Cisco ASDM 7.7(x) リリースノート

初版：2017 年 1 月 23 日

最終更新：2017 年 3 月 9 日

Cisco ASDM 7.7(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 7.7(x) のリリース情報が記載されています。

特記事項

- AnyConnect 4.4 または 4.5 で SAML 認証を使用しており、ASA バージョン 9.7.1.24、9.8.2.28、または 9.9.2.1（リリース日：2018 年 4 月 18 日）を展開している場合、SAML のデフォルト動作は、AnyConnect 4.4 および 4.5 でサポートされていない組み込みブラウザになります。したがって、AnyConnect 4.4 および 4.5 クライアントが外部（ネイティブ）ブラウザを使用して、SAML で認証するには、トンネル グループ設定で **saml external-browser** コマンドを使用する必要があります。

  （注） **saml external-browser** コマンドは、AnyConnect 4.6 以降にアップグレードするクライアントの移行のために使用されます。セキュリティ上の制限のため、AnyConnect ソフトウェアをアップグレードする際の一時的な移行の一環としてのみこのソリューションを使用してください。今後、このコマンド自体がサポートされなくなります。

- 潜在的なトラフィック停止（9.7(1) ～ 9.7(1.2)）：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を渡すこと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。

- 拡張/ストレス環境で AnyConnect リモートアクセス VPN IPv6 DTLS トンネルを使用すると、ASA がトレースバックする可能性があります（たとえば、多数のトンネルがある場合や、トンネルが ASA ヘッドエンドから継続的に接続および切断される場合）。**回避策**：IPv6 AnyConnect IKEv2 または IPv4 AnyConnect DTLS VPN リモート アクセス セッション タイプを使用します。（CSCvc77123）

- 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。

- ASA が TLS プロキシ設定で TLS サーバとして機能する場合、クライアントが TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 暗号または TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 暗号を提示し、それらの暗号が選択されると、TLS ハンドシェイクが失敗する可能性があります。このリリースでは、ASA がサーバとして機能している場合、暗号の選択を制御できません。グローバル **ssl encryption** コマンドがデフォルトの暗号セットとして有効にならないというバグがあるためです。9.8(1) では、TLS プロキシ設定で新しい **server cipher-suite** コマンドを使用して暗号を制御できます。この問題が発生した場合は、9.8(1) にアップグレードしてください。または、クライアントの設定を変更して、前述の暗号が提示されないようにすることもできます。

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。

（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

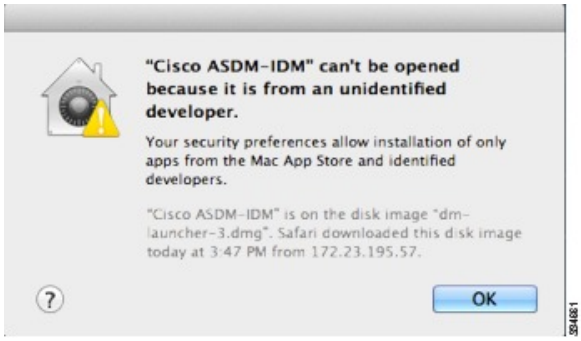
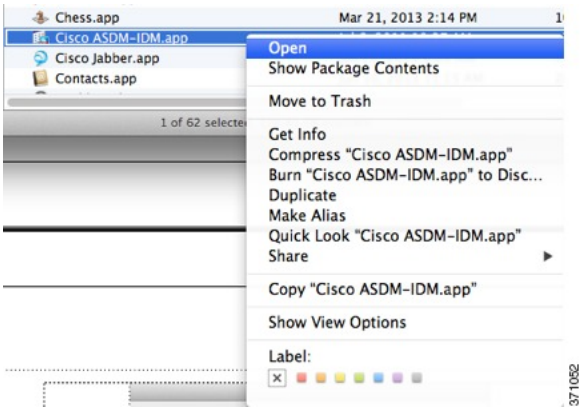
オペレーティング システム	ブラウザ				Oracle JRE
	Internet Explorer	Firefox	Safari	Chrome	
Microsoft Windows（英語および日本語）： 10 8 7 Server 2012 R2 Server 2012 Server 2008	対応	対応	サポートなし	対応	8.0
Apple OS X 10.4 以降	サポートなし	対応	対応	対応（64 ビット バージョンのみ）	8.0

