CHAPTER 40

システム アクセスの管理

この章では、システム管理のために Telnet、SSH、および HTTPS 経由でセキュリティ アプライアンスにアクセスする方法について説明します。また、ユーザを認証および許可する方法とログイン バナーを作成する方法についても説明します。

この章は、次の項で構成されています。

（注） また、管理アクセス用のセキュリティ アプライアンス インターフェイスにアクセスする場合は、ホスト IP アドレスを許可するアクセス リストは不要です。必要なのは、この章の各項の説明に従って管理アクセスを設定することだけです。

Telnet アクセスの許可

セキュリティ アプライアンスは、管理目的でセキュリティ アプライアンスへの Telnet 接続を許可します。IPSec トンネル内で Telnet を使用する場合を除き、最も低いセキュリティ インターフェイスに対して Telnet は使用できません。Telnet を使用してセキュリティ アプライアンスのコンソールにアクセスするには、ユーザ名 **asa** と **password** コマンドで設定したログイン パスワードを入力します。または、**aaa authentication telnet console** コマンドを使用してログインします。

セキュリティ アプライアンスは、コンテキストごとに最大 5 つの同時 Telnet 接続を許可し、可能な場合は、最大 100 の接続がすべてのコンテキストの間で分割されます。

セキュリティ アプライアンスへの Telnet アクセスを設定するには、次の手順を実行します。

ステップ 1 セキュリティ アプライアンスが接続を受け入れる送信元 IP アドレスを指定するには、アドレスまたはサブネットごとに、次のコマンドを入力します。

```
hostname(config)# telnet source_IP_address mask source_interface
```

インターフェイスが 1 つしかない場合は、インターフェイスのセキュリティ レベルが 100 である限り、そのインターフェイスにアクセスするように Telnet を設定することができます。

ステップ 2　（任意）セキュリティ アプライアンスが Telnet セッションを切断するまでに、セッションがアイドル状態を維持する時間の長さを設定するには、次のコマンドを入力します。

```
hostname(config)# telnet timeout minutes
```

タイムアウトは 1 ～ 1440 分に設定します。デフォルトは 5 分です。デフォルト値では一般に短すぎるので、実働前のテストとトラブルシューティングがすべて完了するまでは、長めに設定しておいてください。

たとえば、192.168.1.2 というアドレスを持つ内部インターフェイス上のホストからセキュリティ アプライアンスにアクセスするには、次のように入力します。

```
hostname(config)# telnet 192.168.1.2 255.255.255.255 inside
hostname(config)# telnet timeout 30
```

192.168.3.0 ネットワーク上のすべてのユーザが内部インターフェイス上のセキュリティ アプライアンスにアクセスできるようにするには、次のコマンドを入力します。

```
hostname(config)# telnet 192.168.3.0 255.255.255.0 inside
```

SSH アクセスの許可

セキュリティ アプライアンスは、管理目的でセキュリティ アプライアンスへの SSH 接続を許可します。セキュリティ アプライアンスは、コンテキストごとに最大 5 つの同時 SSH 接続を許可し、可能な場合は、最大 100 の接続がすべてのコンテキストの間で分割されます。

SSH は、強力な認証と暗号化機能を提供する TCP/IP など、信頼性の高いトランスポート層で実行されるアプリケーションです。セキュリティ アプライアンスは SSH バージョン 1 および 2 で提供されている SSH リモート シェル機能をサポートし、DES 暗号および 3DES 暗号をサポートします。SSH を使用してセキュリティ アプライアンスのコンソールにアクセスするには、SSH クライアント プロンプトでユーザ名 **asa** と **password** コマンドで設定したログイン パスワードを入力します。または、**aaa authentication telnet console** コマンドを使用してログインします。

（注）　SSL および SSH での XML 管理はサポートされていません。

この項では、次のトピックについて取り上げます。

- 「SSH アクセスの設定」（P.40-2）
- 「SSH クライアントの使用」（P.40-3）

SSH アクセスの設定

セキュリティ アプライアンスへの SSH アクセスを設定するには、次の手順を実行します。

ステップ 1　SSH に必要な RSA キー ペアを生成するには、次のコマンドを入力します。

```
hostname(config)# crypto key generate rsa modulus modulus_size
```

係数（ビット単位）は 512、768、1024、または 2048 です。指定するキー係数のサイズが大きいほど、RSA の生成にかかる時間は長くなります。値は 1024 にすることをお勧めします。

ステップ 2　永続的なフラッシュ メモリに RSA キーを保存するには、次のコマンドを入力します。

```
hostname(config)# write mem
```

ステップ 3　セキュリティ アプライアンスが接続を受け入れる送信元 IP アドレスを指定するには、アドレスまたはサブネットごとに、次のコマンドを入力します。

```
hostname(config)# ssh source_IP_address mask source_interface
```

セキュリティ アプライアンスは、最も低いセキュリティ レベルの接続も含め、すべてのインターフェイスから SSH 接続を受け入れます。

ステップ 4　（任意）セキュリティ アプライアンスが SSH セッションを切断するまでに、セッションがアイドル状態を維持する時間の長さを設定するには、次のコマンドを入力します。

```
hostname(config)# ssh timeout minutes
```

タイムアウトは 1 ～ 60 分に設定します。デフォルトは 5 分です。デフォルト値では一般に短すぎるので、実働前のテストとトラブルシューティングがすべて完了するまでは、長めに設定しておいてください。

