Cisco ASDM 7.6(x) リリース ノート

初版：2016 年 03 月 21 日

最終更新：2016 年 10 月 24 日

Cisco ASDM 7.6(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 7.6(x) のリリース情報が含まれます。

特記事項

- Microsoft Azure サポートを含む ASAv 9.5.2(200) の各機能は 9.6(1) では使用できません。 これらは、9.6(2) では使用可能です。
- ASDM 7.6(2) は、マルチ コンテキスト モードで AnyConnect クライアント プロファイルをサポートしています。この機能には、AnyConnect バージョン 4.2.00748 または 4.3.03013 以降が必要です。
- （ASA 9.6.2）マルチモード設定を使用している場合のアップグレードの影響：9.5.2 から 9.6.1 にアップグレードし、続いて 9.6.2 にアップグレードすると、マルチモード設定の既存の RAVPN が動作を停止します。9.6.2 イメージへのアップグレード後に、各コンテキストの記憶域を提供し、すべてのコンテキストで新しい AnyConnect イメージを取得するための再設定が必要となります。
- （ASA 9.6(2)）SSH 公開キー認証使用時のアップグレードの影響：SSH 認証が更新されることにより、SSH 公開キー認証を有効にするための新たな設定が必要となります。そのため、公開キー認証を使用した既存の SSH 設定はアップグレード後機能しません。公開キー認証は、Amazon Web サービス（AWS）の ASAv のデフォルトであるため、AWS のユーザはこの問題を確認する必要があります。SSH 接続を失なう問題を避けるには、アップグレードの前に設定を更新します。または（ASDM アクセスが有効になっている場合）アップグレード後に ASDM を使用して設定を修正できます。

  ユーザ名が「admin」の場合の設定例を示します。

```
username admin nopassword privilege 15
username admin attributes
  ssh authentication publickey 55:06:47:eb:13:75:fc:5c:a8:c1:2c:bb:
  07:80:3a:fc:d9:08:a9:1f:34:76:31:ed:ab:bd:3a:9e:03:14:1e:1b hashed
```

ssh authentication コマンドを使用するには、アップグレードの前に次のコマンドを入力します。

```
aaa authentication ssh console LOCAL
username admin password <password> privilege 15
```

nopassword キーワードが存在している場合、これを維持するのではなく、代わりにユーザ名に対応したパスワードを設定することを推奨します。**nopassword** キーワードは、パスワードが入力できないのではなく、どのようなパスワードでも入力できることを意味します。9.6(2) より前のバージョンでは、**aaa** コマンドは SSH 公開キー認証に必須ではありませんでした。このため、**nopassword** キーワードはトリガーされませんでした。本バージョンより **aaa** コマンドは必須となり、**password**（または **nopassword**）キーワードが存在する場合、自動的に **username** の通常のパスワード認証を許可するようになりました。

アップグレード後は、 **username** コマンドに対する **password** または **nopassword** キーワードの指定は任意となり、ユーザがパスワードを入力できなくするよう指定できるようになります。よって、公開キー認証のみを強制的に使用する場合は、**username** コマンドを入力しなおします。

```
username admin privilege 15
```

- Firepower 9300 で ASA をアップグレードする場合のアップグレードの影響：バックエンドにおけるライセンス権限付与名義の変更により、ASA 9.6（1）/FXOS 1.1.4 にアップグレードした場合、最初のリロードの際にスタートアップ コンフィギュレーションが正しく解析されず、アドオンの権利付与に対応する設定が拒否されることがあります。

  スタンドアロン ASA では、新バージョンでのリロード後、権限付与が処理され、「承認済み」状態になるのを待ち（[show license all]または [Monitoring] > [Properties] > [Smart License]）、そのまま設定を保存しないで、もう一度リロード（[reload]または [Tools] > [System Reload]）してください。リロードすると、スタートアップ コンフィギュレーションが正しく解析されます。

  フェールオーバー ペアにアドオンの権限付与がある場合は、FXOS リリースノートのアップグレード手順に従い、さらに各装置のリロード後にフェールオーバーをリセットしてください（[] または **[Monitoring] > [Properties] > [Failover] > [Status]**、**[Monitoring] > [Failover] > [System]** または **[Monitoring] > [Failover] > [Failover Group]** を選択後、[Reset Failover] をクリック）。

  クラスタに関しては、FXOS のリリース ノートのアップグレード手順に従います。以降、さらなる操作は不要です。

- ASA 5508-X および 5516-X を 9.5（x）以降へアップグレードする場合における問題：ASA バージョン 9.5（x）以降へアップグレードする前に、ジャンボ フレーム予約を一度も有効にしたことがない場合は、最大のメモリ フットプリントをチェックする必要があります。製造上の不具合により、ソフトウェアのメモリ制限が誤って適用されていることがあります。以下の修正を適用せずに 9.5（x）以降にアップグレードした場合、デバイスはブートアップ時にクラッシュします。この場合、ROMMON （Load an Image for the ASA 5500-X Series Using

ROMMON） を使用して 9.4 にダウングレードし、次の手順を実行して再度アップグレードする必要があります。

1 次のコマンドを入力して障害のステータスをチェックします。

```
ciscoasa# show memory detail | include Max memory footprint
Max memory footprint        =    456384512
Max memory footprint        =            0
Max memory footprint        =    456384512
```

456,384,512 より少ない値が [Max memory footprint] に戻される場合は障害が発生しているため、アップグレード前に次の手順を実施する必要があります。表示されるメモリが 456,384,512 以上であれば、この手順の残りをスキップして通常通りにアップグレードできます。

2 グローバル コンフィギュレーション モードを開始します。

```
ciscoasa# configure terminal
ciscoasa(config)#
```

3 一時的にジャンボ フレーム予約を有効にします。

```
ciscoasa(config)# jumbo-frame reservation
WARNING: This command will take effect after the running-config
is saved and the system has been rebooted. Command accepted.
INFO: Interface MTU should be increased to avoid fragmenting
jumbo frames during transmit
```

（注） ASA はリロードしません。

4 設定を保存します。

```
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: b511ec95 6c90cadb aaf6b306 41579572
14437 bytes copied in 1.320 secs (14437 bytes/sec)
[OK]
```

5 ジャンボ フレーム予約を無効にします。

```
ciscoasa(config)# no jumbo-frame reservation
WARNING: This command will take effect after the running-config is saved and
the system has been rebooted. Command accepted.
```

（注） ASA はリロードしません。

6 コンフィギュレーション ファイルを再保存します。

```
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: b511ec95 6c90cadb aaf6b306 41579572
14437 bytes copied in 1.320 secs (14437 bytes/sec)
[OK]
```

