ソフトウェアおよびコンフィギュレーション

この章では、ASA ソフトウェアおよびコンフィギュレーションの管理方法について説明します。

ソフトウェアのアップグレード

完全なアップグレードの手順については、『Cisco ASA Upgrade Guide』を参照してください。

ROMMON を使用したイメージのロード（ISA 3000）

TFTP を使用して ROMMON モードから ASA へソフトウェア イメージをロードするには、次の手順を実行します。

手順

ステップ 1 ISA 3000 コンソールへのアクセスに従って、ASA のコンソール ポートに接続します。

ステップ 2 ASA の電源を切ってから、再び電源をオンにします。

ステップ 3 スタートアップの間に、ROMMONモードに入るようにプロンプト表示されたら、**Escape**キーを押します。

ステップ 4 ROMMON モードで、IP アドレス、TFTP サーバ アドレス、ゲートウェイ アドレス、ソフトウェア イメージ ファイル、およびポートを含む、ASA に対するインターフェイス設定を次のように定義します。

```
rommon #1> interface gigabitethernet0/0
rommon #2> address 10.86.118.4
rommon #3> server 10.86.118.21
rommon #4> gateway 10.86.118.21
rommon #5> file asa961-smp-k8.bin
```

（注） ネットワークへの接続がすでに存在することを確認してください。

インターフェイス コマンドは ASA 5506-X、ASA 5508-X、および ASA 5516-X プラットフォームで無視されるため、これらのプラットフォームでManagement 1/1 インターフェイスから TFTP リカバリを実行する必要があります。

ステップ 5 設定を検証します。

```
rommon #6> set
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=asa961-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20
```

ステップ 6 TFTP サーバーに ping を送信します。

```
rommon #7> ping server
Sending 20, 100-byte ICMP Echoes to server 10.86.118.21, timeout is 4 seconds:

Success rate is 100 percent (20/20)
```

ステップ 7 ネットワーク設定を、後で使用できるように保管しておきます。

```
rommon #8> sync
Updating NVRAM Parameters...
```

ステップ 8 システム ソフトウェア イメージをロードします。

```
rommon #9> tftpdnld
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
```

```
  GATEWAY=10.86.118.21
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=asa961-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

tftp asa961-smp-k8.bin@10.86.118.21 via 10.86.118.21

Received 14450688 bytes

Launching TFTP Image...
Cisco ASA Security Appliance admin loader (3.0) #0: Mon Mar 5 16:00:07 MST 2016

Loading...
```

ソフトウェア イメージが正常にロードされると、ASA は自動的に ROMMON モードを終了します。

ステップ 9 ROMMON モードから ASA を起動する場合、システム イメージはリロード間で保持されないため、やはりイメージをフラッシュ メモリにダウンロードする必要があります。ソフトウェアのアップグレード （1 ページ） を参照してください。

ROMMON イメージのアップグレード（ISA 3000）

ISA 3000 の ROMMON イメージをアップグレードするには、次の手順に従います。 ASA モデルの場合、システムの ROMMON バージョンは 1.1.8 以上である必要があります。最新バージョンへのアップグレードを推奨します。

新バージョンへのアップグレードのみ可能です。ダウングレードはできません。

⚠

注意 ISA 3000 の ROMMON 1.0.5 へのアップグレードには、以前の ROMMON バージョンの 2 倍の時間がかかります（約 15 分）。アップグレード中はデバイスの電源を**再投入しないでください**。アップグレードが 30 分以内に完了しないか、または失敗した場合は、シスコ テクニカル サポートに連絡してください。デバイスの電源を再投入したり、リセットしたり**しないでください**。

始める前に

Cisco.com から新しい ROMMON イメージを取得して、サーバー上に置いて ASA にコピーします。ASA は、FTP サーバー、TFTP サーバー、SCP サーバー、HTTP（S）サーバー、および SMB サーバーをサポートしています。次の URL からイメージをダウンロードします。

- ISA 3000： https://software.cisco.com/download/home/286288493/type

手順

ステップ 1 ROMMON イメージを ASA フラッシュ メモリにコピーします。この手順では、FTP コピーを表示します。他のサーバータイプのシンタックスの場合は **copy ?** と入力します。

copy ftp://[*username***:***password***@**]*server_ip*/**asa5500-firmware-***xxxx***.SPA disk0:asa5500-firmware-***xxxx***.SPA**

ステップ 2 現在のバージョンを確認するには、**show module** コマンドを入力して、MAC アドレス範囲テーブルの Mod 1 の出力で Fw バージョンを調べます。

```
ciscoasa# show module
[...]
Mod  MAC Address Range                 Hw Version   Fw Version   Sw Version
---- --------------------------------- ------------ ------------ ---------------
   1 7426.aceb.ccea to 7426.aceb.ccf2  0.3          1.1.5        9.4(1)
 sfr 7426.aceb.cce9 to 7426.aceb.cce9  N/A          N/A
```

ステップ 3 ROMMON イメージをアップグレードします。

upgrade rommon disk0:asa5500-firmware-*xxxx***.SPA**

例：

```
ciscoasa# upgrade rommon disk0:asa5500-firmware-1108.SPA
Verifying file integrity of disk0:/asa5500-firmware-1108.SPA

Computed Hash   SHA2: d824bdeecee1308fc64427367fa559e9
                      eefe8f182491652ee4c05e6e751f7a4f
                      5cdea28540cf60acde3ab9b65ff55a9f
                      4e0cfb84b9e2317a856580576612f4af

Embedded Hash   SHA2: d824bdeecee1308fc64427367fa559e9
                      eefe8f182491652ee4c05e6e751f7a4f
                      5cdea28540cf60acde3ab9b65ff55a9f
                      4e0cfb84b9e2317a856580576612f4af


Digital signature successfully validated
File Name                     : disk0:/asa5500-firmware-1108.SPA
Image type                    : Release
    Signer Information
        Common Name           : abraxas
        Organization Unit     : NCS_Kenton_ASA
        Organization Name     : CiscoSystems
    Certificate Serial Number : 553156F4
    Hash Algorithm            : SHA2 512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A
Verification successful.
Proceed with reload? [confirm]
```

ステップ 4 プロンプトが表示されたら、確認して ASA をリロードします。

ASAがROMMONイメージをアップグレードして、その後オペレーティングシステムをリロードします。

ソフトウェアのダウングレード

多くの場合、ASAソフトウェアをダウングレードし、以前のソフトウェアバージョンからバックアップ設定を復元することができます。ダウングレードの方法は、ASAプラットフォームによって異なります。

ダウングレードに関するガイドラインおよび制限事項

ダウングレードする前に、次のガイドラインを参照してください。

- **クラスタリング用の公式のゼロ ダウンタイム ダウングレードのサポートはありません**：ただし場合によっては、ゼロ ダウンタイム ダウングレードが機能します。ダウングレードに関する次の既知の問題を参照してください。この他の問題が原因でクラスタユニットのリロードが必要になることもあり、その場合はダウンタイムが発生します。
  - **クラスタリングを含む9.9(1)より前のリリースへのダウングレード**：9.9(1)以降では、バックアップの配布が改善されています。クラスタに3つ以上のユニットがある場合は、次の手順を実行する必要があります。
    1. クラスタからすべてのセカンダリユニットを削除します（クラスタはプライマリユニットのみで構成されます）。
    2. 1つのセカンダリ ユニットをダウングレードし、クラスタに再参加させます。
    3. プライマリユニットでクラスタリングを無効にします。そのユニットをダウングレードし、クラスタに再参加させます。
    4. 残りのセカンダリ ユニットをダウングレードし、それらを一度に1つずつクラスタに再参加させます。
  - **クラスタサイトの冗長性を有効にする場合は、9.9(1)より前のリリースにダウングレードします**：ダウングレードする場合（または9.9(1)より前のユニットをクラスタに追加する場合）は、サイトの冗長性を無効にする必要があります。そうしないと、古いバージョンを実行しているユニットにダミーの転送フローなどの副作用が発生します。
  - **クラスタリングおよび暗号マップを使用する場合に9.8(1)からダウングレードする**：暗号マップが設定されている場合に9.8(1)からダウングレードすると、ゼロ ダウンタイム ダウングレードはサポートされません。ダウングレード前に暗号マップ設定をクリアし、ダウングレード後に設定をもう一度適用する必要があります。
  - **クラスタリングユニットのヘルスチェックを0.3 ～ 0.7秒に設定した状態で9.8(1)からダウングレードする**：（**health-check holdtime** で）ホールド時間を0.3 ～ 0.7秒に設

