CHAPTER 23

管理アクセスの設定

この章では、システム管理のために Telnet、SSH、HTTPS、および VPN 経由で FWSM にアクセスする方法について説明します。ユーザ認証および許可の方法についても説明します。

この章では、次の内容について説明します。

（注） また、管理アクセス用の FWSM 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

FWSM は、管理目的で FWSM 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。

FWSM 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。コンテキストごとに許可する Telnet セッション数を管理するには、リソース クラスを使用します （「クラスの設定」（P.4-25）を参照）。管理コンテキストにかぎって、最大 15 の Telnet セッションと 15 の SSH セッションを同時に使用できます。

（注） 2 つ以上の同時 Telnet または SSH セッションを使用しており、いずれかのセッションで **More** プロンプトが表示されている場合、**More** プロンプトが終了するまで他のセッションが中断することがあります。**More** プロンプトをディセーブルにしてこの状況を回避するには、**pager lines 0** コマンドを入力します。

FWSM への同時アクセスは推奨されないことに注意してください。状況によっては、2 つの Telnet セッションで同じコマンドを発行すると、一方のセッションでキーが押されるまで、もう一方のセッションが中断する場合もあります。

FWSM に Telnet アクセスを設定する手順は、次のとおりです。

ステップ 1　FWSM 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）FWSM 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、実動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 FWSM にアクセスするには、次のコマンドを入力します。

```
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 FWSM 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

FWSM は、管理目的で FWSM への SSH 接続を許可します。FWSM 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。各コンテキストに許可する SSH セッション数を管理するには、リソース クラスを使用します（「クラスの設定」（P.4-25）を参照）。管理コンテキストにかぎって、最大 15 の Telnet セッションと 15 の SSH セッションを同時に使用できます。

（注）　2 つ以上の同時 Telnet または SSH セッションを使用しており、いずれかのセッションで **More** プロンプトが表示されている場合、**More** プロンプトが終了するまで他のセッションが中断することがあります。**More** プロンプトをディセーブルにしてこの状況を回避するには、**pager lines 0** コマンドを入力します。

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。FWSM 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。

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

ここでは、次の内容について説明します。

- 「SSH アクセスの設定」（P.23-3）

SSH アクセスの設定

FWSM に SSH アクセスを設定する手順は、次のとおりです。

ステップ 1　SSH に必要な RSA キー ペアを生成するには、「キー ペアの生成」（P.12-4）を参照してください。

ステップ 2　FWSM 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
```

FWSM 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 3　（任意）FWSM 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、実動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。

ステップ 4　（任意）次のコマンドを入力して、FWSM で許可する SSH のバージョンを制限します。デフォルトでは、FWSM は両方のバージョンを許可します。

```
hostname(config)# ssh version {1 | 2}
```

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 FWSM にアクセスするには、次のコマンドを入力します。

```
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 FWSM 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
```

SSH クライアントの使用

SSH を使用して FWSM 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.7-1）を参照）。デフォルトのパスワードは「cisco」です。

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、FWSM 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復号化する場合です。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、FWSM 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 用の 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、FWSM 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、これらの設定は完了します。ここでは、ASDM アクセスを手動で設定する場合の手順について説明します。

FWSM では、コンテキストごとに最大 5 つの同時 ASDM インスタンスを使用でき、全コンテキスト間で最大 80 の ASDM インスタンスの使用が可能です。コンテキストごとに許可する ASDM セッション数を管理するには、リソース クラスを使用します （「クラスの設定」（P.4-25）を参照）。

ASDM アクセスを設定する手順は、次のとおりです。

ステップ 1　FWSM 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
```

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、次のコマンドを入力します。

```
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
```

VPN 管理接続の許可

FWSM は、IPSec を使用した管理アクセスをサポートしています。IPSec Virtual Private Network（VPN; 仮想私設網）では、インターネットなどの安全性の低いネットワーク上で、IP パケットを確実かつ安全に転送できます。2 つの VPN ピア間の通信はすべて、セキュア トンネルを通じて転送されます。つまり、パケットは暗号化され、各ピアに認証されます。

FWSM は、サイトツーサイト トンネルを使用して、Cisco PIX セキュリティ アプライアンスまたは Cisco IOS ルータなどの他の VPN コンセントレータに接続できます。このトンネルを通じて通信できるピア ネットワークを指定します。FWSM の場合、トンネルの FWSM 側で使用できるアドレスは、対象インターフェイスのアドレスだけです。

ルーテッド モードの場合、FWSM は VPN クライアントからの接続も受け入れます。VPN クライアントとは、Cisco VPN クライアント、または Cisco PIX セキュリティ アプライアンスなどの VPN コンセントレータを稼動するホスト、あるいは Easy VPN クライアントを稼動する Cisco IOS ルータを指しま

す。この場合、サイトツーサイト トンネルとは異なり、クライアントの IP アドレスを事前に取得することはできません。クライアント認証に依存することになります。トランスペアレント ファイア ウォール モードでは、リモート クライアントはサポートされていません。トランスペア レント モードでは、サイトツーサイトのトンネルがサポートされます。

FWSM は、最大 5 つの同時 IPSec 接続をサポートし、全コンテキスト間で最大 10 の同時接続が可能です。コンテキストごとに許可する IPSec セッション数を管理するには、リソース クラスを使用します（「クラスの設定」（P.4-25）を参照）。

この項は、次のトピックで構成されています。

- 「全トンネルの基本的な設定」（P.23-5）
- 「VPN クライアント アクセスの設定」（P.23-6）
- 「サイトツーサイト トンネルの設定」（P.23-8）

全トンネルの基本的な設定

VPN クライアント アクセスとサイトツーサイト トンネルの両方で次の手順を実行します。また、IKE ポリシー（IKE は ISAKMP の一部）および IPSec トランスフォームの設定も必要です。

すべてのトンネルに基本設定を適用する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、IKE 暗号化アルゴリズムを設定します。