7 これで、バージョン 9.5（x）以降へアップグレードできます。

- ASA 9.x で使用する RSA ツールキットのバージョンは、ASA 8.4 で使用されたバージョンとは異なるため、これらの 2 つのバージョン間で PKI の動作に違いが生じます。

  たとえば、9.x ソフトウェアを実行している ASA では、フィールド長が 73 文字までの [Organizational Name Value]（OU）フィールドをもつ証明書のインポートが許可されます。8.4 ソフトウェアを実行している ASA では、60 文字までの OU フィールド名をもつ証明書のインポートが許可されます。この相違のため、ASA 9.x でインポートできる証明書を ASA 8.4 ではインポートできません。ASA 9.x 証明書をバージョン 8.4 を実行している ASA にインポートしようとすると、エラー「ERROR: Import PKCS12 operation failed.」が表示されます。

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 クライアントのオペレーティング システムとブラウザの要件

次の表には、ASDM に対応して推奨されるクライアント オペレーティング システムと Java のリストが表示されています。

表 *1*：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				Java SE プラグイン
	Internet Explorer	Firefox	Safari	Chrome	
Microsoft Windows（英語および日本語）： 8 7 Server 2012 R2 Server 2012 Server 2008	Yes	Yes	サポートなし	Yes	7.0 以降
Apple OS X 10.4 以降	サポートなし	Yes	Yes	Yes（64 ビット バージョンのみ）	7.0 以降
Red Hat Enterprise Linux 5（GNOME または KDE）： デスクトップ Desktop with Workstation	該当なし	Yes	該当なし	Yes	7.0 以降

Java およびブラウザの互換性

次の表に、Java、ASDM、およびブラウザの互換性についての互換性警告を示します。

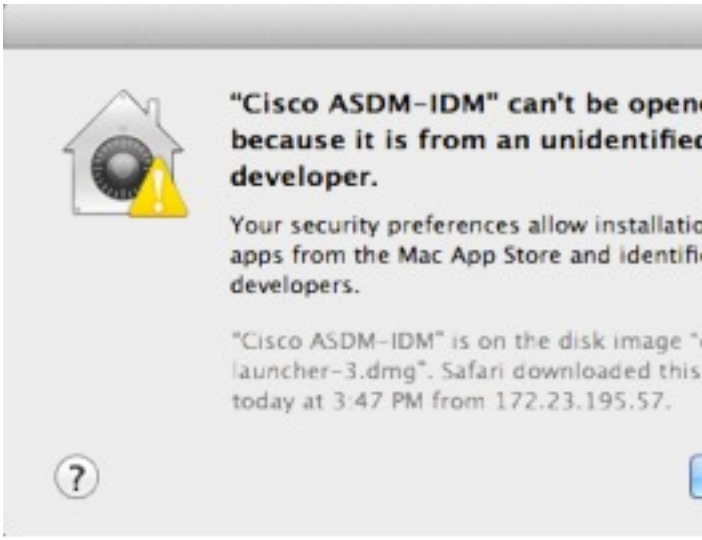
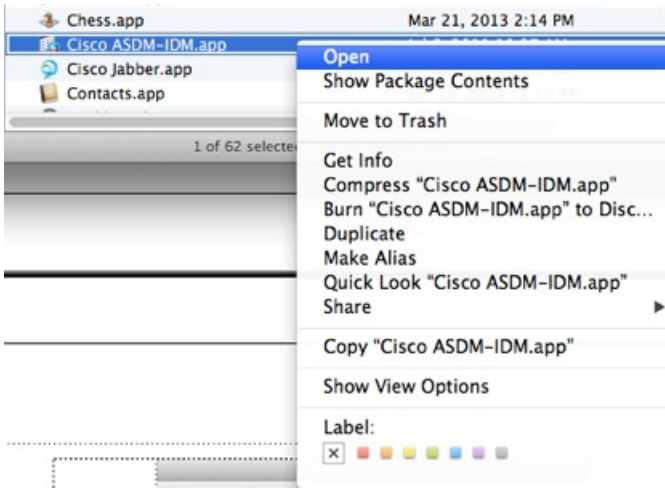
Java バージョン	条件	注意
7 アップデート 51	ASDM ランチャでは信頼できる証明書が必要	ランチャの使用を継続するには、次のいずれかを実行します。 • Java 8 にアップグレードする、または Java を 7 Update 45 以下にダウングレードする。 • ASA に既知の CA から信頼できる証明書をインストールする。 • 自己署名証明書をインストールし、Java に登録する（『Install an Identity Certificate for ASDM』を参照）。 • または、Java Web Start を使用する。 （注） ASDM 7.1(5) 以前は、Java 7 Update 51 ではサポートされていません。すでに Java をアップグレード済みで、バージョン 7.2 以降にアップグレードするために ASDM を起動できない場合は、CLI を使用して ASDM をアップグレードするか、ASDM によって管理する各 ASA について Java コントロールパネルでセキュリティ例外を追加することができます。次の Web ページの「Workaround」の項を参照してください。 http://java.com/en/download/help/java_blocked.xml セキュリティ例外を追加した後に、古いバージョンの ASDM を起動し、7.2 以降にアップグレードします。
	Java Web Start を使用している場合、まれにオンラインヘルプがロードされないことがある	

Java バージョン	条件	注意
		まれに、オンライン ヘルプを起動したときに、ブラウザ ウィンドウがロードを行ってもコンテンツが表示されず、ブラウザにエラー「接続不可能」が表示されることがあります。 回避策： • ASDM ランチャを使用します。 または： • Java ランタイム パラメータの **-Djava.net.preferIPv6Addresses=true** パラメータをクリアします。 1 Java コントロール パネルを起動します。 2 [Java] タブをクリックします。 3 [View] をクリックします。 4 **-Djava.net.preferIPv6Addresses=true** パラメータをクリアします。 5 [OK] をクリックし、[適用] をクリックして、もう一度 [OK] をクリックします。
7 アップデート 45	信頼できない証明書が使用されている場合、ASDM で、不足している権限属性に関する警告が黄色で表示される	Java のバグにより、ASA に信頼できる証明書がインストールされていない場合、JAR マニフェストに不足している権限属性に関する警告が黄色で表示されます。**この警告は無視しても問題ありません**。ASDM 7.2 以降には権限属性が含まれています。警告が表示されないようにするには、既知の CA から信頼できる証明書をインストールするか、ASA で自己署名証明書を生成します（[Configuration] > [Device Management] > [Certificates] > [Identity Certificates] を選択）。ASDM を起動して、証明書に関する警告が表示されたら、[Always trust connections to websites] チェック ボックスをオンにします。

