CHAPTER 3

スタートアップ ガイド

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。この章は、次の項で構成されています。

アプライアンスのコマンドライン インターフェイスへのアクセス

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。その後は、第 43 章「管理アクセスの設定」の方法によって 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。マルチ コンテキスト モードの詳細については、第 6 章「マルチ コンテキスト モードの設定」を参照してください。

手順の詳細

ステップ 1 付属のコンソール ケーブルを使用して PC 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、ご使用の 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。

hostname>

このプロンプトは、ユーザ EXEC モードで作業していることを示します。ユーザ 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 モードにアクセスするには、次のコマンドを入力します。

```
hostname> enable
```

次のプロンプトが表示されます。

```
Password:
```

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。

ステップ 4　プロンプトに対して、イネーブル パスワードを入力します。

デフォルトではパスワードは空白に設定されているため、Enter キーを押して先に進みます。イネーブル パスワードの変更については、「ホスト名、ドメイン名、およびパスワードの設定」（P.15-1）を参照してください。

プロンプトが次のように変化します。

```
hostname#
```

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 5　グローバル コンフィギュレーション モードにアクセスするには、次のコマンドを入力します。

```
hostname# configure terminal
```

プロンプトが次のように変化します。

```
hostname(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。

コマンドライン ASA サービス モジュールインターフェイスへのアクセス

初期設定の場合、スイッチに（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、ASASM に接続します。ここでは、ASASM CLI のアクセス方法について説明します。ここで説明する内容は、次のとおりです。

- 「ASA サービス モジュール へのログイン」（P.3-2）
- 「コンソール セッションのログアウト」（P.3-5）
- 「Telnet セッションのログ アウト」（P.3-6）

ASA サービス モジュール へのログイン

初期設定の場合、スイッチに（スイッチのコンソール 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、ASASM に接続します。

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、スイッチ環境から ASASM にアクセスするとシステムの実行スペースに入ります。マルチ コンテキスト モードの詳細については、第 6 章「マルチ コンテキスト モードの設定」を参照してください。

その後は、「ASDM、Telnet、または SSH の ASA アクセスの設定」（P.43-1）の方法に従って Telnet または SSH を使用してリモート アクセスを ASASM に直接設定できます。

この項は、次の内容で構成されています。

接続方法に関する情報

スイッチ CLI から、ASASM に接続するには、次の 2 つの方法が使用できます。

- Telnet 接続：**session** コマンドを使用して、ASASM への Telnet 接続を作成します。

  利点を次に示します。

  - ASASM への複数のセッションを同時に使用できます。
  - Telnet セッションは、高速接続です。

  制限を次に示します。

  - Telnet セッションは、ASASM リロード時に終了し、タイムアウトします。
  - 完全にロードするまで ASASM にアクセスできません。したがって、ROMMON にアクセスできません。

- 仮想コンソール接続：**service-module session** コマンドを使用して、ASASM への仮想コンソール接続を作成します。仮想コンソール接続は、実際のコンソール接続の利点と制限をすべて備えています。

  利点を次に示します。

  - 接続はリロード中も持続し、タイムアウトしません。
  - ASASM リロード中も接続を維持でき、スタートアップ メッセージが表示されます。
  - ASASM がイメージをロードできない場合、ROMMON にアクセスできます。

  制限を次に示します。

  - 接続が低速です（9600 ボー）。
  - 一度にアクティブにできるコンソール接続は 1 つだけです。

（注） 接続の永続性のため、ASASM を正しくログ アウトしないと、意図よりも長く接続が存在する可能性があります。他の人がログインする場合は、既存の接続を終了する必要があります。詳細については、「コンソール セッションのログアウト」（P.3-5）を参照してください。

ログイン

ASASM にログインし、グローバル コンフィギュレーション モードにアクセスするには、次の手順を実行します。

手順の詳細

	コマンド	目的
ステップ 1	スイッチから、次のいずれかを実行します。	

	session [**switch** {**1** |**2**}] **slot** *number* **processor 1**
	
	ログイン パスワードの入力が求められます。
	`hostname passwd:`
	
	例：
	`Router# session slot number processor 1`
	`hostname passwd: cisco`
	`hostname>`
		スイッチ CLI から、バックプレーンを経由して ASASM に Telnet で接続するには、このコマンドを入力します。
		VSS 内のスイッチの場合、**switch** 引数を入力します。
		（注） **session** *slot* **processor 0** コマンドは、他のサービス モジュールではサポートされていますが、ASASM ではサポートされていません。ASASM にはプロセッサ 0 がありません。
		モジュールのスロット番号を表示するには、スイッチ プロンプトで **show module** コマンドを入力します。
		ASASM にログイン パスワードを入力します。デフォルトのパスワードは、**cisco** です。
		ユーザ EXEC モードにアクセスします。

	service-module session [**switch** {**1** | **2**}] **slot** *number*
	
	例：
	`Router# service-module session slot 3`
	`hostname>`
		スイッチ CLI から、ASASM へのコンソール アクセスを取得するには、このコマンドを入力します。
		VSS 内のスイッチの場合、**switch** 引数を入力します。
		モジュールのスロット番号を表示するには、スイッチ プロンプトで **show module** コマンドを入力します。
		ユーザ EXEC モードにアクセスします。

ステップ 2	**enable**
	
	例：
	`hostname> enable`
	`Password:`
	`hostname#`
		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。
		プロンプトに対して、イネーブル パスワードを入力します。デフォルトでは、パスワードは空白です。イネーブル パスワードを変更するには、「ホスト名、ドメイン名、およびパスワードの設定」（P.15-1）を参照してください。
		特権 EXEC 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	**configure terminal**
	
	例：
	`hostname# configure terminal`
	`hostname(config)#`
		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。
		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** コマンド、**exit** コマンド、または **quit** コマンドを入力します。

コンソール セッションのログアウト

この項は、次の内容で構成されています。

ログアウト

ASASM からログアウトしない場合、コンソール接続は維持され、タイムアウトはありません。ASASM コンソール セッションを終了してスイッチの CLI にアクセスするには、次の手順を実行します。

意図せずに開いたままになっている可能性のある、別のユーザのアクティブな接続を終了するには、「アクティブなコンソール接続の終了」（P.3-5）を参照してください。

手順の詳細

ステップ 1　スイッチ CLI に戻るには、次を入力します。

Ctrl+Shift+6、X

スイッチ プロンプトに戻ります。

