CHAPTER 21

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を説明します。ユーザ認証および許可の方法についても説明します。

この章で説明する内容は次のとおりです。

（注） 管理アクセスのために FWSM インターフェイスにアクセスするには、ホスト IP アドレスを許可するためのアクセス リストは不要です。この章の説明にしたがって、管理アクセスを設定してください。

Telnet アクセスの許可

FWSM では、管理を目的とした FWSM への Telnet 接続を設定できます。IPSec トンネル内部で Telnet を使用する場合を除き、セキュリティが最低のインターフェイスでは Telnet を使用できません。

FWSM では、各コンテキストについて最大 5 つの同時 Telnet 接続を実行でき、全コンテキスト間で最大 100 の接続が可能です。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.4-16] を参照）。

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　各アドレスまたはサブネットについて次のコマンドを入力して、FWSM で接続を許可する IP アドレスを指定します。

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

インターフェイスが 1 つだけの場合、インターフェイスのセキュリティ レベルが 100 であれば、そのインターフェイスへのアクセスに Telnet を設定することができます。

ステップ 2　（任意）FWSM によってセッションが切断されるまでの、Telnet セッションのアイドル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
```

タイムアウトの設定範囲は、1 ～ 1440 分です。デフォルトは 5 分です。ほとんどの場合、デフォルトのタイムアウト値は短すぎるので、すべての事前テストおよびトラブルシューティングが完了するまでは、タイムアウト値を増やしてください。

次に、アドレス 192.168.1.2 の内部インターフェイス上のホストに FWSM へのアクセスを許可する例を示します。

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

次に、192.168.3.0 ネットワーク上のすべてのユーザに、内部インターフェイス上の FWSM へのアクセスを許可する例を示します。

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

SSH アクセスの許可

FWSM では、管理を目的とした FWSM への SSH（セキュア シェル）接続を設定できます。FWSM では、コンテキストごとに最大 5 つの同時 SSH 接続を実行でき、全コンテキスト間で最大 100 の接続が可能です。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.4-16] を参照）。

SSH は、TCP/IP などのトランスポート レイヤの上位で動作し、強力な認証および暗号化機能を提供するアプリケーションです。FWSM は SSH Version 1 および 2 で提供される SSH リモート シェル機能をサポートし、DES および 3DES 暗号をサポートします。

（注）　SSL および SSH 上での XML 管理はサポートされません。

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

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　次のコマンドを入力して、SSH に必要な RSA キー ペアを生成します。

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

モジュール（ビット単位）は 512、768、1024、または 2048 です。指定するキー モジュールのサイズが大きいほど、RSA 生成に時間がかかります。推奨する値は 1024 です。

ステップ 2　次のコマンドを入力して、RSA キーを固定フラッシュ メモリに保存します。

```
hostname(config)# write memory
```

ステップ 3　各アドレスまたはサブネットについて次のコマンドを入力して、FWSM で接続を許可する IP アドレスを指定します。

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

FWSM は、セキュリティ レベルが最低のものを含め、すべてのインターフェイスからの SSH 接続を受け入れます。

ステップ 4　（任意）FWSM によってセッションが切断されるまでの、SSH セッションのアイドル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
```

タイムアウトの設定範囲は、1 ～ 60 分です。デフォルトは 5 分です。ほとんどの場合、デフォルトのタイムアウト値は短すぎるので、すべての事前テストおよびトラブルシューティングが完了するまでは、タイムアウト値を増やしてください。

ステップ 5　（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)
```

次に、RSA キーを生成し、アドレス 192.168.1.2 の内部インターフェイス上のホストに FWSM へのアクセスを許可する例を示します。

```
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
```

次に、192.168.3.0 ネットワーク上のすべてのユーザに、内部インターフェイス上の FWSM へのアクセスを許可する例を示します。

```
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.7-2] を参照）。デフォルトのパスワードは「cisco」です。

SSH セッションが開始すると、FWSM のコンソールにドット（.）が表示され、続いて次のような SSH ユーザ認証プロンプトが表示されます。

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

ドット表示は、SSH の機能には影響を与えません。コンソールのドット表示は、ユーザ認証を実行する前に、サーバ キーを生成しているか、または SSH キー交換中にプライベート キーを使用してメッセージを復号化していることを示しています。これらの処理には 2 分以上かかることがあります。ドットは、FWSM が稼働していて、処理実行中であることを示す進行状況インジケータです。

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て、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.4-16] 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　各アドレスまたはサブネットについて次のコマンドを入力して、FWSM で HTTPS 接続を許可する IP アドレスを指定します。