Java バージョン	条件	注意
7	ASA では強力な暗号化ライセンス（3DES/AES）が必要	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。

Java バージョン	条件	注意
すべて	• 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-sslfalse-start** フラグを使用して Chrome の SSL false start を無効にできます。
	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ディセーブルにしてください。
	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。

Java バージョン	条件	注意
すべて（All）	OS X 10.8 以降	

Java バージョン	条件	注意
		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。

Java バージョン	条件	注意
		

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、「ASDM のアイデンティティ証明書のインストール」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。

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。

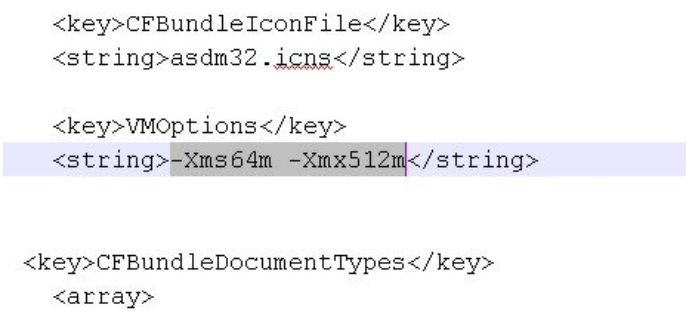
Mac OS での ASDM コンフィギュレーション メモリの増大

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。

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。



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 7.6(2.150) の新機能

リリース：2016年10月12日

このリリースに新機能はありません。

ASA 9.6(2)/ASDM 7.6(2) の新機能

リリース：**2016年8月24日**

機能	説明
プラットフォーム機能	
Firepower 4150 用の ASA を導入しました。	Firepower 4150 用の ASA を導入しました。 FXOS 2.0.1 が必要です。 追加または変更された画面はありません。
ASAv のホット プラグ インターフェイス	システムがアクティブの状態で、ASAv の Virtio 仮想インターフェイスを追加または削除できます。ASAv に新しいインターフェイスを追加すると、仮想マシンがインターフェイスを検出し、プロビジョニングが行われます。既存のインターフェイスを削除すると、仮想マシンはインターフェイスに関連付けられているリソースを解放します。ホットプラグインターフェイスはカーネルベース仮想マシン（KVM）のハイパーバイザ上にある Virtio 仮想インターフェイスに制限されます。
ASAv10 での Microsoft Azure サポート	Microsoft Azure は、プライベート Microsoft Hyper V ハイパーバイザを使用するパブリック クラウド環境です。ASAv は、Hyper V ハイパーバイザの Microsoft Azure 環境でゲストとして実行されます。Microsoft Azure 上の ASAv は、4 つの vCPU、14 GB、4 つのインターフェイスをサポートする Standard D3 の 1 つのインスタンス タイプをサポートします。 バージョン *9.5(2.200)* でも同様です。
ASAv の管理 0/0 インターフェイスでの通過トラフィック サポート	ASAv の管理 0/0 インターフェイスでトラフィックを通過させることができるようになりました。以前は、Microsoft Azure 上の ASAv のみで通過トラフィックをサポートしていました。今後は、すべての ASAv で通過トラフィックがサポートされます。任意で、このインターフェイスを管理専用に設定できますが、デフォルトでは管理専用に設定されていません。

機能	説明
コモン クライテリア証明書	ASA は、コモン クライテリアの要件に適合するように更新されました。この証明書に追加された次の機能については、この表の行を参照してください。 • ASDM での ASA SSL サーバ モード マッチング • SSL クライアントの RFC 6125 サポート： ◦ セキュアな syslog サーバの接続とスマート ライセンシング接続のための参照 ID ◦ ASA クライアントによるサーバ証明書の拡張キーの使用状況確認 ◦ ASA が TLS1.1 と 1.2 の TLS クライアントとして動作する際の相互認証 • PKI デバッグ メッセージ • 暗号キー抹消検査 • IKEv2 の IPsec/ESP トランスポート モードのサポート • 追加された syslog メッセージ
ファイアウォール機能	
TCP 経由での DNS インスペクション	DNS over TCP トラフィック（TCP/53）を検査できるようになりました。 次のページが変更されました。[Configuration] > [Firewall] > [Objects] > [Inspection Maps] > [DNS] > [Add/Edit] ダイアログボックス
MTP3 User Adaptation（M3UA）インスペクション	M3UA トラフィックを検査できるようになりました。また、ポイント コード、サービス インジケータ、およびメッセージのクラスとタイプに基づいてアクションを適用できるようになりました。 次のページが追加または変更されました。[Configuration] > [Firewall] > [Objects] > [Inspection Maps] > [M3UA]、サービス ポリシー ルールの場合は [Rule Action] > [Protocol Inspection] タブ
Session Traversal Utilities for NAT（STUN）インスペクション	Cisco Spark を含む WebRTC アプリケーションの STUN トラフィックを検査できるようになりました。インスペクションでは、リターン トラフィックに必要なピンホールが開きます。 次のタブにオプションが追加されました。[Add/Edit Service Policy] ダイアログボックスの [Rule Actions] > [Protocol Inspection]

