Cisco ASDM 7.8(x) リリースノート

初版：2017 年 5 月 15 日

最終更新：2017 年 10 月 12 日

Cisco ASDM 7.8(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 7.8(x) のリリース情報が記載されています。

特記事項

- **9.8(4.45)/7.18(1.152) 以降で ASDM 署名付きイメージをサポート**：ASA は、ASDM イメージがシスコのデジタル署名付きイメージであるかどうかを検証するようになりました。この修正を適用した ASA バージョンで古い ASDM イメージを実行しようとすると、ASDM がブロックされ、「%ERROR: Signature not valid for file disk0:/<filename>」というメッセージが ASA CLI に表示されます。ASDM リリース 7.18(1.152) 以降は、この修正が適用されていないものも含め、すべての ASA バージョンと下位互換性があります。（CSCwb05291、CSCwb05264）

- 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 Configuration Guide』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**。

- 9.8(2) 以降にアップグレードする前に、FIPS モードではフェールオーバーキーを 14 文字以上にする必要があります。FIPS モードで 9.8(2) 以降にアップグレードする前に、**failover key** または **failover ipsec pre-shared-key** を 14 文字以上に変更する必要があります。フェールオーバーキーが短すぎる場合、最初のユニットをアップグレードした時にフェールオーバーキーが拒否され、フェールオーバーキーを有効な値に設定するまで、両方のユニットがアクティブになります。

- 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。

- Amazon Web サービスの ASAv については 9.8(1) にアップグレードしないようにしてください。CSCve56153 のため、9.8(1) にアップグレードするべきではありません。アップグレード後に、ASAv はアクセス不能になります。代わりに 9.8(1.5) 以降にアップグレードしてください。
- ASAv5 のメモリの問題：バージョン 9.7(1) 以降、ASAv5 では、AnyConnect の有効化やファイルの ASAv へのダウンロードなどの特定の機能が失敗した場合に、メモリが枯渇することがあります。次のバグは 9.8 (1.5) で修正され、メモリ機能を透過的に改善し、必要に応じて ASAv5 により多くのメモリを割り当てられるようになりました（CSCvd90079 および CSCvd90071）。
- 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。

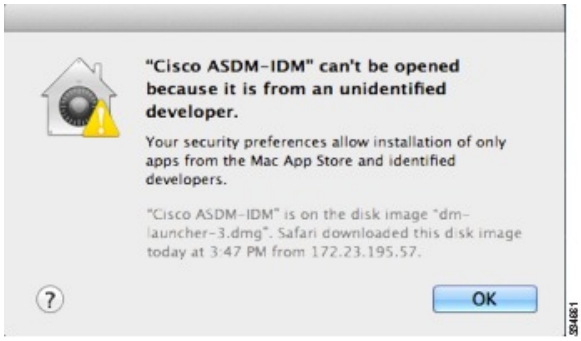
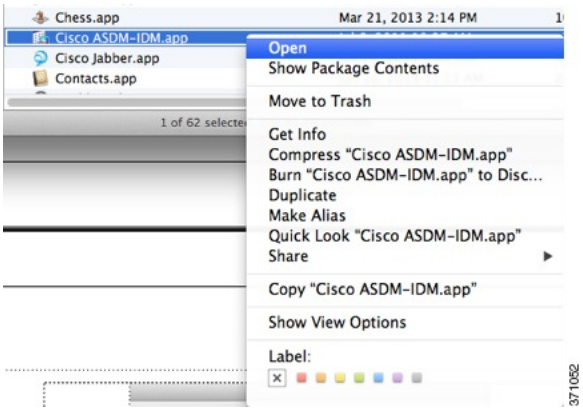
表 *1 : ASA* と *ASA FirePOWER* : *ASDM* オペレーティング システムとブラウザの要件

オペレーティング システム	ブラウザ			Oracle JRE
	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	サポートなし	対応	8.0 バージョン 8u261 以降
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

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	「**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 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。
• 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。

