Cisco ASDM 7.4(x) リリースノート

初版：2015 年 3 月 23 日

最終更新：2016 年 6 月 21 日

Cisco ASDM 7.4(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 7.4(x) のリリース情報が記載されています。

特記事項

- 潜在的なトラフィック停止（9.4(3.11) ～ 9.4(4)）：バグ CSCvd78303 が原因で、ASA は 213 日間の稼働時間後にトラフィックの受け渡しを停止する可能性があります。各ネットワークへの影響は異なりますが、制限された接続の問題から、停止などの広範なものへの影響が及ぶ可能性があります。可能な場合は、こうしたバグのない新しいバージョンにアップグレードする必要があります。それまでの間は、ASA を再起動することでさらに 213 日間稼働させることができます。別の回避策を利用できる場合もあります。影響を受けるバージョンおよび詳細については、Field Notice FN-64291 を参照してください。
- Asa 5506H-X の場合、ASA バージョン 9.5(2) にアップグレードすると、正しいライセンスレベルが適用されます。以前のバージョンの ASA では、ASA 5506-X 基本ライセンスと同じライセンスが適用されます。以前のバージョンでは、シスコに連絡して ASA 5506-X Security Plus ライセンスを受け取ることができます。これは、正しい ASA 5506H-X 基本ライセンスと同等です。または、単に 9.5(2) にアップグレードします。
- ユニファイドコミュニケーション電話プロキシと Intercompany Media Engine プロキシは非推奨：ASA バージョン 9.4 では、電話プロキシと IME プロキシはサポートされなくなりました。
- SSL/TLS の楕円曲線暗号化：楕円曲線対応 SSL VPN クライアントが ASA に接続すると、楕円曲線暗号スイートがネゴシエートされ、対応するインターフェイスが RSA ベースのトラストポイントで設定されている場合でも、ASA は、楕円曲線証明書を使用して SSL VPN クライアントを表示します。ASA が自己署名 SSL 証明書を提示しないようにするために、対応する暗号スイートを管理者が **ssl cipher** コマンドを使用して削除する必要があります。たとえば、RSA トラストポイントが設定されたインターフェイスの場合、管理者は次のコマンドを実行して、RSA ベースの暗号のみがネゴシエートされるようにできます。

```
ssl cipher tlsv1.2 custom
"AES256-SHA:AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA:DES-CBC3-SHA:
```

```
DES-CBC-SHA:RC4-SHA:RC4-MD5"
```

- 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 Java の要件

ASDM は、Oracle JRE 8.0を使用してインストールできます。 OpenJRE はサポートされていません。

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

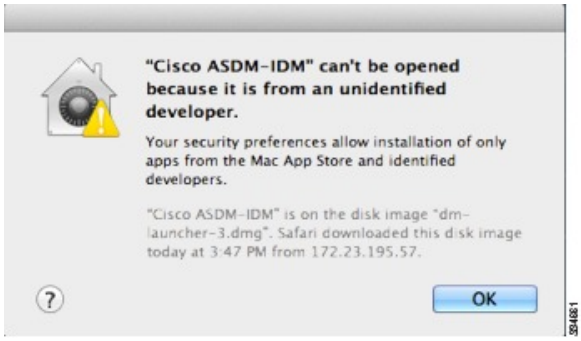
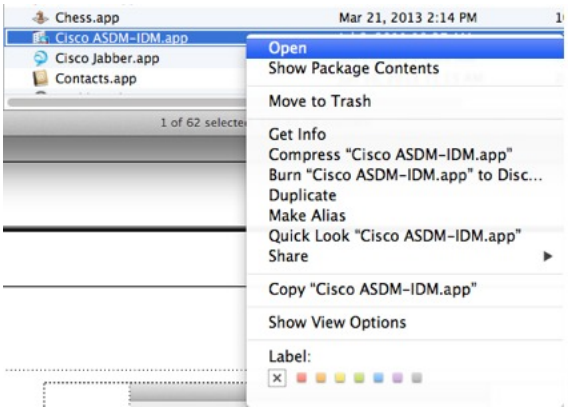
オペレーティングシステム	ブラウザ				Oracle JRE
	Internet Explorer	Firefox	Safari	Chrome	
Microsoft Windows（英語および日本語）： 8 7 Server 2012 Server 2008	対応	対応	サポートなし	対応	8.0
Apple OS X 10.4 以降	サポートなし	対応	対応	対応（64 ビットバージョンのみ）	8.0
Ubuntu Linux 14.04 Debian Linux 7	該当なし	対応	該当なし	対応	8.0

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
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有効）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無効にしてください。
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。

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
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。

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。

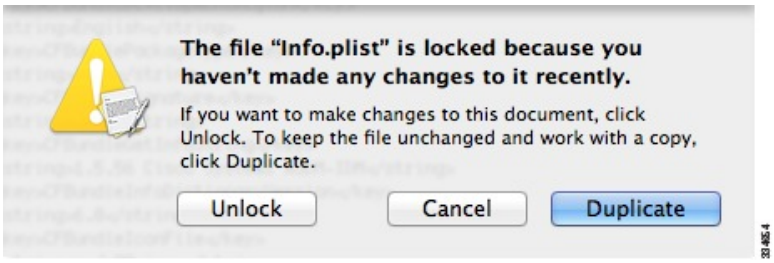
ステップ 3 **[Java]** > **[VMOptions]** で、「-Xmx」のプレフィックスが付いた文字列を変更し、必要なヒープサイズを指定します。たとえば、768 MB の場合は -Xmx768M に変更し、1 GB の場合は -Xmx1G に変更します。

```
