CHAPTER 15

基本設定

この章では、ASA を機能させるためのコンフィギュレーションに一般的に必要となる、基本的な設定を指定する方法を説明します。次の項で構成されています。

ホスト名、ドメイン名、およびパスワードの設定

この項は、次の内容で構成されています。

ログイン パスワードの変更

ログイン パスワードを変更するには、次のコマンドを入力します。

コマンド	目的
{**passwd** | **password**} *password*	ログイン パスワードを変更します。ログイン パスワードは Telnet 接続と SSH 接続に使用されます。デフォルトのログイン パスワードは「cisco」です。 **passwd** または **password** と入力します。パスワードは、最大 16 文字の英数字および特殊文字で、大文字と小文字の区別があります。パスワードには、疑問符とスペースを除いて、任意の文字を使用できます。 パスワードは暗号化された形式でコンフィギュレーションに保存されるため、パスワードの入力後に元のパスワードを表示することはできません。パスワードをデフォルト設定に戻すには、**no password** コマンドを使用します。

イネーブル パスワードの変更

イネーブル パスワードを変更するには、次のコマンドを入力します。

コマンド	目的
enable password *password* **例：** `hostname(config)# passwd Pa$$w0rd`	特権 EXEC モードを開始できるようにイネーブル パスワードを変更します。デフォルトでは、イネーブル パスワードは空白です。 *password* 引数は、最大 16 文字の英数字および特殊文字からなるパスワードで、大文字と小文字は区別されます。パスワードには、疑問符とスペースを除いて、任意の文字を使用できます。 このコマンドは最高の特権レベルにパスワードを変更します。ローカル コマンド許可を設定すると、0 ～ 15 の各特権レベルにイネーブル パスワードを設定できます。 パスワードは暗号化された形式でコンフィギュレーションに保存されるため、パスワードの入力後に元のパスワードを表示することはできません。パスワードを指定せずに **enable password** コマンドを入力すると、パスワードはデフォルトの空白に設定されます。

ホスト名の設定

ホスト名を設定するには、次のコマンドを入力します。

コマンド	目的

hostname *name*
 	
例：
`hostname(config)# hostname farscape`
`farscape(config)#`
	ASA またはコンテキストのホスト名を指定します。
	名前には、63 文字以下の文字を使用できます。ホスト名はアルファベットまたは数字で開始および終了する必要があります。使用できるのはアルファベット、数字、ハイフンのみです。
	ASA のホスト名を設定すると、そのホスト名がコマンド ラインのプロンプトに表示されます。このホスト名によって、複数のデバイスとのセッションを確立する場合に、コマンドを入力する場所が常に把握できます。デフォルトのホスト名はプラットフォームによって異なります。
	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設定したホスト名がすべてのコンテキストのコマンド ラインのプロンプトに表示されます。コンテキスト内にオプションで設定したホスト名はコマンド ラインに表示されませんが、**banner** コマンドの **$(hostname)** トークンで使用できます。

ドメイン名の設定

ドメイン名を設定するには、次のコマンドを入力します。

コマンド	目的
domain-name *name* **例：** `hostname(config)# domain-name example.com`	ASA のドメイン名を指定します。 ASA は、修飾子を持たない名前のサフィクスとして、ドメイン名を付加します。たとえば、ドメイン名を「example.com」に設定し、syslog サーバとして非修飾名「jupiter」を指定した場合は、ASA によって名前が修飾されて「jupiter.example.com」となります。 デフォルト ドメイン名は default.domain.invalid です。 マルチ コンテキスト モードでは、システム実行スペース内だけではなく、各コンテキストに対してドメイン名を設定できます。

日付と時刻の設定

（注） ASASM の日時を設定しないでください。この設定は、ホスト スイッチから受信します。

この項では、次のトピックについて取り上げます。

- 「時間帯と夏時間の日付範囲の設定」（P.15-4）
- 「NTP サーバを使用する日付と時刻の設定」（P.15-5）
- 「手動での日付と時刻の設定」（P.15-6）