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。

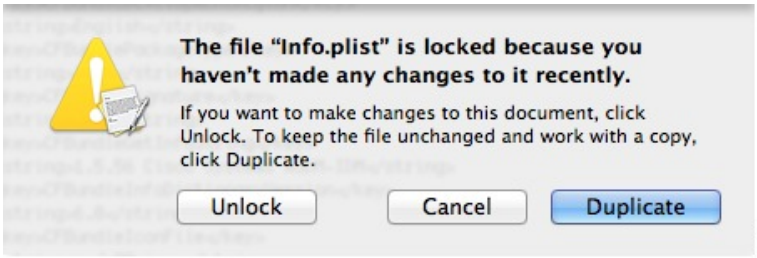
ステップ 3 **[Java]** > **[VMOptions]** で、「-Xmx」のプレフィックスが付いた文字列を変更し、必要なヒープ サイズを指定します。たとえば、768 MB の場合は -Xmx768M に変更し、1 GB の場合は -Xmx1G に変更します。

```
    <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。

ASA 9.8(4) の新機能

リリース日：**2019 年 4 月 24 日**

機能	説明
VPN 機能	
webVPN HSTS へのサブドメインの追加	ドメイン所有者は、Web ブラウザの HSTS プリロードリストに含める必要があるドメインを送信できます。 新しい/変更された画面： **[Configuration]** > **[Remote Access VPN]** > **[Clientless SSL VPN Access]** > **[Advanced]** > **[Proxies]** > [Enable HSTS Subdomains] フィールド *9.12(1)* でも同様です。
管理機能	
非ブラウザベースの HTTPS クライアントによる ASA へのアクセスの許可	非ブラウザベースの HTTPS クライアントが ASA 上の HTTPS サービスにアクセスできるようにすることができます。デフォルトでは、ASDM、CSM、および REST API が許可されています。多くの専門クライアント（python ライブラリ、curl、wget など）は、クロスサイト要求の偽造（CSRF）トークンベースの認証をサポートしていないため、これらのクライアントが ASA 基本認証方式を使用することを明確に許可する必要があります。セキュリティ上の理由から、必要なクライアントのみを許可する必要があります。 新規/変更された画面： **[Configuration]** > **[Device Management]** > **[Management Access]** > **[HTTP Non-Browser Client Support]** *9.12(1)* でも同様です。
show tech-support に追加の出力が含まれている	**show tech-support** の出力が拡張され、次の出力が表示されるようになりました。 • **show ipv6 interface** • **show aaa-server** • **show fragment** 新規/変更されたコマンド： **show tech-support** *9.12(1)* でも同様です。

機能	説明
SNMP ウォーク操作中の空きメモリおよび使用済みメモリの統計情報の結果を有効または無効にするためのサポート	CPU リソースが過剰に使用されないようにするには、SNMP ウォーク操作によって収集された空きメモリと使用済みメモリの統計情報のクエリを有効または無効にすることができます。 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[Management Access]** > **[SNMP]** *9.10(1)* でも同様です。

ASA 9.8(3)/ASDM 7.9(2.152) の新機能

リリース日：**2018 年 7 月 2 日**

機能	説明
プラットフォーム機能	
Firepower 2100 アクティブ LED はスタンバイ モードのときにオレンジ色に点灯するようになりました。	以前は、スタンバイ モード時にはアクティブ LED は点灯していませんでした。
ファイアウォール機能	
カットスルー プロキシ ログイン ページからのログアウト ボタンの削除をサポート。	ユーザー ID 情報（AAA 認証 リスナー）を取得するようにカットスルー プロキシを設定している場合、ページからログアウト ボタンを削除できるようになりました。これは、ユーザーが NAT デバイスの背後から接続し、IP アドレスで識別できない場合に便利です。1 人のユーザーがログアウトすると、その IP アドレスのすべてのユーザーがログアウトされます。 新規/変更されたコマンド：**aaa authentication listener no-logout-button**。 ASDM サポートはありません。
Trustsec SXP 接続の設定可能な削除ホールド ダウン タイマー	デフォルトの SXP 接続ホールド ダウン タイマーは 120 秒です。このタイマーを 120 ～ 64000 秒に設定できるようになりました。 新規/変更されたコマンド：**cts sxp delete-hold-down period**、**show cts sxp connection brief**、**show cts sxp connections** ASDM サポートはありません。
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： **[設定（Configuration）]** > **[リモートアクセスVPN（Remote Access VPN）]** > **[ネットワーク（クライアント）アクセス（Network (Client) Access）]**AnyConnect クライアント**[接続プロファイル（Connection Profiles）]** ページ > **[接続プロファイル（Connection Profiles）]** 領域 > **[追加（Add）]** ボタン > **[追加（Add）]** AnyConnect クライアント**[接続プロファイル（Connection Profile）]** ダイアログ **[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