たとえば、RSA キーを生成し、192.168.1.2 というアドレスを持つ内部インターフェイス上のホストからセキュリティ アプライアンスにアクセスするには、次のように入力します。

```
hostname(config)# crypto key generate rsa modulus 1024
hostname(config)# write mem
hostname(config)# ssh 192.168.1.2 255.255.255.255 inside
hostname(config)# ssh 192.168.1.2 255.255.255.255 inside
hostname(config)# ssh timeout 30
```

192.168.3.0 ネットワーク上のすべてのユーザが内部インターフェイス上のセキュリティ アプライアンスにアクセスできるようにするには、次のコマンドを入力します。

```
hostname(config)# ssh 192.168.3.0 255.255.255.0 inside
```

デフォルトでは、SSH はバージョン 1 とバージョン 2 の両方を許可します。バージョン番号を指定するには、次のコマンドを入力します。

hostname(config)# **ssh version** *version_number*

version_number には *1* または *2* を指定します。

SSH クライアントの使用

SSH を使用して セキュリティ アプライアンス のコンソールにアクセスするには、SSH クライアントからユーザ名 **pix** を入力し、**password** コマンドで設定したログイン パスワードを入力します（「ログイン パスワードの変更」（P.8-1）を参照）。

SSH セッションを開始すると、次のように SSH ユーザ認証プロンプトが表示される前に、セキュリティ アプライアンス コンソール上にドット（.）が表示されます。

```
hostname(config)# .
```

ドットが表示されても、SSH の機能には影響を与えません。コンソールにドットが表示されるのは、ユーザ認証が始まる前で、サーバ キーを生成する場合か、または SSH キー交換中に秘密キーを使用してメッセージを暗号化する場合です。これらのタスクには 2 分以上かかることがあります。ドットは、セキュリティ アプライアンスがビジー状態で、ハングしていないことを示す進捗インジケータです。

ASDM での HTTPS アクセスの許可

ASDM を使用するには、HTTPS サーバをイネーブルにし、セキュリティ アプライアンスへの HTTPS 接続を許可する必要があります。**setup** コマンドを使用すると、これらのタスクがすべて完了します。この項では、ASDM アクセスを手動で設定する方法について説明します。

セキュリティ アプライアンスは、コンテキストごとに最大 5 つの同時 ASDM インスタンスを許可し、可能な場合は、最大 32 の ASDM インスタンスがすべてのコンテキストの間で許可されます。

ASDM アクセスを設定するには、次の手順を実行します。

ステップ 1　セキュリティ アプライアンスが HTTPS 接続を受け入れる送信元 IP アドレスを指定するには、アドレスまたはサブネットごとに、次のコマンドを入力します。

```
hostname(config)# http source_IP_address mask source_interface
```

ステップ 2　HTTPS サーバ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)# http server enable
```

ステップ 3　ASDM イメージの場所を指定するには、次のコマンドを入力します。

```
hostname(config)# asdm image disk0:/asdmfile
```

たとえば、HTTPS サーバをイネーブルにして、192.168.1.2 というアドレスを持つ内部インターフェイス上のホストが ASDM にアクセスできるようにするには、次のように入力します。

```
hostname(config)# crypto key generate rsa modulus 1024
hostname(config)# write mem
hostname(config)# http server enable
hostname(config)# http 192.168.1.2 255.255.255.255 inside
```

192.168.3.0 ネットワーク上のすべてのユーザが内部インターフェイス上の ASDM にアクセスできるようにするには、次のコマンドを入力します。

```
hostname(config)# http 192.168.3.0 255.255.255.0 inside
```

同じインターフェイスでの ASDM および WebVPN の設定

セキュリティ アプライアンスでは、ASDM 管理セッションで WebVPN 接続と HTTPS 接続の両方を同時に同じインターフェイスでサポートできます。HTTPS と WebVPN は両方とも、デフォルトでポート 443 を使用します。このため、HTTPS と WebVPN の両方を同じインターフェイスでイネーブルにする場合は、HTTPS または WebVPN に対して異なるポート番号を指定する必要があります。代替方法は、WebVPN と HTTPS を異なるインターフェイスに設定することです。

HTTPS のポートを指定するには、**http server enable** コマンドの *port* 引数を使用します。次の例では、HTTPS ASDM セッションが外部インターフェイスのポート 444 を使用することを指定します。WebVPN も外部インターフェイスでイネーブルになり、デフォルト ポート（443）を使用します。このコンフィギュレーションでは、リモート ユーザはブラウザに https://<outside_ip>:444 を入力して ASDM セッションを開始します。

```
hostname(config)# http server enable 444
hostname(config)# http 192.168.3.0 255.255.255.0 outside
hostname(config)# webvpn
hostname(config-webvpn)# enable outside
```

WebVPN 用のポートを指定するには、webvpn コンフィギュレーション モードで **port** コマンドを使用します。次の例では、外部インターフェイスのポート 444 で WebVPN をイネーブルにします。ASDM 用の HTTPS も外部インターフェイスで設定され、デフォルト ポート（443）を使用します。このコンフィギュレーションでは、リモート ユーザは、ブラウザに https://<outside_ip>:444 を入力して WebVPN セッションを開始します。