時間帯と夏時間の日付範囲の設定

時間帯および夏時間の日付範囲を設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	**clock timezone** *zone* [**-**]*hours* [*minutes*] **例：** hostname(config)# clock timezone PST -8	時間帯を設定します。デフォルトでは、時間帯は UTC（協定世界時）であり、夏時間の日付範囲は 4 月の第一日曜日の午前 2 時～ 10 月の最終日曜日の午前 2 時です。 ここで、*zone* 値は、時間帯を文字列で指定します。たとえば、**PST** は太平洋標準時（Pacific Standard Time）を表します。 [**-**]*hours* 値は、UTC との時差を時間で設定します。たとえば、PST は **-8** 時間です。 *minutes* 値は、UTC との時差を分で設定します。
ステップ 2	夏時間の日付範囲をデフォルトから変更するには、次のいずれかのコマンドを入力します。定期的な日付範囲のデフォルト値は、3 月の第二日曜日の午前 2 時～ 11 月の第一日曜日の午前 2 時。	
	clock summer-time *zone* **date** {*day month* | *month day*} *year hh*:*mm* {*day month* | *month day*} *year hh*:*mm* [*offset*] **例：** hostname(config)# clock summer-time PDT 1 April 2010 2:00 60	夏時間の開始日と終了日を特定の年の特定の日付に設定します。このコマンドを使用する場合は、日付を毎年再設定する必要があります。 *zone* 値は、時間帯を文字列で指定します。たとえば、**PDT** は太平洋夏時間（Pacific Daylight Time）を表します。 *day* 値は、月の日付として 1 ～ 31 を設定します。標準の日付形式に応じて、月日を **April 1** または **1 April** のように入力できます。 *month* 値は、月を文字列で設定します。標準の日付形式に応じて、月日を **April 1** または **1 April** のように入力できます。 *year* 値は、4 桁で年を設定します（**2004** など）。年の範囲は 1993 ～ 2035 です。 *hh:mm* 値は、24 時間形式で、時間と分を設定します。 *offset* 値は、夏時間用に時間を変更する分数を設定します。デフォルト値は 60 分です。
	clock summer-time *zone* **recurring** [*week weekday month hh*:*mm week weekday month hh*:*mm*] [*offset*] **例：** hostname(config)# clock summer-time PDT recurring first Monday April 2:00 60	夏時間の開始日と終了日を、年の特定の日付ではなく、月の日時の形式で指定します。 このコマンドを使用すると、毎年変更する必要がない、繰り返される日付範囲を設定できます。 *zone* 値は、時間帯を文字列で指定します。たとえば、**PDT** は太平洋夏時間（Pacific Daylight Time）を表します。 *week* 値は、月の特定の週を 1 から 4 までの整数で指定するか、**first** または **last** という単語で指定します。たとえば、日付が 5 週目に当たる場合は、**last** を指定します。 *weekday* 値は、**Monday**、**Tuesday**、**Wednesday** などのように曜日を指定します。 *month* 値は、月を文字列で設定します。 *hh:mm* 値は、24 時間形式で、時間と分を設定します。 *offset* 値は、夏時間用に変更する時間の長さを分単位で設定します。デフォルト値は 60 分です。

