Cisco ASDM 7.12(x) リリースノート

Cisco ASDM 7.12(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 7.12(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 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**。

- ASDM アップグレード ウィザード：内部的な変更により、このウィザードでは ASDM 7.10(1) 以降の使用のみがサポートされています。また、イメージの命名が変更されたため、ASA 9.10(1) 以降にアップグレードするには、ASDM 7.12(1) 以降を使用する必要があります。ASDM には ASA の以前のリリースと下位互換性があるため、実行している ASA バージョンを問わず、ASDM をアップグレードすることができます。

- 9.12(1) での SSH セキュリティの改善と新しいデフォルト設定：次の SSH セキュリティの改善点を参照してください。

  - SSH バージョン 1 はサポートされなくなりました。バージョン 2 のみがサポートされています。**ssh version 1** コマンドは **ssh version 2** に移行されます。

  - Diffie-Hellman Group 14 SHA256 キー交換のサポート。この設定がデフォルト（**ssh key-exchange group dh-group14-sha256**）になりました。以前のデフォルトは Group 1 SHA1 でした。SSH クライアントが Diffie-Hellman Group 14 SHA256 をサポートしていることを確認してください。サポートしていない場合は、「Couldn't agree on a key exchange algorithm」などのエラーが表示されることがあります。たとえば、OpenSSH では Diffie-Hellman Group 14 SHA256 がサポートされています。

- HMAC-SHA256整合性暗号のサポート。デフォルトは、高セキュリティの暗号セット（**ssh cipher integrity high** コマンドによって定義された hmac-sha1 および hmac-sha2-256）になりました。以前のデフォルトは中程度のセットでした。

- ASA 5506-X シリーズおよびASA 5512-X の ASA FirePOWER モジュールについては、9.10(1) 以降ではサポートされない：ASA 5506-X シリーズおよび5512-X では、メモリの制約により、9.10(1) 以降で ASA FirePOWER モジュールがサポートされなくなりました。このモジュールの使用を継続するには、9.9(x) 以前の状態のままにしておく必要があります。その他のモジュール タイプは引き続きサポートされます。9.10(1) 以降にアップグレードすると、FirePOWER モジュールにトラフィックを送信するための ASA 設定が消去されます。アップグレード前に設定を必ずバックアップしてください。FirePOWER イメージとその設定は SSD にそのままの状態で保持されます。ダウングレードする場合は、バックアップから ASA 設定をコピーして機能を復元できます。

- NULL-SHA TLSv1 暗号は廃止され、9.12(1) では削除されている：NULL-SHA は暗号化を提供せず、現在の脅威に対して安全とは見なされなくなったため、**tls-proxy** mode コマンド/オプションおよび **show ssl ciphers all** の出力に TLSv1 でサポートされている暗号を一覧表示すると削除されます。**ssl cipher tlsv1 all** コマンドと **ssl cipher tlsv1 custom NULL-SHA** コマンドも廃止され、削除されます。

- ローカル CA サーバは 9.12(1) で廃止され、以降のリリースで削除される：ASA がローカル CA サーバとして設定されている場合、デジタル証明書の発行、証明書失効リスト（CRL）の発行、および発行された証明書の安全な取り消しを行うために有効になります。この機能は古くなったため、**crypto ca server** コマンドは廃止されています。

- 9.12(1) ではデフォルトの trustpool が削除されている：PSB 要件、SEC-AUT-DEFROOT に準拠するため、「デフォルト」の信頼できる CA バンドルが ASA イメージから削除されています。その結果、 **crypto ca trustpool import default** コマンドと **crypto ca trustpool import clean default** コマンドも、その他の関連ロジックとともに削除されています。ただし、既存の展開では、これらのコマンドを使用して以前にインポートされた証明書はそのまま残ります。

- **ssl encryption** コマンドは 9.12(1) で削除されている：9.3(2) では、廃止が公表され、**ssl cipher** に置き換えられます。9.12(1) では、**ssl encryption** が削除され、サポートされなくなりました。

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（**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

