Cisco ASDM 7.15(x) リリースノート

Cisco ASDM 7.15(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 7.15(x) のリリース情報が記載されています。

特記事項

- 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。
- **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。
- 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) 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。
- 9.13 のアプライアンスモードでの Firepower 1000 と 2100 の ASDM Cisco.com アップグレードウィザードの失敗：ASDM Cisco.com アップグレードウィザードは 9.13 からのアップグレードには使用できません（[Tools] > [Check for ASA/ASDM Updates]）。このウィザードでは ASDM を 7.13 からアップグレードできますが、ASA イメージのアップグレードはグレー表示になっています（CSCvt72183）。回避策として、次のいずれかの方法を使用してください。
  - ASA と ASDM の両方で **[Tools] > [Upgrade Software from Local Computer]** を使用します。
  - **[Tools] > [Check for ASA/ASDM Updates]** を使用して ASDM をアップグレードした後で新しい ASDM を使用して ASA イメージをアップグレードします。**致命的なインストールエラー**が表示されることがあることに注意してください。この場合は、**[OK]** をクリックします。次に、**[Configuration] > [Device Management] > [System Image/Configuration] > [Boot Image/Configuration]** 画面で、ブートイメージを手動で設定する必要があります。設定を保存し、ASA をリロードします。
- **ASA 5506-X、5508-X、および 5516-X の ROMMON のバージョン 1.1.15 以降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**。

- **ISA 3000 の ROMMON のバージョン 1.0.5 以降へのアップグレード**：これらの ISA 3000 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：1.0.5 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**。

- SAMLv1 機能の廃止：SAMLv1 のサポートは廃止されました。
- ASA 9.15(1) での低セキュリティ暗号の削除：IKE および IPsecで使用される安全性の低い次の暗号のサポートが廃止されました。
  - Diffie-Hellman グループ：2 および 24
  - 暗号化アルゴリズム：DES、3DES、AES-GMAC、AES-GMAC-192、AES-GMAC-256、NULL、ESP-3DES、ESP-DES、ESP-MD5-HMAC
  - ハッシュアルゴリズム：MD5

（注） 安全性の低い SSH 暗号と SSL 暗号はまだ廃止されていません。

ASA の以前のバージョンからバージョン 9.15(1) にアップグレードする前に、9.15(1) でサポートされている暗号を使用するように VPN 設定を更新する必要があります。そのようにしないと、古い設定が拒否されます。設定が拒否されると、コマンドに応じて次のいずれかのアクションが実行されます。

- コマンドはデフォルトの暗号を使用する。
- コマンドが削除される。

アップグレード前の設定の修正は、クラスタリングまたはフェールオーバーの展開で特に重要です。たとえば、セカンダリユニットが 9.15(1) にアップグレードされ、削除された暗号がプライマリからこのユニットに同期された場合、セカンダリユニットは設定を拒否します。この拒否により、クラスタへの参加の失敗などの予期しない動作が発生する可能性があります。

IKEv1：次のサブコマンドが削除されています。

- **crypto ikev1 policy** *priority*:
  - **hash md5**
  - **encryption 3des**
  - **encryption des**
  - **group 2**

IKEv2：次のサブコマンドが削除されています。

- **crypto ikev2 policy** *priority*:
  - **prf md5**
  - **integrity md5**
  - **group 2**
  - **group 24**
  - **encryption 3des**
  - **encryption des**
  - **encryption null**

IPsec：次のサブコマンドが削除されています。

- **crypto ipsec ikev1 transform-set** ***name*** **esp-3des esp-des esp-md5-hmac**
- **crypto ipsec ikev2 ipsec-proposal** ***name***
  - **protocol esp integrity md5**
  - **protocol esp encryption 3des aes-gmac aes-gmac- 192 aes-gmac -256 des**
- **crypto ipsec profile** ***name***
  - **set pfs group2 group24**

Crypto Map：次のサブコマンドが削除されています。

- **crypto map** ***name sequence*** **set pfs group2**
- **crypto map** ***name sequence*** **set pfs group24**
- **crypto map** ***name sequence*** **set ikev1 phase1-mode aggressive group2**

- CRL 配布ポイント設定の再導入：9.13(1) で削除された静的 CDP URL 設定オプションが **match-certificate** コマンドに再導入されました。
- バイパス証明書の有効性チェックオプションの復元：CRL またはOCSPサーバーとの接続の問題による失効チェックをバイパスするオプションが復元されました。