NTP サーバを使用する日付と時刻の設定

NTP サーバから日付と時刻を取得するには、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	**ntp authenticate** **例：** `hostname(config)# ntp authenticate`	NTP サーバに関する認証をイネーブルにします。
ステップ 2	**ntp trusted-key** *key_id* **例：** `hostname(config)# ntp trusted-key 1`	認証キー ID が信頼できるキーであると指定します。この信頼できるキーは、NTP サーバに関する認証に必要です。 *key_id* 引数は、1 ～ 4294967295 の値です。複数のサーバで使用できるように複数の信頼できるキーを入力できます。
ステップ 3	**ntp authentication-key** *key_id* **md5** *key* **例：** `hostname(config)# ntp authentication-key 1 md5 aNiceKey`	NTP サーバで認証を行うためのキーを設定します。 *key_id* 引数は、ステップ 2 で **ntp trusted-key** コマンドを使用して設定した ID であり、*key* 引数は長さ 32 文字以下の文字列です。
ステップ 4	**ntp server** *ip_address* [**key** *key_id*] [**source** *interface_name*] [**prefer**] **例：** `hostname(config)# ntp server 10.1.1.1 key 1 prefer`	NTP サーバを指定します。 *key_id* 引数は、ステップ 2 で **ntp trusted-key** コマンドを使用して設定した ID です。 **source** *interface_name* キーワード引数ペアには、NTP パケットの発信インターフェイスを指定します（ルーティング テーブル内のデフォルトのインターフェイスを使用しない場合）。マルチ コンテキスト モードではシステムにインターフェイスが含まれないため、管理コンテキストに定義されているインターフェイス名を指定します。 **prefer** キーワードは、精度が類似する複数のサーバがある場合に、この NTP サーバを優先サーバに設定します。NTP では、どのサーバの精度が最も高いかを判断するためのアルゴリズムを使用し、そのサーバに同期します。サーバの精度に差がない場合は、**prefer** キーワードにどのサーバを使用するかを指定します。ただし、優先サーバよりも精度が大幅に高いサーバがある場合、ASA では、精度の高いそのサーバを使用します。たとえば、ASA では、優先サーバの stratum 3 の代わりに、サーバ stratum 2 を使用します。 複数のサーバを識別できます。ASA では、最も正確なサーバを使用します。 **（注）** マルチ コンテキスト モードの場合、時間はシステム設定でだけ設定します。

手動での日付と時刻の設定

手動で日付と時刻を設定するには、次のコマンドを入力します。

手順の詳細

コマンド	目的
clock set *hh*:*mm*:*ss* {*month day* | *day month*} *year* **例：** hostname# clock set 20:54:00 april 1 2004	日付と時刻を手動で設定します。 *hh*:*mm*:*ss* 引数には、時、分、秒を 24 時間形式で設定します。たとえば、午後 8:54 の場合は、**20:54:00** と入力します。 *day* 値は、月の日付として 1 ～ 31 を設定します。標準の日付形式に応じて、月日を **april 1** または **1 april** のように入力できます。 *month* 値は、月を設定します。標準の日付形式に応じて、月日を **april 1** または **1 april** のように入力できます。 *year* 値は、4 桁で年を設定します（**2004** など）。年の範囲は 1993 ～ 2035 です。 デフォルトの時間帯は UTC です。**clock timezone** コマンドを使用して **clock set** コマンドを入力した後に時間帯を変更した場合、時間は自動的に新しい時間帯に調整されます。 このコマンドはハードウェア チップ内の時間を設定しますが、コンフィギュレーション ファイル内の時間は保存しません。この時間はリブート後も保持されます。他の **clock** コマンドとは異なり、このコマンドは特権 EXEC コマンドです。クロックをリセットするには、**clock set** コマンドを使用して新しい時刻を設定する必要があります。

マスター パスフレーズの設定

この項では、次のトピックについて取り上げます。

マスター パスフレーズに関する情報

マスター パスフレーズを利用すると、プレーン テキストのパスワードが安全に、暗号化形式で保存され、1 つのキーを使用してすべてのパスワードを一様に暗号化またはマスキングできるようになります。このようにしても、機能は一切変更されません。マスター パスフレーズを使用する機能としては、次のものがあります。

- OSPF
- EIGRP
- VPN ロード バランシング
- VPN (リモート アクセスおよびサイトツーサイト)
- フェールオーバー
- AAA サーバ
- ロギング
- 共有ライセンス

