



## Cisco Secure Firewall ASA の概要

Cisco Secure Firewall ASA は、高度なステートフル ファイアウォールおよび VPN コンセントレータ機能を 1 つのデバイスで提供します。ASA は、複数のセキュリティ コンテキスト（仮想ファイアウォールに類似）、クラスタリング（複数のファイアウォールを 1 つのファイアウォールに統合）、トランスペアレント（レイヤ 2）ファイアウォールまたはルーテッド（レイヤ 3）ファイアウォールオペレーション、高度なインスペクションエンジン、IPsec VPN、SSL VPN、クライアントレス SSL VPN サポートなど、多数の高度な機能を含みます。



(注) ASDM では、多数の ASA バージョンをサポートしています。ASDM のマニュアルおよびオンライン ヘルプには、ASA でサポートされている最新機能がすべて含まれています。古いバージョンの ASA ソフトウェアを実行している場合、ご使用のバージョンでサポートされていない機能がこのマニュアルに含まれている場合があります。各章の機能履歴テーブルを参照して、機能がいつ追加されたかを確認してください。ASA の各バージョンでサポートされている ASDM の最小バージョンについては、『Cisco ASA Compatibility (Cisco ASA の互換性)』[英語]を参照してください。特殊なサービス非推奨のサービスおよびレガシーサービス (20 ページ) も参照してください。

- [ASDM 要件 \(2 ページ\)](#)
- [ハードウェアとソフトウェアの互換性 \(9 ページ\)](#)
- [VPN の互換性 \(10 ページ\)](#)
- [新機能 \(10 ページ\)](#)
- [ファイアウォール機能の概要 \(14 ページ\)](#)
- [VPN 機能の概要 \(18 ページ\)](#)
- [セキュリティ コンテキストの概要 \(19 ページ\)](#)
- [ASA クラスタリングの概要 \(19 ページ\)](#)
- [特殊なサービス非推奨のサービスおよびレガシー サービス \(20 ページ\)](#)

# ASDM 要件

## ASDM Java の要件

ASDM は、Oracle JRE 8.0 (**asdm-version.bin**) または OpenJRE 1.8.x (**asdm-openjre-version.bin**) を使用してインストールできます。



(注) ASDM は Linux ではテストされていません。

表 1: ASDM オペレーティングシステムとブラウザの要件

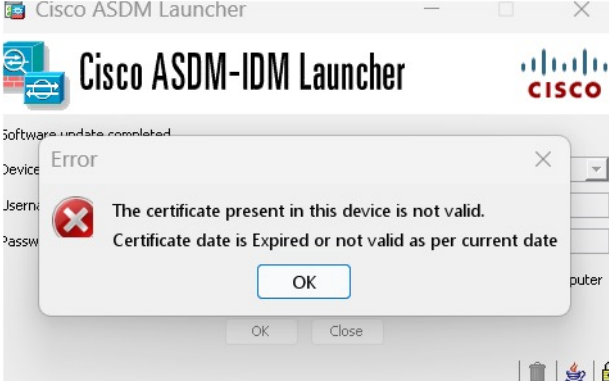
オペレーティング システム	ブラウザ			Oracle JRE	OpenJRE
	Firefox	Safari	Chrome		
Microsoft Windows (英語および日本語) : <ul style="list-style-type: none"> <li>• 11</li> <li>• 10</li> </ul> (注) ASDM ショートカットに問題がある場合は、 <a href="#">ASDM の互換性に関する注意事項 (3 ページ)</a> の「Windows 10」を参照してください。 <ul style="list-style-type: none"> <li>• 8</li> <li>• 7</li> <li>• Server 2016 と Server 2019</li> <li>• Server 2012 R2</li> <li>• Server 2012</li> <li>• Server 2008</li> </ul>	対応	サポートなし	対応	8.0 バージョン 8u261 以降	1.8 (注) Windows 7 または 10 (32 ビット) のサポートなし
Apple OS X 10.4 以降	対応	対応	対応 (64 ビットバージョンのみ)	8.0 バージョン 8u261 以降	1.8