```
hostname(config)# http server enable
hostname(config)# http 192.168.3.0 255.255.255.0 outside
hostname(config)# webvpn
hostname(config-webvpn)# port 444
hostname(config-webvpn)# enable outside
```

システム管理者用 AAA の設定

この項では、システム管理者の認証とコマンド許可をイネーブルにする方法について説明します。システム管理者の AAA を設定する前に、まず第 13 章「AAA サーバおよびローカル データベースのサポート」に従ってローカル データベースまたは AAA サーバを設定します。

この項では、次のトピックについて取り上げます。

CLI アクセスに対する認証の設定

CLI 認証をイネーブルにすると、セキュリティ アプライアンスはログインのためユーザ名とパスワードの入力を求めるプロンプトを表示します。情報を入力した後、ユーザ EXEC モードにアクセスできるようになります。

特権 EXEC モードを開始するには、**enable** コマンドまたは **login** コマンドを入力します（ローカル データベースのみを使用している場合）。

イネーブル認証を設定した場合（「enable コマンドの認証の設定」（P.40-6）を参照）、セキュリティ アプライアンス により、個人のユーザ名とパスワードの入力が要求されます。enable 認証を設定していない場合は、**enable** コマンドを入力するときにシステム イネーブル パスワード（**enable password** コマンドで設定）を入力します。ただし、enable 認証を使用しない場合、**enable** コマンドを入力した後は、特定のユーザとしてログインしていません。ユーザ名を維持するには、enable 認証を使用してください。

ローカル データベースを使用する認証の場合、**login** コマンドを使用できます。このコマンドでは、ユーザ名は維持されますが、認証をオンにするコンフィギュレーションは必要ありません。

（注） セキュリティ アプライアンスで Telnet、SSH、または HTTP ユーザを認証できるようにするには、まず **telnet**、**ssh**、および **http** の各コマンドを使用してセキュリティ アプライアンスへのアクセスを設定する必要があります。これらのコマンドでは、セキュリティ アプライアンスとの通信を許可する IP アドレスを指定します。

CLI にアクセスするユーザを認証するには、次のコマンドを入力します。

```
hostname(config)# aaa authentication {telnet | ssh | http | serial} console {LOCAL | server_group [LOCAL]}
```

http キーワードは、HTTPS を使用してセキュリティ アプライアンスにアクセスする ASDM クライアントを認証します。AAA サーバを使用する場合は、HTTP 認証だけを設定する必要があります。デフォルトでは、このコマンドを設定しなくても、ASDM によってローカル データベースが認証に使用されます。HTTP 管理認証では、AAA サーバ グループの SDI プロトコルをサポートしていません。

認証に AAA サーバ グループを使用する場合は、AAA サーバが使用できないときにローカル データベースをフォールバック方式として使用するようにセキュリティ アプライアンスを設定できます。サーバ グループ名の後ろに **LOCAL** を指定します（**LOCAL** は大文字と小文字を区別します）。ローカル データベースでは AAA サーバと同じユーザ名およびパスワードを使用することを推奨します。これは、セキュリティ アプライアンスのプロンプトでは、いずれの方式が使用されているかが示されないためです。

LOCAL だけを入力して、ローカル データベースを認証の主要方式として（フォールバックなしで）使用することもできます。

特権 EXEC モード アクセスするための認証の設定

ユーザが **enable** コマンドを入力したときに AAA サーバまたはローカル データベースでそれらのユーザを認証するようにセキュリティ アプライアンスを設定することができます。あるいは、ユーザは **login** コマンドを入力したときにローカル データベースで自動的に認証されます。この場合も、ローカル データベース内のユーザ レベルに応じて特権 EXEC モードにアクセスします。

この項では、次のトピックについて取り上げます。

- 「enable コマンドの認証の設定」（P.40-6）
- 「login コマンドによるユーザの認証」（P.40-7）

enable コマンドの認証の設定

ユーザが **enable** コマンドを入力したときに認証されるように、セキュリティ アプライアンスを設定できます。**enable** コマンドを認証しない場合は、**enable** を入力したときに、セキュリティ アプライアンスがシステム イネーブル パスワード（**enable password** コマンドで設定）の入力を求めるプロンプトを表示します。この場合、特定のユーザとしてログインする必要はありません。**enable** コマンドに認証を適用すると、ユーザ名が保持されます。この機能は、ユーザが入力できるコマンドを判別するためにユーザ名が重要な役割を果たすコマンド許可を実行する場合に特に役立ちます。

enable コマンドの入力時にユーザを認証するには、次のコマンドを入力します。

```
hostname(config)# aaa authentication enable console {LOCAL | server_group [LOCAL]}
```

ユーザ名とパスワードの入力を求めるプロンプトがユーザに対して表示されます。

認証に AAA サーバ グループを使用する場合は、AAA サーバが使用できないときにローカル データベースをフォールバック方式として使用するようにセキュリティ アプライアンスを設定できます。サーバ グループ名の後ろに **LOCAL** を指定します（**LOCAL** は大文字と小文字を区別します）。ローカル データベースでは AAA サーバと同じユーザ名およびパスワードを使用することを推奨します。これは、セキュリティ アプライアンスのプロンプトでは、いずれの方式が使用されているかが示されないためです。

LOCAL だけを入力して、ローカル データベースを認証の主要方式として（フォールバックなしで）使用することもできます。

login コマンドによるユーザの認証

ユーザ EXEC モードから、**login** コマンドを使用してローカル データベース内のユーザ名でログインすることができます。

この機能を使用すると、ユーザは独自のユーザ名とパスワードでログインして特権 EXEC モードにアクセスすることができるので、システム イネーブル パスワードを全員に提供する必要がなくなります。ユーザがログイン時に特権 EXEC モード（およびすべてのコマンド）にアクセスできるようにするには、ユーザの特権レベルを 2（デフォルト）～ 15 に設定します。ローカル コマンド許可を設定した場合、ユーザは、その特権レベル以下のレベルに割り当てられているコマンドのみを入力できます。詳細については、「ローカル コマンド許可の設定」（P.40-8）を参照してください。

注意　CLI にアクセスできるユーザや特権 EXEC モードを開始できないようにするユーザをローカル データベースに追加する場合は、コマンド許可を設定する必要があります。コマンド許可がない場合、特権レベルが 2 以上（2 がデフォルト）のユーザは、CLI で自分のパスワードを使用して特権 EXEC モード（およびすべてのコマンド）にアクセスできます。あるいは、認証処理で AAA サーバを使用するか、またはすべてのローカル ユーザをレベル 1 に設定することにより、システム イネーブル パスワードを使用して特権 EXEC モードにアクセスできるユーザを制御できます。

ローカル データベースからユーザとしてログインするには、次のコマンドを入力します。

