Cisco ASDM 7.14(x) リリースノート

Cisco ASDM 7.14(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 7.14(x) のリリース情報が記載されています。

特記事項

- アプライアンスモードの Firepower 1000 および 2100 での 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、9.14 へのアップグレードには使用できません（[Tools] > [Check for ASA/ASDM Updates]）。ウィザードでは ASDM を 7.13 から 7.14 に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されます（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。9.14(1) バンドルの ASDM イメージ（7.14(1)）にも CSCvt72183 のバグがあることに注意してください。ウィザードを正しく機能させるには、より新しい 7.14(1.46) イメージをダウンロードする必要があります。
  - **[Tools] > [Check for ASA/ASDM Updates]** を使用して ASDM 7.14 にアップグレードします（バージョンは 7.14(1.46) になる）。次に、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。
- 9.14(1) 以降のフェールオーバーペアの場合、ASA は SNMP クライアントエンジンデータをピアと共有しません。
- ASA 9.14(1) 以降では、cnatAddrBindNumberOfEntries および cnatAddrBindSessionCount の OID はサポートされません（CSCvy22526）。
- ASA 5512-X、ASA 5515-X、ASA 5585-X、および ASASM 用の ASA 9.13(1) 以降ではサポートされていません。ASA 9.12(x) が最後にサポートされていたバージョンです。ASA 5515-X および ASA 5585-X FirePOWER モジュールについては、サポートされる最後のバージョンは 6.4 です。

  注：ASDM 7.13(1) および ASDM 7.14(1) でも、これらのモデルはサポートされていません。ASDM のサポートを復活させるには、ASDM 7.13(1.101) または 7.14(1.48) にアップグレードする必要があります。

- 9.13(1) 以降では ASAv に 2GB のメモリが必要：9.13(1) 以降の ASAv の最小メモリ要件は 2GB です。現在の ASAv が 2 GB 未満のメモリで動作している場合は、以前のバージョンから 9.13(1) にアップグレードできません。アップグレードする前にメモリサイズを調整する必要があります。バージョン 9.13(1) でサポートされているリソース割り当て（vCPU とメモリ）については、ASAv のスタートアップガイドを参照してください。

- プラットフォームモードでの 9.13/9.14 から 9.12 以前への Firepower 2100 のダウングレードの問題：プラットフォームモードに変換した 9.13 または 9.14 を新規インストールした Firepower 2100 の場合：9.12 以前にダウングレードすると、FXOS で新しいインターフェイスの設定や、既存インターフェイスの編集ができなくなります（9.12 以前ではプラットフォームモードのみがサポートされています）。バージョンを 9.13 以降に戻すか、または FXOS の erase configuration コマンドを使用して設定をクリアする必要があります。この問題は、元々以前のリリースから 9.13 または 9.14 にアップグレードした場合は発生しません。新しいデバイスや再イメージ化されたデバイスなど、新規インストールのみが影響を受けます。（CSCvr19755）

- 9.13(1) でのクラスタ制御リンク MTU の変更：9.13(1) 以降では、多くのクラスタ制御パケットが以前のリリースよりも大きくなっています。クラスタ制御リンクに推奨されている MTU は常に 1600 以上であり、この値が適切です。ただし、MTU を1600に設定しても接続スイッチの MTU と一致しなかった場合は（スイッチの MTU を1500 のままにしたなど）、ドロップされたクラスタ制御パケットとのこの不一致の影響が現れ始めます。クラスタ制御リンク上のすべてのデバイスが同じ MTU（具体的には 1600 以上）に設定されていることを確認します。

- **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**。

- **tls-proxy** キーワード、および SCCP/Skinny 暗号化インスペクションのサポートは、**inspect skinny** コマンドから削除されました。

- **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。ASDM 7.13 と 7.14 は、ASA 5512-X、5515-X、5585-X、または ASASM をサポートしていませんでした。そのため、ASDM 7.13(1.101) または 7.14(1.48) にアップグレードして ASDM のサポートを復活させる必要があります。
- Windows DNS クライアントの最適化の制限：Windows 8 以降の制限により、スプリット DNS ドメインと一致しないため、nslookup などの特定の名前解決が FQDN で失敗することが確認されています。回避策は、次の変更を加えて、Windows DNS クライアントの最適化を無効にすることです。