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。

条件	注意
• 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。
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。

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。

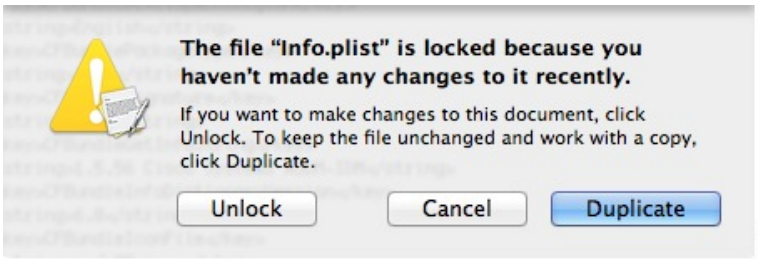
ステップ 3 **[Java]** > **[VMOptions]** で、「-Xmx」のプレフィックスが付いた文字列を変更し、必要なヒープ サイズを指定します。たとえば、768 MB の場合は -Xmx768M に変更し、1 GB の場合は -Xmx1G に変更します。

```
<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 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 7.7(1.151) の新機能

リリース：2017年4月28日

（注） ASDM 7.7(1.150) は、バグ CSCvd90344 に基づき Cisco.com から削除されました。

機能	説明
管理機能	

機能	説明
ASDM アップグレード ツールの新しいバックグラウンド サービス	ASDM は、[Tools] > [Check for ASA/ASDM Upgrades] の新しいバックグラウンド サービスです。Cisco は、前のバージョンの ASDM で使用されていた古いサービスを将来廃止する予定です。

ASA 9.7(1.4)/ASDM 7.7(1) の新機能

リリース：**2017年4月4日**

（注） バージョン 9.7(1) は、バグ CSCvd78303 に基づき Cisco.com から削除されました。

機能	説明
プラットフォーム機能	

機能	説明
Integrated Routing and Bridging（IRB; 統合ルーティングおよびブリッジング）を使用した ASA 5506-X シリーズ用の新しいデフォルト設定	新しいデフォルト設定が ASA 5506-X シリーズに使用されます。統合ブリッジングおよびルーティング機能は、外部レイヤ 2 スイッチの使用に代わる手段を提供します。ハードウェア スイッチを含む ASA 5505 を交換するユーザの場合、この機能を使用することにより、追加のハードウェア使用せずに ASA 5505 を ASA 5506-X やその他の ASA モデルに置き換えることができます。 新しいデフォルト設定には次の内容が含まれます。 • GigabitEthernet 1/1、DHCP からの IP アドレスの外部インターフェイス • GigabitEthernet ½（inside1）から 1/8（inside7）、IP アドレス 192.168.1.1 が指定された内部ブリッジグループ BVI 1 • 内部 --> 外部へのトラフィック フロー • 内部 --> メンバー インターフェイス用内部トラフィック フロー • （ASA 5506W-X）GigabitEthernet 1/9、IP アドレス 192.168.10.1 の Wi-Fi インターフェイス • （ASA 5506W-X） WiFi<--> 内部のトラフィック フロー、WiFi --> 外部へのトラフィック フロー • 内部および WiFi 上のクライアントに対する DHCP。アクセス ポイント自体とそのすべてのクライアントが ASA を DHCP サーバとして使用します。 • 管理 1/1 インターフェイスが稼働しているが、そうでない場合は未設定。ASA FirePOWER モジュールは、このインターフェイスを使用して ASA 内部ネットワークに接続し、内部インターフェイスをインターネットへのゲートウェイとして使用できます。 • ASDM アクセス：内部ホストと Wi-Fi ホストが許可されます。 • NAT：内部、WiFi、および管理から外部へのすべてのトラフィックのインターフェイス PAT。 アップグレードする場合、**configure factory-default** コマンドを使用して設定を消去しデフォルトを適用するか、必要に応じて BVI とブリッジ グループのメンバーを手動で設定することができます。内部ブリッジグループの通信を簡単に許可するには、**same-security-traffic permit inter-interface** コマンドを有効にする必要があります（このコマンドは、ASA 5506W-X のデフォルト設定にすでに存在します）。

機能	説明