```
hostname(config)# isakmp policy priority encryption {des | 3des}
```

3des キーワードの方が、**des** キーワードよりも安全です。

複数の IKE ポリシーを設定できます。FWSM は、ピアのポリシーと一致するまで、*priority* の順序で各ポリシーを検証します。*priority* の値は 1 ～ 65,534 です。プライオリティは 1 が最高で、65,534 が最低です。次の **isakmp** コマンドにも、同じプライオリティ値を使用してください。

ステップ 2　次のコマンドを入力して、キー交換に使用する Diffie-Hellman グループを設定します。

```
hostname(config)# isakmp policy priority group {1 | 2}
```

グループ 1 は 768 ビット、グループ 2 は 1,024 ビット（より安全性が高い）です。

ステップ 3　次のコマンドを入力して、認証アルゴリズムを設定します。

```
hostname(config)# isakmp policy priority hash {md5 | sha}
```

sha キーワードの方が、**md5** キーワードよりも安全です。

ステップ 4　次のコマンドを入力して、IKE 認証方式を共有キーとして設定します。

```
hostname(config)# isakmp policy priority authentication pre-share
```

rsa-sig オプションを指定すると、共有キーの代わりに証明書を使用できます。この方式の詳細については、*『Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference』* を参照してください。

ステップ 5　次のコマンドを入力して、トンネル インターフェイス上で IKE をイネーブルにします。

```
hostname(config)# isakmp enable interface_name
```

ステップ 6　次のコマンドを入力して、トランスフォーム セットの IPSec トンネルに使用する認証方式および暗号化方式を設定します。

```
hostname(config)# crypto ipsec transform-set transform_name [esp-md5-hmac | esp-sha-hmac]
{esp-aes-256 | esp-aes-192 | esp-aes | esp-des | esp-3des}
```

認証だけ、または暗号化だけを指定することもできますが、これらの方式は安全ではありません。

このトランスフォーム セットは、VPN クライアント グループまたはサイトツーサイト トンネルの設定時に参照します。

トンネルでは最大 6 つのトランスフォーム セットを参照できます。トランスフォームが一致するまで、各セットが検証されます。

このトランスフォームの認証および暗号化アルゴリズムは通常、IKE ポリシー（**isakmppolicy** コマンド）と一致します。サイトツーサイト トンネルの場合には、このトランスフォームがピアのトランスフォームと一致する必要があります。

認証オプションは、（安全性の高い方から順に）次のとおりです。

- **esp-sha-hmac**
- **esp-md5-hmac**

暗号化オプションは、（安全性の高い方から順に）次のとおりです。

- **esp-aes-256**
- **esp-aes-192**
- **esp-aes**
- **esp-3des**
- **esp-des**

（注）　**esp-null**（暗号化なし）を使用するのは、テストを行う場合だけです。

次に、複数の IKE ポリシーおよび IPSec トランスフォーム セットを設定する例を示します。

```
hostname(config)# isakmp policy 1 authentication pre-share
hostname(config)# isakmp policy 1 encryption 3des
hostname(config)# isakmp policy 1 group 2
hostname(config)# isakmp policy 1 hash sha
hostname(config)# isakmp enable outside
hostname(config)# crypto ipsec transform-set vpn_client esp-3des esp-sha-hmac
hostname(config)# crypto ipsec transform-set site_to_site esp-3des ah-sha-hmac
```

VPN クライアント アクセスの設定

ルーテッド モードの場合、Cisco VPN クライアントの Version 3.0 がインストールされているホストであれば、インターネットなどの公衆ネットワークを通じて、管理目的で FWSM に接続できます。

トランスペアレント ファイアウォール モードでは、リモート クライアントはサポートされていません。トランスペアレント モードでは、サイトツーサイトのトンネルがサポートされます。

VPN の基本設定（「全トンネルの基本的な設定」を参照）を完了したあと、リモート クライアントから FWSM への管理アクセスを許可する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、クライアント トンネルに許可するトランスフォーム セット（「全トンネルの基本的な設定」（P.23-5）で定義したセット）を指定します。

```
hostname(config)# crypto dynamic-map dynamic_map_name priority set transform-set
transform_set1 [transform_set2] [...]
```

複数のトランスフォーム セットをプライオリティ順（最高のプライオリティのものが最初）に列挙します。

ダイナミック クリプト マップでは、未知の IP アドレスから FWSM に接続できます。

dynamic-map の名前は、ステップ 2 で使用します。

priority には、複数のコマンドを評価する優先順位を指定します。1 つのコマンドに 1 つのトランスフォーム セットを指定し、別のコマンドに別のセットを指定した場合、プライオリティの値に基づいて最初に評価されるコマンドが決まります。

ステップ 2　次のコマンドを入力して、スタティック トンネルに（ステップ 1 で指定した）ダイナミック クリプト マップを割り当てます。

