Cisco ASDM 7.9(x) リリースノート

初版：2017 年 12 月 4 日

最終更新：2018 年 5 月 9 日

Cisco ASDM 7.9(x) リリースノート

このドキュメントには、Cisco ASA シリーズ対応 Cisco ASDM バージョン 7.9(x) のリリース情報が記載されています。

特記事項

- ASA 5506-X、5508-X、および 5516-X の ROMMON のバージョン 1.1.15 へのアップグレード：これらの ASA モデルには新しい ROMMON バージョンがあります（2019 年 5 月 15 日）。最新バージョンにアップグレードすることを強くお勧めします。アップグレードするには、『ASA コンフィギュレーション ガイド』の手順を参照してください。

  注意 1.1.15 の ROMMON のアップグレードには、以前の ROMMON バージョンの 2 倍の時間がかかります（約 15 分）。アップグレード中はデバイスの電源を**再投入しないでください**。アップグレードが 30 分以内に完了しないか、または失敗した場合は、シスコ テクニカルサポートに連絡してください。デバイスの電源を再投入したり、リセットしたり**しないでください**。

- AnyConnect 4.4 または 4.5 で SAML 認証を使用しており、ASA バージョン 9.7.1.24、9.8.2.28、または 9.9.2.1（リリース日：2018 年 4 月 18 日）を展開している場合、SAML のデフォルト動作は、AnyConnect 4.4 および 4.5 でサポートされていない組み込みブラウザになります。したがって、AnyConnect 4.4 および 4.5 クライアントが外部（ネイティブ）ブラウザを使用して、SAML で認証するには、トンネル グループ設定で **saml external-browser** コマンドを使用する必要があります。

  （注） **saml external-browser** コマンドは、AnyConnect 4.6 以降にアップグレードするクライアントの移行のために使用されます。セキュリティ上の制限のため、AnyConnect ソフトウェアをアップグレードする際の一時的な移行の一環としてのみこのソリューションを使用してください。今後、このコマンド自体がサポートされなくなります。

- 9.9(2) での大規模な構成における ASA 5506-X のメモリの問題：9.9(2) にアップグレードする場合、大規模な構成の一部がメモリ不足のため拒否され、「エラーが発生しました：ルールをインストールするためのメモリが不足しています（ERROR: Insufficient memory to install the rules）」のメッセージが表示される場合があります。これを回避する方法の 1 つに、**object-group-search access-control** コマンドを入力して、ACL のメモリ使用量を改善する方法があります。ただし、パフォーマンスに影響する可能性があります。または、9.9(1) にダウングレードすることができます。
- ASA 5506-X、5508-X、および 5516-X 向けの新しい ROMMON バージョン 1.1.12：重要な修正が複数あるため、ROMMON をアップグレードすることを推奨します。https://www.cisco.com/go/asa-firepower-sw を参照し、ご使用のモデル > [ASA Rommon ソフトウェア（ASA Rommon Software）] > [1.1.12] を選択します。詳細については、[ソフトウェアダウンロード（Software Download）] ページの「リリースノート」を参照してください。ROMMON をアップグレードするには、「Upgrade the ROMMON Image (ASA 5506-X, 5508-X, and 5516-X）」を参照してください。Firepower Threat Defense を実行している ASA では、この ROMMON バージョンへのアップグレードはまだサポートされいません。ただし、ASA で正常にアップグレードしてから、Firepower Threat Defense に再イメージ化することができます。
- ASA 9.x で使用する RSA ツールキットのバージョンは、ASA 8.4 で使用されたバージョンとは異なるため、これらの 2 つのバージョン間で PKI の動作に違いが生じます。

  たとえば、9.x ソフトウェアを実行している ASA では、フィールド長が 73 文字までの [Organizational Name Value]（OU）フィールドをもつ証明書のインポートが許可されます。8.4 ソフトウェアを実行している ASA では、60 文字までの OU フィールド名をもつ証明書のインポートが許可されます。この相違のため、ASA 9.x でインポートできる証明書を ASA 8.4 ではインポートできません。ASA 9.x 証明書をバージョン 8.4 を実行している ASA にインポートしようとすると、エラー「ERROR: Import PKCS12 operation failed.」が表示されます。