次のサブコマンドが復元されました。

- **revocation-check crl none**
- **revocation-check ocsp none**
- **revocation-check crl ocsp none**
- **revocation-check ocsp crl none**

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。

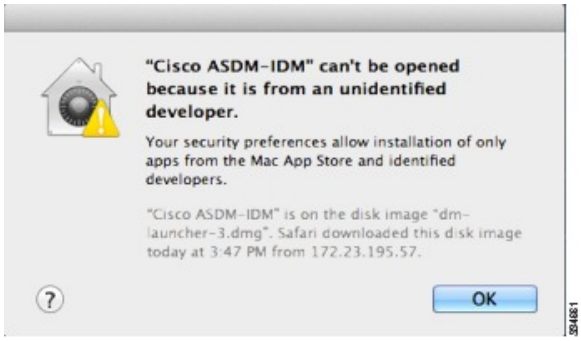
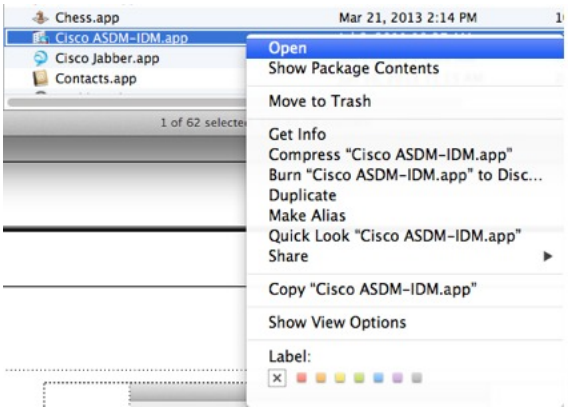
表 *1 : ASA* と *ASA FirePOWER* : *ASDM* オペレーティングシステムとブラウザの要件

オペレーティング システム	ブラウザ			Oracle JRE	OpenJRE
	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 （5 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 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 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。