```
asasm# [Ctrl-Shift-6, x]
Router#
```

（注）　米国および英国キーボードの Shift+6 はキャレット記号（^）を出力します。別のキーボードを使用しており、単独の文字としてキャレット記号（^）を出力できない場合、一時的または永続的に、エスケープ文字を別の文字に変更できます。**terminal escape-character** *ascii_number* コマンド（このセッションで変更する）、または **default escape-character** *ascii_number* コマンド（永続的に変更する）を使用します。たとえば、現在のセッションのシーケンスを Ctrl+w、x に変更するには、**terminal escape-character 23** を入力します。

アクティブなコンソール接続の終了

コンソール接続の永続性のため、ASASM を正しくログ アウトしないと、意図よりも長く接続が存在する可能性があります。他の人がログインする場合は、既存の接続を終了する必要があります。

手順の詳細

ステップ 1　スイッチ CLI から、**show users** コマンドを使用して、接続されたユーザを表示します。コンソール ユーザは「con」と呼ばれます。ホスト アドレスは、127.0.0.*slot*0 と表示されます（*slot* はモジュールのスロット番号です）。

```
Router# show users
```

たとえば、次のコマンド出力は、スロット 2 にあるモジュールのライン 0 のユーザの「con」を示しています。

```
Router# show users
```

```
Line       User       Host(s)              Idle       Location
*  0       con 0     127.0.0.20           00:00:02
```

ステップ 2　コンソール接続のあるラインをクリアするには、次のコマンドを入力します。

```
Router# clear line number
```

例：

```
Router# clear line 0
```

Telnet セッションのログ アウト

スイッチの CLI へのアクセスを終了し、Telnet セッションを再開または切断するには、次の手順を実行します。

手順の詳細

ステップ 1　スイッチ CLI に戻るには、次を入力します。

Ctrl+Shift+6、X

スイッチ プロンプトに戻ります。

```
asasm# [Ctrl-Shift-6, x]
Router#
```

（注）　米国および英国キーボードの Shift+6 はキャレット記号（^）を出力します。別のキーボードを使用しており、単独の文字としてキャレット記号（^）を出力できない場合、一時的または永続的に、エスケープ文字を別の文字に変更できます。Cisco IOS では、ASASM とセッションを開始する前に、**terminal escape-character** *ascii_number* コマンド（このセッションで変更する）、または **default escape-character** *ascii_number* コマンド（永続的に変更する）を使用します。たとえば、Ctrl+w、x にシーケンスを一時的に変更するには、**terminal escape-character 23** を入力します。次にスイッチにログインしたときには、エスケープ文字はデフォルトに戻ります。

ステップ 2　Telnet セッションを再開するには、スイッチ プロンプトで Enter キーを押します。

ステップ 3　Telnet セッションを切断するには、スイッチの CLI で次のコマンドを入力します。

