CHAPTER 5

ホスト名、ドメイン名、パスワードなどの基本的な設定

この章では、ASA 1000V 上でコンフィギュレーションを機能させるために通常必要とされる基本設定を行う方法について説明します。次の項目を取り上げます。

ホスト名、ドメイン名、およびパスワードの設定

この項では、デバイス名とパスワードの変更方法について説明します。次の項目を取り上げます。

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 コマンド認可を設定すると、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 1000V 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、間の文字にはアルファベット、数字、またはハイフンのみを使用する必要があります。
	
	ASA 1000V 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。

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 1000V のドメイン名を指定します。 ASA 1000V 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 サーバに非修飾名「jupiter」を指定する場合、ASA 1000V には「jupiter.example.com」という名前が与えられます。 デフォルト ドメイン名は default.domain.invalid です。

日付と時刻の設定

ここでは、次の内容について説明します。

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変更するには、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自動更新の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。

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、**ntp trusted-key** コマンドを使用してステップ 2 で設定する ID です。*key* 引数は 32 文字までの文字列です。
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、**ntp trusted-key** コマンドを使用してステップ 2 で設定する ID です。 **source** *interface_name* のキーワードと引数のペアは、ルーティング テーブルにデフォルトのイーサネット インターフェイスを使用しない場合に、NTP パケットの発信イーサネット インターフェイスを識別します。 **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 1000V では、精度の高いそのサーバを使用します。たとえば、ASA 1000V 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 1000V では、最も正確なサーバを使用します。

手動での日付と時刻の設定

日付と時刻を手動で設定するには、次の手順を実行します。

手順の詳細

コマンド	目的
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、24 時間形式で、時間、分、秒を設定します。たとえば、午後 8 時 54 分の場合は、**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** コマンドで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、マスター パスフレーズの設定方法について説明します。次の項目を取り上げます。

- 「マスター パスフレーズに関する情報」（P.5-6）
- 「マスター パスフレーズの追加または変更」（P.5-7）
- 「マスター パスフレーズのディセーブル化」（P.5-9）
- 「マスター パスフレーズの回復」（P.5-10）

マスター パスフレーズに関する情報

マスター パスフレーズ機能を利用すると、プレーン テキスト パスワードを暗号化された形式で安全に保存できます。マスター パスフレーズは、機能を変更することなく、すべてのパスワードを一般的に暗号化またはマスキングするために使用するキーです。マスター パスフレーズを実装する機能として次のものがあります。

- IPsec サイトツーサイト
- フェールオーバー
- AAA サーバ

- ロギング

マスター パスフレーズの追加または変更

この項では、マスター パスフレーズを追加または変更する方法について説明します。

前提条件

- フェールオーバーがイネーブルで、フェールオーバー共有キーが設定されていない場合、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に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。
- 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際は、現在のパスフレーズも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.5-8）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。
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有効になり、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せず、以前に暗号化で保存されていない場合、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表示されます。

例

次の設定例には、以前のキーがありません。

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

次の設定例には、キーがすでに存在しています。

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

次の設定例では、対話形式の入力を求めていますが、キーはすでに存在しています。**key config-key password-encryption** コマンドを入力して、Enter キーを押し、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。

前提条件

- 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.5-10）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。

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 パスフレーズが失われたか、不明な場合は、**reload** コマンドに続いて、**write erase** コマンドを使用して削除できます。これらのコマンドは、暗号化されたパスワードを含むコンフィギュレーションとマスター キーを削除します。

DNS サーバの設定

一部の ASA 1000V 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 1000V では、DNS サーバと通信してこの名前を解決できます。

（注） ASA 1000V 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。

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.7-1）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 1000V が DNS サーバに DNS 要求を送信できるようにします。 *interface_name* 引数には、イーサネット インターフェイスの名前を指定します。
ステップ 2	**dns server-group DefaultDNS** **例：** `hostname(config)# dns server-group DefaultDNS`	ASA 1000V 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 1000V では、応答を受信するまで各 DNS サーバを順に試します。