機能	説明
Cisco クラウド Web セキュリティのアプリケーション層健全性チェック	サーバが正常かどうかを判断する際に、クラウド Web セキュリティ アプリケーションの健全性をチェックするように Cisco クラウド Web セキュリティを設定できるようになりました。アプリケーションの健全性を確認することで、プライマリ サーバが TCP スリーウェイ ハンドシェイクに応答する場合に、システムはバックアップ サーバにフェールオーバーできますが、要求を処理することはできません。これにより、より信頼性の高いシステムを実現します。 次の画面が変更されました。[Configuration] > [Device Management] > [Cloud Web Security]
ルートの収束に対する接続ホールドダウン タイムアウト	接続で使用されているルートがもう存在していない、または非アクティブになったときに、システムが接続を保持する時間を設定できるようになりました。このホールドダウン期間内にルートがアクティブにならない場合、接続は解放されます。ルートの収束がさらに迅速に行われるようにホールドダウン タイマーを短縮することができます。ただし、ほとんどのネットワークでは、ルートのフラッピングを防止するためにデフォルトの 15 秒が適切です。 次の画面が変更されました。[Configuration] > [Firewall] > [Advanced] > [Global Timeouts] バージョン *9.4(3)* でも同様です。
TCP オプション処理の変更	TCP マップを設定する際にパケットの TCP ヘッダー内の TCP MSS および MD5 オプションに対するアクションを指定できるようになりました。さらに、MSS、タイムスタンプ、ウィンドウサイズ、および選択的確認応答オプションのデフォルトの処理が変更されました。以前は、これらのオプションは、ヘッダーに特定のタイプのオプションが 2 つ以上ある場合でも許可されていました。現在は、パケットに特定のタイプのオプションが 2 つ以上含まれている場合、そのパケットはデフォルトでドロップされます。たとえば、以前は2つのタイムスタンプ オプションがあるパケットは許可されていましたが、現在はドロップされます。 MD5、MSS、選択的確認応答、タイムスタンプ、およびウィンドウサイズに対し、同じタイプの複数のオプションを有効にするための TCP マップを設定できます。MD5 オプションの場合、以前のデフォルトではオプションがクリアされたのに対し、現在のデフォルトでは許可されます。また、MD5 オプションを含むパケットをドロップすることもできます。MSS オプションの場合は、TCP マップで最大セグメント サイズを設定できます（トラフィック クラスごとに）。他のすべての TCP オプションのデフォルトに変更はありません。これらはクリアされます。 次の画面が変更されました。[Configuration] > [Firewall] > [Objects] > [TCP Maps] > [Add/Edit] ダイアログボックス
トランスペアレント モードで、ブリッジ グループごとのインターフェイス数が最大で 64 に増加	ブリッジ グループあたりのインターフェイスの最大数が 4 から 64 に拡張されました。 変更された画面はありません。

機能	説明
トランスペアレント モードでのマルチキャスト接続のフロー オフロードのサポート	トランスペアレントモードのFirepower4100および9300シリーズデバイスで、NICに直接切り替えられるマルチキャスト接続をオフロードできるようになりました。マルチキャスト オフロードは、インターフェイスを 2 つだけ含むブリッジ グループに使用できます。 この機能には、新規のコマンドまたは ASDM 画面はありません。
カスタマイズ可能な ARP レート制限	1秒あたり許可されるARPパケットの最大数を設定できます。デフォルト値はASAモデルによって異なります。この値は ARP ストーム攻撃を防ぐためにカスタマイズできます。 次の画面が変更されました。[Configuration] > [Device Management] > [Advanced] > [ARP] > [ARP Static Table]
IEEE 802.2 論理リンク制御（LLC）パケットの Destination Service Access Point（DSAP）アドレスに対する Ethertype ルールのサポート	IEEE 802.2 論理リンク制御パケットの Destination Service Access Point（DSAP）アドレスに対して、Ethertypeのアクセス制御ルールを記述できるようになりました。この追加により、**bpdu** キーワードが対象トラフィックに一致しなくなります。**bpdu** ルールを **dsap 0x42** に書き換えます。 次の画面が変更されました。[Configuration] > [Firewall] > [EtherType Rules].
リモート アクセス機能	
マルチ コンテキスト モードの場合の証明書の事前入力/ユーザ名	AnyConnect SSL サポートが拡張され、これまでシングル モードでのみ使用可能だった証明書の事前入力とユーザ名取得機能のCLIがマルチコンテキストモードでも有効にできるようになりました。 変更された画面はありません。
マルチ コンテキスト モードの VPN 強化	マルチコンテキストモードのリモートアクセス VPN はフラッシュ仮想化をサポートします。使用可能な合計フラッシュに基づき、コンテキストごとにプライベート記憶域と共有ストレージの場所が設定できます。 • プライベート記憶域：該当ユーザのみに関連付けられ、該当ユーザ対象コンテンツ固有のファイルを保存します。 • 共有ストレージ：有効になると、この領域にファイルがアップロードされ、あらゆるユーザ コンテキストが読み取り/書き込みできるようこの領域へのアクセスが許可されます。 次の画面が変更されました。[Configuration] > [Context Management] > [Security Contexts].
マルチコンテキスト デバイスでの AnyConnect クライアント プロファイルのサポート	AnyConnect クライアント プロファイルがマルチコンテキストのデバイスでサポートされました。ASDM を使用して新しいプロファイルを追加するには、AnyConnect セキュア モビリティ クライアント リリース 4.2.00748 または 4.3.03013 以降が必要です。

機能	説明
Umbrella ローミング セキュリティ モジュールのサポート	アクティブな VPN がない場合には、DNS 層のセキュリティを強化するため、AnyConnect セキュア モビリティ クライアントの Umbrella ローミング セキュリティ モジュールを設定できます。 次の画面が変更されました。[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Client Profile].
IKEv2 の IPsec/ESP トランスポート モードのサポート	ASA IKEv2 ネゴシエーションでトランスポート モードがサポートされるようになりました。これは、トンネル（デフォルト）モードの代わりに使用できます。トンネル モードでは IP パケット全体がカプセル化されます。トランスポート モードでは IP パケットの上位層プロトコルだけがカプセル化されます。トランスポート モードでは、送信元ホストと宛先ホストの両方が IPSec をサポートしている必要があります。また、トランスポート モードは、トンネルの宛先ピアが IP パケットの最終宛先である場合にだけ使用されます。 次の画面が変更されました。[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPsec] > [IPsec Proposals (Transform Sets)] > [IKEv2 proposals] > [Add/Edit]
IPsec 内部パケットに対するパケット単位のルーティング ルックアップ	デフォルトでは、外部 ESP パケットに対してはパケット単位の隣接関係（アジャセンシー）ルックアップが行われ、IPsec トンネル経由で送信されるパケットに対してはルックアップが行われません。一部のネットワーク トポロジでは、ルーティング アップデートによって内部パケットのパスが変更され、ローカル IPsec トンネルが引き続きアップ状態である場合、トンネル経由のパケットは正しくルーティングされず、宛先に到達しません。これを防止するには、新しいオプションを使用し、IPsec 内部パケットに対してパケット単位のルーティング ルックアップを有効にします。 次の画面に [Enable IPsec Inner Routing Lookup] チェックボックスが追加されました。[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPsec] > [Crypto Maps]
証明書とセキュアな接続の機能	
ASA クライアントによるサーバ証明書の拡張キーの使用状況確認	syslog、スマート ライセンス サーバ証明書は、[Extended Key Usage] フィールドに [ServerAuth] を含める必要があります。そうしない場合、接続は失敗します。
ASA が TLS1.1 と 1.2 の TLS クライアントとして動作する際の相互認証	サーバが認証のために ASA からクライアント証明書を要求した場合、ASA はそのインターフェイス用に設定されたクライアント アイデンティティ証明書を送信します。証明書は **ssl trust-point** コマンドで設定されます。
PKI デバッグ メッセージ	ASA PKI モジュールは、SCEP 登録、HTTP を使用した失効チェックなどのために CA サーバへ接続します。これらすべての ASA PKI 通信はデバッグ追跡のため、debug crypto ca メッセージ 5 を付してログに記録されます。

