Cisco Secure Firewall ASDM 7.19(x) リリースノート

最終更新：2023 年 4 月 18 日

Cisco Secure Firewall ASDM 7.19(x) リリースノート

このドキュメントには、 Cisco Secure Firewall ASA シリーズ対応の ASDM バージョン 7.19(x) のリリース情報が記載されています。

特記事項

- **Firepower 4110、4120、4140、4150 に対する ASA 9.19(1) 以降のサポート、および Firepower 9300 に対するセキュリティモジュール SM-24、SM-36、SM-44 のサポートはありません。** ASA 9.18(x) がサポートされている最後のバージョンです。
- （CSCwd82040）TLS 1.3 が設定されている場合、ASA 9.19.1 に接続し、クライアント証明書認証を使用する 4.xx Linux、macOS、または iOS AnyConnect VPN クライアントは、TLS ネゴシエーションに失敗する可能性があります。iOS でこの問題が発生した場合は、App Store の最新バージョンにアップグレードすると問題が解決します。macOS でこの問題が発生した場合は、ファイルベースではなくキーチェーンベースの証明書を使用してください。次の AnyConnect 4.10 リリースでは、TLS ネゴシエーションが修正されます。
- **ASDM 7.19(1) には Oracle Java バージョン 8u261 以降が必要です。**ASDM 7.19 にアップグレードする前に、Oracle Java（使用している場合）をバージョン 8u261 以降に更新してください。このバージョンでは、ASDM Launcher のアップグレードに必要な TLSv1.3 がサポートされています。OpenJRE は影響を受けません。
- **ASDM アップグレードウィザード**：2022 年 3 月以降の内部変更により、アップグレードウィザードは ASDM 7.17(1.150) より前のバージョンでは機能しなくなります。ウィザードを使用するには、手動で 7.17(1.150) にアップグレードする必要があります。

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（**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。

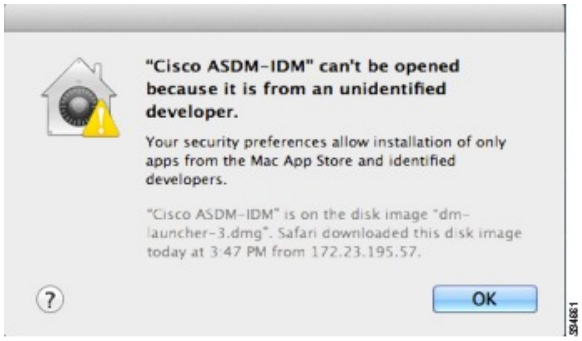
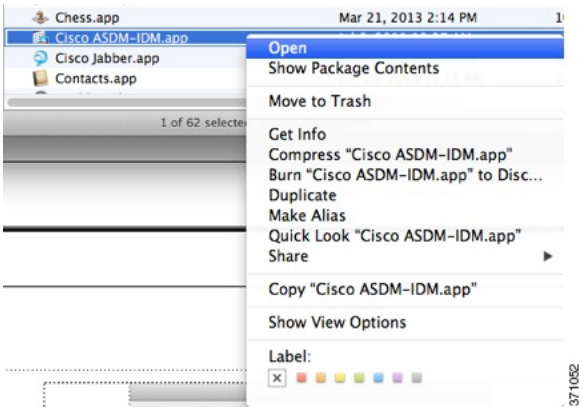
表 *1 : ASDM* オペレーティングシステムとブラウザの要件

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 （2 ページ）の「Windows 10」を参照してください。 • 8 • 7 • Server 2016 と Server 2019 • 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。