```
Router# disconnect
```

セッションを切断しない場合、ASASM 設定に従って、最終的にタイムアウトします。

アプライアンス用の ASDM アクセスの設定

ASDM アクセスでは、管理インターフェイスを使用してネットワーク経由で通信するための、最小限の設定を行う必要があります。この項では、次のトピックについて取り上げます。

- 「工場出荷時のデフォルト設定を使用した ASDM へのアクセス」（P.3-7）

- 「デフォルト以外の設定を使用した ASDM へのアクセス（ASA 5505）」（P.3-7）
- 「デフォルト以外の設定を使用した ASDM へのアクセス（ASA 5510 以降）」（P.3-9）

工場出荷時のデフォルト設定を使用した ASDM へのアクセス

工場出荷時のデフォルト設定を使用する場合（「工場出荷時のデフォルト コンフィギュレーション」（P.3-18）を参照）、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。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。
  - ASA 5505 : ASDM への接続に使用するスイッチ ポートは Ethernet 0/0 以外であればどのポートでもかまいません。
  - ASA 5510 以降：ASDM に接続するインターフェイスは Management 0/0 です。
- デフォルトの管理アドレスは 192.168.1.1 です。
- ASDM へのアクセスを許可されるクライアントは、192.168.1.0/24 ネットワーク上にある必要があります。デフォルト設定により DHCP がイネーブルにされるため、管理ステーションにはこの範囲内の IP アドレスを割り当てることができます。他のクライアント IP アドレスから ASDM にアクセスできるようにするには、「ASDM、Telnet、または SSH の ASA アクセスの設定」（P.43-1）を参照してください。

ASDM を起動するには、「ASDM の起動」（P.3-14）を参照してください。

（注） マルチ コンテキスト モードを変更するには、「マルチ コンテキスト モードのイネーブル化とディセーブル化」（P.6-16）を参照してください。マルチ コンテキスト モードに変更すると、管理コンテキストから上記のネットワーク設定を使用して ASDM にアクセスできるようになります。

デフォルト以外の設定を使用した ASDM へのアクセス（ASA 5505）

工場出荷時のデフォルト設定がない場合や、設定を変更する場合、またはトランスペアレント ファイアウォール モードに変更する場合は、次の手順を実行します。「ASA 5505 のデフォルト コンフィギュレーション」（P.3-19）のサンプル設定も参照してください。

前提条件

「アプライアンスのコマンドライン インターフェイスへのアクセス」（P.3-1）に従って、CLI にアクセスします。

手順の詳細

	コマンド	目的
ステップ 1	（任意） **firewall transparent** **例：** `hostname(config)# firewall transparent`	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。詳細については、「ファイアウォール モードの設定」（P.5-1）を参照してください。
ステップ 2	ご使用のモードに応じて、次のいずれかの操作を行って管理インターフェイスを設定します。	

	コマンド	目的
	ルーテッド モード： **interface vlan** *number* 　**ip address** *ip_address* [*mask*] 　**nameif** *name* 　**security-level** *level* **例：** hostname(config)# interface vlan 1 hostname(config-if)# ip address 192.168.1.1 255.255.255.0 hostname(config-if)# nameif inside hostname(config-if)# security-level 100	ルーテッド モードでインターフェイスを設定します。 **security-level** は、1 ～ 100 の数字です。100 が最も安全です。
	トランスペアレント モード： **interface bvi** *number* 　**ip address** *ip_address* [*mask*] **interface vlan** *number* 　**bridge-group** *bvi_number* 　**nameif** *name* 　**security-level** *level* **例：** hostname(config)# interface bvi 1 hostname(config-if)# ip address 192.168.1.1 255.255.255.0 hostname(config)# interface vlan 1 hostname(config-if)# bridge-group 1 hostname(config-if)# nameif inside hostname(config-if)# security-level 100	ブリッジ仮想インターフェイスを設定し、ブリッジ グループに管理 VLAN を割り当てます。**security-level** は、1 ～ 100 の数字です。100 が最も安全です。
ステップ 3	**interface ethernet 0/***n* 　**switchport access vlan** *number* 　**no shutdown** **例：** hostname(config)# interface ethernet 0/1 hostname(config-if)# switchport access vlan 1 hostname(config-if)# no shutdown	管理スイッチポートをイネーブルにして、管理 VLAN に割り当てます。
ステップ 4	**dhcpd address** *ip_address-ip_address* *interface_name* **dhcpd enable** *interface_name* **例：** hostname(config)# dhcpd address 192.168.1.5-192.168.1.254 inside hostname(config)# dhcpd enable inside	管理インターフェイス ネットワーク上の管理ホストに対して DHCP をイネーブルにします。この範囲内には管理アドレスを含めないでください。 **（注）** IPS モジュールがインストールされている場合、IPS モジュールはデフォルトで 192.168.1.2 を内部管理アドレス用に使用します。そのため、このアドレスは DHCP 範囲内に含めないでください。必要に応じて、ASA を使用して IPS モジュール管理アドレスを後から変更できます。
ステップ 5	**http server enable** **例：** hostname(config)# http server enable	ASDM 用に HTTP サーバをイネーブルにします。

	コマンド	目的
ステップ 6	**http** *ip_address mask interface_name* **例：** `hostname(config)# http 192.168.1.0 255.255.255.0 inside`	管理ホストが ASDM にアクセスできるようにします。
ステップ 7	**write memory** **例：** `hostname(config)# write memory`	設定を保存します。
ステップ 8	ASDM を起動するには、「ASDM の起動」（P.3-14）を参照してください。	

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、VLAN 1 インターフェイスが設定されて BVI 1 に割り当てられ、スイッチポートがイネーブルにされ、管理ホストに対して ASDM がイネーブルにされます。

```
firewall transparent
interface bvi 1
    ip address 192.168.1.1 255.255.255.0
interface vlan 1
    bridge-group 1
    nameif inside
    security-level 100
interface ethernet 0/1
    switchport access vlan 1
    no shutdown
dhcpd address 192.168.1.5-192.168.1.254 inside
dhcpd enable inside
http server enable
http 192.168.1.0 255.255.255.0 inside
```

デフォルト以外の設定を使用した ASDM へのアクセス（ASA 5510 以降）

工場出荷時のデフォルト設定がない場合、またはファイアウォール モードまたはコンテキスト モードに変更する場合は、次の手順を実行します。

前提条件

「アプライアンスのコマンドライン インターフェイスへのアクセス」（P.3-1）に従って、CLI にアクセスします。

手順の詳細

	コマンド	目的
ステップ 1	（任意） **firewall transparent** **例：** `hostname(config)# firewall transparent`	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。詳細については、「ファイアウォール モードの設定」（P.5-1）を参照してください。

ステップ 2	**interface management 0/0**
	ip address *ip_address mask*
	nameif *name*
	security-level *number*
	no shutdown
	
	例：
	`hostname(config)# interface management 0/0`
	`hostname(config-if)# ip address 192.168.1.1 255.255.255.0`
	`hostname(config-if)# nameif management`
	`hostname(config-if)# security-level 100`
	`hostname(config-if)# no shutdown`
		Management 0/0 インターフェイスを設定します。**security-level** は、1 ～ 100 の数字です。100 が最も安全です。

ステップ 3	（直接接続された管理ホストの場合）
	dhcpd address *ip_address-ip_address interface_name*
	dhcpd enable *interface_name*
	
	例：
	`hostname(config)# dhcpd address 192.168.1.2-192.168.1.254 management`
	`hostname(config)# dhcpd enable management`
		管理インターフェイス ネットワーク上の管理ホストに対して DHCP をイネーブルにします。この範囲内には Management 0/0 アドレスを含めないでください。

ステップ 4	（リモート管理ホストの場合） **route** *management_ifc management_host_ip mask gateway_ip* **1** **例：** `hostname(config)# route management 10.1.1.0 255.255.255.0 192.168.1.50`	管理ホストへのルートを設定します。
ステップ 5	**http server enable** **例：** `hostname(config)# http server enable`	ASDM 用に HTTP サーバをイネーブルにします。
ステップ 6	**http** *ip_address mask interface_name* **例：** `hostname(config)# http 192.168.1.0 255.255.255.0 management`	管理ホストが ASDM にアクセスできるようにします。

	コマンド	目的
ステップ 7	**write memory** **例：** `hostname(config)# write memory`	設定を保存します。
ステップ 8	（任意） **mode multiple** **例：** `hostname(config)# mode multiple`	モードをマルチ モードに設定します。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。ASASM をリロードするよう求められます。詳細については、第 6 章「マルチ コンテキスト モードの設定」を参照してください。
ステップ 9	ASDM を起動するには、「ASDM の起動」（P.3-14）を参照してください。	

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
```