機能	説明
ASDM での ASA SSL サーバ モード マッチング	証明書マップと照合するために、証明書で認証を行う ASDM ユーザに対して証明書を要求できるようになりました。 次の画面が変更されました。[Configuration] > [Device Management] > [Management Access] > [ASDM/HTTPS/Telnet/SSH]
セキュアな syslog サーバの接続とスマート ライセンシング接続のための参照 ID	TLS クライアント処理は、RFC 6125 のセクション 6 に定義されるサーバ ID の検証ルールをサポートするようになりました。ID 確認は syslog サーバとスマート ライセンス サーバへの TLS 接続の PKI 確認中に行われます。提示された ID が設定されたリファレンス ID と一致しない場合、接続を確立できません。 次の画面が変更されました。 [Configuration] > [Remote Access VPN] > [Advanced] [Configuration] > [Device Management] > [Logging] > [Syslog Servers] > [Add/Edit] [Configuration] > [Device Management] > [Smart Call Home]
暗号キー抹消検査	ASA の暗号化システムは、新しい暗号キー抹消要件に適合するように更新されました。キーはすべてゼロで上書きされ、データを読み出して上書きが正しく行われたか確認する必要があります。
SSH 公開キー認証の改善	以前のリリースでは、ローカル ユーザ データベースを使用して AAA SSH 認証を同時に有効にすることなく、SSH 公開キー認証を有効にできました。この設定は修正されたため、AAA SSH 認証を明示的に有効にする必要があります。ユーザが秘密キーの代わりにパスワードを使用することができないよう、パスワード未定義のユーザ名を作成することができるようになりました。 次の画面が変更されました。 [Configuration] > [Device Management] > [Management Access] > [ASDM/HTTPS/Telnet/SSH] [Configuration] > [Device Management] > [Users/AAA] > [User Accounts] > [Add/Edit User Account]
インターフェイス機能	
FXOS シャーシ の ASA のMTU サイズ増加	Firepower 4100 および 9300 で、最大 MTU を 9188 バイトに設定できます。これまでは 9000 バイトが最大でした。この MTU は FXOS 2.0.1.68 以降でサポートされます。 次の画面が変更されました。[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Advanced]
ルーティング機能	

機能	説明
Bidirectional Forwarding Detection（BFD）のサポート	ASAは、BFD ルーティング プロトコルをサポートするようになりました。BFD テンプレート、インターフェイスおよびマッピングの設定が新たにサポートされました。BFD を使用するための BGP ルーティング プロトコルのサポートも追加されました。 次の画面が追加または変更されました。 [Configuration] > [Device Setup] > [Routing] > [BFD] > [Template] [Configuration] > [Device Setup] > [Routing] > [BFD] > [Interface] [Configuration] > [Device Setup] > [Routing] > [BFD] > [Map] [Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv6 Family] > [Neighbors]
IPv6 DHCP	ASA で IPv6 アドレッシングの次の機能がサポートされました。 • DHCPv6 アドレス クライアント：ASA は DHCPv6 サーバから IPv6 グローバル アドレスとオプションのデフォルト ルートを取得します。 • DHCPv6 プレフィックス委任クライアント：ASA は DHCPv6 サーバから委任プレフィックスを取得します。ASA は、これらのプレフィックスを使用して他の ASA インターフェイスのアドレスを設定し、ステートレス アドレス自動設定（SLAAC）クライアントが同じネットワーク上で IPv6 アドレスを自動設定できるようにします。 • 委任プレフィックスの BGP ルータ アドバタイズメント • DHCPv6 ステートレス サーバ：SLAAC クライアントが ASA に情報要求（IR）パケットを送信すると、ASA はドメインインネームなどの他の情報を SLAAC クライアントに提供します。ASA は、IR パケットを受け取るだけで、クライアントにアドレスを割り当てません。 次の画面が追加または変更されました。 [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add Interface] > [IPv6] [Configuration] > [Device Management] > [DHCP] > [DHCP Pool] [Configuration] > [Device Setup] > [Routing > BGP] > [IPv6 Family] > [Networks] [Monitoring] > [interfaces] > [DHCP]
ハイ アベイラビリティとスケーラビリティの機能	
アクティブ/スタンバイ フェールオーバーを使用するとき、AnyConnect からのダイナミック ACL の同期時間が改善されました。	フェールオーバー ペアで AnyConnect を使用するとき、関連付けられているダイナミック ACL（dACL）のスタンバイ ユニットへの同期時間が改善されました。以前は、大規模な dACL の場合、スタンバイ ユニットが可用性の高いバックアップを提供するのではなく同期作業で忙しい間は、同期時間が長時間に及ぶことがありました。 変更された画面はありません。

機能	説明
ライセンシング機能	
ASAv の永続ライセンス予約	Cisco Smart Software Manager との通信が許可されていない非常にセキュアな環境では、ASAv 用に永続ライセンスを要求できます。9.6(2) では、Amazon Web サービスの ASAv 向けに、この機能のサポートが追加されました。この機能は Microsoft Azure ではサポートされません。 （注） すべてのアカウントがパーマネント ライセンスの予約について承認されているわけではありません。設定を開始する前に、この機能についてシスコの承認があることを確認します。 次のコマンドが導入されました。**license smart reservation、license smart reservation cancel、license smart reservation install、license smart reservation request universal、license smart reservation return** ASDM サポートはありません。 バージョン *9.5(2.200)* でも同様です。
ASAvの短かい文字列の拡張機能向けの永続ライセンス予約	スマートエージェント（1.6.4への）の更新により、要求と認証コードには短い文字列が使用されます。 変更された画面はありません。
FXOS シャーシ上での ASA の永続ライセンス予約	Cisco Smart Software Manager との通信が許可されていない非常にセキュアな環境では、FirePOWER 9300 および FirePOWER 4100 の ASA 用に永続ライセンスを要求できます。永続ライセンスには、標準層、高度暗号化（該当する場合）、セキュリティ コンテキスト、キャリア ライセンスをはじめ、使用可能なすべてのライセンス権限が含まれます。FXOS 2.0.1 が必要です。 すべての設定はFXOS シャーシで実行されるため、ASA での設定は不要です。
ASAv 用スマート エージェントの v1.6 へのアップグレード	スマート エージェントはバージョン 1.1 からバージョン 1.6 へアップグレードされました。このアップグレードは永続ライセンス予約をサポートするほか、ライセンス アカウントに設定された権限に従って、高度暗号化（3DES/AES）ライセンス権限の設定もサポートします。 （注） バージョン9.5（2.200）からダウングレードした場合、ASAvはライセンス登録状態を保持しません。[Configuration] > [Device Management] > [Licensing] > [Smart Licensing] ページで [Force registration] オプションを指定して、再登録する必要があります。Smart Software Manager から ID トークンを取得します。 変更された画面はありません。 バージョン *9.5(2.200)* でも同様です。
モニタリング機能	

