



Cisco ASA 5500-X シリーズ リリース ノート、バージョン 8.6(x)

リリース：2012 年 2 月 28 日

更新：2016 年 7 月 12 日

このドキュメントには、Cisco ASA 5500-X ソフトウェア バージョン 8.6(1) のリリース情報が記載されています。

このマニュアルの構成は、次のとおりです。

- [特記事項、1 ページ](#)
- [システム要件、2 ページ](#)
- [新機能、2 ページ](#)
- [ソフトウェアのアップグレード、4 ページ](#)
- [未解決の不具合、7 ページ](#)
- [エンド ユーザー ライセンス契約書、7 ページ](#)
- [関連資料、8 ページ](#)
- [マニュアルの入手方法、テクニカル サポート、およびセキュリティ ガイドライン、8 ページ](#)

特記事項

- Cisco ASA クライアントレス SSL VPN ポータルのカスタマイズにおける整合性の脆弱性：
ASA 上のクライアントレス SSL VPN に対して複数の脆弱性修正が行われているため、修正版へソフトウェアをアップグレードする必要があります。脆弱性の詳細と、修正が済んだ ASA バージョンのリストについては、
<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20141008-asa> を参照してください。脆弱性をもった構成で以前のバージョンの ASA を運用したことがある場合は、現在実行中のバージョンに関係なく、ポータルのカスタマイズが危殆化されていないか確認する必要があります。過去に攻撃者がカスタマイゼーション オブジェクトを危殆化した場合、ASA を修正版にアップグレードした後も危殆化されたオブジェクトが存続します。ASA をアップグレードすることで今後の危殆化を阻止できますが、すでに危殆化されているカスタマイゼーション オブジェクトは一切変更されず、システムに存続します。



システム要件

バージョン 8.6(1) は、Cisco ASA 5500-X シリーズのみをサポートします。これには、Cisco ASA 5512-X、5515-X、5525-X、5545-X、および 5555-X が含まれます。このバージョンは、ASA 5585-X では使用できません。

表 1 に、ASDM、モジュール、および VPN と ASA 5500 シリーズとの互換性に関する情報を示します。

表 1 ASDM、SSM、SSC、および VPN の互換性

アプリケーション	説明
ASDM	ASA バージョン 8.6 には、ASDM バージョン 6.6 以降が必要です。 他のリリースの ASDM 要件については、Cisco ASA の互換性を参照してください。 http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrix.html
VPN	最新の OS とブラウザのテスト結果については、サポートされる VPN プラットフォーム、Cisco ASA 5500 シリーズを参照してください。 http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html
モジュール アプリケーション	モジュールアプリケーションの要件については、Cisco ASA の互換性を参照してください。 http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrix.html

新機能

リリース : 2012 年 2 月 28 日

表 2 に、ASA バージョン 8.6(1) の新機能を示します。この ASA ソフトウェア バージョンは、ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、および ASA 5555-X でのみサポートされます。



注 バージョン 8.6(1) には、8.4(2) のすべての機能と、この表に示されている機能が含まれています。8.4(3) で追加された機能は、この表で明示されていない限り、8.6(1) には含まれていません。

表 2 ASA バージョン 8.6(1) の新機能

特長	説明
ハードウェア機能	
ASA 5512-X ~ ASA 5555-X のサポート	ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、および ASA 5555-X のサポートが導入されました。
IPS 機能	
ASA 5512-X ~ ASA 5555-X に対する IPS SSP のサポート	ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、および ASA 5555-X に対する IPS SSP ソフトウェア モジュールのサポートが導入されました。 session、show module、sw-module の各コマンドが導入または変更されました。
リモート アクセス機能	

表 2 ASA バージョン 8.6(1) の新機能 (続き)