<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 message guide』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 9.4(4.5)/ASDM 7.6(2) の新機能

リリース：2017年4月3日

（注） バージョン 9.4(4) は、バグ CSCvd78303 のため、Cisco.com から削除されました。

このリリースに新機能はありません。

ASA 9.4(3)/ASDM 7.6(1) の新機能

リリース：**2016年4月25日**

機能	説明
ファイアウォール機能	
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]**
リモートアクセス機能	
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。 次の画面が導入されました。**[Configuration]** > **[Device Management]** > **[Advanced]** > **[SSH Ciphers]** *9.1(7)* でも使用可能です。
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)* でも使用可能です。
モニタリング機能	
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。

機能	説明
show tech support の強化	**show tech support** コマンドは現在次のとおりです。 • **dir all-filesystems** の出力が含まれます。この出力は次の場合に役立つことがあります。 • SSL VPN コンフィギュレーション：必要なリソースが ASA にあるかどうかを確認します。 • クラッシュ：クラッシュファイルの日付のタイムスタンプと存在を確認します。 • **show kernel cgroup-controller detail** の出力の削除：このコマンド出力は **show tech-support detail** の出力内に残されます。 追加または変更された画面はありません。 *9.1(7)* でも使用可能です。
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)* でも使用可能です。

ASA 9.4(2.145)/ASDM 7.5(1) の新機能

リリース：2015年11月13日

このリリースに新機能はありません。

（注） このリリースは Firepower 9300 ASA セキュリティモジュールのみをサポートします。

ASA 9.4(2)/ASDM 7.5(1) の新機能

リリース：2015年9月24日

このリリースに新機能はありません。

（注） ASAv 9.4(1.200) の各機能はこのリリースには含まれません。

（注） このバージョンは ISA 3000 をサポートしません。

ASA 9.4(1.225)/ASDM 7.5(1) の新機能

リリース：**2015年9月17日**

（注） このリリースは Cisco ISA 3000 のみをサポートします。

機能	説明
プラットフォーム機能	
Cisco ISA 3000 サポート	Cisco ISA 3000 は、DIN レールにマウントされた高耐久型の産業用セキュリティアプライアンスです。ギガビットイーサネットと専用管理ポートを備えた、低消費電型ファンレスデバイスです。このモデルには ASA Firepower モジュールが事前にインストールされています。このモデルの特別な機能として、カスタマイズされたトランスペアレントモードのデフォルト設定と、電源喪失時もトラフィックがアプライアンスを通過することを可能にするハードウェアバイパス機能があります。 次の画面が導入されました。**[Configuration]** > **[Device Management]** > **[Hardware Bypass]** **hardware-bypass boot-delay** コマンドは ASDM 7.5(1) では使用できません。 この機能は、バージョン *9.5(1)* では使用できません。

ASA 9.4(1.152)/ASDM 7.4(3) の新機能

リリース：**2015年7月13日**

（注） このリリースは、Firepower 9300 の ASA のみをサポートします。

機能	説明
プラットフォーム機能	

機能	説明
Firepower 9300 の ASA セキュリティモジュール	Firepower 9300 の ASA セキュリティモジュールに ASA を導入しました。 （注） Firepower Chassis Manager 1.1.1 は Firepower 9300 の ASA セキュリティモジュールの VPN 機能（サイト間またはリモートアクセス）を一切サポートしません。
高可用性機能	
Firepower 9300用シャーシ内ASAクラスタリング	FirePOWER 9300 シャーシ内では、最大 3 つセキュリティモジュールをクラスタ化できます。シャーシ内のすべてのモジュールは、クラスタに属している必要があります。 次の画面を導入しました。**[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster Replication]**
ライセンシング機能	