ISA 3000 でのアラーム ポートのサポート	ISA 3000 は、2 つのアラーム入力インターフェイスと 1 つのアラーム出力インターフェイスをサポートします。ドア センサーなどの外部センサーは、アラーム入力に接続できます。ブザーなどの外部デバイスは、アラーム出力インターフェイスに接続できます。トリガーされたアラームは、2 つの LED、syslog、SNMP トラップを経由し、アラーム出力インターフェイスに接続されたデバイスを介して伝えられます。ユーザは、外部アラームの説明を設定できます。また、外部アラームと内部アラームの重大度とトリガーも指定できます。すべてのアラームは、リレー、モニタリング、およびロギングに設定できます。 次の画面が導入されました。 **[Configuration] > [Device Management] > [Alarm Port] > [Alarm Contact]** **[Configuration] > [Device Management] > [Alarm Port] > [Redundant Power Supply]** **[Configuration] > [Device Management] > [Alarm Port] > [Temperature]** **[Monitoring] > [Properties] > [Alarm] > [Alarm Settings]** **[Monitoring] > [Properties] > [Alarm] > [Alarm Contact]** **[Monitoring] > [Properties] > [Alarm] > [Facility Alarm Status]**
ASAv10 での Microsoft Azure Security Center のサポート	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。Microsoft Azure Security Center は、非常にセキュアなパブリック クラウドインフラストラクチャの導入を簡素化する、Azure 上の Microsoft オーケストレーションおよび管理レイヤです。ASAv を Azure Security Center に統合することにより、Azure 環境を保護するファイアウォール オプションとして ASAv を提供できます。

ISA 3000 用の Precision Time Protocol（PTP）	ISA 3000 は PTP（ネットワークに分散したノードの時刻同期プロトコル）をサポートします。PTP は、そのハードウェア タイムスタンプ機能により、NTP などの他の時刻同期プロトコルより高い精度を実現します。ISA 3000 は、ワンステップのエンドツーエンド トランスペアレント クロックに加えて、PTP 転送モードもサポートします。インスペクションのために PTP トラフィックが ASA FirePOWER モジュールに送信されることのないようにするため、デフォルト設定に次のコマンドが追加されました。既存の導入がある場合は、次のコマンドを手動で追加する必要があります。
	
	`object-group service bypass_sfr_inspect`
	`  service-object udp destination range 319 320`
	`access-list sfrAccessList extended deny object-group bypass_sfr_inspect any any`
	
	次の画面が導入されました。
	
	[Configuration] > [Device Management] > [PTP]
	
	[Monitoring] > [Properties] > [PTP]

機能	説明
ISA 3000 の自動バックアップと復元	バックアップ コマンドと復元コマンドのプリセット パラメータを使用して、自動バックアップ機能や自動復元機能を有効にできます。これらの機能は、外部メディアからの初期設定、デバイス交換、作動可能状態へのロールバックなどで使用されます。 次の画面が導入されました。**[Configuration]** > **[Device Management]** > **[Auto Backup & Restore Configuration]**
ファイアウォール機能	
SCTPマルチストリーミングの並べ替えとリアセンブル、およびフラグメンテーションのサポート。SCTPエンドポイントに複数のIPアドレスが設定されたSCTPマルチホーミングのサポート。	このシステムは、SCTP マルチストリーミングの並べ替え、リアセンブル、およびフラグメンテーションを完全にサポートしており、これにより SCTP トラフィックに対する Diameter および M3UA インスペクションの有効性が改善されています。このシステムは、各エンドポイントに複数の IP アドレスが設定された SCTP マルチホーミングもサポートしています。マルチホーミングでは、セカンデリ アドレスに必要なピンホールをシステムが開くので、セカンデリ アドレスを許可するためのアクセス ルールをユーザが設定する必要はありません。SCTP エンドポイントは、それぞれ 3 つの IP アドレスに制限する必要があります。 変更された画面はありません。
M3UAインスペクションの改善。	M3UAインスペクションは、ステートフル フェールオーバー、半分散クラスタリング、およびマルチホーミングをサポートするようになりました。また、アプリケーション サーバ プロセス（ASP）の状態の厳密な検証や、さまざまなメッセージの検証も設定できます。ASP状態の厳密な検証は、ステートフル フェールオーバーとクラスタリングに必要です。 次の画面が変更されました。**[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspection Maps]** > **[M3UA]** [Add/Edit] ダイアログボックス。
TLSプロキシでのTLSv1.2、およびCisco Unified Communications Manager 10.5.2 のサポート。	暗号化 SIP 用の TLS プロキシでの TLSv1.2、または Cisco Unified Communications Manager 10.5.2 での SCCP インスペクションを使用できるようになりました。TLS プロキシは、**client cipher-suite** コマンドの一部として追加されたTLSv1.2暗号スイートをサポートします。 変更された画面はありません。