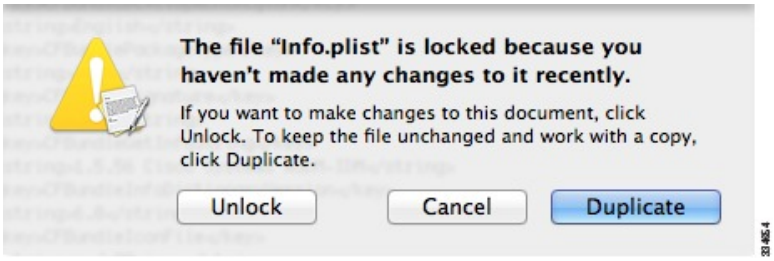
ステップ 3 **[Java]** > **[VMOptions]** で、「-Xmx」のプレフィックスが付いた文字列を変更し、必要なヒープ サイズを指定します。たとえば、768 MB の場合は -Xmx768M に変更し、1 GB の場合は -Xmx1G に変更します。

```
    <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 Secure Firewall 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 9.19(1)/ASDM 7.19(1) の新機能

リリース日：**2022 年 11 月 29 日**

機能	説明
プラットフォーム機能	
Azure ゲートウェイロードバランサを使用した ASA Virtual 自動スケールソリューション	Microsoft Azure にゲートウェイロードバランサを使用して ASA Virtual 自動スケールソリューションを展開できます。詳細については、インターフェイス機能を参照してください。
ファイアウォール機能	
ネットワークサービスグループのサポート	最大 1024 のネットワーク サービス グループを定義できるようになりました。
ハイ アベイラビリティとスケーラビリティの各機能	
バイアス言語の除去	「Master」と「Slave」という用語を含むコマンド、コマンド出力、syslog メッセージは、「Control」と「Control」に変更されました。 新規/変更されたコマンド：**cluster control-node**、**enable as-data-node**、**prompt**、**show cluster history**、**show cluster info**
ASA Virtual Amazon Web Services（AWS）クラスタリング	ASA Virtual は AWS で最大 16 ノードの個別インターフェイスのクラスタリングをサポートします。AWS ゲートウェイロードバランサ の有無にかかわらず、クラスタリングを使用できます。 ASDM サポートはありません。
ルーティング機能	
IPv6 の BGP グレースフルリスタート	IPv6 アドレスファミリの BGP グレースフルリスタートサポートを追加しました。 新規/変更されたコマンド：**[設定（Configuration）]** > **[デバイスのセットアップ（Device Setup）]** > **[ルーティング（Routing）]** > **[BGP]** > **[IPv6 ファミリ（IPv6 Family）]** > **[ネイバー（Neighbor）]**

機能	説明
ASDM での BGP トラフィックのループバック インターフェイス サポート	ASDM は、BGP ネイバーシップのソースインターフェイスとしてループバック インターフェイスの設定をサポートするようになりました。ループバック インターフェイスは、パス障害の克服に役立ちます。 新規/変更された画面：**[設定（Configuration）] > [デバイスのセットアップ（Device Setup）] > [ルーティング（Routing）] > [BGP] > [IPv4ファミリ（IPv4 Family）]/[IPv6 ファミリ（IPv6 Family）] > [ネイバー（Neighbor）] > [追加（Add）] > [全般（General）]**
インターフェイス機能	
ASA Virtual で IPv6 をサポート	ASAv は、プライベートおよびパブリック クラウド プラットフォームで IPv6 ネットワークプロトコルをサポートします。 ユーザーは次のことができるようになりました。 • day0 設定で IPv6 管理アドレスを有効にして構成します。 • DHCP および静的な方法を使用して IPv6 アドレスを割り当てます。
Azure ゲートウェイロードバランサーの ASA Virtual のペアプロキシ VXLAN	Azure ゲートウェイ ロードバランサー（GWLB）で使用するために、Azure の ASA Virtual のペアプロキシモード VXLAN インターフェイスを構成できます。ASA Virtual は、ペアプロキシの VXLAN セグメントを利用して、単一の NIC に外部インターフェイスと内部インターフェイスを定義します。 新規/変更されたコマンド：**external-port、external-segment-id、internal-port、internal-segment-id、プロキシがペアリングされました** ASDM サポートはありません。
Secure Firewall 3100 固定ポートのデフォルトの前方誤り訂正（FEC）が、25 GB+ SR、CSR、および LR トランシーバの cl74-fc から cl108-rs に変更されました	Secure Firewall 3100 の固定ポートで FEC を Auto に設定すると、25 GB SR、CSR、および LR トランシーバのデフォルトのタイプが cl74-fc ではなく cl108-rs に設定されるようになりました。 新規/変更された画面：**[設定（Configuration）] > [デバイスのセットアップ（Device Setup）] > [インターフェイスの設定（Interface 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）] > [FEC モード（FEC Mode）]**
ASDM でのループバック インターフェイスのサポート	ASDM は、ループバック インターフェイスをサポートするようになりました。 新規/変更された画面：[設定（Configuration）] > [デバイスのセットアップ（Device Setup）] > [インターフェイスの設定（Interface Settings）] > [インターフェイス（Interfaces）] > [ループバックインターフェイスの追加（Add Loopback Interface）]