ASA サービス モジュール の ASDM アクセスの設定

ASASM には物理インターフェイスがないため、ASDM アクセス用に事前設定されていません。ASASM の CLI を使用して ASDM アクセスを設定する必要があります。ASDM アクセス用に ASASM を設定するには、次の手順を実行します。

前提条件

- 「ASA サービス モジュールへの VLAN の割り当て」（P.2-4）従って、ASASM に VLAN インターフェイスを割り当てます。
- 「コマンドライン ASA サービス モジュールインターフェイスへのアクセス」（P.3-2）に従って、ASASM に接続し、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。

手順の詳細

	コマンド	目的
ステップ 1	（任意） **firewall transparent** **例：** `hostname(config)# firewall transparent`	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、コンフィギュレーションをクリアします。詳細については、「ファイアウォール モードの設定」（P.5-1）を参照してください。
ステップ 2	モードに応じて、次のいずれかの手順を実行し、管理インターフェイスを設定します。	

	ルーテッド モード：
	interface vlan *number*
	　ip address *ip_address* [*mask*]
	　nameif *name*
	　security-level *level*
	
	例：
	`hostname(config)# interface vlan 1`
	`hostname(config-if)# ip address 192.168.1.1 255.255.255.0`
	`hostname(config-if)# nameif inside`
	`hostname(config-if)# security-level 100`
		ルーテッド モードでインターフェイスを設定します。**security-level** は、1 ～ 100 の番号です（100 が最も安全です）。

	トランスペアレント モード：
	interface bvi *number*
	　ip address *ip_address* [*mask*]
	
	interface vlan *number*
	　bridge-group *bvi_number*
	　nameif *name*
	　security-level *level*
	
	例：
	`hostname(config)# interface bvi 1`
	`hostname(config-if)# ip address 192.168.1.1 255.255.255.0`
	
	`hostname(config)# interface vlan 1`
	`hostname(config-if)# bridge-group 1`
	`hostname(config-if)# nameif inside`
	`hostname(config-if)# security-level 100`
		ブリッジ仮想インターフェイスを設定し、ブリッジ グループに管理 VLAN を割り当てます。**security-level** は、1 ～ 100 の番号です（100 が最も安全です）。

ステップ 3	（直接接続された管理ホストの場合）
	dhcpd address *ip_address-ip_address interface_name*
	dhcpd enable *interface_name*
	
	例：
	`hostname(config)# dhcpd address 192.168.1.2-192.168.1.254 inside`
	`hostname(config)# dhcpd enable inside`
		管理インターフェイスのネットワーク上の管理ホストの DHCP をイネーブルにします。管理アドレスがその範囲が含まれていないことを確認します。

	コマンド	目的
ステップ 4	（リモート管理ホストの場合） **route** *management_ifc management_host_ip mask gateway_ip* **1** **例：** hostname(config)# route management 10.1.1.0 255.255.255.0 192.168.1.50	管理ホストへのルートを設定します。
ステップ 5	**http server enable** **例：** hostname(config)# http server enable	ASDM の HTTP サーバをイネーブルにします。
ステップ 6	**http** *ip_address mask interface_name* **例：** hostname(config)# http 192.168.1.0 255.255.255.0 management	管理ホストの ASDM へのアクセスを許可します。
ステップ 7	**write memory** **例：** hostname(config)# write memory	設定を保存します。
ステップ 8	（任意） **mode multiple** **例：** hostname(config)# mode multiple	モードをマルチ モードに設定します。プロンプトが表示されたら、既存のコンフィギュレーションを管理コンテキストに変換することを確定します。ASASM をリロードするよう求められます。詳細については、第 6 章「マルチ コンテキスト モードの設定」を参照してください。
ステップ 9	ASDM を起動するには、「ASDM の起動」（P.3-14）を参照してください。	

例

次のルーテッド モードの設定では、VLAN 1 のインターフェイスを設定し、管理ホストの ASDM のイネーブルにします。

```
interface vlan 1
    nameif inside
    ip address 192.168.1.1 255.255.255.0
    security-level 100
dhcpd address 192.168.1.3-192.168.1.254 inside
dhcpd enable inside
http server enable
http 192.168.1.0 255.255.255.0 inside
```

次の設定では、ファイアウォール モードをトランスペアレント モードに変換し、VLAN 1 インターフェイスを設定してから、BVI 1 に割り当て、管理ホストの ASDM をイネーブルにします。

```
firewall transparent
interface bvi 1
    ip address 192.168.1.1 255.255.255.0
interface vlan 1
    bridge-group 1
    nameif inside
```

```
    security-level 100
dhcpd address 192.168.1.3-192.168.1.254 inside
dhcpd enable inside
http server enable
http 192.168.1.0 255.255.255.0 inside
```

