



## 使用する前に

---

この章では、ASA の使用を開始する方法について説明します。

- [コマンドラインインターフェイス \(CLI\) のコンソールへのアクセス \(1 ページ\)](#)
- [ASDM アクセスの設定 \(9 ページ\)](#)
- [ASDM の起動 \(13 ページ\)](#)
- [工場出荷時のデフォルト設定 \(14 ページ\)](#)
- [アプライアンスまたはプラットフォーム モードへの Firepower 2100 の設定 \(33 ページ\)](#)
- [コンフィギュレーション作業 \(35 ページ\)](#)
- [接続の設定変更の適用 \(41 ページ\)](#)
- [ASA のリロード \(41 ページ\)](#)

## コマンドラインインターフェイス (CLI) のコンソールへのアクセス

初期設定を行うには、コンソールポートから直接 CLI にアクセスします。その後、[管理アクセス](#)に従って Telnet または SSH を使用して、リモートアクセスを設定できます。システムがすでにマルチ コンテキスト モードで動作している場合は、コンソールポートにアクセスするとシステムの実行スペースに入ります。



---

(注) [ASA](#)v のコンソールアクセスについては、[ASA](#)v のクイックスタートガイドを参照してください。

---

## ASA ハードウェアまたは ISA 3000 コンソールへのアクセス

アプライアンス コンソールにアクセスするには、次の手順に従います。

## 手順

---

**ステップ 1** 付属のコンソール ケーブルを使用してコンピュータをコンソール ポートに接続します。ターミナルエミュレータを回線速度 9600 ボー、データ ビット 8、パリティなし、ストップ ビット 1、フロー制御なしに設定して、コンソールに接続します。

コンソール ケーブルの詳細については、ASA のハードウェア ガイドを参照してください。

**ステップ 2** **Enter** キーを押して、次のプロンプトが表示されることを確認します。

```
ciscoasa>
```

このプロンプトは、ユーザー EXEC モードで作業していることを示します。ユーザー EXEC モードでは、基本コマンドのみを使用できます。

**ステップ 3** 特権 EXEC モードにアクセスします。

### **enable**

**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。

例：

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: *****
Repeat Password: *****
ciscoasa#
```

設定以外のすべてのコマンドは、特権 EXEC モードで使用できます。特権 EXEC モードからコンフィギュレーション モードに入ることもできます。

特権モードを終了するには、**disable** コマンド、**exit** コマンド、または **quit** コマンドを入力します。

**ステップ 4** グローバル コンフィギュレーション モードにアクセスします。

### **configure terminal**

例：

```
ciscoasa# configure terminal
ciscoasa(config)#
```

グローバル コンフィギュレーション モードから ASA の設定を開始できます。グローバル コンフィギュレーション モードを終了するには、**exit** コマンド、**quit** コマンド、または **end** コマンドを入力します。

---

## Firepower 2100 プラットフォーム モードのコンソールへのアクセス

Firepower 2100 コンソールポートで Firepower eXtensible オペレーティングシステム (FXOS CLI) に接続します。次に、FXOS CLI から ASA コンソールに接続し、再度戻ることができます。FXOS に SSH 接続する場合は、ASA CLI にも接続できます。SSH からの接続はコンソール接続ではないため、FXOS SSH 接続から複数の ASA 接続を行うことができます。同様に、ASA に SSH 接続する場合は、FXOS CLI に接続できます。

### 始める前に

一度に保持できるコンソール接続は 1 つだけです。FXOS コンソールから ASA のコンソールに接続する場合、Telnet または SSH 接続の場合とは異なり、この接続は永続的接続です。

### 手順

**ステップ 1** 管理コンピュータをコンソールポートに接続します。Firepower 2100 には DB-9 to RJ-45 シリアルケーブルが付属しているため、接続するためにはサードパーティ製のシリアル to USB ケーブルが必要です。ご使用のオペレーティングシステムに必要な USB シリアルドライバを必ずインストールしてください。次のシリアル設定を使用します。

- 9600 ボー
- 8 データ ビット
- パリティなし
- 1 ストップ ビット

FXOS CLI に接続します。ユーザー クレデンシャルを入力します。デフォルトでは、**admin** ユーザーとデフォルトのパスワード **Admin123** を使用してログインできます。

**ステップ 2** ASA に接続します。

**connect asa**

例 :

```
firepower-2100# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
ciscoasa>
```

**ステップ 3** 特権 EXEC モードにアクセスします。

**enable**

**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。

例 :

```
ciscoasa> enable
```

```
Password:
The enable password is not set. Please set it now.
Enter Password: *****
Repeat Password: *****
ciscoasa#
```

設定以外のすべてのコマンドは、特権 EXEC モードで使用できます。特権 EXEC モードからコンフィギュレーションモードに入ることもできます。

特権モードを終了するには、**disable** コマンド、**exit** コマンド、または **quit** コマンドを入力します。

**ステップ 4** グローバル コンフィギュレーション モードにアクセスします。

#### **configure terminal**

例：

```
ciscoasa# configure terminal
ciscoasa(config)#
```

グローバルコンフィギュレーションモードから ASA の設定を開始できます。グローバルコンフィギュレーションモードを終了するには、**exit** コマンド、**quit** コマンド、または **end** コマンドを入力します。

**ステップ 5** FXOS コンソールに戻るには、**Ctrl+a, d** と入力します。

**ステップ 6** ASA に SSH 接続する場合（ASA で SSH アクセスを設定した後）、FXOS CLI に接続します。

#### **connect fxos**

FXOS への認証を求められます。デフォルトのユーザー名：**admin** およびパスワード：**Admin123** を使用します。ASA CLI に戻るには、**exit** と入力するか、または **Ctrl-Shift-6, x** と入力します。

例：

```
ciscoasa# connect fxos
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.

FXOS 2.2(2.32) kp2110

kp2110 login: admin
Password: Admin123
Last login: Sat Jan 23 16:20:16 UTC 2017 on pts/1
Successful login attempts for user 'admin' : 4
Cisco Firepower Extensible Operating System (FX-OS) Software

[...]

kp2110#
kp2110# exit
Remote card closed command session. Press any key to continue.
Connection with fxos terminated.
Type help or '?' for a list of available commands.
```

```
ciscoasa#
```

## Firepower1000、2100（アプライアンスモード）コンソールへのアクセス

Firepower 1000、2100（アプライアンスモード）コンソールポートは、ASA CLI に接続します（FXOS CLI に接続する Firepower 2100 プラットフォームモードのコンソールとは異なります）。ASA CLI から、トラブルシューティングのために Telnet を使用して FXOS CLI に接続できます。

### 手順

**ステップ1** 管理コンピュータをコンソールポートに接続します。Firepower 1000 には、USB A to B シリアルケーブルが付属しています。Firepower 2100 には DB-9 to RJ-45 シリアルケーブルが付属しているため、接続するためにはサードパーティ製のシリアル to USB ケーブルが必要です。ご使用のオペレーティングシステムに必要な USB シリアルドライバを必ずインストールしてください（次を参照『Firepower 1010 [hardware guide](#)』または『Firepower 1100 [hardware guide](#)』）。次のシリアル設定を使用します。

- 9600 ボー
- 8 データ ビット
- パリティなし
- 1 ストップ ビット

ASA CLI に接続します。デフォルトでは、コンソールアクセスに必要なユーザークレデンシャルはありません。

**ステップ2** 特権 EXEC モードにアクセスします。

**enable**

**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。

例：

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: *****
Repeat Password: *****
ciscoasa#
```

ASA で設定したイネーブルパスワードは、FXOS 管理者のユーザーパスワードでもあり、ASA の起動に失敗した場合は、FXOS フェールセーフモードに移行します。

設定以外のすべてのコマンドは、特権 EXEC モードで使用できます。特権 EXEC モードからコンフィギュレーションモードに入ることもできます。

特権 EXEC モードを終了するには、**disable**、**exit**、または **quit** コマンドを入力します。

**ステップ 3** グローバル コンフィギュレーション モードにアクセスします。

**configure terminal**

例：

```
ciscoasa# configure terminal
ciscoasa(config)#
```

グローバルコンフィギュレーションモードから ASA の設定を開始できます。グローバルコンフィギュレーションモードを終了するには、**exit**、**quit**、または **end** コマンドを入力します。