```
hostname> login
```

セキュリティ アプライアンスにより、ユーザ名とパスワードの入力を求めるプロンプトが表示されます。パスワードを入力すると、セキュリティ アプライアンスにより、ユーザはローカル データベースで指定されている特権レベルに置かれます。

コマンド許可の設定

デフォルトでは、ログインするとユーザ EXEC モードにアクセスでき、最低限のコマンドだけが提供されます。**enable** コマンド（または、ローカル データベースを使用するときは **login** コマンド）を入力すると、特権 EXEC モードおよびコンフィギュレーション コマンドを含む高度なコマンドにアクセスできます。コマンドへのアクセスを制御する場合、セキュリティ アプライアンスではコマンド許可を設定でき、ユーザが使用できるコマンドを決定できます。

この項では、次のトピックについて取り上げます。

コマンド許可の概要

次の 2 つのコマンド許可方式のいずれかを使用できます。

- ローカル データベース：セキュリティ アプライアンス でコマンド イネーブル レベルを設定します。**enable** コマンドで認証された（または **login** コマンドでログインした）ローカル ユーザは、セキュリティ アプライアンス により、ローカル データベースに定義されているイネーブル レベルに設定されます。ユーザは、その特権レベル以下のコマンドにこれでアクセスできます。

（注）　ローカル データベース内にユーザが存在しなくても、また CLI 認証や enable 認証がない場合でも、ローカル コマンド許可を使用できます。代わりに、**enable** コマンドを入力するときにシステム イネーブル パスワードを入力すると、セキュリティ アプライアンスによってレベル 15 に置かれます。次に、すべてのレベルのイネーブル パスワードを作成します。これにより、**enable** *n*（2 ～ 15）を入力したときに、セキュリティ アプライアンスによってレベル *n* に置かれるようになります。これらのレベルは、ローカル コマンド許可をオンにするまで使用されません（後述の「ローカル コマンド許可の設定」を参照してください）。（**enable** の詳細については、『*Cisco Security Appliance Command Reference*』を参照してください）

- TACACS+ サーバ：TACACS+ サーバ上で、CLI アクセスの認証後にユーザまたはグループに許可するコマンドを設定します。CLI でユーザが入力するすべてのコマンドは、TACACS+ サーバでチェックされます。

ローカル コマンド許可の設定

ローカル コマンド許可を使用すると、各ユーザにイネーブル レベルが設定されます。ユーザは、各自のイネーブル レベル以下である任意のコマンドを入力できます。セキュリティ アプライアンス では、各コマンドに 16 のイネーブル レベル（0 ～ 15）のいずれかを指定できます。デフォルトでは、各コマンドは特権レベル 0 または 15 に割り当てられます。

この項では、次のトピックについて取り上げます。

ローカル コマンド許可の前提条件

コマンド許可コンフィギュレーションの一部として、次のタスクを実行します。

- **enable** 認証を設定します （「特権 EXEC モード アクセスするための認証の設定」（P.40-6）を参照）。

  または、コンフィギュレーションが不要な **login** コマンド（認証を伴う **enable** コマンドと同じ）を使用できます。enable 認証ほどセキュアではないため、このオプションは推奨しません。

  CLI 認証を使用することもできますが、必須ではありません。
- ローカル データベース内の各ユーザに、0 ～ 15 のイネーブル レベルを設定します

デフォルトのコマンド特権レベル

デフォルトでは、次のコマンドが特権レベル 0 に割り当てられます。その他のすべてのコマンドは、レベル 15 です。

- **show checksum**
- **show curpriv**
- **enable**（イネーブル モード）
- **help**
- **show history**
- **login**

- **logout**
- **pager**
- **show pager**
- **clear pager**
- **quit**
- **show version**

コンフィギュレーション モード コマンドを 15 より低いレベルに移動する場合は、**configure** コマンドも同じレベルに移動してください。このようにしないと、ユーザはコンフィギュレーション モードに入ることができません。

すべての特権レベルを表示する方法は、「コマンド特権レベルの表示」（P.40-10）を参照してください。

コマンドへの特権レベルの割り当てと許可のイネーブル化

コマンドを新しい特権レベルに割り当て、許可をイネーブル化するには、次の手順を実行します。

ステップ 1　次のコマンドを入力して、コマンドにイネーブル レベルを指定します。