Firepower 9300 の ASA のシスコ スマート ソフトウェア ライセンシング	FirePOWER 9300 に ASA のシスコ スマート ソフトウェア ライセンシングが導入されました。 次の画面が変更されました。**[Configuration] > [Device Management] > [Licensing] > [Smart License]**

ASAv 9.4(1.200)/ASDM 7.4(2) の新機能

リリース：**2015年5月12日**

（注） このリリースは、ASAv のみをサポートします。

機能	説明
プラットフォーム機能	
VMware 上の ASAv では vCenter サポートは不要になりました。	vCenter なしで、vSphere クライアントまたは OVFTool のデイゼロ設定を使用して ASAv を VMware 上にインストールできるようになりました。
Amazon Web Services（AWS）の ASAv	Amazon Web Services（AWS）とデイゼロ設定で ASAv を使用できるようになりました。 （注） Amazon Web Services は ASAv10 と ASAv30 のモデルのみをサポートします。

ASDM 7.4(2) の新機能

リリース：**2015年5月6日**

機能	説明
リモートアクセス機能	
AnyConnect バージョン 4.1 のサポート	ASDM は AnyConnect バージョン 4.1 をサポートするようになりました。 次の画面が変更されました。[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Client Profile]（[AMP Enabler Service Profile] という新しいプロファイル）

ASA 9.4(1)/ASDM 7.4(1) の新機能

リリース：**2015年3月30日**

機能	説明
プラットフォーム機能	
ASA 5506W-X、ASA 5506H-X、ASA 5508-X、ASA 5516-X	ワイヤレスアクセスポイントを内蔵した ASA 5506W-X、強化された ASA 5506H-X、ASA 5508-X、ASA 5516-X の各モデルが導入されました。 変更された ASDM 画面はありません。
認定機能	
国防総省（DoD）統一機能規則（UCR）2013 証明書	ASA は、DoD UCR 2013 規則を遵守するように更新されています。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。 • 定期的な証明書認証 • 証明書有効期限のアラート • 基本制約 CA フラグの適用 • 証明書コンフィギュレーションの ASDM ユーザ名 • ASDM 管理認証 • IKEv2 無効セレクタの通知設定 • 16 進数の IKEv2 事前共有キー

機能	説明
FIPS 140-2 認証のコンプライアンス更新	ASA で FIPS モードを有効にすると、ASA が FIPS 140-2 に準拠するように追加制限が設定されます。次の制限があります。 • RSA および DH キーサイズの制限：RSA および DH キー 2K（2048 ビット）以上のみが許可されます。DH の場合、これはグループ 1（768 ビット）、2（1024 ビット）、5（1536 ビット）が許可されないことを意味します。 （注） キーサイズの制限により、FIPS での IKEv1 の使用が無効になります。 • デジタル署名のハッシュアルゴリズムの制限：SHA 256 以上のみが許可されます。 • SSH 暗号の制限：許可された暗号は aes128-cbc または aes256-cbc です。MAC は SHA1 です。 ASA の FIPS 認証ステータスを表示するには、次の URL を参照してください。 http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140InProcess.pdf この PDF は毎週更新されます。 詳細については、Computer Security Division Computer Security Resource Center のサイトを参照してください。 http://csrc.nist.gov/groups/STM/cmvp/inprocess.html **fips enable** コマンドが変更されました。
ファイアウォール機能	
複数のコアを搭載した ASA での SIP インスペクションのパフォーマンスが向上。	複数のコアで ASA を通過する SIP シグナリングフローが複数存在する場合の SIP インスペクション パフォーマンスが向上しました。ただし、TLS、電話、または IME プロキシを使用する場合、パフォーマンスの向上は見られません。 変更された画面はありません。
電話プロキシおよび UC-IME プロキシに対する SIP インスペクションのサポートが削除されました。	SIP インスペクションを設定する際、電話プロキシまたは UC-IME プロキシは使用できなくなります。暗号化されたトラフィックを検査するには、TLS プロキシを使用します。 [Select SIP Inspect Map] サービス ポリシー ダイアログボックスから [Phone Proxy] と [UC-IME Proxy] が削除されました。