ASDM の起動

次の 2 種類の方法を使用して ASDM を起動できます。

- 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、Launcher を再度ダウンロードする必要はありません。ラウンチャでは、ローカルにダウンロードされたファイルを使用してデモ モードで仮想 ASDM を実行することができます。
- Java Web Start：管理する ASA それぞれに対して 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 PC にアプリケーションを保存できます。ただし、ASA IP アドレスごとにアプリケーションを分ける必要があります。

（注） ASDM では、管理のために別の ASA IP アドレスを選択できます。Launcher と Java Web Start アプリケーション機能性の違いは、主に、ユーザがどのように ASA に接続し、ASDM を起動するかにあります。

この項では、まず ASDM に接続する方法について説明します。次に Launcher または Java Web Start アプリケーションを使用して ASDM を起動する方法について説明します。この項は、次の内容で構成されています。

- 「ASDM への初回の接続」（P.3-14）
- 「ASDM-IDM ランチャによる ASDM の起動」（P.3-15）
- 「Java Web Start アプリケーションによる ASDM の起動」（P.3-16）
- 「デモ モードでの ASDM の使用」（P.3-16）

（注） ASDM では複数の PC やワークステーションでそれぞれブラウザ セッションを開き、同じ ASA ソフトウェアを使用できます。1 つの ASA で、シングル ルーテッド モードの ASDM 並行セッションを 5 つまでサポートできます。PC またはワークステーションはそれぞれ、指定した ASA のセッションを 1 つだけブラウザで実行できます。マルチ コンテキスト モードの場合、コンテキストあたり 5 つの ASDM 並行セッションを実行でき、ASA あたり合計 32 セッションまで接続できます。

ASDM への初回の接続

ASDM-IDM Launcher または Java Web Start アプリケーションをダウンロードするために、ASDM に最初に接続するには、次の手順を実行します。

ステップ 1　ASA ネットワーク上のサポートされる Web ブラウザで、次の URL を入力します。

https://*interface_ip_address***/admin**

interface_ip_address は ASA の管理 IP アドレスです。管理アクセスの詳細については、「アプライアンス用の ASDM アクセスの設定」（P.3-6）または「ASA サービス モジュール の ASDM アクセスの設定」（P.3-11）を参照してください。

ASDM の実行要件については、お使いのリリースの ASDM リリース ノートを参照してください。

ASDM の起動ページには、次のボタンが表示されます。

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

ステップ 2　Launcher 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. ユーザ名とパスワードを入力し、[OK] をクリックします。工場出荷時のデフォルト設定の場合、これらのフィールドを空白のままにしておきます。HTTPS 認証が設定されていない場合、ユーザ名はなしで、デフォルトが空白である**イネーブル** パスワードを使用して、ASDM へのアクセスを取得できます。HTTPS 認証がイネーブルの場合、ユーザ名と関連付けられたパスワードを入力します。

c. インストーラを PC 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 Launcher が自動的に開きます。

d. Launcher を使用して ASDM へ接続するには、「ASDM-IDM ランチャによる ASDM の起動」（P.3-15）を参照してください。

ステップ 3　Java Web Start アプリケーションを使用するには、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、PC にアプリケーションを保存します。保存する代わりに任意で Java Web Start アプリケーションを開くことができます。

c. Java Web Start アプリケーション使用して ASDM へ接続するには、「Java Web Start アプリケーションによる ASDM の起動」（P.3-16）を参照してください。

ASDM-IDM ランチャによる ASDM の起動

ASDM-IDM ランチャから ASDM を起動するには、次の手順を実行します。

前提条件

「ASDM への初回の接続」（P.3-14）に従って、ASDM-IDM Launcher をダウンロードします。

手順の詳細

ステップ 1　ASDM-IDM Launcher アプリケーションを起動します。

ステップ 2　接続する ASA IP アドレスまたはホスト名を入力するか選択します。IP アドレスのリストをクリアするには、[Device/IP Address/Name] フィールドの横にあるゴミ箱アイコンをクリックします。

ステップ 3　ユーザ名とパスワードを入力し、[OK] をクリックします。

工場出荷時のデフォルト設定の場合、これらのフィールドを空白のままにしておきます。HTTPS 認証が設定されていない場合、ユーザ名はなしで、デフォルトが空白である**イネーブル** パスワードを使用して、ASDM へのアクセスを取得できます。HTTPS 認証がイネーブルの場合、ユーザ名と関連付けられたパスワードを入力します。

新しいバージョンの ASDM が ASA にある場合、ASDM ランチャは自動的に新しいバージョンをダウンロードし、ASDM を起動する前に現在のバージョンをアップデートするようにユーザに要求します。

メイン ASDM ウィンドウが表示されます。

Java Web Start アプリケーションによる ASDM の起動

Java Web Start アプリケーションから ASDM を起動するには、次の手順を実行します。

前提条件

「ASDM への初回の接続」（P.3-14）に従って Java Web Start アプリケーションをダウンロードします。

手順の詳細

ステップ 1　Java Web Start アプリケーションを起動します。

ステップ 2　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。

ステップ 3　ユーザ名とパスワードを入力し、[OK] をクリックします。工場出荷時のデフォルト設定の場合、これらのフィールドを空白のままにしておきます。HTTPS 認証が設定されていない場合、ユーザ名はなしで、デフォルトが空白である**イネーブル** パスワードを使用して、ASDM へのアクセスを取得できます。HTTPS 認証がイネーブルの場合、ユーザ名と関連付けられたパスワードを入力します。

メイン ASDM ウィンドウが表示されます。

デモ モードでの ASDM の使用

アプリケーション ASDM Demo Mode を別途インストールして使用すると、実デバイスを使用せずに ASDM を実行できます。このモードでは、次の操作を実行できます。