**ステップ 4** (任意) FXOS CLI に接続します。

**connect fxos [admin]**

- **admin** : 管理者レベルのアクセスを提供します。このオプションを指定しないと、ユーザーのアクセス権は読み取り専用アクセスになります。管理者モードであっても、コンフィギュレーション コマンドは使用できないことに注意してください。

ユーザーはクレデンシャルの入力を求められません。現在の ASA ユーザー名が FXOS に渡されるため、追加のログインは必要ありません。ASA CLI に戻るには、**exit** と入力するか、**Ctrl+Shift+6** を押し、**x** と入力します。

FXOS 内では、**scope security/show audit-logs** コマンドを使用してユーザーアクティビティを表示できます。

例：

```
ciscoasa# connect fxos admin
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.
firepower#
firepower# exit
Connection with FXOS terminated.
Type help or '?' for a list of available commands.
ciscoasa#
```

---

## Firepower 4100/9300 シャーシ上の ASA コンソールへのアクセス

初期設定の場合、Firepower 4100/9300 シャーシ スーパーバイザに（コンソールポートに、あるいは Telnet または SSH を使用してリモートで）接続してコマンドライン インターフェイスにアクセスし、ASA セキュリティ モジュールに接続します。

## 手順

**ステップ 1** Firepower 4100/9300 シャーシスーパーバイザ CLI（コンソールまたは SSH）に接続し、次に ASA にセッション接続します。

```
connect module slot {console | telnet}
```

Telnet 接続を使用する利点は、モジュールに同時に複数のセッションを設定でき、接続速度が速くなることです。

初めてモジュールにアクセスするときは、FXOS モジュールの CLI にアクセスします。その後 ASA アプリケーションに接続する必要があります。

```
connect asa
```

例：

```
Firepower# connect module 1 console  
Firepower-module1> connect asa
```

```
asa>
```

**ステップ 2** 最高の特権レベルである特権 EXEC モードにアクセスします。

```
enable
```

**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。

例：

```
asa> enable  
Password:  
The enable password is not set. Please set it now.  
Enter Password: *****  
Repeat Password: *****  
asa#
```

設定以外のすべてのコマンドは、特権 EXEC モードで使用できます。特権 EXEC モードからコンフィギュレーションモードに入ることもできます。

特権モードを終了するには、**disable** コマンド、**exit** コマンド、または **quit** コマンドを入力します。

**ステップ 3** グローバル コンフィギュレーションモードを開始します。

```
configure terminal
```

例：

```
asa# configure terminal  
asa(config)#
```

グローバル コンフィギュレーションモードを終了するには、**disable**、**exit**、または **quit** コマンドを入力します。

**ステップ 4** **Ctrl-a, d** と入力し、アプリケーション コンソールを終了して FXOS モジュール CLI に移動します。

トラブルシューティングのために FXOS モジュールの CLI を使用する場合があります。

**ステップ 5** FXOS CLI のスーパーバイザ レベルに戻ります。

コンソールを終了します。

a) ~ と入力

Telnet アプリケーションに切り替わります。

b) Telnet アプリケーションを終了するには、次を入力します。

telnet>**quit**

**Telnet セッションを終了します。**

a) **Ctrl-], .** と入力

---

## ソフトウェア モジュール コンソールへのアクセス

ASA 5506-X に ASA FirePOWER などのソフトウェア モジュールをインストールしている場合、モジュール コンソールへのセッションを実行できます。



---

(注) **session** コマンドを使用して ASA バックプレーンを介してハードウェア モジュール CLI にアクセスすることはできません。

---

### 手順

---

ASA CLI から、モジュールへのセッションを実行します。

**session {sfr | cxsc | ips} console**

例 :

```
ciscoasa# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.
```

```
Cisco ASA SFR Boot Image 5.3.1
asasfr login: admin
Password: Admin123
```

---



## ASA 5506W-X ワイヤレス アクセス ポイント コンソールへのアクセス

ワイヤレス アクセス ポイント コンソールにアクセスするには、次の手順を実行します。

### 手順

**ステップ 1** ASA CLI から、アクセス ポイントへのセッションを実行します。

**session wlan console**

例：

```
ciscoasa# session wlan console
opening console session with module wlan
connected to module wlan. Escape character sequence is 'CTRL-^X'

ap>
```

**ステップ 2** アクセス ポイント CLI については、『[Cisco IOS Configuration Guide for Autonomous Aironet Access Points](#)』を参照してください。

## ASDM アクセスの設定

ここでは、デフォルト設定で ASDM にアクセスする方法、およびデフォルト設定がない場合にアクセスを設定する方法について説明します。

## ASDM アクセスの工場出荷時のデフォルト設定の使用

工場出荷時のデフォルト コンフィギュレーションでは、ASDM 接続はデフォルトのネットワーク設定で事前設定されています。

### 手順

次のインターフェイスおよびネットワーク設定を使用して ASDM に接続します。

- 管理インターフェイスは、ご使用のモデルによって異なります。
  - Firepower 1010：管理 1/1（192.168.45.1）、または内部イーサネット 1/2 ～ 1/8（192.168.1.1）。管理ホストは 192.168.45.0/24 ネットワークに限定され、内部ホストは 192.168.1.0/24 ネットワークに限定されます。
  - アプライアンスモードの Firepower 1100、2100：内部イーサネット 1/2（192.168.1.1）、または管理 1/1（DHCP から）。内部ホストは 192.168.1.0/24 ネットワークに限定されます。管理ホストは任意のネットワークからアクセスできます。

- プラットフォーム モードの Firepower 2100 : 管理 1/1 (192.168.45.1) 。管理ホストは 192.168.45.0/24 ネットワークに限定されます。
- Firepower 4100/9300 : 展開時に定義された管理タイプ インターフェイスと IP アドレス。管理ホストは任意のネットワークからアクセスできます。
- ASA 5506-X、ASA 5506W-X : 内部 GigabitEthernet 1/2 ~ 1/8、および Wi-Fi GigabitEthernet 1/9 (192.168.10.1) 。内部ホストは 192.168.1.0/24 ネットワークに限定され、Wi-Fi ホストは 192.168.10.0/24 に限定されます。
- ASA 5508-X および ASA 5516-X : 内部 GigabitEthernet 1/2 (192.168.1.1) 。 Inside hosts are limited to the 192.168.1.0/24 network.
- ASA 5525-X 以降 : 管理 0/0 (192.168.1.1) 。管理ホストは 192.168.1.0/24 ネットワークに限定されます。
- ASA v : 管理 0/0 (展開時に設定) 。管理ホストは管理ネットワークに限定されます。
- ISA 3000 : 管理 1/1 (192.168.1.1) 。管理ホストは 192.168.1.0/24 ネットワークに限定されます。

(注) マルチ コンテキスト モードに変更すると、上記のネットワーク設定を使用して管理 コンテキストから ASDM にアクセスできるようになります。

---

#### 関連トピック

[工場出荷時のデフォルト設定](#) (14 ページ)

[マルチ コンテキスト モードの有効化または無効化](#)

[ASDM の起動](#) (13 ページ)

## ASDM アクセスのカスタマイズ

次の条件に 1 つ以上当てはまる場合は、この手順を使用します。

- 工場出荷時のデフォルト コンフィギュレーションがない。
- 管理 IP アドレスを変更したい。
- トランスペアレント ファイアウォール モードに変更したい。
- マルチ コンテキスト モードに変更したい。

シングルルーテッドモードの場合、ASDM に迅速かつ容易にアクセスするために、独自の管理 IP アドレスを設定できるオプションを備えた工場出荷時のデフォルトコンフィギュレーションを適用することを推奨します。この項に記載されている手順は、特別なニーズ (トランスペアレントモードやマルチ コンテキスト モードの設定など) がある場合や、他の設定を維持する必要がある場合にのみ使用してください。



- (注) ASAv の場合、導入時にトランスペアレント モードを設定できるため、この手順は、設定をクリアする必要がある場合など、導入後に特に役立ちます。

## 手順

**ステップ1** コンソール ポートで CLI にアクセスします。

**ステップ2** (オプション) トランスペアレント ファイアウォール モードをイネーブルにします。

このコマンドは、設定をクリアします。

**firewall transparent**

**ステップ3** 管理インターフェイスを設定します。

```
interface interface_id
  nameif name
  security-level level
  no shutdown
  ip address ip_address mask
```

例 :

```
ciscoasa(config)# interface management 0/0
ciscoasa(config-if)# nameif management
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
```