定した後で ASA ソフトウェアをダウングレードすると、新しい設定はサポートされないため、設定値はデフォルトの 3 秒に戻ります。

- **クラスタリング（CSCuv82933）を使用している場合に 9.5(2) 以降から 9.5(1) 以前にダウングレードする**：9.5(2) からダウングレードする場合、ゼロ ダウンタイム ダウングレードはサポートされません。ユニットがオンラインに戻ったときに新しいクラスタが形成されるように、すべてのユニットをほぼ同時にリロードする必要があります。ユニットが順番にリロードされるのを待つと、クラスタを形成できなくなります。
- **クラスタリングを使用する場合に 9.2(1) 以降から 9.1 以前にダウングレードする**：ゼロ ダウンタイム ダウングレードはサポートされません。

- **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。
- プラットフォームモードでの 9.13/9.14 から 9.12 以前への Firepower 2100 のダウングレードの問題：プラットフォームモードに変換した 9.13 または 9.14 を新規インストールした Firepower 2100 の場合：9.12 以前にダウングレードすると、FXOS で新しいインターフェイスの設定や、既存インターフェイスの編集ができなくなります（9.12 以前ではプラットフォームモードのみがサポートされています）。バージョンを 9.13 以降に戻すか、または FXOS の erase configuration コマンドを使用して設定をクリアする必要があります。この問題は、元々以前のリリースから 9.13 または 9.14 にアップグレードした場合は発生しません。新しいデバイスや再イメージ化されたデバイスなど、新規インストールのみが影響を受けます。（CSCvr19755）
- **スマートライセンスの 9.10(1) からのダウングレード**：スマートエージェントの変更により、ダウングレードする場合、デバイスを Cisco Smart Software Manager に再登録する必要があります。新しいスマートエージェントは暗号化されたファイルを使用するので、古いスマートエージェントが必要とする暗号化されていないファイルを使用するために再登録する必要があります。
- **PBKDF2（パスワードベースのキー派生関数 2）ハッシュをパスワードで使用する場合に 9.5 以前のバージョンにダウングレードする**：9.6 より前のバージョンは PBKDF2 ハッシュをサポートしていません。9.6(1) では、32 文字より長い **enable** パスワードおよび **username** パスワードで PBKDF2 ハッシュを使用します。9.7(1) では、すべての新しいパスワードは、長さに関わらず PBKDF2 ハッシュを使用します（既存のパスワードは引き続き MD5 ハッシュを使用します）。ダウングレードすると、**enable** パスワードがデフォルト（空白）に戻ります。ユーザー名は正しく解析されず、**username** コマンドが削除されます。ローカル ユーザーをもう一度作成する必要があります。
- **ASA 仮想 用のバージョン 9.5(2.200) からのダウングレード**：ASA 仮想 はライセンス登録状態を保持しません。**license smart register idtoken id_token force** コマンドで再登録する必要があります（ASDM の場合、[Configuration] > [Device Management] > [Licensing] > [Smart

Licensing] ページで [Force registration] オプションを使用）。Smart Software Manager から ID トークンを取得します。

- **元のトンネルがネゴシエートした暗号スイートをサポートしないソフトウェアバージョンをスタンバイ装置が実行している場合でも、VPN トンネルがスタンバイ装置に複製されます**：このシナリオは、ダウングレード時に発生します。その場合、VPN接続を切断して再接続してください。

ダウングレード後に削除される互換性のない設定

以前のバージョンにダウングレードすると、それ以降のバージョンで導入されたコマンドは設定から削除されます。ダウングレードする前に、ターゲットバージョンに対して設定を自動的にチェックする方法はありません。新しいコマンドが ASA の新しい機能にいつ追加されたかをリリースごとに表示できます。

show startup-config errors コマンドを使用してダウングレードした後、拒否されたコマンドを表示できます。ラボデバイスでダウングレードを実行できる場合は、実稼働デバイスでダウングレードを実行する前にこのコマンドを使用して効果を事前に確認できます。

場合によっては、ASAはアップグレード時にコマンドを新しいフォームに自動的に移行するため、バージョンによっては新しいコマンドを手動で設定しなかった場合でも、設定の移行によってダウングレードが影響を受けることがあります。ダウングレード時に使用できる古い設定のバックアップを保持することを推奨します。8.3 へのアップグレード時には、バックアップが自動的に作成されます（<old_version>_startup_cfg.sav）。他の移行ではバックアップが作成されません。ダウングレードに影響する可能性がある自動コマンド移行の詳細については、『ASAアップグレードガイド』の「バージョン固有のガイドラインと移行」を参照してください。

ダウングレードに関するガイドラインおよび制限事項 （5 ページ）の既知のダウングレードの問題も参照してください。

たとえば、バージョン9.8(2) を実行している ASA には、次のコマンドが含まれています。

```
access-list acl1 extended permit sctp 192.0.2.0 255.255.255.0 198.51.100.0 255.255.255.0
username test1 password $sha512$1234$abcdefghijklmnopqrstuvwxyz privilege 15
snmp-server user snmpuser1 snmpgroup1 v3 engineID abcdefghijklmnopqrstuvwxyz encrypted
auth md5 12:ab:34 priv aes 128 12:ab:34
```

9.0(4) にダウングレードすると、起動時に次のエラーが表示されます。

```
access-list acl1 extended permit sctp 192.0.2.0 255.255.255.0 198.51.100.0 255.255.255.0

                                    ^
ERROR: % Invalid input detected at '^' marker.

username test1 password $sha512$1234$abcdefghijklmnopqrstuvwxyz pbkdf2 privilege 15
                                                                ^
ERROR: % Invalid input detected at '^' marker.

snmp-server user snmpuser1 snmpgroup1 v3 engineID abcdefghijklmnopqrstuvwxyz encrypted
auth md5 12:ab:34 priv aes 128 12:ab:34
```

```
                                                ^
ERROR: % Invalid input detected at '^' marker.
```

この例では、**access-list extended** コマンドでの **sctp** のサポートがバージョン 9.5(2) で、**username** コマンドでの **pbkdf2** のサポートがバージョン 9.6(1) で、**snmp-server user** コマンドでの **engineID** のサポートがバージョン9.5(3) で追加されました。

Firepower 1000、2100（アプライアンスモード）、Cisco Secure Firewall 3100 のダウングレード

ASA のバージョンを古いバージョンに設定し、バックアップ設定をスタートアップ コンフィギュレーションに復元してからリロードすることによって、ASA ソフトウェアのバージョンをダウングレードすることができます。

始める前に

この手順ではアップグレードする前に ASA のバックアップ設定を行う必要があるため、古い設定を復元することができます。古い設定を復元しない場合は、新規または変更された機能を表す互換性のないコマンドが存在する可能性があります。新しいコマンドは、ソフトウェアの古いバージョンをロードすると拒否されます。

手順

ステップ 1 スタンドアロン、フェールオーバー、またはクラスタリング展開のために、『ASA Upgrade Guide』のアップグレード手順を使用して、ASA ソフトウェアの古いバージョンをロードします。この場合は、ASA の新しいバージョンではなく、古いバージョンを指定します。**重要**：まだ ASAをリロードしないでください。

ステップ 2 ASA CLI で、バックアップの ASA 設定をスタートアップ コンフィギュレーションにコピーします。フェールオーバーの場合は、アクティブユニットでこの手順を実行します。この手順では、コマンドをスタンバイ装置に複製します。

copy *old_config_url* **startup-config**

write memory を使用して実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存しないことが重要です。このコマンドは、バックアップ設定を上書きします。

例：

```
ciscoasa# copy disk0:/9.13.1_cfg.sav startup-config
```

ステップ 3 ASA をリロードします。

ASA CLI

reload

ASDM

[Tools] > **[System Reload]** を選択します。

プラットフォームモードでの Firepower 2100 のダウングレード

バックアップ設定をスタートアップ コンフィギュレーションに復元し、ASA のバージョンを古いバージョンに設定してからリロードすることによって、ASA ソフトウェアのバージョンをダウングレードすることができます。

始める前に

この手順ではアップグレードする前に ASA のバックアップ設定を行う必要があるため、古い設定を復元することができます。古い設定を復元しない場合は、新規または変更された機能を表す互換性のないコマンドが存在する可能性があります。新しいコマンドは、ソフトウェアの古いバージョンをロードすると拒否されます。

手順

ステップ 1 ASA CLI で、バックアップの ASA 設定をスタートアップ コンフィギュレーションにコピーします。フェールオーバーの場合は、アクティブユニットでこの手順を実行します。この手順では、コマンドをスタンバイ装置に複製します。

copy *old_config_url* **startup-config**

write memory を使用して実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存しないことが重要です。このコマンドは、バックアップ設定を上書きします。