```
hostname(config)# crypto map crypto_map_name priority ipsec-isakmp dynamic
dynamic_map_name
```

ステップ 3　次のコマンドを入力して、クライアント トンネルを終端するインターフェイスを指定します。

```
hostname(config)# crypto map crypto_map_name interface interface_name
```

1 つのインターフェイスに割り当てることのできる **crypto map** 名は 1 つだけです。したがって、サイトツーサイト トンネルと VPN クライアントの両方を同じインターフェイス上で終端する場合は、同じ **crypto map** 名を共有する必要があります。

ステップ 4　次のコマンドを入力して、VPN クライアントが FWSM 上で使用するアドレス範囲を指定します。

```
hostname(config)# ip local pool pool_name first_ip_address-last_ip_address [mask mask]
```

クライアントからのトンネル経由の全パケットが、送信元アドレスとして、これらのアドレスの 1 つを使用します。

ステップ 5　次のコマンドを入力して、FWSM 宛てのトラフィックを指定します。ステップ 7 の **tunnel group** コマンドで指定したトラフィックだけをトンネル化できます。

```
hostname(config)# access-list acl_name [extended] permit {protocol} host
fwsm_interface_address pool_addresses mask
```

このアクセス リストでは、ローカル プール（ステップ 4 を参照）から FWSM のインターフェイスに送信するトラフィックを特定しています。アクセス リストの詳細については、「拡張アクセス リストの追加」（P.13-6）を参照してください。

ステップ 6　次のコマンドを入力して、トンネル グループに VPN アドレス プールを割り当てます。

```
hostname(config)# tunnel-group name general-attributes address-pool pool_name
```

このグループは、クライアントの接続に必要な VPN 特性です。クライアントは、FWSM への接続時に、このトンネル グループ名と、ステップ 8 で指定するパスワードを入力する必要があります。

ステップ 7　次のコマンドを入力して、FWSM 宛てのトラフィックだけをトンネル化します。

```
hostname(config)# group-policy name attributes
hostname(config-group-policy)# split-tunnel-policy tunnelall
```

（注）　このコマンドは必須です。

ステップ 8　次のコマンドを入力して、VPN グループのパスワードを設定します。

```
hostname(config)# group-policy group_name external server-group server_group_name password
server_password
```

ステップ 9　「Telnet アクセスの許可」（P.23-1）および「SSH アクセスの許可」（P.23-2）を参照して、Telnet アクセスまたは SSH アクセスを許可します。

telnet コマンドおよび **ssh** コマンドに、VPN プール アドレスを指定してください。

次に、VPN クライアントに、外部インターフェイス（209.165.200.225）上での Telnet の使用を許可する例を示します。ユーザ認証はローカル データベースです。この場合、指定のトンネル グループ名とパスワード、およびユーザ名「admin」とパスワード「passw0rd」を持つユーザが、FWSM に接続できます。

```
hostname(config)# isakmp policy 1 authentication pre-share
hostname(config)# isakmp policy 1 encryption 3des
hostname(config)# isakmp policy 1 group 2
hostname(config)# isakmp policy 1 hash sha
hostname(config)# isakmp enable outside
hostname(config)# username admin password passw0rd
hostname(config)# crypto ipsec transform-set vpn esp-3des esp-sha-hmac
hostname(config)# crypto dynamic-map vpn_client 1 set transform-set vpn
hostname(config)# crypto map telnet_tunnel 1 ipsec-isakmp dynamic vpn_client
hostname(config)# crypto map telnet_tunnel interface outside
hostname(config)# crypto map telnet_tunnel client authentication LOCAL
hostname(config)# ip local pool Firstpool 10.1.1.1-10.1.1.2
hostname(config)# access-list VPN_SPLIT extended permit ip host 209.165.200.225 host 10.1.1.1
hostname(config)# access-list VPN_SPLIT extended permit ip host 209.165.200.225 host 10.1.1.2
hostname(config)# tunnel-group StocktonAAA general-attributes address-pool Firstpool
hostname(config)# group-policy name attributes
hostname(config-group-policy)# split-tunnel-policy tunnelall
hostname(config)# group-policy ExternalGroup external server-group LodiAAA password $ecure23
hostname(config)# telnet 10.1.1.1 255.255.255.255 outside
hostname(config)# telnet 10.1.1.2 255.255.255.255 outside
hostname(config)# telnet timeout 30
```

サイトツーサイト トンネルの設定

VPN の基本設定（「全トンネルの基本的な設定」を参照）を完了したあと、サイトツーサイト トンネルを設定する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、両方のピアで使用する共有キーを設定します。

```
hostname(config)# isakmp key keystring address peer-address
```

ステップ 2　次のコマンドを入力して、トンネルを通過させるトラフィックを特定します。