ISystemMapper UUID メッセージ RemoteGetClassObject opnum3 の DCERPC インスペクションのサポート。	ASA は、リリース 8.3 で EPM 以外の DCERPC メッセージのサポートを開始し、ISystemMapper UUID メッセージ RemoteCreateInstance opnum4 をサポートしています。この変更により、RemoteGetClassObject opnum3 メッセージまでサポートが拡張されます。 変更された画面はありません。

機能	説明
コンテキストごとに無制限の SNMP サーバトラップホスト	ASA では、コンテキストごとに SNMP サーバのトラップホスト数の制限がありません。**show snmp-server host** コマンドの出力には ASA をポーリングしているアクティブなホストと、静的に設定されたホストのみが表示されます。 変更された画面はありません。
VXLAN パケットインスペクション	ASA は、標準形式に準拠するために VXLAN ヘッダーを検査できます。 次の画面が変更されました。[Configuration] > [Firewall] > [Service Policy Rules] > [Add Service Policy Rule] > [Rule Actions] > [Protocol Inspection]
IPv6 の DHCP モニタリング	IPv6 の DHCP 統計情報および DHCP バインディングをモニタできます。 次の画面が導入されました。 [Monitoring] > [Interfaces] > [DHCP] > [IPV6 DHCP Statistics Monitoring] > [Interfaces] > [DHCP] > [IPV6 DHCP Binding]
ESMTP インスペクションの TLS セッションでのデフォルトの動作が変更されました。	ESMTP インスペクションのデフォルトが、検査されない、TLS セッションを許可するように変更されました。ただし、このデフォルトは新しい、または再イメージングされたシステムに適用されます。**no allow-tls** を含むシステムをアップグレードする場合、このコマンドは変更されません。 デフォルトの動作の変更は、古いバージョンでも行われました：8.4（7.25）、8.5（1.23）、8.6（1.16）、8.7（1.15）、9.0（4.28）、9.1（6.1）、9.2（3.2）、9.3（1.2）、9.3（2.2）。
高可用性機能	
スタンバイ ASA での syslog 生成のブロック	スタンバイ装置で特定の syslog の生成をブロックできます。 変更された画面はありません。
インターフェイスごとに ASA クラスタのヘルスモニタリングを有効または無効にする	ヘルスモニタリングは、インターフェイスごとに有効または無効にすることができます。デフォルトでは、ポートチャネル、冗長、および単一のすべての物理インターフェイスでヘルスモニタリングが有効になっています。ヘルスモニタリングは VLAN サブインターフェイス、または VNI や BVI などの仮想インターフェイスでは実行されません。クラスタ制御リンクのモニタリングは設定できません。このリンクは常にモニタされています。たとえば、管理インターフェイスなど、必須以外のインターフェイスのヘルスモニタリングを無効にすることができます。 次の画面が変更されました。[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Interface Health Monitoring]
DHCP リレーの ASA クラスタリングのサポート	ASA クラスタで DHCP リレーを設定できます。クライアントの DHCP 要求は、クライアントの MAC アドレスのハッシュを使用してクラスタメンバにロードバランスされます。DHCP クライアントおよびサーバ機能はサポートされていません。 変更された画面はありません。

機能	説明
ASA クラスタリングでの SIP インスペクションのサポート	ASA クラスタで SIP インスペクションを設定できます。制御フローは、任意のユニットで作成できますが（ロードバランシングのため）、その子データフローは同じユニットに存在する必要があります。TLS プロキシ設定はサポートされていません。 変更された画面はありません。
ルーティング機能	
Policy Based Routing：ポリシーベースルーティング	ポリシーベースルーティング（PBR）は、ACL を使用して指定された QoS でトラフィックが特定のパスを経由するために使用するメカニズムです。ACL では、パケットのレイヤ 3 および レイヤ 4 ヘッダーの内容に基づいてトラフィックを分類できます。このソリューションにより、管理者は区別されたトラフィックに QoS を提供し、低帯域幅、低コストの永続パス、高帯域幅、高コストのスイッチドパスの間でインタラクティブ トラフィックとバッチトラフィックを分散でき、インターネット サービス プロバイダーとその他の組織は明確に定義されたインターネット接続を介して一連のさまざまなユーザから送信されるトラフィックをルーティングできます。 次の画面が導入または変更されました。 **[Configuration] > [Device Setup] > [Routing] > [Route Maps] > [Policy Based Routing] [Configuration] > [Device Setup] > [Routing] > [Interface Settings] > [Interfaces]**
