプライアンスでの制約:

アプライアンスでは、Cisco Defense Orchestrator から管理される機能は設定できません。アプライアンスのオンボーディング時に、これらの機能の設定が Cisco Defense Orchestrator に移行されます。アプライアンスのその他の設定はデフォルトに設定されます。

Cisco Defense Orchestrator から管理される機能を除き、その他のすべての機能はアプライアンスで使用可能になります。

オンボーディング後は、アクセス ポリシーは Cisco Defense Orchestrator から制御されます。以下に例外を示します。次のアクセス ポリシー機能は Web セキュリティ アプライアンスだけで設定できます。

- アクセス ポリシー:ポリシー定義
  - プロトコルとユーザエージェント(Protocols and User Agents)
  - マルウェア対策とレピュテーション(Anti-Malware and Reputation)
- カスタム URL カテゴリ(外部ライブ フィード カテゴリ)(Custom URL Categories (External Live Feed Category))

次の機能は Cisco Defense Orchestrator でのみ設定できます。

- カスタム URL カテゴリ(ローカル カスタム カテゴリ):この機能は間もなく使用可能になる予定です。
- URL フィルタリング、アプリケーション、およびオブジェクト(サイズおよびカスタム MIME タイプを除く)
- グローバル アクセス ポリシーと非グローバル アクセス ポリシー
- アクセス ポリシーでは次の操作がサポートされています。
  - 複数のアクセス ポリシーの追加がサポートされています。
  - アクセス ポリシーの追加、並べ替え、削除がサポートされています。
  - URL フィルタリング(定義済み URL カテゴリ フィルタリング)、アプリケーション、およびオブジェクト(オブジェクト タイプ)には次の制限があります。
  - アプリケーションとアプリケーション タイプの帯域幅制限はサポートされていません。
  - オブジェクト サイズ、カスタム MIME タイプはサポートされていません。
  - アーカイブ済みオブジェクトの場合、検査はサポートされていません。
  - アクセス ポリシーとアイデンティティの詳細なメンバーシップ定義はサポートされていません。
  - 範囲要求転送はサポートされていません。
  - 時間とボリュームのクォータ管理はサポートされていません。
  - URL でのセーフ サーチ、参照例外、サイト コンテンツ レーティングはサポートされていません。

Cisco Defense Orchestrator でのレポートが有効な場合は次のようになります。

- Cisco Defense Orchestrator で要約レポートが使用可能になります。
- Web セキュリティ アプライアンスでもレポート機能が使用可能になります。
- セキュリティ管理アプライアンスではレポート機能は使用可能になりません。

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

次のモデルがあります。

- S000V
- S100V
- S300V
- S600V
- x90
- x80
- x70（Cisco Web セキュリティ アプライアンス S170 はサポートされていません）。

一部のハードウェアモデルでは、この AsyncOS リリースをインストールまたはアップグレードする前に、メモリをアップグレードする必要があります。詳細については、http://www.cisco.com/c/en/us/support/docs/field-notices/638/fn63931.html を参照してください。

アップグレードの方法

（注） アップグレード プロセスを開始する前に、「アップグレード前の要件（15 ページ）」と「インストールおよびアップグレードに関する注意事項（16 ページ）」を参照してください。

- 11.5.3 016 のアップグレード パス：MD（メンテナンス導入）（13 ページ）
- 11.5.2-020 のアップグレード パス：MD（メンテナンス導入）（13 ページ）
- 11.5.1-125 のアップグレード パス：GD（一般導入）更新（14 ページ）
- 11.5.1-124 のアップグレード パス：GD（一般導入）更新（14 ページ）
- 11.5.1-115 のアップグレード パス：GD（一般導入）（14 ページ）
- 11.5.0-614 のアップグレード パス：LD（限定的な導入）（15 ページ）

11.5.3 016 のアップグレード パス：MD（メンテナンス導入）

次のバージョンから AsyncOS 11.5.x for Cisco Web Security Appliances リリース 11.5.3-016 にアップグレードできます。

- 10.1.3-039
- 10.1.4-007
- 10.1.4-017
- 10.5.1-296
- 10.5.2-072
- 10.5.3-025
- 10.5.4-018
- 11.5.0-614
- 11.5.1-125
- 11.5.2-020
- 11.5.3-007

11.5.2-020 のアップグレード パス：MD（メンテナンス導入）

次のバージョンから AsyncOS 11.5.x for Cisco Web Security Appliances リリース 11.5.2-020 にアップグレードできます。

- 10.1.1-235
- 10.1.3-039
- 10.1.3-054
- 10.1.4-007
- 10.1.4-017
- 10.5.1-296
- 10.5.2-072
- 10.5.3-025
- 10.5.4-018
- 11.5.0-614
- 11.5.1-125