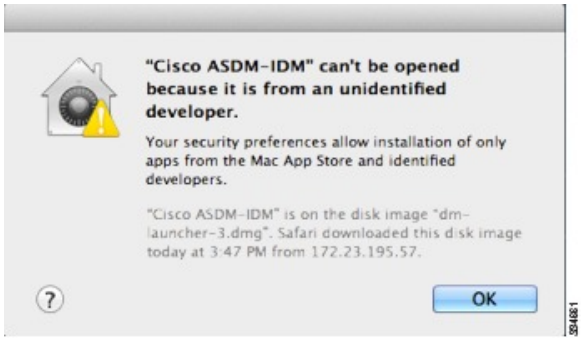
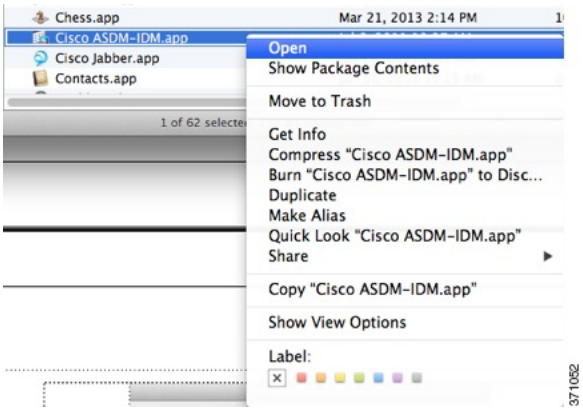
オペレーティング システム	ブラウザ				Oracle JRE	OpenJRE
	Internet Explorer	Firefox	Safari	Chrome		
• Microsoft Windows（英語および日本語）： • 10（SR 1809 については、CSCvp26795 の回避策を参照） • 8 • 7 • Server 2016 と Server 2019（ASA 管理のみ。FirePOWER モジュールの ASDM 管理はサポートされていません。その代わりに、ASA 管理に ASDM を使用しているときは、Firepower Management Center を使用して 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
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	注記
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。

条件	注記
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無効にしてください。
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	注記
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	注記
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。

