Cisco Secure Firewall ASDM 7.18(x) リリースノート

初版：2022 年 6 月 6 日

最終更新：2024 年 5 月 22 日

Cisco Secure Firewall ASDM 7.18(x) リリースノート

このドキュメントには、Secure Firewall ASA シリーズ対応 ASDM バージョン 7.18(x) のリリース情報が記載されています。

特記事項

- **9.18(2)/7.18(1.152) 以降で ASDM 署名付きイメージをサポート**：ASA は、ASDM イメージがシスコのデジタル署名付きイメージであるかどうかを検証するようになりました。この修正を適用した ASA バージョンで古い ASDM イメージを実行しようとすると、ASDM がブロックされ、「%ERROR: Signature not valid for file disk0:/<filename>」というメッセージが ASA CLI に表示されます。ASDM リリース 7.18(1.152) 以降は、この修正が適用されていないものも含め、すべての ASA バージョンと下位互換性があります。（CSCwb05291、CSCwb05264）
- **9.18 以降からのダウングレードの問題**：9.18 では動作が変更され、**access-group** コマンドがその **access-list** コマンドの前にリストされます。ダウングレードすると、**access-group** コマンドはまだ **access-list** コマンドをロードしていないため拒否されます。以前に **forward-reference enable** コマンドを有効にしていた場合でも、このコマンドは現在削除されているため同じ結果となります。ダウングレードする前にすべての **access-group** コマンドを手動でコピーし、ダウングレード後に再入力してください。
- **同じポートを使用した同じインターフェイスで HTTPS/ASDM（HTTPS 認証を使用）および SSL を有効にした場合の 9.18(1) アップグレードの問題**：同じインターフェイス上で SSL（[webvpn]>[インターフェイスの有効化（enable interface）]）と HTTPS/ASDM（**http**）アクセスの両方を有効にした場合、**https://***ip_address* から AnyConnect にアクセスでき、**https://***ip_address*/**admin** から ASDM にアクセスできます。どちらもポート 443 を使用します。ただし、HTTPS 認証（**aaa authentication http console**）も有効にする場合は、9.18(1) 以降、ASDM アクセス用に別のポートを指定する必要があります。**http** コマンドを使用してアップグレードする前に、ポートを変更してください。（CSCvz92016）
- **9.18(2.7) での Cisco Secure Firewall 3100 の動作変更**：Cisco Secure Firewall 3100 の固定ポートで **fec** コマンドを使用して 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。（CSCwc75082）

- **ASDM アップグレードウィザード**：ASD API 移行のため、ASA 9.18 以降にアップグレードするには ASDM 7.18 以降を使用する必要があります。ASDM は以前の ASA バージョンと下位互換性があるため、どの ASA バージョンでも ASDM を 7.18 以降にアップグレードできます。
- **ASDM 7.18 で Java Web Launch のサポートが終了**：ASDM 7.18 以降、Oracle による JRE 8 および Java Network Launching Protocol（JNLP）のサポートが終了したため、ASDM は Java Web Start をサポートしません。ASDM を起動するには、ASDM Launcher をインストールする必要があります。