**security-level** は、1 ~ 100 の数字です。100 が最も安全です。

**ステップ4** (直接接続された管理ホスト用) 管理ネットワークの DHCP プールを設定します。

```
dhcpd address ip_address-ip_address interface_name
dhcpd enable interface_name
```

例 :

```
ciscoasa(config)# dhcpd address 192.168.1.2-192.168.1.254 management
ciscoasa(config)# dhcpd enable management
```

その範囲にインターフェイス アドレスが含まれていないことを確認します。

**ステップ5** (リモート管理ホスト用) 管理ホストへのルートを設定します。

```
route management_ifc management_host_ip mask gateway_ip 1
```

例 :

```
ciscoasa(config)# route management 10.1.1.0 255.255.255.0 192.168.1.50 1
```

**ステップ 6** ASDM の HTTP サーバーをイネーブルにします。

**http server enable**

**ステップ 7** 管理ホストの ASDM へのアクセスを許可します。

**http ip\_address mask interface\_name**

例 :

```
ciscoasa(config)# http 192.168.1.0 255.255.255.0 management
```

**ステップ 8** 設定を保存します。

**write memory**

**ステップ 9** (オプション) モードをマルチ モードに設定します。

**mode multiple**

プロンプトが表示されたら、既存の設定を管理コンテキストに変換することを承認します。ASA をリロードするよう求められます。

---

## 例

次の設定では、ファイアウォール モードがトランスペアレント モードに変換され、Management 0/0 インターフェイスが設定され、管理ホストに対して ASDM がイネーブルにされます。

```
firewall transparent
interface management 0/0

ip address 192.168.1.1 255.255.255.0
nameif management
security-level 100
no shutdown

dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
http server enable
http 192.168.1.0 255.255.255.0 management
```

## 関連トピック

[工場出荷時のデフォルト設定の復元 \(16 ページ\)](#)

[ファイアウォール モードの設定](#)

[ASA ハードウェアまたは ISA 3000 コンソールへのアクセス \(1 ページ\)](#)

[ASDM の起動 \(13 ページ\)](#)

## ASDM の起動

ASDM は、次の 2 つの方法で起動できます。

- **ASDM-IDM ランチャ**：ランチャは、ASA から Web ブラウザを使用してダウンロードされるアプリケーションです。これを使用すると、任意の ASA IP アドレスに接続できます。他の ASA に接続する場合、ランチャを再度ダウンロードする必要はありません。
- **Java Web Start**：管理する ASA ごとに Web ブラウザで接続して、Java Web Start アプリケーションを保存または起動する必要があります。任意でコンピュータにショートカットを保存できます。ただし、ASA IP アドレスごとにショートカットを分ける必要があります。



- (注) Web Start を使用する場合は、Java キャッシュをクリアしてください。クリアしない場合、Hostscan などのログイン前ポリシーに対する変更が失われる可能性があります。この問題は、ランチャを使用している場合には発生しません。

ASDM では、管理のために別の ASA IP アドレスを選択できます。ランチャと Java Web Start の機能の違いは、主に、ユーザーが最初にどのように ASA に接続し、ASDM を起動するかにあります。

ここでは、まず ASDM に接続する方法について説明します。次にランチャまたは Java Web Start を使用して ASDM を起動する方法について説明します。

ASDM はローカルの \Users\\.asdm ディレクトリ内にキャッシュ、ログ、設定などのファイルを保存し、Temp ディレクトリ内にも AnyConnect クライアントプロファイルなどのファイルを保存します。

### 手順

**ステップ 1** ASDM クライアントとして指定したコンピュータで次の URL を入力します。

**https://asa\_ip\_address/admin**

- (注) **http://** や IP アドレス（デフォルトは HTTP）ではなく、必ず **https://** を指定してください。ASA は、HTTP 要求を HTTPS に自動的に転送しません。

次のボタンを持つ ASDM 起動ページが表示されます。

- **Install ASDM Launcher and Run ASDM**
- **Run ASDM**
- **Run Startup Wizard**

**ステップ 2** ランチャをダウンロードするには、次の手順を実行します。

- a) [Install ASDM Launcher and Run ASDM] をクリックします。

- b) 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。ホスト名、ドメイン名、およびイネーブルパスワードと Telnet パスワードの設定を参照してください。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。
- c) インストーラをコンピュータに保存して、インストーラを起動します。インストールが完了すると、ASDM-IDM ランチャが自動的に開きます。
- d) 管理 IP アドレス、および同じユーザー名とパスワード（新規インストールの場合は空白）を入力し、[OK] をクリックします。

**ステップ 3** Java Web Start を使用するには、次の手順を実行します。

- a) [Run ASDM] または [Run Startup Wizard] をクリックします。
- b) プロンプトが表示されたら、ショートカットをコンピュータに保存します。オプションで、アプリケーションを保存せずに開くこともできます。
- c) ショートカットから Java Web Start を起動します。
- d) 表示されたダイアログボックスに従って、任意の証明書を受け入れます。Cisco ASDM-IDM Launcher が表示されます。
- e) 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。ホスト名、ドメイン名、およびイネーブルパスワードと Telnet パスワードの設定を参照してください。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。

## 工場出荷時のデフォルト設定

工場出荷時のデフォルト設定とは、シスコが新しい ASA に適用したコンフィギュレーションです。

- ASA 5506-X：工場出荷時のデフォルト設定により、機能内部/外部設定が有効になります。内部インターフェイスから ASDM を使用して ASA を管理できます。内部インターフェイスは、統合ルーティングとブリッジングを使用してブリッジ グループに配置されます。

- ASA 5508-Xおよび5516-X：工場出荷時のデフォルト設定により、機能内部/外部設定が有効になります。ASAは、内部インターフェイスから ASDM を使用して管理できます。
- ASA 5525-X～ASA 5555-X：管理用のインターフェイスは工場出荷時のデフォルト設定によって設定されるため、ASDMを使用してこのインターフェイスに接続して設定を完了できます。
- Firepower 1010：工場出荷時のデフォルト設定により、機能内部/外部設定が有効になりません。ASAは、管理インターフェイスまたは内部スイッチポートから ASDM を使用して管理できます。
- Firepower 1100：工場出荷時のデフォルト設定により、機能内部/外部設定が有効になりません。ASAは、管理インターフェイスまたは内部インターフェイスから ASDM を使用して管理できます。
- Firepower 2100：プラットフォームモード（デフォルト）：工場出荷時のデフォルト設定により、機能内部/外部設定が有効になります。ASAは、管理インターフェイスから Firepower Chassis Managerと ASDM を使用して管理できます。  
アプライアンスモード：アプライアンスモードに変更すると、工場出荷時のデフォルト設定により、機能内部/外部設定が有効になります。ASAは、管理インターフェイスまたは内部インターフェイスから ASDM を使用して管理できます。
- Firepower 4100/9300 シャーシ：ASAのスタンドアロンまたはクラスタを展開する場合、管理用のインターフェイスは工場出荷時のデフォルト設定によって設定されるため、ASDMを使用してこのインターフェイスに接続して設定を完了できます。
- ASA v：ハイパーバイザによっては、展開の一環として、展開設定（初期の仮想展開設定）によって管理用のインターフェイスが設定されるため、ASDMを使用してこのインターフェイスに接続して設定を完了できます。フェールオーバーIPアドレスも設定できます。また、必要に応じて、「工場出荷時のデフォルト」コンフィギュレーションを適用することもできます。
- ISA 3000：工場出荷時のデフォルト設定は、同じネットワーク上のすべての内部および外部インターフェイスを使用した、ほぼ完全なトランスペアレントファイアウォールモード設定です。ASDMを使用して管理インターフェイスに接続し、ネットワークのIPアドレスを設定できます。ハードウェアバイパスは2つのインターフェイスペアに対して有効になっていて、すべてのトラフィックはインラインタップモニター専用モードで ASA FirePOWER モジュールに送信されます。このモードでは、モニタリング目的でのみトラフィックの重複ストリームが ASA Firepower モジュールに送信されます。

アプライアンスの場合、工場出荷時のデフォルト設定は、工場出荷時のデフォルト設定がトランスペアレントモードでのみ使用可能な ISA 3000 を除き、ルーテッドファイアウォールモードとシングルコンテキストモードのみで使用できます。ASA v および Firepower 4100/9300 シャーシの場合、展開時にトランスペアレントモードまたはルーテッドモードを選択できます。