システム要件

このセクションでは、このリリースを実行するためのシステム要件を一覧表で示します。

ASDM Java の要件

ASDM は、Oracle JRE 8.0を使用してインストールできます。 OpenJRE はサポートされていません。

（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

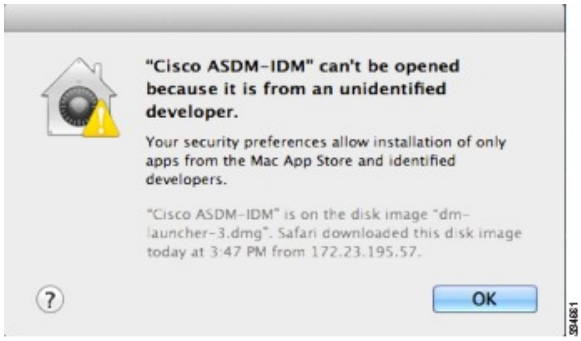
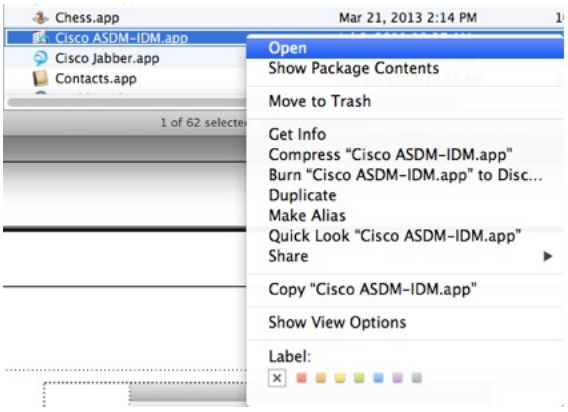
オペレーティング システム	ブラウザ				Oracle JRE
	Internet Explorer	Firefox	Safari	Chrome	
Microsoft Windows（英語および日本語）： 10 8 7 Server 2012 R2 Server 2012 Server 2008	対応	対応	サポートなし	対応	8.0
Apple OS X 10.4 以降	サポートなし	対応	対応	対応（64 ビット バージョンのみ）	8.0

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
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 での最初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 ライセンスを要求できます。 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。

条件	注意
• 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 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 **--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。
サーバの IE9	サーバの 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。
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
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。

ASDM のアイデンティティ証明書のインストール

Java 7 Update 51 以降を使用する場合、ASDM ランチャには信頼できる証明書が必要です。証明書の要件は、自己署名付きの ID 証明書をインストールすることによって簡単に満たすことができます。証明書をインストールするまで、Java Web Start を使用して ASDM を起動することができます。

ASDM と一緒に使用するために ASA に自己署名アイデンティティ証明書をインストールしたり、証明書を Java に登録したりするには、『Install an Identity Certificate for ASDM』を参照してください。

ASDM コンフィギュレーション メモリの増大

ASDM でサポートされる最大設定サイズは 512 KB です。このサイズを超えると、パフォーマンスの問題が生じることがあります。たとえば、コンフィギュレーションのロード時には、完了したコンフィギュレーションの割合がステータスダイアログボックスに表示されます。このとき、サイズの大きいコンフィギュレーションでは、ASDM によってまだコンフィギュレーションの処理が行われていても、完了した割合の増分が停止し、操作が中断されているように見えます。このような状況が発生した場合は、ASDM システム ヒープ メモリの増大を検討することを推奨します。

Windows での ASDM コンフィギュレーション メモリの増大

ASDM ヒープ メモリ サイズを増大するには、次の手順を実行して **run.bat** ファイルを編集します。

手順

ステップ 1 ASDM インストール ディレクトリ（たとえば、C:\Program Files (x86)\Cisco Systems\ASDM）に移動します。

ステップ 2 任意のテキスト エディタを使用して **run.bat** ファイルを編集します。

ステップ 3 「start javaw.exe」で始まる行で、「-Xmx」のプレフィックスが付いた引数を変更し、目的のヒープ サイズを指定します。たとえば、768 MB の場合は -Xmx768M に変更し、1 GB の場合は -Xmx1G に変更します。

ステップ 4 **run.bat** ファイルを保存します。

Mac OS での ASDM コンフィギュレーション メモリの増大

ASDM ヒープ メモリ サイズを増大するには、次の手順を実行して **Info.plist** ファイルを編集します。

手順

ステップ 1 [Cisco ASDM-IDM] アイコンを右クリックし、[Show Package Contents] を選択します。

ステップ 2 [Contents] フォルダで、Info.plist ファイルをダブルクリックします。開発者ツールをインストールしている場合は、**プロパティ リスト エディタ** で開きます。そうでない場合は、**TextEdit** で開きます。