□□□HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters □□
DisableParallelAandAAA □□□□1
□□□HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\DNSClient □□
DisableSmartNameResolution □□□□1

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。

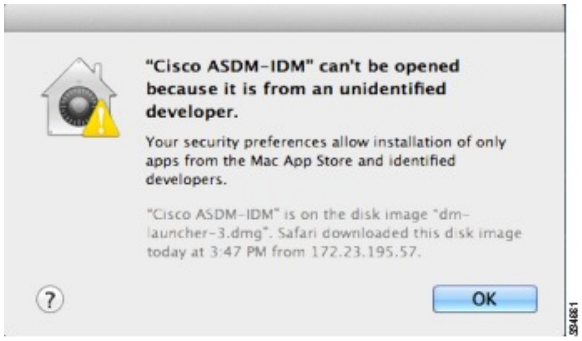
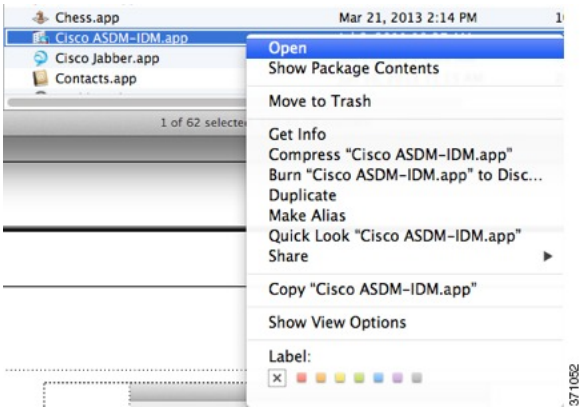
表 *1*：*ASA* と *ASA FirePOWER*：*ASDM* オペレーティング システムとブラウザの要件

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 （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 （4 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	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。