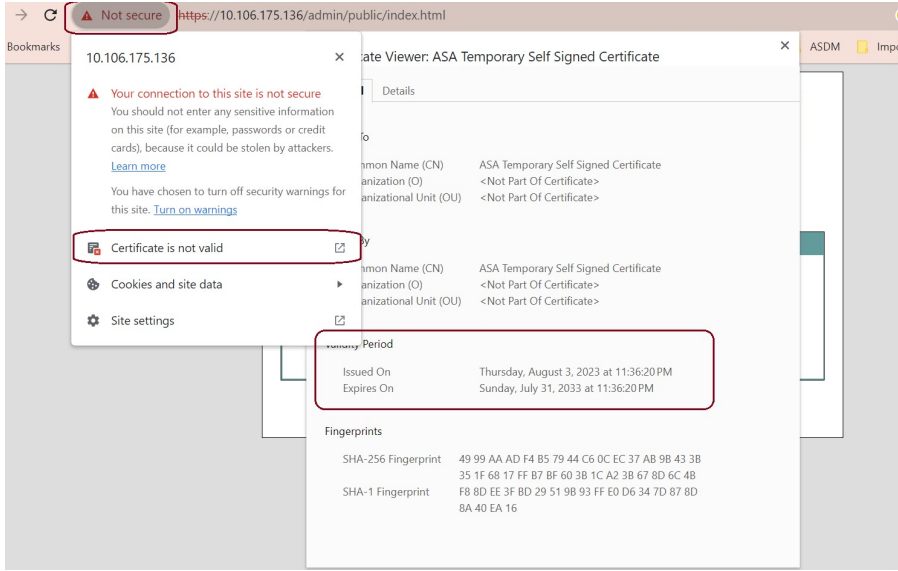
## ASDM の互換性に関する注意事項

次の表に、ASDM の互換性に関する警告を示します。

## ASDM の互換性に関する注意事項

条件	注意
ASA との日時の不一致により、自己署名証明書が無効になります	

条件	注意
	<p>ASDM は自己署名 SSL 証明書を検証し、ASA の日付が証明書の <b>[発行日 (Issued On)]</b> と <b>[有効期限 (Expires On)]</b> の日付の範囲内でない場合は起動しません。日時が一致しない場合は、次のエラーが表示されます。</p> <p>図 1: 証明書が無効です</p>  <p>この問題を解決するには、ASA で正しい時刻を設定し、リロードします。</p> <p>証明書の日付を確認するには、次の手順を実行します (例は Chrome)。</p> <ol style="list-style-type: none"> <li>1. <code>https://device_ip</code> に移動します。</li> <li>2. メニューバーの <b>[安全ではない (Not secure)]</b> テキストをクリックします。</li> <li>3. <b>[証明書が無効です (Certificate is not valid)]</b> をクリックして、証明書ビューアを開きます。</li> <li>4. <b>[有効期間 (Validity Period)]</b> をオンにします。</li> </ol> <p>図 2: 証明書ビューア</p>

条件	注意
	
Windows Active Directory ディレクトリアクセス	<p>場合によっては、Windows ユーザーの Active Directory 設定によって、Windows で ASDM を正常に起動するために必要なプログラムファイルの場所へのアクセスが制限されることがあります。次のディレクトリへのアクセスが必要です。</p> <ul style="list-style-type: none"> <li>• デスクトップフォルダ</li> <li>• C:\Windows\System32\Users\<username>\.asdm</username></li> <li>• C:\Program Files (x86)\Cisco Systems</li> </ul> <p>Active Directory がディレクトリアクセスを制限している場合は、Active Directory 管理者にアクセスを要求する必要があります。</p>

条件	注意
Windows 10	<p>「このアプリはお使いの PC では実行できません (This app can't run on your PC)」エラーメッセージ。</p> <p>ASDM ランチャをインストールすると、Windows 10 によって ASDM ショートカットターゲットが Windows Scripting Host パスに置き換えられて、このエラーが発生することがあります。ショートカットターゲットを修正するには、次の手順を実行します。</p> <ol style="list-style-type: none"> <li>1. [スタート (Start) ]&gt; [Cisco ASDM-IDM ランチャー (Cisco ASDM-IDM Launcher) ] を選択し、[Cisco ASDM-IDM ランチャー (Cisco ASDM-IDM Launcher) ] アプリケーションを右クリックします。</li> <li>2. [その他 (More) ]&gt; [ファイルの場所を開く (Open file location) ] を選択します。 Windows は、ショートカットアイコンを使用してディレクトリを開きます。</li> <li>3. ショートカットアイコンを右クリックして、[プロパティ (Properties) ] を選択します。</li> <li>4. [リンク先 (Target) ] を次のように変更します。 <b>C:\Windows\System32\wscript.exe invisible.vbs run.bat</b></li> <li>5. [OK (OK) ] をクリックします。</li> </ol>
OS X	<p>OS X では、ASDM の初回実行時に、Java のインストールを要求される場合があります。必要に応じて、プロンプトに従います。インストールの完了後に ASDM が起動します。</p>

条件	注意
OS X 10.8 以降	<p>ASDM は Apple Developer ID で署名されていないため、実行できるようにする必要があります。セキュリティの設定を変更しないと、エラー画面が表示されます。</p>  <p>1. ASDM を実行できるようにするには、[Cisco ASDM-IDM ランチャー (Cisco ASDM-IDM Launcher) ] アイコンを右クリック (または Ctrl キーを押しながらクリック) して、[開く (Open) ] を選択します。</p>  <p>2. 同様のエラー画面が表示されますが、この画面から ASDM を起動できます。[開く (Open) ] をクリックします。ASDM-IDM ランチャが起動します。</p> 