システム要件

ASDM には、4 コア以上の CPU を搭載したコンピュータが必要です。コア数が少ないと、メモリ使用量が高くなる可能性があります。

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

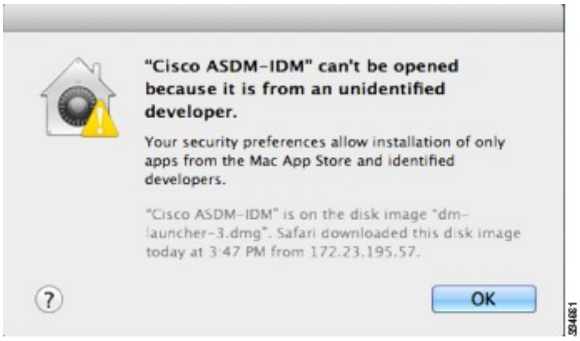
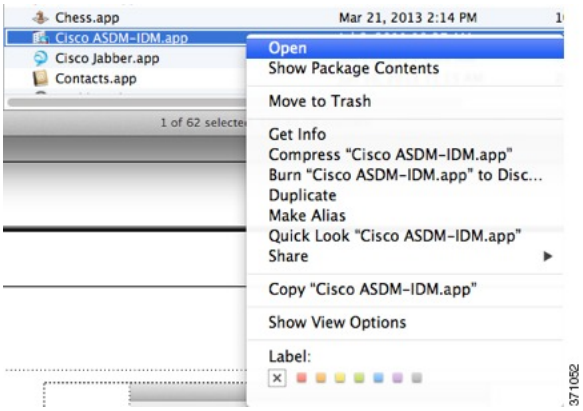
オペレーティング システム	ブラウザ			Oracle JRE	OpenJRE
	Firefox	Safari	Chrome		
Microsoft Windows（英語および日本語）： • 10 （注） ASDM ショートカットに問題がある場合は、ASDM の互換性に関する注意事項 （3 ページ）の「Windows 10」を参照してください。 • 8 • 7 • Server 2016 と Server 2019 • Server 2012 R2 • Server 2012 • Server 2008	対応	サポートなし	対応	8.0 バージョン 8u261 以降	1.8 （注） Windows 7 または 10（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
ASDM Launcher と ASDM バージョンの互換性	「デバイスマネージャを起動できません（Unable to Launch Device Manager）」というエラーメッセージが表示されます。 新しいASDMバージョンにアップグレードしてからこのエラーが発生した場合は、最新の Launcher を再インストールする必要があります。 **1.** ASA（https://<asa_ip_address>）で ASDM Web ページを開きます。 **2.** [ASDMランチャーのインストール（Install ASDM Launcher）] をクリックします。 **図 *1 : ASDM Launcher* のインストール**  **3.** ユーザー名とパスワードのフィールドを空のままにし（新規インストールの場合）、[OK] をクリックします。 HTTPS 認証が設定されていない場合は、ユーザー名および**イネーブル**パスワード（デフォルトで空白）を入力しないで ASDM にアクセスできます。CLI で **enable** コマンドを最初に入力したときに、パスワードを変更するように求められます。ASDMにログインしたときには、この動作は適用されません。空白のままにしないように、できるだけ早くイネーブルパスワードを変更することをお勧めします。**注**：HTTPS 認証をイネーブルにした場合、ユーザー名と関連付けられたパスワードを入力します。認証が有効でない場合でも、ログイン画面で（ユーザー名をブランクのままにしないで）ユーザー名とパスワードを入力すると、ASDMによってローカルデータベースで一致がチェックされます。

条件	注意
Windows Active Directory ディレクトリアクセス	場合によっては、Windows ユーザーの Active Directory 設定によって、Windows で ASDM を正常に起動するために必要なプログラムファイルの場所へのアクセスが制限されることがあります。次のディレクトリへのアクセスが必要です。 • デスクトップフォルダ • C:\Windows\System32C:\Users\<username>\.asdm • C:\Program Files (x86)\Cisco Systems Active Directory がディレクトリ アクセスを制限している場合は、Active Directory 管理者にアクセスを要求する必要があります。
Windows 10	「このアプリはお使いの PC では実行できません（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. **[スタート（Start）] > [Cisco ASDM-IDM ランチャー（Cisco ASDM-IDM Launcher）]** を選択し、[Cisco ASDM-IDM ランチャー（Cisco ASDM-IDM Launcher）] アプリケーションを右クリックします。 2. **[その他（More）] > [ファイルの場所を開く（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、[プロパティ（Properties）] を選択します。 4. [リンク先（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 ランチャー（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、[開く（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。[開く（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 [英語] にアクセスします。 2. [製品ライセンスの登録を続行（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 [その他のライセンスの取得（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、暗号、その他...（IPS, Crypto, Other...）] を選択します。 5. [キーワードで検索（Search by Keyword）] フィールドに「ASA」と入力します。 6. [製品（Product）] リストで [Cisco ASA 3DES/AESライセンス（Cisco ASA 3DES/AES License）] を選択し、[次へ（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際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 [英語] 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いずれかを再度有効にすることを推奨します（**[設定（Configuration）] > [デバイス管理（Device Management）] > [詳細（Advanced）] > [SSL設定（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。