インターフェイス機能	
VXLAN のサポート	VXLAN のサポートが追加されました（VXLAN トンネルエンドポイント（VTEP）のサポートを含む）。ASA またはセキュリティコンテキストごとに 1 つの VTEP 送信元インターフェイスを定義できます。 次の画面が導入されました。 **[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add] > [VNI Interface] [Configuration] > [Device Setup] > [Interface Settings] > [VXLAN]**
モニタリング機能	
EEM のメモリトラッキング	メモリの割り当てとメモリの使用状況をログに記録してメモリロギングのラップイベントに応答するための新しいデバッグ機能が追加されました。 次の画面が変更されました。[Configuration] > [Device Management] > [Advanced] > [Embedded Event Manager] > [Add Event Manager Applet] > [Add Event Manager Applet Event]
トラブルシューティングのクラッシュ	**show tech-support** コマンドの出力と **show crashinfo** コマンドの出力には、生成された syslog の最新 50 行が含まれます。これらの結果を表示できるようにするには、**logging buffer** コマンドを有効にする必要があります。
リモートアクセス機能	

機能	説明
ECDHE-ECDSA 暗号のサポート	TLSv1.2 では、次の暗号のサポートが追加されています。 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • DHE-RSA-AES256-GCM-SHA384 • AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • DHE-RSA-AES128-GCM-SHA256 • RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 （注） 優先度が最も高いのは ECDSA 暗号および DHE 暗号です。 次の画面が変更されました。[Configuration] > [Remote Access VPN] > [Advanced] > [SSL Settings]。

機能	説明
クライアントレス SSL VPN セッション Cookie アクセスの制限	クライアントレス SSL VPN セッション Cookie が JavaScript などのクライアント側のスクリプトを介してサードパーティからアクセスされないようにすることができます。 （注） この機能は、Cisco TAC から使用を推奨された場合のみ使用してください。このコマンドをイネーブルにすると、次のクライアントレス SSL VPN 機能が警告なしで動作しなくなるため、セキュリティ上のリスクが発生します。 • Java プラグイン • Java リライタ • ポートフォワーディング。 • ファイルブラウザ • デスクトップ アプリケーション（Microsoft Office アプリケーションなど）を必要とする Sharepoint 機能 • AnyConnect Web 起動 • Citrix Receiver、XenDesktop、および Xenon • その他の非ブラウザ ベース アプリケーションおよびブラウザプラグインベースのアプリケーション 次の画面が変更されました。[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [HTTP Cookie]。 この機能は、*9.2(3)* にもあります。
セキュリティ グループ タギングを使用した仮想デスクトップのアクセス制御	ASA では、内部アプリケーションおよび Web サイトへのクライアントレス SSL リモートアクセス用にセキュリティ グループ タギングベースのポリシー制御をサポートしています。この機能では、配信コントローラおよび ASA のコンテンツ変換エンジンとして XenDesktop による Citrix の仮想デスクトップ インフラストラクチャ（VDI）を使用します。 詳細については、次の Citrix 製品のマニュアルを参照してください。 • XenDesktop および XenApp のポリシー：http://support.citrix.com/proddocs/topic/infocenter/ic-how-to-use.html • XenDesktop 7 でのポリシーの管理：http://support.citrix.com/proddocs/topic/xendesktop-7/cds-policies-wrapper-rho.html • XenDesktop 7 のポリシー用のグループポリシーエディタの使用：http://support.citrix.com/proddocs/topic/xendesktop-7/cds-policies-use-gpmc.html

機能	説明
