Cisco ASDM 7.16(x) リリースノート

初版：2021 年 5 月 26 日

最終更新：2023 年 8 月 16 日

Cisco ASDM 7.16(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 7.16(x) のリリース情報が記載されています。

特記事項

- **9.16(3.19)/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）
- **MD5 ハッシュと DES 暗号化を使用する SNMPv3 ユーザーはサポートされなくなり、9.16(1) にアップグレードするとユーザーが削除されます。**アップグレードする前に、**snmp-server user** コマンドを使用してユーザー設定をより高いセキュリティアルゴリズムに変更してください。
- **9.16(1) では SSH ホストキーアクションが必要**：RSA に加えて、EDDSA および ECDSA ホストキーのサポートが追加されました。ASA は、存在する場合、EDDSA、ECDSA、RSA の順にキーの使用を試みます。9.16(1) にアップグレードすると、ASA は既存の RSA キーを使用するようにフォールバックします。ただし、できるだけ早く **crypto key generate {eddsa | ecdsa}** コマンドを使用してセキュリティレベルの高いセキュリティキーを生成することを推奨します。また、**ssh key-exchange hostkey rsa** コマンドで RSA キーを使用するように ASA を明示的に設定する場合は、2048 ビット以上のキーを生成する必要があります。アップグレードの互換性のために、ASA はデフォルトのホストキー設定が使用されている場合にのみ、より小さい RSA ホストキーを使用します。RSA のサポートは今後のリリースで削除されます。
- **9.16 以降では、RSA キーを使用した証明書は ECDSA 暗号と互換性がない**：ECDHE_ECDSA 暗号グループを使用する場合は、ECDSA 対応キーを含む証明書を使用してトラストポイントを設定します。
- **2048 よりも小さい RSA キーは、9.16(1) では生成できません**：**crypto key generate rsa** コマンドを使用して 2048 よりも小さい RSA キーを生成することはできません。

SSH の場合、アップグレード後も既存の小さいキーを引き続き使用できますが、より大きなサイズまたはより高いセキュリティキータイプにアップグレードすることを推奨します。

その他の機能については、2048 よりも小さい RSA キーサイズで署名された既存の証明書は、ASA 9.16.1 以降では使用できません。**crypto ca permit-weak-crypto** コマンドを使用して既存の小さいキーの使用を許可できますが、このコマンドを使用しても、新しい小さい RSA キーを生成することはできません。

- **ssh version コマンドは 9.16(1) で削除されました**：このコマンドは削除されました。SSH バージョン 2 のみサポートされます。
- **SAMLv1 機能は 9.16(1) で削除されました**：SAMLv1 のサポートは削除されました。
- **9.16(1) では DH グループ 2、5、24 はサポートされません**：SSL DH グループ設定の DH グループ 2、5、および 24 のサポートは削除されました。**ssl dh-group** コマンドが更新され、コマンドオプション **group2**、**group5**および**group24**が削除されました。
- **シスコは、ASA バージョン 9.17(1) で有効なクライアントレス SSL VPN の非推奨機能を発表**：9.17(1) より前のリリースでは、限定的なサポートが継続されます。
- ASA 9.15(1) 以降では、ASA 5525-X、ASA 5545-X、および ASA 5555-X はサポート対象外：ASA 9.14(x) がサポートされている最後のバージョンです。ASA FirePOWER モジュールについては、6.6 がサポートされている最後のバージョンです。
- **Firepower 1010 の場合の無効な VLAN ID による問題発生の可能性**：9.15(1) 以降にアップグレードする前に、3968 ー 4047 の範囲内のスイッチポートに VLAN を使用していないことを確認してください。これらの ID は内部使用専用であり、9.15(1) には、これらの ID を使用していないことを確認するチェックが含まれます。たとえば、フェールオーバーペアのアップグレード後にこれらの ID が使用されていた場合、フェールオーバーペアは一時停止状態になります。詳細については、「CSCvw33057」を参照してください。
- **Chacha-poly 暗号**：AnyConnect には、更新された一連のサポートされている暗号化アルゴリズムがあります。『AnyConnect Secure Mobility Client Features, Licenses, and OSs, Release 4.10』[英語] は、TLS ベースの VPN トラフィックを開始するときに ASA に提案されます。