条件	注意
サーバーの IE9	サーバーの 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。

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。

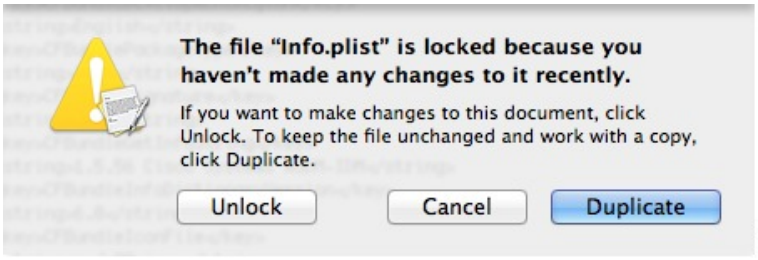
ステップ 3 **[Java]** > **[VMOptions]** で、「-Xmx」のプレフィックスが付いた文字列を変更し、必要なヒープ サイズを指定します。たとえば、768 MB の場合は -Xmx768M に変更し、1 GB の場合は -Xmx1G に変更します。

```
    <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 9.14(4)/ASDM 7.17(1) の新機能

リリース日：2022 年 2 月 2 日

このリリースに新機能はありません。

ASA 9.14(3)/ASDM 7.15(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 9.14(2) の新機能

リリース：2020 年 11 月 9 日

機能	説明
SNMP 機能	
サイト間 VPN 経由の SNMP ポーリング	サイト間 VPN 経由のセキュアな SNMP ポーリングの場合、VPN 設定の一部として外部インターフェイスの IP アドレスを暗号マップアクセスリストに含めます。

ASA 9.14(1.30) の新機能

リリース：**2020 年 9 月 23 日**

機能	説明
ライセンシング機能	
ASAv100 永続ライセンス予約	ASAv100 で製品 ID L-ASAV100SR-K9= を使用した永続ライセンス予約がサポートされるようになりました。**注**：すべてのアカウントが永続ライセンス予約について承認されているわけではありません。

ASDM 7.14(1.48) の新機能

リリース日：**2020 年 4 月 30 日**

機能	説明
プラットフォーム機能	
ASA 9.12 以前について、ASA 5512-X、5515-X、5585-X、および ASASM に対するサポートが復活	この ASDM リリースでは、9.12 以前を実行している場合、ASA 5512-X、5515-X、5585-X、および ASASM に対するサポートが復活しました。これらのモデルの最終 ASA バージョンは 9.12 です。元の 7.13(1) リリースと 7.14(1) リリースでは、これらのモデルでの後方互換性がブロックされていましたが、このバージョンでは互換性が復活しています。

ASAv 9.14(1.6) の新機能

リリース日：**2020 年 4 月 30 日**

（注） このリリースは、ASAv でのみサポートされています。

機能	説明
プラットフォーム機能	
ASAv100 プラットフォーム	ASAv 仮想プラットフォームに、20 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 モデルの ASAv100 が追加されました。ASAv100 はサブスクリプションベースのライセンスで、期間は 1 年、3 年、または 5 年です。 ASAv100 は、VMware ESXi および KVM でのみサポートされます。

ASA 9.14(1)/ASDM 7.14(1) の新機能

リリース日：**2020** 年 **4** 月 **6** 日

機能	説明
プラットフォーム機能	
Firepower 4112 用の ASA	Firepower 4112 用の ASA を導入しました。 変更された画面はありません。 （注） FXOS 2.8(1) が必要です。
ファイアウォール機能	
show access-list の出力でポート番号を表示できる。	**show access-list** コマンドに数値キーワードが追加されました。これを使用すると、アクセス制御エントリの名前ではなくポート番号を表示できます。たとえば、www の代わりに 80 を表示できます。
object-group icmp-type コマンドが非推奨になった。	**object-group icmp-type** コマンドは、このリリースでも引き続きサポートされますが、推奨されず、将来のリリースで削除される可能性があります。すべての ICMP タイプのオブジェクトをサービス オブジェクト グループに変更し（**object-group service**）、オブジェクト内で **service icmp** を指定してください。
Kerberos キー発行局（KDC）認証。	Kerberos キー配布局（KDC）からキータブファイルをインポートできます。システムは、Kerberos サーバーを使用してユーザーを認証する前にサーバーがスプーフィングされていないことを認証できます。KDC 認証を実行するには、Kerberos KDC で**ホスト**/*ASA_hostname* サービスプリンシパル名（SPN）を設定してから、その SPN のキータブをエクスポートする必要があります。その後に、キータブを ASA にアップロードし、KDC を検証するように Kerberos AAA サーバーグループを設定する必要があります。 新規/変更された画面：**[構成（Configuration）] > [デバイス管理（Device Management）] > [ユーザー/AAA（Users/AAA）] > [AAA Kerberos]**、**[構成（Configuration）] > [デバイス管理（Device Management）] > [ユーザー/AAA（Users/AAA）] > [AAAサーバーグループ（AAA Server Groups）]**Kerberos サーバーグループの [追加/編集（Add/Edit）] ダイアログボックス。
ハイ アベイラビリティとスケーラビリティの各機能	
データユニットとの設定の並列同期	制御ユニットでは、デフォルトで設定変更がデータユニットと同時に同期化されるようになりました。以前は、順番に同期が行われていました。 新規/変更された画面：**[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Configuration] > [Enable parallel configuration replicate]** チェックボックス

機能	説明