- (注) イメージファイルと（隠された）デフォルト コンフィギュレーションに加え、`log/`、`crypto_archive/`、および `coredumpinfo/coredump.cfg` がフラッシュ メモリ内の標準のフォルダとファイルです。フラッシュ メモリ内で、これらのファイルの日付は、イメージファイルの日付と一致しない場合があります。これらのファイルは、トラブルシューティングに役立ちますが、障害が発生したことを示すわけではありません。

## 工場出荷時のデフォルト設定の復元

この項では、工場出荷時のデフォルト コンフィギュレーションを復元する方法について説明します。ASA では、この手順を実行することで展開設定が消去され、ASA 5525-X の場合と同じ工場出荷時のデフォルト設定が適用されます。



- (注) Firepower 4100/9300 では、工場出荷時のデフォルト設定を復元すると単に設定が消去されるだけです。デフォルト設定を復元するには、スーパーバイザから ASA をもう一度展開する必要があります。

### 始める前に

この機能は、ISA 3000 を除き、ルーテッドファイアウォールモードでのみ使用できます（ISA 3000 では、このコマンドはトランスペアレントモードでのみサポートされます）。さらに、この機能はシングルコンテキストモードでのみ使用できます。コンフィギュレーションがクリアされた ASA には、この機能を使用して自動的に設定する定義済みコンテキストがありません。

### 手順

**ステップ 1** 工場出荷時のデフォルト コンフィギュレーションを復元します。

**configure factory-default** [*ip\_address* [*mask*]]

例 :

```
ciscoasa(config)# configure factory-default 10.1.1.1 255.255.255.0
```

- (注) このコマンドは、Firepower 2100 の現在設定されているモード（アプライアンスまたはプラットフォーム）をクリアしません。

*ip\_address* を指定する場合は、デフォルトの IP アドレスを使用する代わりに、お使いのモデルに応じて、内部または管理インターフェイスの IP アドレスを設定します。*ip\_address* オプションで設定されているインターフェイスについては、次のモデルのガイドラインを参照してください。

- Firepower 1010 : 管理インターフェイスの IP アドレスを設定します。



- Firepower 1100 : 内部インターフェイスの IP アドレスを設定します。
- アプライアンスモードの Firepower 2100 : 内部インターフェイスの IP アドレスを設定します。
- プラットフォームモードの Firepower 2100 : 管理インターフェイスの IP アドレスを設定します。
- Firepower 4100/9300 : 効果はありません。
- ASAv : 管理インターフェイスの IP アドレスを設定します。
- ASA 5506-X : 内部インターフェイスの IP アドレスを設定します。
- ASA 5508-X および 5516-X : 内部インターフェイスの IP アドレスを設定します。
- ASA 5525-X、5545-X、5555-X : 管理インターフェイスの IP アドレスを設定します。
- ISA 3000 : 管理インターフェイスの IP アドレスを設定します。

**http** コマンドでは、ユーザーが指定するサブネットが使用されます。同様に、**dhcpd address** コマンドの範囲は、指定した IP アドレスよりも大きい使用可能なすべてのアドレスで構成されます。たとえば、サブネットマスク 255.255.255.0 で 10.5.6.78 を指定した場合、DHCP アドレスの範囲は 10.5.6.79 ~ 10.5.6.254 になります。

Firepower 1000、およびアプライアンスモードの Firepower 2100 の場合 : このコマンドは、残りの設定とともに **boot system** コマンドをクリアします (存在する場合)。この設定変更は、ブートアップ時のイメージには影響を与えず、現在ロードされているイメージが引き続き使用されます。

プラットフォームモードの Firepower 2100 の場合 : このモデルでは、**boot system** コマンドは使用されません。パッケージは FXOS によって管理されます。

その他すべてのモデルの場合 : このコマンドは、残りの設定とともに **boot system** コマンドをクリアします (存在する場合)。**boot system** コマンドを使用すると、特定のイメージから起動できます。出荷時の設定に戻した後、次回 ASA をリロードすると、内部フラッシュメモリの最初のイメージからブートします。内部フラッシュメモリにイメージがない場合、ASA はブートしません。

例 :

```
docs-bxb-asa3(config)# configure factory-default 10.86.203.151 255.255.254.0
Based on the management IP address and mask, the DHCP address
pool size is reduced to 103 from the platform limit 256
```

```
WARNING: The boot system configuration will be cleared.
The first image found in disk0:/ will be used to boot the
system on the next reload.
Verify there is a valid image on disk0:/ or the system will
not boot.
```

```
Begin to apply factory-default configuration:
Clear all configuration
```

```
WARNING: The new maximum-session limit will take effect after the running-config is saved
and the system boots next time. Command accepted
```

```
WARNING: Local user database is empty and there are still 'aaa' commands for 'LOCAL'.
Executing command: interface management0/0
Executing command: nameif management
INFO: Security level for "management" set to 0 by default.
Executing command: ip address 10.86.203.151 255.255.254.0
Executing command: security-level 100
Executing command: no shutdown
Executing command: exit
Executing command: http server enable
Executing command: http 10.86.202.0 255.255.254.0 management
Executing command: dhcpd address 10.86.203.152-10.86.203.254 management
Executing command: dhcpd enable management
Executing command: logging asdm informational
Factory-default configuration is completed
ciscoasa(config)#
```

**ステップ2** デフォルト コンフィギュレーションをフラッシュ メモリに保存します。

#### **write memory**

このコマンドでは、事前に **boot config** コマンドを設定して、別の場所を設定していた場合でも、実行コンフィギュレーションはスタートアップコンフィギュレーションのデフォルトの場所に保存されます。コンフィギュレーションがクリアされると、このパスもクリアされます。

## ASA v 導入設定の復元

この項では、ASA v の導入（0 日）設定を復元する方法について説明します。

### 手順

**ステップ1** フェールオーバーを行うために、スタンバイ装置の電源を切ります。

スタンバイ ユニットがアクティブになることを防ぐために、電源をオフにする必要があります。電源を入れたままにした場合、アクティブ装置の設定を消去すると、スタンバイ装置がアクティブになります。以前のアクティブ ユニートをリロードし、フェールオーバー リンクを介して再接続すると、古い設定は新しいアクティブユニットから同期し、必要な導入コンフィギュレーションが消去されます。

**ステップ2** リロード後に導入設定を復元します。フェールオーバーを行うために、アクティブ装置で次のコマンドを入力します。

#### **write erase**

(注) ASA v が現在の実行イメージをブートするため、元のブート イメージには戻りません。元のブートイメージを使用するには、**boot image** コマンドを参照してください。コンフィギュレーションは保存しないでください。

**ステップ3** ASA v をリロードし、導入設定をロードします。

#### **reload**

**ステップ 4** フェールオーバーを行うために、スタンバイ装置の電源を投入します。

アクティブ装置のリロード後、スタンバイ装置の電源を投入します。導入設定がスタンバイ装置と同期されます。

## ASA 5506-X シリーズのデフォルト設定

ASA 5506-X シリーズの出荷時のデフォルトのコンフィギュレーションは、次のとおりです。

- Integrated Routing and Bridging 機能 : GigabitEthernet 1/2 ~ 1/8 はブリッジグループ 1 に所属、ブリッジ仮想インターフェイス (BVI) 1
- 内部 --> 外部へのトラフィックフロー : GigabitEthernet 1/1 (外部)、BVI 1 (内部)
- DHCP の外部 IP アドレス、内部 IP アドレス : 192.168.1.1
- (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 : GigabitEthernet 1/9 (WiFi)
- (ASA 5506W-X) WiFi の IP アドレス : 192.168.10.1
- 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 サーバーとして使用します。
- 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。