機能	説明
type asp-drop のパケット キャプチャは、ACL と一致フィルタリングをサポートします。	asp-drop タイプのパケット キャプチャを作成するとき、ACL または一致するオプションを指定してキャプチャの範囲を制限できるようになりました。 変更された画面はありません。
フォレンジック分析の強化	ASA で実行されているすべてのプロセスのコア ダンプを作成できます。主な ASA プロセスのテキスト セクションを抽出し、検証用にコピーできます。 変更された画面はありません。
NetFlow経由の接続ごとのトラッキング パケット数の追跡	NetFlow ユーザがある接続上で双方向に送受信されるレイヤ 4 パケットの数を確認することを可能にする 2 つのカウンタが追加されました。これらのカウンタを使用して、平均パケット レートおよびサイズを判断し、トラフィック タイプ、異常、イベントをより適切に予測できます。 変更された画面はありません。
フェールオーバーの SNMP engineID の同期	フェールオーバー ペアでは、一対の ASA の SNMP engineID は両方のユニットで同期されます。ASA ごとに、同期された engineID、ネイティブ engineID、およびリモート engineID による engineID が 3 セット維持されます。 SNMPv3 ユーザは、ローカライズされた **snmp-server user** 認証とプライバシー オプションを保存するためのプロファイルを作成するときに ASA の engineID も指定できます。ユーザがネイティブ engineID を指定しない場合、**show running config** 出力に engineID がユーザごとに 2 つずつ表示されます。 次のコマンドが変更されました。**snmp-server user** ASDM サポートはありません。 バージョン *9.4(3)* でも同様です。

ASA 9.6(1)/ASDM 7.6(1) の新機能

リリース：2016年3月21日

（注） Microsoft Azure サポートを含む ASAv 9.5.2(200) の各機能は 9.6(1) では使用できません。これらは、9.6(2) では使用可能です。

機能	説明
プラットフォーム機能	

機能	説明
Firepower 4100 シリーズ の ASA	Firepower 4110、4120、4140 用の ASA を導入しました。 FXOS 1.1.4 が必要です。 追加または変更された画面はありません。
ISA 3000 の SD カードのサポート	ISA 3000 の外部ストレージとして SD カードが使用できるようになりました。カードは、ASA ファイル システムのディスク 3 として表示されます。プラグ アンド プレイをサポートするにはハードウェア バージョン 2.1 以降が必要です。ハードウェア バージョンをチェックするには、**show module** コマンドを使用します。 追加または変更された画面はありません。
ISA 3000 のデュアル電源サポート	ISA 3000 のデュアル電源では、ASA OS に望ましい構成としてデュアル電源を設定できます。1 つの電源に障害が発生すると、ASA はアラームを発します。デフォルトでは、ASA は単一電源を想定していますが、装備される電源のいずれかが機能しているかぎりアラームを発しません。 ASDM サポートはありません。
ファイアウォール機能	
Diameter インスペクションの改善	TCP/TLS トラフィック上の Diameter を検査し、厳密なプロトコル準拠チェックを適用し、クラスタ モードで SCTP 上の Diameter を検査できるようになりました。 次の画面が追加または変更されました。 [Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [Diameter] [Configuration] > [Firewall] > [Service Policy] の [add/edit] ウィザードの [Rule Actions] > [Protocol Inspection] タブ
クラスタ モードでの SCTP ステートフル インスペクション	SCTP ステートフル インスペクションがクラスタ モードで動作するようになりました。また、クラスタ モードで SCTP ステートフル インスペクション バイパスを設定することもできます。 追加または変更された画面はありません。
H.460.18 互換性に関連する H.225 SETUP メッセージの前に着信する H.255 FACILITY メッセージに対する H.323 インスペクションのサポート。	H.225 FACILITY メッセージが H.225 SETUP メッセージの前に着信する（これは、エンドポイントが H.460.18 に準拠する場合に発生する場合があります）ことを許可するように H.323 インスペクション ポリシー マップを設定できるようになりました。 H.323 インスペクション ポリシー マップの [Call Attributes] タブにオプションが追加されました。

機能	説明
Security Exchange Protocol（SXP）バージョン 3 の Cisco TrustSec サポート。	ASA の Cisco Trustsec は、ホスト バインディングよりも効率的な SGT とサブネット間のバインディングを可能にする SXPv3 を実装するようになりました。 [Configuration] > [Firewall] > [Identity By TrustSec] と [SGT Map Setup] ダイアログボックスが変更されました。
Firepower 4100 シリーズ のフロー オフロードのサポート。	ASA からオフロードされ、Firepower 4100 シリーズ の NIC で直接切り替える必要があるフローを特定できるようになりました。 FXOS 1.1.4 が必要です。 追加または変更された画面はありません。
リモート アクセス機能	
IKEv2 フラグメンテーション、RFC-7383 サポート	ASA では、IKEv2 パケットのこの標準的なフラグメンテーションがサポートされるようになりました。これにより、Apple、Strongswan など、他の IKEv2 の実装との相互運用性を実現します。ASA は、AnyConnect クライアントなどの RFC-7383 をサポートしないシスコ製品との後方互換性を保つため、独自の IKEv2 フラグメンテーションを引き続きサポートします。
Firepower 9300 と Firepower 4100 シリーズでの VPN スループット パフォーマンス強化	**crypto engine accelerator-bias** コマンドが Firepower 9300 と Firepower 4100 シリーズ上の ASA セキュリティ モジュールでサポートされるようになりました。このコマンドにより、IPSec または SSL に対して暗号コアを「優先的に使用」できます。 追加または変更された画面はありません。
設定可能な SSH 暗号機能と HMAC アルゴリズム	ユーザは SSH 暗号化を管理するときに暗号化モードを選択し、さまざまなキー交換アルゴリズムに対して HMAC と暗号化を設定できます。アプリケーションに応じて、暗号の強度を強くしたり弱くする必要がある場合があります。セキュアなコピーのパフォーマンスは暗号化アルゴリズムに一部依存します。デフォルトで、ASA は 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr の順にアルゴリズムをネゴシエートします。提示された最初のアルゴリズム（3des-cbc）が選択された場合、aes128-cbc などの一層効率的なアルゴリズムが選択された場合よりも大幅にパフォーマンスが低下します。提案されたアルゴリズムを変更するには、たとえば、**ssh cipher encryption custom aes128-cbc** を使用します。 次の画面が導入されました。[Configuration] > [Device Management] > [Advanced] > [SSH Ciphers] *9.1(7)* 、*9.4(3)* および *9.5(3)* でも使用可能です。