条件	注意
<p>ASA では強力な暗号化ライセンス (3DES/AES) が必要</p> <p>(注) スマートライセンスモデルを使用すると、強力な暗号化ライセンスを使用せずに ASDM での最初のアクセスが可能になります。</p>	<p>ASDM では、ASA に SSL 接続する必要があります。シスコが提供している 3DES ライセンスを要求できます。</p> <ol style="list-style-type: none"> <li><a href="http://www.cisco.com/go/license">www.cisco.com/go/license</a> [英語] にアクセスします。</li> <li>[製品ライセンスの登録を続行 (Continue to Product License Registration)] をクリックします。</li> <li>ライセンシングポータルで、テキストフィールドの横にある [その他のライセンスの取得 (Get Other Licenses)] をクリックします。</li> <li>ドロップダウンリストから、[IPS、暗号、その他... (IPS, Crypto, Other...)] を選択します。</li> <li>[キーワードで検索 (Search by Keyword)] フィールドに「ASA」と入力します。</li> <li>[製品 (Product)] リストで [Cisco ASA 3DES/AES License] を選択し、[Next] をクリックします。</li> <li>ASA のシリアル番号を入力し、プロンプトに従って ASA の 3DES/AES ライセンスを要求します。</li> </ol>
<ul style="list-style-type: none"> <li>自己署名証明書または信頼できない証明書</li> <li>IPv6</li> <li>Firefox および Safari</li> </ul>	<p>ASA が自己署名証明書または信頼できない証明書を使用する場合、Firefox と Safari では、IPv6 を介した HTTPS を使用して参照する場合にはセキュリティ例外を追加することはできません。 <a href="https://bugzilla.mozilla.org/show_bug.cgi?id=633001">https://bugzilla.mozilla.org/show_bug.cgi?id=633001</a> [英語] を参照してください。この警告は、Firefox または Safari から ASA に発信されるすべての SSL 接続に影響します (ASDM 接続を含む)。この警告を回避するには、信頼できる認証局が ASA に対して発行した適切な証明書を設定します。</p>
<ul style="list-style-type: none"> <li>ASA で SSL 暗号化を行うには、RC4-MD5 と RC4-SHA1 を両方とも含めるか、Chrome で SSL false start を無効にする必要があります。</li> <li>Chrome</li> </ul>	<p>RC4-MD5 および RC4-SHA1 アルゴリズム (これらのアルゴリズムはデフォルトでイネーブル) の両方を除外するために ASA の SSL 暗号化を変更した場合、Chrome の「SSL false start」機能のために Chrome は ASDM を起動できません。これらのアルゴリズムのいずれかを再度有効にすることを推奨します ([設定 (Configuration)] &gt; [デバイス管理 (Device Management)] &gt; [詳細 (Advanced)] &gt; [SSL設定 (SSL Settings)] ペインを参照)。または、「Run Chromium with flags」に従って <code>--disable-ssl-false-start</code> フラグを使用して Chrome の SSL false start を無効にできます。</p>

## ハードウェアとソフトウェアの互換性

サポートされるすべてのハードウェアおよびソフトウェアの一覧は、[『Cisco ASA Compatibility』](#) を参照してください。

## VPN の互換性

『Supported VPN Platforms, Cisco ASA Series』を参照してください。

## 新機能

このセクションでは、各リリースの新機能を示します。



(注) syslog メッセージガイドに、新規、変更済み、および廃止された syslog メッセージを記載しています。

### ASA 9.20(1)/ASDM 7.20(1) の新機能

リリース : 2023 年 9 月 7 日



(注) このリリースは、Cisco Secure Firewall 4200 でのみサポートされます。

機能	説明
プラットフォーム機能	
Cisco Secure Firewall 4200	Cisco Secure Firewall 4215、4225、および 4245 向けの ASA を導入しました。Cisco Secure Firewall 4200 は、スパンド EtherChannel クラスタリングで最大 8 ユニットのサポートします。ファイアウォールの電源が入っているときに、再起動することなく、同じタイプのネットワークモジュールをホットスワップできます。他のモジュールの変更を行う場合には、再起動が必要です。Cisco Secure Firewall 4200 の 25 Gbps 以上のインターフェイスは、Forward Error Correction と、インストールされている SFP に基づく速度検出をサポートします。SSD は自己暗号化ドライブ (SED) です。SSD が 2 つある場合、ソフトウェア RAID を形成します。管理インターフェイスが 2 つあります。
ファイアウォール機能	
<b>sysopt connection</b> <b>tcp-max-unprocessed-seg</b> コマンドの ASDM サポート	TCP 未処理セグメントの最大数を 6 ~ 24 に設定できます。デフォルト値は 6 です。SIP 電話機が Call Manager に接続していないことを確認したら、未処理の TCP セグメントの最大数を増やすことができます。  新規/変更された画面 : [設定 (Configuration)] > [ファイアウォール (Firewall)] > [高度 (Advanced)] > [TCP オプション (TCP Options)]