クラスタへの参加失敗や削除のメッセージが、以下に追加されました。 **show cluster history**	クラスタユニットがクラスタへの参加に失敗した場合や、クラスタを離脱した場合の新しいメッセージが、 **show cluster history** コマンドに追加されました。 新規/変更されたコマンド： **show cluster history** 変更された画面はありません。
インターフェイス機能	
Firepower 1000 および 2100 の 1GB ファイバインターフェイスで速度の自動ネゴシエーションを無効にできる	自動ネゴシエーションを無効にするように Firepower 1100 または 2100 SFP インターフェイスを設定できるようになりました。10GB インターフェイスの場合、自動ネゴシエーションなしで速度を 1GB に設定できます。速度が 10 GB に設定されているインターフェイスの自動ネゴシエーションは無効にできません。 新規/変更された画面：**[構成（Configuration）] > [デバイスの設定（Device Settings）] > [インターフェイス（Interfaces）] > [インターフェイスの編集（Edit Interface）] > [ハードウェアプロパティの構成（Configure Hardware Properties）] > [速度（Speed）]**
管理およびトラブルシューティングの機能	
新しい **connection-data-rate** コマンド	この **connection-data-rate** コマンドは、ASA での個別接続のデータレートの概要を提供するために導入されました。このコマンドを有効にすると、フローごとのデータレートが既存の接続情報とともに提供されます。この情報は、高いデータレートの望ましくない接続を識別してブロックし、最適な CPU 使用率を確保するために役立ちます。 新規/変更されたコマンド：**conn data-rate**、**show conn data-rate**、**show conn detail**、**clear conn data-rate** 変更された画面はありません。
HTTPS アイドルタイムアウトの設定	ASDM、WebVPN、および他のクライアントを含む、ASA へのすべての HTTPS 接続のアイドルタイムアウトを設定できるようになりました。これまでは、**http server idle-timeout** コマンドを使用して ASDM アイドルタイムアウトを設定することしかできませんでした。両方のタイムアウトを設定した場合は、新しいコマンドによる設定が優先されます。 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）] > [ASDM/HTTPS/Telnet/SSH] > [HTTP設定（HTTP Settings）] > [接続アイドルタイムアウト（Connection Idle Timeout）]** チェックボックス。
NTPv4 のサポート	ASA が NTPv4 をサポートするようになりました。 変更された画面はありません。

機能	説明
新しい **clear logging counter** コマンド	**show logging** コマンドは、ASA で設定された各ロギングカテゴリについてログに記録されたメッセージの統計を提供します。**clear logging counter** コマンドは、ログに記録されたカウンタと統計をクリアするために導入されました。 新規/変更されたコマンド： **clear logging counter** 変更された画面はありません。
アプライアンスモードの Firepower 1000 および 2100 での FXOS のデバッグコマンドの変更	**debug fxos_parser** コマンドは簡素化され、FXOS に関して一般に使用されるトラブルシューティングメッセージを提供するようになりました。その他の FXOS デバッグコマンドは、**debug menu fxos_parser** コマンドの下に移動されました。 新規/変更されたコマンド：**debug fxos_parser**、**debug menu fxos_parser** 変更された画面はありません。
show tech-support コマンドの拡張	**show ssl objects** コマンドと **show ssl errors** コマンドが **show tech-support** コマンドの出力に追加されました。 新規/変更されたコマンド： **show tech-support** 変更された画面はありません。 *9.12(4)* でも同様です。
モニタリング機能	
Net-SNMP バージョン 5.8 のサポート	ASA は Net-SNMP（IPv4 と IPv6 の両方を使用して SNMP v1、SNMP v2c、および SNMP v3 を実装するために使用されるアプリケーションスイート）を使用しています。 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]**
SNMP の MIB および OID	ASA は、CISCO-REMOTE-ACCESS-MONITOR-MIB のサポートを拡張し、SNMP を介して RADIUS からの認証の拒否/失敗を追跡します。この機能により、次の 3 つの SNMP OID が実装されます。 • crasNumTotalFailures（失敗の総数） • crasNumSetupFailInsufResources（AAA およびその他の内部エラー） • crasNumAbortedSessions（中断されたセッション）オブジェクト ASA は、Advanced Encryption Standard（AES）暗号アルゴリズムのサポートを提供します。この機能により、次の SNMP OID が実装されます。 • usmAesCfb128Protocol • usmNoPrivProtocol

機能	説明
SNMPv3 認証	ユーザー認証に SHA-256 HMAC を使用できるようになりました。 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]**
debug telemetry 表示されていません。	**debug telemetry** コマンドを使用すると、テレメトリに関連するデバッグメッセージが表示されます。このデバッグは、テレメトリレポートの生成時にエラーの原因を特定するために役立ちます。 変更された画面はありません。
VPN 機能	