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。 *9.9 (2)* 以降でも同様です。

ASDM 7.8(2.151) の新機能

リリース：**2017年10月12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。 この機能は、9.8(2.9)およびその他の暫定リリースでサポートされています。詳細については、CSCvf57908 を参照してください。 次の画面が変更されました：**[Configuration]** > **[Firewall]** > **[Ethertype Rules]**.

ASA 9.8(2)/ASDM 7.8(2) の新機能

リリース：**2017年8月28日**

機能	説明
プラットフォーム機能	
FirePOWER 2100 シリーズ用の ASA	FirePOWER 2110、2120、2130、2140 用の ASA を導入しました。FirePOWER 4100 および 9300 と同様に、FirePOWER 2100 は基盤の FXOS オペレーティング システムを実行してから、ASA オペレーティング システムをアプリケーションとして実行します。FirePOWER 2100 実装では、FirePOWER 4100 および 9300 よりも緊密に FXOS を ASA と連携させます（軽量な FXOS 機能、単一デバイス イメージ バンドル、ASA および FXOS の両方に対する簡単な管理アクセス）。 FXOS には、EtherChannel の作成、NTP サービス、ハードウェアのモニタリング、およびその他の基本機能を含む、インターフェイスの構成ハードウェア設定があります。この構成では、Firepower Chassis Manager または FXOS CLI を使用できます。ASA には、（FirePOWER 4100 および 9300 とは異なり）スマート ライセンスを含む、その他すべての機能があります。ASA および FXOS はそれぞれ、管理 1/1 インターフェイスでの独自の IP アドレスを持っています。ユーザーは、任意のデータ インターフェイスから ASA および FXOS インスタンス両方の管理を設定できます。 次の画面が導入されました。 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[FXOS Remote Management]**

機能	説明
国防総省（DoD）統合機能認定製品リスト	ASA は、統合機能認定製品リスト（UC APL）の要件に準拠するように更新されました。このリリースでは、**fips enable** コマンドを入力すると、ASA がリロードされます。フェールオーバーを有効にする前に、両方のフェールオーバー ピアが同じ FIPS モードになっている必要があります。 **fips enable** コマンドが変更されました。
Amazon Web Services M4 インスタンスサポートの ASAv	ASAv を M4 インスタンスとして展開できるようになりました。 変更された画面はありません。
ASAv5 1.5 GB RAM 機能	バージョン 9.7(1) 以降、ASAv5 では、AnyConnect クライアント の有効化や ASAv へのファイルのダウンロードなど、特定の機能が失敗した場合にメモリが枯渇することがあります。1.5 GB の RAM を ASAv5 に割り当てられるようになりました（1 GB から増加しました）。 変更された画面はありません。
VPN 機能	
HTTP Strict Transport Security（HSTS）ヘッダーのサポート	HSTS は、クライアントレス SSL VPN でのプロトコル ダウングレード攻撃や Cookie ハイジャックから Web サイトを保護します。これにより Web サーバーは、Web ブラウザ（またはその他の準拠しているユーザー エージェント）が Web サーバーと通信するにはセキュア HTTPS 接続を使用する必要があり、非セキュアな HTTP プロトコルを使用して通信することはできないことを宣言できます。HSTS は IETF 標準化過程プロトコルであり、RFC 6797 で指定されます。 次の画面が変更されました：[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [Proxies]
インターフェイス機能	
ASAv50 の VLAN サポート	ASAv50 では、SR-IOV インターフェイスの ixgbe-vf vNIC で VLAN がサポートされるようになりました。 変更された画面はありません。

ASA 9.8(1.200) の新機能

リリース：2017年7月30日

（注） このリリースは、Microsoft Azure の ASAv でのみサポートされます。これらの機能は、バージョン 9.8(2) ではサポートされていません。

機能	説明
ハイ アベイラビリティとスケーラビリティの各機能	
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。 次のコマンドが導入されました。**failover cloud** ASDM サポートはありません。

ASDM 7.8(1.150) の新機能

リリース：2017年6月20日

このリリースに新機能はありません。

ASA 9.8(1)/ASDM 7.8(1) の新機能

リリース：2017年5月15日

機能	説明
プラットフォーム機能	
ASAv50 プラットフォーム	ASAvプラットフォームに、10 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 ASAv50 プラットフォームが追加されました。ASAv50 には ixgbe-vf vNIC が必要です。これは VMware および KVM でのみサポートされます。