機能	説明
データプレーンにオフロードされた ASP ルールエンジンのコンパイル。	<p>デフォルトでは、ルールベースのポリシー（ACL、NAT、VPN など）に 100 を超えるルール更新がある場合、ASP ルールエンジンのコンパイルはコントロールプレーンではなくデータプレーンにオフロードされます。このオフロードにより、コントロールプレーンで他のタスクを実行する時間が長くなります。</p> <p>次のコマンドが追加または変更されました。 <b>asp rule-engine compile-offload</b>、<b>show asp rule-engine</b>。</p>
<b>ハイ アベイラビリティとスケーラビリティの各機能</b>	
ASA の高可用性のための偽フェールオーバーの削減	<p>ASA 高可用性のデータプレーンに追加のハートビートモジュールが導入されました。このハートビートモジュールは、コントロールプレーンのトラフィックの輻輳や CPU の過負荷が原因で発生する可能性のある、偽フェールオーバーやスプリットブレインシナリオを回避するのに役立ちます。</p> <p>9.18(4) でも同様です。</p>
フローステータスの設定可能なクラスタキープアライブ間隔	<p>フローオーナーは、キープアライブ（clu_keepalive メッセージ）と更新（clu_update メッセージ）をディレクタおよびバックアップオーナーに送信して、フローの状態を更新します。キープアライブ間隔を設定できるようになりました。デフォルトは 15 秒で、15～55 秒の範囲で間隔を設定できます。クラスタ制御リンクのトラフィック量を減らすために長い間隔を設定できます。</p> <p>新規/変更された画面：[設定（Configuration）]&gt;[デバイス管理（Device Management）]&gt;[高可用性と拡張性（High Availability and Scalability）]&gt;[ASA クラスタ（ASA Cluster）]&gt;[クラスタの設定（Cluster Configuration）]</p>
<b>ルーティング機能</b>	
EIGRPv6	<p>EIGRP for IPv6 を設定し、それらを個別に管理できるようになりました。各インターフェイスで EIGRP を設定するときは、IPv6 を明示的に有効にする必要があります。</p> <p>新規/変更された画面：[設定（Configuration）]&gt;[デバイスの設定（Device Setup）]&gt;[ルーティング（Routing）]&gt;[EIGRPv6]、[セットアップ（Setup）]、[フィルタルール（Filter Rules）]、[インターフェイス（Interface）]、[パッシブインターフェイス（Passive Interface）]、[再配布（Redistribution）]、および [スタティックネイバー（Static Neighbor）] タブ。</p>

機能	説明
HTTP クライアントによるパスモニタリング	<p>PBR は、特定の宛先 IP のメトリックではなく、アプリケーションドメインの HTTP クライアントを介したパスモニタリングによって収集されたパフォーマンスメトリック（RTT、ジッター、パケット損失、および MOS）を使用できるようになりました。インターフェイスの HTTP ベースのアプリケーションモニタリングオプションは、デフォルトで有効になっています。HTTP ベースのパスモニタリングは、ネットワーク サービス グループのオブジェクトを使用してインターフェイスで設定できます。モニタリング対象のアプリケーションが搭載され、パスを決定するためのインターフェイスの順序付けを行う一致 ACL を使用して、PBR ポリシーを設定できます。</p> <p>新規/変更された画面：[設定（Configuration）]&gt;[デバイス設定（Device Setup）]&gt;[インターフェイス設定（Interface Settings）]&gt;[パスモニタリング（Path Monitoring）]</p>
インターフェイス機能	
VXLAN VTEP IPv6 のサポート	<p>VXLAN VTEP インターフェイスに IPv6 アドレスを指定できるようになりました。IPv6 では、ASA 仮想 クラスタ制御リンクまたは Geneve カプセル化がサポートされていません。</p> <p>新しい/変更された画面：</p> <ul style="list-style-type: none"> <li>• [構成（Configuration）]&gt;[デバイスの設定（Device Setup）]&gt;[インターフェイスの設定（Interface Settings）]&gt;[VXLAN]</li> <li>• [構成（Configuration）]&gt;[デバイスの設定（Device Setup）]&gt;[インターフェイスの設定（Interface Settings）]&gt;[インターフェイス（Interfaces）]&gt;[追加（Add）]&gt;[VNI インターフェイス（VNI Interface）]</li> </ul>
DNS、HTTP、ICMP、IPsec フローオフロードのループバックインターフェイスのサポート	<p>ループバック インターフェイスを追加して、以下に使用できるようになりました。</p> <ul style="list-style-type: none"> <li>• DNS</li> <li>• HTTP</li> <li>• ICMP</li> <li>• IPsec フローのオフロード</li> </ul>
ライセンス機能	
スマートライセンスや Smart Call Home といったクラウドサービスの IPv6	<p>ASA は、スマートライセンスや Smart Call Home などのクラウドサービスの IPv6 をサポートするようになりました。</p>
証明書の機能	