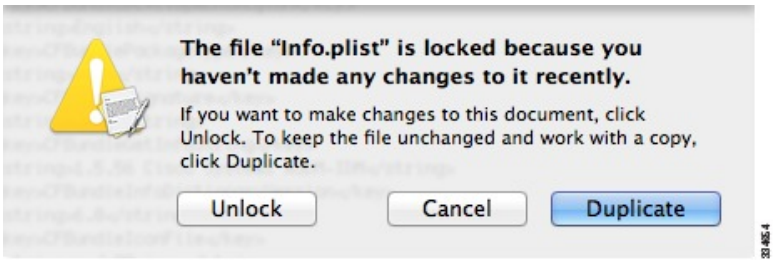
ステップ 3 **[Java]** > **[VMOptions]** で、「-Xmx」のプレフィックスが付いた文字列を変更し、必要なヒープ サイズを指定します。たとえば、768 MB の場合は -Xmx768M に変更し、1 GB の場合は -Xmx1G に変更します。

```
    <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。

ASA 9.12(4) の新機能

リリース日：**2020 年 5 月 26 日**

機能	説明
ルーティング機能	

機能	説明
マルチキャスト IGMP インターフェイスの状態制限の 500 から 5000 への引き上げ	マルチキャスト IGMP インターフェイスの状態制限が 500 から 5000 に引き上げられました。 新規/変更されたコマンド： **igmp limit** ASDM サポートはありません。
VPN 機能	
ネゴシエーション中の SA の絶対値としての最大数設定に対するサポート	ネゴシエーション中の SA の最大数を絶対値として 15000 まで、または最大デバイスキャパシティから得られる最大値を設定できるようになりました（以前はパーセンテージのみが許可されていました）。 新規/変更されたコマンド： **crypto ikev2 limit max-in-negotiation-sa value** ASDM サポートはありません。

ASA 9.12(3) の新機能

リリース日：2019 年 11 月 25 日

このリリースに新機能はありません。

ASA 9.12(2)/ASDM 7.12(2) の新機能

リリース日：2019 年 5 月 30 日

機能	説明
プラットフォーム機能	
Firepower 9300 SM-56 のサポート	セキュリティ モジュール、SM-56 を導入しました。 FXOS 2.6.1.157 が必要です。 変更された画面はありません。
管理機能	
SSH キー交換モードの設定は、管理コンテキストに限定されています。	管理コンテキストでは SSH キー交換を設定する必要があります。この設定は、他のすべてのコンテキストによって継承されます。 新規/変更された画面：**[Configuration] > [Device Management] > [Management Access] > [ASDM/HTTPS/Telnet/SSH] > [SSH Settings] > [DH Key Exchange]**
ASDM 機能	
ASDM の OpenJRE バージョン	OracleJRE ではなく、OpenJRE 1.8.x を使用する ASDM のバージョンをインストールできます。OpenJRE バージョンのファイル名は、**asdm-openjre-*version*.bin** です。

機能	説明
[Tools] > **[Preferences]** オプションで ASA FirePOWER モジュールのローカル管理ファイル フォルダを指定	ASA FirePOWER モジュールのローカル管理ファイルをインストールする場所を指定できるようになりました。設定された場所に対して読み取り/書き込み権限を持っている必要があります。 新規/変更された画面： **[Tools]** > **[Preferences]** > **SFR Location ウィザード**領域

ASA 9.12(1)/ASDM 7.12(1) の新機能

リリース：**2019 年 3 月 13 日**

機能	説明
プラットフォーム機能	
Firepower 4115、4125、および 4145 向け ASA	Firepower 4115、4125、および 4145 が導入されました。 FXOS 2.6.1 が必要です。 変更された画面はありません。
ASA および FTD を同じ Firepower 9300 の別のモジュールでサポート	ASA および FTD 論理デバイスを同じ Firepower 9300 上で展開できるようになりました。 FXOS 2.6.1 が必要です。 変更された画面はありません。
Firepower 9300 SM-40 および SM-48 のサポート	2 つのセキュリティ モジュール、SM-40 および SM-48 が導入されました。 FXOS 2.6.1 が必要です。 変更された画面はありません。
ファイアウォール機能	
GTPv1 リリース 10.12 のサポート	システムで GTPv1 リリース 10.12 がサポートされるようになりました。以前は、リリース 6.1 がサポートされていました。新しいサポートでは、25 件の GTPv1 メッセージおよび 66 件の情報要素の認識が追加されています。 さらに、動作の変更もあります。不明なメッセージ ID が許可されるようになりました。以前は、不明なメッセージはドロップされ、ログに記録されていました。 変更された画面はありません。

機能	説明
Cisco Umbrella の強化	Cisco Umbrella をバイパスする必要があるローカル ドメイン名を特定できるようになりました。これらのドメインの DNS 要求は、Umbrella を処理せず DNS サーバに直接送信されます。また、DNS 要求の解決に使用する Umbrella サーバも特定できるようになりました。さらに、Umbrella サーバを使用できない場合は、DNS 要求がブロックされないように、Umbrella インスペクション ポリシーをフェール オープンに定義することができます。 新規/変更された画面：**[Configuration]** > **[Firewall]** > **[Objects]** > **[Umbrella]**、**[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspect Maps]** > **[DNS]**
オブジェクト グループの検索しきい値がデフォルトで無効になりました。	これまではオブジェクト グループの検索が有効になると、この機能によりしきい値が適用され、パフォーマンスの低下を防止していました。そのしきい値が、デフォルトで無効になりました。しきい値は、**object-group-search threshold** コマンドを使用して有効にできます。 次の画面が変更されました：**[Configuration]** > **[Access Rules]** > **[Advanced]**
