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 （23 ページ） も参照してください。

ASDM 要件

ASDM Java の要件

ASDM は、Oracle JDK 11（**asdm-*version*.bin**）または OpenJRE 11（**asdm-openjre-*version*.bin**）を使用してインストールできます。Oracle バージョンの場合、Oracle JDK 11 をインストールする必要があります（https://www.oracle.com/java/technologies/javase/jdk11-archive-downloads.html）。以降のバージョンは互換性がありません。ASDM の以前のバージョンには Java 8 を使用する必要があります。OpenJRE バージョンでは、Java をインストールする必要はありません。これは組み込みです。

ASDM の Oracle バージョンが ASA パッケージに含まれています。OpenJRE バージョンを使用する場合は、それを ASA にコピーし、そのバージョンの ASDM を使用するように ASA を構成する必要があります。

（注） ASDM は Linux ではサポートされていません。

表 *1* : *ASDM* の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 JDK	OpenJRE
	Firefox	Safari	Chrome		
Microsoft Windows（英語および日本語）： • 11 • 10 （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 および Server 2019 • Server 2012 R2 • Server 2012 • Server 2008	対応	サポートなし	対応	11	11 （注） Windows 7 または 10（32 ビット）のサポートなし

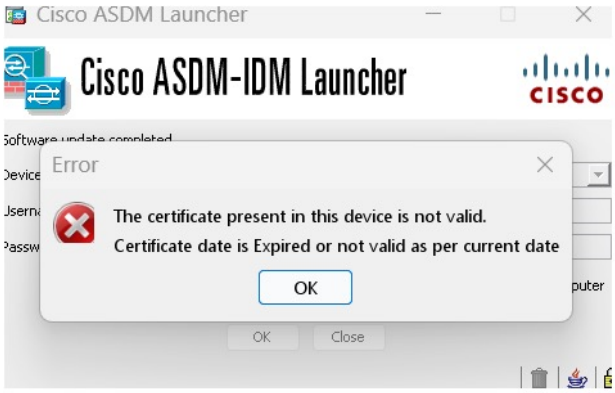
オペレーティング システム	ブラウザ			Oracle JDK	OpenJRE
	Firefox	Safari	Chrome		
Apple OS X 10.4 以降	対応	対応	対応（64 ビット バージョンのみ）	11	11