ライセンス機能	

機能	説明
KVM および VMware 上の ASAv5 の ASA Virtual 永久ライセンス予約のサポート	デフォルトの PLR ソフトウェア利用資格を上書きし、KVM および VMware に 2GB RAM の ASAv を展開するときに Cisco Smart Software Manager（SSM）に ASAv5 PLR ライセンスを発行するように要求する新しいコマンドを利用できます。RAM の設定に合わせてソフトウェア利用資格を ASAv5 からデフォルトの PLR ライセンスに戻すための <*no*> 形式を追加することにより、このコマンドを変更できます。
VPN 機能	
VTI ループバック インターフェイスのサポート	ループバック インターフェイスを VTI の送信元インターフェイスとして設定できるようになりました。静的に設定された IP アドレスの代わりに、ループバック インターフェイスから IP アドレスを継承するサポートも追加されました。ループバック インターフェイスは、パス障害の克服に役立ちます。インターフェイスがダウンした場合、ループバック インターフェイスに割り当てられた IP アドレスを使用してすべてのインターフェイスにアクセスできます。 新規/変更された画面：**[設定（Configuration）] > [デバイスのセットアップ（Device Setup）] > [インターフェイスの設定（Interface Settings）] > [インターフェイス（Interfaces）] > [VTIインターフェイスの追加（Add VTI Interface）] > [詳細（Advanced）]**
ダイナミック仮想トンネルインターフェイス（ダイナミック VTI）のサポート	ダイナミック VTI により ASA が強化されました。ハブの複数のスタティック VTI 構成を単一のダイナミック VTI に置き換えることができます。ハブの構成を変更せずに、新しいスポークをハブに追加できます。ダイナミック VTI はダイナミック（DHCP）スポークをサポートします。 新規/変更された画面：**[設定（Configuration）] > [デバイスのセットアップ（Device Setup）] > [インターフェイスの設定（Interface Settings）] > [インターフェイス（Interfaces）] > [追加（Add）] > [DVTIインターフェイス（DVTI Interface）] > [詳細（Advanced）]**
EIGRP および OSPF の VTI サポート	EIGRP および OSPFv2/v3 ルーティングが仮想トンネルインターフェイスでサポートされるようになりました。これらのルーティングプロトコルを使用して、ルーティング情報を共有し、ピア間の VTI ベースの VPN トンネルを介してトラフィックフローをルーティングできます。
リモートアクセス VPN の TLS 1.3	TLS 1.3 を使用して、リモートアクセス VPN 接続を暗号化できます。 TLS 1.3 では、次の暗号方式のサポートが追加されています。 • TLS_AES_128_GCM_SHA256 • TLS_CHACHA20_POLY1305_SHA256 • TLS_AES_256_GCM_SHA384 この機能には、Cisco Secure Client バージョン 5.0.01242 以降が必要です。 新規/変更された画面：**[設定（Configuration）] > [デバイス管理（Device Management）] > [詳細（Advanced）] > [SSL設定（SSL Settings）]**

機能	説明
IKEv2 サードパーティクライアントのデュアルスタックサポートが追加されました。	Cisco Secure Firewall ASA は、IKEv2 サードパーティのリモートアクセス VPN クライアントからのデュアルスタック IP 要求をサポートするようになりました。サードパーティのリモートアクセス VPN クライアントが IPv4 アドレスと IPv6 アドレスの両方を要求した場合、ASA は、複数のトラフィックセレクタを使用して両方の IP バージョンアドレスを割り当てることができます。この機能により、サードパーティのリモートアクセス VPN クライアントは、単一の IPsec トンネルを使用して IPv4 および IPv6 データトラフィックを送信できます。

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） 9.18(x) は Firepower 4110、4120、4140、4150、および Firepower 9300 のセキュリティモジュール SM-24、SM-36、SM-44 の最終バージョンです。

ASA 9.16(x) は ASA 5506-X、5508-X、および 5516-X の最終バージョンです。

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
9.18(x)	—	次のいずれかになります。 → **9.19(x)**
9.17(x)	—	次のいずれかになります。 → **9.19(x)** → **9.18(×)**
9.16(x)	—	次のいずれかになります。 → **9.19(x)** → **9.18(×)** → 9.17(x)
9.15(x)	—	次のいずれかになります。 → **9.19(x)** → **9.18(×)** → 9.17(x) → **9.16(x)**