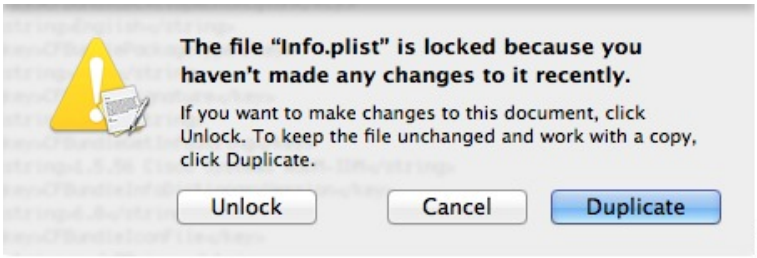
ステップ 3 **[Java]** > **[VMOptions]** で、「-Xmx」のプレフィックスが付いた文字列を変更し、必要なヒープ サイズを指定します。たとえば、768 MB の場合は -Xmx768M に変更し、1 GB の場合は -Xmx1G に変更します。

```
    <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。

ASDM 7.15(1.150) の新機能

リリース日：2021 年 2 月 8 日

このリリースに新機能はありません。

ASA 9.15(1)/ASDM 7.15(1) の新機能

リリース：2020 年 11 月 2 日

機能	説明
プラットフォーム機能	
パブリッククラウド向け ASAv	次のパブリッククラウドサービスに ASAv を導入しました。 • Oracle Cloud Infrastrucure（OCI） • Google Cloud Platform（GCP） 変更された画面はありません。
自動スケールに対する ASAv のサポート	ASAv は、次のパブリッククラウドサービスの自動スケールをサポートするようになりました。 • Amazon Web Services（AWS） • Miscrosoft Azure 自動スケーリングは、キャパシティの要件に基づいて ASAv アプリケーションのインスタンス数を増減します。 変更された画面はありません。
ASAv for Microsoft Azure の Accelerated Networking に対するサポート（SR-IOV）	Microsoft Azure パブリッククラウド上の ASAv は、Azure の Accelerated Networking（AN）をサポートするようになりました。これにより、VM に対するシングルルート I/O の仮想化（SR-IOV）が可能になり、ネットワーキングのパフォーマンスが大幅に向上しています。 変更された画面はありません。

機能	説明
ファイアウォール機能	
クラスタリングでの PAT アドレス割り当ての変更。PAT プールの **flat** オプションがデフォルトで有効になり、設定できなくなりました。	PAT アドレスがクラスタのメンバーに配布される方法が変更されます。以前は、アドレスはクラスタのメンバーに配布されていたため、PAT プールにはクラスタメンバーごとに少なくとも 1 つのアドレスが必要でした。マスターは各 PAT プールアドレスを等しいサイズのポートブロックに分割し、それらをクラスタメンバーに配布するようになりました。各メンバーには、同じ PAT アドレスのポートブロックがあります。したがって、通常 PAT に必要な接続量に応じて、PAT プールのサイズを 1 つの IP アドレスにまで減らすことができます。ポートブロックは、1024 ～ 65535 の範囲で 512 ポートのブロック単位で割り当てられます。オプションで、PAT プールルールを設定するときに、このブロック割り当てに予約ポート 1 ー 1023 を含めることができます。たとえば、単一ノードでは PAT プール IP アドレスあたり 65535 個の接続すべてを処理するのに対し、4 ノードクラスタでは、各ノードは 32 個のブロックを取得し、PAT プール IP アドレスあたり 16384 個の接続を処理できます。 この変更の一環として、スタンドアロンまたはクラスタ内での動作に関わりなく、すべてのシステムの PAT プールは、フラットなポート範囲 1023 ー 65535 を使用できるようになりました。以前は、**flat** オプションを PAT プールルールに含めることで、フラットな範囲をオプションで使用できました。**flat** キーワードはサポートされなくなりました。PAT プールは常にフラットになります。**include-reserve** キーワードは、以前は **flat** のサブキーワードでしたが、PAT プール構成内の独立したキーワードになりました。このオプションを使用すると、PAT プール内に 1 ー 1023 のポート範囲を含めることができます。 ポートブロック割り当てを設定する（**block-allocation** PAT プールオプション）と、デフォルトの 512 ポートブロックではなく、独自のブロック割り当てサイズが使用されます。また、クラスタ内のシステムの PAT プールに拡張 PAT を設定することはできません。 新規/変更された画面：[NAT PAT Pool configuration]
新規インストールでは、デフォルトで XDMCP インスペクションが無効になっています。	以前は、すべてのトラフィックに対して XDMCP インスペクションがデフォルトで有効になっていました。新しいシステムと再イメージ化されたシステムを含む新規インストールでは、XDMCP はデフォルトで無効になっています。このインスペクションが必要な場合は、有効にしてください。アップグレードでは、デフォルトのインスペクション設定を使用して XDMCP インスペクションを有効にしただけでも、XDMCP インスペクションの現在の設定は保持されます。
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
フェールオーバー遅延の無効化	ブリッジグループまたは IPv6 DAD を使用する場合、フェールオーバーが発生すると、新しいアクティブユニットは、スタンバイユニットがネットワーキングタスクを完了してスタンバイ状態に移行するまで、最大3000ミリ秒待機します。その後、アクティブユニットはトラフィックの受け渡しを開始できます。この遅延を回避するために、待機時間を無効にすると、スタンバイユニットが移行する前にアクティブユニットがトラフィックの受け渡しを開始します。 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[Failover]** > **[Enable switchover waiting for peer state]**
ルーティング機能	
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。 *9.12(4)* でも同様です。
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 アドレスの生成に関する ASDM のサポート	ASDM でシングルコンテキストモードの VLAN サブインターフェイス用に一意の MAC アドレスを生成すること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。ASA 9.8(3)、9.8(4)、および 9.9(2) で CLI のサポートが追加された。 新規/変更された画面：**[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]**
DDNS の Web 更新方式のサポート	DDNS の Web 更新方式を使用するようにインターフェイスを設定できるようになりました。 新規/変更された画面：**[Configuration]** > **[Device Management]** > **[DNS]** > **[Dynamic DNS]**
証明書の機能	
スタティック CRL 分散ポイント URL をサポートするための match certificate コマンドの変更	静的 CDP URL コンフィギュレーション コマンドでは、CDP を検証中のチェーン内の各証明書に一意にマッピングできます。ただし、このようなマッピングは各証明書で 1 つだけサポートされていました。今回の変更で、静的に設定された CDP を認証用の証明書チェーンにマッピングできるようになりました。
管理およびトラブルシューティングの機能	

機能	説明
SDI AAA サーバーグループで使用するノードシークレットファイルの RSA Authentication Managerからの手動インポート。	SDI AAA サーバーグループで使用するために RSA Authentication Manager からエクスポートしたノードシークレットファイルをインポートできます。 次の画面が追加されました。**[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[AAA SDI]**。