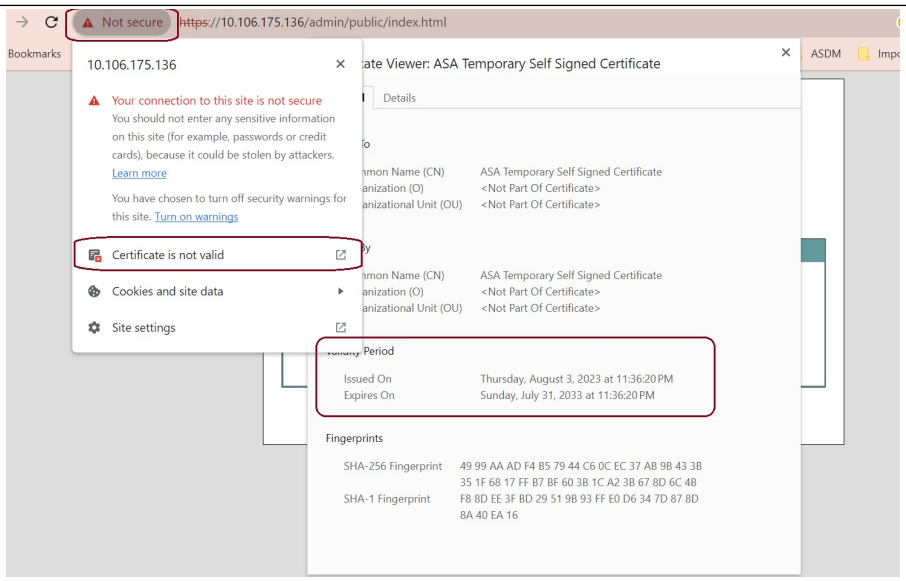
ASDM の互換性に関する注意事項

次の表に、ASDM の互換性に関する警告を示します。

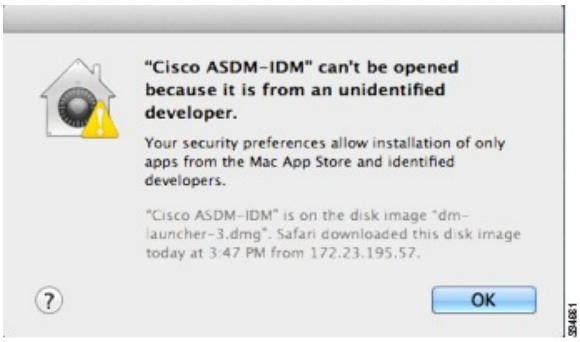
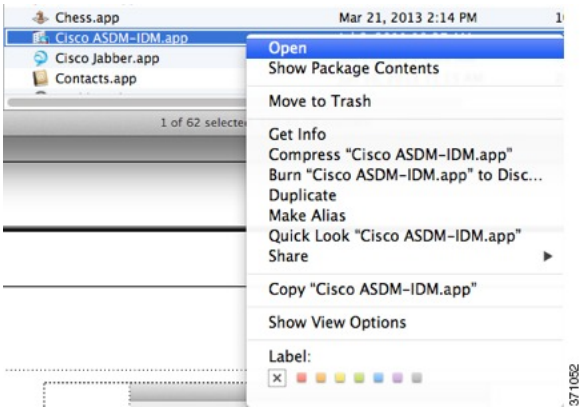
条件	注意
ASDM Launcher と ASDM バージョンの互換性	「デバイスマネージャを起動できません（Unable to Launch Device Manager）」というエラーメッセージが表示されます。 新しいASDMバージョンにアップグレードしてからこのエラーが発生した場合は、最新の Launcher を再インストールする必要があります。 **1.** ASA（https://<asa_ip_address>）で ASDM Web ページを開きます。 **2.** [ASDMランチャーのインストール（Install ASDM Launcher）] をクリックします。 **図 *1 : ASDM Launcher* のインストール**  **3.** ユーザー名とパスワードのフィールドを空のままにし（新規インストールの場合）、[OK] をクリックします。 HTTPS 認証が設定されていない場合は、ユーザー名および**イネーブル**パスワード（デフォルトで空白）を入力しないで ASDM にアクセスできます。CLI で **enable** コマンドを最初に入力したときに、パスワードを変更するように求められます。ASDMにログインしたときには、この動作は適用されません。空白のままにしないように、できるだけ早くイネーブルパスワードを変更することをお勧めします。**注**：HTTPS 認証をイネーブルにした場合、ユーザー名と関連付けられたパスワードを入力します。認証が有効でない場合でも、ログイン画面で（ユーザー名をブランクのままにしないで）ユーザー名とパスワードを入力すると、ASDMによってローカルデータベースで一致がチェックされます。

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
	ASDM は自己署名 SSL 証明書を検証し、ASA の日付が証明書の [発行日（Issued On）] と [有効期限（Expires On）] の日付の範囲内に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。 **図 *2*：証明書が無効です**  **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。 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）。 **1.** https://*device_ip* に移動します。 **2.** メニューバーの [安全ではない（Not secure）] テキストをクリックします。 **3.** [証明書が無効です（Certificate is not valid）] をクリックして、証明書ビューアを開きます。 **4.** [有効期間（Validity Period）] をオンにします。 **図 *3*：証明書ビューア**

条件	注意
	
Windows Active Directory ディレクトリアクセス	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。 • デスクトップフォルダ • C:\Windows\System32C:\Users\<username>\.asdm • C:\Program Files (x86)\Cisco Systems 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。

条件	注意
Windows 10	「**This app can't run on your PC**」エラー メッセージ。 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。 **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	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。

条件	注意
OS X 10.8 以降	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。  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。  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。 

条件	注意
（ASA 5500 および ISA 3000）ASA では強力な暗号化ライセンス（3DES/AES）が必要 （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 でのアクセスが可能になります。	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 PAK ライセンスを要求できます。 1. https://www.cisco.com/jp/go/license にアクセスします。 2. [従来のライセンス（Traditional Licenses）] で、[LRPにアクセス（Access LRP）] をクリックします。 3. [ライセンスを取得（Get Licenses）] をクリックし、ドロップダウンリストから [IPS、Crypto、その他...（IPS, Crypto, Other...）] を選択します。 4. [Search by Keyword] フィールドに「ASA」と入力します。 5. [Product] リストで [Cisco ASA 3DES/AES License] を選択し、[Next] をクリックします。 6. 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。
• 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	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。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。
• 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	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）]** > **[デバイス管理（Device Management）]** > **[詳細（Advanced）]** > **[SSL設定（SSL Settings）]** ペインを参照）。または、「Run Chromium with flags」に従って **--disable-ssl-false-start** フラグを使用して Chrome の SSL false start を無効にできます。