11.5.1-125 のアップグレード パス：GD（一般導入）更新

次のバージョンから AsyncOS 11.5.x for Cisco Web Security Appliances リリース 11.5.1-125 にアップグレードできます。

- 9.1.1-074
- 9.1.2-022
- 9.1.3-024
- 10.1.1-235
- 10.1.3-039
- 10.1.3-054
- 10.5.1-296
- 10.5.2-072
- 11.0.0-641
- 11.5.0-476
- 11.5.0-614
- 11.5.1-115
- 11.5.1-124

11.5.1-124 のアップグレード パス：GD（一般導入）更新

次のバージョンから AsyncOS 11.5.x for Cisco Web Security Appliances リリース 11.5.1-124 にアップグレードできます。

- 9.1.1-074
- 9.1.2-022
- 9.1.3-024
- 10.1.1-235
- 10.1.3-039
- 10.1.3-054
- 10.5.1-296
- 10.5.2-042
- 10.5.2-061
- 10.5.2-072
- 11.0.0-641
- 11.5.0-476
- 11.5.0-614
- 11.5.1-115

11.5.1-115 のアップグレード パス：GD（一般導入）

次のバージョンから AsyncOS 11.5.x for Cisco Web Security Appliances リリース 11.5.1-115 にアップグレードできます。

- 9.1.1-074
- 9.1.2-022
- 9.1.3-024
- 10.1.1-235
- 10.1.3-039
- 10.1.3-054
- 10.5.1-296
- 10.5.2-042
- 10.5.2-061
- 10.5.2-072
- 11.0.0-641
- 11.5.0-476
- 11.5.0-614
- 11.5.1-102
- 11.5.1-105

11.5.0-614 のアップグレード パス：LD（限定的な導入）

次のバージョンから AsyncOS 11.5.x for Cisco Web Security Appliances リリース 11.5.0-614 にアップグレードできます。

- 9.1.2-022
- 9.1.3-024
- 10.1.1-235
- 10.1.2-050
- 10.5.1-296
- 10.5.2-042
- 11.0.0-641
- 11.5.0-476

アップグレード前の要件

- CTA ログ サブスクリプションを使用した以前のバージョンの AsyncOS から AsyncOS 11.5 へのアップグレード（15 ページ）
- Cloudlock ログ サブスクリプションを使用した以前のバージョンの AsyncOS から AsyncOS 11.5 へのアップグレード（16 ページ）
- アップグレードの前にアップグレード後の要件を確認（16 ページ）

CTA ログ サブスクリプションを使用した以前のバージョンの AsyncOS から AsyncOS 11.5 へのアップグレード

- AsyncOS 11.0 から 11.5 へのアップグレード（15 ページ）
- AsyncOS 11.0 より前のリリースから 11.5 へのアップグレード（16 ページ）

AsyncOS 11.0 から 11.5 へのアップグレード

AsyncOS 11.0 バージョンで CTA ログをすでに設定している場合に AsyncOS 11.5 バージョンにアップグレードするには、次の条件を満たす必要があります。

- ログ名が「cta_log」であること。
- ログの取得方法が「scp_push」であること。
- [CTA が有効（CTA Enable）] チェックボックスがオンになっていること。11.5 バージョンにアップグレードした後でのみ、CTA ログと見なされます。
- 上記の条件のいずれかが満たされていない場合、アップグレード後にログは標準ログと見なされます。

AsyncOS 11.0 より前のリリースから 11.5 へのアップグレード

AsyncOS 11.0 より前のリリースで CAT ログをすでに設定している場合に AsyncOS 11.5 バージョンにアップグレードするには、次の条件を満たす必要があります。

- ログ名が「cta_log」であること。
- ログの取得方法が「scp_push」であること。11.5 バージョンにアップグレードした後でのみ、CTA ログと見なされます。
- 上記の条件のいずれかが満たされていない場合、アップグレード後にログは標準ログと見なされます。

Cloudlock ログ サブスクリプションを使用した以前のバージョンの AsyncOS から AsyncOS 11.5 へのアップグレード

AsyncOS の以前のリリースで Cloudlock ログをすでに設定している場合に AsyncOS 11.5 バージョンにアップグレードするには、次の条件を満たす必要があります。

- ログ名が「cloudlock_log」であること。
- ログの取得方法が「scp_push」であること。11.5 バージョンにアップグレードした後でのみ、Cloudlock ログと見なされます。
- 上記の条件のいずれかが満たされていない場合、アップグレード後にログは標準的な W3C ログと見なされます。

アップグレードの前にアップグレード後の要件を確認

既存の機能の中には、変更を加えるまではアップグレード後に機能しないものがあります。ダウンタイムを最小限に抑えるため、アップグレード前にこれらの要件について理解し、準備します。「重要:アップグレード後に必要なアクション」を参照してください。