マスター パスフレーズのライセンス要件

モデル	ライセンス要件
すべてのモデル	基本ライセンス

ガイドラインと制限事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

フェールオーバーのガイドライン

フェールオーバーがイネーブルであっても、フェールオーバー共有キーが設定されていない場合に、マスター パスフレーズを変更すると、エラー メッセージが表示されます。このメッセージには、マスター パスフレーズの変更がプレーン テキストとして送信されないよう、フェールオーバー共有キーを入力する必要があることが示されます。

マスター パスフレーズの追加または変更

この手順を実行できるのは、HTTPS を介したコンソール、SSH、ASDM などによるセキュア セッションにおいてのみです。

マスター パスフレーズを追加または変更するには、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	**key config-key password-encryption** [*new_passphrase* [*old_passphrase*]] **例：** hostname(config)# key config-key password-encryption Old key: bumblebee New key: haverford Confirm key: haverford	暗号キーの生成に使用されるパスフレーズを設定します。パスフレーズの長さは、8 ～ 128 文字にする必要があります。パスフレーズには、バックスペースと二重引用符を除くすべての文字を使用できます。 コマンドに新しいパスフレーズを入力しないと、入力を求めるプロンプトが表示されます。 パスフレーズを変更するには、古いパスフレーズを入力する必要があります。 インタラクティブ プロンプトの例については、「例」（P.15-9）を参照してください。 **（注）** インタラクティブ プロンプトを使用してパスワードを入力し、パスワードがコマンド履歴バッファに記録されないようにします。 暗号化されたパスワードがプレーン テキスト パスワードに変換されるため、**no key config-key password-encrypt** コマンドは注意して使用してください。パスワードの暗号化がサポートされていないソフトウェア バージョンにダウングレードするときは、このコマンドの **no** 形式を使用できます。

	コマンド	目的
ステップ 2	**password encryption aes** **例：** hostname(config)# password encryption aes	パスワードの暗号化をイネーブルにします。パスワードの暗号化がイネーブルになり、マスター パスワードが使用可能になると、ただちにすべてのユーザ パスワードが暗号化されます。実行コンフィギュレーションには、パスワードは暗号化された形式で表示されます。 パスワードの暗号化をイネーブルにしたときに、パスフレーズが設定されていない場合、パスフレーズが将来的に使用可能になるものとしてコマンドは正常に実行されます。 後から **no password encryption aes** コマンドを使用してパスワードの暗号化をディセーブルにすると、暗号化された既存のパスワードは変更されず、マスター パスフレーズが存在する限り、暗号化されたパスワードはアプリケーションによって必要に応じて復号化されます。
ステップ 3	**write memory** **例：** hostname(config)# write memory	マスター パスフレーズのランタイム値と結果のコンフィギュレーションを保存します。このコマンドを入力しなければ、スタートアップ コンフィギュレーションのパスワードは引き続き可読状態となります（過去に暗号化された状態で保存されていない場合）。 また、マルチ コンテキスト モードでは、マスター パスフレーズはシステム コンテキスト コンフィギュレーション内で変更されます。その結果、すべてのコンテキスト内のパスワードが影響を受けます。すべてのユーザ コンテキストではなく、システム コンテキスト モードで **write memory** コマンドを入力しないと、ユーザ コンテキストで暗号化されたパスワードは失効する可能性があります。また、すべての設定を保存するには、システム コンテキストで **write memory all** コマンドを使用します。

例

次の例は、これまでにキーが何も存在していないことを示します。

```
hostname (config)# key config-key password-encryption 12345678
```

次の例は、キーがすでに存在することを示します。

```
Hostname (config)# key config-key password-encryption 23456789
Old key: 12345678
hostname (config)#
```

次の例では、キーを対話形式で設定しようとしていますが、キーがすでに存在しています。**key config-key password-encryption** コマンドを入力し、Enter キーを押してインタラクティブ モードに入ると、[Old key]、[New key]、および [Confirm key] のプロンプトが画面に表示されます。

```
hostname (config)# key config-key password-encryption
Old key: 12345678
New key: 23456789
Confirm key: 23456789
```