```
hostname(config)# privilege [show | clear | cmd] level level [mode {enable | cmd}] command command
```

再割り当てする各コマンドに対してこのコマンドを繰り返します。

このコマンド内のオプションについては、次の情報を参照してください。

- **show** | **clear** | **cmd**：これらのオプション キーワードを使用すると、コマンドの show、clear、または configure 形式に対してだけ特権を設定できます。コマンドの configure 形式は、通常、未修正コマンド（**show** または **clear** プレフィックスなしで）または **no** 形式として、コンフィギュレーションの変更を引き起こす形式です。これらのキーワードのいずれかを使用しない場合は、コマンドのすべての形式が影響を受けます。
- **level** *level*：0 ～ 15 のレベル。
- **mode** {**enable** | **configure**}：ユーザ EXEC/ 特権 EXEC モードおよびコンフィギュレーション モードでコマンドを入力することができ、そのコマンドが各モードで異なるアクションを実行する場合は、それらのモードの特権レベルを個別に設定することができます。
  - **enable**：ユーザ EXEC モードと特権 EXEC モードの両方を指定します。
  - **configure**：**configure terminal** コマンドを使用してアクセスされるコンフィギュレーション モードを指定します。
- **command** *command*：設定しているコマンド。設定できるのは、*main* コマンドの特権レベルだけです。たとえば、すべての **aaa** コマンドのレベルを設定できますが、**aaa authentication** コマンドと **aaa authorization** コマンドのレベルを個別に設定できません。

  また、サブコマンドの特権レベルは main コマンドと別に設定することもできません。たとえば、**context** コマンドは設定できますが、**allocate-interface** コマンドは **context** コマンドから設定を継承するため、設定できません。

ステップ 2　次のコマンドを入力して、ローカル コマンド許可をイネーブルにします。

```
hostname(config)# aaa authorization command LOCAL
```

コマンドのイネーブル レベルを設定しても、このコマンドを使用してコマンド許可をイネーブルにしないと、コマンド許可は実行されません。

たとえば、**filter** コマンドには次の形式があります。

- **filter**（**configure** オプションで表されます）
- **show running-config filter**
- **clear configure filter**

特権レベルを形式ごとに個別に設定することができます。または、このオプションを省略してすべての形式に同じ特権レベルを設定することもできます。たとえば、それぞれの形式を別々に設定するには、次のように指定します。

```
hostname(config)# privilege show level 5 command filter
hostname(config)# privilege clear level 10 command filter
hostname(config)# privilege cmd level 10 command filter
```

また、すべてのフィルタ コマンドを同じレベルに設定できます。

```
hostname(config)# privilege level 5 command filter
```

show privilege コマンドは、形式を分けて表示します。

次の例では、**mode** キーワードの使用方法を示します。**enable** コマンドは、ユーザ EXEC モードから入力する必要があります。一方、**enable password** コマンドは、コンフィギュレーション モードでアクセスでき、最も高い特権レベルが必要です。

```
hostname(config)# privilege cmd level 0 mode enable command enable
hostname(config)# privilege cmd level 15 mode cmd command enable
hostname(config)# privilege show level 15 mode cmd command enable
```

次に、追加のコマンド **configure** コマンドの例を示します。このコマンドでは **mode** キーワードを使用します。

```
hostname(config)# privilege show level 5 mode cmd command configure
hostname(config)# privilege clear level 15 mode cmd command configure
hostname(config)# privilege cmd level 15 mode cmd command configure
hostname(config)# privilege cmd level 15 mode enable command configure
```

（注） この最後の行は、**configure terminal** コマンドで使用します。

コマンド特権レベルの表示

次のコマンドを使用すると、コマンドの特権レベルを表示できます。

- すべてのコマンドのレベルを表示するには、次のコマンドを入力します。

  ```
  hostname(config)# show running-config all privilege all
  ```

- 特定レベルのコマンドを表示するには、次のコマンドを入力します。

  ```
  hostname(config)# show running-config privilege level level
  ```

  level は 0 ～ 15 の整数です。

- 特定コマンドのレベルを表示するには、次のコマンドを入力します。

  ```
  hostname(config)# show running-config privilege command command
  ```

たとえば、**show running-config all privilege all** コマンドの場合、システムは特権レベルに対する各 CLI コマンドの現在の割り当てを表示します。次に、このコマンドの出力例を示します。

```
hostname(config)# show running-config all privilege all
privilege show level 15 command aaa
privilege clear level 15 command aaa
privilege configure level 15 command aaa
```

```
privilege show level 15 command aaa-server
privilege clear level 15 command aaa-server
privilege configure level 15 command aaa-server
privilege show level 15 command access-group
privilege clear level 15 command access-group
privilege configure level 15 command access-group
privilege show level 15 command access-list
privilege clear level 15 command access-list
privilege configure level 15 command access-list
privilege show level 15 command activation-key
privilege configure level 15 command activation-key
....
```

次に、イネーブル レベル 10 が設定されているコマンドを表示する例を示します。

```
hostname(config)# show running-config privilege level 10
privilege show level 10 command aaa
```

次に、**access-list** コマンドのレベル設定を表示する例を示します。