show fragment コマンドの出力の拡張	**show fragment** コマンドの出力が拡張され、IP フラグメント関連のドロップとエラーカウンタが含まれるようになりました。 変更された画面はありません
show tech-support コマンドの出力の拡張	**show tech-support** コマンドの出力が拡張され、暗号アクセラレータに設定されたバイアスが含まれるようになりました。バイアス値はssl、ipsec、またはbalancedになります。 変更された画面はありません
モニタリング機能	
cplane キープアライブ ホールドタイム値の設定のサポート	高い CPU 使用率によって通信が遅延するため、キープアライブイベントへの応答が ASA に到達できず、カード障害によるフェールオーバーが発生します。キープアライブタイムアウト期間と最大キープアライブカウンタ値を設定して、十分な時間と再試行が行われるようにできます。 次の画面を追加しました。**[Configuration]** > **[Device Management]** > **[Service Module Settings]**
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。 *9.12(4)* でも同様です。
WebVPN ハンドラのクロスサイト リクエスト フォージェリ（CSRF）の脆弱性の防止	ASA は、WebVPN ハンドラの CSRF 攻撃に対する保護を提供します。CSRF 攻撃が検出されると、警告メッセージでユーザーに通知します。この機能は、デフォルトで有効にされています。

機能	説明
Kerberos Constrained Delegation（KCD）のケルベロスサーバーの検証	KCD 用に設定されている場合、ASA は Kerberos キーを取得するために、設定されたサーバーとの AD ドメイン参加を開始します。これらのキーは、ASA がクライアントレス SSL VPN ユーザーに代わってサービスチケットを要求するために必要です。必要に応じて、ドメイン参加時にサーバーのアイデンティティを検証するように ASA を設定できます。 次の画面を変更しました。 **[Configuration]** > **[Remote Access VPN]** > **[Clientless SSL VPN Access]** > **[Advanced]** > **[Microsoft KCD Server]**

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

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
9.14(x)	—	次のいずれかになります。 → 9.15(x)
9.13(x)	—	次のいずれかになります。 → 9.15(x) → 9.14(x)
9.12(x)	—	次のいずれかになります。 → 9.15(x) → 9.14(x)
9.10(x)	—	次のいずれかになります。 → 9.15(x) → 9.14(x) → 9.12(x)
9.9(x)	—	次のいずれかになります。 → 9.15(x) → 9.14(x) → 9.12(x)
9.8(x)	—	次のいずれかになります。 → 9.15(x) → 9.14(x) → 9.12(x)
9.7(x)	—	次のいずれかになります。 → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(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
9.6(x)	—	次のいずれかになります。 → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(x)
9.5(x)	—	次のいずれかになります。 → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(x)
9.4(x)	—	次のいずれかになります。 → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(x)
9.3(x)	—	次のいずれかになります。 → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(x)
9.2(x)	—	次のいずれかになります。 → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(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
9.1(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(x) → **9.12(x)** → 9.8(x) → 9.1(7.4)
9.1(1)	→ 9.1(2)	次のいずれかになります。 → 9.14(x) → **9.12(x)** → 9.8(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。 → 9.14(x) → **9.12(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。 → 9.14(x) → **9.12(x)** → 9.8(x) → 9.1(7.4)
8.6(1)	→ 9.0(4)	次のいずれかになります。 → 9.14(x) → **9.12(x)** → 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
8.5(1)	→ 9.0(4)	次のいずれかになります。 → **9.12(x)** → 9.8(x) → 9.1(7.4)
8.4(5+)	—	次のいずれかになります。 → **9.12(x)** → 9.8(x) → 9.1(7.4) → 9.0(4)
8.4(1) ～ 8.4(4)	→ 9.0(4)	→ **9.12(x)** → 9.8(x) → 9.1(7.4)
8.3(x)	→ 9.0(4)	次のいずれかになります。 → **9.12(x)** → 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。 → **9.12(x)** → 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 7.15(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

バージョン 7.15(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

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 7.15(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
CSCvv76201	ASDM 接続が制限され、コンテキストの 1 つで「該当なし」と表示される
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

バージョン 7.15(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
CSCvq80097	ルーテッドコンテキストからトランスペアレントコンテキストに切り替えると ASDM パケットトレーサの宛先 MAC が表示されない
CSCvr63410	管理専用チェックボックスへのインターフェイスの選択を解除できない
CSCvr78019	パスワード暗号化が有効になっていると ASDM で事前共有キーを変更できない
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
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
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
CSCvv27284	AnyConnect カスタム属性名の値を編集できない

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。