機能	説明
Integrated Routing and Bridging（IRB）	Integrated Routing and Bridging（統合ルーティングおよびブリッジング）は、ブリッジグループとルーテッド インターフェイス間をルーティングする機能を提供します。ブリッジグループとは、ASA がルートの代わりにブリッジするインターフェイスのグループのことです。ASA は、ASA がファイアウォールとして機能し続ける点で本来のブリッジとは異なります。つまり、インターフェイス間のアクセス制御が実行され、通常のファイアウォール検査もすべて実行されます。以前は、トランスペアレント ファイアウォール モードでのみブリッジグループの設定が可能だったため、ブリッジグループ間でのルーティングはできませんでした。この機能を使用すると、ルーテッド ファイアウォール モードのブリッジ グループの設定と、ブリッジグループ間およびブリッジグループとルーテッドインターフェイス間のルーティングを実行できます。ブリッジ グループは、ブリッジ仮想インターフェイス（BVI）を使用して、ブリッジ グループのゲートウェイとして機能することによってルーティングに参加します。そのブリッジグループに指定する ASA 上に別のインターフェイスが存在する場合、Integrated Routing and Bridging（IRB）は外部レイヤ 2 スイッチの使用に代わる手段を提供します。ルーテッド モードでは、BVI は名前付きインターフェイスとなり、アクセス ルールや DHCP サーバなどの一部の機能に、メンバー インターフェイスとは個別に参加できます。 トランスペアレント モードでサポートされるマルチ コンテキスト モードや ASA クラスタリングの各機能は、ルーテッド モードではサポートされません。マルチキャスト ルーティングとダイナミック ルーティングの機能も、BVI ではサポートされません。 次の画面が変更されました。 **[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces]** **[Configuration] > [Device Setup] > [Routing] > [Static Routes]** **[Configuration] > [Device Management] > [DHCP] > [DHCP Server]** **[Configuration] > [Firewall] > [Access Rules]** **[Configuration] > [Firewall] > [EtherType Rules]**
VM 属性	ネットワーク オブジェクトを定義することにより、VMware vCenter で管理している VMware ESXi 環境の 1 つ以上の仮想マシン（VM）に関連付けられている属性に従ってトラフィックをフィルタリングできます。アクセス コントロール リスト（ACL）を定義して、1 つ以上の属性を共有する VM のグループからのトラフィックにポリシーを指定することができます。 次の画面が追加されました。 **[Configuration] > [Firewall] > [VM Atttribute Agent]**
内部ゲートウェイ プロトコルの古いルートのタイムアウト	OSPF などの内部ゲートウェイ プロトコルの古いルートを削除するためのタイムアウトを設定できるようになりました。 **[Configuration] > [Firewall] > [Advanced] > [Global Timeouts]** の画面が変更されました。

機能	説明
オブジェクト グループ検索に関するネットワーク オブジェクトの制限。	**object-group-search access-control** コマンドを使用してオブジェクト グループ検索を有効にすることで、アクセス ルールの検索に必要なメモリを抑えることができます。オブジェクト グループ検索を有効にした場合、ネットワーク オブジェクトまたはサービス オブジェクトは拡張されませんが、それらのグループの定義に基づいて一致するアクセス ルールが検索されます。 このリリース以降、以下の制限が適用されます。接続ごとに、送信元と宛先の両方の IP アドレスがネットワーク オブジェクトと照合されます。発信元アドレスに一致するオブジェクトの数が、宛先アドレスと一致する数の 1 万倍を超えると接続が切断されます。 このチェックは、パフォーマンスの低下を防止します。一致件数が膨大になることを防ぐためにルールを設定します。
ルーティング機能	
31 ビット サブネットマスク	ルーテッドインターフェイスに関しては、ポイントツーポイント接続向けの31 ビットのサブネットに IP アドレスを設定できます。31 ビット サブネットには 2 つのアドレスのみが含まれます。通常、サブネットの最初と最後のアドレスはネットワーク用とブロードキャスト用に予約されており、2 アドレス サブネットは使用できません。ただし、ポイントツーポイント接続があり、ネットワーク アドレスやブロードキャスト アドレスが不要な場合は、IPv4 形式でアドレスを保持するのに 31 サブネット ビットが役立ちます。たとえば、2 つの ASA 間のフェールオーバー リンクに必要なアドレスは 2 つだけです。リンクの一方の側から送信されるパケットはすべてもう一方の側で受信され、ブロードキャスティングは必要ありません。また、SNMP や Syslog を実行する管理ステーションを直接接続することもできます。この機能は、ブリッジグループまたはマルチキャスト ルーティング用の BVI ではサポートされていません。 次の画面が変更されました。 **[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add Interface] > [General]**