```
hostname(config)# access-list acl_name [extended] {deny | permit} {protocol} host
fwsm_interface_address dest_address mask
```

宛先アドレスには、FWSM へのアクセスを許可したアドレスを指定します。

アクセス リストの詳細については、「拡張アクセス リストの追加」（P.13-6）を参照してください。

ステップ 3　次のコマンドを入力して、IPSec トンネルを作成します。

```
hostname(config)# crypto map crypto_map_name priority ipsec-isakmp
```

トンネルの属性はすべて、同じ **crypto map** 名で識別します。

priority には、複数のコマンドを評価する優先順位を指定します。1 つのコマンドでこの **crypto map** 名と **ipsec-isakmp** を指定し、別のコマンドで **ipsec-isakmp dynamic**（VPN クライアント接続用）を指定した場合、プライオリティの値に基づいて最初に評価されるコマンドが決まります。

ステップ 4　次のコマンドを入力して、トンネルに（ステップ 2 で指定した）アクセス リストを割り当てます。

```
hostname(config)# crypto map crypto_map_name priority match address acl_name
```

ステップ 5　次のコマンドを入力して、トンネルを終端するリモート ピアを指定します。

```
hostname(config)# crypto map crypto_map_name priority set peer ip_address
```

ステップ 6　次のコマンドを入力して、トンネルに使用するトランスフォーム セット（「全トンネルの基本的な設定」（P.23-5）で定義したもの）を指定します。

```
hostname(config)# crypto map crypto_map_name priority set transform-set transform_set1
[transform_set2] [...]
```

複数のトランスフォーム セットをプライオリティ順（最高のプライオリティのものが最初）に列挙します。最大 6 つのトランスフォーム セットを指定できます。

ステップ 7　次のコマンドを入力して、トンネルを終端するインターフェイスを指定します。

```
hostname(config)# crypto map crypto_map_name interface interface_name
```

1 つのインターフェイスに割り当てることのできる **crypto map** 名は 1 つだけです。したがって、サイトツーサイト トンネルと VPN クライアントの両方を同じインターフェイス上で終端する場合は、同じ **crypto map** 名を共有する必要があります。

このコマンドは、必ず他のすべての **crypto map** コマンドを入力したあとで、最後に指定してください。いずれかの **crypto map** コマンドの設定を変更する場合は、このコマンドの **no** 形式を入力して一度削除してから、再度入力してください。

ステップ 8　「Telnet アクセスの許可」（P.23-1）および「SSH アクセスの許可」（P.23-2）を参照して、Telnet アクセスまたは SSH アクセスを許可します。

次に、ピア ルータ（209.165.202.129）に接続しているホストに、外部インターフェイス（209.165.200.225）上での Telnet の使用を許可する例を示します。

```
hostname(config)# isakmp policy 1 authentication pre-share
hostname(config)# isakmp policy 1 encryption 3des
hostname(config)# isakmp policy 1 group 2
hostname(config)# isakmp policy 1 hash sha
hostname(config)# isakmp enable outside
hostname(config)# crypto ipsec transform-set vpn esp-3des esp-sha-hmac
hostname(config)# isakmp key 7mfi02lirotn address 209.165.200.223
hostname(config)# access-list TUNNEL extended permit ip host 209.165.200.225 209.165.201.0
255.255.255.224
hostname(config)# crypto map telnet_tunnel 2 ipsec-isakmp
hostname(config)# crypto map telnet_tunnel 1 match address TUNNEL
hostname(config)# crypto map telnet_tunnel 1 set peer 209.165.202.129
hostname(config)# crypto map telnet_tunnel 1 set transform-set vpn
hostname(config)# crypto map telnet_tunnel interface outside
hostname(config)# telnet 209.165.201.0 255.255.255.224 outside
hostname(config)# telnet timeout 30
```

FWSM との ICMP 送受信の許可

デフォルトでは、FWSM インターフェイスに対する（または FWSM を経由する）ICMP（ping を含む）は許可されていません（FWSM を*経由*する ICMP の許可については、第 15 章「ネットワーク アクセスの許可または拒否」を参照してください）。ICMP はネットワーク接続をテストする重要なツールですが、同時に FWSM またはネットワークを攻撃する手段にもなります。ICMP は初期テストの実行時にかぎって許可し、通常の運用中は許可しないことを推奨します。

システム全体で許可される ICMP ルールの最大数については、「ルールの制限」（P.A-6）を参照してください。

ICMP を使用して、FWSM のインターフェイスに到達するアドレスを許可または拒否するには（ホストから FWSM へ、または FWSM からホストへ送信し、ICMP 応答の返信を許可する）、次のコマンドを入力します。

```
hostname(config)# icmp {permit | deny} {host ip_address | ip_address mask | any}
[icmp_type] interface_name
```

icmp_type を指定しないと、すべてのタイプが対象になります。番号または名前を入力できます。ping を制御するには、**echo-reply** （**0**）（FWSM からホストへ）または **echo** （**8**）（ホストから FWSM へ）を指定します。ICMP タイプのリストについては、「ICMP タイプ」（P.E-16）を参照してください。

アクセス リストと同様に、FWSM はパケットを、各 **icmp** ステートメントに対して順番に照合します。特定のステートメントを最初に設定し、一般的なステートメントをあとに設定してください。最後に暗黙の拒否を設定します。たとえば、最初にすべてのアドレスを許可し、次に特定のアドレスを拒否した場合、そのアドレスは最初のステートメントにすでに一致しているので、許可されることになります。

（注） FWSM からホストへの ping を許可（すなわち、インターフェイスへのエコー応答を許可）し、ホストから FWSM への ping を許可したくない場合には、上記のコマンドを入力する代わりに、ICMP インスペクション エンジンをイネーブルにする方法もあります。第 22 章「アプリケーション層プロトコル検査の適用」を参照してください。

たとえば、10.1.1.15 のホストを除くすべてのホストに対して内部インターフェイスへの ICMP の使用を許可するには、次のコマンドを入力します。

