



Cisco ASA の概要

Cisco ASA は、追加モジュールとの統合サービスに加え、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 (14 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 \(6 ページ\)](#)
- [VPN の互換性 \(6 ページ\)](#)
- [新機能 \(6 ページ\)](#)
- [ファイアウォール機能の概要 \(8 ページ\)](#)
- [VPN 機能の概要 \(13 ページ\)](#)
- [セキュリティ コンテキストの概要 \(14 ページ\)](#)
- [ASA クラスタリングの概要 \(14 ページ\)](#)
- [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 \(14 ページ\)](#)

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: ASA と ASA FirePOWER : ASDM オペレーティング システムとブラウザの要件

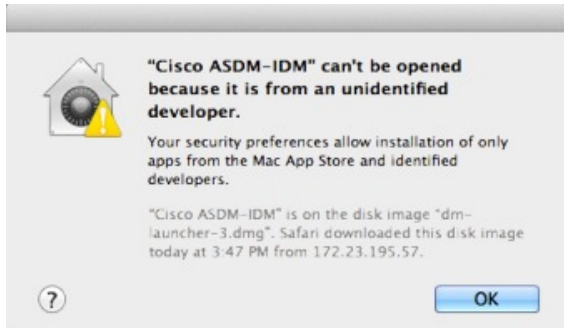
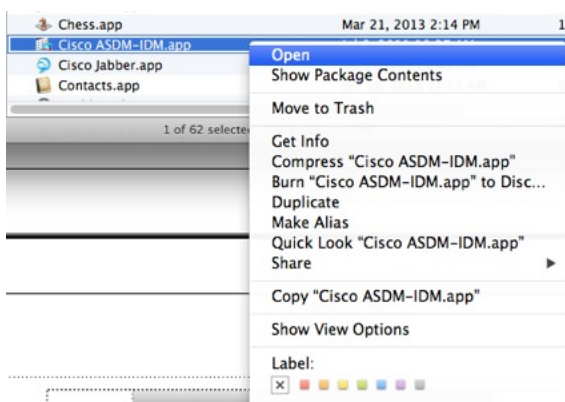

オペレーティング システム	ブラウザ				Oracle JRE	OpenJRE
	Internet Explorer	Firefox	Safari	Chrome		
<ul style="list-style-type: none"> • Microsoft Windows (英語および日本語) : • 10 <ul style="list-style-type: none"> (注) ASDM ショートカットに問題がある場合は、ASDM の互換性に関する注意事項 (3 ページ) の「Windows 10」を参照してください。 • 8 • 7 • Server 2016 と Server 2019 (ASA 管理のみ。FirePOWER モジュールの ASDM 管理はサポートされていません。その代わりに、ASA 管理に ASDM を使用しているときは、Firepower Management Center を使用して FirePOWER モジュールを管理できます。) • Server 2012 R2 • Server 2012 • Server 2008 	対応	対応	サポートなし	対応	8.0	1.8 (注) Windows 7 32 ビットのサポートなし

オペレーティング システム	ブラウザ				Oracle JRE	OpenJRE
	Internet Explorer	Firefox	Safari	Chrome		
Apple OS X 10.4 以降	サポートなし	対応	対応	対応 (64 ビットバージョンのみ)	8.0	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。

条件	注意
Windows 10	<p>「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"> 1. [Start] > [Cisco ASDM-IDM Launcher] を選択し、[Cisco ASDM-IDM Launcher] アプリケーションを右クリックします。 2. [More] > [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。 3. ショートカットアイコンを右クリックして、[Properties] を選択します。 4. [Target] を次のように変更します。 C:\Windows\System32\wscript.exe invisible.vbs run.bat 5. [OK] をクリックします。
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 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、[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。[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"> 1. www.cisco.com/go/license にアクセスします。 2. [Continue to Product License Registration] をクリックします。 3. 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 [Get Other Licenses] をクリックします。 4. ドロップダウンリストから、[IPS, Crypto, Other...] を選択します。 5. [Search by Keyword] フィールドに「ASA」と入力します。 6. [Product] リストで [Cisco ASA 3DES/AES License] を選択し、[Next] をクリックします。 7. 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。
<ul style="list-style-type: none"> • 自己署名証明書または信頼できない証明書 • IPv6 • Firefox および Safari 	<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。</p> <p>https://bugzilla.mozilla.org/show_bug.cgi?id=633001 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"> • 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。 • Chrome 	<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1つを再度有効にすることを推奨します ([Configuration] > [Device Management] > [Advanced] > [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>