例：

```
ciscoasa# copy disk0:/9.12.4_cfg.sav startup-config
```

ステップ 2 FXOS では、スタンドアロン、フェールオーバー、あるいはクラスタリング展開のために、Chassis Manager または FXOS CLI を使用し、『ASA Upgrade Guide』のアップグレード手順に従って ASA ソフトウェアの古いバージョンを使います。この場合は、ASA の新しいバージョンではなく、古いバージョンを指定します。

Firepower 4100/9300 のダウングレード

バックアップ設定をスタートアップ コンフィギュレーションに復元し、ASA のバージョンを古いバージョンに設定してからリロードすることによって、ASA ソフトウェアのバージョンをダウングレードすることができます。

始める前に

- この手順ではアップグレードする前に ASA のバックアップ設定を行う必要があるため、古い設定を復元することができます。古い設定を復元しない場合は、新規または変更された機能を表す互換性のないコマンドが存在する可能性があります。新しいコマンドは、ソフトウェアの古いバージョンをロードすると拒否されます。
- ASA の古いバージョンが、FXOS の現在のバージョンと互換性があることを確認します。互換性がない場合は、古い ASA 設定を復元する前に最初の手順として FXOS をダウングレードします。ダウングレードされた FXOS も、（ダウングレードする前に）ASA の現在のバージョンと互換性があることを確認してください。互換性を実現できない場合は、ダウングレードを実行しないことをお勧めします。

手順

ステップ 1 ASA CLI で、バックアップの ASA 設定をスタートアップ コンフィギュレーションにコピーします。フェールオーバーまたはクラスタリングの場合は、アクティブ/制御ユニットでこの手順を実行します。この手順では、コマンドをスタンバイ/データユニットに複製します。

copy *old_config_url* **startup-config**

write memory を使用して実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存しないことが重要です。このコマンドは、バックアップ設定を上書きします。

例：

```
ciscoasa# copy disk0:/9.8.4_cfg.sav startup-config
```

ステップ 2 FXOS では、スタンドアロン、フェールオーバー、あるいはクラスタリング展開のために、Chassis Manager または FXOS CLI を使用し、『ASA Upgrade Guide』のアップグレード手順に従って ASA ソフトウェアの古いバージョンを使います。この場合は、ASA の新しいバージョンではなく、古いバージョンを指定します。

ステップ 3 また、FXOS をダウングレードする場合は、スタンドアロン、フェールオーバー、あるいはクラスタリング展開のために、Chassis Manager または FXOS CLI を使用し、『ASA Upgrade Guide』のアップグレード手順に従って FXOS ソフトウェアの古いバージョンを最新のバージョンに設定します。

ISA 3000 のダウングレード

ダウングレードでは、ISA 3000 モデルで以下の機能を完了するためのショートカットが存在します。

- ブート イメージ コンフィギュレーションのクリア（**clear configure boot**）。
- 古いイメージへのブート イメージの設定（**boot system**）。

- （オプション）新たなアクティベーション キーの入力（**activation-key**）。
- 実行コンフィギュレーションのスタートアップへの保存（**write memory**）。これにより、BOOT環境変数を古いイメージに設定します。このため、リロードすると古いイメージがロードされます。
- 古いコンフィギュレーションのバックアップをスタートアップ コンフィギュレーションにコピーします（**copy** *old_config_ur* **startup-config**）。
- リロード（**reload**）。

始める前に

- この手順ではアップグレードする前に ASA のバックアップ設定を行う必要があるため、古い設定を復元することができます。

手順

ステップ 1 **[Tools]** > **[Downgrade Software]** を選択します。

[Downgrade Software] ダイアログボックスが表示されます。

ステップ 2 ASA イメージの場合、[Select Image File] をクリックします。

[Browse File Locations] ダイアログボックスが表示されます。

ステップ 3 次のいずれかのオプション ボタンをクリックします。

- [Remote Server]：ドロップダウン リストで [ftp]、[smb]、[http] のいずれかを選択し、以前のイメージ ファイルのパスを入力します。
- [Flash File System]：[Browse Flash] をクリックして、ローカル フラッシュ ファイル システムにある以前のイメージ ファイルを選択します。

ステップ 4 [Configuration] で [Browse Flash] をクリックし、移行前の設定ファイルを選択します。

ステップ 5 （任意） バージョン 8.3 よりも前のアクティベーション キーに戻す場合は、[Activation Key] フィールドで以前のアクティベーション キーを入力します。

ステップ 6 [Downgrade] をクリックします。

ファイルの管理

ASDM には、基本的なファイル管理タスクを実行するのに便利なファイル管理ツール セットが用意されています。ファイル管理ツールにより、フラッシュ メモリに保存されているファイルの表示、移動、コピー、および削除、ファイルの転送、およびリモート ストレージ デバイス（マウント ポイント）のファイルの管理を行うことができます。

（注） マルチコンテキスト モードの場合、このツールはシステムのセキュリティ コンテキストでだけ使用できます。

ファイル アクセスの設定

ASA では、FTP クライアント、セキュア コピー クライアント、または TFTP クライアントを使用できます。また、ASA をセキュア コピー サーバーとして設定することもできるため、コンピュータでセキュア コピー クライアントを使用できます。

FTP クライアント モードの設定

ASA では、FTP サーバーとの間で、イメージ ファイルやコンフィギュレーション ファイルのアップロードおよびダウンロードを実行できます。パッシブ FTP では、クライアントは制御接続およびデータ接続の両方を開始します。パッシブ モードではデータ接続の受け入れ側となるサーバーは、今回の特定の接続においてリッスンするポート番号を応答として返します。

手順

ステップ 1 [Configuration] > [Device Management] > [Management Access] > [File Access] > [FTP Client] ペインで、[Specify FTP mode as passive] チェックボックスをオンにします。

ステップ 2 [Apply] をクリックします。

FTP クライアントのコンフィギュレーションが変更され、その変更内容が実行コンフィギュレーションに保存されます。

セキュア コピー サーバーとしての ASA の設定

ASA 上でセキュア コピー（SCP）サーバーをイネーブルにできます。SSH による ASA へのアクセスを許可されたクライアントだけが、セキュア コピー接続を確立できます。

始める前に

- サーバーにはディレクトリ サポートがありません。ディレクトリ サポートがないため、ASA の内部ファイルへのリモート クライアント アクセスは制限されます。
- サーバーでは、バナーまたはワイルドカードがサポートされていません。
- ASDM、その他のクライアントの HTTPS アクセスの設定 に従って、ASA で SSH を有効にします。
- SSH バージョン 2 接続をサポートするには、ASA のライセンスに強力な暗号化（3DES/AES）ライセンスが必要です。

- 特に指定されていないかぎり、マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。まだシステム コンフィギュレーション モードに入っていない場合、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。
- セキュア コピーのパフォーマンスは、使用する暗号化アルゴリズムにある程度依存します。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。提示された暗号方式を変更するには、**[Configuration]** > **[Device Management]** > **[Advanced]** > **[SSH Ciphers]** ペインを使用します。たとえば、**[Custom]** を選択して aes128-cbc に設定します。

手順

ステップ 1 コンテキスト モードによって次のように異なります。

- シングル モードの場合、[Configuration] > [Device Management] > [Management Access] > [File Access] > [Secure Copy (SCP)] の順に選択します。
- マルチ モードの場合、[Configuration] > [Device Management] > [Device Administration] > [Secure Copy] の順に選択します。

ステップ 2 [Enable secure copy server] チェック ボックスをオンにします。

ステップ 3 （オプション）ASA は接続先の各 SCP サーバーの SSH ホストキーを保存します。必要に応じて、ASA データベースから手動でサーバとそのキーを追加または削除できます。

キーを追加するには、次の手順を実行します。

a) 新しいサーバーの [Add] をクリックするか、または信頼できる SSH ホストのテーブルからサーバーを選択し、[Edit] をクリックします。
b) 新しいサーバーの [Host] フィールドに、サーバーの IP アドレスを入力します。
c) [Add public key for the trusted SSH host] チェックボックスをオンにします。
d) 次のいずれかのキーを指定します。

- フィンガープリント：すでにハッシュされているキーを入力します。たとえば、**show** コマンドの出力からコピーしたキーです。
- キー：SSH ホストの公開キーまたはハッシュ値を入力します。キー ストリングはリモート ピアの Base64 で符号化された RSA 公開キーです。オープン SSH クライアントから（言い換えると .ssh/id_rsa.pub ファイルから）公開キー値を取得できます。Base64 で符号化された公開キーを送信した後、SHA-256 によってそのキーがハッシュされます。