このコンフィギュレーションは次のコマンドで構成されています。

```
interface Management1/1
  management-only
  no nameif
  no security-level
  no ip address
  no shutdown
interface GigabitEthernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface GigabitEthernet1/2
  nameif inside_1
  security-level 100
  bridge-group 1
  no shutdown
interface GigabitEthernet1/3
  nameif inside_2
  security-level 100
  no shutdown
  bridge-group 1
interface GigabitEthernet1/4
```

```
nameif inside_3
security-level 100
no shutdown
bridge-group 1
interface GigabitEthernet1/5
nameif inside_4
security-level 100
no shutdown
bridge-group 1
interface GigabitEthernet1/6
nameif inside_5
security-level 100
no shutdown
bridge-group 1
interface GigabitEthernet1/7
nameif inside_6
security-level 100
no shutdown
bridge-group 1
interface GigabitEthernet1/8
nameif inside_7
security-level 100
no shutdown
bridge-group 1
!
interface bvi 1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
!
object network obj_any1
subnet 0.0.0.0 0.0.0.0
nat (inside_1,outside) dynamic interface
object network obj_any2
subnet 0.0.0.0 0.0.0.0
nat (inside_2,outside) dynamic interface
object network obj_any3
subnet 0.0.0.0 0.0.0.0
nat (inside_3,outside) dynamic interface
object network obj_any4
subnet 0.0.0.0 0.0.0.0
nat (inside_4,outside) dynamic interface
object network obj_any5
subnet 0.0.0.0 0.0.0.0
nat (inside_5,outside) dynamic interface
object network obj_any6
subnet 0.0.0.0 0.0.0.0
nat (inside_6,outside) dynamic interface
object network obj_any7
subnet 0.0.0.0 0.0.0.0
nat (inside_7,outside) dynamic interface
!
same-security-traffic permit inter-interface
!
http server enable
http 192.168.1.0 255.255.255.0 inside_1
http 192.168.1.0 255.255.255.0 inside_2
http 192.168.1.0 255.255.255.0 inside_3
http 192.168.1.0 255.255.255.0 inside_4
http 192.168.1.0 255.255.255.0 inside_5
http 192.168.1.0 255.255.255.0 inside_6
http 192.168.1.0 255.255.255.0 inside_7
!
dhcpd auto_config outside
```

```
dhcpd address 192.168.1.5-192.168.1.254 inside
dhcpd enable inside
!
logging asdm informational
```

ASA 5506W-X の場合は、次のコマンドも含まれます。

```
interface GigabitEthernet 1/9
 security-level 100
 nameif wifi
 ip address 192.168.10.1 255.255.255.0
 no shutdown
!
object network obj_any_wifi
 subnet 0.0.0.0 0.0.0.0
 nat (wifi,outside) dynamic interface
!
http 192.168.10.0 255.255.255.0 wifi
!
dhcpd address 192.168.10.2-192.168.10.254 wifi
dhcpd enable wifi
```

## ASA 5508-Xおよび5516-Xのデフォルト設定

ASA 5508-Xおよび5516-Xの工場出荷時のデフォルト設定は、次のとおりです。

- **内部 --> 外部**へのトラフィックフロー：GigabitEthernet 1/1（外部）、GigabitEthernet 1/2（内部）
- DHCPからの**外部 IP アドレス**
- **内部 IP アドレス**：192.168.1.1
- 内部。
- 外部 DHCPからの**デフォルト ルート**
- **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：内部ホストとホストが許可されます。
- **NAT**：内部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。

このコンフィギュレーションは次のコマンドで構成されています。

```
interface Management1/1
 management-only
 no nameif
 no security-level
 no ip address
 no shutdown
interface GigabitEthernet1/1
 nameif outside
```

```
security-level 0
ip address dhcp setroute
no shutdown
interface GigabitEthernet1/2
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
no shutdown
!
object network obj_any
subnet 0.0.0.0 0.0.0.0
nat (any,outside) dynamic interface
!
http server enable
http 192.168.1.0 255.255.255.0 inside
!
dhcpd auto_config outside
dhcpd address 192.168.1.5-192.168.1.254 inside
dhcpd enable inside
!
logging asdm informational
```

## ASA 5525-X ~ ASA 5555-X デフォルト設定

ASA 5525-X ~ ASA 5555-X の工場出荷時のデフォルト設定は、次のとおりです。

- 管理インターフェイス：Management 0/0（管理）。
- IP アドレス：管理アドレスは 192.168.1.1/24 です。
- DHCP サーバー：管理ホストでは DHCP サーバーがイネーブルにされているため、管理インターフェイスに接続するコンピュータには、192.168.1.2 ~ 192.168.1.254 の間のアドレスが割り当てられます。
- ASDM アクセス：管理ホストに許可されます。

このコンフィギュレーションは次のコマンドで構成されています。

```
interface management 0/0
ip address 192.168.1.1 255.255.255.0
nameif management
security-level 100
no shutdown
!
asdm logging informational
asdm history enable
!
http server enable
http 192.168.1.0 255.255.255.0 management
!
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
```

## Firepower 1010 のデフォルト設定

Firepower 1010 の工場出荷時のデフォルト設定は、次のとおりです。

- **ハードウェア スイッチ** : イーサネット 1/2 ~ 1/8 は VLAN 1 に属しています。
- **内部から外部** へのトラフィック フロー : イーサネット 1/1 (外部) 、 VLAN 1 (内部)
- **管理** : 管理 1/1 (管理) 、 IP アドレス : 192.168.45.1
- **DHCP の外部 IP アドレス**、内部 IP アドレス : 192.168.1.1
- 内部インターフェイスの **DHCP サーバー**、管理インターフェイス
- 外部 DHCP からの **デフォルト ルート**
- **ASDM** アクセス : 管理ホストと内部ホストに許可されます。管理ホストは 192.168.45.0/24 ネットワークに限定され、内部ホストは 192.168.1.0/24 ネットワークに限定されます。
- **NAT** : 内部から外部へのすべてのトラフィック用のインターフェイス PAT。
- **DNS** サーバー : OpenDNS サーバーはあらかじめ構成されています。

このコンフィギュレーションは次のコマンドで構成されています。

```
interface Vlan1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
no shutdown
!
interface Management1/1
management-only
nameif management
no shutdown
security-level 100
ip address 192.168.45.1 255.255.255.0
!
interface Ethernet1/1
nameif outside
ip address dhcp setroute
no shutdown
!
interface Ethernet1/2
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/3
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/4
no shutdown
switchport
switchport mode access
```

```
switchport access vlan 1
!
interface Ethernet1/5
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/6
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/7
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/8
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd address 192.168.45.10-192.168.45.12 management
dhcpd enable inside
dhcpd enable management
!
http server enable
http 192.168.45.0 255.255.255.0 management
http 192.168.1.0 255.255.255.0 inside
!
dns domain-lookup outside
dns server-group DefaultDNS
  name-server 208.67.222.222 outside
  name-server 208.67.220.220 outside
!
```

## Firepower 1100 のデフォルト設定

Firepower 1100 の工場出荷時のデフォルト設定は、次のとおりです。

- 内部から外部へのトラフィック フロー : Ethernet 1/1 (外部) 、 Ethernet 1/2 (内部)
- DHCP の外部 IP アドレス、内部 IP アドレス : 192.168.1.1
- 管理 : Management 1/1 (管理) 、 DHCP からの IP アドレス
- 内部インターフェイスの **DHCP サーバー**
- 外部 DHCP、管理 DHCP からのデフォルトルート



- **ASDM** アクセス：管理ホストと内部ホストに許可されます。内部ホストは 192.168.1.0/24 ネットワークに限定されます。
- **NAT**：内部から外部へのすべてのトラフィック用のインターフェイス PAT。
- **DNS** サーバー：OpenDNS サーバーはあらかじめ構成されています。

このコンフィギュレーションは次のコマンドで構成されています。

```
interface Management1/1
  management-only
  nameif management
  security-level 100
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/2
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shutdown
!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
!
http server enable
http 0.0.0.0 0.0.0.0 management
http 192.168.1.0 255.255.255.0 inside
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
dns domain-lookup outside
dns server-group DefaultDNS
  name-server 208.67.222.222 outside
  name-server 208.67.220.220 outside
!
```

## Firepower 2100 プラットフォームモードのデフォルト設定

Firepower 2100 はプラットフォーム モードで実行するように設定できます。デフォルトはアプリケーション モードです。



- (注) 9.13(1) 以前のバージョンでは、プラットフォーム モードがデフォルトであり、唯一のオプションでした。プラットフォーム モードからアップグレードする場合、このモードが維持されます。

## ASA の設定

Firepower 2100 上の ASA の工場出荷時のデフォルト設定は、次のとおりです。

- 内部から外部へのトラフィック フロー：Ethernet 1/1（外部）、Ethernet 1/2（内部）
- DHCP の外部 IP アドレス、内部 IP アドレス：192.168.1.1
- 内部インターフェイスの DHCP サーバー
- 外部 DHCP からのデフォルト ルート
- 管理：管理 1/1（管理）、IP アドレス：192.168.45.1
- ASDM アクセス：管理ホストに許可されます。
- NAT：内部から外部へのすべてのトラフィック用のインターフェイス PAT。
- FXOS 管理トラフィックの開始：FXOS シャーシは、ASA 外部インターフェイス上で管理トラフィックを開始できます。
- DNS サーバー：OpenDNS サーバーはあらかじめ構成されています。