機能	説明
IPv6 の HTTP リダイレクト サポート	ASDM アクセスまたはクライアントレス SSL VPN 用の HTTPS に HTTP リダイレクトを有効にすると、IPv6 アドレスへ送信されるトラフィックもリダイレクトできるようになりました。 次の画面に機能が追加されました。[Configuration] > [Device Management] > [HTTP Redirect] *9.1(7)* および *9.4(3)* でも使用可能です。
ルーティング機能	
IS-IS ルーティング	ASA で Intermediate System to Intermediate System（IS-IS）のルーティング プロトコルがサポートされました。IS-IS ルーティング プロトコルを使用した、データのルーティング、認証の実行、およびルーティング情報の再配布とモニタについて、サポートが追加されました。 次の画面が導入されました。 [Configuration] > [Device Setup] > [Routing] > [ISIS] [Monitoring] > [Routing] > [ISIS]
ハイ アベイラビリティとスケーラビリティの機能	
ルーテッドおよびスパンド EtherChannel モードのサイト固有の IP アドレスのポート	スパンド EtherChannel のルーテッド モードでのサイト間クラスタリングの場合、サイト個別の MAC アドレスに加えて、サイト個別の IP アドレスを設定できるようになりました。サイト IP アドレスを追加することにより、グローバル MAC アドレスからの ARP 応答を防止するために、ルーティング問題の原因になりかねない Data Center Interconnect（DCI）経由の移動によるオーバーレイ トランスポート仮想化（OTV）デバイスの ARP 検査を使用することができます。MAC アドレスをフィルタ処理するために VACL を使用できないスイッチには、ARP 検査が必要です。 次の画面が変更されました。[Configuration] > [Device Setup] > [Interface Settings] > Interfaces] > [Add/Edit EtherChannel Interface] > [Advanced]
管理機能	
ローカルの**username**および**enable**パスワードでより長いパスワード（127文字まで）がサポートされます。	127 文字までのローカル **username**と**enable**パスワードを作成できます（以前の制限は 32 文字でした）。32 文字以上のパスワードを作成すると、PBKDF2（パスワードベース キー派生関数2）のハッシュを使用して設定に保存されます。これよりも短いパスワードは引き続き MD5 ベースのハッシュを使用します。 次の画面が変更されました。 [Configuration] > [Device Setup] > [Device Name/Password] > [Enable Password] [Configuration] > [Device Management] > [Users/AAA] > [User Accounts] > [Add/Edit User Account] > [Identity]

機能	説明
CISCO-ENHANCED-MEMPOOL-MIB の cempMemPoolTable のサポート	CISCO-ENHANCED-MEMPOOL-MIB の cempMemPoolTable がサポートされました。これは、管理型システムのすべての物理エンティティのメモリプールモニタリングエントリのテーブルです。 （注） CISCO-ENHANCED-MEMPOOL-MIB は 64 ビットのカウンタを使用して、プラットフォーム上の 4 GB 以上のメモリのレポーティングをサポートします。 追加または変更された画面はありません。 *9.1(7)* および *9.4(3)* でも使用可能です。
REST API バージョン 1.3.1	REST API バージョン 1.3.1 のサポートが追加されました。

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。

アップグレード パス

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、最新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。

現在の ASA バージョン	最初のアップグレード先：	次のアップグレード先：
8.2(x) 以前	8.4(5)	9.1(3) 以降
8.3(x)	8.4(5)	9.1(3) 以降
8.4(1) ～ 8.4(4)	8.4(5) または 9.0(2+)	9.1(3) 以降
8.4(5+)	—	9.1(3) 以降
8.5(1)	9.0(2+)	9.1(3) 以降
8.6(1)	9.0(2+)	9.1(3) 以降
9.0(1)	9.0(2+)	9.1(3) 以降
9.0(2+)	—	9.1(3) 以降
9.1(1)	9.1(2)	9.1(3) 以降

現在の ASA バージョン	最初のアップグレード先：	次のアップグレード先：
9.1(2+)	—	9.1(3) 以降
9.2(x)	—	9.2(2) 以降
9.3(x)	—	9.3(2) 以降
9.4(x)	—	9.4(2) 以降
9.5(x)	—	9.5(2) 以降
9.6(x)	—	9.6(2) 以降
9.7(x)	—	9.8(1) 以降

アップグレード リンク

アップグレードを完了するには、Upgrade to ASA 9.6 and ASDM 7.6 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 Cisco バグ追跡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 Help & 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 7.6(2.150) で未解決のバグ

シスコ サポート契約がある場合は、次のダイナミック検索を使用して、バージョン 7.6(2.150) で重大度 3 以上のすべての未解決のバグを検索できます：

- 7.6(2.150) open bug search。

次の一覧表は、このリリース ノートの発行時点で未解決のバグです。

警告 ID 番号	説明
CSCuz92899	プリログイン ポリシーの変更が保存されない
CSCva89785	ASDM：サービス ポリシーの下の TCP タイムアウト値が ASA に間違った値をプッシュする
CSCva91507	ASDM が 0 ~ 65535 のポート範囲を許容しない

バージョン 7.6(2) で未解決のバグ

シスコ サポート契約がある場合は、次のダイナミック検索を使用して、バージョン 7.6(2) で重大度 3 以上のすべての未解決のバグを検索できます：

- 7.6(2) open bug search。

次の一覧表は、このリリース ノートの発行時点で未解決のバグです。

警告 ID 番号	説明
CSCuz92899	プリログイン ポリシーの変更が保存されない
CSCva89785	ASDM：サービス ポリシーの下の TCP タイムアウト値が ASA に間違った値をプッシュする
CSCva91507	ASDM が 0 ~ 65535 のポート範囲を許容しない