キーを削除するには、信頼できる SSH ホストのテーブルからサーバーを選択し、[Delete] をクリックします。

ステップ 4 （オプション）新しいホストキーが検出されたときに通知を受け取るには、[Inform me when a new host key is detected] チェックボックスをオンにします。

デフォルトで、このオプションは有効になっています。このオプションがイネーブルになっている場合、ASA にまだ格納されていないホストキーを許可または拒否するように求められます。このオプションがディセーブルになっている場合、ASA は過去に保存されたことがないホストキーを自動的に許可します。

ステップ 5 [適用（Apply）] をクリックします。

例

外部ホストのクライアントから、SCP ファイル転送を実行します。たとえば、Linux では次のコマンドを入力します。

scp -v -pw *password* [*path*/]*source_filename* *username@asa_address*:{**disk0**|**disk1**}:/[*path*/]*dest_filename*

-v は冗長を表します。**-pw** が指定されていない場合は、パスワードの入力を求めるプロンプトが表示されます。

ASA TFTP クライアントのパス設定

TFTP は、単純なクライアント/サーバー ファイル転送プロトコルで、RFC 783 および RFC 1350 Rev. 2 で規定されています。TFTP サーバーとの間でファイルをコピーできるように、ASA を TFTP クライアントとして設定できます。これにより、コンフィギュレーション ファイルをバックアップし、それらを複数の ASA にプロパゲートできます。

ここでは、TFTP サーバーへのパスを事前定義できるため、**copy** および **configure net** などのコマンドで入力する必要がなくなります。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[File Access]** > **[TFTP Client]** の順に選択し、[Enable] チェックボックスをオンにします。

ステップ 2 [Interface Name] ドロップダウン リストから、TFTP クライアントとして使用するインターフェイスを選択します。

ステップ 3 コンフィギュレーション ファイルの保存先とする TFTP サーバーの IP アドレスを [IP Address] フィールドに入力します。

ステップ 4 コンフィギュレーション ファイルの保存先とする TFTP サーバーへのパスを [Path] フィールドに入力します。

例：/tftpboot/asa/config3

ステップ 5 **Apply** をクリックします。

マウント ポイントの追加

CIFS マウント ポイントまたは FTP マウント ポイントを追加できます。

CIFS マウント ポイントの追加

共通インターネット ファイル システム（CIFS）マウント ポイントを定義するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[File Access]** > **[Mount-Points]** の順に選択し、**[Add]** > **[CIFS Mount Point]** の順にクリックします。

[Add CIFS Mount Point] ダイアログボックスが表示されます。

ステップ 2 [Enable mount point] チェックボックスをオンにします。

これにより、ASA 上の CIFS ファイル システムが UNIX のファイル ツリーに接続されます。

ステップ 3 [Mount Point Name] フィールドに、既存の CIFS が存在する位置の名前を入力します。

ステップ 4 [Server Name] フィールドまたは [IP Address] フィールドに、マウント ポイントを配置するサーバーの名前または IP アドレスを入力します。

ステップ 5 [Share Name] フィールドに、CIFS サーバー上のフォルダの名前を入力します。

ステップ 6 [NT Domain Name] フィールドに、サーバーが常駐する NT ドメインの名前を入力します。

ステップ 7 サーバーに対するファイル システムのマウントを認可されているユーザーの名前を、[User Name] フィールドに入力します。

ステップ 8 サーバーに対するファイル システムのマウントを認可されているユーザーのパスワードを、[Password] フィールドに入力します。

ステップ 9 [Confirm Password] フィールドにパスワードを再入力します。

ステップ 10 [OK] をクリックします。

[Add CIFS Mount Point] ダイアログボックスが閉じます。

ステップ 11 [Apply] をクリックします。

FTP マウント ポイントの追加

FTP マウント ポイントの場合、FTP サーバーには UNIX のディレクトリ リスト スタイルが必要です。Microsoft FTP サーバーには、デフォルトで MS-DOS ディレクトリ リスト スタイルがあります。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[File Access]** > **[Mount-Points]** の順に選択し、**[Add]** > **[FTP Mount Point]** の順にクリックします。

[Add FTP Mount Point] ダイアログボックスが表示されます。

ステップ 2 [Enable] チェックボックスを選択します。

これにより、ASA 上の FTP ファイル システムが UNIX のファイル ツリーに接続されます。

ステップ 3 [Mount Point Name] フィールドに、既存の FTP が存在する位置の名前を入力します。

ステップ 4 [Server Name] フィールドまたは [IP Address] フィールドに、マウント ポイントを配置するサーバーの名前または IP アドレスを入力します。

ステップ 5 [Mode] フィールドで、オプション ボタン（[Active] または [Passive]）をクリックして FTP モードを選択します。[Passive] モードを選択した場合、クライアントでは、FTP コントロール接続とデータ接続がともに起動します。サーバーは、この接続をリッスンするポートの番号で応答します。

ステップ 6 FTP ファイル サーバへのディレクトリ パス名を [Path to Mount] フィールドに入力します。

ステップ 7 サーバーに対するファイル システムのマウントを認可されているユーザーの名前を、[User Name] フィールドに入力します。

ステップ 8 サーバーに対するファイル システムのマウントを認可されているユーザーのパスワードを、[Password] フィールドに入力します。

ステップ 9 [Confirm Password] フィールドにパスワードを再入力します。

ステップ 10 [OK] をクリックします。

[Add FTP Mount Point] ダイアログボックスが閉じます。

ステップ 11 [Apply] をクリックします。

ファイル管理ツールへのアクセス

ファイル管理ツールを使用するには、次の手順を実行します。

手順

ステップ 1 メイン ASDM アプリケーション ウィンドウで、**[Tools]** > **[File Management]** の順に選択します。

[File Management] ダイアログボックスが表示されます。

- [Folders] ペインには、ディスク上にあるフォルダが表示されます。
- [Flash Space] は、フラッシュ メモリの合計容量と、使用可能なメモリ容量を示します。

- [Files] 領域には、選択したフォルダのファイルについて次の情報が表示されます。
  - パス
  - ファイル名
  - サイズ（バイト単位）
  - 修正時刻
  - 選択したファイルの種類（ブート コンフィギュレーション、ブート イメージ ファイル、ASDM イメージ ファイル、SVC イメージ ファイル、CSD イメージ ファイル、または APCF イメージ ファイル）を示す、ステータス

ステップ 2 選択したファイルをブラウザに表示するには、[View] をクリックします。

ステップ 3 選択したファイルを切り取って別のディレクトリに貼り付けるには、[Cut] をクリックします。

ステップ 4 選択したファイルをコピーして別のディレクトリに貼り付けるには、[Copy] をクリックします。

ステップ 5 コピーしたファイルを選択した場所に貼り付けるには、[Paste] をクリックします。

ステップ 6 選択したファイルをフラッシュ メモリから削除するには、[Delete] をクリックします。

ステップ 7 ファイルの名前を変更するには、[Rename] をクリックします。

ステップ 8 ファイルを保存するディレクトリを新規作成するには、[New Directory] をクリックします。

ステップ 9 [File Transfer] ダイアログボックスを開くには、[File Transfer] をクリックします。詳細については、「ファイルの転送 （17 ページ）」を参照してください。

ステップ 10 [Manage Points] ダイアログボックスを開くには、[Mount Points] をクリックします。詳細については、マウント ポイントの追加 （15 ページ）を参照してください。

ファイルの転送

File Transfer ツールにより、ローカルにあるファイルとリモートにあるファイルを転送できます。PC またはフラッシュ ファイル システムのローカル ファイルを ASA との間で転送できます。HTTP、HTTPS、TFTP、FTP、または SMB を使用して、ASA との間でファイルを転送できます。

（注） IPS SSP ソフトウェア モジュールの場合、IPS ソフトウェアを disk0 にダウンロードする前に、フラッシュ メモリに少なくとも 50% の空きがあることを確認してください。IPS をインストールするときに、IPS のファイル システム用に内部フラッシュ メモリの 50% が予約されます。

ローカル PC とフラッシュ間でのファイル転送

ローカル PC とフラッシュ ファイル システムとの間でファイルを転送するには、次の手順を実行します。

手順

ステップ 1 メイン ASDM アプリケーション ウィンドウで、**[Tools]** > **[File Management]** の順に選択します。

[File Management] ダイアログボックスが表示されます。

ステップ 2 [File Transfer] の横にある下矢印をクリックし、続いて [Between Local PC and Flash] をクリックします。

[File Transfer] ダイアログボックスが表示されます。

ステップ 3 ローカル PC またはフラッシュ ファイル システムのどちらかで、アップロードまたはダウンロードしたいファイルを選択し、目的の場所にドラッグします。または、ローカル PC またはフラッシュ ファイル システムのどちらかで、アップロードまたはダウンロードしたいファイルを選択し、右矢印または左矢印をクリックし、目的の場所にファイルを転送します。