NAT のポート ブロック割り当てに対する暫定ログ	NAT のポート ブロックの割り当てを有効にすると、ポート ブロックの作成および削除中にシステムで syslog メッセージが生成されます。暫定ログの記録を有効にすると、指定した間隔でメッセージ 305017 が生成されます。メッセージは、その時点で割り当てられているすべてのアクティブ ポート ブロックをレポートします（プロトコル（ICMP、TCP、UDP）、送信元および宛先インターフェイス、IP アドレス、ポート ブロックを含む）。 新規/変更された画面：**[Configuration]** > **[Firewall]** > **[Advanced]** > **[PAT Port Block Allocation]**
VPN 機能	
debug aaa の新しい **condition** オプション	**condition** オプションが **debug aaa** コマンドに追加されました。このオプションを使用すると、グループ名、ユーザ名またはピア IP アドレスに基づいて VPN デバッグをフィルタ処理できます。 変更された画面はありません。
IKEv2 での RSA SHA-1 のサポート	IKEv2 の RSA SHA-1 ハッシュ アルゴリズムを使用して署名を生成できるようになりました。 新しい/変更された画面：
DES と3DES の両方の暗号化ライセンス、および使用可能な暗号のデフォルトの SSL 設定を表示します。	3DES 暗号化ライセンスの有無にかかわらず、デフォルトの SSL 設定を表示できるようになりました。さらに、デバイスでサポートされているすべての暗号を表示することもできます。 新規/変更されたコマンド： **show ssl information** 変更された画面はありません。

機能	説明
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
ハイ アベイラビリティとスケーラビリティの各機能	
サイトごとのクラスタリング用 Gratuitous ARP	ASA では、Gratuitous ARP（GARP）パケットを生成してスイッチング インフラストラクチャを常に最新の状態に保つようになりました。各サイトの優先順位値が最も高いメンバによって、グローバル MAC/IP アドレスの GARP トラフィックが定期的に生成されます。クラスタから送信されたサイトごとの MAC および IP アドレスとパケットがサイト固有の MAC アドレスおよび IP アドレスを使用するのに対し、クラスタで受信したパケットは、グローバル MAC アドレスおよび IP アドレスを使用します。トラフィックがグローバル MAC アドレスから定期的に生成されない場合、グローバル MAC アドレスのスイッチで MAC アドレスのタイムアウトが発生する可能性があります。タイムアウト後にグローバル MAC アドレスへのトラフィックがスイッチングインフラストラクチャ全体にわたりフラッディングされ、これによりパフォーマンスおよびセキュリティ上の問題が発生することがあります。各スパンド EtherChannel のユニットおよびサイト MAC アドレスごとにサイト ID を設定すると、GARP がデフォルトで有効になります。 新規/変更された画面：**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** > **[Cluster Configuration]** > **[Site Periodic GARP]** フィールド
マルチコンテキストモードの HTTPS リソース管理	リソースクラスの非 ASDM HTTPS セッションの最大数を設定できるようになりました。デフォルトでは、制限はコンテキストあたり最大 6 に設定でき、すべてのコンテキスト全体では最大 100 の HTTPS セッションを使用できます。 新規/変更されたコマンド： **limit-resource http** ASDM サポートはありません。
ルーティング機能	

機能	説明
認証のための OSPF キー チェーンのサポート	OSPF は、MD5 キーを使用してネイバーおよびルートアップデートを認証します。ASA では、MD5 ダイジェストの生成に使用されるキーには関連付けられている有効期間がありませんでした。したがって、キーを定期的に変更するにはユーザによる介入が必要でした。この制限を打破するために、OSPFv2 は循環キーを使用した MD5 認証をサポートしています。 キー チェーンのキーの承認と送信の有効期間に基づいて、OSPF 認証でキーおよびフォームの隣接関係を承認または拒否します。 新しい/変更された画面： • **[Configuration]** > **[Device Setup]** > **[Key Chain]** • **[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Setup]** > **[Authentication]** • **[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Setup]** > **[Virtual Link]**
証明書の機能	
登録用 URL のローカル CA を設定可能な FQDN	ASA の構成済み FQDN を使用する代わりに設定可能な登録用 URL の FQDN を作成するため、新しい CLI オプションが導入されました。この新しいオプションは、**crypto ca server** の **smpt** モードに追加されます。 新規/変更されたコマンド： **fqdn**
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	
enable ログイン時にパスワードの変更が必要になりました	デフォルトの **enable** のパスワードは空白です。ASA で特権 EXEC モードへのアクセスを試行する場合に、パスワードを 3 文字以上の値に変更することが必須となりました。空白のままにすることはできません。**no enable password** コマンドはサポートされなくなりました。 CLI で **aaa authorization exec auto-enable** を有効にすると、**enable** コマンド、**login** コマンド（特権レベル 2 以上のユーザ）、または SSH/Telnet セッションを使用して特権 EXEC モードにアクセスできます。これらの方法ではすべて、イネーブルパスワードを設定する必要があります。 このパスワード変更の要件は、ASDM のログインには適用されません。ASDM のデフォルトでは、ユーザ名を使用せず **enable** パスワードを使用してログインすることができます。 変更された画面はありません。

機能	説明