```
hostname(config)# icmp deny host 10.1.1.15 inside
hostname(config)# icmp permit any inside
```

10.1.1.15 のホストに内部インターフェイスへの ping の使用だけを許可するには、次のコマンドを入力します。

```
hostname(config)# icmp permit host 10.1.1.15 inside
```

システム管理者用の AAA

ここでは、システム管理者が CLI 認証、コマンド許可、およびコマンド アカウンティング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 11 章「AAA サーバとローカル データベースの設定」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。

（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で AAA コマンドを設定できません。ただし、管理コンテキストで Telnet 認証を設定した場合、認証はスイッチから FWSM へのセッション（システム実行スペースへのアクセス時）にも適用されます。詳細については、「CLI および ASDM アクセスの認証の設定」（P.23-11）を参照してください。

ここでは、次の内容について説明します。

CLI および ASDM アクセスの認証の設定

ここでは、Telnet または SSH を使用する場合に CLI 認証を設定する方法、および ASDM 認証を設定する方法について説明します。ここでは、次の内容について説明します。

CLI アクセスの概要

FWSM で Telnet または SSH ユーザを認証するには、**telnet** または **ssh** コマンドを使用して、事前に FWSM へのアクセスを設定しておく必要があります（「Telnet アクセスの許可」（P.23-1）および「SSH アクセスの許可」（P.23-2）を参照）。これらのコマンドでは、FWSM との通信を許可する IP アドレスを指定します。ただし、マルチコンテキスト モードのシステムへのアクセスについては例外です。この場合、スイッチから FWSM へのセッションは Telnet セッションですが、**telnet** コマンドは不要です。

FWSM に接続した後、ログインしてユーザ EXEC モードにアクセスします。

- Telnet の認証をイネーブルにしていない場合は、ユーザ名を入力しません。ログイン パスワード（**password** コマンドで設定）を入力します。SSH の場合、ユーザ名に「pix」と入力し、ログイン パスワードを入力します。
- この項の説明に従って Telnet または SSH 認証をイネーブルにした場合は、AAA サーバまたはローカル ユーザ データベースで定義されているユーザ名とパスワードを入力します。

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）。

- 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。
- 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.23-13）を参照）、FWSM 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。

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。

ASDM アクセスの概要

デフォルトでは、ブランクのユーザ名と **enable password** コマンドで設定したイネーブル パスワードを使用して ASDM にログインできます。ただし、ログイン画面で（ユーザ名をブランクのままにしないで）ユーザ名とパスワードを入力した場合は、ASDM によってローカル データベースで一致がチェックされます。

この項の説明に従って HTTP 認証を設定し、ローカル データベースを指定できますが、その機能は常にデフォルトでイネーブルになります。認証用に RADIUS または TACACS+ サーバを使用する場合は、HTTP 認証を設定するだけで済みます。

スイッチから FWSM へのセッションの認証

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で AAA コマンドを設定できません。ただし、管理コンテキストで Telnet 認証を設定した場合、認証はスイッチから FWSM へのセッション（システム実行スペースへのアクセス時）にも適用されます。この場合、管理コンテキストの AAA サーバまたはローカル ユーザ データベースが使用されます。

CLI または ASDM 認証のイネーブル化

CLI または ASDM 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} console {LOCAL |
server_group [LOCAL]}
```

telnet キーワードを指定すると、Telnet セッションの認証がイネーブルになります。また、管理コンテキストでこのコマンドを設定する場合は、スイッチから FWSM へのセッションの認証もイネーブルになります。

ssh キーワードを指定すると、SSH セッションの認証がイネーブルになります。

http キーワードは、HTTPS を使用して FWSM にアクセスする ASDM クライアントを認証します。

認証に TACACS+ または RADIUS サーバ グループを使用する場合、AAA サーバが使用できないときには、フォールバック方式としてローカル データベースを使用するように FWSM 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、FWSM 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。

たとえば、スイッチから FWSM システム実行スペースへのセッションの認証をイネーブルにするには、スイッチの CLI で次のコマンドを入力します。

```
Router# session slot 1 processor 1（スロット 1 の FWSM）
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.41 ... Open

User Access Verification

Password: cisco（デフォルトのログイン パスワード）
Type help or '?' for a list of available commands.
hostname> enable
hostname# configure terminal
hostname(config)# changeto context admin（システム実行スペースから管理コンテキスト「admin」に変更）
hostname/admin (config)# aaa-server RADS protocol radius（サーバ グループ RADS を追加）
hostname/admin (config-aaa-server-group)# aaa-server RADS (mgmt) host 192.168.1.4 cisco
（RADIUS サーバを RADS サーバ グループに追加）
hostname/admin (config-aaa-server-group)# exit
hostname/admin (config)# aaa authentication telnet console RADS（RADS サーバ グループを使用して Telnet 認証をイネーブル化）
```