ステップ 4 完了したら [Close] をクリックします。

リモート サーバーとフラッシュ間でのファイル転送

リモート サーバーとフラッシュ ファイル システムとの間でファイルを転送するには、次の手順を実行します。

手順

ステップ 1 メイン ASDM アプリケーション ウィンドウで、**[Tools]** > **[File Management]** の順に選択します。

[File Management] ダイアログボックスが表示されます。

ステップ 2 [File Transfer] ドロップダウン リストで下矢印をクリックし、[Between Remote Server and Flash] をクリックします。

[File Transfer] ダイアログボックスが表示されます。

ステップ 3 リモート サーバーからファイルを転送するには、[Remote server] オプションをクリックします。

ステップ 4 転送対象になるソース ファイルを定義します。

a) （オプション）ASAがサーバーとの通信に使用するインターフェイスを指定します。インターフェイスを指定しない場合、ASA は管理専用のルーティング テーブルをチェックします。ここで一致が見つからない場合はデータのルーティング テーブルをチェックします。

b) サーバーの IP アドレスを含めたファイルの場所へのパスを選択します。

（注） ファイル転送は IPv4 および IPv6 のアドレスをサポートしています。

c) FTP の場合はリモート サーバーのタイプを、HTTP または HTTPS の場合はリモート サーバーのポート番号を入力します。有効な FTP タイプは次のとおりです。

- ap：パッシブ モードの ASCII ファイル
- an：非パッシブ モードの ASCII ファイル
- ip：パッシブ モードのバイナリ イメージ ファイル
- in：非パッシブ モードのバイナリ イメージ ファイル

ステップ 5 フラッシュ ファイル システムからファイルを転送するには、[Flash file system] オプションを選択します。

ステップ 6 ファイルの場所へのパスを入力するか、[Browse Flash] をクリックしてファイルの場所を指定します。

ステップ 7 また、CLI により、スタートアップ コンフィギュレーション、実行コンフィギュレーション、または SMB ファイル システムからファイルをコピーすることもできます。**Copy** コマンドの使用方法については、CLI コンフィギュレーション ガイドを参照してください。

ステップ 8 転送するファイルの宛先を定義します。

a) フラッシュ ファイル システムにファイルを転送するには、[Flash file system] オプションを選択します。
b) ファイルの場所へのパスを入力するか、[Browse Flash] をクリックしてファイルの場所を指定します。

ステップ 9 リモート サーバーにファイルを転送するには、[Remote server] オプションを選択します。

a) （オプション）ASA がサーバーとの通信に使用するインターフェイスを指定します。インターフェイスを指定しない場合、ASA は管理専用のルーティング テーブルをチェックします。ここで一致が見つからない場合はデータのルーティング テーブルをチェックします。
b) ファイルの場所へのパスを入力します。
c) FTP 転送の場合はタイプを入力します。有効なタイプは次のとおりです。

- ap：パッシブ モードの ASCII ファイル
- an：非パッシブ モードの ASCII ファイル
- ip：パッシブ モードのバイナリ イメージ ファイル
- in：非パッシブ モードのバイナリ イメージ ファイル

ステップ 10 [Transfer] をクリックしてファイル転送を開始します。

[Enter Username and Password] ダイアログボックスが表示されます。

ステップ 11 リモート サーバーのユーザー名、パスワード、ドメイン（必要な場合）が表示されます。

ステップ 12 [OK] をクリックし、ファイル転送を続行します。

ファイル転送プロセスには数分かかる場合があります。必ず終了するまでお待ちください。

ステップ 13 ファイル転送が完了したら [Close] をクリックします。

ASA イメージ、ASDM、およびスタートアップ コンフィギュレーションの設定

複数の ASA または ASDM イメージがある場合は、ブートするイメージを指定する必要があります。イメージを設定しない場合はデフォルトのブートイメージが使用され、そのイメージは意図されたものではない可能性があります。スタートアップ コンフィギュレーションでは、コンフィギュレーション ファイルを任意で指定できます。

次のモデルのガイドラインを参照してください。

- Firepower 4100/9300 シャーシ：ASA のアップグレードは FXOS によって管理されます。ASA オペレーティング システム内で ASA をアップグレードすることはできないため、ASA イメージに対してこの手順を使用しないでください。ASA と FXOS は個別にアップグレードでき、FXOSディレクトリリストに別々に表示されます。ASAパッケージには必ず ASDM が含まれています。
- プラットフォーム モードの Firepower 2100：ASA、ASDM、および FXOS のイメージは 1 つのパッケージに一緒にバンドルされています。パッケージの更新はFXOSによって管理されます。ASA オペレーティング システム内で ASA をアップグレードすることはできないため、ASA イメージに対してこの手順を使用しないでください。ASA と FXOS は個別にアップグレードできません。常に一緒にバンドルされています。
- Firepower 1000、アプライアンスモードの 2100、Cisco Secure Firewall 3100：ASA、ASDM、および FXOS のイメージは 1 つのパッケージに一緒にバンドルされています。パッケージの更新は、次の手順を使用して ASA によって管理されます。これらのプラットフォームでは、ブートするイメージを識別するために ASA が使用されますが、基盤となるメカニズムはレガシー ASA とは異なります。詳細については、以下のコマンドの説明を参照してください。
- モデルの ASDM：ASDM は ASA オペレーティングシステム内からアップグレードできるため、バンドルされたASDMイメージのみを使用する必要はありません。プラットフォームモードの Firepower 2100 ではFirepower 4100/9300、手動でアップロードする ASDM イメージは FXOS イメージリストに表示されません。ASA から ASDM イメージを管理する必要があります。

（注） ASA バンドルをアップグレードすると、同じ名前（**asdm.bin**）であるため、バンドル内の ASDM イメージが ASA 上の前の ASDM バンドルイメージに置き換わります。ただし、アップロードした別の ASDM イメージ（たとえば **asdm-782.bin**）を手動で選択すると、バンドルアップグレード後も引き続き同じイメージが使用されます。互換性のある ASDM バージョンを実行していることを確認するには、バンドルをアップグレードする前に ASDM をアップグレードするか、または ASA バンドルをアップグレードする直前に、バンドルされた ASDM イメージ（**asdm.bin**）を使用するように ASA を再設定する必要があります。

- ASA 仮想：初期導入時の ASA 仮想 パッケージでは、ASA イメージが読み取り専用 boot:/ パーティションに配置されます。ASA 仮想 をアップグレードする際は、フラッシュメモリ内の別のイメージを指定します。後でコンフィギュレーションをクリアすると、ASA 仮想は元の展開のイメージをロードするようになることに注意してください。初期導入時の ASA 仮想 パッケージには、フラッシュメモリに配置される ASDM イメージも含まれています。ASDM イメージを個別にアップグレードできます。

次のデフォルト設定を参照してください。

- ASA イメージ：
  - Firepower 1000、アプライアンスモードの 2100、Cisco Secure Firewall 3100：以前実行していたブートイメージをブートします。
  - その他の物理 ASA：内部フラッシュ メモリ内で見つかった最初のアプリケーションイメージをブートします。
  - ASA 仮想：最初に展開したときに作成された、読み取り専用の boot:/ パーティションにあるイメージをブートします。
  - Firepower 4100/9300 シャーシ：どの ASA イメージをブートするかは FXOS システムによって決定されます。この手順を使用して ASA イメージを設定することはできません。
  - プラットフォーム モードの Firepower 2100：どの ASA/FXOS パッケージをブートするかは FXOS システムによって決定されます。この手順を使用して ASA イメージを設定することはできません。
- すべての ASA 上の ASDM イメージ：内部フラッシュ メモリ内で見つかった（この場所にイメージがない場合は外部フラッシュ メモリ内で見つかった）最初の ASDM イメージをブートします。
- スタートアップ コンフィギュレーション：デフォルトで、ASA は、隠しファイルであるスタートアップ コンフィギュレーションからブートします。

手順

ステップ 1 **[設定（Configuration）] > [デバイス管理（Device Management）] > [システム イメージ/設定（System Image/Configuration）] > [ブート イメージ/設定（Boot Image/Configuration）]** を選択します。