システム要件

ASDM には、4 コア以上の CPU を搭載したコンピュータが必要です。コア数が少ないと、メモリ使用量が高くなる可能性があります。

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。

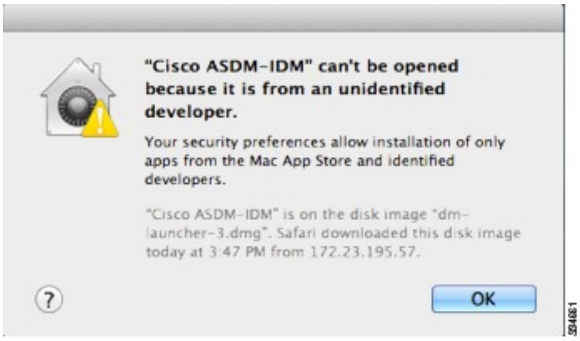
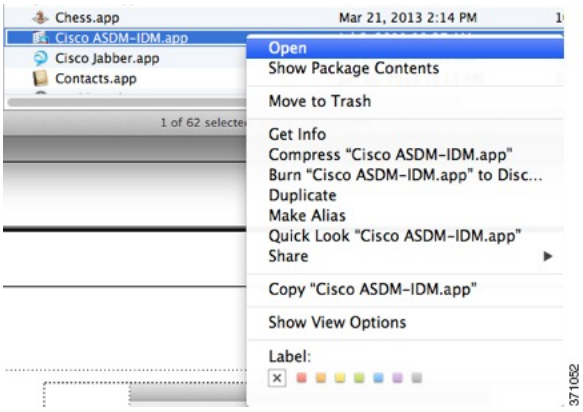
表 *1 : ASA* と *ASA FirePOWER* : *ASDM* オペレーティングシステムとブラウザの要件

オペレーティング システム	ブラウザ			Oracle JRE	OpenJRE
	Firefox	Safari	Chrome		
Microsoft Windows（英語および日本語）： • 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 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、FMC 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	サポートなし	対応	8.0 バージョン 8u261 以降	1.8 （注） Windows 7 または 10（32 ビット）のサポートなし
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	1.8

ASDM の互換性に関する注意事項

次の表に、ASDM の互換性に関する警告を示します。

条件	注意
Windows 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。
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。メモリが枯渇していることを確認するには、Java コンソールで「java.lang.OutOfMemoryError」メッセージをモニターします。