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』[英語] 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。メモリが枯渇していることを確認するには、Java コンソールで「java.lang.OutOfMemoryError」メッセージをモニターします。

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。

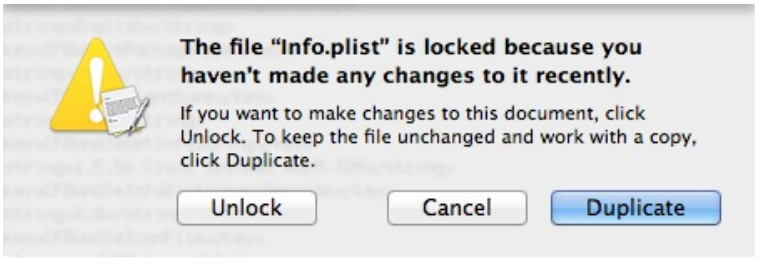
ステップ 3 **[Java]** > **[VMOptions]** で、「-Xmx」のプレフィックスが付いた文字列を変更し、必要なヒープサイズを指定します。たとえば、768 MB の場合は -Xmx768M に変更し、1 GB の場合は -Xmx1G に変更します。

```
    <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』[英語] 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 』[英語] 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 7.18(1.161) の新機能

リリース：**2023年 7 月 3 日**

このリリースに新機能はありません。

ASA 9.18(4)/ASDM 7.20(1) の新機能

リリース：**2023 年10 月 3 日**

機能	説明
高可用性とスケーラビリティの各機能	
ASA の高可用性のための偽フェールオーバーの削減	ASA 高可用性のデータプレーンに追加のハートビートモジュールが導入されました。このハートビートモジュールは、コントロールプレーンのトラフィックの輻輳や CPU の過負荷が原因で発生する可能性のある、偽フェールオーバーやスプリットブレインシナリオを回避するのに役立ちます。 9.20(1) でも同様です。
show failover statistics にクライアント統計情報を追加	フェールオーバー クライアントのパケット統計情報が拡張され、デバッグ機能が向上しました。**show failover statistics** コマンドは、**np-clients**（データパスクライアント）および **cp-clients**（コントロールプレーン クライアント）の情報を表示するように拡張されています。 変更されたコマンド：**show failover statistics cp-clients**、**show failover statistics dp-clients** 9.20(2) でも同様です。
show failover statistics events に新しいイベントを追加	**show failover statistics events** コマンドが拡張され、アプリケーション エージェントによって通知されるローカル障害（フェールオーバーリンクの稼働時間、スーパーバイザハートビート障害、およびディスクフルの問題）を表示するようになりました。 変更されたコマンド： **show failover statistics events** 9.20(2) でも同様です。
インターフェイス機能	

機能	説明
FXOS local-mgtm **show** コマンドの改善	FXOS local-mgmt のインターフェイス show コマンドに関する追加項目は次のとおりです。 • **show portmanager switch tail-drop-allocated buffers all** コマンドが追加されました。 • **show portmanager switch status** コマンドにイーサネットポート ID が含まれます。 • Cisco Secure Firewall 3100 に、**show portmanager switch default-rule-drop-counter** コマンドが追加されました。 新規/変更された FXOS コマンド：**show portmanager switch tail-drop-allocated buffers all**、**show portmanager switch status**、**show portmanager switch default-rule-drop-counter**
管理、モニタリング、およびトラブルシューティングの機能	
show tech support の改善	次の項目に対して、**show tech support** への出力が追加されました。 • Cisco Secure Firewall 3100 の **show storage detail**、**show slot expand detail**（**show tech support brief** 内） • ASA Virtual のフラッシュ内の dpdk.log からの最近のメッセージ • Firepower 1010 の制御リンク状態 • **show failover** 統計情報 • FXOS local-mgmt **show portmanager switch tail-drop-allocated buffers all** • **show controller** • DPDK mbuf プール統計情報 新規/変更されたコマンド： **show tech support**

ASA 9.18(3)/ASDM 7.19(1.90) の新機能