機能	説明
OCSP および CRL の IPv6 PKI	<p>ASA で、IPv4 と IPv6 両方の OCSP および CRL URL をサポートするようになりました。URL で IPv6 を使用する場合は、角カッコで囲む必要があります。</p> <p>新規/変更された画面：[設定 (Configuration)]&gt;[サイト間VPN (Site-to-Site VPN)]&gt;[証明書管理 (Certificate Management)]&gt;[CA証明書 (CA Certificates)]&gt;[追加 (Add)]</p>
<b>管理、モニタリング、およびトラブルシューティングの機能</b>	
SNMP syslog のレート制限	<p>システム全体のレート制限を設定しない場合、SNMP サーバーに送信される syslog に対して個別にレート制限を設定できるようになりました。</p> <p>新規/変更されたコマンド： <b>logging history rate-limit</b></p>
スイッチの packets キャプチャ	<p>スイッチの出力および入力トラフィックパケットをキャプチャするように設定できるようになりました。このオプションは、Secure Firewall 4200 モデルデバイスに対してのみ使用できます。</p> <p>新規/変更された画面：[ウィザード (Wizards)]&gt;[パケットキャプチャウィザード (Packet Capture Wizard)]&gt;[入力トラフィックセレクタ (Ingress Traffic Selector)]および[ウィザード (Wizards)]&gt;[パケットキャプチャウィザード (Packet Capture Wizard)]&gt;[出力トラフィックセレクタ (Egress Traffic Selector)]</p>
<b>VPN 機能</b>	
暗号デバッグの機能拡張	<p>暗号デバッグの機能拡張は次のとおりです。</p> <ul style="list-style-type: none"> <li>• 暗号アーカイブは、テキスト形式とバイナリ形式の2つの形式で使用できるようになりました。</li> <li>• 追加の SSL カウンタ。</li> <li>• スタックした暗号化ルールは、デバイスを再起動せずに ASP テーブルから削除できます。</li> </ul>
IKEv2 の複数のキー交換	<p>ASA は、量子コンピュータ攻撃から IPsec 通信を保護するために、IKEv2 で複数のキー交換をサポートします。</p>
SAML を使用したセキュアクライアント 接続認証	<p>DNS ロードバランシングクラスタでは、SAML 認証を ASA で設定するときに、設定が適用されるデバイスに一意に解決されるローカルベース URL を指定できます。</p> <p>新規/変更された画面：[設定 (Configuration)]&gt;[リモートアクセスVPN (Remote Access VPN)]&gt;[ネットワーク (クライアント) アクセス (Network (Client) Access)]&gt;[安全なクライアント接続プロファイル (Secure Client Connection Profiles)]&gt;[追加/編集 (Add/Edit)]&gt;[ベーシック (Basic)]&gt;[SAMLアイデンティティプロバイダー (SAML Identity Provider)]&gt;[管理 (Manage)]&gt;[追加/編集 (Add/Edit)]</p>
<b>ASDM 機能</b>	
Windows 11 のサポート	<p>ASDM は Windows 11 で動作することが確認されています。</p>

## ファイアウォール機能の概要

ファイアウォールは、外部ネットワーク上のユーザーによる不正アクセスから内部ネットワークを保護します。また、ファイアウォールは、人事部門ネットワークをユーザーネットワークから分離するなど、内部ネットワーク同士の保護も行います。Web サーバーまたは FTP サーバーなど、外部のユーザーが使用できるようにする必要のあるネットワーク リソースがあれば、ファイアウォールで保護された別のネットワーク（非武装地帯（DMZ）と呼ばれる）上に配置します。ファイアウォールによって DMZ に許可されるアクセスは限定されますが、DMZ にあるのは公開サーバーだけのため、この地帯が攻撃されても影響を受けるのは公開サーバーに限定され、他の内部ネットワークに影響が及ぶことはありません。また、特定アドレスだけに許可する、認証または認可を義務づける、または外部の URL フィルタリングサーバーと協調するといった手段によって、内部ユーザーが外部ネットワーク（インターネットなど）にアクセスする機会を制御することもできます。

ファイアウォールに接続されているネットワークに言及する場合、外部ネットワークはファイアウォールの手前にあるネットワーク、内部ネットワークはファイアウォールの背後にある保護されているネットワーク、そして DMZ はファイアウォールの背後にあるが、外部ユーザーに制限付きのアクセスが許されているネットワークです。ASA を使用すると、数多くのインターフェイスに対してさまざまなセキュリティポリシーが設定できます。このインターフェイスには、多数の内部インターフェイス、多数の DMZ、および必要に応じて多数の外部インターフェイスが含まれるため、ここでは、このインターフェイスの区分は一般的な意味で使用するだけです。