- 実デバイス接続時と同じように、ASDM から設定と選択した監視タスクを実行する。
- ASDM インターフェイスによる ASDM または ASA 機能のデモを実行する。
- CSC SSM を使用して設定および監視タスクを実行する。
- リアルタイムの syslog メッセージを含む、シミュレーションされたモニタリングデータとロギング データを取得する。表示データはランダムに生成されますが、実デバイスに接続しているような体験ができます。

このモードは、次の機能をサポートするように更新されました。

- シングル ルーテッド モードの ASA および侵入防御でのグローバル ポリシー。
- シングル ルーテッド モードの ASA およびファイアウォール DMZ でのオブジェクト NAT。

- シングル ルーテッド モードの ASA およびセキュリティ コンテキストでのボットネット トラフィック フィルタ。
- IPv6 のサイト間 VPN（クライアントレス SSL VPN および IPSec VPN）
- 無差別モードの IDS（侵入防御）
- Unified Communication Wizard

このモードでは、次の機能はサポートされません。

- GUI に表示されたコンフィギュレーションに加えた変更内容の保存
- ファイルまたはディスクの操作
- 履歴モニタリングデータ
- 非管理ユーザ
- 次の機能
  - [File] メニュー
    Save Running Configuration to Flash
    Save Running Configuration to TFTP Server
    Save Running Configuration to Standby Unit
    Save Internal Log Buffer to Flash
    Clear Internal Log Buffer
  - [Tools] メニュー
    Command Line Interface
    ping
    File Management
    Update Software
    File Transfer
    Upload Image from Local PC
    System Reload
  - ツールバー / ステータスバー > [Save]
  - [Configuration] > [Interface] > [Edit Interface] > [Renew DHCP Lease]
  - フェールオーバー後のスタンバイ デバイスの設定
- コンフィギュレーションの再読み込みが発生する操作。再読み込みが行われると GUI が元のコンフィギュレーションに戻ります。
  - コンテキストの切り換え
  - [Interface] ペインの変更
  - [NAT] ペインの変更
  - [Clock] ペインの変更

ASDM のデモ モードを実行するには、次の手順を実行します。

ステップ 1　ASDM Demo Mode インストーラの asdm-demo-*version*.msi を次の場所からダウンロードします。
http://www.cisco.com/cisco/web/download/index.html

ステップ 2　インストーラをダブルクリックして、ソフトウェアをインストールします。

ステップ 3　デスクトップ上の Cisco ASDM Launcher のショートカットをダブルクリックするか、または、[Start] メニューから開きます。

ステップ 4　[Run in Demo Mode] チェックボックスをオンにします。

[Demo Mode] ウィンドウが表示されます。

工場出荷時のデフォルト コンフィギュレーション

出荷時のデフォルトのコンフィギュレーションは、シスコが新しい ASA に適用しているコンフィギュレーションです。

- ASA 5505：工場出荷時のデフォルト設定によりインターフェイスと NAT が設定されているため、ASA をすぐにネットワークで使用できます。
- ASA 5510 以降：工場出荷時のデフォルト設定により管理用のインターフェイスが設定されており、ASDM を使用してこれに接続できます。このインターフェイスを使用して、設定を完了できます。

工場出荷時のデフォルト コンフィギュレーションは、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 モードだけで使用できます。マルチ コンテキスト モードの詳細については、第 6 章「マルチ コンテキスト モードの設定」を参照してください。ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードの詳細については、第 5 章「トランスペアレント ファイアウォールまたはルーテッド ファイアウォールの設定」を参照してください。ASA 5505 のトランスペアレント モードのサンプル設定は、この項に示されています。

（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。

この項では、次のトピックについて取り上げます。

工場出荷時のデフォルト コンフィギュレーションの復元

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。

制限事項

この機能は、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。トランスペアレント モードの場合、インターフェイスの IP アドレスがサポートされません。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のコンテキストがありません。

手順の詳細

	コマンド	目的
ステップ 1	**configure factory-default** [*ip_address* [*mask*]] **例：** hostname(config)# **configure factory-default 10.1.1.1 255.255.255.0**	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。 *ip_address* を指定する場合は、デフォルトの IP アドレス 192.168.1.1 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。**http** コマンドでは、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、指定したサブネット内のアドレスで構成されます。 **（注）** このコマンドは、**boot system** コマンド（存在する場合）も、他のコンフィギュレーションとともにクリアします。**boot system** コマンドを使用すると、外部フラッシュ メモリ カードに保存されているイメージなどの、特定のイメージからブートできます。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。
ステップ 2	**write memory** **例：** active(config)# write memory	デフォルト設定をフラッシュ メモリに保存します。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。

次の作業

ASA の設定を開始するには、「コンフィギュレーションの処理」（P.3-23）を参照してください。

ASA 5505 のデフォルト コンフィギュレーション

デフォルト設定は、ルーテッド モードでのみ使用できます。この項では、デフォルト設定について説明するほか、コピーして貼り付け、出発点として使用できるトランスペアレント モードのサンプル設定も紹介します。この項では、次のトピックについて取り上げます。