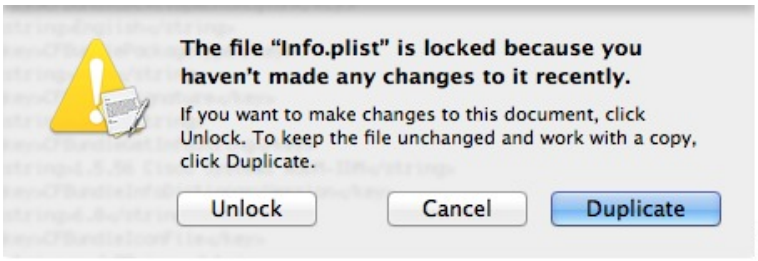
ステップ 3 **[Java]** > **[VMOptions]** で、「-Xmx」のプレフィックスが付いた文字列を変更し、必要なヒープ サイズを指定します。たとえば、768 MB の場合は -Xmx768M に変更し、1 GB の場合は -Xmx1G に変更します。

```
<key>CFBundleIconFile</key>
<string>asdm32.icns</string>

<key>VMOptions</key>
<string>-Xms64m -Xmx512m</string>


<key>CFBundleDocumentTypes</key>
  <array>
```

ステップ 4 このファイルがロックされると、次のようなエラーが表示されます。



ステップ 5 [Unlock] をクリックし、ファイルを保存します。

[Unlock] ダイアログボックスが表示されない場合は、エディタを終了します。[Cisco ASDM-IDM] アイコンを右クリックし、[Copy Cisco ASDM-IDM] を選択して、書き込み権限がある場所（デスクトップなど）に貼り付けます。その後、このコピーからヒープ サイズを変更します。

ASA と ASDM の互換性

ASA/ASDM ソフトウェアおよびハードウェアの要件およびモジュールの互換性を含む互換性の詳細については、『Cisco ASA Compatibility』を参照してください。

VPN の互換性

VPN の互換性については、『Supported VPN Platforms, Cisco ASA 5500 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。

ASDM 7.9(2.152) の新機能

リリース日：**2018 年 5 月 9 日**

機能	説明
VPN 機能	

機能	説明
従来の SAML 認証のサポート	CSCvg65072 の修正とともに ASA を展開すると、SAML のデフォルト動作で、AnyConnect 4.4 または 4.5 ではサポートされていない組み込みブラウザが使用されます。そのため、引き続き AnyConnect 4.4 または 4.5 を使用するには、従来の外部ブラウザで SAML 認証方式を有効にする必要があります。セキュリティ上の制限があるため、このオプションは、AnyConnect 4.6 に移行するための一時的な計画の一環としてのみ使用してください。このオプションは近い将来に廃止されます。 新しい/変更された画面： **[Configuration]** > **[Remote Access VPN]** > **[Network (Client) Access]** > **[AnyConnect Connection Profiles]** ページ > [Connection Profiles] 領域 > [Add] ボタン > [Add AnyConnect Connection Profile] ダイアログボックス **[Configuration]** > **[Remote Access VPN]** > **[Clientless SSL VPN Access]** > **[Connection Profiles]** > ページ > [Connection Profiles] 領域 > [Add] ボタン > [Add Clientless SSL VPN Connection Profile] ダイアログボックス 新規および変更されたオプション：[SAML External Browser] チェックボックス

ASA 9.9(2)/ASDM 7.9(2) の新機能

リリース：**2018年3月26日**

機能	説明
プラットフォーム機能	
VMware ESXi 6.5 用の ASAv サポート	ASAv 仮想プラットフォームは、VMware ESXi 6.5 で動作するホストをサポートしています。*vi.ovf* および *esxi.ovf* ファイルに新しい VMware ハードウェア バージョンが追加され、ESXi 6.5 で ASAv の最適なパフォーマンスと使いやすさを実現しました。 変更された画面はありません。
VMXNET3 インターフェイス用の ASAv サポート	ASAv 仮想プラットフォームは、VMware ハイパーバイザ上の VMXNET3 インターフェイスをサポートしています。 変更された画面はありません。
初回起動時の仮想シリアル コンソール用の ASAv サポート	ASAv にアクセスして設定するために、仮想 VGA コンソールではなく初回起動時に仮想シリアル コンソールを使用するように ASAv を設定できるようになりました。
Microsoft Azure 上での高可用性のために複数の Azure サブスクリプションでユーザ定義ルートを更新する ASAv サポート	Azure 高可用性構成で ASAv を構成して、複数の Azure サブスクリプションでユーザ定義ルートを更新できるようになりました。 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[Failover]** > **[Route-Table]**
VPN 機能	