```
hostname(config)# show running-config privilege command access-list
privilege show level 15 command access-list
privilege clear level 15 command access-list
privilege configure level 15 command access-list
```

TACACS+ コマンド許可の設定

TACACS+ コマンド許可をイネーブルにし、ユーザが CLI でコマンドを入力すると、セキュリティ アプライアンスはそのコマンドとユーザ名を TACACS+ サーバに送信し、コマンドが許可されているかどうかを判別します。

TACACS+ サーバによるコマンド許可を設定するときは、意図したとおりに機能することが確認できるまで、コンフィギュレーションを保存しないでください。間違いによりロック アウトされた場合、通常はセキュリティ アプライアンスを再起動することによってアクセスを回復できます。それでもロックアウトされたままの場合は、「ロックアウトからの回復」（P.40-16）を参照してください。

TACACS+ システムが完全に安定して信頼できることを確認します。必要な信頼性レベルについて、通常は、完全冗長 TACACS+ サーバ システムとセキュリティ アプライアンスへの完全冗長接続が必要です。たとえば、TACACS+ サーバ プールに、インターフェイス 1 に接続された 1 つのサーバとインターフェイス 2 に接続された別のサーバを含めます。TACACS+ サーバが使用できない場合にフォールバック方式としてローカル コマンド許可を設定することもできます。この場合は、「コマンド許可の設定」（P.40-7）に従ってローカル ユーザとコマンド特権レベルを設定する必要があります。

この項では、次のトピックについて取り上げます。

- 「TACACS+ コマンド許可の前提条件」（P.40-11）
- 「TACACS+ サーバでのコマンドの設定」（P.40-12）
- 「TACACS+ コマンド許可のイネーブル化」（P.40-14）

TACACS+ コマンド許可の前提条件

コマンド許可コンフィギュレーションの一部として、次のタスクを実行します。

- CLI 認証を設定します（「ローカル コマンド許可の設定」（P.40-8）を参照）。
- **enable** 認証を設定する（「特権 EXEC モード アクセスするための認証の設定」（P.40-6）を参照）。

TACACS+ サーバでのコマンドの設定

グループまたは個々のユーザの共有プロファイル コンポーネントとしての Cisco Secure Access Control Server（ACS）TACACS+ サーバでコマンドを設定できます。サードパーティの TACACS+ サーバの場合は、コマンド許可サポートの詳細については、ご使用のサーバのマニュアルを参照してください。

Cisco Secure ACS バージョン 3.1 でコマンドを設定する場合は、次のガイドラインを参照してください。

- セキュリティ アプライアンスは、「シェル」コマンドとして許可するコマンドを送信し、TACACS+ サーバでシェル コマンドとしてコマンドを設定します。

（注） Cisco Secure ACS には、「pix-shell」と呼ばれるコマンド タイプが含まれている場合があります。このタイプはセキュリティ アプライアンスコマンド許可に使用しないでください。

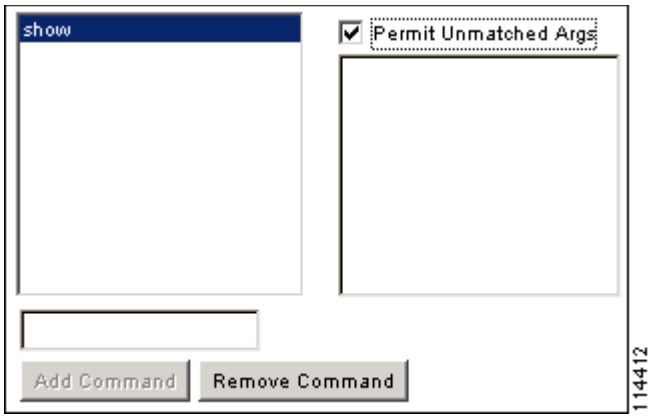
- コマンドの最初のワードは、メイン コマンドと見なされます。その他のワードはすべて引数と見なされます。これは、**permit** または **deny** の後に置く必要があります。

  たとえば、**show running-configuration aaa-server** コマンドを許可するには、**show running-configuration** をコマンド ボックスに追加し、**permit aaa-server** を引数ボックスに入力します。

- **Permit Unmatched Args** チェックボックスを選択することによって、明示的に拒否していないコマンドのすべての引数を許可することができます。

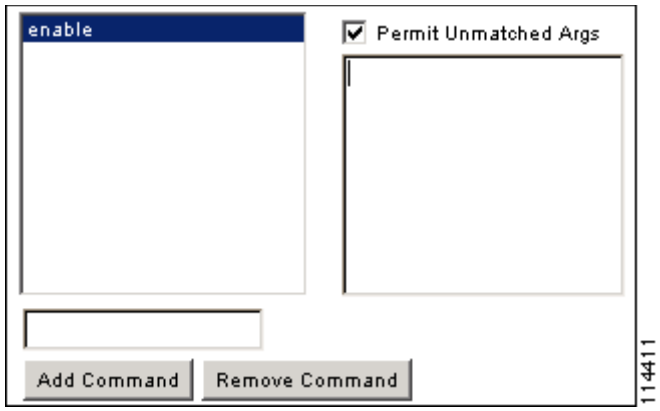
  たとえば、特定の **show** コマンドを設定するだけで、すべての **show** コマンドが許可されます。CLI の使用法を示す **?** や省略形など、コマンドの変形をすべて予想する必要がなくなるので、この方法を使用することをお勧めします（図 40-1 を参照）。

図 40-1　関連するすべてのコマンドの許可



- **enable** や **help** など、単一ワードのコマンドについては、そのコマンドに引数がない場合でも、一致しない引数を許可する*必要があります*（図 40-2 を参照）。

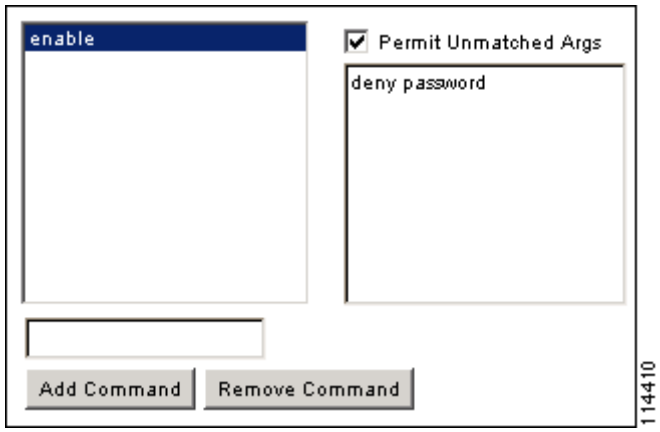
図 40-2　単一ワードのコマンドの許可



- 引数を拒否するには、その引数の前に **deny** を入力します。

  たとえば、**enable** を許可し、**enable password** を許可しない場合は、コマンド ボックスに **enable** と入力し、引数ボックスに **deny password** と入力します。**enable** だけが許可されるように、Permit Unmatched Args チェックボックスを選択してください（図 40-3 を参照）。

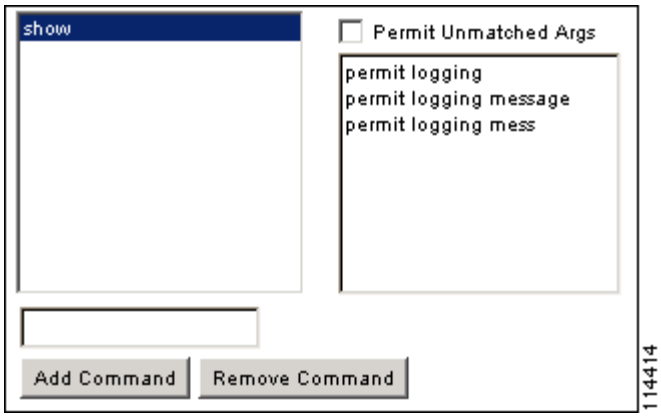
図 40-3　引数の拒否



- コマンドラインでコマンドを省略形で入力した場合、セキュリティ アプライアンスはプレフィックスとメイン コマンドを完全なテキストに展開しますが、その他の引数は入力したとおりに TACACS+ サーバに送信します。

  たとえば、**sh log** と入力すると、セキュリティ アプライアンスは完全なコマンド **show logging** を TACACS+ サーバに送信します。一方、**sh log mess** と入力すると、セキュリティ アプライアンスは展開されたコマンド **show logging message** ではなく、**show logging mess** を TACACS+ サーバに送信します。省略形を予想して同じ引数に複数のスペルを設定できます（図 40-4 を参照）。

図 40-4　　省略形の指定



- すべてのユーザに対して次の基本コマンドを許可することをお勧めします。
  - **show checksum**
  - **show curpriv**
  - **enable**
  - **help**
  - **show history**
  - **login**
  - **logout**
  - **pager**
  - **show pager**
  - **clear pager**
  - **quit**
  - **show version**

TACACS+ コマンド許可のイネーブル化

TACACS+ コマンド許可をイネーブルにする前に、TACACS+ サーバで定義されたユーザとしてセキュリティ アプライアンスにログインしていること、およびセキュリティ アプライアンスの設定を続けるために必要なコマンド許可があることを確認してください。たとえば、すべてのコマンドが許可された管理ユーザとしてログインする必要があります。このようにしないと、意図せずロックアウトされる可能性があります。

TACACS+ サーバを使用してコマンド許可を実行するには、次のコマンドを入力します。