次回、スイッチから FWSM へのセッションを開始しようとすると、RADIUS サーバで定義されたユーザ名とパスワードの入力を要求されます。

```
Router# session slot 1 processor 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.41 ... Open

User Access Verification

Username: myRADIUSusername
Password: myRADIUSpassword
Type help or '?' for a list of available commands.
```

イネーブル EXEC モード アクセス認証の設定

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 FWSM 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。

ここでは、次の内容について説明します。

- 「enable コマンドの認証の設定」（P.23-13）
- 「login コマンドを使用したユーザ認証」（P.23-13）

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、FWSM を設定できます。**enable** コマンドの認証を行わない場合、**enable** コマンドを入力すると、FWSM により（**enable password** コマンドで設定した）イネーブル パスワードの入力を要求されます。この場合、特定ユーザとしてのログインではなくなります。**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認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 TACACS+ または RADIUS サーバ グループを使用する場合、AAA サーバが使用できないときには、フォールバック方式としてローカル データベースを使用するように FWSM 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、FWSM 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 コマンドを使用したユーザ認証

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。

イネーブル認証と異なり、この方法は、マルチコンテキスト モードのシステム実行スペースで使用できます。システム実行スペースで **login** コマンドを入力すると、管理コンテキストのローカル ユーザ データベースが使用されます。システム コンフィギュレーションには、ローカル ユーザ データベースは含まれません（**username** コマンドは入力できません）。

このログイン方法では、ユーザは独自のユーザ名とパスワードを使用して特権 EXEC モードにアクセスできるので、すべてのユーザにシステム イネーブル パスワードを提供する必要はありません。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 コマンド認可を設定した場合、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 コマンド認可の設定」（P.23-16）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、コマンド認可を設定する必要があります。コマンド認可がない場合、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。または、RADIUS または TACACS+ 認証を使用できます。あるいは、すべてのローカル ユーザをレベル 1 に設定して、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
```

FWSM 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、FWSM 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。ユーザ EXEC モードで入力できるコマンドは、**login** コマンドだけです。特権 EXEC モードからユーザ EXEC モードに戻るには、**disable** コマンドを入力します。

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には、FWSM にコマンド許可を設定し、各ユーザに許可するコマンドを制限します。

ここでは、次の内容について説明します。

コマンド許可の概要

次の 2 つのコマンド認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：FWSM 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、FWSM 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、自身のイネーブル レベル以下のコマンドにアクセスできます。

  ローカル コマンド認可は、ローカル データベース内にユーザがなくても、CLI または enable 認証がなくても使用できます。この場合、**enable** コマンドの入力時にシステム イネーブル パスワードを使用すると、FWSM によってデフォルトのユーザ名が「enable_15」に設定され、レベルは 15 となります。管理者はすべてのレベルにイネーブル パスワードを作成できるため、**enable** *n*（2 ～ 15）を入力したときに FWSM から指定されるレベルは *n* になります。これらのレベルは、ローカル コマンド許可をイネーブルにした場合にかぎり、使用されます（「ローカル コマンド認可の設定」を参照）。**enable** コマンドの詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module 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。

セキュリティ コンテキストとコマンド許可

次に、複数のセキュリティ コンテキストでコマンド認可を実装する際の重要な考慮点を示します。

- AAA 設定はコンテキストごとに個別であり、コンテキスト間で共有されません。

  コマンド認可を設定する場合、各セキュリティ コンテキストを別々に設定する必要があります。これにより、異なるセキュリティ コンテキストに対して異なるコマンド認可を実行できます。

  セキュリティ コンテキストを切り替える場合、管理者は、ログイン時に指定されたユーザ名に対して許可されるコマンドが新しいコンテキスト セッションでは異なる場合があること、または新しいコンテキストではコマンド認可がまったく設定されていない場合があることに注意する必要があります。セキュリティ コンテキストによってコマンド認可が異なる場合があることを理解していないと、管理者は混乱することがあります。この動作は、次の点によってさらに複雑になります。

- **changeto** コマンドによって開始された新しいコンテキスト セッションでは、前のコンテキスト セッションで使用されたユーザ名に関係なく、管理者 ID として常にデフォルトの「enable_15」ユーザ名が使用されます。この動作は、enable_15 ユーザに対してコマンド認可が設定されていない場合や、enable_15 ユーザに対する認可が前のコンテキスト セッションでのユーザに対する認可と異なる場合に、混乱を招くことがあります。

  また、この動作はコマンド アカウンティングにも影響を及ぼします。コマンド アカウンティングは、発行された各コマンドを特定の管理者に正確に関連付けることができる場合にのみ役立ちます。**changeto** コマンドを使用する権限を持つすべての管理者は、enable_15 ユーザ名を他のコンテキストで使用できるため、誰が enable_15 ユーザ名としてログインしたかをコマンド アカウンティング レコードで識別することが困難になる場合があります。コンテキストごとに異なるアカウンティング サーバを使用する場合、誰が enable_15 ユーザ名を使用していたかを追跡するには、複数のサーバからのデータを関連付ける必要があります。

  コマンド認可を設定する場合は、次のことを考慮します。

  - **changeto** コマンドを使用する権限を持つ管理者は、実質的に、他の各コンテキストで、enable_15 ユーザに対して許可されているすべてのコマンドを使用する権限を持ちます。
  - コンテキストごとにコマンドを認可する場合は、各コンテキストで、**changeto** コマンドを使用する許可を持つ管理者に対して拒否されているコマンドの使用を、enable_15 ユーザ名に対しても拒否するようにします。

  セキュリティ コンテキストを切り替える場合、管理者は特権 EXEC モードを終了し、再度 **enable** コマンドを入力して必要なユーザ名を使用できます。

（注） システム実行スペースでは AAA コマンドがサポートされないため、システム実行スペースではコマンド認可を使用できません。

ローカル コマンド認可の設定

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。FWSM 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。

ここでは、次の内容について説明します。

- 「コマンド特権レベルの表示」（P.23-19）

ローカル コマンド認可の前提条件

コマンド認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。（「イネーブル EXEC モード アクセス認証の設定」（P.23-13）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 （「ローカル データベースの設定」（P.11-7）を参照）。

デフォルトのコマンド特権レベル

デフォルトでは、次のコマンドに特権レベル 0 が割り当てられます。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 よりも低いレベルに移動する場合は、**configure** コマンドもそのレベルに移動してください。そうしないと、ユーザはコンフィギュレーション モードを開始できません。

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.23-19）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認可のイネーブル化

コマンドに新しいイネーブル レベルを指定し、許可をイネーブルにする手順は、次のとおりです。

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、変更されていないコマンド（**show** または **clear** プレフィクスなし）または **no** 形式としてコンフィギュレーションの変更が発生するコマンド形式です。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のみです。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** コマンドや **aaa authorization** コマンドのレベルは別々に設定できません。

  また、メイン コマンドとは別に、コンフィギュレーション モードでメイン コマンドを使用して入力するコマンドのイネーブル レベルを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** オプションの部分）
- **show running-config filter**
- **clear configure filter**

形式ごとに別々に特権レベルを設定することも、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、画面に表示する形式を別々にします。

次に、**mode** キーワードを使用する例を示します。**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、**mode** キーワードを使用して、**configure** コマンドにレベルを設定する例を示します。