Firepower 1000、アプライアンスモードの 2100、Cisco Secure Firewall 3100：1 つのイメージのみ追加できます。新しいイメージにアップグレードする場合は、以前に設定したイメージを削除する必要があります。この変更を適用すると、システムによってアクションが実行されます。システムはイメージを検証して解凍し、ブート場所 (FXOS によって管理される disk0 の内部ロケーション) にコピーします。ASA をリロードすると、新しいイメージがロードされます。リロードする前に注意してください。**ブートイメージの場所**を削除して再適用すると、ブートロケーションから新しいイメージを削除できます。そのため、現在のイメージは引き続き実行されます。この変更を適用した後、ASA のフラッシュメモリから元のイメージファイルを削除することもできます。また、ASA はブート場所から正しく起動します。他のモデルとは異なり、スタートアップコンフィギュレーション内のこのコマンドは、ブートイメージには影響しません。リロード時には、最後にロードされたブートイメージが常に実行されます。Cisco ダウンロードサイトからロードできるのは、元のファイル名のイメージのみです。ファイル名を変更した場合はロードされません。

他のモデル：起動イメージとして使用するバイナリ イメージ ファイルは、ローカルから 4 つまで指定できます。また TFTP サーバーのイメージを 1 つ指定して、そこからデバイスをブートできます。TFTP サーバーに格納されているイメージを指定する場合は、そのファイルをリスト内の先頭に配置する必要があります。デバイスが、イメージのロード元の TFTP サーバに到達できない場合は、フラッシュ メモリに保存されているリスト内の次のイメージ ファイルのロードが試行されます。

ステップ 2 [ブート イメージ/設定（Boot Image/Configuration）] ペインで [追加（Add）] をクリックします。

ステップ 3 ブートするイメージを参照します。TFTP イメージの場合は、[ファイル名（File Name）] フィールドに TFTP URL を入力します。[OK] をクリックします。

ステップ 4 [上へ移動（Move Up）] ボタンと [下へ移動（Move Down）] ボタンを使用してイメージの順番を並べ替えます。

ステップ 5 （オプション）[ブート設定ファイル パス（Boot Configuration File Path）] フィールドで、[フラッシュを参照（Browse Flash）] をクリックしてコンフィギュレーションを選択してスタートアップ コンフィギュレーション ファイルを指定します。[OK] をクリックします。

ステップ 6 [ASDM イメージ ファイル パス（ASDM Image File Path）] フィールドで、[フラッシュを参照（Browse Flash）] をクリックしてイメージを選択して ASDM イメージを指定します。[OK] をクリックします。

ステップ 7 [Apply] をクリックします。

コンフィギュレーションまたはその他のファイルのバックアップと復元

システム障害に備えて、コンフィギュレーション ファイルなどのシステム ファイルを定期的にバックアップすることを推奨します。

完全なシステム バックアップまたは復元の実行

次の手順では、コンフィギュレーションおよびイメージの zipバックアップ zip ファイルへのバックアップおよび復元方法と、そのファイルのローカル コンピュータへの転送方法について説明します。

バックアップまた復元を開始する前に

- バックアップまたは復元を開始する前に、バックアップまたは復元場所に使用可能なディスク領域が少なくとも 300 MB ある必要があります。
- ASA は、シングル コンテキスト モードである必要があります。
- バックアップ中またはバックアップ後にコンフィギュレーションを変更した場合、その変更内容はバックアップに含められません。バックアップの実行後にコンフィギュレーションを変更してから復元を実行した場合、このコンフィギュレーションの変更は上書きされます。結果として、ASA は異なる挙動をすることもあります。
- 一度に開始できるバックアップまたは復元は 1 つだけです。
- コンフィギュレーションは、元のバックアップを実行したときと同じ ASA バージョンにのみ復元できます。復元ツールを使用して、ASA の異なるバージョン間でコンフィギュレーションを移行することはできません。コンフィギュレーションの移行が必要な場合、ASA は、新しい ASA OS をロードした時に常駐するスタートアップ コンフィギュレーションを自動的にアップグレードします。
- クラスタリングを使用する場合、バックアップまたは復元できるのは、スタートアップ コンフィギュレーション、実行コンフィギュレーション、およびアイデンティティ証明書のみです。ユニットごとに別々にバックアップを作成および復元する必要があります。
- フェールオーバーを使用する場合、バックアップの作成および復元は、アクティブ ユニットとスタンバイ ユニットに対して別々に行う必要があります。
- ASA にマスター パスフレーズを設定している場合は、この手順で作成したバックアップ コンフィギュレーションの復元時にそのマスター パスフレーズが必要となります。ASA のマスターパスフレーズが不明な場合は、マスターパスフレーズの設定を参照して、バックアップを続行する前に、マスター パスフレーズをリセットする方法を確認してください。

- PKCS12 データをインポート（**crypto ca trustpoint** コマンドを使用）する際にトラストポイントが RSA キーを使用している場合、インポートされたキー ペアにはトラストポイントと同じ名前が割り当てられます。この制約のため、ASDM コンフィギュレーションを復元した後でトラストポイントおよびそのキー ペアに別の名前を指定した場合、スタートアップ コンフィギュレーションは元のコンフィギュレーションと同じになるのに、実行コンフィギュレーションには異なるキー ペア名が含まれることになります。つまり、キー ペアとトラストポイントに別の名前を使用した場合は、元のコンフィギュレーションを復元できないということです。この問題を回避するため、トラストポイントとそのキーペアには必ず同じ名前を使用してください。
- CLI を使用してバックアップしてから ASDM を使用して復元したり、その逆を行うことはできません。
- 各バックアップ ファイルに含まれる内容は次のとおりです。
  - 実行コンフィギュレーション
  - スタートアップ コンフィギュレーション
  - すべてのセキュリティ イメージ

    Cisco Secure Desktop およびホスト スキャンのイメージ

    Cisco Secure Desktop およびホスト スキャンの設定

    AnyConnect クライアント（SVC）画像とプロファイル

    AnyConnect クライアント（SVC）のカスタマイズおよびトランスフォーム
  - アイデンティティ証明書（アイデンティティ証明書に関連付けられた RSA キー ペアは含まれるが、スタンドアロン キーは除外される）
  - VPN 事前共有キー
  - SSL VPN コンフィギュレーション
  - アプリケーション プロファイルのカスタム フレームワーク（APCF）
  - ブックマーク
  - カスタマイゼーション
  - ダイナミック アクセス ポリシー（DAP）
  - プラグイン
  - 接続プロファイル用の事前入力スクリプト
  - プロキシ自動設定
  - 変換テーブル
  - Web コンテンツ
  - バージョン情報

システムのバックアップ

この手順では、完全なシステム バックアップを実行する方法について説明します。

手順

ステップ 1 コンピュータ上にフォルダを作成し、バックアップ ファイルを保存します。こうすると、後で復元するときに探しやすくなります。

ステップ 2 **[Tools]** > **[Backup Configurations]** を選択します。

[Backup Configurations] ダイアログボックスが表示されます。[SSL VPN Configuration] 領域の下矢印をクリックし、SSL VPN コンフィギュレーションのバックアップ オプションを確認します。デフォルトでは、すべてのコンフィギュレーション ファイルがチェックされ、利用できる場合にはバックアップされます。リスト内のすべてのファイルをバックアップするには、手順 5 に進みます。

ステップ 3 バックアップするコンフィギュレーションを選択する場合は、[Backup All] チェックボックスをオフにします。

ステップ 4 バックアップするオプションの横にあるチェックボックスをオンにします。

ステップ 5 [Browse Local to specify a directory and file name for the backup .zip file] をクリックします。

ステップ 6 [Select] ダイアログボックスで、バックアップ ファイルを格納するディレクトリを選択します。

ステップ 7 [Select] をクリックします。[Backup File] フィールドにパスが表示されます。

ステップ 8 ディレクトリ パスの後にバックアップ ファイルの宛先の名前を入力します。バックアップ ファイルの名前の長さは、3 ～ 232 文字の間である必要があります。

ステップ 9 [Backup] をクリックします。証明書をバックアップする場合や、ASA でマスター パスフレーズを使用している場合を除き、すぐにバックアップが続行されます。

ステップ 10 ASA でマスター パスフレーズを設定し、イネーブルにしている場合、バックアップを続行する前に、マスターパスフレーズが不明な場合は変更することを推奨する警告メッセージが表示されます。マスター パスフレーズがわかっている場合は、[Yes] をクリックしてバックアップを続行します。ID 証明書をバックアップする場合を除き、すぐにバックアップが続行されます。