```
hostname(config)# aaa authorization command tacacs+_server_group [LOCAL]
```

TACACS+ サーバを使用できない場合は、ローカル データベースをフォールバック方式として使用するようにセキュリティ アプライアンスを設定できます。フォールバックをイネーブルにするには、サーバ グループ名の後ろに **LOCAL** を指定します（**LOCAL** は大文字と小文字を区別します）。セキュリティ アプライアンスは、どちらの方式を使用しているかを示すプロンプトを表示しないため、ローカル データベースと TACACS+ サーバで同じユーザ名とパスワードを使用することをお勧めします。必ずローカル データベースのユーザ（「コマンド許可の設定」（P.40-7）を参照）とコマンド特権レベル（「ローカル コマンド許可の設定」（P.40-8）を参照）を設定してください。

コマンド アカウンティングの設定

CLI で **show** コマンド以外のコマンドを入力する場合、アカウンティング メッセージを TACACS+ アカウンティング サーバに送信できます。**privilege** コマンドを使用してコマンド イネーブル レベルをカスタマイズする場合（「コマンドへの特権レベルの割り当てと許可のイネーブル化」（P.40-9）を参照）、最低のイネーブル レベルを指定することにより、セキュリティ アプライアンス の対象となるコマンドを制限できます。最小特権レベルよりも下のコマンドは、セキュリティ アプライアンスで処理の対象となりません。

コマンド アカウンティング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)# aaa accounting command [privilege level] server-tag
```

level は最小特権レベルで、*server-tag* は、セキュリティ アプライアンスがコマンド アカウンティング メッセージを送信する TACACS+ サーバ グループの名前です。TACACS+ サーバ グループ設定をあらかじめ行っておく必要があります。AAA サーバ グループを設定する方法の詳細については、「AAA サーバ グループおよびサーバの識別」（P.13-12）を参照してください。

現在のログイン ユーザの表示

現在のログイン ユーザを表示するには、次のコマンドを入力します。

```
hostname# show curpriv
```

次の **show curpriv** コマンドの出力例を参照してください。各フィールドの説明については、下記を参照してください。

```
hostname# show curpriv
Username : admin
Current privilege level : 15
Current Mode/s : P_PRIV
```