特長	説明
ブラウザでのクライアントレス SSL VPN のサポート	ASA は、Microsoft Internet Explorer 9 および Firefox 4 を使用してクライアントレス SSL VPN をサポートするようになりました。 バージョン 8.4(3) でも使用可能です。
DTLS および TLS における圧縮	スループットを向上させるため、シスコは AnyConnect 3.0 以降での DTLS と TLS の圧縮をサポートするようになりました。各トンネリング メソッドは個別に圧縮を構成します。優先設定は SSL と DTLS の両方の圧縮を LZS とすることです。この機能は、従来の VPN クライアントからの移行を強化します。 注 高圧縮データを渡す高速リモート アクセス接続でデータ圧縮を使用するには、ASA にかんりの処理能力が要求されます。ASA で他の活動やトラフィックがあると、プラットフォームでサポートできるセッションの数は減ります。 次のコマンドを導入、または変更しました：<code>anyconnect dtls compression [lzs none]</code> および <code>anyconnect ssl compression [deflate lzs none]</code>。 バージョン 8.4(3) でも使用可能です。
クライアントレス SSL VPN セッション タイムアウトアラート	ユーザーの VPN セッションが、無活動またはセッション タイムアウトにより終了することをユーザーに警告するカスタム メッセージを作成できます。 次のコマンドが導入されました。<code>vpn-session-timeout alert-interval</code>、<code>vpn-idle-timeout alert-interval</code> バージョン 8.4(3) でも使用可能です。
マルチ コンテキスト モード機能	
MAC アドレス プレフィックスの自動生成	マルチ コンテキスト モードで、ASA が MAC アドレス自動生成のコンフィギュレーションを変換し、デフォルトのプレフィックスを使用できるようになりました。ASA は、インターフェイスの MAC アドレスの最後の 2 バイトに基づいてプレフィックスを自動生成します。この変換は、リロード時または MAC アドレス生成を再度イネーブルにすると、自動的に行われます。生成のプレフィックス方式は、セグメント上で一意の MAC アドレスがより適切に保証されるなど、多くの利点をもたらします。 <code>show running-config mac-address</code> コマンドを入力して、自動生成されたプレフィックスを表示できます。プレフィックスを変更する場合、カスタム プレフィックスによって機能を再設定できます。MAC アドレス生成の従来の方法は使用できなくなります。 注 フェールオーバー ペアのヒットレス アップグレードを維持するため、フェールオーバーが有効である場合、ASA は既存の構成の MAC アドレス メソッドをリロード時に変換しません。ただし、生成のプレフィックス方式に手動で変更することを強く推奨します。アップグレード後に、MAC アドレス生成のプレフィックス方式を使用するには、デフォルトのプレフィックスを使用する MAC アドレス生成を再びイネーブルにします。 <code>mac-address auto</code> コマンドが変更されました。
AAA 機能	

表 2 ASA バージョン 8.6(1) の新機能 (続き)

特長	説明
属性あたりの最大 LDAP 値が増加	単一の属性に対して ASA が受け取ることができる値の最大数は、1000 (デフォルト) から 5000 に増やされました。許可される範囲は 500 ~ 5000 です。設定された制限を超えた応答メッセージを受信した場合、ASA は認証を拒否します。ASA が、1000 を超える値を持つ単一の属性を検出した場合、ASA は情報 syslog 109036 を生成します。属性が 5000 を超える場合、ASA はエラー レベル syslog 109037 を生成します。 次のコマンドを導入しました。ldap-max-value-range number (このコマンドは aaa-server ホスト構成モードで入力します)。 バージョン 8.4(3) でも使用可能です。
LDAP 検索結果の下位範囲のサポート	サーバ設定に応じて、LDAP 検索が多数の値を持つ属性という結果になる場合、値のサブ範囲を返し、ASA が残りの値範囲に対して追加のクエリを開始することを予期することがあります。ASA は残りの範囲に対して複数のクエリを行い、応答を属性値の完全な配列に結合するようになりました。 バージョン 8.4(3) でも使用可能です。
トラブルシューティング機能	
show asp table classifier および show asp table filter コマンドでの正規表現マッチング	出力のフィルタ処理のため、show asp table classifier および show asp table filter コマンドで正規表現を入力できるようになりました。 次のようにコマンドを変更しました：show asp table classifier match regex、show asp table filter match regex バージョン 8.4(3) でも使用可能です。

ソフトウェアのアップグレード

このセクションでは、最新バージョンへのアップグレード方法を説明しており、次のトピックを含んでいます。

- [現在のバージョンの表示、4 ページ](#)
- [オペレーティング システムおよび ASDM イメージのアップグレード、5 ページ](#)
- [IPS ソフトウェア モジュールのインストール、6 ページ](#)
- [Cisco Secure Desktop のインストールまたはアップグレード、6 ページ](#)