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 9.24(1)/ASDM 7.24(1) の新機能

リリース日：**2025 年 12 月 3 日**

機能	説明
プラットフォーム機能	
Cisco Secure Firewall 220	Cisco Secure Firewall 220 は、コストと機能のバランスを取るため、ブランチオフィスやリモートロケーション向けにお求めやすい価格のセキュリティアプライアンスです。
Cisco Secure Firewall 6160、6170	Cisco Secure Firewall 6160 および 6170 は、要求が厳しいデータセンターおよび電気通信ネットワーク用の超ハイエンドファイアウォールです。例外的な価格対パフォーマンス、モジュール型機能、および高いスループットを備えています。
ASA 仮想 Grub ブートローダーが UEFI ファームウェアおよびセキュアブートでアップグレードされました。	Grub ブートローダーの Grub 0.94 から Grub 2.12 へのアップグレードでは、レガシー BIOS モードとともに、セキュアブート機能の有無にかかわらない UEFI ファームウェアをサポートするようになりました。セキュアブート機能により、ブートレベルのマルウェア保護が提供されます。新しい展開では、MS-DOS パーティション分割ディスクの代わりに GPT パーティション分割イメージも使用されます。アップグレードする場合、UEFI およびセキュアブートに変更することはできません。新しい展開でのみ新しいオプションを使用できます。 （注） 9.24 にアップグレードした後は、以前のバージョンにダウングレードすることはできません。新しいバージョンにアップグレードするには、最初に 9.24 にアップグレードする必要があります。
ASA 仮想 AWS デュアル アーム クラスタリング	デュアルアームモードでは、検査後、ASA 仮想 は NAT を実行し、外部インターフェイスからインターネットゲートウェイを介して直接インターネットにアウトバウンドトラフィックを転送します。アウトバウンドトラフィックは、GWLB と GWLB エンドポイントを往復することなく、検査後にインターネットに直接転送されるため、トラフィックホップが 2 つだけ減少します。この削減は、マルチ VPC 展開に共通の出力パスを提供する場合に特に役立ちます。デュアルアーム展開の場合、出力通信のみがサポートされます。

機能	説明
ASA 仮想 自動スケーリングを使用した GCP クラスタリング	自動スケーリングを使用した GCP クラスタリングが、ASAv30、ASAv50、および ASAv100 でサポートされるようになりました。
ASA 仮想OCI アンペア A1 ARM コンピューティングシェーピング サポート	OCI の新しい形。 （注） OCI の ASA 仮想 について、Arm インスタンスでは、レガシーハイパーバイザ（特に SR-IOV が有効）でスループットが低下する可能性があります。詳細は、https://docs.oracle.com/en-us/iaas/Content/Compute/known-issues.htm を参照してください。サポートが必要な場合は、OCI にお問い合わせください。
ASA 仮想KVM フローオフロード	KVM 用 DPU でフローオフロードがサポートされるようになりました。
ASA 仮想 Nutanix AOS 6.8 のサポート	Nutanix AOS 6.8 では、パブリッククラウドの VPC と同様に VPC がサポートされます。
ASA 仮想 Caracal に対する OpenStack のサポート	ASA 仮想 展開は、OpenStack の Caracal リリースでサポートされています。
ASA 仮想 MANA NIC サポート	ASA 仮想 は、次のインスタンスで、Microsoft Azure の MANA NIC ハードウェアをサポートします。 • Standard_D8s_v5 • Standard_D16s_v5
ファイアウォール機能	
Cisco Secure Firewall 6100 のアプリケーションの可視性と制御（AVC）	アプリケーションの可視性と制御（AVC）を使用すると、IP アドレスとポートだけでなく、アプリケーションに基づいてアクセス制御ルールを作成できます。AVC は脆弱性データベース（VDB）をダウンロードします。このデータベースでは、アクセス制御ルールで使用できるネットワークサービスオブジェクトとグループが作成されます。オブジェクトはさまざまなアプリケーションを定義し、グループはアプリケーションカテゴリを定義します。これにより、IP アドレスやポートを指定せずに、アプリケーションまたは接続のクラス全体を簡単にブロックできます。 次の画面を導入しました。[**Configuration** > **Firewall** > **Advanced** > **Enable AVC**]、[**Monitoring** > **Properties** > **AVC** > **Status**]、[**Monitoring** > **Properties** > **AVC** > **Top N**]、[**Monitoring** > **Properties** > **AVC** > **App Category**]、[**Monitoring** > **Properties** > **AVC** > **Allowed/Blocked Applications**]、[**Monitoring** > **Properties** > **Service Policy**]、[**Monitoring** > **Properties** > **Network Object** > **Object Group Network Service**] サポートされているプラットフォーム： Cisco Secure Firewall 6100
ハイ アベイラビリティとスケーラビリティの各機能	