ステップ 11 ID 証明書をバックアップする場合は、証明書を PKCS12 形式でエンコーディングするために使用する別のパスフレーズを入力するように求められます。パスフレーズを入力するか、またはこの手順をスキップすることができます。

（注） ID 証明書だけがこのプロセスによってバックアップされます。

- 証明書を暗号化するには、[Certificate Passphrase] ダイアログボックスで証明書のパスフレーズを入力および確認し、[OK] をクリックします。証明書の復元時に必要となるため、このダイアログボックスに入力したパスワードを覚えておく必要があります。
- [Cancel] をクリックすると、この手順がスキップされ、証明書はバックアップされません。

[OK] または [Cancel] をクリックすると、すぐにバックアップが開始されます。

ステップ 12 バックアップが完了すると、ステータス ウィンドウが閉じ、[Backup Statistics] ダイアログボックスが表示され、成功または失敗のメッセージが示されます。

（注） バックアップの「失敗」メッセージは多くの場合、指定されたタイプの既存のコンフィギュレーションが存在しない場合に表示されます。

ステップ 13 [OK] をクリックし、[Backup Statistics] ダイアログボックスを閉じます。

バックアップの復元

zip tar.gz ファイルからローカル PC に復元するコンフィギュレーションやイメージを指定します。

手順

ステップ 1 **[Tools]** > **[Restore Configurations]** を選択します。

ステップ 2 [Restore Configurations] ダイアログボックスで、[Browse Local Directory] をクリックし、ローカル コンピュータ上の、復元するコンフィギュレーションが含まれている zip ファイルを選択し、[Select] をクリックします。[Local File] フィールドにパスと zip ファイル名が表示されます。

復元する zip ファイルは、[Tools] > [Backup Configurations] オプションを選択して作成したものである必要があります。

ステップ 3 [Next] をクリックします。2 つ目の [Restore Configuration] ダイアログボックスが表示されます。復元するコンフィギュレーションの横にあるチェックボックスをオンにします。使用可能なすべての SSL VPN コンフィギュレーションがデフォルトで選択されています。

ステップ 4 [Restore] をクリックします。

ステップ 5 バックアップ ファイルの作成時に、証明書の暗号化に使用する証明書パスフレーズを指定している場合は、このパスフレーズを入力するように ASDM から求められます。

ステップ 6 実行コンフィギュレーションの復元を選択した場合、実行コンフィギュレーションを結合するか、実行コンフィギュレーションを置換するか、または復元プロセスのこの部分をスキップするかを尋ねられます。

- コンフィギュレーションの結合では、現在の実行コンフィギュレーションとバックアップされた実行コンフィギュレーションが結合されます。
- 実行コンフィギュレーションの置換では、バックアップされた実行コンフィギュレーションのみが使用されます。
- この手順をスキップすると、バックアップされた実行コンフィギュレーションは復元されません。

ASDM では、復元操作が完了するまでステータス ダイアログボックスが表示されます。

ステップ 7 実行コンフィギュレーションを置換または結合した場合は、ASDM を閉じてから再起動します。実行コンフィギュレーションを復元しなかった場合は、ASDMセッションをリフレッシュして、変更を有効にします。

自動バックアップおよび復元の設定（ISA 3000）

ISA 3000 では、設定を保存するたびに、特定の場所への自動バックアップを設定できます。

自動復元では、完全な設定を SD フラッシュメモリカードにロードして、新しいデバイスを簡単に設定できます。工場出荷時のデフォルト設定では、自動復元が有効になっています。

自動バックアップの設定（ISA 3000）

ISA 3000 では、設定を保存するたびに、特定の場所への自動バックアップを設定できます。

始める前に

この機能は、ISA 3000 のみで使用できます。

手順

ステップ 1 **[構成（Configuration）] > [デバイス管理（Device Management）] > [自動バックアップと復元の設定（Auto Backup & Restore Configuration）]** の順に選択します。

ステップ 2 [自動バックアップ設定（Automatic Restore Configuration）] をオンまたはオフにして、自動バックアップを有効または無効にします。

自動バックアップを有効にした場合、設定を保存すると、その設定は自動的にバックアップの場所とスタートアップ コンフィギュレーションに保存されます。バックアップファイルの名前は「auto-backup-asa.tgz」です。

次のパラメータを設定します。

- [インターフェイス（Interface）] : オフデバイスストレージを指定した場合に、バックアップ URL に到達するためのインターフェイスを指定します。interface name を指定しない場合、ASA は管理専用のルーティング テーブルをチェックします。ここで一致が見つからない場合はデータのルーティング テーブルをチェックします。
- [場所（Location）] : データのバックアップに使用するストレージメディアを指定します。URL またはローカルストレージを指定できます。disk0 は内部フラッシュドライブです。disk1 は USB 1 のオプションの USB メモリスティックです。disk2 は USB 2 のオプションの USB メモリスティックです。disk3 は SD メモリカードです。自動復元のデフォルトは disk3: です。

- [パスフレーズ（Passphrase）]：バックアップデータを保護するためのパスフレーズを設定します。自動復元のデフォルトは「cisco」です。

自動復元の設定（ISA 3000）

自動復元モードは、ユーザの操作なしでデバイスのシステム設定を復元します。たとえば、保存したバックアップ設定を含むSDメモリカードを新しいデバイスに挿入し、デバイスの電源をオンにします。デバイスが起動すると、システム設定を復元する必要があるかどうかを判断するためにSDカードがチェックされます。（復元は、バックアップファイルに別のデバイスの「フィンガープリント」がある場合にのみ開始されます。バックアップファイルのフィンガープリントは、バックアップまたは復元操作中に現在のデバイスに一致するように更新されます。そのため、デバイスがすでに復元を完了している場合、またはデバイスが独自のバックアップを作成している場合は、自動復元はスキップされます。）フィンガープリントに復元が必要であることが示されている場合、デバイスはシステム設定を置き換えます（startup-config、running-config、SSL VPN設定など。バックアップの内容の詳細については、システムのバックアップ （25 ページ）を参照してください）。デバイスの起動が完了すると、保存された設定が実行されます。

工場出荷時のデフォルト設定では自動復元が有効になっているため、デバイスの事前設定を実行しなくても、SDメモリカードにロードされた完全な設定で新しいデバイスを簡単に設定できます。

デバイスは、システム設定を復元する必要があるかどうかをブートプロセスの早い段階で決定する必要があるため、ROMMON変数をチェックして、デバイスが自動復元モードかどうかを判断し、バックアップ設定の場所を取得します。次のROMMON変数が使用されます。

- **RESTORE_MODE** = {**auto** | **manual**}

  デフォルトは **auto** です。

- **RESTORE_LOCATION** = {**disk0:** | **disk1:** | **disk2:** | **disk3:**}

  デフォルトは **disk3:** です。

- **RESTORE_PASSPHRASE** = *key*

  デフォルトは **cisco** です。

自動復元設定を変更するには、次の手順を実行します。

始める前に

- この機能は、ISA 3000のみで使用できます。
- デフォルトの復元設定を使用する場合は、SDメモリカード（部品番号SD-IE-1GB=）を取り付ける必要があります。
- 自動復元を有効にするためにデフォルト設定を復元する必要がある場合は、**configure factory default** コマンドを使用します。このコマンドは、トランスペアレント ファイア

ウォール モードでのみ使用できます。そのため、ルーテッド ファイアウォール モードの場合は、最初に **firewall transparent** コマンドを使用します。

手順

ステップ 1 **[構成（Configuration）] > [デバイス管理（Device Management）] > [自動バックアップと復元の設定（Auto Backup & Restore Configuration）]** の順に選択します。

ステップ 2 [自動復元設定（Automatic Restore Configuration）] をオンまたはオフにして、自動復元を有効または無効にします。

復元されるファイルの名前は「auto-backup-asa.tgz」です。自動復元を有効にする場合は、次のパラメータを設定します。

- [場所（Location）]：データの復元に使用するストレージメディアを指定します。disk0 は内部フラッシュドライブです。disk1 は USB 1 のオプションの USB メモリスティックです。disk2 は USB 2 のオプションの USB メモリスティックです。disk3 は SD メモリカードです。デフォルトは disk3 です。
- [パスフレーズ（Passphrase）]：バックアップデータを読み取るパスフレーズを設定します。デフォルトは「cisco」です。

TFTP サーバーへの実行コンフィギュレーションの保存

この機能により、現在の実行コンフィギュレーション ファイルのコピーを TFTP サーバーに保存します。

手順

ステップ 1 **[File] > [Save Running Configuration to TFTP Server]** を選択します。

[Save Running Configuration to TFTP Server] ダイアログボックスが表示されます。

ステップ 2 TFTP サーバーの IP アドレスと、コンフィギュレーション ファイルの保存先となる TFTP サーバー上のファイル パスを入力して、[Save Configuration] をクリックします。