バージョン 7.6(1) で未解決のバグ

シスコ サポート契約がある場合は、次のダイナミック検索を使用して、バージョン 7.6(1) で重大度 3 以上のすべての未解決のバグを検索できます：

- 7.6(1) open bug search。

次の一覧表は、このリリース ノートの発行時点で未解決のバグです。

ID	説明
CSCuw54048	SFR モジュール搭載の ASDM に Windows 10 のサポート機能を追加する
CSCuy01413	ASDM：IKEv2 接続プロファイルの [Send certificate chain] がグレーアウトされる

ID	説明
CSCuy15812	同じメトリックの異なるインターフェイスに複数のデフォルトルートを設定できない
CSCuy47135	WebVPN が無効な場合に ASDM が SSL トラストポイントを変更しない
CSCuy48673	ASDM で DAP:endpoint.as.TrendMicroAS が誤設定される

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 7.6(2.150) で解決済みのバグ

シスコ サポート契約がある場合は、次の検索を使用して、すべてのバグ解決済みのバグを検索できます：

- 7.6(2.150) fixed bug search

次の一覧表は、このリリース ノートの発行時点で解決済みのバグです。

警告 ID 番号	説明
CSCvb16663	ASDM 7.6.2 が VPN セッションを表示できない。97% のローディングで先に進まない

バージョン 7.6(2) で解決済みのバグ

シスコ サポート契約がある場合は、次の検索を使用して、すべてのバグ解決済みのバグを検索できます：

- 7.6(2) fixed bug search

次の一覧表は、このリリース ノートの発行時点で解決済みのバグです。

警告 ID 番号	説明
CSCuy01413	ASDM：IKEv2 接続プロファイルの [Send certificate chain] がグレーアウトされる
CSCuy15812	同じメトリックの異なるインターフェイスに複数のデフォルトルートを設定できない
CSCuy47135	WebVPN が無効な場合に ASDM が SSL トラストポイントを変更しない

警告 ID 番号	説明
CSCuy47429	ASDM ERROR: % Incomplete command でコンテキストを作成できない
CSCuy60531	[Traffic Selection] タブが選択されると ASDM ダイナミック トンネルで any/any が許可されてしまう
CSCuy73370	フィードバック サービス プロファイルの間違ったファイル拡張子
CSCuy75518	コマンド認可で ASDM ロギング フィルタが動作しない
CSCuy76658	複数の ACE が一度に編集されると、ASDM が ACL のコメントを複製する
CSCuy83681	適用後に、ASDM NAT 免除インターフェイスを変更できない
CSCuy97880	ASDM が IKEv2 ポリシーでの aes-gcm 暗号方式の追加を許可しない
CSCuz01625	IKEv1 のみが有効な場合にグループポリシーを適用すると、IKEv2 が有効になる
CSCuz18280	ASDM キャプチャ（ASA クラスタの管理）が正しく機能しない
CSCuz19708	ASDM：「without-csd」CLI 設定が GUI に反映されない
CSCuz23820	ASDM が間違ってサービス オブジェクト定義をグループ化する
CSCuz31043	ASDM：マルチキャスト igmp アクセス グループ パネルの問題
CSCuz32502	ASDM：マルチキャスト PIM プロトコルの問題
CSCuz43269	複数のコメントを削除すると、ASDMが正しく行をインデックス付けしない
CSCuz47825	重複エラー メッセージが応答に含まれない
CSCuz54866	ASA5505 で ASDM を使用してインターフェイス セキュリティ レベルを設定できない
CSCuz55053	サービス オブジェクト グループを編集および追加すると、ASDM が送信元ポートを変更する
CSCuz58354	アルファベット順にソートした後、ASDM で AAA サーバ グループが不一致となる
CSCuz58762	AV をアクティブ化する DAP ルールが AV のインストールされていないクライアントと一致する
CSCuz79772	ASDM を介して Hostscan イメージをバックアップできない

警告 ID 番号	説明
CSCuz89301	ASDM から、nameif に or を含むインターフェイスに設定されたサーバが見つからない
CSCuz99734	ASDM に max-anyconnect-premium-or-essentials-limit を無効にするオプションがない
CSCva31853	ASDM 7.6(1) で「User authenticated using MSCHAP」オプションが欠落している
CSCva32027	オンボックス：コンテキストの切り替え後に ASDM の SFR への接続が失われる
CSCva55292	DOC：HA：イメージをアクティブに設定する前に、ASDM イメージがスタンバイに事前アップロードされる

バージョン 7.6(1) で解決済みのバグ

シスコ サポート契約がある場合は、次の検索を使用して、すべてのバグ解決済みのバグを検索できます：

- 7.6(1) fixed bug search

次の一覧表は、このリリース ノートの発行時点で解決済みのバグです。

ID	説明
CSCut04399	Java 8 にアップグレード後に ASDM が MAC 上でハングする
CSCux20823	オブジェクト グループからオブジェクトを削除する際、ASDM のコマンド順序に誤りがある
CSCux26490	DAP ブックマーク リストが 245 文字を超えると、ASDM がリスト全体を削除する
CSCux33151	ASDM が ACL でのコメントを置換する代わりに複製する
CSCux33960	ASDM が IKEv2 ポリシーで 5 を超える Diffie-Hellman グループを設定できない
CSCux35016	ASDM の暗号マップに矛盾がある
CSCux37581	ASDM 7.5.2 がアクティブな AnyConnect クライアントを表示しない

ID	説明
CSCux39599	ASDM で AnyConnect プロファイルを変更するとアクセスリスト エラーとなる
CSCux59901	CLI から無効にするとヘルス チェック オプションが ASDM で同期されない
CSCux61213	ASDM：ASDM を使用している AAA ルール設定で「any6」オプションが欠落している
CSCux63050	実行コンフィギュレーションがシステム コンテキスト内で TFTP の誤ったインターフェイスに保存される
CSCux68972	ASD：単一エントリの ACL が暗号マップを削除する
CSCux93603	ASDM 7.6.1.11 が VPN セッションを表示できない。97% のローディングで先に進まない
CSCuy01349	ASDM が、CLI 2-255 であるにも関わらず、0-255 からの IPv6 ルーティング タイプの設定を許容してしまう
CSCuy09605	ASDM：10 文字を超えるコミュニティ名のルートマップ エントリを編集できない
CSCuy12402	マイナーな変更を追加すると、ASDM 設定が不必要に再適用される
CSCuy13768	ACL の変更後、ASDM が ACL を暗号マップに再適用できない
CSCuy15891	ASDM でエラー「The Maximum AnyConnect Sessions must be between 0 and 1」が発生する
CSCuy47429	ASDM ERROR: % Incomplete command でコンテキストを作成できない

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。