リリース日：**2023 年 2 月 16 日**

機能	説明
インターフェイス機能	

機能	説明
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）]** 9.19(1) および 9.18(2.7) でも同様です。
VPN 機能	
SAML を使用した AnyConnect 接続認証	DNS ロードバランシングクラスタでは、SAML 認証を ASA で設定するときに、設定が適用されるデバイスに一意に解決されるローカルベース URL を指定できます。

ASA 9.18(2)/ASDM 7.18(1.152) の新機能

リリース日：**2022 年 8 月 10 日**

機能	説明
インターフェイス機能	
BGP および管理トラフィックのループバックインターフェイスをサポート	ループバック インターフェイスを追加して、次の機能に使用できるようになりました。 • AAA • BGP • SNMP • SSH • Syslog • Telnet 新規/変更されたコマンド：**interface loopback**、**logging host**、**neighbor update-source**、**snmp-server host**、**ssh**、**telnet** ASDM サポートはありません。

機能	説明
ping コマンドの変更	ループバック インターフェイスの ping をサポートするために、**ping** コマンドの動作が変更されました。コマンドでインターフェイスを指定する場合、送信元IPアドレスは指定されたインターフェイスのIPアドレスと一致しますが、実際の出力インターフェイスは、データルーティングテーブルを使用したルートルックアップによって決定されます。 新規/変更されたコマンド： **ping**

ASDM 7.18(1.152) の新機能

リリース日：**2022 年 8 月 2 日**

このリリースに新機能はありません。

ASA 9.18(1)/ASDM 7.18(1) の新機能

リリース日：**2022 年 6 月 6 日**

機能	説明
プラットフォーム機能	
AWS GuardDuty の ASAv-AWS Security center integration	Amazon GuardDuty サービスを ASAv と統合できるようになりました。この統合ソリューションは、Amazon GuardDutyによって報告された脅威分析データや結果（悪意のある IP アドレス）をキャプチャして処理するのに役立ちます。ASAv で悪意のある IP アドレスを設定およびフィードし、基盤となるネットワークとアプリケーションを保護できます。
ファイアウォール機能	

機能	説明
ACL とオブジェクトの前方参照は常に有効にです。さらに、アクセス制御のオブジェクトグループ検索がデフォルトで有効になりました。	アクセスグループまたはアクセスルールを設定するときに、まだ存在していない ACL またはネットワークオブジェクトを参照できます。 さらに、オブジェクトグループ検索が新規展開のアクセス制御に対してデフォルトで有効になりました。デバイスをアップグレードしても、引き続きこのコマンドは無効になります。有効にする場合（推奨）、手動で行う必要があります。 **注意** ダウングレードすると、**access-group** コマンドはまだ **access-list** コマンドをロードしていないため拒否されます。以前に **forward-reference enable** コマンドを有効にしていた場合でも、このコマンドは現在削除されているため同じ結果となります。ダウングレードする前にすべての **access-group** コマンドを手動でコピーし、ダウングレード後に再入力してください。 **forward-reference enable** コマンドを削除し、新規展開のデフォルト値を変更して **object-group-search access-control** を有効にしました。
ルーティング機能	
PBR のパスモニタリングメトリック。	PBR はメトリックを使用して、トラフィックを転送するための最適なパス（出力インターフェイス）を決定します。パスモニタリングは、メトリックが変更されたモニタリング対象インターフェースを PBR に定期的に通知します。PBR は、モニタリング対象インターフェイスの最新のメトリック値をパスモニタリングデータベースから取得し、データパスを更新します。 新規/変更された画面：**[設定（Configuration）] > [デバイス設定（Device Setup）] > [インターフェイス設定（Interface Settings）] > [インターフェイス（Interfaces）]**
インターフェイス機能	
Cisco Secure Firewall 3100 のフロー制御に対応するためのフレームの一時停止	トラフィック バーストが発生している場合、バーストが NIC の FIFO バッファまたは受信リングバッファのバッファリング容量を超えると、パケットがドロップされる可能性があります。フロー制御用のポーズフレームをイネーブルにすると、このような問題の発生を抑制できます。 新規/変更された画面：**[設定（Configuration）] > [デバイス設定（Device Setup）] > [インターフェイス（Interface）] > [全般（General）]**