機能	説明
IKEv2 プロトコルに拡張されたリモートアクセス VPN マルチコンテキスト サポート	AnyConnect やサード パーティ製標準ベース IPSec IKEv2 VPN クライアントがマルチコンテキスト モードで稼働する ASA へのリモート アクセス VPN セッションを確立できるように、ASA を構成することをサポートします。
RADIUS サーバへの IPv6 接続	ASA 9.9.2 では、外部 AAA RADIUS サーバへの IPv6 接続がサポートされるようになりました。
BVI サポートのための Easy VPN 拡張	Easy VPN は、ブリッジ型仮想インターフェイス（BVI）を内部セキュア インターフェイスとしてサポートするように拡張され、インターフェイスを内部セキュアインターフェイスとして使用するように直接設定できるようになりました。それ以外の場合は、ASA がセキュリティ レベルを使用して、その内部セキュアインターフェイスを選択します。 また、VPN **管理アクセス**がその BVI で有効になっている場合、**telnet**、**http**、**ssh** などの管理サービスを BVI で設定できるようになりました。非 VPN 管理アクセスの場合は、ブリッジ グループ メンバ インターフェイスでこれらのサービスの設定を続行する必要があります。
分散型 VPN セッションの改善	• 分散型 S2S VPN のアクティブ セッションとバックアップ セッションのバランスをとるアクティブセッションの再配布ロジックが改善されました。また、管理者が入力した単一の **cluster redistribute vpn-sessiondb** コマンドに対し、バランシング プロセスをバックグラウンドで最大 8 回繰り返すことができます。 • クラスタ全体のダイナミック リバース ルート インジェクション（RRI）の処理が改善されました。
ハイ アベイラビリティとスケーラビリティの各機能	
内部障害発生後に自動的にクラスタに再参加する	以前は、多くのエラー状態によりクラスタ ユニットがクラスタから削除されていました。この問題を解決した後、手動でクラスタに再参加する必要がありました。現在は、ユニットはデフォルトで 5 分、10 分、および 20 分の間隔でクラスタに自動的に再参加を試行します。これらの値は設定できます。内部の障害には、アプリケーション同期のタイムアウト、矛盾したアプリケーション ステータスなどがあります。 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** > **[Auto Rejoin]**

機能	説明
ASA 5000-X シリーズに対してインターフェイスを障害としてマークするために設定可能なデバウンス時間	ASA がインターフェイスを障害が発生していると見なし、ASA 5500-X シリーズ上のクラスタからユニットが削除されるまでのデバウンス時間を設定できるようになりました。この機能により、インターフェイスの障害をより迅速に検出できます。デバウンス時間を短くすると、誤検出の可能性が高くなることに注意してください。インターフェイスのステータス更新が発生すると、ASA はインターフェイスを障害としてマークし、クラスタからユニットを削除するまで指定されたミリ秒数待機します。デフォルトのデバウンス時間は 500 ms で、有効な値の範囲は 300 ms ～ 9 秒です。この機能は以前は Firepower 4100/9300 で使用できました。 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]**
クラスタの信頼性の高いトランスポート プロトコル メッセージのトランスポートに関連する統計情報の表示	ユニットごとのクラスタの信頼性の高いトランスポート バッファ使用率を確認して、バッファがコントロール プレーンでいっぱいになったときにパケット ドロップの問題を特定できるようになりました。 新規または変更されたコマンド：**show cluster info transport cp detail**
ピア ユニットからのフェールオーバー履歴の表示	ピア ユニットから、**details** キーワードを使用して、フェールオーバー履歴を表示できるようになりました。これには、フェールオーバー状態の変更と状態変更の理由が含まれます。 新規または変更されたコマンド：**show failover**
インターフェイス機能	
シングル コンテキスト モード用の一意の MAC アドレス生成	シングル コンテキスト モードで VLAN サブインターフェイスの一意の MAC アドレス生成を有効にできるようになりました。通常、サブインターフェイスはメインインターフェイスと同じ MAC アドレスを共有します。IPv6 リンクローカル アドレスは MAC アドレスに基づいて生成されるため、この機能により一意の IPv6 リンクローカル アドレスが許可されます。 新規または変更されたコマンド：**mac-address auto** ASDM サポートはありません。 *9.8(3)* と *9.8(4)* も同様です。
管理機能	
RSA キー ペアによる 3072 ビット キーのサポート	モジュラス サイズを 3072 に設定できるようになりました。 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[Certificate Management]** > **[Identity Certificates]**
FXOS ブートストラップ設定によるイネーブル パスワードの設定	Firepower 4100/9300 に ASA を展開すると、ブートストラップ設定のパスワード設定により、イネーブル パスワードと管理者ユーザ パスワードが設定されるようになりました。FXOS バージョン 2.3.1 が必要です。
モニタリング機能とトラブルシューティング機能	