機能	説明
VPN モードを変更するための再起動は必要ありません	分散モードと集中型モードの間で VPN モードを変更する場合、再起動は必要なくなりました。ただし、モードを変更する前に、すべてのノードでクラスタリングを無効にする必要があります。
データノードはクラスターに同時に参加できます	以前は、制御ノードで一度に 1 つのデータノードのみがクラスターに参加できました。設定の同期に時間がかかる場合、データノードの結合に時間がかかることがあります。同時結合はデフォルトで有効になっています。NAT および VPN 分散モードが有効になっている場合、同時結合は使用できません。 次の画面が追加/変更されました。 • **Configuration** > **Device Management** > **High Availablility and Scalability** > **ASA Cluster** • **Monitoring** > **ASA Cluster** > **ASA Cluster Concurrent Join**
クラスターノード結合での MTU ping テストでは、MTU を小さくすることでより多くの情報が提供されます。	クラスタに参加したノードは、クラスタ制御リンク MTU と一致するパケットサイズで制御ノードに ping を送信することで MTU の互換性をチェックします。ping が失敗した場合は、MTU を 2 で割った値を試し、MTU ping が成功するまで 2 で割った値を返しません。通知が生成されるため、MTU を適切な値に修正して再試行できます。スイッチ MTU サイズを推奨値に増やすことを推奨しますが、スイッチ設定を変更できない場合は、クラスター制御リンクの有効な値を使用してクラスターを形成できます。 追加/変更された画面：[**Monitoring** > **ASA Cluster** > **Cluster Summary**]
CPU 使用率が高いクラスター制御リンクの正常性チェックの改善	クラスターノードの CPU 使用率が高い場合、正常性チェックは一時停止され、ノードは異常とはマークされません。正常性チェックを一時停止する CPU 使用率のしきい値を設定できます。 追加/変更された画面：[**Configuration** > **Device Management** > **High Availablility and Scalability** > **ASA Cluster**]
Cisco Secure Firewall 6100 でのクラスタリング	最大 4 つの Cisco Secure Firewall 6100 ノードをスパンド EtherChannel または個別インターフェイスモードでクラスター化できます。
クラスタリングでの枯渇モニタリングのブロック	ブロックの枯渇が発生すると、ASA はトラブルシューティングログを収集し、syslog を送信します。クラスタリングでは、ノードがクラスターから離脱し、他のノードがトラフィックを処理できるようになります。ASA は、クラッシュおよびリロードを強制して枯渇から回復することもできます。
分散型サイト間 VPN モードのダイナミック PAT サポート	分散型モードでダイナミック PAT がサポートされるようになりました。ただし、インターフェイス PAT はまだサポートされていません。
SNMP の機能拡張	このリリースでは、ENTITY-MIB および IF-MIB のポーリングエクスペリエンスを改善するために、SNMP が強化されました。これらの改善は、Cisco Secure Firewall 4200 および Cisco Secure Firewall 6100 シリーズプラットフォーム専用です。