Secure Firewall 3130 および 3140 のブレークアウトポート	Cisco Secure Firewall 3130 および 3140 の 40 GB インターフェースごとに 4 つの 10 GB ブレークアウトポートを構成できるようになりました。 新規/変更された画面：**[設定（Configuration）] > [デバイス管理（Device Management）] > [詳細（Advanced）] > [EPM]**
ライセンス機能	

機能	説明
キャリアライセンスの Secure Firewall 3100 サポート	キャリアライセンスは、Diameter、GTP/GPRS、SCTP 検査を有効にします。 新規/変更された画面：**[設定（Configuration）]** > **[デバイス管理（Device Management）]** > **[ライセンス（Licensing）]** > **[スマートライセンス（Smart Licensing）]**。
証明書の機能	
相互l LDAPS 認証。	ASA が認証のために証明書を要求したときに LDAP サーバーに提示するように ASA のクライアント証明書を設定できます。この機能は、LDAP over SSL を使用する場合に適用されます。LDAP サーバーがピア証明書を要求するように設定されている場合、セキュア LDAP セッションが完了せず、認証/許可要求が失敗します。 新規/変更された画面：**[設定（Configuration）]** > **[デバイス管理（Device Management）]** > **[ユーザー/AAA（Users/AAA）]** > > **[AAAサーバーグループ（AAA Server Groups）]**、LDAP サーバーを追加または編集。
認証：証明書名または SAN の検証	機能固有の参照 ID が設定されている場合、ピア証明書 ID は、指定された一致基準 **crypto ca reference-identity** <*name*> コマンドで検証されます。ピア証明書のサブジェクト名または SAN に一致するものが見つからない場合、または reference-identity サブモードコマンドで指定された FQDN が解決されない場合、接続は終了します。 reference-identity CLI は、AAA サーバーホスト設定および ddns 設定のサブモードコマンドとして設定されます。 新しい/変更された画面： • **[設定（Configuration）]** > **[デバイス管理（Device Management）]** > **[ユーザー/AAA（Users/AAA）]** > > **[AAAサーバーグループ（AAA Server Groups）]** > **[認証/認可用のLDAPパラメータ（LDAP Parameters for authentication/authorization）]** • **[設定（Configuration）]** > **[デバイス管理（Device Management）]** > **[DNS]** > **[ダイナミックDNS（Dynamic DNS）]** > **[メソッドを更新（Update Methods）]**
管理、モニタリング、およびトラブルシューティングの機能	
複数の DNS サーバーグループ	複数の DNS サーバーグループを使用できるようになりました。1 つのグループがデフォルトで、他のグループを特定のドメインに関連付けることができます。DNS サーバーグループに関連付けられたドメインに一致する DNS 要求は、そのグループを使用します。たとえば、内部の eng.cisco.com サーバー宛てのトラフィックで内部の DNS サーバーを使用する場合は、eng.cisco.com を内部の DNS グループにマッピングできます。ドメインマッピングと一致しないすべての DNS 要求は、関連付けられたドメインを持たないデフォルトの DNS サーバーグループを使用します。たとえば、DefaultDNS グループには、外部インターフェイスで使用可能なパブリック DNS サーバーを含めることができます。 新規/変更された画面：**[設定（Configuration）]** > **[デバイス管理（Device Management）]** > **[DNS]** > **[DNSクライアント（DNS Client）]**

機能	説明
ダイナミックログインのレート制限	ブロック使用量が指定されたしきい値を超えたときにロギングレートを制限する新しいオプションが追加されました。ブロックの使用量が通常の値に戻るとレート制限が無効になるため、ロギングレートが動的に制限されます。 新規/変更された画面：**[設定（Configuration）] > [デバイス管理（Device Management）] > [ロギング（Logging）] > [レート制限（Rate Limit）]**
Secure Firewall 3100 デバイスのパケットキャプチャ	スイッチパケットをキャプチャするプロビジョニングが追加されました。このオプションは、Secure Firewall 3100 デバイスに対してのみ有効にできます。 新規/変更された画面：**[ウィザード（Wizards）] > [パケットキャプチャウィザード（Packet Capture Wizard）] > [バッファおよびキャプチャ（Buffers & Captures）]**
VPN 機能	
IPsec フローのオフロード。	Cisco Secure Firewall 3100 では、IPsec フローはデフォルトでオフロードされます。IPsec サイト間 VPN またはリモートアクセス VPN セキュリティ アソシエーション (SA) の初期設定後、IPsec 接続はデバイスのフィールドプログラマブル ゲート アレイ (FPGA) にオフロードされるため、デバイスのパフォーマンスが向上します。 新規/変更された画面：**[設定（Configuration）] > [ファイアウォール（Firewall）] > [高度（Advanced）] > [IPsecオフロード（IPsec Offload）]**