機能	説明
SNMP IPv6 のサポート	ASA は、IPv6 経由での SNMP サーバとの通信、IPv6 経由でのクエリとトラップの実行許可、既存の MIB に対する IPv6 アドレスのサポートなど、SNMP over IPv6 をサポートするようになりました。RFC 8096 で説明されているように、次の新しい SNMP IPv6 MIB オブジェクトが追加されました。 • ipv6InterfaceTable（OID：1.3.6.1.2.1.4.30）：インターフェイスごとの IPv6 固有の情報が含まれています。 • ipAddressPrefixTable（OID：1.3.6.1.2.1.4.32）：このエンティティによって学習されたすべてのプレフィックスが含まれています。 • ipAddressTable（OID：1.3.6.1.2.1.4.34）：エンティティのインターフェイスに関連するアドレッシング情報が含まれています。 • ipNetToPhysicalTable（OID：1.3.6.1.2.1.4.35）：IP アドレスから物理アドレスへのマッピングが含まれています。 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[Management Access]** > **[SNMP]**
単一ユーザ セッションのトラブルシューティングのための条件付きデバッグ	条件付きデバッグ機能は、設定されたフィルタ条件に基づく特定の ASA VPN セッションのログを確認することを支援するようになりました。IPv4 および IPv6 サブネットの「any, any」のサポートが提供されます。