機能	説明
インターフェイス機能	
DNS サーバーとドメインのリストを IPv6 クライアントにアドバタイズする再帰 DNS サーバー（RDNSS）およびDNS検索リスト（DNSSL）オプション	再帰DNSサーバー（RDNSS）およびDNS検索リスト（DNSSL）オプションを設定することで、ルータアドバタイズメントを使用して DNS サーバーとドメインを SLAAC クライアントに提供できるようになりました。 新規/変更された画面： **[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add Interface] > [IPv6]**
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	
SSH X.509 証明書認証	X.509v3 証明書を使用して SSH のユーザーを認証できるようになりました（RFC 6187）。 （注） この機能は、Firepower 4100/9300 ではサポートされていません。 新しい/変更された画面： • **[設定（Configuration）] > [デバイス管理（Device Management）] > [ユーザー/AAA（Users/AAA）] > [AAAアクセス（AAA Access）] > [承認（Authorization）]** • **[設定（Configuration）] > [デバイス管理（Device Management）] > [証明書管理（Certificate Management）] > [CA証明書（CA Certificates）] > [トラストポイントの追加/編集（Add/Edit Trustpoint）] > [詳細設定（Advanced）]** • **[Configuration] > [Device Management] > [Management Access] > [ASDM/HTTPS/Telnet/SSH]** *9.20(4)* でも同様です。
AES-256-GCM SSH 暗号	ASA は、SSH の AES-256-GCM 暗号をサポートしています。デフォルトでは、暗号化レベル [すべて（all）] と [高（high）] で有効になっています。 新規/変更された画面：**[設定（Configuration）] > [デバイス管理（Device Management）] > [詳細設定（Advanced）] > [SSH暗号（SSH Ciphers）]** *9.20(4)* でも同様です。

機能	説明
Message-of-the-day (motd) バナーにフェールオーバー状態と最後のフェールオーバー時刻を表示	フェールオーバーを使用する場合、message-of-the-day (motd) バナーを設定すると、ログインしているユニットのフェールオーバー状態と最後のフェールオーバー時刻に関する情報がバナーに表示されます。この情報は、CLI で障害対応などのアクションを実行しており、セッション間でフェールオーバーが発生する場合に役立ちます。 新規または変更された画面： **[Configuration] > [Device Management] > [Management Access] > [Command Line (CLI)] > [Banner]** *9.22(3)* でも同様です。
接続ステータス出力での UDP のイニシエータ値とレスポンダ値の表示	UDP 通信フローの場合、ASA は接続詳細ステータスにイニシエータとレスポンダのフィールド値を表示します。これらのフィールド値は通信の方向を示すため、ネットワーク接続の問題の障害対応に役立ちます。 9.20(1) でも同様です。
Linux カーネルクラッシュダンプ	Linux カーネルクラッシュダンプ機能を使用すると、カーネルクラッシュイベントをデバッグし、根本原因を見つけることができます。この機能は、デフォルトでイネーブルにされています。 新規/変更されたコマンド：**show kernel crash-dump**、**kernel crash-dump**、**crashinfoforce kernel-dump**
ASA Virtual での同意トークンを使用したルートシェルアクセスのサポート	ASA Virtual は、承認ユーザーが管理者パスワードなしでトラブルシューティングまたは診断の目的で Linux ルートシェルにワンタイムアクセスできるようにする新しい同意トークンメカニズムをサポートします。 新規/変更されたコマンド：**consent-token generate-challenge shell-access**、**consent-token accept-response shell-access**
ASDM 機能	
ASDM 7.24 では Java 11 が必要になりました	ASDM 7.24 では Java 11 が必要になりました。ASA イメージにバンドルされている Oracle バージョンの場合、Oracle JDK 11 をインストールする必要があります（https://www.oracle.com/java/technologies/javase/jdk11-archive-downloads.html）。以降のバージョンは互換性がありません。リスクを最小限に抑え、Java との互換性と安定性を向上させるために、シスコでは段階的に Java 8 から Java 11 への移行を開始していきます。7.24 に付属している ASDM ランチャー 1.9 (10) 以降にアップグレードした場合でも、ASDM の以前のバージョンを起動できます。 OpenJRE バージョンでは、Java をインストールする必要はありません。これは組み込みです。