- 「ASA 5505 ルーテッド モードのデフォルト設定」（P.3-19）
- 「ASA 5505 トランスペアレント モードのサンプル設定」（P.3-21）

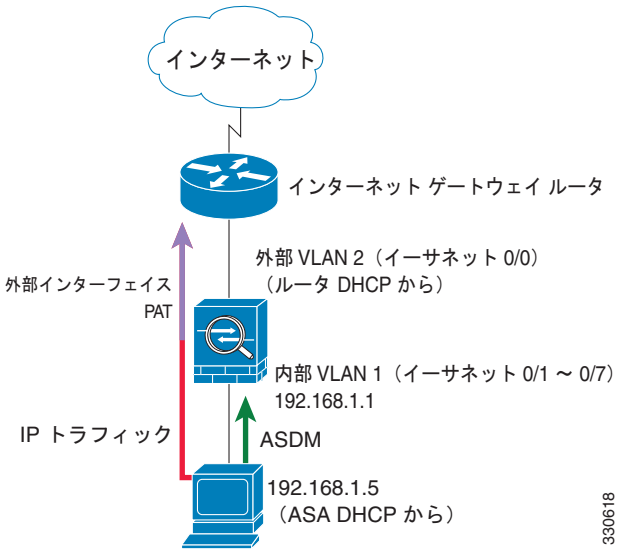
ASA 5505 ルーテッド モードのデフォルト設定

ASA 5505 の工場出荷時のデフォルト設定は、次のとおりです。

- インターフェイス：内部（VLAN 1）および外部（VLAN 2）。
- イネーブルにされ割り当てられているスイッチポート：Ethernet 0/1 ～ 0/7 スイッチポートが内部に割り当てられています。Ethernet 0/0 は外部に割り当てられています。
- IP アドレス：外部アドレスは DHCP から取得されます。内部アドレスは手動で 192.168.1.1/24 に設定します。

- ネットワーク アドレス変換（NAT）：すべての内部 IP アドレスが、外部にアクセスするときにインターフェイス PAT によって変換されます。
- トラフィック フロー：内部から外部への IPv4 および IPv6 トラフィックが許可されます（この動作は ASA で暗黙的に行われます）。外部ユーザが内部にアクセスすることはできません。
- DHCP サーバ：内部ホストでは DHCP サーバがイネーブルにされているため、内部インターフェイスに接続する PC には、192.168.1.5 ～ 192.168.1.254 の間のアドレスが割り当てられます。外部インターフェイス上の DHCP クライアントから取得される DNS、WINS、およびドメイン情報は、内部インターフェイス上の DHCP クライアントに渡されます。
- デフォルト ルート：DHCP から取得されます。
- ASDM アクセス：内部ホストに許可されます。

図 3-1　　ASA 5505 ルーテッド モード



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 Ethernet 0/0
   switchport access vlan 2
   no shutdown
interface Ethernet 0/1
   switchport access vlan 1
   no shutdown
interface Ethernet 0/2
   switchport access vlan 1
   no shutdown
interface Ethernet 0/3
   switchport access vlan 1
   no shutdown
interface Ethernet 0/4
   switchport access vlan 1
   no shutdown
interface Ethernet 0/5
   switchport access vlan 1
   no shutdown
interface Ethernet 0/6
   switchport access vlan 1
   no shutdown
interface Ethernet 0/7
   switchport access vlan 1
```

```
   no shutdown
interface vlan2
   nameif outside
   no shutdown
   ip address dhcp setroute
interface vlan1
   nameif inside
   ip address 192.168.1.1 255.255.255.0
   security-level 100
   no shutdown
object network obj_any
   subnet 0 0
   nat (inside,outside) dynamic interface
http server enable
http 192.168.1.0 255.255.255.0 inside
dhcpd address 192.168.1.5-192.168.1.254 inside
dhcpd auto_config outside
dhcpd enable inside
logging asdm informational
```

（注）　テストのために、ICMP インスペクションをイネーブルにして、内部から外部への ping を許可できます。次のコマンドをデフォルト設定に追加します。

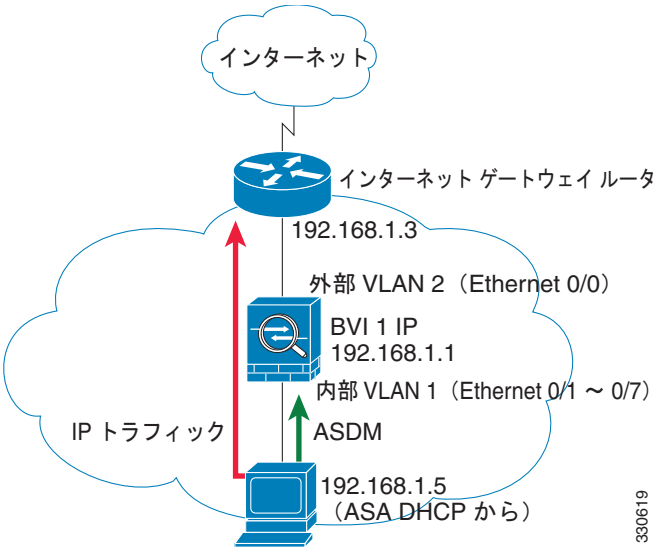
```
policy-map global_policy
   class inspection_default
      inspect icmp
```

ASA 5505 トランスペアレント モードのサンプル設定

モードをトランスペアレント モードに変更すると、設定が消去されます。設定を始めるには、まず CLI で次のサンプル設定をコピーして貼り付けます。この設定では、デフォルト設定を出発点として使用しています。次の部分は変更する必要がある場合があります。

- IP アドレス：設定されている IP アドレスは、接続しているネットワークに一致するよう変更する必要があります。
- スタティック ルート：トラフィックの種類によっては、スタティック ルートが必要です。「MAC アドレス ルックアップと ルート ルックアップ」（P.5-4）を参照してください。

図 3-2　ASA 5505 トランスペアレント モード