ASDM 7.9(1.151) の新機能

リリース：2018 年 2 月 14 日

このリリースに新機能はありません。

ASA 9.9(1)/ASDM 7.9(1) の新機能

リリース：2017年12月4日

機能	説明
ファイアウォール機能	

機能	説明
Ethertype アクセス コントロール リストの変更	EtherType アクセス コントロール リストは、Ethernet II IPX（EII IPX）をサポートするようになりました。さらに、DSAP キーワードに新しいキーワードが追加され、共通 DSAP 値（BPDU（0x42）、IPX（0xE0）、Raw IPX（0xFF）、および ISIS（0xFE））をサポートします。その結果、BPDU または ISIS キーワードを使用する既存の EtherType アクセス コントロール エントリは自動的に DSAP 仕様を使用するように変換され、IPX のルールは 3 つのルール（DSAP IPX、DSAP Raw IPX、および EII IPX）に変換されます。さらに、IPX を EtherType 値として使用するパケットキャプチャは廃止されました。これは、IPX が 3 つの個別の EtherType に対応するためです。 新規または変更された画面：**[Configuration]** > **[Firewall]** > **[Ethertype Rules]**
VPN 機能	
Firepower 9300 上のクラスタリングによる分散型サイト間 VPN	Firepower 9300 上の ASA クラスタは、分散モードでサイト間 VPN をサポートします。分散モードでは、（集中モードなどの）制御ユニットだけでなく、ASA クラスタのメンバー間で多数のサイト間 IPsec IKEv2 VPN 接続を分散させることができます。これにより、集中型 VPN の機能を超えて VPN サポートが大幅に拡張され、高可用性が実現します。分散型 S2S VPN は、それぞれ最大 3 つのモジュールを含む最大 2 つのシャーシのクラスタ（合計 6 つのクラスタ メンバー）上で動作し、各モジュールは最大約 36,000 のアクティブ セッション（合計 72,000)に対し、最大 6,000 のアクティブ セッション（合計 12,000）をサポートします。 新規または変更された画面： **[Monitoring] > [ASA Cluster] > [ASA Cluster] > [VPN Cluster Summary]** **[Monitoring] > [VPN] > [VPN Statistics] > [Sessions]** **[Configuration] > [Device Management] > [High Availablility and Scalability] > [ASA Cluster]** **[Wizards] > [Site-to-Site]** **[Monitoring] > [VPN] > [VPN Statistics] > [Sessions]** **[Monitoring] > [ASA Cluster] > [ASA Cluster] > [VPN Cluster Summary]** **[Monitoring] > [ASA Cluster] > [ASA Cluster] > [System Resource Graphs] > [CPU/Memory]** **[Monitoring] > [Logging] > [Real-Time Log Viewer]**
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
Microsoft Azure での ASAv のアクティブ/バックアップの高可用性	アクティブな ASAv の障害が Microsoft Azure パブリック クラウドのバックアップ ASAv へのシステムの自動フェールオーバーをトリガーするのを許可するステートレスなアクティブ/バックアップ ソリューション。 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[Failover]** **[Monitoring]** > **[Properties]** > **[Failover]** > **[Status]** **[Monitoring]** > **[Properties]** > **[Failover]** > **[History]** バージョン *9.8(1.200)* でも同様です。
Firepower シャーシのシャーシ ヘルス チェックの障害検出の向上	シャーシ ヘルス チェックの保留時間をより低い値（100 ms）に設定できるようになりました。以前の最小値は 300 ms でした。 新規または変更されたコマンド：**app-agent heartbeat interval** ASDM サポートはありません。
クラスタリングのサイト間冗長性	サイト間の冗長性により、トラフィック フローのバックアップ オーナーは常にオーナーとは別のサイトに置かれます。この機能によって、サイトの障害から保護されます。 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]**
動作と一致する**cluster remove unit**コマンドの動作**no enable**	**cluster remove unit** コマンドは、**no enable** コマンドと同様に、クラスタリングまたはリロードを手動で再度有効にするまで、クラスタからユニットを削除するようになりました。以前は、FXOS からブートストラップ設定を再展開すると、クラスタリングが再度有効になりました。無効化されたステータスは、ブートストラップ設定の再展開の場合でも維持されるようになりました。ただし、ASA をリロードすると、クラスタリングが再度有効になります。 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]**
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 バージョン 1 の廃止	SSH バージョン 1 は廃止され、今後のリリースで削除される予定です。デフォルト設定が SSH v1 と v2 の両方から SSH v2 のみに変更されました。 新しい/変更された画面： • **[Configuration]** > **[Device Management]** > **[Management Access]** > **[ASDM/HTTPS/Telnet/SSH]**

機能	説明
強化されたパケット トレーサおよびパケット キャプチャ機能	パケット トレーサは次の機能で強化されました。 • パケットがクラスタ ユニット間を通過するときにパケットを追跡します。 • シミュレートされたパケットが ASA から出られるようにします。 • シミュレートされたパケットのセキュリティ チェックをバイパスします。 • シミュレートされたパケットを IPsec/SSL で復号化されたパケットとして扱います。 パケット キャプチャは次の機能で強化されました。 • パケットを復号化した後にキャプチャします。 • トレースをキャプチャし、永続リストに保持します。 新規または変更された画面： **[Tools]** > **[Packet Tracer]** 次のオプションをサポートする [Cluster Capture] フィールドを追加しました：[decrypted]、[persist]、[bypass-checks]、[transmit] [All Sessions] ドロップダウンリストの下の [Filter By] ビューに 2 つの新しいオプションを追加しました：[Origin] および [Origin-ID] **[Monitoring]** > **[VPN]** > **[VPN Statistics]** > **[Packet Tracer and Capture]** [Packet Capture Wizard] 画面に [ICMP Capture] フィールドを追加しました：**[Wizards]** > **[Packet Capture Wizard]** ICMP キャプチャをサポートする 2 つのオプション、**include-decrypted** および **persist** を追加しました。