```
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） 最後の行は、**configure terminal** コマンド用です。

コマンド特権レベルの表示

コマンドのイネーブル レベルを表示するには、次のコマンドを使用します。

- 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
  ```

次に、**show running-config all privilege all** コマンドの出力例を示します。各 CLI コマンドの現在のイネーブル レベル設定状況が表示されます。

```
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+ コマンド認可をイネーブルにし、ユーザが CLI でコマンドを入力する場合、FWSM によってコマンドとユーザ名が TACACS+ サーバに送信され、コマンドが認可されているかどうかが判別されます。

TACACS+ サーバによるコマンド認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 FWSM 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.23-24）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 FWSM 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 コマンド認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.23-15）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。

ここでは、次の内容について説明します。

TACACS+ コマンド認可の前提条件

コマンド認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（「CLI および ASDM アクセスの認証の設定」（P.23-11）を参照）。
- **enable** 認証を設定する（「イネーブル EXEC モード アクセス認証の設定」（P.23-13）を参照）。

TACACS+ サーバでのコマンドの設定

グループまたは個人ユーザの共有プロファイル コンポーネントとして、Cisco Secure Access Control Server（ACS）上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、コマンド認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。これらのガイドラインの多くは、サードパーティ サーバにも適用されます。

- FWSM は、「シェル」コマンドとして認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 FWSM コマンド認可に使用しないでください。

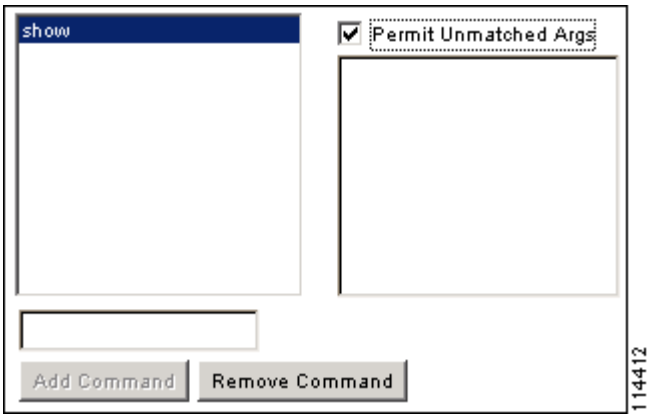
- コマンドの最初のワードは、メイン コマンドと見なされます。その他のワードはすべて引数と見なされます。これは、**permit** または **deny** の後に置く必要があります。

  たとえば、**show running-configuration aaa-server** コマンドを許可するには、コマンド フィールドに **show running-configuration** を追加し、引数フィールドに **permit aaa-server** を入力します。