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。

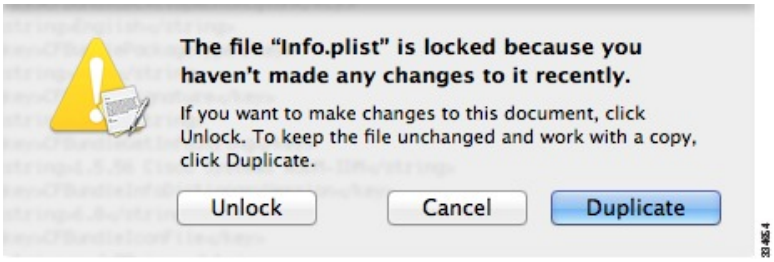
ステップ 3 **[Java]** > **[VMOptions]** で、「-Xmx」のプレフィックスが付いた文字列を変更し、必要なヒープサイズを指定します。たとえば、768 MB の場合は -Xmx768M に変更し、1 GB の場合は -Xmx1G に変更します。

```
    <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 9.16(4) の新機能

リリース日：2022 年 10 月 13 日

このリリースに新機能はありません。

ASA 9.16(3) の新機能

リリース日：2022 年 4 月 6 日

このリリースに新機能はありません。

ASA 9.16(2) の新機能

リリース：2021 年 8 月 18 日

このリリースに新機能はありません。

ASDM 7.16(1.150) の新機能

リリース：2021 年 6 月 15 日

このリリースに新機能はありません。

ASA 9.16(1)/ASDM 7.16(1) の新機能

リリース日：2021 年 5 月 26 日

機能	説明
ファイアウォール機能	

機能	説明
システム定義の NAT ルールの新しいセクション 0。	新しいセクション 0 が NAT ルールテーブルに追加されました。このセクションは、システムの使用に限定されます。システムが正常に機能するために必要なすべての NAT ルールがこのセクションに追加され、これらのルールは作成したルールよりも優先されます。以前は、システム定義のルールがセクション 1 に追加され、ユーザー定義のルールがシステムの適切な機能を妨げる可能性がありました。セクション 0 のルールを追加、編集、または削除することはできませんが、**show nat detail** コマンド出力に表示されます。
デフォルトの SIP インスペクション ポリシー マップは、非 SIP トラフィックをドロップします。	SIP インスペクションされるトラフィックでは、現在、デフォルトでは非 SIP トラフィックがドロップされます。以前のデフォルトでは、SIP のインスペクション対象ポートで非 SIP トラフィックが許可されていました。 デフォルトの SIP ポリシーマップが変更され、**no traffic-non-sip** コマンドが追加されました。
GTP インスペクションでドロップされる IMSI プレフィックスを指定する機能です。	GTP インスペクションでは、許可する Mobile Country Code/Mobile Network Code（MCC/MNC）の組み合わせを識別するために、IMSI プレフィックス フィルタリングを設定できます。ドロップする MCC/MNC の組み合わせに対して IMSI フィルタリングを実行できるようになりました。これにより、望ましくない組み合わせをリストにして、デフォルトで他のすべての組み合わせを許可することができます。 次の画面が変更されました：GTP インスペクションマップの [IMSI Prefix Filtering] タブに [Drop] オプションが追加されました。
初期接続の最大セグメントサイズ（MSS）を設定します。	サービスポリシーを設定して、初期接続制限に達したときに初期接続の SYN cookie を生成するためのサーバーの最大セグメントサイズ（MSS）を設定できます。これは、最大初期接続数も設定するサービスポリシーの場合に意味があります。 新規/変更された画面：[Add/Edit Service Policy] ウィザードの **[Connection Settings]**
多対 1 および 1 対多接続の CPU 使用率とパフォーマンスが向上しました。	ダイナミック NAT / PAT およびスキャン脅威検出とホスト統計情報を含む接続を除き、システムは接続の作成時に、ローカルホストオブジェクトを作成せず、ロックすることもなくなりました。これにより、多数の接続を同じサーバー（ロードバランサや Web サーバーなど）に対して確立する場合や、1 つのエンドポイントが多数のリモートホストに接続する場合に、パフォーマンスと CPU 使用率が向上します。 次のコマンドが変更されました：**clear local-host**（廃止）、 **show local-host**
プラットフォーム機能	
VMware ESXi 7.0 用の ASAv サポート	ASAv 仮想プラットフォームは、VMware ESXi 7.0 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 7.0 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。 変更されたコマンドはありません。 変更された画面はありません。

機能	説明
ASAv の Intel® QuickAssist テクノロジー（QAT）	ASAv は、 Intel QuickAssist（QAT）8970 PCI アダプタを使用する ASAv 展開にハードウェア暗号化アクセラレーションを提供します。ASAv を使用した ASAv のハードウェア暗号化アクセラレーションは、VMware ESXi および KVM でのみサポートされます。 変更されたコマンドはありません。 変更された画面はありません。
OpenStack の ASAv	ASAv 仮想プラットフォームに OpenStack のサポートが追加されました。 変更されたコマンドはありません。 変更された画面はありません。
ハイ アベイラビリティとスケーラビリティの各機能	