## セキュリティ ポリシーの概要

他のネットワークにアクセスするために、ファイアウォールを通過することが許可されるトラフィックがセキュリティポリシーによって決められます。デフォルトでは、内部ネットワーク（高セキュリティ レベル）から外部ネットワーク（低セキュリティ レベル）へのトラフィックは、自由に流れることが ASA によって許可されます。トラフィックにアクションを適用してセキュリティ ポリシーをカスタマイズすることができます。

## アクセスルールによるトラフィックの許可または拒否

アクセスルールを適用することで、内部から外部に向けたトラフィックを制限したり、外部から内部に向けたトラフィックを許可したりできます。ブリッジグループインターフェイスでは、EtherType アクセスルールを適用して、非 IP トラフィックを許可できます。

## NAT の適用

NAT の利点のいくつかを次に示します。

- 内部ネットワークでプライベートアドレスを使用できます。プライベートアドレスは、インターネットにルーティングできません。
- NAT はローカルアドレスを他のネットワークから隠蔽するため、攻撃者はホストの実際のアドレスを取得できません。

- NAT は、重複 IP アドレスをサポートすることで、IP ルーティングの問題を解決できます。

## IP フラグメントからの保護

ASA は、IP フラグメント保護を提供します。この機能は、すべての ICMP エラー メッセージの完全なリアセンブリと、ASA 経由でルーティングされる残りの IP フラグメントの仮想リアセンブリを実行します。セキュリティチェックに失敗したフラグメントは、ドロップされログに記録されます。仮想リアセンブリはディセーブルにできません。

## HTTP、HTTPS、または FTP フィルタリングの適用

アクセスリストを使用して、特定の Web サイトまたは FTP サーバーへの発信アクセスを禁止できますが、このような方法で Web サイトの使用方法を設定し管理することは、インターネットの規模とダイナミックな特性から、実用的とはいえません。

ASA でクラウド Web セキュリティを設定できます。ASA は、Cisco Web セキュリティ アプライアンス (WSA) などの外部製品とともに使用することも可能です。

## アプリケーションインスペクションの適用

インスペクションエンジンは、ユーザーのデータ パケット内に IP アドレッシング情報を埋め込むサービスや、ダイナミックに割り当てられるポート上でセカンダリチャネルを開くサービスに必要です。これらのプロトコルは、ASA によるディープ パケット インスペクションの実行を必要とします。

## QoS ポリシーの適用

音声やストリーミング ビデオなどのネットワーク トラフィックでは、長時間の遅延は許容されません。QoS は、この種のトラフィックにプライオリティを設定するネットワーク機能です。QoS とは、選択したネットワーク トラフィックによりよいサービスを提供するネットワークの機能です。

## 接続制限と TCP 正規化の適用

TCP 接続、UDP 接続、および初期接続を制限することができます。接続と初期接続の数を制限することで、DoS 攻撃（サービス拒絶攻撃）から保護されます。ASA では、初期接続の制限を利用して TCP 代行受信を発生させます。代行受信によって、TCP SYN パケットを使用してインターフェイスをフラッディングする DoS 攻撃から内部システムを保護します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。

TCP 正規化は、正常に見えないパケットをドロップするように設計された高度な TCP 接続設定で構成される機能です。

## 脅威検出のイネーブル化

スキャン脅威検出と基本脅威検出、さらに統計情報を使用して脅威を分析する方法を設定できます。

基本脅威検出は、DoS 攻撃などの攻撃に関係している可能性のあるアクティビティを検出し、自動的にシステム ログ メッセージを送信します。

典型的なスキャン攻撃では、あるホストがサブネット内の IP アドレスにアクセスできるかどうかを 1 つずつ試みます（サブネット内の複数のホストすべてを順にスキャンするか、1 つのホストまたはサブネットの複数のポートすべてを順にスキャンする）。スキャン脅威検出機能は、いつホストがスキャンを実行するかを判別します。トラフィック署名に基づく IPS スキャン検出とは異なり、ASA のスキャン脅威検出機能は、スキャンアクティビティに関して分析できるホスト統計を含む膨大なデータベースを維持します。

ホストデータベースは、不審なアクティビティを追跡します。このようなアクティビティには、戻りアクティビティのない接続、閉じているサービスポートへのアクセス、脆弱な TCP 動作（非ランダム IPID など）、およびその他の多くの動作が含まれます。

攻撃者に関するシステム ログ メッセージを送信するように ASA を設定できます。または、自動的にホストを排除できます。

## ファイアウォール モードの概要

ASA は、次の 2 つのファイアウォール モードで動作します。

- ルーテッド
- トランスペアレント

ルーテッドモードでは、ASA は、ネットワークのルータ ホップと見なされます。

トランスペアレントモードでは、ASA は「Bump In The Wire」または「ステルス ファイアウォール」のように動作し、ルータ ホップとは見なされません。ASA は「ブリッジグループ」の内部および外部インターフェイスと同じネットワークに接続します。