ハイ アベイラビリティとスケーラビリティの各機能	
Firepower 4100/9300 シャーシ 上の ASA のサイト間クラスタリングの改善	ASA クラスタを展開すると、それぞれの Firepower 4100/9300 シャーシのサイト ID を設定できます。以前は ASA アプリケーション内でサイト ID を設定する必要がありました。この新しい機能は、初期導入を簡単にします。ASA 構成内でサイト ID を設定できなくなったことに注意してください。また、サイト間クラスタリングとの互換性を高めるために、安定性とパフォーマンスに関する複数の改善が含まれる ASA 9.7(1) および FXOS 2.1.1 にアップグレードすることを推奨します。 次の画面が変更されました。**[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Configuration]**

機能	説明
ディレクタ ローカリゼーション：データセンターのサイト間クラスタリングの改善	データ センターのパフォーマンスを向上し、サイト間クラスタリングのトラフィックを維持するために、ディレクタ ローカリゼーションを有効にできます。通常、新しい接続は特定のサイト内のクラスタ メンバーによってロード バランスされ、所有されています。しかし、ASA は任意のサイトのメンバーにディレクタ ロールを割り当てます。ディレクタ ローカリゼーションにより、所有者と同じサイトのローカル ディレクタ、どのサイトにも存在可能なグローバル ディレクタという追加のディレクタ ロールが有効になります。所有者とディレクタが同一サイトに存在すると、パフォーマンスが向上します。また、元の所有者が失敗した場合、ローカルなディレクタは同じサイトで新しい接続の所有者を選択します。グローバルなディレクタは、クラスタ メンバーが別のサイトで所有される接続のパケットを受信する場合に使用されます。 次の画面を変更しました。**[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Configuration]**
高速検出の設定が可能な、フェールオーバーのポーリングをモニタリングするインターフェイス リンク ステート	デフォルトでは、フェールオーバー ペアの ASA は、500 ミリ秒ごとにインターフェイスのリンク ステートをチェックします。ポーリングの間隔を 300 ミリ秒から 799 ミリ秒の間で設定できるようになりました。たとえば、ポーリング時間を 300 ミリ秒に設定すると、ASA はインターフェイス障害やトリガーのフェールオーバーをより迅速に検出できます。 次の画面が変更されました。**[Configuration] > [Device Management] > [High Availability and Scalability] > [Failover] > [Criteria]**
FirePOWER 9300 および 4100 でのアクティブ/スタンバイ フェールオーバー ヘルス モニタリングで、双方向フォワーディング検出（BFD）がサポートされました。	FirePOWER 9300 および 4100 上のアクティブ/スタンバイ ペアの 2 つのユニット間のフェールオーバー ヘルス チェックに対して、双方向フォワーディング検出（BFD）を有効にできるようになりました。ヘルス チェックに BFD を使用すると、デフォルトのヘルスチェックより信頼性が高まり、CPU の使用を抑えることができます。 次の画面が変更されました。**[Configuration] > [Device Management] > [High Availability and Scalability] > [Failover] > [Setup]**
VPN 機能	
IKEv2 静的暗号マップ用ダイナミック RRI	**crypto map** に **dynamic** が指定されている場合、IPSec セキュリティ アソシエーション（SA）の確立に成功すると、ダイナミック リバース ルート インジェクションが発生します。ルートは、ネゴシエートされたセレクタの情報に基づいて追加されます。IPsec SA's が削除されると、このルートは削除されます。ダイナミック RRI は、IKEv2 ベースの静的暗号マップでのみサポートされます。 次の画面が変更されました。[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [IPsec] > [Crypto Maps] > [Add/Edit] > [Tunnel Policy (Crypto Maps) - Advanced]

機能	説明