Firepower 4100/9300 でのクラスタリングの PAT ポートブロック割り当てが改善されました	PAT ポートブロック割り当ての改善により、制御ユニットはノードに参加するためにポートを確保し、未使用のポートを積極的に再利用できるようになります。割り当てを最適化するために、**cluster-member-limit** コマンドを使用して、クラスタ内に配置する予定の最大ノードを設定できます。これにより、制御ユニットは計画されたノード数にポートブロックを割り当てることができ、使用する予定のない追加のノード用にポートを予約する必要がなくなります。デフォルトは 16 ノードです。また、syslog 747046 を監視して、新しいノードに使用できるポートが十分にあることを確認することもできます。 新規/変更された画面：**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** > **[Cluster Configuration]** > **[Cluster Member Limit]** フィールド
show cluster history コマンドの改善	**show cluster history** コマンドの出力が追加されました。 新規/変更されたコマンド： **show cluster history brief**、**show cluster history latest**、**show cluster history reverse**、**show cluster history time**
Firepower 1140 の最大コンテキスト数が 5 から 10 に増加	Firepower 1140 は、最大 10 のコンテキストをサポートするようになりました。
証明書の機能	
認定のための Enrollment over Secure Transport（EST）	ASA は、Enrollment over Secure Transport（EST）を使用した証明書の登録をサポートしています。ただし、EST 登録は、RSA キーおよび ECDSA キーとのみ使用するように設定できます。EST 登録用に設定されたトラストポイント用に EdDSA キーペアを使用することはできません。 新規/変更された画面：**[Configuration]** > **[Device Management]** > **[Certificate Management]** > **[Identity Certificate]** > **[Advanced]**.

機能	説明
新しい EdDSA キーのサポート	新しいキーオプション EdDSA が、既存の RSA および ECDSA オプションに追加されました。 新規/変更された画面：**[Configuration]** > **[Device Management]** > **[Certificate Management]** > **[Identity Certificate]** > **[Add Identity Certificates]** > **[Add Key Pair]**
証明書キーの制限を上書きするコマンド	認定に SHA1with RSA 暗号化アルゴリズムを使用するためのサポート、および RSA キーサイズが 2048 未満の証明書のサポートが削除されました。**crypto ca permit-weak-crypto** コマンドを使用して、これらの制限を上書きできます。 新規/変更された画面：**[Configuration]** > **[Device Management]** > **[Certificate Management]** > **[Identity Certificate]**、**[Configuration]** > **[Remote Access VPN]** > **[Certificate Management]** > **[Identity Certificate]**、および**[Configuration]** > **[Remote Access VPN]** > **[Certificate Management]** > **[Code Signer]**
管理およびトラブルシューティングの機能	
SSH セキュリティの改善	SSH が次の SSH セキュリティの改善をサポートするようになりました。 • ホストキーの形式：**crypto key generate** {**eddsa** | **ecdsa**}。RSA に加えて、EdDSA および ECDSA ホストキーのサポートが追加されました。ASA は、存在する場合、EdDSA、ECDSA、RSA の順にキーの使用を試みます。**ssh key-exchange hostkey rsa** コマンドで RSA キーを使用するように ASA を明示的に設定する場合は、2048 ビット以上のキーを生成する必要があります。アップグレードの互換性のために、ASA はデフォルトのホストキー設定が使用されている場合にのみ、より小さい RSA ホストキーを使用します。RSA のサポートは今後のリリースで削除されます。 • キー交換アルゴリズム：**ssh key-exchange group** {**ecdh-sha2-nistp256** | **curve25519-sha256**} • 暗号化アルゴリズム：**ssh cipher encryption chacha20-poly1305@openssh.com** • SSH バージョン 1 はサポートされなくなりました。**ssh version** コマンドは削除されました。 新しい/変更された画面： • **[Configuration]** > **[Device Management]** > **[Management Access]** > **[ASDM/HTTPS/Telnet/SSH]** • **[Configuration]** > **[Device Management]** > **[Certificate Management]** > **[Identity Certificates]** • **[Configuration]** > **[Device Management]** > **[Advanced]** > **[SSH Ciphers]**