- [Permit Unmatched Args] チェックボックスを選択すると、明示的に拒否していないすべてのコマンド引数を許可できます。

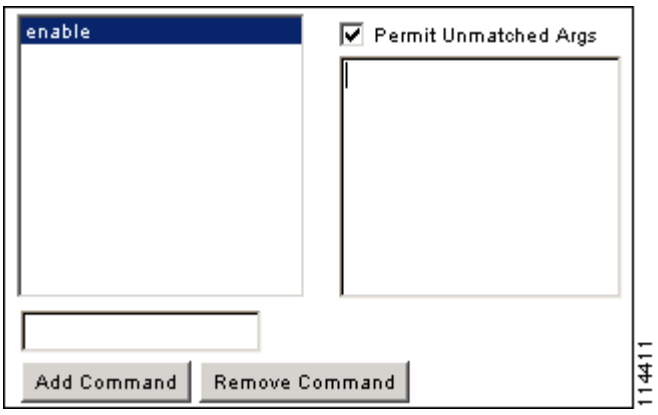
たとえば、特定の **show** コマンドを設定するだけで、すべての **show** コマンドが許可されます。CLI の使用法を示す疑問符や省略形など、コマンドの変形をすべて予想する必要がなくなるので、この方法を使用することをお勧めします（図 23-1 を参照）。

図 23-1　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 23-2 を参照）。

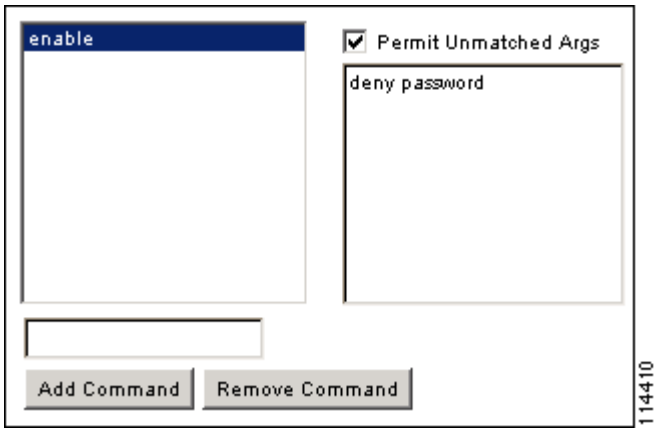
図 23-2　単一ワードのコマンドの許可



- 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** コマンドを許可し、**enable password** コマンドを許可しない場合には、コマンド フィールドに **enable** を入力し、引数フィールドに **deny password** を入力します。**enable** だけが許可されるように、必ず、[Permit Unmatched Args] チェックボックスを選択してください（図 23-3 を参照）。

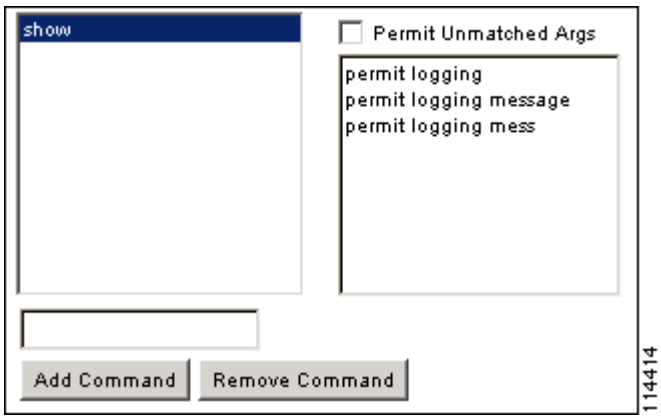
図 23-3　引数の拒否



- コマンドラインでコマンドを省略形で入力した場合、FWSM はプレフィクスとメイン 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、FWSM 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、FWSM 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 23-4 を参照）。

図 23-4　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+ コマンド認可のイネーブル化

TACACS+ コマンド許可をイネーブルにするには、設定者が TACACS+ サーバ上に定義されているユーザとして FWSM にログインし、FWSM の設定を行うために必要なコマンド許可を得ている必要があります。たとえば、すべてのコマンドが認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 FWSM 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）。FWSM 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（「ローカル データベースの設定」（P.11-7）を参照）とコマンド特権レベル（「ローカル コマンド認可の設定」（P.23-16）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認可のイネーブル化」（P.23-17）を参照）、最低のイネーブル レベルを指定することにより、FWSM 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、FWSM 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、FWSM 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.11-9）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
```

次に、**show curpriv** コマンドの出力例を示します。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 23-1 に、**show curpriv** コマンドの出力の説明を示します。

表 23-1　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 コマンド認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

一部の状況では、コマンド許可または CLI 認証をイネーブルにすると、FWSM の CLI からロックアウトされることがあります。通常は、FWSM 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 23-2 に、一般的なロックアウト条件と回復方法を示します。

表 23-2　CLI 認証およびコマンド認可のロックアウト 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 FWSM へのセッションを開始します。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+ コマンドの認可 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. FWSM 上のネットワーク設定が不正であるためにサーバに到達できない場合には、スイッチから FWSM へのセッションを開始します。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 23-2　CLI 認証およびコマンド認可のロックアウト 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+ コマンドの認可	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。	コマンド認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、FWSM 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 FWSM へのセッションを開始します。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認可をディセーブルにすることもできます。
ローカル コマンド認可	十分な特権のないユーザとしてログインしている。	コマンド認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 FWSM へのセッションを開始します。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。