ASA VPN モジュールの仮想トンネル インターフェイス（VTI）のサポート	ASA VPN モジュールが、仮想トンネル インターフェイス（VTI）と呼ばれる新しい論理インターフェイスによって強化されており、ピアへの VPN トンネルを表すために使用されます。これは、トンネルの各終端に接続されている IPsec プロファイルを利用したルートベースの VPN をサポートします。VTI を使用することにより、静的暗号マップのアクセスリストを設定してインターフェイスにマッピングすることが不要になります。 次の画面が導入されました。 **[Configuration] > [Site-to-Site VPN] > [Advanced] > [IPsec Proposals (Transform Sets)] > [IPsec Profile]** **[Configuration] > [Site-to-Site VPN] > [Advanced] > [IPsec Proposals (Transform Sets)] > [IPsec Profile] > [Add] > [Add IPsec Profile]** **[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add] > [VTI Interface]** **[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add] > [VTI Interface] > [General]** **[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add] > [VTI Interface] > [Advanced]**
AnyConnect 用 SAML 2.0 ベースの SSO	SAML 2.0 ベースのサービス プロバイダー IdP が、プライベート ネットワークでサポートされます。ユーザとサービス間のゲートウェイとして ASA を使用すると、IdP の認証は制限付きの名前非表示 webvpn セッションで処理され、IdP とユーザ間のすべてのトラフィックは変換されます。 次の画面が変更されました。**[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [Single Sign On Servers] > [Add SSO Server]**.
CMPv2	ワイヤレス LTE ネットワークのセキュリティ ゲートウェイ デバイスとして配置できるように、ASA が証明書の管理プロトコル（CMPv2）を使用した特定の管理機能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] > [Certificate Management] > [Identity Certificates] > [Add an Identity Certificate]**
マルチ証明書認証	AnyConnect SSL クライアント プロトコルと IKEv2 クライアント プロトコルを使用して、セッションごとに複数の認証を検証できるようになりました。マルチ証明書認証のプロトコル交換を定義し、これを両方のセッション タイプで利用できるように、集約認証プロトコルが拡張されました。 次の画面が変更されました。 **[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Dynamic Access Policies] > [Edit AnyConnect Connection Profile]** **[Configuration] > [Remote Access VPN] > [Network Client Access] > [AnyConnect Connection Profiles] > [Edit AnyConnect Connection Profiles]**

機能	説明
スプリット トンネリング ルーティングの制限の引き上げ	AC-SSL および AC-IKEv2 のスプリット トンネリング ルートの制限は、200 から 1200 に引き上げられました。IKEv1 の制限は 200 で変わりません。
Chrome のスマート トンネル サポート	Mac デバイスや Windows デバイスの Chrome ブラウザでスマート トンネルをサポートするための新しいメソッドが作成されました。Chrome Smart Tunnel Extension は、Netscape プラグイン アプリケーション プログラム インターフェイス（NPAPI）に代わるものです。NPAPI は、Chrome ではサポートされなくなりました。この拡張プログラムをインストールしていない Chrome でスマート トンネルに対応したブックマークをクリックすると、ユーザは拡張プログラムを取得できるように Chrome ウェブストアにリダイレクトされます。Chrome を新規インストールする場合、ユーザは拡張プログラムを取得できるように Chrome ウェブストアに移動されます。この拡張プログラムは、スマート トンネルの実行に必要なバイナリを ASA からダウンロードします。通常のブックマーク、およびスマートトンネルを使用する際のアプリケーション設定は、この新しい拡張プログラムのインストールプロセス以外は変更されません。
クライアントレス SSL VPN：すべての Web インターフェイスのセッション情報	すべての Web インターフェイスが、ログインに使用されたユーザ名などの現在のセッションの詳細と、現在割り当てられているユーザ権限を表示するようになりました。これは、ユーザが現在のユーザセッションを知るのに役立ち、ユーザ セキュリティの向上につながります。