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

ステップ 2　次のコマンドを入力して、HTTPS サーバをイネーブルにします。

```
hostname(config)# http server enable
```

次に、HTTPS サーバをイネーブルに設定し、アドレス 192.168.1.2 の内部インターフェイス上のホストに ASDM へのアクセスを許可する例を示します。

```
hostname(config)# http server enable
hostname(config)# http 192.168.1.2 255.255.255.255 inside
```

次に、192.168.3.0 ネットワーク上の全ユーザに、内部インターフェイス上の ASDM へのアクセスを許可する例を示します。

```
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働するホスト、あるいは Easy VPN クライアントを稼働する 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ないため、クライアント認証に依存することになります。透過ファイアウォール 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。透過モードでは、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.4-16] を参照）。

ここでは、次の内容について説明します。

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、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 キーワードのほうが、**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 1024 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 キーワードのほうが、**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 認証方式を共有鍵として設定します。

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

rsa-sig オプションを指定すると、共有鍵の代わりに証明書を使用できます。この方法の詳細については『*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}
```

認証のみ、または暗号化のみを指定することもできますが、これらの方法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（**isakmp policy** 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、（安全性の高いほうから順に）次のとおりです。

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

暗号化オプションは、（安全性の高いほうから順に）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。Cisco VPN クライアント Version 4.0 では、リモート アクセス VPN トンネルのエンド ポイントとして設定されたファイアウォール インターフェイスへの Telnet または SSH は許可されていません。

透過ファイアウォール 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。透過モードでは、サイトツーサイトのトンネルがサポートされています。

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.21-6] 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 セットを使用する場合は、プライオリティの順序（最高のプライオリティが最初）で指定します。

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.10-7）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、VPN グループに VPN アドレス プールを割り当てます。

```
hostname(config)# vpngroup group_name 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 VPN グループ名と、ステップ 8 で指定する VPN グループ 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)# vpngroup group_name split-tunnel acl_name
```

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)# vpngroup group_name password password
```

ステップ 9　「Telnet アクセスの許可」（p.21-2）および「SSH アクセスの許可」（p.21-3）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 VPN 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 client_pool 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)# vpngroup admin address-pool client_pool
hostname(config)# vpngroup admin split-tunnel VPN_SPLIT
hostname(config)# vpngroup admin 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鍵を設定します。

```
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.10-7）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
```

トンネルのアトリビュートはすべて、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.21-6] 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 セットを使用する場合は、プライオリティの順序（最高のプライオリティが最初）で指定します。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ができる **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には、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.21-2）および「SSH アクセスの許可」（p.21-3）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

デフォルトの場合、FWSM のインターフェイス（または FWSM を経由。FWSM を*経由*する ICMP の許可については、第 11 章「ネットワーク アクセスの許可または拒否」を参照）上では、ICMP（ping を含む）は許可されていません。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限って許可し、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。番号または名前で指定できます。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 のタイプ」（p.D-17）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 20 章「アプリケーション レイヤ プロトコル検査の適用」を参照してください。

次に、10.1.1.15 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 の使用を許可する例を示します。

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

次に、10.1.1.15 のホストに、内部インターフェイスへの ping だけを許可する例を示します。

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

システム管理者用の AAA

ここでは、システム管理者が認証、コマンド許可、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。システム管理者用の AAA を設定する前に、第 14 章「AAA サーバとローカル データベースの設定」にしたがってローカル データベースまたは AAA サーバを設定してください。

ここでは、次の内容について説明します。

CLI アクセスの認証の設定

CLI 認証をイネーブルにすると、FWSM により、ログイン用のユーザ名とパスワードの入力が要求されます。これらの情報を入力すると、ユーザ EXEC モードにアクセスできます。

イネーブル EXEC モードを開始するには、**enable** コマンドまたは **login** コマンド（ローカル データベースだけを使用する場合）を入力します。

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.21-14] 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。イネーブル認証を設定していない場合は、**enable** コマンドの入力時に（**enable password** コマンドで設定した）システム イネーブル パスワードを入力します。ただし、イネーブル認証を使用しない場合は、**enable** コマンドを入力しても、特定ユーザとしてログインできません。個人ユーザ名を保持するには、イネーブル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では、**login** コマンドを使用できます。この場合、ユーザ名が保持されますが、認証を有効にするための設定は不要です。

（注）　FWSM で Telnet、SSH、または HTTP ユーザを認証する前に、**telnet** コマンド、**ssh** コマンド、および **http** コマンドを使用して FWSM へのアクセスを設定しておく必要があります。これらのコマンドを使用して、FWSM と通信するための 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 キーワードを指定すると、HTTPS を使用して FWSM にアクセスする ASDM クライアントが認証されます。RADIUS または TACACS+ サーバを使用するには、HTTP 認証を設定します。デフォルトでは、このコマンドを設定しなくても、ASDM は認証にローカル データベースを使用します。

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。**LOCAL**（**LOCAL** はすべて大文字）のあとに、サーバ グループ名を指定してください。FWSM のプロンプトでは使用中の方法を判別できないので、ローカル データベースには 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。

LOCAL だけを入力して、ローカル データベースをメインの認証方法（フォールバックなし）として設定することもできます。

イネーブル EXEC モード アクセス認証の設定

enable コマンドの入力時に、AAA サーバまたはローカル データベースを使用してユーザ認証を行うように FWSM を設定できます。または、**login** コマンドの入力時にローカル データベースを使用してユーザを自動的に認証します。この場合、イネーブル EXEC モードへのアクセスは、ローカル データベース内のユーザ レベルに応じて許可されます。

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.21-14）
- login コマンドを使用したユーザ認証（p.21-14）

enable コマンドの認証の設定

enable コマンドの入力時に、ユーザ認証を行うように 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）システム 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、ユーザ名は保持されます。この機能は、コマンド許可を実行する場合に役立ちます。各ユーザが入力できるコマンドを制御するには、ユーザ名が重要になるからです。

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]}
```