クライアントレスSSL VPN に OWA 2013 機能のサポートを追加	クライアントレス SSL VPN では、以下を除き、OWA 2013 の新機能をサポートしています。 • タブレットおよびスマートフォンのサポート • オフラインモード • Active Directory Federation Services（AD FS）2.0. ASA および AD FS 2.0 は、暗号化プロトコルをネゴシエートできません。 変更された画面はありません。
クライアントレスSSL VPN に Citrix XenDesktop 7.5 および StoreFront 2.5 のサポートを追加	クライアントレス SSL VPN では、XenDesktop 7.5 および StoreFront 2.5 のアクセスをサポートしています。 XenDesktop 7.5 の機能の完全なリストと詳細については、http://support.citrix.com/proddocs/topic/xenapp-xendesktop-75/cds-75-about-whats-new.html を参照してください。 StoreFront 2.5 の機能の完全なリストと詳細については、http://support.citrix.com/proddocs/topic/dws-storefront-25/dws-about.html を参照してください。 変更された画面はありません。
定期的な証明書認証	定期的な証明書認証を有効にすると、ASA は、VPN クライアントから受信した証明書チェーンを保存し、それらを定期的に再認証します。 次の画面が変更されました。 **[Configuration] > [Device Management] > [Certificate Management] > [Identity Certificates] [Configuration] > [Device Management] > [Certificate Management] > [CA Certificates]**
証明書有効期限のアラート	ASA は、トラストポイントですべての CA および ID の証明書の有効期限について 24 時間ごとにチェックします。証明書の有効期限がまもなく切れる場合は、syslog がアラートとして発行されます。リマインダおよび繰り返しの間隔を設定できます。デフォルトでは、リマインダは有効期限の 60 日前に開始し、7 日ごとに繰り返されます。 次の画面が変更されました。 **[Configuration] > [Device Management] > [Certificate Management] > [Identity Certificates] [Configuration] > [Device Management] > [Certificate Management] > [CA Certificates]**

機能	説明
基本制約 CA フラグの適用	デフォルトでは、CA フラグのない証明書を CA 証明書として ASA にインストールできなくなりました。基本制約拡張は、証明書のサブジェクトが CA で、この証明書を含む有効な認証パスの最大深さかどうかを示すものです。必要に応じて、これらの証明書のインストールを許可するように ASA を設定できます。 次の画面が変更されました。[Configuration] > [Device Management] > [Certificate Management] > [CA Certificates]
IKEv2 無効セレクタの通知設定	現在、ASA が SA 上で着信パケットを受信し、そのパケットのヘッダーフィールドが SA 用のセレクタに適合しなかった場合、ASA はそのパケットを廃棄します。ピアへの IKEv2 通知の送信を有効または無効にすることができます。この通知の送信はデフォルトで無効になっています。 （注） この機能は、AnyConnect 3.1.06060 以降でサポートされています。
16 進数の IKEv2 事前共有キー	16 進数の IKEv2 事前共有キーを設定できます。
管理機能	
ASDM 管理認証	HTTP アクセスと Telnet および SSH アクセス別に管理認証を設定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] > [Users/AAA] > [AAA Access] > [Authorization]**
証明書コンフィギュレーションの ASDM ユーザ名	ASDM の証明書認証を有効にすると、ASDM が証明書からユーザ名を抽出する方法を設定できます。また、ログインプロンプトでユーザ名を事前に入力して表示できます。 次の画面が導入されました。**[Configuration] > [Device Management] > [Management Access] > [HTTP Certificate Rule]**
CLI で **?** の入力時にヘルプを有効または無効にするための **terminal interactive** コマンド	通常、ASA CLI で **?** を入力すると、コマンドヘルプが表示されます。コマンド内にテキストとして **?** を入力できるようにするには（たとえば、URL の一部として ? を含めるには）、**no terminal interactive** コマンドを使用してインタラクティブなヘルプを無効にします。 次のコマンドが導入されました。terminal interactive
REST API の機能	
REST API バージョン 1.1	REST API バージョン 1.1 のサポートが追加されました。