認証用の証明書と SAML	証明書および SAML 認証用にリモートアクセス VPN 接続プロファイルを設定できます。ユーザーは、SAML 認証/承認が開始される前に、マシン証明書やユーザー証明書を認証するように VPN を設定できます。これは、ユーザー固有の SAML DAP 属性と DAP 証明書属性を使用して実行できます。 新規/変更された画面：**[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [ネットワーク(クライアント)アクセス（Network (Client) Access）] > [IPsec(IKEv1)接続プロファイル（IPsec(IKEv1) Connection Profiles）] > [追加/編集（Add/Edit）] > [ベーシック（Basic）]**

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：**[ホーム（Home）] > [デバイスダッシュボード（Device Dashboard）] > [デバイス情報（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 [英語] を参照してください。

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

ASA 9.14 は ASA 5525-X、5545-X、および 5555-X の最終バージョンです。

ASA 9.12 は ASA 5512-X、5515-X、5585-X、および ASASM 用の最終バージョン、

ASA 9.2 は ASA 5505 の最終バージョンです。

ASA 9.1 は ASA 5510、5520、5540、5550、および 5580 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
9.17	—	次のいずれかになります。 → **9.18**
9.16	—	次のいずれかになります。 → **9.18** → 9.17
9.15	—	次のいずれかになります。 → **9.18** → 9.17 → **9.16**

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
9.14	—	次のいずれかになります。 → **9.18** → 9.17 → **9.16** → 9.15
9.13	—	次のいずれかになります。 → **9.18** → 9.17 → **9.16** → 9.15 → 9.14
9.12	—	次のいずれかになります。 → **9.18** → 9.17 → **9.16** → 9.15 → 9.14
9.10	—	次のいずれかになります。 → **9.18** → 9.17 → **9.16** → 9.15 → 9.14 → 9.12

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	—	次のいずれかになります。 → **9.18** → 9.17 → **9.16** → 9.15 → 9.14 → 9.12
9.8	—	次のいずれかになります。 → **9.18** → 9.17 → **9.16** → 9.15 → 9.14 → 9.12
9.7	—	次のいずれかになります。 → **9.18** → 9.17 → **9.16** → 9.15 → 9.14 → 9.12 → 9.8

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	—	次のいずれかになります。 → **9.18** → 9.17 → **9.16** → 9.15 → 9.14 → 9.12 → 9.8
9.5	—	次のいずれかになります。 → **9.18** → 9.17 → **9.16** → 9.15 → 9.14 → 9.12 → 9.8
9.4	—	次のいずれかになります。 → **9.18** → 9.17 → **9.16** → 9.15 → 9.14 → 9.12 → 9.8

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	—	次のいずれかになります。 → **9.18** → 9.17 → **9.16** → 9.15 → 9.14 → 9.12 → 9.8
9.2	—	次のいずれかになります。 → **9.18** → 9.17 → **9.16** → 9.15 → 9.14 → 9.12 → 9.8
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 → **9.12** → 9.8 → 9.1(7.4)
9.1(1)	→ 9.1(2)	次のいずれかになります。 → 9.14 → **9.12** → 9.8 → 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 → **9.12** → 9.8 → 9.6 → 9.1(7.4)
9.0(1)	→ 9.0(4)	次のいずれかになります。 → 9.14 → **9.12** → 9.8 → 9.1(7.4)
8.6(1)	→ 9.0(4)	次のいずれかになります。 → 9.14 → **9.12** → 9.8 → 9.1(7.4)