インストールおよびアップグレードに関する注意事項

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

ステップ 1 「仮想アプライアンスの展開(18 ページ)」で説明されているマニュアルを使用して、この AsyncOS リリースで仮想アプライアンスをセットアップします。

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。

デモ セキュリティ証明書の暗号化の強度

デモ セキュリティ証明書の暗号化強度は、AsyncOS 8.5 へのアップグレードの前後で 1024 ビットです。AsyncOS 9.1.1 へアップグレードすると、2048 ビットになります。AsyncOS 10.5 以降では、FIPS モードが有効になっている場合、デモ セキュリティ証明書の強度は 4096 ビットに変更されます。

アップグレード後の再起動

アップグレード後に Web Security Appliance を再起動する必要があります。

AsyncOS for Web のアップグレード

はじめる前に

アップグレード前の要件を満たします。「アップグレード前の要件（15 ページ）」を参照してください。

ステップ 1 管理者としてログインします。

ステップ 2 [システム管理（System Administration）] > [設定ファイル（Configuration File）] ページで、Web Security Appliance から XML コンフィギュレーション ファイルを保存します。

ステップ 3 [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（Upgrades Options）] をクリックします。

ステップ 4 必要に応じて、[ダウンロード（Download）] または [ダウンロードとインストール（Download and Install）] を選択します。

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 5 [続行（Proceed）] をクリックして、アップグレードまたはダウンロードを開始します。表示される質問に答えます。

[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）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、Web Security 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。

通常、デフォルトでは新しい機能は有効になっていません。

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

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:!EXPORT:!3DES:!RC4:!RC2:!DES:!SEED:!CAMELLIA:!SRP:!IDEA:!ECDHE-ECDSA-AES256-SHA:!ECDHE-RSA-AES256-SHA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA
```

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。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150625-ironport に示されているセキュリティの脆弱性がアプライアンスに存在していれば、アップグレード時に修正されます。

(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、高度なマルウェア保護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

ユーザ ガイドの PDF は、オンライン ヘルプよりも最新のものである場合があります。この製品のユーザ ガイドの PDF 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(24 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

シスコのバグ検索ツールを使用して、このリリースの既知および修正済みの不具合に関する情報を検索します。

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://tools.cisco.com/RPF/register/register.do 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 11.5.3-016 の既知および修正済みの問題

修正済みの問題	https://bst.cloudapps.cisco.com/bugsearch? kw = * & pf = prdNm & pfVal = 282521310 & rls = 11.5.3-016 & sb = fr & svr = 3nH & bt = custV
既知の問題	https://bst.cloudapps.cisco.com/bugsearch?kw=*&pf=prdNm&pfVal=282521310&rls=11.5.3&sb=afr&sts=open&svr=3nH&bt=custV

リリース 11.5.2-020 の既知および修正済みの問題

修正済みの問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.5.2-020&sb=fr&svr=3nH&bt=custV
既知の問題	https://bst.cloudapps.cisco.com/bugsearch/searchkw=*&pf=prdNm&pfVal=282521310&rls=11.5.2&sb=afr&sts=open&svr=3nH&bt=custV

リリース 11.5.1-125 の既知および修正済みの問題

修正済みの問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.5.1-125&sb=fr&svr=3nH&bt=custV
既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.5.1&sb=afr&sts=open&svr=3nH&bt=custV

リリース 11.5.1-124 の既知および修正済みの問題

修正済みの問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.5.1-124&sb=fr&svr=3nH&bt=custV
既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.5.1&sb=afr&sts=open&svr=3nH&bt=custV

リリース 11.5.1-115 の既知および修正済みの問題

修正済みの問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.5.1-115&sb=fr&svr=3nH&bt=custV
既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.5.1&sb=afr&sts=open&svr=3nH&bt=custV

リリース 11.5.0-614 の既知および修正済みの問題

修正済みの問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.5.0-614&sb=fr&svr=3nH&bt=custV
既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.5.0&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。

はじめる前に

シスコ アカウントを持っていない場合は、登録します。https://tools.cisco.com/RPF/register/register.do 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(Release)] フィールドに、リリースのバージョン(たとえば、11.5.1)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、[バグの表示(Show Bugs)] 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、[バグの表示(Show Bugs)] 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

この製品のドキュメントは http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html から入手できます。

仮想アプライアンスのドキュメントは、次の URL から入手できます。

https://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html

Cisco コンテンツ セキュリティ管理アプライアンスのドキュメントは http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html から入手できます。

AsyncOS 11.5. for Cisco Web Security Appliances の暗号リストは次の URL から入手できます。

https://www.cisco.com/c/en/us/support/security/web-security-appliance/products-release-notes-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://community.cisco.com/t5/web-security/bd-p/5786-discussions-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

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。