ASAvプラットフォームの SR-IOV	ASAvプラットフォームでは、Single Root I/O Virtualization（SR-IOV）インターフェイスがサポートされます。これにより、複数の VM でホスト内の 1 つの PCIe ネットワークアダプタを共有できるようになります。ASAv SR-IOV サポートは、VMware、KVM、および AWS でのみ使用可能です。
自動 ASP ロードバランシングが ASAv でサポートされるようになりました。	以前は、ASP ロード バランシングは手動でのみ有効または無効にできました。 次の画面が変更されました。[Configuration] > [Device Management] > [Advanced] > [ASP Load Balancing]。
ファイアウォール機能	
TLS プロキシ サーバーの SSL 暗号スイートの設定サポート	ASA が TLS プロキシ サーバーとして動作している場合は、SSL 暗号スイートを設定できるようになりました。以前は、**[Configuration]** > **[Device Management]** > **[Advanced]** > **[SSL Settings]** > **[Encryption]** ページでASA のグローバル設定のみが可能でした。 次の画面が変更されました。**[Configuration]** > **[Firewall]** > **[Unified Communications]** > **[TLS Proxy]**、追加/編集ダイアログ ボックス、[Server Configuration] ページ。

機能	説明
ICMP エラーのグローバル タイムアウト	ASA が ICMP エコー応答パケットを受信してから ICMP 接続を削除するまでのアイドル時間を設定できるようになりました。このタイムアウトが無効（デフォルト）で、ICMP インスペクションが有効に設定されている場合、ASA はエコー応答を受信するとすぐに ICMP 接続を削除します。したがって、終了しているその接続に対して生成されたすべての ICMP エラーは破棄されます。このタイムアウトは ICMP 接続の削除を遅らせるので、重要な ICMP エラーを受信することが可能になります。 **[Configuration]** > **[Firewall]** > **[Advanced]** > **[Global Timeouts]** の画面が変更されました。
ハイ アベイラビリティとスケーラビリティの各機能	
改善されたクラスタ ユニットのヘルス チェック障害検出	ユニット ヘルスチェックの保留時間をより低めの値に設定できます（最小値は .3 秒）以前の最小値は .8 秒でした。この機能は、ユニット ヘルス チェック メッセージング スキームを、コントロール プレーンのキープアライブからデータ プレーンのハートビートに変更します。ハートビートを使用すると、コントロールプレーン CPUのホッギングやスケジューリングの遅延の影響を受けないため、クラスタリングの信頼性と応答性が向上します。保留時間を短く設定すると、クラスタ制御リンクのメッセージングアクティビティが増加することに注意してください。保留時間を短く設定する前にネットワークを分析することをお勧めします。たとえば、ある保留時間間隔の間に3つのハートビートメッセージが存在するため、クラスタ制御リンクを介してあるユニットから別のユニットへのpingが保留時間/3以内に戻ることを確認します。保留時間を 0.3 ～ 0.7 に設定した後に ASA ソフトウェアをダウングレードした場合、新しい設定がサポートされていないので、この設定はデフォルトの 3 秒に戻ります。 次の画面を変更しました。**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]**
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 Firepower 4100/9300 シャーシ	ASAがインターフェイスを障害が発生していると見なし、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。 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]**
VPN 機能	

機能	説明
VTI での IKEv2、証明書ベース認証、および ACL のサポート	仮想トンネル インターフェイス（VTI）は、BGP（静的 VTI）をサポートするようになりました。スタンドアロン モードとハイ アベイラビリティ モードで、IKEv2 を使用できます。IPsec プロファイルにトラストポイントを設定することにより、証明書ベースの認証を使用できます。また、入力トラフィックをフィルタリングする access-group コマンドを使用して、VTI 上でアクセス リストを適用することもできます。 次の画面で、証明書ベース認証のトラストポイントを選択するオプションが導入されました。 **[Configuration] > [Site-to-Site VPN] > [Advanced] > [IPsec Proposals (Transform Sets)] > [IPsec Profile] > [Add]**
モバイル IKEv2（MobIKE）はデフォルトで有効になっています	リモート アクセス クライアントとして動作するモバイル デバイスは、移動中にトランスペアレント IP アドレスを変更する必要があります。ASA で MobIKE をサポートすることにより、現在の SA を削除せずに現在の IKE セキュリティ アソシエーション（SA）を更新することが可能になります。MobIKE は [always on] に設定されます。
