



CHAPTER 8

基本設定

この章では、セキュリティ アプライアンス 上で機能を果たすコンフィギュレーション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。この章は、次の項で構成されています。

- 「ログイン パスワードの変更」(P.8-1)
- 「イネーブル・パスワードの変更」(P.8-1)
- 「ホスト名の設定」(P.8-2)
- 「ドメイン名の設定」(P.8-2)
- 「日付と時刻の設定」(P.8-2)
- 「透過ファイアウォールの管理 IP アドレスの設定」(P.8-5)

ログイン パスワードの変更

ログイン パスワードは Telnet 接続と SSH 接続に使用されます。デフォルトでは、ログイン パスワードは「cisco」です。パスワードを変更するには、次のコマンドを入力します。

```
hostname(config)# {passwd | password} password
```

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 パスワードを使用すると、特権 EXEC モードに入ることができます。デフォルトでは、イネーブル 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、次のコマンドを入力します。

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

password 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せん。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

セキュリティ アプライアンス 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。

セキュリティ アプライアンス 用のホスト名なのか、コンテキスト用のホスト名なのかを指定するには、次のコマンドを入力します。

```
hostname(config)# hostname name
```

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。

この名前がコマンドライン プロンプトに表示されます。次に例を示します。

```
hostname(config)# hostname farscape  
farscape(config)#
```

ドメイン名の設定

セキュリティ アプライアンス 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** サーバを修飾子を持たない名前の「**jupiter**」に指定した場合、セキュリティ アプライアンスによって名前は「**jupiter.example.com**」に修飾されます。

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。

セキュリティ アプライアンス のドメイン名を指定するには、次のコマンドを入力します。

```
hostname(config)# domain-name name
```

たとえば、ドメインを **example.com** として設定する場合、次のコマンドを入力します。

```
hostname(config)# domain-name example.com
```

日付と時刻の設定

この項では、日付と時刻の設定方法として、手動で行う方法と NTP サーバを使用するダイナミックな方法について説明します。手動で設定した時刻はすべて、NTP サーバから取得された時刻によって上書きされます。この項では、時間帯および夏時間の日付範囲の設定方法についても説明します。



(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。

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.8-3)
- 「NTP サーバを使用する日付と時刻の設定」(P.8-4)
- 「手動での日付と時刻の設定」(P.8-5)

時間帯と夏時間の日付範囲の設定

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。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。

ステップ 1 時間帯を設定するには、グローバル コンフィギュレーション モードで次のコマンドを入力します。

```
hostname(config)# clock timezone zone [-]hours [minutes]
```

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、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。

- 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するには、次のコマンドを入力します。

```
hostname(config)# clock summer-time zone date {day month | month day} year hh:mm {day month | month day} year hh:mm [offset]
```

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。

- 夏時間の開始日と終了日を、ある月の日付および時刻という形式で指定し、ある年の特定の日付としては指定しない場合は、次のコマンドを入力します。

```
hostname(config)# clock summer-time zone recurring [week weekday month hh:mm week weekday month hh:mm] [offset]
```

このコマンドによって定期的な日付範囲が設定されるため、毎年変更する必要はありません。

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。

ステップ 1 NTP サーバを使用して認証を設定するには、次の手順を実行します。

- a. 認証をイネーブルにするには、次のコマンドを入力します。

```
hostname(config)# ntp authenticate
```

- b. 認証キー ID が信頼できるキーであると指定するには、次のコマンドを入力します。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。

```
hostname(config)# ntp trusted-key key_id
```

ここで、*key_id* は 1 ~ 4294967295 の数字です。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。

- c. NTP サーバで認証を行うためのキーを設定するには、次のコマンドを入力します。

```
hostname(config)# ntp authentication-key key_id md5 key
```

ここで、*key_id* には、**ntp trusted-key** コマンドを実行して手順 1b で設定した ID を指定し、*key* には最大 32 文字の文字列を指定します。

ステップ 2 NTP サーバを識別するには、次のコマンドを入力します。

```
hostname(config)# ntp server ip_address [key key_id] [source interface_name] [prefer]
```

ここで、*key_id* には、**ステップ 1b** の **ntp trusted-key** コマンドを実行して設定した ID を指定します。

source interface_name には、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に、NTP パケットを転送する発信インターフェイスを指定します。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、セキュリティ アプライアンス では、精度の高いそのサーバを使用します。たとえば、セキュリティ アプライアンス 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。セキュリティ アプライアンス では、最も正確なサーバを使用します。



(注)

SNTTP はサポートされていません。NTP だけがサポートされています。

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。

```
hostname# clock set hh:mm:ss {month day | day month} year
```

ここで、*hh:mm:ss* 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 分は **20:54:00** のように設定します。

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** コマンドの新しい時刻を設定する必要があります。

透過ファイアウォールの管理 IP アドレスの設定

トランスペアレント ファイアウォール モード限定

トランスペアレント ファイアウォールは、IP ルーティングに参加しません。セキュリティ アプライアンスに必要な唯一の IP コンフィギュレーションは、管理 IP アドレスを設定することです。このアドレスが必要になるのは、セキュリティ アプライアンスがシステム メッセージや AAA サーバとの通信などセキュリティ アプライアンスで発信されるトラフィックの送信元アドレスとしてこのアドレスを使用するためです。このアドレスは、リモート管理アクセスにも使用できます。

マルチ コンテキスト モードの場合、各コンテキスト内の管理 IP アドレスを設定します。

管理 IP アドレスを設定するには、次のコマンドを入力します。

```
hostname(config)# ip address ip_address [mask] [standby ip_address]
```

このアドレスは、上流のルータおよび下流のルータと同じサブネットに存在する必要があります。サブネットにホストサブネット (255.255.255.255) を設定することはできません。このアドレスは IPv4 でなければなりません。これは、トランスペアレント ファイアウォールが IPv6 をサポートしていないためです。

フェールオーバーには、**standby** キーワードおよびアドレスを使用します。詳細については、[第 14 章「フェールオーバーの設定」](#)を参照してください。