このコンフィギュレーションは次のコマンドで構成されています。

```
interface Management1/1
  management-only
  nameif management
  security-level 100
  ip address 192.168.45.1 255.255.255.0
  no shutdown
!
interface Ethernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/2
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shutdown
!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
!
http server enable
http 192.168.45.0 255.255.255.0 management
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
ip-client outside
!
dns domain-lookup outside
dns server-group DefaultDNS
  name-server 208.67.222.222 outside
```

```
name-server 208.67.220.220 outside
```

## FXOS の設定

Firepower 2100 上の FXOS の工場出荷時のデフォルト設定は、次のとおりです。

- 管理 1/1 : IP アドレス 192.168.45.45
- デフォルト ゲートウェイ : ASA データ インターフェイス
- Firepower Chassis Manager および SSH アクセス : 管理ネットワークからのみ。
- デフォルトのユーザー名 : **admin**、デフォルトのパスワード : **Admin123**
- DHCP サーバー : クライアント IP アドレス範囲 192.168.45.10 ~ 192.168.45.12
- NTP サーバー : Cisco NTP サーバー : 0.sourcefire.pool.ntp.org、1.sourcefire.pool.ntp.org、2.sourcefire.pool.ntp.org
- DNS サーバー : OpenDNS : 208.67.222.222、208.67.220.220
- イーサネット 1/1 およびイーサネット 1/2 : 有効

## Firepower 2100 アプライアンス モードのデフォルト設定

デフォルトでは、Firepower 2100 はアプライアンス モードで実行されます。



- (注) 9.13(1) 以前のバージョンでは、プラットフォーム モードがデフォルトであり、唯一のオプションでした。プラットフォームモードからアップグレードする場合、プラットフォームモードが維持されます。

アプライアンスモードの Firepower 2100 の工場出荷時のデフォルト設定は、次のとおりです。

- 内部から外部へのトラフィック フロー : Ethernet 1/1 (外部) 、 Ethernet 1/2 (内部)
- DHCP の外部 IP アドレス、内部 IP アドレス : 192.168.1.1
- DHCP からの管理 IP アドレス : 管理 1/1 (管理)
- 内部インターフェイスの DHCP サーバー
- 外部 DHCP、管理 DHCP からのデフォルト ルート
- ASDM アクセス : 管理ホストと内部ホストに許可されます。内部ホストは 192.168.1.0/24 ネットワークに限定されます。
- NAT : 内部から外部へのすべてのトラフィック用のインターフェイス PAT。
- DNS サーバー : OpenDNS サーバーはあらかじめ構成されています。

このコンフィギュレーションは次のコマンドで構成されています。

```
interface Management1/1
  management-only
  nameif management
  security-level 100
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/2
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shutdown
!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
!
http server enable
http 0.0.0.0 0.0.0.0 management
http 192.168.1.0 255.255.255.0 management
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
dns domain-lookup outside
dns server-group DefaultDNS
  name-server 208.67.222.222 outside
  name-server 208.67.220.220 outside
!
```

## Firepower 4100/9300 シャーシ デフォルト設定

Firepower 4100/9300 シャーシ上に ASA を展開した場合、ASDM を使用して管理インターフェイスへの接続が可能になる多くのパラメータを事前設定できます。一般的な構成には次の設定があります。

- 管理インターフェイス：
  - Firepower 4100/9300 シャーシスーパーバイザ上で定義された任意の管理タイプインターフェイス
  - 名前は「management」
  - 任意の IP アドレス
  - セキュリティ レベル 0
  - 管理専用

- 管理インターフェイス内のデフォルトルート
- ASDM アクセス：すべてのホストが許可されます。

スタンドアロンユニットの設定は、次のコマンドで構成されます。クラスタユニットの追加の設定については、[ASA クラスタの作成](#) を参照してください。

```
interface <management_ifc>
  management-only
  ip address <ip_address> <mask>
  ipv6 address <ipv6_address>
  ipv6 enable
  nameif management
  security-level 0
  no shutdown
!
http server enable
http 0.0.0.0 0.0.0.0 management
http ::/0 management
!
route management 0.0.0.0 0.0.0.0 <gateway_ip> 1
ipv6 route management ::/0 <gateway_ipv6>
```

## ISA 3000 のデフォルト設定

ISA 3000 の工場出荷時のデフォルト設定は、次のとおりです。

- **トランスペアレントファイアウォールモード**：トランスペアレントファイアウォールは、「Bump In The Wire」または「ステルスファイアウォール」のように動作するレイヤ2ファイアウォールであり、接続されたデバイスへのルータホップとしては認識されません。
- **1ブリッジ仮想インターフェイス**：すべてのメンバーインターフェイスは同じネットワーク内に存在しています（**IPアドレスは事前設定されていません。ネットワークと一致するように設定する必要があります**）：GigabitEthernet 1/1（outside1）、GigabitEthernet 1/2（inside1）、GigabitEthernet 1/3（outside2）、GigabitEthernet 1/4（inside2）
- すべての**内部および外部**インターフェイスは相互通信できます。
- **管理 1/1** インターフェイス：ASDM アクセスの 192.168.1.1/24。
- 管理上のクライアントに対する **DHCP**。
- **ASDM** アクセス：管理ホストに許可されます。
- **ハードウェアバイパス**は、次のインターフェイスペアで有効になっています。GigabitEthernet 1/1 および 1/2。GigabitEthernet 1/3 および 1/4



(注) ISA 3000 への電源が切断され、ハードウェア バイパス モードに移行すると、通信できるのは上記のインターフェイスペアのみになります。inside1 と inside2 および outside1 と outside2 は通信できなくなります。これらのインターフェイス間の既存の接続がすべて失われます。電源が再投入されると、ASA がフローを引き継ぐため、接続が短時間中断されます。

- **ASA FirePOWER モジュール** : すべてのトラフィックが、Inline Tap Monitor-Only モードのモジュールに送信されます。このモードでは、モニタリング目的でのみトラフィックの重複ストリームが ASA Firepower モジュールに送信されます。
- **高精度時間プロトコル** : PTP トラフィックは、Firepower のモジュールに送信されません。

このコンフィギュレーションは次のコマンドで構成されています。

```
firewall transparent

interface GigabitEthernet1/1
  bridge-group 1
  nameif outside1
  security-level 0
  no shutdown
interface GigabitEthernet1/2
  bridge-group 1
  nameif inside1
  security-level 100
  no shutdown
interface GigabitEthernet1/3
  bridge-group 1
  nameif outside2
  security-level 0
  no shutdown
interface GigabitEthernet1/4
  bridge-group 1
  nameif inside2
  security-level 100
  no shutdown
interface Management1/1
  management-only
  no shutdown
  nameif management
  security-level 100
  ip address 192.168.1.1 255.255.255.0
interface BVI1
  no ip address

access-list allowAll extended permit ip any any
access-group allowAll in interface outside1
access-group allowAll in interface outside2

same-security-traffic permit inter-interface

hardware-bypass GigabitEthernet 1/1-1/2
hardware-bypass GigabitEthernet 1/3-1/4
```

```
http server enable
http 192.168.1.0 255.255.255.0 management

dhcpd address 192.168.1.5-192.168.1.254 management
dhcpd enable management

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
access-list sfrAccessList extended permit ip any any
class-map sfrclass
  match access-list sfrAccessList
policy-map global_policy
  class sfrclass
    sfr fail-open monitor-only
service-policy global_policy global
```

## ASAによる展開の設定

ASAを導入すると、ASDMを使用して、Management 0/0 インターフェイスへの接続を可能にする多数のパラメータをプリセットできます。一般的な構成には次の設定があります。