SAML 2.0 SSO の更新	SAML 要求におけるシグネチャのデフォルト署名メソッドが SHA1 から SHA2 に変更され、ユーザーが rsa-sha1、rsa-sha256、rsa-sha384、rsa-sha512 の中から署名メソッドを選択して設定できるようになりました。 次の画面が変更されました。**[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [Single Sign On Servers] > [Add]**。
tunnelgroup webvpn-attributesの変更	**pre-fill-username** および **secondary-pre-fill-username** の値を **ssl-client** から **client** に変更しました。
AAA 機能	
ログイン履歴	デフォルトでは、ログイン履歴は 90 日間保存されます。この機能を無効にするか、期間を最大 365 日まで変更できます。1 つ以上の管理メソッド（SSH、ASDM、Telnet など）でローカル AAA 認証を有効にしている場合、この機能はローカル データベースのユーザー名にのみ適用されます。 次の画面が導入されました。**[Configuration] > [Device Management] > [Users/AAA] > [Login History]**
パスワードの再利用とユーザー名と一致するパスワードの使用を禁止するパスワード ポリシーの適用	最大 7 世代にわたるパスワードの再利用と、ユーザー名と一致するパスワードの使用を禁止できるようになりました。 次の画面が変更されました。**[Configuration] > [Device Management] > [Users/AAA] > [Password Policy]**

機能	説明
SSH公開キー認証を使用するユーザーの認証とパスワードを使用するユーザーの認証を区別します。	9.6(2) より前のリリースでは、ローカルユーザーデータベース（**ssh authentication**）を使用して AAA SSH 認証を明示的に有効にしなくても、SSH 公開キー認証（**aaa authentication ssh console LOCAL**）を有効にすることができました。9.6(2) では、ASA で AAA SSH 認証を明示的に有効にする必要がありました。このリリースでは、AAA SSH 認証を明示的に有効にする必要はありません。ユーザーに対して **ssh authentication** コマンドを設定すると、このタイプの認証を使用するユーザーのローカル認証がデフォルトで有効になります。さらに、明示的に AAA SSH 認証を設定すると、この設定はパスワード付きのユーザー名にのみ適用されます。また、任意の AAA サーバー タイプ（**aaa authentication ssh console radius_1** など）を使用できます。たとえば、一部のユーザーはローカルデータベースを使用して公開キー認証を使用し、他のユーザーは RADIUS でパスワードを使用できます。 変更された画面はありません。 バージョン *9.6(3)* でも同様です。
モニタリング機能とトラブルシューティング機能	
ASA クラッシュ発生時に実行中のパケット キャプチャの保存	以前は、ASA がクラッシュするとアクティブなパケット キャプチャは失われました。現在は、クラッシュが発生すると、パケット キャプチャは disk 0 に以下のファイル名で保存されます。[*context_name*.]*capture_name*.**pcap**。 変更された画面はありません。

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。

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

次の表に、ASA のアップグレードパスを示します。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） 開始バージョンと終了バージョンの間で、各リリースのアップグレードガイドラインを必ず確認してください。場合によっては、アップグレードする前に構成を変更する必要があります。そうしないと、停止が発生する可能性があります。

（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
9.7(x)	—	次のいずれかになります。 → 9.8(x)
9.6(x)	—	次のいずれかになります。 → 9.8(x)
9.5(x)	—	次のいずれかになります。 → 9.8(x)
9.4(x)	—	次のいずれかになります。 → 9.8(x)
9.3(x)	—	次のいずれかになります。 → 9.8(x)
9.2(x)	—	次のいずれかになります。 → 9.8(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。 → 9.8(x) → 9.1(7.4)
9.1(1)	→ 9.1(2)	次のいずれかになります。 → 9.8(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
9.0(2)、9.0(3)、または 9.0(4)	—	次のいずれかになります。 → 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。 → 9.8(x) → 9.1(7.4)
8.6(1)	→ 9.0(4)	次のいずれかになります。 → 9.8(x) → 9.1(7.4)
8.5(1)	→ 9.0(4)	次のいずれかになります。 → 9.8(x) → 9.1(7.4)
8.4(5+)	—	次のいずれかになります。 → 9.8(x) → 9.1(7.4) → 9.0(4)
8.4(1) ～ 8.4(4)	→ 9.0(4)	→ 9.8(x) → 9.1(7.4)
8.3(x)	→ 9.0(4)	次のいずれかになります。 → 9.8(x) → 9.1(7.4)