トランスペアレントファイアウォールは、ネットワーク コンフィギュレーションを簡単にするために使用できます。トランスペアレントモードは、攻撃者からファイアウォールが見えないようにする場合にも有効です。トランスペアレントファイアウォールは、他の場合にはルーテッドモードでブロックされるトラフィックにも使用できます。たとえば、トランスペアレントファイアウォールでは、EtherType アクセスリストを使用するマルチキャストストリームが許可されます。

ルーテッドモードでブリッジグループの設定、およびブリッジグループと通常インターフェイスの間のルートの設定を行えるように、ルーテッドモードでは Integrated Routing and Bridging をサポートしています。ルーテッドモードでは、トランスペアレントモードの機能を複製できます。マルチコンテキストモードまたはクラスタリングが必要ではない場合、代わりにルーテッドモードを使用することを検討してください。



## ステートフル インспекションの概要

ASA を通過するトラフィックはすべて、アダプティブ セキュリティ アルゴリズムを使用して検査され、通過が許可されるか、またはドロップされます。単純なパケットフィルタは、送信元アドレス、宛先アドレス、およびポートが正しいかどうかはチェックできますが、パケットシーケンスまたはフラグが正しいかどうかはチェックしません。また、フィルタはすべてのパケットをフィルタと照合してチェックするため、処理が低速になる場合があります。



(注) TCP ステート バイパス機能を使用すると、パケット フローをカスタマイズできます。

ただし、ASA のようなステートフル ファイアウォールは、パケットの次のようなステートについて検討します。

- 新規の接続かどうか。

新規の接続の場合、ASA は、パケットをアクセス リストと照合してチェックする必要があり、これ以外の各種のタスクを実行してパケットの許可または拒否を決定する必要があります。このチェックを行うために、セッションの最初のパケットは「セッション管理パス」を通過しますが、トラフィックのタイプに応じて、「コントロールプレーンパス」も通過する場合があります。

セッション管理パスで行われるタスクは次のとおりです。

- アクセス リストとの照合チェック
- ルートルックアップ
- NAT 変換 (xlates) の割り当て
- 「ファストパス」でのセッションの確立

ASA は、TCP トラフィックのファストパスに転送フローとリバース フローを作成します。ASA は、高速パスも使用できるように、UDP、ICMP (ICMP インспекションがイネーブルの場合) などのコネクションレス型プロトコルの接続状態の情報も作成するので、これらのプロトコルもファストパスを使用できます。



(注) SCTP などの他の IP プロトコルの場合、ASA はリバース パス フローを作成しません。そのため、これらの接続を参照する ICMP エラー パケットはドロップされます。

レイヤ7インспекションが必要なパケット (パケットのペイロードの検査または変更が必要) は、コントロールプレーンパスに渡されます。レイヤ7インспекションエンジンは、2つ以上のチャネルを持つプロトコルが必要です。2つ以上のチャネルの1つは周知のポート番号を使用するデータチャネルで、その他はセッションごとに異なるポート番号を使用するコントロールチャネルです。このようなプロトコルには、FTP、H.323、および SNMP があります。

- 確立済みの接続かどうか。

接続がすでに確立されている場合は、ASA でパケットの再チェックを行う必要はありません。一致するパケットの大部分は、両方向で「ファースト」パスを通過できます。高速パスで行われるタスクは次のとおりです。

- IP チェックサム検証
- セッションルックアップ
- TCP シーケンス番号のチェック
- 既存セッションに基づく NAT 変換
- レイヤ 3 ヘッダー調整およびレイヤ 4 ヘッダー調整

レイヤ 7 インスペクションを必要とするプロトコルに合致するデータパケットも高速パスを通過できます。

確立済みセッションパケットの中には、セッション管理パスまたはコントロールプレーンパスを引き続き通過しなければならないものがあります。セッション管理パスを通過するパケットには、インスペクションまたはコンテンツフィルタリングを必要とする HTTP パケットが含まれます。コントロールプレーンパスを通過するパケットには、レイヤ 7 インスペクションを必要とするプロトコルのコントロールパケットが含まれます。

## VPN 機能の概要

VPN は、TCP/IP ネットワーク（インターネットなど）上のセキュアな接続で、プライベートな接続として表示されます。このセキュアな接続はトンネルと呼ばれます。ASA は、トンネリングプロトコルを使用して、セキュリティパラメータのネゴシエート、トンネルの作成および管理、パケットのカプセル化、トンネルを通じたパケットの送信または受信、パケットのカプセル化の解除を行います。ASA は、双方向トンネルのエンドポイントとして機能します。たとえば、プレーンパケットを受信してカプセル化し、それをトンネルのもう一方のエンドポイントに送信することができます。そのエンドポイントで、パケットはカプセル化を解除され、最終的な宛先に送信されます。また、セキュリティアプライアンスは、カプセル化されたパケットを受信してカプセル化を解除し、それを最終的な宛先に送信することもできます。ASA は、これらの機能を実行するためにさまざまな標準プロトコルを起動します。