VTI での DHCP リレーサーバーのサポート	DHCP リレーサーバーを設定して、VTI トンネルインターフェイスを介して DHCP メッセージを転送できるようになりました。 新規/変更された画面：**[構成（Configuration）] > [デバイス管理（Device Management）] > [DHCP] > [DHCPリレー（DHCP Relay）]**
複数ピアクリプトマップのIKEv2サポート	複数ピアクリプトマップでIKEv2を設定できるようになりました。トンネル内のピアがダウンすると、IKEv2 はリスト内の次のピアで SA の確立を試みます。 新規/変更された画面：**[構成（Configuration）]>[サイト間VPN（Site-to-Site VPN）]>[詳細設定（Advanced）]>[クリプトマップ（Crypto Maps）]>[IPsecルールの作成/編集（Create / Edit IPsec Rule）]>[トンネルポリシー（クリプトマップ）- 基本（Tunnel Policy (Crypto Map) - Basic）]**
複数証明書認証のユーザー名オプション	複数証明書認証で、1つの証明書（マシン証明書）または2つ目の証明書（ユーザー証明書）のどちらからの属性を AAA 認証に使用するのかを指定できるようになりました。 新規/変更された画面： • **[接続プロファイル（Connection Profile）] > [詳細設定（Advanced）] > [認証（Authentication）]** • **[接続プロファイル（Connection Profile）] > [詳細設定（Advanced）] > [セカンダリ認証（Secondary Authentication）]**

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
9.13(x)	—	次のいずれかになります。 → **9.14(x)**
9.12(x)	—	次のいずれかになります。 → 9.14(x)
9.10(x)	—	次のいずれかになります。 → 9.14(x) → **9.12(x)**
9.9(x)	—	次のいずれかになります。 → 9.14(x) → **9.12(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。 → 9.14(x) → **9.12(x)**
9.7(x)	—	次のいずれかになります。 → 9.14(x) → **9.12(x)** → 9.8(x)
9.6(x)	—	次のいずれかになります。 → 9.14(x) → **9.12(x)** → 9.8(x)
9.5(x)	—	次のいずれかになります。 → 9.14(x) → **9.12(x)** → 9.8(x)
9.4(x)	—	次のいずれかになります。 → 9.14(x) → **9.12(x)** → 9.8(x)
9.3(x)	—	次のいずれかになります。 → 9.14(x) → **9.12(x)** → 9.8(x)
9.2(x)	—	次のいずれかになります。 → 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 7.14(1.48) 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
CSCvp26795	Windows 10 1809 に ASDM をインストールすると、間違ったデスクトップショートカット リンクが作成される
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
CSCvs35014	ASDM：PC からのコピーでローカルディレクトリが読み取られない（Mac Catalina）
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

バージョン 7.14(1.46) 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
CSCvp26795	Windows 10 1809 に ASDM をインストールすると、間違ったデスクトップショートカット リンクが作成される
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
CSCvs35014	ASDM：PC からのコピーでローカルディレクトリが読み取られない（Mac Catalina）

バージョン 7.14(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
CSCvp26795	Windows 10 1809 に ASDM をインストールすると、間違ったデスクトップ ショートカット リンクが作成される
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
CSCvs35014	ASDM：PC からのコピーでローカルディレクトリが読み取られない（Mac Catalina）
CSCvt72183	アプライアンスモードでの 9.131/7131 から 9141/7141 へのアップグレードが失敗する

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 7.14(1.48) で解決済みのバグ

このリリースでは解決済みのバグはありません。

バージョン 7.14(1.46) 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
CSCvt72183	アプライアンスモードでの 9.131/7131 から 9141/7141 へのアップグレードが失敗する

バージョン 7.14(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
CSCvq68530	ASDM：Cisco クライアントレス SSL VPN と OWA および SSO に関する問題
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
CSCvr15019	ASA5506 ASDM 7.12.1：いくつかのページ/ボタンが機能しない
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

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。

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。