ソフトウェアのアップグレード

このセクションには、アップグレードを完了するためのアップグレードパス情報とリンクが記載されています。

ASA のアップグレードパス

現在のバージョンとモデルを表示するには、次のいずれかの方法を使用します。

- CLI：**show version** コマンドを使用します。
- ASDM：**[Home]** > **[Device Dashboard]** > **[Device Information]**の順に選択します。

次の表で、お使いのバージョンのアップグレードパスを参照してください。バージョンによっては、新しいバージョンにアップグレードする前に、中間アップグレードが必要な場合があります。推奨バージョンは**太字**で示されています。

（注） ASA のセキュリティの問題と、各問題に対する修正を含むリリースについては、ASA Security Advisories を参照してください。

（注） ASA 9.12(x) は ASA 5512-X、5515-X、5585-X、および ASASM 用の最終バージョン、

ASA 9.2(x) は ASA 5505 用の最終バージョン、

ASA 9.1(x) は ASA 5510、5520、5540、5550、および 5580 用の最終バージョンです。

現在のバージョン	暫定アップグレードバージョン	ターゲットバージョン
9.8(x)	—	次のいずれかになります。 → 9.9(x) → **9.8(x)**
9.7(x)	—	次のいずれかになります。 → 9.9(x) → **9.8(x)**
9.6(x)	—	次のいずれかになります。 → 9.9(x) → **9.8(x)** → 9.6(x)
9.5(x)	—	次のいずれかになります。 → 9.9(x) → **9.8(x)** → 9.6(x)
9.4(x)	—	次のいずれかになります。 → 9.9(x) → **9.8(x)** → 9.6(x)

現在のバージョン	暫定アップグレードバージョン	ターゲットバージョン
9.3(x)	—	次のいずれかになります。 → 9.9(x) → **9.8(x)** → 9.6(x)
9.2(x)	—	次のいずれかになります。 → 9.9(x) → **9.8(x)** → 9.6(x)
9.1(2)、9.1(3)、9.1(4)、9.1(5)、9.1(6)、または 9.1(7.4)	—	次のいずれかになります。 → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)
9.1(1)	→ 9.1(2)	次のいずれかになります。 → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)
9.0(2)、9.0(3)、または 9.0(4)	—	次のいずれかになります。 → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)
9.0(1)	→ 9.0(4)	次のいずれかになります。 → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)

現在のバージョン	暫定アップグレードバージョン	ターゲットバージョン
8.6(1)	→ 9.0(4)	次のいずれかになります。 → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)
8.5(1)	→ 9.0(4)	次のいずれかになります。 → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)
8.4(5+)	—	次のいずれかになります。 → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4) → 9.0(4)
8.4(1) ～ 8.4(4)	→ 9.0(4)	→ 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)
8.3(x)	→ 9.0(4)	次のいずれかになります。 → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)

現在のバージョン	暫定アップグレードバージョン	ターゲットバージョン
8.2(x) 以前	→ 9.0(4)	次のいずれかになります。 → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)

アップグレードリンク

アップグレードを完了するには、『ASA アップグレード ガイド』を参照してください。

未解決のバグおよび解決されたバグ

このリリースで未解決のバグおよび解決済みのバグには、Cisco Bug Search Tool を使用してアクセスできます。この Web ベース ツールから、この製品やその他のシスコハードウェアおよびソフトウェア製品でのバグと脆弱性に関する情報を保守するシスコ バグ トラッキング システムにアクセスできます。

（注） Cisco Bug Search Tool にログインしてこのツールを使用するには、Cisco.com アカウントが必要です。アカウントがない場合は、アカウントを登録できます。シスコサポート契約がない場合は、ID でのみバグを探すことができます。検索は実行できません。

Cisco Bug Search Tool の詳細については、Bug Search Tool（BST）ヘルプおよび FAQ を参照してください。

未解決のバグ

このセクションでは、各バージョンの未解決のバグを一覧表で示します。

バージョン 7.9(2.152) で未解決のバグ

次の表に、このリリースノートの発行時点で未解決のバグを示します。

不具合 ID 番号	説明
CSCvh80794	インターフェイスのスローによるマルチキャストルートの設定：エラー：検証が必要
CSCvi23649	EasyVpnRemote：VPN セキュアクライアントに関連付けられたインターフェイスのインターフェイス名を削除可能。