- ルーテッドファイアウォールモードまたはトランスペアレントファイアウォールモード
- Management 0/0 インターフェイス：
  - 名前は「management」
  - IP アドレスまたは DHCP
  - セキュリティ レベル 0
- 管理ホスト IP アドレスのスタティック ルート（管理サブネット上にない場合）
- HTTP サーバーの有効または無効
- 管理ホスト IP アドレス用の HTTP アクセス
- (オプション) GigabitEthernet 0/8 用のフェールオーバー リンク IP アドレス、Management 0/0 のスタンバイ IP アドレス
- DNS サーバー
- スマート ライセンス ID トークン
- スマート ライセンスのスループット レベルおよび標準機能ティア
- (オプション) Smart Call Home HTTP プロキシ URL およびポート
- (オプション) SSH 管理設定：
  - クライアント IP アドレス
  - ローカル ユーザー名とパスワード
  - ローカル データベースを使用する SSH に必要な認証

- (オプション) REST API の有効または無効



(注) Cisco Licensing Authority に ASA を正常に登録するには、ASA にインターネットアクセスが必要です。インターネットに接続してライセンス登録を完了させるには、導入後に追加の設定が必要になることがあります。

スタンドアロンユニットについては、次の設定例を参照してください。

```
interface Management0/0
  nameif management
  security-level 0
  ip address ip_address

  no shutdown
  http server enable
  http management_host_IP mask management
  route management management_host_IP mask gateway_ip 1
  dns server-group DefaultDNS
  name-server ip_address
  call-home
  http-proxy ip_address port port
  license smart
  feature tier standard
  throughput level {100M | 1G | 2G}
  license smart register idtoken id_token
  aaa authentication ssh console LOCAL
  username username password password
  ssh source_IP_address mask management
  rest-api image boot:/path
  rest-api agent
```

フェールオーバー ペアのプライマリ ユニットについては、次の設定例を参照してください。

```
nameif management
  security-level 0
  ip address ip_address standby standby_ip

  no shutdown
  route management management_host_IP mask gateway_ip 1
  http server enable
  http management_host_IP mask management
  dns server-group DefaultDNS
  name-server ip_address
  call-home
  http-proxy ip_address port port
  license smart
  feature tier standard
  throughput level {100M | 1G | 2G}
  license smart register idtoken id_token
  aaa authentication ssh console LOCAL
  username username password password
  ssh source_IP_address mask management
  rest-api image boot:/path
  rest-api agent
  failover
```



```
failover lan unit primary
failover lan interface fover gigabitethernet0/8
failover link fover gigabitethernet0/8
failover interface ip fover primary_ip mask standby standby_ip
```

## アプライアンスまたはプラットフォーム モードへの Firepower 2100 の設定

Firepower 2100 は、FXOS と呼ばれる基盤となるオペレーティングシステムを実行します。Firepower 2100 は、次のモードで実行できます。

- アプライアンスモード (デフォルト) : アプライアンスモードでは、ASA のすべての設定を行うことができます。FXOS CLI からは、高度なトラブルシューティング コマンドのみ使用できます。
- プラットフォーム モード : プラットフォーム モードでは、FXOS で、基本的な動作パラメータとハードウェア インターフェイスの設定を行う必要があります。これらの設定には、インターフェイスの有効化、EtherChannels の確立、NTP、イメージ管理などが含まれます。Firepower Chassis Manager Web インターフェイスまたは FXOS CLI を使用できます。その後、ASDM または ASA CLI を使用して ASA オペレーティング システムにセキュリティ ポリシーを設定できます。

この手順では、モードの変更方法について説明します。モードを変更すると、設定がクリアされ、システムをリロードする必要があります。デフォルト設定は、リロード時に適用されます。**clear configure all** および **configure factory-default** コマンドは、現在のモードをクリアしません。

### 始める前に

モードは、CLI でのみ変更できます。

### 手順

**ステップ 1** (任意) 現在の設定をバックアップします。 [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](#) を参照してください。

アプライアンスモードの設定とプラットフォームモードの設定には多少の違いがありますが、古い設定のコピーを出発点にすることをお勧めします。たとえば、プラットフォームモードの場合、NTP、DNS、および EtherChannel の設定は ASA 設定の一部ではないため、バックアップには含まれませんが、その他のほとんどの ASA 設定は両方のモードで有効です。

**ステップ 2** 現在のモードを表示します。

```
show fxos mode
```

例 :

```
ciscoasa(config)# show fxos mode
Mode is currently set to appliance
```

**ステップ 3** モードをプラットフォームモードに設定します。

**no fxos mode appliance**

**write memory**

**reload**

モードを設定したら、設定を保存してデバイスをリロードする必要があります。リロードする前に、中断することなく、モードを元の値に戻すことができます。

例：

```
ciscoasa(config)# no fxos mode appliance
Mode set to platform mode
WARNING: This command will take effect after the running-config is saved and the system
has been rebooted. Command accepted.
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: c0532471 648dc7c2 4f2b4175 1f162684

23736 bytes copied in 1.520 secs (23736 bytes/sec)
[OK]
ciscoasa(config)# reload
Proceed with reload? [confirm]
```

**ステップ 4** モードをアプライアンス モードに設定します。

**fxos mode appliance**

**write memory**

**reload**

モードを設定したら、設定を保存してデバイスをリロードする必要があります。リロードする前に、中断することなく、モードを元の値に戻すことができます。

例：

```
ciscoasa(config)# fxos mode appliance
Mode set to appliance mode
WARNING: This command will take effect after the running-config is saved and the system
has been rebooted. Command accepted.
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: c0532471 648dc7c2 4f2b4175 1f162684

23736 bytes copied in 1.520 secs (23736 bytes/sec)
[OK]
ciscoasa(config)# reload
Proceed with reload? [confirm]
```

---

## コンフィギュレーション作業

この項では、コンフィギュレーションを処理する方法について説明します。ASAは、スタートアップコンフィギュレーションと呼ばれるコンフィギュレーションをテキストファイルからロードします。このファイルは、デフォルトでは隠しファイルとして内部フラッシュメモリに常駐しています。ただし、ユーザーはスタートアップコンフィギュレーションに異なるパスを指定することができます。

コマンドを入力すると、メモリ上の実行コンフィギュレーションに対してだけ変更が適用されます。変更内容をリブート後も維持するには、実行コンフィギュレーションを手動でスタートアップコンフィギュレーションに保存する必要があります。

この項で説明する内容は、特に指定がない限り、シングルモードとマルチモードの両セキュリティコンテキストに適用されます。

## コンフィギュレーションの変更の保存

この項では、コンフィギュレーションを保存する方法について説明します。

### シングルコンテキストモードでのコンフィギュレーションの変更の保存

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するには、次の手順を実行します。

#### 手順

---

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ます。

#### **write memory**

(注) **copy running-config startup-config** コマンドは、**write memory** コマンドに相当します。

---

### マルチコンテキストモードでのコンフィギュレーションの変更の保存

各コンテキスト（およびシステム）コンフィギュレーションを個別に保存することも、すべてのコンテキストコンフィギュレーションを同時に保存することもできます。

#### 各コンテキストとシステムの個別保存

システムまたはコンテキストのコンフィギュレーションを保存するには、次の手順を使用します。

## 手順

---

コンテキストまたはシステム内から、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ます。

### write memory

マルチ コンテキスト モードでは、コンテキストのスタートアップ コンフィギュレーションを外部サーバーに置くことができます。この場合、ASA は、コンテキスト URL で指定したサーバにコンフィギュレーションを戻して保存します。ただし HTTP URL および HTTPS URL の場合は例外で、サーバにコンフィギュレーションを保存できません。

(注) **copy running-config startup-config** コマンドは、**write memory** コマンドに相当します。

---

## すべてのコンテキスト コンフィギュレーションの同時保存

すべてのコンテキスト コンフィギュレーションとシステム コンフィギュレーションを同時に保存するには、次の手順を使用します。

## 手順

---

システム実行スペースから、すべてのコンテキストとシステム コンフィギュレーションの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ます。

### write memory all [/noconfirm]

**/noconfirm** キーワードを入力しない場合、次のプロンプトが表示されます。

```
Are you sure [Y/N]:
```

**Y** を入力すると、ASA によってシステム コンフィギュレーションと各コンテキストが保存されます。コンテキストのスタートアップコンフィギュレーションは、外部サーバーに配置できます。この場合、ASA は、コンテキスト URL で指定したサーバーにコンフィギュレーションを戻して保存します。ただし HTTP URL および HTTPS URL の場合は例外で、サーバーにコンフィギュレーションを保存できません。

ASA によって各コンテキストが保存された後、次のメッセージが表示されます。

```
'Saving context 'b' ... ( 1/3 contexts saved ) '
```