表 40-1 に、**show curpriv** コマンドの出力の説明を示します。

表 40-1　show curpriv の表示の説明

フィールド	説明
Username	ユーザ名。デフォルト ユーザとしてログインすると、名前は enable_1（ユーザ EXEC）または enable_15（特権 EXEC）になります。
Current privilege level	0 ～ 15 のレベル。ローカル コマンド許可を設定してコマンドを中間特権レベルに割り当てない限り、使用されるレベルはレベル 0 と 15 だけです。
Current Mode/s	アクセス モードを表示します。 • P_UNPR：ユーザ EXEC モード（レベル 0 と 1） • P_PRIV：特権 EXEC モード（レベル 2 ～ 15） • P_CONF：コンフィギュレーション モード

ロックアウトからの回復

状況によっては、コマンド許可や CLI 認証をオンにすると、セキュリティ アプライアンス CLI からロックアウトされる場合があります。通常は、セキュリティ アプライアンスを再起動することによってアクセスを回復できます。ただし、すでにコンフィギュレーションを保存した場合は、ロックアウトされたままになる可能性があります。表 40-2 に、一般的なロックアウト条件と回復方法を示します。

表 40-2　CLI 認証およびコマンド許可のロックアウト シナリオ

機能	ロックアウト条件	説明	対応策：シングル モード	対応策：マルチ モード
ローカル CLI 認証	ローカル データベース内にユーザが存在しない。	ローカル データベース内にユーザが存在しない場合は、ログインできず、ユーザの追加もできません。	ログインし、パスワードと **aaa** コマンドをリセットします。	スイッチからセキュリティ アプライアンスへのセッションを接続します。システム実行スペースから、コンテキストに切り替えてユーザを追加することができます。
TACACS+ コマンド許可 TACACS+ CLI 認証 RADIUS CLI 認証	サーバがダウンしているか到達不能で、フォールバック方式を設定していない。	サーバが到達不能である場合は、ログインもコマンドの入力もできません。	1. ログインし、パスワードと AAA コマンドをリセットします。 2. サーバがダウンしたときにロックアウトされないように、ローカル データベースをフォールバック方式として設定します。	1. セキュリティ アプライアンスでネットワーク コンフィギュレーションが正しくないためサーバが到達不能である場合は、スイッチからセキュリティ アプライアンスへのセッションを接続します。システム実行スペースから、コンテキストに切り替えてネットワークを再設定することができます。 2. サーバがダウンしたときにロックアウトされないように、ローカル データベースをフォールバック方式として設定します。

表 40-2　CLI 認証およびコマンド許可のロックアウト シナリオ （続き）

機能	ロックアウト条件	説明	対応策：シングル モード	対応策：マルチ モード
TACACS+ コマンド許可	十分な特権のないユーザまたは存在しないユーザとしてログインした。	コマンド許可がイネーブルになりますが、ユーザはこれ以上コマンドを入力できなくなります。	TACACS+ サーバのユーザ アカウントを修正します。 TACACS+ サーバへのアクセス権がなく、セキュリティ アプライアンスをすぐに設定する必要がある場合は、メンテナンス パーティションにログインして、パスワードと **aaa** コマンドをリセットします。	スイッチからセキュリティ アプライアンスへのセッションを接続します。システム実行スペースから、コンテキストに切り替えてコンフィギュレーションの変更を完了することができます。また、TACACS+ コンフィギュレーションを修正するまでコマンド許可をディセーブルにすることもできます。
ローカル コマンド許可	十分な特権のないユーザとしてログインしている。	コマンド許可がイネーブルになりますが、ユーザはこれ以上コマンドを入力できなくなります。	ログインし、パスワードと **aaa** コマンドをリセットします。	スイッチからセキュリティ アプライアンスへのセッションを接続します。システム実行スペースから、コンテキストに切り替えてユーザ レベルを変更することができます。

ログイン バナーの設定

ユーザがセキュリティ アプライアンスに接続し、ユーザがログインする前または特権 EXEC モードに入る前に表示されるメッセージを設定できます。

ログイン バナーを設定するには、システム実行スペースで、またはコンテキスト内で、次のコマンドを入力します。

```
hostname(config)# banner {exec | login | motd} text
```

ユーザが最初に接続したとき（「今日のお知らせ」（**motd**））、ユーザがログインしたとき（**login**）、ユーザが特権 EXEC モードにアクセスしたとき（**exec**）のいずれかに表示するバナーを追加します。ユーザがセキュリティ アプライアンスに接続すると、まず「今日のお知らせ」バナーが表示され、その後にログイン バナーとプロンプトが表示されます。ユーザがセキュリティ アプライアンスに正常にログインすると、exec バナーが表示されます。

バナー テキストには、スペースは許可されますが、タブは CLI を使用して入力できません。セキュリティ アプライアンスのホスト名またはドメイン名は、**$(hostname)** 文字列と **$(domain)** 文字列を組み込むことによって動的に追加できます。システム コンフィギュレーションでバナーを設定する場合は、コンテキスト コンフィギュレーションで **$(system)** 文字列を使用することによって、コンテキスト内でそのバナー テキストを使用できます。

複数の行を追加する場合は、各行の前に **banner** コマンドを置きます。

たとえば、「今日のお知らせ」バナーを追加するには、次のように入力します。

```
hostname(config)# banner motd Welcome to $(hostname).
hostname(config)# banner motd Contact me at admin@example.com for any
hostname(config)# banner motd issues.
```