管理セッションの設定可能な制限	集約、ユーザ単位、およびプロトコル単位の管理セッションの最大数を設定できます。これまでは、セッションの集約数しか設定できませんでした。この機能がコンソール セッションに影響を与えることはありません。マルチ コンテキスト モードでは HTTPS セッションの数を設定することはできず、最大セッション数は 5 で固定されています。また、**quota management-session** コマンドはシステム コンフィギュレーションでは受け入れられず、代わりにコンテキスト コンフィギュレーションで使用できるようになっています。集約セッションの最大数が 15 になりました。0（無制限）または 16 以上に設定してアップグレードすると、値は 15 に変更されます。 新規/変更された画面：**[Configuration]** > **[Device Management]** > **[Management Access]** > **[Management Session Quota]**
管理権限レベルの変更通知	有効なアクセス（**aaa authentication enable console**）を認証するか、または特権 EXEC への直接アクセス（**aaa authorization exec auto-enable**）を許可すると、前回のログイン以降に割り当てられたアクセス レベルが変更された場合に ASA からユーザへ通知されるようになりました。 新しい/変更された画面： [Status] バー > [Login History] アイコン
IPv6 での NTP サポート	NTP サーバに IPv6 アドレスを指定できるようになりました。 新規/変更された画面：**[Configuration]** > **[Device Setup]** > **[System Time]** > **[NTP]** > **[Add]** ボタン > [Add NTP Server Configuration] ダイアログ ボックス
SSH によるセキュリティの強化	次の SSH セキュリティの改善を参照してください。 • SSH バージョン 1 はサポートされなくなりました。バージョン 2 のみがサポートされています。 • Diffie-Hellman Group 14 SHA256 キー交換のサポート。この設定がデフォルトになりました。以前のデフォルトは Group 1 SHA1 でした。 • HMAC-SHA256 整合性暗号のサポート。デフォルトは、高セキュリティの暗号セット（hmac-sha1 および hmac-sha2-256）になりました。以前のデフォルトは中程度のセットでした。 新しい/変更された画面： • **[Configuration]** > **[Device Management]** > **[Management Access]** > **[ASDM/HTTPS/Telnet/SSH]** • **[Configuration]** > **[Device Management]** > **[Advanced]** > **[SSH Ciphers]**

機能	説明
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。 新規/変更された画面： **[Configuration] > [Device Management] > [Management Access] > [HTTP Non-Browser Client Support]**
クラスタ制御リンク上でのみのコントロールプレーン パケットのキャプチャ	クラスタ制御リンク（およびデータ プレーン パケットなし）でのみコントロールプレーン パケットをキャプチャできるようになりました。このオプションは、マルチコンテキスト モードのシステムで、ACL を使用してトラフィックを照合できない場合に役立ちます。 新規/変更された画面： **[Wizards] > [Packet Capture Wizard] > [Cluster Option]**
debug conn コマンド	接続処理を記録する 2 つの履歴メカニズムを提供するために **debug conn** コマンドが追加されました。1 つ目の履歴リストはスレッドの操作を記録するスレッドごとのリストです。2 つ目の履歴リストは conn グループに操作を記録するリストです。接続が有効になっている場合、接続のロック、ロック解除、削除などの処理イベントが 2 つの履歴リストに記録されます。問題が発生すると、これら 2 つのリストを使用して不正なロジックを判断する処理で確認することができます。 新規/変更されたコマンド： **debug conn**
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**
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の有効化および無効化の ASDM 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]**
マルチコンテキスト モードのシステムの ASDM [Home] ペインに設定可能なグラフ更新間隔	マルチコンテキスト モードのシステムでは、[Home] ペインのグラフの更新間隔の時間を設定できるようになりました。 新規/変更された画面： **[Tools] > [Preferences] > [Graph User time interval in System Context]**

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
9.10(x)	—	次のいずれかになります。 → **9.12(x)** → 9.10(x)
9.9(x)	—	次のいずれかになります。 → **9.12(x)** → 9.10(x) → 9.9(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
9.8(x)	—	次のいずれかになります。 → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)**
9.7(x)	—	次のいずれかになります。 → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)**
9.6(x)	—	次のいずれかになります。 → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x)
9.5(x)	—	次のいずれかになります。 → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x)