ASA は、次の機能を実行します。

- トンネルの確立
- トンネルパラメータのネゴシエーション
- ユーザーの認証
- ユーザーアドレスの割り当て
- データの暗号化と復号化

- セキュリティ キーの管理
- トンネルを通じたデータ転送の管理
- トンネル エンドポイントまたはルータとしての着信と発信のデータ転送の管理

ASA は、これらの機能を実行するためにさまざまな標準プロトコルを起動します。

## セキュリティ コンテキストの概要

単一の ASA は、セキュリティ コンテキストと呼ばれる複数の仮想デバイスにパーティション化できます。各コンテキストは、独自のセキュリティポリシー、インターフェイス、および管理者を持つ独立したデバイスです。マルチ コンテキストは、複数のスタンドアロン デバイスを使用することに似ています。マルチコンテキストモードでは、ルーティングテーブル、ファイアウォール機能、IPS、管理など、さまざまな機能がサポートされています。ただし、サポートされていない機能もあります。詳細については、機能に関する各章を参照してください。

マルチ コンテキスト モードの場合、ASA には、セキュリティ ポリシー、インターフェイス、およびスタンドアロン デバイスで設定できるほとんどのオプションを識別するコンテキストごとのコンフィギュレーションが含まれます。システム管理者がコンテキストを追加および管理するには、コンテキストをシステムコンフィギュレーションに設定します。これが、シングルモード設定と同じく、スタートアップコンフィギュレーションとなります。システムコンフィギュレーションは、ASA の基本設定を識別します。システム コンフィギュレーションには、ネットワーク インターフェイスやネットワーク設定は含まれません。その代わりに、ネットワーク リソースにアクセスする必要が生じたときに（サーバーからコンテキストをダウンロードするなど）、システムは管理コンテキストとして指定されているコンテキストのいずれかを使用します。

管理コンテキストは、他のコンテキストとまったく同じです。ただし、ユーザーが管理コンテキストにログインすると、システム管理者権限を持つので、システムコンテキストおよび他のすべてのコンテキストにアクセス可能になる点が異なります。

## ASA クラスタリングの概要

ASA クラスタリングを利用すると、複数の ASA をグループ化して、1つの論理デバイスにすることができます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。

すべてのコンフィギュレーション作業（ブートストラップ コンフィギュレーションを除く）は、制御ユニット上でのみ実行します。コンフィギュレーションは、メンバーユニットに複製されます。

# 特殊なサービス非推奨のサービスおよびレガシー サービス

一部のサービスのマニュアルは、主要な設定ガイドおよびオンラインヘルプとは別の場所にあります。

## 特殊なサービスに関するガイド

特殊なサービスを利用して、たとえば、電話サービス (Unified Communications) 用のセキュリティ プロキシを提供したり、ボットネット トラフィック フィルタリングを Cisco アップデート サーバーのダイナミック データベースと組み合わせて提供したり、Cisco Web セキュリティ アプライアンス用の WCCP サービスを提供したりすることにより、ASA と他のシスコ製品の相互運用が可能になります。これらの特殊なサービスの一部については、別のガイドで説明されています。

- 『[Cisco ASA Botnet Traffic Filter Guide](#)』
- 『[Cisco ASA NetFlow Implementation Guide](#)』
- 『[Cisco ASA Unified Communications Guide](#)』
- 『[Cisco ASA WCCP Traffic Redirection Guide](#)』
- 『[SNMP Version 3 Tools Implementation Guide](#)』

## 非推奨のサービス

非推奨の機能については、ASA バージョンの設定ガイドを参照してください。同様に、設計の見直しが行われた機能 (NAT (バージョン 8.2 と 8.3 の間に見直しを実施)、トランスペアレント モードのインターフェイス (バージョン 8.3 と 8.4 の間に見直しを実施) など) については、各バージョンの設定ガイドを参照してください。ASDM は以前の ASA リリースとの後方互換性を備えていますが、設定ガイドおよびオンラインヘルプでは最新のリリースの内容しか説明されていません。

## レガシー サービス ガイド

レガシー サービスは現在も ASA でサポートされていますが、より高度なサービスを代わりに使用できる場合があります。レガシー サービスについては別のガイドで説明されています。

『[Cisco ASA Legacy Feature Guide](#)』

このマニュアルの構成は、次のとおりです。

- RIP の設定
- ネットワーク アクセスの AAA 規則

- IP スプーフィングの防止などの保護ツールの使用 (**ip verify reverse-path**)、フラグメントサイズの設定 (**fragment**)、不要な接続のブロック (**shun**)、TCP オプションの設定 (ASDM 用)、および基本 IPS をサポートする IP 監査の設定 (**ip audit**)。
- フィルタリング サービスの設定



## 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。