トークンベース認証が（既存の基本認証に加えて）サポートされるようになりました。	クライアントは特定の URL にログイン要求を送信でき、成功すると、（応答ヘッダーに）トークンが返されます。クライアントはさらなる API コールを送信するために、（特別な要求ヘッダー内で）このトークンを使用します。トークンは明示的に無効にするまで、またはアイドル/セッション タイムアウトに到達するまで有効です。

機能	説明
マルチコンテキストモードの限定的なサポート	REST API エージェントをマルチコンテキストモードで有効にできるようになりました。CLI コマンドはシステムコンテキストモードでのみ発行できます（シングルコンテキストモードと同じコマンド）。 次のようにパススルー CLI の API コマンドを使用して、コンテキストを設定できます。 `https://<asa_admin_context_ip>/api/cli?context=<context_name>` **context** パラメータがない場合、要求は **admin** コンテキストに向けられたものとみなされます。
高度な（粒状の）インスペクション	次のプロトコルの詳細なインスペクションをサポートします。 • DNS over UDP • HTTP • ICMP • ICMP ERROR • RTSP • SIP • FTP • DCERPC • IP オプション • NetBIOS Name Server over IP • SQL*Net

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。

- CLI：**show version** コマンドを使用します。
- ASDM：**[Home**）**]** > **[Device Dashboard]** > **[Device Information]** の順に選択します。

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、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。

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。 → 9.4(x) → 9.3(x)
9.2(x)	—	次のいずれかになります。 → 9.4(x) → 9.3(x) → 9.2(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。 → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3)、9.1(4)、9.1(5)、9.1(6)、9.1(7.4)
9.1(1)	→ 9.1(2)	次のいずれかになります。 → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3)、9.1(4)、9.1(5)、9.1(6)、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。 → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3)、9.1(4)、9.1(5)、9.1(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(2)、9.0(3) または 9.0(4)	次のいずれかになります。 → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3)、9.1(4)、9.1(5)、9.1(6)、9.1(7.4)
8.6(1)	→ 9.0(2)、9.0(3) または 9.0(4)	次のいずれかになります。 → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3)、9.1(4)、9.1(5)、9.1(6)、9.1(7.4)
8.5(1)	→ 9.0(2)、9.0(3) または 9.0(4)	次のいずれかになります。 → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3)、9.1(4)、9.1(5)、9.1(6)、9.1(7.4)
8.4(5+)	—	次のいずれかになります。 → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3)、9.1(4)、9.1(5)、9.1(6)、9.1(7.4)
8.4(1) ～ 8.4(4)	次のいずれかになります。 → 9.0(2)、9.0(3) または 9.0(4) → 8.4(6)	→ 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3)、9.1(4)、9.1(5)、9.1(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
8.3(x)	→ 8.4(6)	次のいずれかになります。 → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3)、9.1(4)、9.1(5)、9.1(6)、9.1(7.4)