注

ASDM の手順については、ASDM のリリース ノートを参照してください。

現在のバージョンの表示

お使いの ASA のソフトウェア バージョンを確認するには、show version コマンドを使用します。

オペレーティングシステムおよびASDMイメージのアップグレード

このセクションでは、TFTP を使用して ASDM およびオペレーティング システム (OS) イメージをインストールする方法について説明します。FTP または HTTP を使用する場合には、CLI 構成ガイドの「ソフトウェアと構成の管理」の章を参照してください。

OS イメージの前に ASDM イメージをアップグレードすることを推奨します。ASDM には下位互換性があるため、新しい ASDM を使用して OS をアップグレードすることは可能です。ただし、新しい OS で古い ASDM イメージを使用することはできません。

フェールオーバー ペアでのソフトウェアのアップグレードの詳細については、CLI 構成ガイドの「フェールオーバー ペアでのゼロ ダウンタイム アップグレードの実行」の章を参照してください。

手順の詳細

ステップ 1 Cisco.com にログインしている場合は、次の Web サイトから OS および ASDM イメージを取得できます：<http://www.cisco.com/cisco/software/navigator.html>

ステップ 2 構成ファイルをバックアップします。ターミナルに構成を出力するには、特権 EXEC モードで次のコマンドを入力します：

```
hostname# show running-config
```

このコマンドの出力をコピーして、構成をテキスト ファイルに貼り付けます。



注 8.3 よりも前のバージョンからアップグレードする場合、実行構成は自動的にバックアップされます。

その他のバックアップ方法については、CLI 構成ガイドの「ソフトウェアと構成の管理」の章を参照してください。

ステップ 3 TFTP を使用して新しいイメージをインストールします。このコマンドは、OS イメージと ASDM イメージに対して個別に入力します。

```
hostname# copy tftp://server[/path]/filename disk0:[/path/]filename
```

次に例を示します。

```
hostname# copy tftp://10.1.1.1/asa840-4-k8.bin disk0:/asa861-k8.bin
...
hostname# copy tftp://10.1.1.1/asdm-64099.bin disk0:/asdm-661.bin
```

ASA に 2 つのイメージを保持する十分なメモリがない場合は、既存のイメージと同じ宛先ファイル名を指定して、古いイメージを新しいイメージで上書きしてください。

ステップ 4 OS ブート イメージを新しいイメージ名に変更するには、グローバル構成モードで次のコマンドを入力します。

```
hostname (config) # clear configure boot
hostname (config) # boot system disk0:[/path/]new_filename
```

次に例を示します。

```
hostname (config) # clear configure boot
hostname (config) # boot system disk0:/asa861-k8.bin
```

ステップ 5 ASDM イメージに新しいイメージ名を構成するには、次のコマンドを入力します。

```
hostname (config) # asdm image disk0:[/path/]new_filename
```

ステップ 6 以下のコマンドを入力して、構成を保存し、リロードします。

```
hostname(config)# write memory
hostname(config)# reload
```

IPS ソフトウェア モジュールのインストール

ASA は、通常、Disk0 に IPS モジュール ソフトウェアが添付された状態で出荷されます。ただし、モジュールが実行されていない場合は、モジュールをインストールする必要があります。

手順の詳細

ステップ 1 フラッシュ メモリ内の IPS モジュール ソフトウェア ファイル名を表示するには、次のように入力します。

```
hostname# dir disk0:
```

たとえば、IPS-SSP_5512-K9-sys-1.1-a-7.1-4-E4.aip のようなファイル名を探します。ファイル名に注意してください。このファイル名は、この手順の後半で必要になります。

ステップ 2 新しいイメージを disk0 にコピーする必要がある場合、Cisco.com から TFTP サーバーにイメージをダウンロードして、次のように入力します。

```
hostname# copy tftp://server/file_path disk0:/file_path
```

その他のサーバー タイプについては、[23 ページの「ファイルのダウンロード」](#)のセクションを参照してください。

ステップ 3 disk0 で IPS モジュール ソフトウェアの場所を特定するには、次のコマンドを入力します。

```
hostname# sw-module module ips recover configure image disk0:file_path
```

たとえば、ステップ 1 の例のファイル名を使用して、次のように入力します。

```
hostname# sw-module module ips recover configure image
disk0:IPS-SSP_5512-K9-sys-1.1-a-7.1-4-E4.aip
```

ステップ 4 IPS モジュール ソフトウェアをインストールしてロードするには、次のコマンドを入力します。

```
hostname# sw-module module ips recover boot
```