```
firewall transparent
interface Ethernet 0/0
   switchport access vlan 2
   no shutdown
interface Ethernet 0/1
   switchport access vlan 1
   no shutdown
interface Ethernet 0/2
   switchport access vlan 1
   no shutdown
interface Ethernet 0/3
   switchport access vlan 1
   no shutdown
interface Ethernet 0/4
   switchport access vlan 1
   no shutdown
interface Ethernet 0/5
   switchport access vlan 1
   no shutdown
interface Ethernet 0/6
   switchport access vlan 1
   no shutdown
interface Ethernet 0/7
   switchport access vlan 1
   no shutdown
interface bvi 1
   ip address 192.168.1.1 255.255.255.0
interface vlan2
   nameif outside
   security-level 0
   bridge-group 1
   no shutdown
interface vlan1
   nameif inside
   security-level 100
   bridge-group 1
   no shutdown
http server enable
http 192.168.1.0 255.255.255.0 inside
dhcpd address 192.168.1.5-192.168.1.254 inside
```

```
dhcpd enable inside
```

（注）　テストのために、ICMP インスペクションをイネーブルにして、内部から外部への ping を許可できます。次のコマンドをサンプル設定に追加します。

```
policy-map global_policy
   class inspection_default
      inspect icmp
```

ASA 5510 以降のデフォルト コンフィギュレーション

ASA 5510 以降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：管理ホストでは DHCP サーバ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 PC 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 100
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 lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

コンフィギュレーションの処理

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（詳細については、第 85 章「ソフトウェアとコンフィギュレーションの管理」を参照してください）。

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。コンテキストの詳細については、第 6 章「マルチ コンテキスト モードの設定」を参照してください。

この項は、次の内容で構成されています。

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。次の項目を取り上げます。

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、次のコマンドを入力します。

コマンド	目的
write memory **例：** `hostname# write memory`	実行中の設定をスタートアップ コンフィギュレーションに保存します。 **（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。この項は、次の内容で構成されています。

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 コンフィギュレーションを保存するには、システムまたはコンテキスト内で次のコマンドを入力します。

コマンド	目的
write memory **例：** hostname# write memory	実行中の設定をスタートアップ コンフィギュレーションに保存します。 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に置くことができます。この場合、そのコンフィギュレーションは、コンテキスト URL（HTTP URL および HTTPS URL を除く）に指定されているサーバに ASA によって戻され、保存されるため、サーバにコンフィギュレーションを保存する必要はありません。 （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、およびシステム コンフィギュレーションを同時に保存するには、システム実行スペースで次のコマンドを入力します。

コマンド	目的
write memory all [**/noconfirm**] **例：** hostname# write memory all /noconfirm	すべてのコンテキストおよびシステム コンフィギュレーションのスタートアップ コンフィギュレーションに実行コンフィギュレーションを保存します。 **/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、外部サーバに配置できます。この場合、そのコンフィギュレーションは、コンテキスト URL（HTTP URL および HTTPS URL を除く）に指定されているサーバに ASA によって戻され、保存されるため、サーバにコンフィギュレーションを保存する必要はありません。

ASA によって各コンテキストが保存されると、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す。

  ```
  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

次のいずれかのオプションを使用して、新規スタートアップ 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します。

コマンド	目的
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、予期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 **copy 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。

コンフィギュレーションの表示

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。

コマンド	目的
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と削除

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。

コマンド	目的
clear configure *configurationcommand* [*level2configurationcommand*] **例：** hostname(config)# clear configure aaa	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。 hostname(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。 hostname(config)# **clear configure aaa authentication**
no *configurationcommand* [*level2configurationcommand*] *qualifier* **例：** hostname(config)# no nat (inside) 1	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* で特定されるコンフィギュレーションを削除します。 たとえば、特定の **nat** コマンドを削除するには、次のように、それを一意に識別するのに十分なコマンドを入力します。 hostname(config)# **no nat (inside) 1**
write erase **例：** hostname(config)# 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。
clear configure all **例：** hostname(config)# 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。

テキスト コンフィギュレーション ファイルのオフラインでの作成

このマニュアルでは、ASA を設定するための CLI の使用方法について説明しています。コマンドを保存すると、変更内容はテキスト 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 PC 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。また、ASA の内部フラッシュ メモリにテキスト ファイルをダウンロードできます。コンフィギュレーション ファイルを ASA にダウンロードする方法の詳細については、第 85 章「ソフトウェアとコンフィギュレーションの管理」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。次の例では、CLI プロンプトは「hostname(config)#」です。

```
hostname(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
```

テキスト コンフィギュレーション ファイルのフォーマッティングの詳細については、付録 A「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。

接続に対するコンフィギュレーションの変更の適用

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続行されます。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、次のいずれかのコマンドを入力します。

コマンド	目的
clear local-host [*ip_address*] [**all**] **例：** `hostname(config)# clear local-host all`	このコマンドは、接続制限値や初期接続の制限など、クライアントごとのランタイム ステートを再初期化します。これにより、このコマンドは、これらの制限を使用しているすべての接続を削除します。現在のすべての接続をホスト別に表示するには、**show local-host all** 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、影響を受けるすべての 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。特定の IP アドレスへの、または特定の IP アドレスからの接続をクリアするには、*ip_address* 引数を使用します。
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*]] **例：** `hostname(config)# clear conn all`	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。
clear xlate [*arguments*] **例：** `hostname(config)# clear xlate`	このコマンドは、ダイナミック NAT セッションをクリアします。スタティック セッションは影響を受けません。その結果、これらの NAT セッションを使用するすべての接続が削除されます。 引数を指定しないと、このコマンドはすべての NAT セッションをクリアします。使用可能な引数の詳細については、コマンド リファレンスを参照してください。

ASA のリロード

ASA をリロードするには、次のコマンドを入力します。

コマンド	目的
reload **例：** `hostname (config)# reload`	ASA をリロードします。 **（注）** 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。