エラーのためにコンテキストが保存されない場合もあります。エラーについては、次の情報を参照してください。

- メモリ不足のためにコンテキストが保存されない場合は、次のメッセージが表示されません。

```
The context 'context a' could not be saved due to Unavailability of resources
```

- リモートの宛先に到達できないためにコンテキストが保存されない場合は、次のメッセージが表示されます。

```
The context 'context a' could not be saved due to non-reachability of destination
```

- コンテキストがロックされているために保存されない場合は、次のメッセージが表示されます。

```
Unable to save the configuration for the following contexts as these contexts are locked.  
context 'a' , context 'x' , context 'z' .
```

コンテキストがロックされるのは、別のユーザーがすでにコンフィギュレーションを保存している場合、またはコンテキストを削除している場合のみです。

- スタートアップコンフィギュレーションが読み取り専用であるために（たとえば、HTTPサーバーで）コンテキストが保存されない場合は、他のすべてのメッセージの最後に次のメッセージレポートが出力されます。

```
Unable to save the configuration for the following contexts as these contexts have read-only config-urls:  
context 'a' , context 'b' , context 'c' .
```

- フラッシュメモリのセクターが壊れているためコンテキストを保存できない場合は、次のメッセージが表示されます。

```
The context 'context a' could not be saved due to Unknown errors
```

---

## スタートアップコンフィギュレーションの実行コンフィギュレーションへのコピー

新しいスタートアップコンフィギュレーションを実行コンフィギュレーションにコピーするには、次のいずれかのコマンドを使用します。

- **copy startup-config running-config**

スタートアップコンフィギュレーションを実行コンフィギュレーションとマージします。マージによって、新しいコンフィギュレーションから実行コンフィギュレーションに新しいコマンドが追加されます。コンフィギュレーションが同じ場合、変更は発生しません。コマンドが衝突する場合、またはコマンドがコンテキストの実行に影響を与える場合、

マージの結果はコマンドによって異なります。エラーが発生することも、予想できない結果が生じることもあります。

- **reload**

ASA をリロードします。その結果、スタートアップ コンフィギュレーションがロードされ、実行コンフィギュレーションが破棄されます。

- **clear configure all**、続いて **thencopy startup-config running-config**

スタートアップ コンフィギュレーションをロードし、実行コンフィギュレーションを破棄します。リロードは不要です。

## 設定の表示

実行コンフィギュレーションとスタートアップ コンフィギュレーションを表示するには、次のコマンドを使用します。

- **show running-config**

実行コンフィギュレーションを表示します。

- **show running-config command**

特定のコマンドの実行コンフィギュレーションを表示します。

- **show startup-config**

スタートアップ コンフィギュレーションを表示します。

## コンフィギュレーション設定のクリアおよび削除

設定を消去するには、次のいずれかのコマンドを入力します。

- **clear configure configurationcommand [level2configurationcommand]**

指定されたコマンドのすべてのコンフィギュレーションをクリアします。コマンドの特定バージョンのコンフィギュレーションだけをクリアする場合は、*level2configurationcommand* に値を入力します。

たとえば、すべての **aaa** コマンドのコンフィギュレーションをクリアするには、次のコマンドを入力します。

```
ciscoasa (config) # clear configure aaa
```

**aaa authentication** コマンドのコンフィギュレーションだけをクリアするには、次のコマンドを入力します。

```
ciscoasa (config) # clear configure aaa authentication
```

- **no configurationcommand [level2configurationcommand] qualifier**

コマンドの特定のパラメータまたはオプションをディセーブルにします。この場合、**no** コマンドを使用して、*qualifier*で識別される特定のコンフィギュレーションを削除します。

たとえば、特定の **access-list** コマンドを削除するには、それを一意に特定するのに十分なコマンドを入力します。コマンド全体を入力しなければならない場合もあります。

```
ciscoasa(config)# no access-list abc extended permit icmp any any object-group  
obj_icmp_1
```

- **write erase**

スタートアップ コンフィギュレーションを消去します。



---

(注) ASA の場合、このコマンドはリロード後に導入設定を復元します。コンフィギュレーションを完全に消去するには、**clear configure all** コマンドを使用します。

---

- **clear configure all**

実行コンフィギュレーションを消去します。



---

(注) マルチ コンテキスト モードでは、システム コンフィギュレーションから **clear configure all** を入力すると、すべてのコンテキストを削除し、実行中のコンフィギュレーションを停止することにもなります。コンテキストコンフィギュレーションファイルは消去されず、元の場所に保持されます。

---



(注) Firepower 1000、Firepower 2100 (アプライアンスモード) の場合：このコマンドは、残りの設定とともに **boot system** コマンドをクリアします (存在する場合)。この設定変更は、ブートアップ時のイメージには影響を与えず、現在ロードされているイメージが引き続き使用されます。

プラットフォームモードの Firepower 2100 の場合：このモデルでは、**boot system** コマンドは使用されません。パッケージは FXOS によって管理されます。

その他すべてのモデルの場合：このコマンドは、残りの設定とともに **boot system** コマンドをクリアします (存在する場合)。**boot system** コマンドは、外部フラッシュ メモリ カードのイメージを含む、特定のイメージからの起動を可能にします。ASA を次回リロードすると、内部フラッシュ メモリの最初のイメージから起動します。内部フラッシュ メモリにイメージがない場合、ASA は起動しません。



(注) このコマンドは、Firepower 2100 の現在設定されているモード (アプライアンスまたはプラットフォーム) をクリアしません。

## オフラインでテキスト コンフィギュレーション ファイルの作成

このガイドは、CLIを使用したASAの設定方法について説明します。コマンドを保存すると、変更がテキスト ファイルに書き込まれます。一方、CLIを使用する代わりに、テキスト ファイルをコンピュータで直接編集して、コンフィギュレーション モードのコマンドライン プロンプトから、コンフィギュレーションを全部または1行ずつペーストすることができます。別の方法として、ASA 内部フラッシュ メモリにテキスト ファイルをダウンロードします。ASA への設定ファイルのダウンロードについては、[ソフトウェアおよびコンフィギュレーション](#)を参照してください。

ほとんどの場合、このマニュアルで説明するコマンドには、CLIプロンプトが先行します。次の例でのプロンプトは「`ciscoasa(config)#`」です。

```
ciscoasa(config)# context a
```

コマンドの入力が要求されないテキスト コンフィギュレーション ファイルの場合は、プロンプトは次のように省略されます。

```
context a
```



ファイルのフォーマットの詳細については、[コマンドラインインターフェイスの使用](#)を参照してください。

## 接続の設定変更の適用

コンフィギュレーションに対してセキュリティポリシーの変更を加えた場合は、すべての新しい接続で新しいセキュリティポリシーが使用されます。既存の接続では、その接続が確立された時点で設定されていたポリシーの使用が継続されます。古い接続に対する **show** コマンドの出力は古いコンフィギュレーションを反映しており、場合によっては古い接続に関するデータが含まれないことがあります。

たとえば、インターフェイスから **QoS service-policy** を削除し、修正バージョンを再度追加する場合、**show service-policy** コマンドには、新しいサービス ポリシーと一致する新規接続と関連付けられている **QoS** カウンタのみ表示されます。古いポリシーの既存の接続はコマンド出力には表示されません。

すべての接続が新しいポリシーを確実に使用するように、現在の接続を解除し、新しいポリシーを使用して再度接続できるようにします。

接続を解除するには、次のコマンドを入力します。

```
• clear conn[all] [protocol {tcp|udp}] [ address src_ip [-src_ip] [ netmask mask] [ port src_port [-src_port] [ address dest_ip [-dest_ip] [ netmask mask] [ port dest_port [-dest_port]
```

このコマンドは、すべての状態の接続を終了します。現在のすべての接続を表示するには、**show conn** コマンドを参照してください。

引数を指定しないと、このコマンドはすべての **through-the-box** 接続をクリアします。**to-the-box** 接続もクリアするには（現在の管理セッションを含む）、**all** キーワードを使用します。送信元 IP アドレス、宛先 IP アドレス、ポート、プロトコルに基づいて特定の接続をクリアするには、必要なオプションを指定できます。

## ASA のリロード

ASA をリロードするには、次の手順を実行します。

**reload** コマンドは、クラスタリング用のデータノードやフェールオーバー用のスタンバイ/セカンダリユニットには複製されません。

マルチ コンテキスト モードでは、システム実行スペース以外からはリロードできません。

### 手順

---

ASA をリロードします。

**reload**

---

## 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。