9.4(x)	—	次のいずれかになります。 → **9.12(x)** → 9.10(x) → 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。 → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x)
9.2(x)	—	次のいずれかになります。 → **9.12(x)** → 9.10(x) → 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。 → **9.12(x)** → 9.10(x) → 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。 → **9.12(x)** → 9.10(x) → 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
9.0(2)、9.0(3)、または 9.0(4)	—	次のいずれかになります。 → **9.12(x)** → 9.10(x) → 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。 → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)
8.6(1)	→ 9.0(4)	次のいずれかになります。 → **9.12(x)** → 9.10(x) → 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。 → **9.12(x)** → 9.10(x) → 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
8.4(5+)	—	次のいずれかになります。 → **9.12(x)** → 9.10(x) → 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)	→ **9.12(x)** → 9.10(x) → 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。 → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)
8.2(x) 以前	→ 9.0(4)	次のいずれかになります。 → **9.12(x)** → 9.10(x) → 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 7.12(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。

警告 ID 番号	説明
CSCvo10929	アクセス リスト エラー：サイト間 VPN の RSA 署名をオフにしている間

バージョン 7.12(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。

警告 ID 番号	説明
CSCvo10929	アクセス リスト エラー：サイト間 VPN の RSA 署名をオフにしている間

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 7.12(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。

警告 ID 番号	説明
CSCvo26166	ASDM が外部グループ ポリシーを AnyConnect/IKEv1/IKEv2 RA トンネル グループに適用できない
CSCvp01248	ASDM スタートアップ ウィザードのインターフェイス 編集ボタンが機能しない
CSCvp67520	ASDM 7.12.1：既存の NAT ルールの編集が ASA（9.12.1）に正常にプッシュできない
CSCvp69678	AnyConnect イメージが ASDM から消える

バージョン 7.12(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。

警告 ID 番号	説明
CSCuz09934	ASDM：パスワードの有効期限警告メッセージがログイン後に表示されなくなる
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
CSCvi38815	ACL 行のログ レベルを変更すると、ASDM によって注釈が削除される
CSCvi66705	読み取り専用ユーザがマルチコンテキスト モードの ASDM をオープンできない
CSCvi87301	ASDM：ASA クラスタの詳細が表示されず、管理コンテキストに「Page not found」というエラーが表示される
CSCvj37182	ASDM でリモート アクセス VPN の DAP を起動できない
CSCvj91403	ASDM 経由でポート チャネルを編集すると常に MIO ポート チャネル ID が要求される
CSCvk71176	ASDM 7.9 (2) 152 で「uploaded file is not a valid ASA-SM image」という警告が表示される
CSCvm21655	ASDM では、ACL の注釈が重複し、すべてのサブエントリに表示される
CSCvm37098	ASDM で変更を加えずにサイト間トンネルを編集しようとすると NAT Exempt ルールが削除される
CSCvm64354	30 秒に設定されたチャート更新頻度による ASDM イメージ特別リリース
CSCvm68799	ASDM 復元機能が実行され、複数の同一カテゴリ ファイルで AC プロファイルのファイルが上書きされる

警告 ID 番号	説明
CSCvn08410	split-tunnel-all-dns を CLI から有効にしても ASDM 上に反映されない。ASDM から CLI に動作する
CSCvn20484	クラスマップに単一のルールがある場合、ASDM はルールアクションを無効/ネゲートしようとするとエラーをスローする
CSCvn32924	Firepower のタブがマルチコンテキスト環境の ASDM v7.9.2.X を使用した ASA v9.9 (2) 上の ASDM に表示されない
CSCvn38874	ACL の IP で TCT/HTTP を置換したときの ASDM エラー
CSCvn72617	ASDM：ネストされた TCP-UDP オブジェクト グループがリストとしても、子オブジェクトとしても表示されない
CSCvo23506	マルチコンテキスト モードの ASDM が「show flow-offload info」というメッセージを表示し、オープンできない

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/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。