機能	説明
ASDM 証明書認証	ASDM 7.24 に付属している ASDM ランチャー 1.9(10) では、ユーザー証明書認証がサポートされるようになりました。以前は、この機能は Java Web Start でのみサポートされていました（7.18 で廃止）。ASA コマンドが 9.18 で廃止されていないため、ASDM ランチャー 1.9(10) を含む ASDM バージョンを使用する場合は証明書認証を使用するように以前の ASA バージョンを設定できます。 新規/変更された画面： • ASDM ランチャーのログインウィンドウ。 • [**Configuration** > **Device Management** > **Management Access** > **ASDM/HTTPS/Telnet/SSH**] • [**Configuration** > **Site-to-Site VPN** > **Advanced** > **IPSec** > **Certificate to Connection Map** > **Rules**] • [**Configuration** > **Device Management** > **Management Access** > **HTTP Certificate Rule**]
ASDM FIPS 準拠	デフォルトでは、ASDM は非 FIPS モードで起動します。FIPS モードをイネーブルにするには、次の手順を実行します。 • Windows—FIPS.conf ファイルで、**fips_mode** 値を **true** に変更します。FIPS.conf ファイルは、ASDM ランチャーのインストールディレクトリにあります。 • MacOS—FIPS.plist ファイルで、**fipsMode** 値を **true** に変更します。FIPS.plist ファイルは、dm-launcher の Contents フォルダにあります。 FIPS モードは、ASDM 7.24 以降でのみサポートされています。 （注） DNS のリバースルックアップエラーが原因で、FIPS モードで ASDM ランチャーを起動すると 3 分以上かかることがあります。この遅延は、DNS サーバーがリバース DNS ルックアップの有効な PTR レコードを返さない場合に発生します。そのため、ASDM は NetBIOS ネームサービスにフォールバックし、スタートアップ時間に数分かかることがあります。 新規/変更された画面：ASDM ランチャーのログインウィンドウ。
Cisco.com ウィザードからのアップグレードソフトウェア用の新しい認証方式	**Cisco.com 認証** ダイアログボックスは、Cisco.com の新しい認証方式を使用する **Cisco.com デバイスの有効化** ダイアログボックスに置き換えられました。 新規/変更された画面：[**Tools** > **Check for ASA/ASDM Updates**]
VPN 機能	

機能	説明
SGT over VTI	VTI トンネルで Cisco TrustSec SGT タグがサポートされるようになりました。 新しい/変更された画面： • [**Configuration** > **Device Setup** > **Interface Settings** > **Interfaces** > **VTI/DVTI Interface** > **Advanced** > **Secure Group Tagging**] • [**Configuration** > **Site-to-Site VPN** > **Network (client) Access** > **Advanced** > **IPsec** > **IKE Parameters** > **Secure Group Tagging**]
VTI 向け ECMP および BFD 障害検出のサポート	1 つ以上のダイナミック VTI インターフェイスを Equal-Cost Multi-Path（ECMP）ゾーンに含めることができます。ゾーンを使用すると、スポークへのトラフィックのロードバランシングができます。Bidirectional Forwarding Detection（BFD）リンクの検出が高速になり、障害のある VTI リンクを数ミリ秒またはマイクロ秒単位で検出します。 新規/変更されたコマンド：**bfd template**、**vtemplate-bfd**、**vtemplate-zone-member**、**show zone**、**show conn all**、**show route** ECMP で新規/変更された画面：VTI では BFD の ASDM サポートはありません。 • [**Configuration** > **Site-to-Site VPN** > **Advanced** > **Tunnel Group** > **Add** > **Dynamic VTI** >] • [**Configuration** > **Site-to-Site VPN** > **Connection Profiles** > **Advanced** > **Tunnel Group** > **Add** > **Dynamic VTI** >]
分散型サイト間 VPN のループバック インターフェイスのサポート	分散サイト間モードでループバック インターフェイスを使用して、サイト間 VPN トンネルを作成できるようになりました。ロケーションネットワークに関連付けられている外部アドレスとは異なり、ループバック インターフェイスは独立しています。これは、アドレスを別のクラスターに移動し、ルーティングプロトコルを使用して新しい場所をアップストリームルータに伝播できることを意味します。その後、ピアのトラフィックは新しい場所に送信されます。
Cisco Secure Firewall 6100 の IPsec フロー オフロードおよび DTLS 暗号化アクセラレーション	Cisco Secure Firewall 6100 は AES-GCM-128 および AES-GCM-256 暗号のみをサポートします。
KVM上の ASA 仮想 のIPsec フローオフロード	IPSec フローオフロードが KVM の DPU でサポートされるようになりました。

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 グ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 つずつ試します（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イープする）。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 のスキャニ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 インスペクションの概要

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 つ以上のチャネルを持つプロトコルで必要です。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、トンネルを通し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
- トンネルを通し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。

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。