9.14(x)	—	次のいずれかになります。 → **9.19(x)** → **9.18(×)** → 9.17(x) → **9.16(x)** → 9.15(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
9.13(x)	—	次のいずれかになります。 → **9.19(x)** → **9.18(×)** → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x)
9.12(x)	—	次のいずれかになります。 → **9.19(x)** → **9.18(×)** → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x)
9.10(x)	—	次のいずれかになります。 → **9.19(x)** → **9.18(×)** → 9.17(x) → **9.16(x)** → 9.15(x) → 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
9.9(x)	—	次のいずれかになります。 → **9.19(x)** → **9.18(×)** → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x)
9.8(x)	—	次のいずれかになります。 → **9.19(x)** → **9.18(×)** → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x)
9.7(x)	—	次のいずれかになります。 → **9.19(x)** → **9.18(×)** → 9.17(x) → **9.16(x)** → 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。 → **9.19(x)** → **9.18(×)** → 9.17(x) → **9.16(x)** → 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。 → **9.19(x)** → **9.18(×)** → 9.17(x) → **9.16(x)** → 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。 → **9.19(x)** → **9.18(×)** → 9.17(x) → **9.16(x)** → 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
9.3(x)	—	次のいずれかになります。 → **9.19(x)** → **9.18(×)** → 9.17(x) → **9.16(x)** → 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。 → **9.19(x)** → **9.18(×)** → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x) → 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。 → 9.14(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)

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。 → 9.14(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)
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)

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
8.3(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 7.19(1.90) 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。

ID	見出し
CSCwc48458	/api/monitoring/authusers の GET 結果に AnyConnect 認証ユーザーが表示されない
CSCwd58653	ASDM の初期接続またはロード時間の増加

バージョン 7.19(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。

ID	見出し
CSCwc48458	/api/monitoring/authusers の GET 結果に AnyConnect 認証ユーザーが表示されない
CSCwd58653	ASDM の初期接続またはロード時間の増加

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 7.19(1.90) で解決済みのバグ

このリリースで解決されたバグはありません。

バージョン 7.19(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。

ID	見出し
CSCwc21296	Cisco ASDM MSI インストーラが正しく署名されていない
CSCwc63675	ASA の一部のコンテキストから、ASDM のリアルタイムログにログが送信されていない
CSCwc84975	SAML 設定が ASDM 内で保持されない
CSCwd16386	ASDM:DAP 設定に AAA 属性タイプがない（Radius/LDAP）
CSCwd19658	ASDM により、IKEv1 サイト間 VPN のデフォルトグループが誤って DH 5 に設定される

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 Secure Firewall 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。