次の例では、対話形式の入力を求めていますが、キーは存在しません。インタラクティブ モードに入ると、[New key] および [Confirm key] のプロンプトが表示されます。

```
hostname (config)# key config-key password-encryption
New key: 12345678
Confirm key: 12345678
```

マスター パスフレーズのディセーブル化

マスター パスフレーズをディセーブルにすると、暗号化されたパスワードがプレーン テキスト パスワードに戻ります。暗号化されたパスワードをサポートしていない以前のソフトウェア バージョンにダウングレードする場合は、パスフレーズを削除しておくと便利です。

ディセーブルにする現在のマスター パスフレーズがわかっていなければなりません。パスフレーズが不明の場合は、「マスター パスフレーズの回復」（P.15-11）を参照してください。

この手順を実行できるのは、HTTPS を介した Telnet、SSH、または ASDM によるセキュア セッションだけです。

マスター パスフレーズをディセーブルにするには、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	**no key config-key password-encryption** [*old_passphrase*]] **例：** hostname(config)# no key config-key password-encryption Warning! You have chosen to revert the encrypted passwords to plain text. This operation will expose passwords in the configuration and therefore exercise caution while viewing, storing, and copying configuration. Old key: bumblebee	マスター パスフレーズを削除します。 コマンドにパスフレーズを入力しないと、入力を求めるプロンプトが表示されます。
ステップ 2	**write memory** **例：** hostname(config)# write memory	マスター パスフレーズのランタイム値と結果のコンフィギュレーションを保存します。パスフレーズを含む不揮発性メモリは消去され、0xFF パターンで上書きされます。 マルチ モードでは、システム コンテキスト コンフィギュレーション内のマスター パスフレーズが変更されます。その結果、すべてのコンテキスト内のパスワードが影響を受けます。すべてのユーザ コンテキストではなく、システム コンテキスト モードで **write memory** コマンドを入力しないと、ユーザ コンテキストで暗号化されたパスワードは失効する可能性があります。また、すべての設定を保存するには、システム コンテキストで **write memory all** コマンドを使用します。

マスター パスフレーズの回復

マスター パスフレーズは回復できません。マスター パスフレーズがわからなくなった場合や不明な場合は、削除できます。

マスター パスフレーズを削除するには、次の手順を実行します。

	コマンド	目的
ステップ 1	**write erase** **例：** `hostname(config)# write erase`	マスター キーと、暗号化されたパスワードが含まれているコンフィギュレーションを削除します。
ステップ 2	**reload** **例：** `hostname(config)# reload`	ASA を、マスター キーや暗号化パスワードのないスタートアップ コンフィギュレーションを使用してリロードします。

マスター パスフレーズの機能履歴

表 15-1 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。

表 15-1　マスター パスフレーズの機能履歴

機能名	プラットフォーム リリース	機能情報
マスター パスフレーズ	8.3(1)	この機能が導入されました。 **key config-key password-encryption**、**password encryption aes**、**clear configure password encryption aes**、**show running-config password encryption aes**、**show password encryption** コマンドが導入されました。
パスワード暗号化の可視性	8.4(1)	**show password encryption** コマンドが変更されました。

DNS サーバの設定

一部の ASA 機能では、ドメイン名で外部サーバにアクセスするために DNS サーバを使用する必要があります。たとえば、ボットネット トラフィック フィルタ機能では、ダイナミック データベース サーバにアクセスして、スタティック データベースのエントリを解決するために DNS サーバが必要です。

他の機能（**ping** コマンドや **traceroute** コマンドなど）では、トレースルートのために ping する名前を入力できます。ASA では、DNS サーバと通信してこの名前を解決できます。名前は、多くの SSL VPN コマンドおよび certificate コマンドでもサポートされます。