8.2(x) 以前	→ 8.4(6)	次のいずれかになります。 → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3)、9.1(4)、9.1(5)、9.1(6)、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 Upgrade Guide』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 7.4(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 7.4(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。

- 7.4(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
CSCuz92899	プリログインポリシーの変更が保存されない

バージョン 7.4(2) で未解決のバグ

バージョン 7.4 (2) で未解決のバグはありません。

バージョン 7.4(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 7.4(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。

- 7.4(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
CSCuz92899	プリログインポリシーの変更が保存されない

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 7.4(3) 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：

- 7.4(3) 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
CSCut74372	asdm：コア使用率の出力によりホームページのロードで問題が発生
CSCuu29995	DOC：ASDM：「DM_INLINE_NETWORK」がオブジェクトグループのデフォルト名

バージョン 7.4(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：

- 7.4(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。

ID	説明
CSCut49785	ASDM 7.4.X が「software update completed」でスタックする
CSCut50204	ASDM：ssl コマンド解析時の NPE
CSCut57751	実行コンフィギュレーションの検証中に ASDM 7.4.1 が87% でハングする

バージョン 7.4(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：

- 7.4(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
CSCup27452	CX がインストールされた ASA を ASDM が永続的にポーリング
CSCuq59377	ASDM：ボットネット トラフィック フィルタが ASDM 7.3 のリアルタイム レポートで機能しない
CSCur16710	VXLAN：nve のみの送信中にインターフェイス cli が欠落している
CSCur21416	フェールオーバーパネルでヌルポインタ例外がスローされた
CSCur23947	ASDM 7.3.2 で DAP の「Endpoint Attribute Type: Policy」が表示されない
CSCur45190	ASDM：IPv6 DHCP リレーパネルが欠落している
CSCur60489	usage-keys により ASDM Identity Certificate Wizard でエラー
CSCur90915	ASDM DAP：エンドポイント OS 属性リストに Windows 10 を追加する必要がある
CSCur96423	SFR モジュールを使用する ASA のサブインターフェイスを ASDM が追加できない
CSCus05440	ASDM：特定のオブジェクト名を使用して正しい NAT ルールを表示できない

ID	説明
CSCus11684	HPM を有効にすると ASDM が応答しなくなる
CSCus14883	FirePOWER モジュールのステータスを ASDM が継続的にポーリング
CSCus26083	Syslog サーバテーブルで tcp プロトコルが udp として表示される（逆も同様）
CSCus30737	hpm topN が有効にされていると ASDM 7.3.2 が遅くなる
CSCus54556	「All Remote Access」フィルタをロードすると ASDM 7.3.2 がハングする
CSCus56092	5506、5508、および 5516 の最大 TLS セッション値の追加
CSCus86770	ASDM による ACL の破損でトラフィック障害が発生
CSCus87127	Transparent FW に名前付き int の数を 32 を超えて作成すると ASDM でエラーが表示される
CSCut04386	トラフィックキャプチャウィザード：入力用に作成された ACL が出力用に表示されない
CSCut04499	トラフィックキャプチャウィザード：一致条件の変更でインターフェイスがリセット

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。

【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。