クライアントレス SSL VPN：Web アプリケーション セッションのクッキーすべての検証	すべての Web アプリケーションは、セキュリティ関連のクッキーすべてを検証してはじめて、アクセス権を付与するようになります。要求があるごとに、認証トークンまたはセッション ID を持つ各クッキーが検証され、その後にユーザ セッションへのアクセスが付与されます。同じ要求に複数のセッション Cookie が含まれている場合、その接続は破棄されます。検証に失敗したクッキーは無効なクッキーとして扱われ、そのイベントは監査ログに追加されます。
AnyConnect：最大接続時間アラート間隔が、AnyConnect VPN Client の接続に関するグループ ポリシーでサポートされるようになりました。	このアラート間隔は、最大接続時間に達する前に、終了を警告するメッセージをユーザに表示する間隔を指定します。有効な時間間隔は 1 ～ 30 分です。デフォルトは 30 分です。以前は、クライアントレス接続とサイト間 VPN 接続でサポートされていました。 次の画面が変更されました。[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add/Edit] > [General] > [More Options]。[Maximum Connect Time Alert Interval] フィールドが追加されました。
AAA 機能	
AAA 用 LDAP サーバおよび TACACS+ サーバの IPv6 アドレスのサポート	AAA に使用する LDAP サーバおよび TACACS+ サーバで IPv4 アドレスか IPv6 アドレスのいずれかを使用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 Server Groups] > [Add AAA Server Group]**
管理機能	

機能	説明
すべてのローカル **username** および **enable** パスワードに対する PBKDF2 ハッシュ	長さ制限内のすべてのローカル **username** および **enable** パスワードは、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。以前は、32 文字以下のパスワードが MD5 ベースのハッシュ メソッドを使用していました。既存のパスワードでは、ユーザが新しいパスワードを入力しない限り、MD5 ベースのハッシュが引き続き使用されます。ダウングレードのガイドラインについては、『一般操作構成ガイド』の「ソフトウェアおよびコンフィギュレーション」の章を参照してください。 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]**
ライセンシング機能	
Firepower 4100/9300 シャーシ 上のフェールオーバー ペアのライセンス変更	アクティブなユニットのみがライセンス権限を要求します。以前は、両方のユニットがライセンスの権限付与を要求していました。FXOS 2.1.1 でサポートされます。
モニタリング機能とトラブルシューティング機能	
トレースルート用の IPv6 アドレスのサポート	**traceroute** コマンドが変更され、IPv6 アドレスも受け入れられるようになりました。 次の画面が変更されました。**[Tools] > [Traceroute]**
ブリッジ グループ メンバー インターフェイス用のパケット トレーサのサポート	ブリッジ グループ メンバー インターフェイスにパケット トレーサを使用できるようになりました。 パケット トレーサの画面に [VLAN ID] および [Destination MAC Address] フィールドが追加されました。**[Tools] > [Packet Tracer]**
syslog サーバの IPv6 アドレスのサポート	syslog サーバに IPv6 アドレスを設定して、TCP や UDP 経由で syslog を記録または送信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] > [Logging] > [Syslog Servers] > [Add Syslog Server]**
SNMP の MIB および OID	ASA は、ISA 3000 の Precision Time Protocol（PTP）の一部として、エンドツーエンド トランスペアレント クロック モードに対応する SNMP MIB オブジェクトをサポートするようになりました。次の SNMP MIB オブジェクトがサポートされます。 • ciscoPtpMIBSystemInfo • cPtpClockDefaultDSTable • cPtpClockTransDefaultDSTable • cPtpClockPortTransDSTable

機能	説明
手動によるパケット キャプチャの停止と開始	キャプチャを手動で停止および開始できるようになりました。 追加/変更された画面：**[Wizards]** > **[Packet Capture Wizard]** > **[Run Captures]** 追加/変更されたオプション：[Start] ボタン、[Stop] ボタン

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。

（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
9.6(x)	—	次のいずれかになります。 → 9.6(x)