8.5(1)	→ 9.0(4)	次のいずれかになります。 → **9.12** → 9.8 → 9.1(7.4)
8.4(5+)	—	次のいずれかになります。 → **9.12** → 9.8 → 9.1(7.4) → 9.0(4)
8.4(1) ～ 8.4(4)	→ 9.0(4)	→ **9.12** → 9.8 → 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	→ 9.0(4)	次のいずれかになります。 → **9.12** → 9.8 → 9.1(7.4)
8.2 以前	→ 9.0(4)	次のいずれかになります。 → **9.12** → 9.8 → 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』[英語] 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 Help & FAQ [英語] 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 7.18(1.161) 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
CSCvu01215	アプライアンスモード：CCO から ASA イメージをダウンロードしている間にチェックサムが一致しない問題
CSCvv83043	9161/7161 CLI に従って VPN ウィザードで暗号を変更する必要がある

バージョン 7.18(1.152) 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
CSCvu01215	アプライアンスモード：CCO から ASA イメージをダウンロードしている間にチェックサムが一致しない問題
CSCvv83043	9161/7161 CLI に従って VPN ウィザードで暗号を変更する必要がある

バージョン 7.18(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
CSCvu01215	アプライアンスモード：CCO から ASA イメージをダウンロードしている間にチェックサムが一致しない問題
CSCvv83043	9161/7161 CLI に従って VPN ウィザードで暗号を変更する必要がある

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 7.18(1.161) 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
CSCwd58653	ASDM の初期接続またはロード時間の増加
CSCwd85545	CLI から設定されたクラスマップ ACL が削除されるため、すべてのクラスマップ設定が ASDM によって削除される
CSCwd98702	ASDM の「使用場所（Where used）」オプションが機能しない
CSCwe00348	ASDM からホストスキャンファイルを更新できない。ホストスキャンイメージをインストールすると、DAP を編集できない

ID	見出し
CSCwe34665	ACL オブジェクトがすでに使用されている場合は編集できず、例外が発生する。
CSCwe52019	ASDM がセキュリティ例外エラーで起動に失敗する：無効な SHA1 署名ファイル

バージョン 7.18(1.152) 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
CSCvw79912	Cisco Adaptive Security Device Manager でリモートコードが実行される脆弱性
CSCwb05264	Cisco ASDM および ASA ソフトウェアのクライアント側で任意のコードが実行される脆弱性

バージョン 7.18(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
CSCvv17403	同時接続 prempt で遅延のなくトンネルの削除を無効にするためのチェックボックスが使用できない
CSCvx31842	SDM に HS4.10.x がある場合、Hostscan 4.3.x から 4.6.x への移行手順は表示されない。
CSCvy17527	「ロードバランシング」項目は ASDM には表示されない。
CSCvy38427	ASDM：複数の AC モジュールを有効にするには、変換ファイル名を「_」の下線で始める必要がある
CSCvz62261	ASDM の使用時にユーザーアクセスを制限できない
CSCvz89126	マルチ コンテキスト スイッチオーバーが ASDM から実行される場合、ASA で ASDM セッション/クォータカウントの不一致が発生する
CSCwa48034	ASA #CSCvz89126 の ASDM 側の変更
CSCwa70482	MAC ポップアップの ASDM によって hostscan/CSD pkg が削除される
CSCwa99370	ASDM:DAP 設定に AAA 属性タイプがない（Radius/LDAP）
CSCwb84225	ASDM および ASA REST API の評価版 OpenJDK CVE

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 [英語] 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』[英語] 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。