8.2(x) 以前	→ 9.0(4)	次のいずれかになります。 → 9.8(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 7.8(2.151) 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
CSCvf74630	DAP UI での互換性のないボタンの可視性

バージョン 7.8(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
CSCvf74630	DAP UI での互換性のないボタンの可視性
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

バージョン 7.8(1.150) 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

バージョン 7.8(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

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 7.8(2.151) 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
CSCvf67423	パフォーマンス修正が再導入された（ASDM 7.5.1 で導入され、ASDM 7.6.1 でバックアウトされた）
CSCvf82966	ASDM - ロギング：リアルタイムログを表示できない
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」

バージョン 7.8(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
CSCvc23816	ASDM のユーザー属性の変更によりユーザーパスワードが破壊される
CSCvd58610	マルチコンテキストモード使用時に DAP の選択条件が表示されなくなる
CSCvd81711	ASDM がユーザーアイデンティティ機能の NetBIOS プローブ設定のデフォルト設定を検出しない
CSCvd83906	ASDM が事前定義されたサービスオブジェクトの使用状況を検出できない
CSCvd90344	ASDM 7.7.150 アップロードウィザードが機能していない
CSCvd95382	ASDM がデフォルトのアイドルタイマー値を 1193:0:0（49D17H）と表示し、接続タイマーを変更する
CSCve02504	特定のブリッジグループに 5 つ以上のインターフェイスを追加できない
CSCve26349	ASDM がオブジェクトの説明を表示しない
CSCve55694	サービスオブジェクトで範囲を設定すると、ASDM が「service tcp destination eq-1」としてサービスを設定する

不具合 ID 番号	説明
CSCve64342	[Dynamic Access Policies] ページが凍結されており、HS イメージのアンインストール後はアクセスできない
CSCve69985	ASDM でトランスペアレントモードのインターフェイスごとに複数のスタティック MAC アドレステーブルエントリを使用できない
CSCve72433	ダイナミック ルーティング プロトコルのルートマップで使用されるプレフィックスリストの削除を要求する ASDM エラー
CSCve72787	オブジェクトで「Where Used」関数を使用すると、オブジェクトが手動 NAT の場合は java.lang.NullPointerException を発生させる
CSCve76967	ASDM Where Used オプションで結果が表示されない
CSCve93019	ダイナミックサイト間トンネルに関連付けられた暗号マップを編集すると ASDM がハングする
CSCvf08411	TLS 1.2 の暗号セキュリティレベルが「medium」の場合、ASDM が暗号アルゴリズムを正しく表示しない

バージョン 7.8(1.150) 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
CSCve66939	AWS で ASA のアップグレードオプションとして 9.8.1 が提供されない

バージョン 7.8(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
CSCvc65799	ASDM によってプッシュされた不正な NAT 免除ルール
CSCvc75477	注釈が編集され、時間範囲が追加されている場合、ASDM によって「Specified remark does not exist」が表示される
CSCvc77732	暗号マップの編集時に [Apply] ボタンが有効にならない
CSCvc86115	ASDM で 7.5.2.153 traceroute とコマンド ライン ユーティリティを併用すると機能しない
CSCvc90621	ASDM が VPN AnyConnect セッションのモニタリングをサポートしていない

不具合 ID 番号	説明
CSCvc92151	ASDM の [User] フィールドと [Security Group] フィールドに無効なコンテンツとランダムオブジェクトが表示される
CSCvd03071	グループポリシーが編集用にロックされている
CSCvd12493	ASDM が停止し、ソフトウェアアップデートの後はロードしない
CSCvd24557	ASDM が不適切なパブリックサーバー設定を ASA にプッシュしている
CSCvd90344	ASDM 7.7.150 アップロードウィザードが機能していない

エンドユーザーライセンス契約書

エンドユーザー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。

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

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。