9.5(x)	—	次のいずれかになります。 → 9.6(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
9.4(x)	—	次のいずれかになります。 → 9.6(x)
9.3(x)	—	次のいずれかになります。 → 9.6(x)
9.2(x)	—	次のいずれかになります。 → 9.6(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。 → 9.6(x) → 9.1(7.4)
9.1(1)	→ 9.1(2)	次のいずれかになります。 → 9.6(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。 → 9.6(x) → 9.1(7.4)
9.0(1)	→ 9.0(4)	次のいずれかになります。 → 9.6(x) → 9.1(7.4)
8.6(1)	→ 9.0(4)	次のいずれかになります。 → 9.6(x) → 9.1(7.4)
8.5(1)	→ 9.0(4)	次のいずれかになります。 → 9.6(x) → 9.1(7.4)
8.4(5+)	—	次のいずれかになります。 → 9.6(x) → 9.1(7.4) → 9.0(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
8.4(1) ～ 8.4(4)	→ 9.0(4)	→ 9.6(x) → 9.1(7.4)
8.3(x)	→ 9.0(4)	次のいずれかになります。 → 9.6(x) → 9.1(7.4)
8.2(x) 以前	→ 9.0(4)	次のいずれかになります。 → 9.6(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 7.7(1.151) で未解決のバグ

バージョン 7.7(1.151) で未解決の新しいバグはありません。バージョン 7.7(1) で未解決のバグ（22 ページ） を参照してください。

バージョン 7.7(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 7.7(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。

- 7.7(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。

不具合 ID 番号	説明
CSCvc73791	ASDM 設定の SNMPv3 ユーザにエラーが発生しています。

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 7.7(1.151) 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
CSCvd90344	ASDM 7.7.150 アップロードウィザードが機能していない

バージョン 7.7(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、重大度 3 以上の解決済みのバグを検索できます。

- 7.7(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。

不具合 ID 番号	説明
CSCva50676	ASDM がネットワーク IP をアクセスリスト内のホストベースのオブジェクトに置き換えている
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
CSCva99049	ASDM：リストを並べ替えた後に誤ったサービスオブジェクトが追加された
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
CSCvb24760	ASDM：Launcher および cisco.com からデモ機能を削除する

不具合 ID 番号	説明
CSCvb37828	ASDM 7.6.x に「pre-fill-username」オプションが表示されない
CSCvb48973	ASDM：VPN ウィザードが誤って設定を組み合わせている
CSCvb49232	ASDM：VPN が暗号アクセスリストを削除する
CSCvb53989	連続していないオブジェクトのサブネットマスクの修正を ASDM が許可しない
CSCvb63008	ASDM 7.6.2 がアクティブな AnyConnect クライアントを表示しない
CSCvb68442	ASDM の [ファイル管理（File Management）] に Disk1 が表示されない
CSCvb99770	ASDM が ACL のさまざまな行番号から同一のコメントを削除しない
CSCvb99824	ACE からオブジェクトグループを削除するときに ASDM が重複するコメントを追加する
CSCvc10201	ASDM 7.6.2 が IPsec RA 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

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/jp/go/warranty にアクセスしてください。

関連資料

ASA の詳細については、『Navigating the Cisco ASA Series Documentation』を参照してください。

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2017 Cisco Systems, Inc. All rights reserved.