ステップ 5 イメージの転送とモジュールの再起動プロセスの進行状況を確認するには、次のコマンドを入力します。

```
hostname# show module ips details
```

出力の [ステータス (Status)] フィールドは、モジュールの動作ステータスを示します。正常に動作しているモジュールのステータスは [アップ (Up)] と表示されます。ASA がモジュールにアプリケーション イメージを転送している間、出力の [ステータス (Status)] フィールドには [回復 (Recover)] と表示されます。ASA がイメージの転送を完了してモジュールを再起動すると、新しく転送されたイメージが実行されます。

Cisco Secure Desktop のインストールまたはアップグレード

ASA バージョン 8.6.(1) には、Cisco Secure Desktop リリース 3.2 以降が必要です。Cisco Secure Desktop のインストールまたはアップグレード後に、ASA を再起動する必要はありません。

Cisco Secure Desktop ソフトウェアをインストールまたはアップグレードするには、次のステップに従います。

- ステップ1** 次の Web サイトから最新の Cisco Secure Desktop パッケージファイルをダウンロードします：
<http://www.cisco.com/cisco/software/navigator.html>
- ステップ2** TFTP を使用して新しいイメージをインストールします。

```
hostname# copy tftp://server[/path]/filename disk0:[/path]/filename
```
- ステップ3** 次のコマンドを入力して、（グローバル構成モードから）webvpn 構成モードにアクセスします。

```
hostname(config)# webvpn
hostname(config-webvpn)#
```
- ステップ4** Cisco Secure Desktop 配布パッケージを検証し、それを実行構成に追加するには、次のコマンドを入力します。

```
hostname(config-webvpn)# csd image disk0:/securedesktop_asa_3_2_0_build.pkg
```
- ステップ5** 管理およびリモート ユーザー アクセス用に Cisco Secure Desktop を有効にするには、次のコマンドを使用します。

```
hostname(config-webvpn)# csd enable
```

未解決の不具合

表 3 に、バージョン 8.6(1) で未解決の不具合を示します。

Cisco.com に登録しているユーザーの場合は、次の Web サイトのバグ ツールキットを使用して、それぞれの不具合の詳細を確認してください。

<http://tools.cisco.com/Support/BugToolKit/>

表 3 ASA バージョン 8.6(1) で未解決の不具合

DDTS 番号	注意事項
CSCtr71193	IPS ソフトウェア モジュールが回復状態のときにリロードが実行されない
CSCts89380	Salesen：ASDM ハンドラが envmon psu 電源入力センサーをサポートしていない
CSCtt98015	Saleen：ライセンスのアップグレード後も暗号化エンジンのアーカイブが継続的に実行される
CSCtu59747	Saleen：show inventory が発行される前に 1 分間待つ必要がある
CSCtv22976	トンネル制限に対するネガティブテスト後に、Saleen がクラッシュする
CSCtv27382	Salesen の RDP および ICA プラグインの問題

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、次を参照してください：

<https://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN.html>

関連資料

ASA の追加情報については、*Cisco ASA シリーズ マニュアルのナビゲーション*を参照してください：

<http://www.cisco.com/en/US/docs/security/asa/roadmap/asaroadmap.html>

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカルサポート、マニュアルに関するフィードバックの提供、セキュリティガイドライン、および推奨エイリアスや一般的なシスコのマニュアルについては、次でアクセスでき、毎月更新される *What's New in Cisco Product Documentation* を参照してください。シスコの新規および改訂版の技術マニュアルのリストも示されています。

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html> [英語]

このドキュメントは、[関連資料](#)のセクションに掲載されているマニュアルと併せてご利用ください。

シスコおよびシスコのロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の国における登録商標または商標です。シスコの商標の一覧については、https://www.cisco.com/c/ja_jp/about/legal/trademarks.html をご覧ください。記載されているサードパーティの商標は、それぞれの所有者に帰属します。「パートナー」という言葉が使用されていても、シスコと他社の間にパートナーシップ関係が存在することを意味するものではありません。(1110R)。

このマニュアルで使用している IP アドレスは、実際のアドレスを示すものではありません。マニュアル内の例、コマンド出力、および図は、説明のみを目的として使用されています。説明の中に実際のアドレスが使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2012 Cisco Systems, Inc.

All rights reserved.