モニタリング機能	

機能	説明
SNMPv3 認証	ユーザー認証に SHA-224 および SHA-384 を使用できるようになりました。ユーザー認証に MD5 を使用できなくなりました。 暗号化に DES を使用できなくなりました。 新規/変更された画面：**[構成（Configuration）] > [デバイス管理（Device Management）] > [管理アクセス（Management Access）] > [SNMP]**
VPN 機能	
スタティック VTI での IPv6 のサポート	ASA は、仮想トンネルインターフェイス（VTI）の設定で IPv6 アドレスをサポートしています。 VTI トンネル送信元インターフェイスには、トンネルエンドポイントとして使用するように設定できる IPv6 アドレスを設定できます。トンネル送信元インターフェイスに複数の IPv6 アドレスがある場合は、使用するアドレスを指定できます。指定しない場合は、リストの最初の IPv6 グローバルアドレスがデフォルトで使用されます。 トンネルモードは、IPv4 または IPv6 のいずれかです。ただし、トンネルをアクティブにするには、VTI で設定されている IP アドレスタイプと同じである必要があります。IPv6 アドレスは、VTI のトンネル送信元インターフェイスまたはトンネル宛先インターフェイスに割り当てることができます。
デバイスあたり 1024 個の VTI インターフェイスのサポート	デバイスに設定できる VTI の最大数が、100 個から 1024 個に増加しました。 プラットフォームが 1024 個を超えるインターフェイスをサポートしている場合でも、VTI の数はそのプラットフォームで設定可能な VLAN の数に制限されます。たとえば、ASA 5510 は 100 個の VLAN をサポートしているため、トンネル数は 100 から設定された物理インターフェイスの数を引いた数になります。 新規/変更された画面：なし
SSL の DH グループ 15 のサポート	SSL 暗号化の DH グループ 15 のサポートが追加されました。 新規/変更されたコマンド： **ssl dh-group group15**
IPsec 暗号化の DH グループ 31 のサポート	IPsec 暗号化の DH グループ 31 のサポートが追加されました。 新規/変更されたコマンド： **set pfs**
IKEv2 キューの SA を制限するサポート	SA-INIT パケットのキュー数を制限するサポートが追加されました。 新規/変更されたコマンド： **crypto ikev2 limit queue sa_init**
IPsec 統計情報をクリアするオプション	IPsec 統計情報をクリアおよびリセットするための CLI が導入されました。 新規/変更されたコマンド：**clear crypto ipsec stats** および**clear ipsec stats**

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 9.14 は ASA 5525-X、5545-X、および 5555-X の最終バージョンです。

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

ASA 9.2 は ASA 5505 の最終バージョンです。

ASA 9.1 は ASA 5510、5520、5540、5550、および 5580 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
9.15	—	次のいずれかになります。 → **9.16**
9.14	—	次のいずれかになります。 → **9.16** → 9.15

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
9.13	—	次のいずれかになります。 → **9.16** → 9.15 → 9.14
9.12	—	次のいずれかになります。 → **9.16** → 9.15 → 9.14
9.10	—	次のいずれかになります。 → **9.16** → 9.15 → 9.14 → 9.12
9.9	—	次のいずれかになります。 → **9.16** → 9.15 → 9.14 → 9.12
9.8	—	次のいずれかになります。 → **9.16** → 9.15 → 9.14 → 9.12

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	—	次のいずれかになります。 → **9.16** → 9.15 → 9.14 → 9.12 → 9.8
9.6	—	次のいずれかになります。 → **9.16** → 9.15 → 9.14 → 9.12 → 9.8
9.5	—	次のいずれかになります。 → **9.16** → 9.15 → 9.14 → 9.12 → 9.8
9.4	—	次のいずれかになります。 → **9.16** → 9.15 → 9.14 → 9.12 → 9.8

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	—	次のいずれかになります。 → **9.16** → 9.15 → 9.14 → 9.12 → 9.8
9.2	—	次のいずれかになります。 → **9.16** → 9.15 → 9.14 → 9.12 → 9.8
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。 → 9.14 → **9.12** → 9.8 → 9.1(7.4)