バージョン 7.9(2) で未解決のバグ

次の表に、このリリースノートの発行時点で未解決のバグを示します。

不具合 ID 番号	説明
CSCvh80794	インターフェイスのスローによるマルチキャストルートの設定：エラー：検証が必要
CSCvi23649	EasyVpnRemote：VPN セキュアクライアントに関連付けられたインターフェイスのインターフェイス名を削除可能。

バージョン 7.9(1.151) で未解決のバグ

次の表に、このリリースノートの発行時点で未解決のバグを示します。

不具合 ID 番号	説明
CSCvc44203	ONBOX：管理コンテキスト以外の SFR モジュールを削除する必要がある
CSCvg34789	SecGwy：大量の VPN S2S トンネルのセッション詳細を取得するために ASDM が大幅に遅延する
CSCvg88749	EtherType - Delete EtherType - After Edit

バージョン 7.9(1) で未解決のバグ

次の表に、このリリースノートの発行時点で未解決のバグを示します。

不具合 ID 番号	説明
CSCvc44203	ONBOX：管理コンテキスト以外の SFR モジュールを削除する必要がある
CSCvg34789	SecGwy：大量の VPN S2S トンネルのセッション詳細を取得するために ASDM が大幅に遅延する
CSCvg88749	EtherType - Delete EtherType - After Edit

解決済みのバグ

このセクションでは、リリースごとに解決済みのバグを一覧表で示します。

バージョン 7.9(2.152) で解決済みのバグ

次の表に、このリリースノートの発行時点で解決済みのバグを示します。

不具合 ID 番号	説明
CSCvi21519	複数の ACL の注釈を編集するときに ASDM 7.8(2)151 では「Specified remark does not exist」と表示される
CSCvi43311	ASDM のトンネルグループ webvpn 属性に新しい CLI が含まれる

不具合 ID 番号	説明
CSCvi54306	オブジェクトサービスまたはオブジェクト グループ サービスを作成すると、ASDM で vxlan が udp-1 と表示される

バージョン 7.9(2) で解決済みのバグ

次の表に、このリリースノートの発行時点で解決済みのバグを示します。

不具合 ID 番号	説明
CSCvg44558	ASDM が UDP ポート範囲サービスオブジェクトを TCP サービスオブジェクトとして作成する
CSCvg81125	ASDM 7.8.2.151：[VPN Statistics] -> [Sessions] に誤った値が表示される
CSCvg88749	EtherType - Delete EtherType - After Edit
CSCvg94453	ASDM ACL Manager：複数の ACE を削除できない
CSCvh20595	[Device Dashboard] タブの ASDM 7.9(1) VPN サマリーが不完全
CSCvh48054	基本アクセスリストを編集すると、誤った設定になる
CSCvh56769	ASDM のデフォルトプロトコル以外の「set connection conn-max」値を変更できない
CSCvh83068	[Enable Easy VPN Option] ボックスをオンにすると [Apply] ボタンが有効にならず、外部インターフェイスで DHCP が使用される

バージョン 7.9(1.151) で解決済みのバグ

次の表に、このリリースノートの発行時点で解決済みのバグを示します。

不具合 ID 番号	説明
CSCvg94453	ASDM ACL Manager：複数の ACE を削除できない
CSCvh48054	基本アクセスリストを編集すると、誤った設定になる

バージョン 7.9(1) で解決済みのバグ

次の表に、このリリースノートの発行時点で解決済みのバグを示します。

不具合 ID 番号	説明
CSCvd68637	ASDM で複数の IPV6 プレフィックスリストを作成または表示できない
CSCvf82966	ASDM - ロギング：リアルタイムログを表示できない

不具合 ID 番号	説明
CSCvf91260	ASDM：無視できないフィールドがあるため、CCOからのアップグレードが機能しない「Meta data request failed」
CSCvg15782	ASDM：バージョン7.8(2) へのアップグレード後に変更された SFR トラフィックのリダイレクトを表示できない
CSCvg31344	DAP 設定が ASDM に表示されない
CSCvg43291	アクセスルールの変更時に ASDM が重複するランダムなコメントを追加する
CSCvg51001	GroupLock 設定を有効にすると、ローカルユーザのパスワードが自動的に変更される

エンドユーザライセンス契約書

エンドユーザライセンス契約書の詳細については、http://www.cisco.com/jp/go/warranty にアクセスしてください。

関連資料

ASA の詳細については、『Navigating the Cisco ASA Series Documentation』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。