（注） デフォルトの TFTP 設定を行うには、[Configuration] > [Device Management] > [Management Access] > [File Access] > [TFTP Client] の順に選択します。この設定を行った後は、このダイアログボックスに、TFTP サーバーの IP アドレスと TFTP サーバー上でのファイル パスが自動的に表示されます。

システム再起動のスケジュール

System Reload ツールにより、システムの再起動をスケジュールしたり、現在の再起動をキャンセルしたりできます。

手順

ステップ 1 **[Tools]** > **[System Reload]** を選択します。

ステップ 2 [Reload Scheduling] 領域で、次の設定を定義します。

a) [Configuration State] では、再起動時に実行コンフィギュレーションを保存するか、破棄するかのどちらかを選択します。

b) [Reload Start Time] では、次のオプションから選択します。

- 再起動をただちに実行するには、[Now] をクリックします。
- 指定した時間だけ再起動を遅らせるには、[Delay by] をクリックします。再起動開始までの時間を、時間と分単位、または分単位だけで入力します。
- 指定した時刻と日付に再起動を実行するようにスケジュールするには、[Schedule at] をクリックします。再起動の実行時刻を入力し、再起動のスケジュール日を選択します。

c) [Reload Message] フィールドに、再起動時に開いている ASDM インスタンスに送信するメッセージを入力します。

d) 再起動を再試行するまでの経過時間を時間と分単位で、または分単位だけで表示するには、[On reload failure force immediate reload after] チェックボックスをオンにします。

e) 設定に従って再起動をスケジュールするには、[Schedule Reload] をクリックします。

[Reload Status] 領域には、再起動のステータスが表示されます。

ステップ 3 次のいずれかを選択します。

- スケジュールされた再起動を停止するには、[Cancel Reload] をクリックします。
- スケジュールされた再起動の終了後に [Reload Status] 表示をリフレッシュするには、[Refresh] をクリックします。
- スケジュールされた再起動の詳細を表示するには、[Details] をクリックします。

Cisco Secure Firewall 3100 での SSD のホットスワップ

SSD が 2 つある場合、起動時に RAID が形成されます。ファイアウォールの電源が入っている状態で CLI で次のタスクを実行できます。

- SSD の 1 つをホットスワップする：SSD に障害がある場合は、交換できます。SSD が 1 つしかない場合、ファイアウォールの電源がオンになっている間 SSD は取り外せません。
- SSD の 1 つを取り外す：SSD が 2 つある場合は、1 つを取り外すことができます。
- 2 つ目の SSD を追加する：SSD が 1 つの場合は、2 つ目の SSD を追加して RAID を形成できます。

⚠

注意 この手順を使用して、SSD を RAID から削除する前に SSD を取り外さないでください。データが失われる可能性があります。

手順

ステップ 1 SSD の 1 つを取り外します。

a) SSD を RAID から取り外します。

raid remove-secure local-disk {**1** | **2**}

remove-secure キーワードは SSD を RAID から削除し、自己暗号化ディスク機能を無効にして、SSD を安全に消去します。SSD を RAID から削除するだけでデータをそのまま維持する場合は、**remove** キーワードを使用できます。

例：

```
ciscoasa(config)# raid remove-secure local-disk 2
```

b) SSD がインベントリに表示されなくなるまで、RAID ステータスを監視します。

show raid

SSD が RAID から削除されると、**操作性**と**ドライブの状態**が**劣化**として表示されます。2 つ目のドライブは、メンバーディスクとして表示されなくなります。

例：

```
ciscoasa# show raid
Virtual Drive
ID:                         1
Size (MB):                  858306
Operability:                operable
Presence:                   equipped
Lifecycle:                  available
Drive State:                optimal
```

```
Type:                        raid
Level:                       raid1
Max Disks:                   2
Meta Version:                1.0
Array State:                 active
Sync Action:                 idle
Sync Completed:              unknown
Degraded:                    0
Sync Speed:                  none

RAID member Disk:
Device Name:                 nvme0n1
Disk State:                  in-sync
Disk Slot:                   1
Read Errors:                 0
Recovery Start:              none
Bad Blocks:
Unacknowledged Bad Blocks:

Device Name:                 nvme1n1
Disk State:                  in-sync
Disk Slot:                   2
Read Errors:                 0
Recovery Start:              none
Bad Blocks:
Unacknowledged Bad Blocks:

ciscoasa# show raid
Virtual Drive
ID:                          1
Size (MB):                   858306
Operability:                 degraded
Presence:                    equipped
Lifecycle:                   available
Drive State:                 degraded
Type:                        raid
Level:                       raid1
Max Disks:                   2
Meta Version:                1.0
Array State:                 active
Sync Action:                 idle
Sync Completed:              unknown
Degraded:                    1
Sync Speed:                  none

RAID member Disk:
Device Name:                 nvme0n1
Disk State:                  in-sync
Disk Slot:                   1
Read Errors:                 0
Recovery Start:              none
Bad Blocks:
Unacknowledged Bad Blocks:
```

c) SSD をシャーシから物理的に取り外します。

ステップ 2 SSD を追加します。

a) SSD を空のスロットに物理的に追加します。

b) SSD を RAID に追加します。

raid add local-disk {**1** | **2**}

新しい SSD と RAID の同期が完了するまでに数時間かかることがありますが、その間、ファイアウォールは完全に動作します。再起動もでき、電源投入後に同期は続行されます。ステータスを表示するには、**show raid** コマンドを使用します。

以前に別のシステムで使用されており、まだロックされている SSD を取り付ける場合は、次のコマンドを入力します。

raid add local-disk {**1** | **2**} *psid*

psid は SSD の背面に貼られたラベルに印刷されています。または、システムを再起動し、SSD を再フォーマットして RAID に追加できます。

ソフトウェアとコンフィギュレーションの履歴

機能名	プラットフォームリリース	機能情報
セキュアコピークライアントおよびサーバ	9.1(5)/9.2(1)	SCP サーバとの間でファイルを転送するため、ASA は Secure Copy（SCP）クライアントおよびサーバ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。 [Tools] > [File Management] > [File Transfer] > [Between Remote Server and Flash] [Configuration] > [Device Management] > [Management Access] > [File Access] > [Secure Copy (SCP) Server]
設定可能な SSH 暗号機能と整合性アルゴリズム	9.1(7)/9.4(3)/9.5(3)/9.6(1)	ユーザーは 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。たとえば、提示された暗号方式に変更するには、**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]**

機能名	プラットフォームリリース	機能情報
デフォルトでイネーブルになっている Auto Update サーバー証明書の検証	9.2(1)	Auto Update サーバ証明書の検証がデフォルトでイネーブルになりました。新しいコンフィギュレーションでは証明書の検証を明示的にディセーブルにする必要があります。証明書の確認をイネーブルにしていなかった場合に、以前のリリースからアップグレードしようとすると、証明書の確認はイネーブルではなく、次の警告が表示されます。 `WARNING: The certificate provided by the auto-update servers will not be verified. In order to verify this certificate please use the verify-certificate option.` 設定を移行する場合は、次のように確認なしを明示的に設定します。 次の画面が変更されました。[Configuration] > [Device Management] > [System/Image Configuration] > [Auto Update] > [Add Auto Update Server]。
CLI を使用したシステムのバックアップと復元	9.3(2)	CLI を使用してイメージや証明書を含む完全なシステムコンフィギュレーションをバックアップおよび復元できるようになりました。 変更された ASDM 画面はありません。
新しい ASA 5506W-X イメージの回復およびロード	9.4(1)	新しい ASA 5506W-X イメージのリカバリおよびロードがサポートされています。 変更された ASDM 画面はありません。
ISA 3000 の自動バックアップと復元	9.7(1)	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]**
SCP クライアントを使用する場合、CiscoSSH スタックには SSH アクセスが必要です	9.17(1)	CiscoSSH スタックを使用する場合、ASA **copy** コマンドを使用して SCP サーバとの間でファイルをコピーするには、SCP サーバサブネット/ホストの SSH アクセスを ASA で有効にする必要があります。

機能名	プラットフォームリリース	機能情報
Cisco Secure Firewall 3100 での SSD の RAID サポート	9.17(1)	SSD は自己暗号化ドライブ（SED）です。SSD が 2 つある場合、ソフトウェア RAID を形成します。 新規/変更されたコマンド： **raid, show raid, show ssd**

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。