（注）　ASA では、機能に応じて DNS サーバの使用が限定的にサポートされます。たとえば、ほとんどのコマンドでは、IP アドレスを入力する必要があります。名前を使用できるのは、名前と IP アドレスを関連付けるように **name** コマンドを手動で設定し、**names** コマンドを使用して名前の使用をイネーブルにした場合だけです。

ダイナミック DNS の詳細については、「DDNS の設定」（P.17-2）を参照してください。

前提条件

DNS ドメイン ルックアップをイネーブルにするすべてのインターフェイスに対して適切なルーティングを設定し、DNS サーバに到達できるようにしてください。ルーティングの詳細については、「ルーティングに関する情報」（P.25-1）を参照してください。

手順の詳細

	コマンド	目的
ステップ 1	**dns domain-lookup** *interface_name* **例：** `hostname(config)# dns domain-lookup inside`	サポートされているコマンドに対してネーム ルックアップを実行するために、ASA が DNS サーバに DNS 要求を送信できるようにします。
ステップ 2	**dns server-group DefaultDNS** **例：** `hostname(config)# dns server-group DefaultDNS`	ASA が発信要求に使用する DNS サーバ グループを指定します。 PN トンネル グループ用に他の DNS サーバ グループを設定できます。詳細については、コマンド リファレンスの **tunnel-group** コマンドを参照してください。
ステップ 3	**name-server** *ip_address* [*ip_address2*] [...] [*ip_address6*] **例：** `hostname(config-dns-server-group)# name-server 10.1.1.5 192.168.1.67 209.165.201.6`	1 つまたは複数の DNS サーバを指定します。同じコマンドで 6 つの IP アドレスすべてをスペースで区切って入力するか、各コマンドを別々に入力できます。ASA では、応答を受信するまで各 DNS サーバを順に試します。

http://www.cisco.com/en/US/products/ps6121/products_tech_note09186a0080aaeff5.shtml

パスワード回復の実行

この項では、次のトピックについて取り上げます。

- 「ASA のパスワードの回復」（P.15-13）
- 「パスワード回復のディセーブル化」（P.15-14）

ASA のパスワードの回復

ASA のパスワードを回復するには、次の手順を実行します。

ステップ 1　「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）または「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）の手順に従って、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、投入します。

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

ステップ 4　コンフィギュレーション レジスタ値をアップデートするには、次のコマンドを入力します。

```
rommon #1> confreg 0x41
Update Config Register (0x41) in NVRAM...
```

ステップ 5　スタートアップ コンフィギュレーションを無視するように ASA を設定するには、次のコマンドを入力します。

```
rommon #1> confreg
```

ASA によって現在のコンフィギュレーションのレジスタ値が表示され、それを変更するかどうかが尋ねられます。

```
Current Configuration Register: 0x00000041
Configuration Summary:
boot default image from Flash
  ignore system configuration

Do you wish to change this configuration?y/n [n]: y
```

ステップ 6　後で回復できるように、現在のコンフィギュレーションのレジスタ値を記録します。

ステップ 7　値を変更する場合は、プロンプトに対して **Y** を入力します。

ASA によって、新しい値の入力を求めるプロンプトが表示されます。

ステップ 8　すべての設定についてデフォルト値を受け入れます。プロンプトに対して、**Y** を入力します。

ステップ 9　次のコマンドを入力して、ASA をリロードします。

```
rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.

Loading disk0:/asa800-226-k8.bin... Booting...Loading...
```

ASA は、スタートアップ コンフィギュレーションの代わりにデフォルト コンフィギュレーションをロードします。

ステップ 10　次のコマンドを入力して、特権 EXEC モードにアクセスします。

```
hostname# enable
```

ステップ 11　パスワードの入力を求められたら、Enter キーを押します。

パスワードは空白です。

ステップ 12　次のコマンドを入力して、スタートアップ コンフィギュレーションをロードします。

```
hostname# copy startup-config running-config
```