条件	注意
サーバーの IE9	サーバーの Internet Explorer 9.0 の場合は、[Do not save encrypted pages to disk] オプションがデフォルトで有効になっています ([Tools] > [Internet Options] > [Advanced] を参照)。このオプションでは、最初の ASDM のダウンロードは失敗します。ASDM でダウンロードを行うには、このオプションを確実にディセーブルにしてください。

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 9.14(3)/ASDM 7.15(1.150) の新機能

リリース : 2021 年 6 月 15 日

このリリースに新機能はありません。

ASA 9.14(2) の新機能

リリース：2020年11月9日

機能	説明
SNMP 機能	
サイト間 VPN 経由の SNMP ポーリング	サイト間 VPN 経由のセキュアな SNMP ポーリングの場合、VPN 設定の一部として外部インターフェイスの IP アドレスを暗号マップアクセスリストに含めます。

ASA 9.14(1.30) の新機能

リリース：2020年9月23日

機能	説明
ライセンス機能	
ASAv100 永続ライセンス予約	ASAv100 で製品 ID L-ASAV100SR-K9= を使用した永続ライセンス予約がサポートされるようになりました。注：すべてのアカウントが永続ライセンス予約について承認されているわけではありません。

ASDM 7.14(1.48) の新機能

リリース日：2020年4月30日

機能	説明
プラットフォーム機能	
ASA 9.12 以前について、ASA 5512-X、5515-X、5585-X、および ASASM に対するサポートが復活	この ASDM リリースでは、9.12 以前を実行している場合、ASA 5512-X、5515-X、5585-X、および ASASM に対するサポートが復活しました。これらのモデルの最終 ASA バージョンは 9.12 です。元の 7.13(1) リリースと 7.14(1) リリースでは、これらのモデルでの後方互換性がブロックされていましたが、このバージョンでは互換性が復活しています。

ASA 9.14(1.6) の新機能

リリース日：2020 年 4 月 30 日



(注) このリリースは、ASA 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	
ASA 100 プラットフォーム	<p>ASA 仮想プラットフォームに、20 Gbps のファイアウォール スループット レベルを提供するハイエンドパフォーマンス モデルの ASA 100 が追加されました。ASA 100 はサブスクリプションベースのライセンスで、期間は 1 年、3 年、または 5 年です。</p> <p>ASA 100 は、VMware ESXi および KVM でのみサポートされます。</p>

ASA 9.14(3)/ASDM 7.15(1.150) の新機能

リリース：2021 年 6 月 15 日

このリリースに新機能はありません。

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したり、URL およびその他のフィルタリングサービス（ASA CX や ASA FirePOWER など）を提供する ASA モジュールをインストールすることができます。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。

サポート対象のハードウェアモジュールまたはソフトウェアモジュールへのトラフィックの送信

一部の ASA モデルでは、ソフトウェアモジュールの設定、またはハードウェアモジュールのシャーシへの挿入を行うことで、高度なサービスを提供することができます。これらのモジュールを通じてトラフィックインスペクションを追加することにより、設定済みのポリシーに基づいてトラフィックをブロックできます。また、これらのモジュールにトラフィックを送信することで、高度なサービスを利用することができます。

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ドする 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。

脅威検出のインテグレーション

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 のスキャンング脅威検出機能は、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ます。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 インスペク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インスペク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インスペクションエンジンは、2つ以上のチャンネルを持つプロトコルで必要です。2つ以上のチャンネルの1つは周知のポート番号を使用するデータチャンネルで、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ンネルです。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あるときに（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