9.1(1)	→ 9.1(2)	次のいずれかになります。 → 9.14 → **9.12** → 9.8 → 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。 → 9.14 → **9.12** → 9.8 → 9.6 → 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(1)	→ 9.0(4)	次のいずれかになります。 → 9.14 → **9.12** → 9.8 → 9.1(7.4)
8.6(1)	→ 9.0(4)	次のいずれかになります。 → 9.14 → **9.12** → 9.8 → 9.1(7.4)
8.5(1)	→ 9.0(4)	次のいずれかになります。 → **9.12** → 9.8 → 9.1(7.4)
8.4(5+)	—	次のいずれかになります。 → **9.12** → 9.8 → 9.1(7.4) → 9.0(4)
8.4(1) ～ 8.4(4)	→ 9.0(4)	→ **9.12** → 9.8 → 9.1(7.4)
8.3	→ 9.0(4)	次のいずれかになります。 → **9.12** → 9.8 → 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 以前	→ 9.0(4)	次のいずれかになります。 → **9.12** → 9.8 → 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 7.16(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
CSCvu01215	アプライアンスモード：CCO から ASA イメージをダウンロードしている間にチェックサムが一致しない問題
CSCvu60781	ASDM：Launcher 1.9.1 での MAC のサポートが必要
CSCvv17403	同時接続 prempt で遅延のなくトンネルの削除を無効にするためのチェックボックスが使用できない

不具合 ID 番号	説明
CSCvv83043	9161/7161 CLI に従って VPN ウィザードで暗号を変更する必要がある

バージョン 7.16(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
CSCvu01215	アプライアンスモード：CCO から ASA イメージをダウンロードしている間にチェックサムが一致しない問題
CSCvu60781	ASDM：Launcher 1.9.1 での MAC のサポートが必要
CSCvv17403	同時接続 prempt で遅延のなくトンネルの削除を無効にするためのチェックボックスが使用できない
CSCvv83043	9161/7161 CLI に従って VPN ウィザードで暗号を変更する必要がある

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 7.16(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
CSCvx31769	異なる管理者やコンテキスト間で切り替えると、ASDM セッションが突然終了する
CSCvy44376	SSH 暗号（aes128-gcm@openssh.com および chacha20-poly1305@openssh.com）が ASDM GUI にない
CSCvy50917	ssh key-exchange group オプションは、MC モード、ユーザーコンテキストでは無効にする必要がある

バージョン 7.16(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
CSCvr82737	ASDM 7.12.2 が SSL ハンドシェイク中にクライアント証明書を送信しない
CSCvt34517	LZMA/LzmaInputStream.class の無効な SHA1 署名ファイルダイジェストによるエラーで ASDM が起動できない

不具合 ID 番号	説明
CSCvt88739	ASDM v7.14.1.46 でグループポリシーにスプリットトンネリングを設定できない
CSCvu54682	Power over Ethernet ダイアログのチェックボックスのラベルが誤っている
CSCvu67773	ASDMが s2s VPNの 接続プロファイルの作成中に誤った外部アイデンティティ NAT ルールを作成する
CSCvu69664	DNS Class-Map 内の dns-class の値が誤っている
CSCvu82820	ASDM UI から engineID フィールドが削除される：ASA トレースバック
CSCvu90263	ASDM：「no management-only」で設定されたインターフェイスでも管理に関する ACL を追加できない
CSCvv12123	ASDM OSPF プロセスの詳細プロパティの NSF 待機間隔は必須ではない
CSCvv27284	AnyConnect カスタム属性名の値を編集できない
CSCvv39481	ASDM を使用している場合、スタートアップ コンフィギュレーションを復元できない
CSCvv87029	ASDMのチェックボックスの横をクリックすると、チェックボックスが選択される
CSCvw39124	誤った値を設定すると、NSF 待機間隔警告ポップアップが表示されない
CSCvw61817	メモリステータスの [Context Usage] タブの [Peak Usage (KB)] に ASDM から「該当なし」と表示される
CSCvw86103	マスターとスレーブで同じイベントを表示する ASA クラスタ ASDM リアルタイムログビューア
CSCvx40955	ASDM がパーサーエラーごとに SCTP ポートを認識しない

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。

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。