ステップ 13　次のコマンドを入力して、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。

```
hostname# configure terminal
```

ステップ 14　次のコマンドを入力して、デフォルト コンフィギュレーションで必要に応じてパスワードを変更します。

```
hostname(config)# password password
hostname(config)# enable password password
hostname(config)# username name password password
```

ステップ 15　次のコマンドを入力して、デフォルト コンフィギュレーションをロードします。

```
hostname(config)# no config-register
```

デフォルト コンフィギュレーションのレジスタ値は 0x1 です。コンフィギュレーション レジスタの詳細については、コマンド リファレンスを参照してください。

ステップ 16　次のコマンドを入力して、新しいパスワードをスタートアップ コンフィギュレーションに保存します。

```
hostname(config)# copy running-config startup-config
```

パスワード回復のディセーブル化

権限のないユーザがパスワード回復メカニズムを使用して ASA を危険にさらすことがないように、パスワード回復をディセーブルにするには、次のコマンドを入力します。

コマンド	目的
no service password-recovery **例：** `hostname (config)# no service password-recovery`	パスワード回復をディセーブルにします。

ASA で、**no service password-recovery** コマンドを使用すると、ROMMON モードに入って、コンフィギュレーションを変更するのを防ぐことができます。ROMMON モードを開始するときに、すべてのフラッシュ ファイル システムを消去するかどうかを尋ねる ASA のプロンプトが表示されます。この消去を実行してからでなければ、ROMMON モードを開始できません。フラッシュ ファイル システムを消去しない場合、ASA はリロードされます。パスワードを回復するには、ROMMON モードの使用と既存のコンフィギュレーションの保持が必要であるため、この消去を行うと、パスワードの回復ができなくなります。ただし、パスワードを回復できなくすることで、不正なユーザがコンフィギュレーションを表示したり、別のパスワードを挿入したりすることがなくなります。この場合、システムを動作可能な状態に回復するには、新しいイメージとバックアップ コンフィギュレーション ファイル（入手できる場合）をロードします。

コンフィギュレーション ファイルに表示される **service password-recovery** コマンドは、情報のためだけのものです。CLI プロンプトに対してコマンドを入力すると、設定は NVRAM に保存されます。設定を変更する唯一の方法は、CLI プロンプトでコマンドを入力することです。このコマンドの異なるバージョンで新規コンフィギュレーションをロードしても、設定は変更されません。ASA が（パスワード回復の準備で）スタートアップ時にスタートアップ コンフィギュレーションを無視するように設定されている場合にパスワード回復をディセーブルにすると、ASA は通常どおりスタートアップ コンフィギュレーションをロードするように設定を変更します。フェールオーバーを使用し、スタートアップ コンフィギュレーションを無視するようにスタンバイ装置が設定されている場合は、**no service password recovery** コマンドでスタンバイ装置に複製したときにコンフィギュレーション レジスタに同じ変更が加えられます。

DNS キャッシュのモニタリング

ASA では、特定のクライアントレス SSL VPN および certificate コマンドに送信された外部 DNS クエリーの DNS 情報にローカル キャッシュを提供します。各 DNS 変換要求は、ローカル キャッシュで最初に検索されます。ローカル キャッシュに情報がある場合、結果の IP アドレスが戻されます。ローカル キャッシュで要求を解決できない場合、設定されているさまざまな DNS サーバに DNS クエリーが送信されます。外部 DNS サーバによって要求が解決された場合、結果の IP アドレスと、対応するホスト名が一緒にローカル キャッシュに格納されます。

DNS キャッシュをモニタするには、次のコマンドを入力します。

コマンド	目的
show dns-hosts	DNS キャッシュが表示されます。これには、DNS サーバからダイナミックに学習したエントリと **name** コマンドを使用して手動で入力された名前および IP アドレスが含まれます。