ユーザは、ユーザ名とパスワードの入力を要求されます。

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。**LOCAL**（**LOCAL** はすべて大文字）のあとに、サーバ グループ名を指定してください。FWSM のプロンプトでは使用中の方法を判別できないので、ローカル データベースには 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。

LOCAL だけを入力して、ローカル データベースをメインの認証方法（フォールバックなし）として設定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 モードで **login** コマンドを使用すると、ローカル データベース内の任意のユーザ名でログインできます。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。

この方法では、ユーザは独自のユーザ名とパスワードを使用してイネーブル 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がありません。ログイン時にユーザにイネーブル EXEC モード（およびすべてのコマンド）へのアクセスを許可するには、ユーザのイネーブル レベルを 2（デフォルト値）～ 15 に設定します。ローカル コマンド許可を設定すると、ユーザが入力できるコマンドは、そのユーザのイネーブル レベル以下のコマンドだけに限定されます。詳細については、「ローカル コマンド許可の設定」（p.21-16）を参照してください。

注意　CLI へのアクセスを許可し、イネーブル EXEC モードの使用を許可したくないユーザをローカル データベースに追加する場合には、コマンド許可を設定する必要があります。コマンド許可を使用しない場合、イネーブル レベルが 2 以上（2 はデフォルト値）のユーザは、個人のパスワードを使用して CLI のイネーブル EXEC モード（およびすべてのコマンド）にアクセスできます。別の方法として、RADIUS または TACACS+ 認証を使用できます。または、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イネーブル EXEC モードにアクセスできるユーザを制御することもできます。

ローカル データベースの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、個人のユーザ名とパスワードの入力が要求されます。パスワードを入力すると、ユーザはローカル データベースに指定されているイネーブル レベルになります。

コマンド許可の設定

デフォルトでは、ログイン時にアクセスできるのは最小限のコマンドだけを使用できるユーザ EXEC モードです。**enable** コマンド（またはローカル データベースを使用する場合は **login** コマンド）を入力すると、イネーブル EXEC モードにアクセスでき、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を使用できます。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（p.21-15）
- ローカル コマンド許可の設定（p.21-16）
- TACACS+ コマンド許可の設定（p.21-20）

コマンド許可の概要

2 つのコマンド許可方法のいずれかを使用することができます。

- 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 コマンド許可は、ローカル データベースにユーザを設定しない場合、および CLI 認証またはイネーブル認証を設定しない場合にも使用できます。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。各レベルで、イネーブル パスワードを作成できます。**enable** *n*（2 ～ 15）と入力すると、FWSM によってレベルが *n* に設定されます。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限り、使用されます（「ローカル コマンド許可の設定」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。ユーザが CLI から入力したコマンドはすべて、TACACS+ サーバによって検証されます。

セキュリティ コンテキストとコマンド許可

複数のセキュリティ コンテキストでコマンド許可を実装する際、次の点を考慮する必要があります。

- AAA 設定はコンテキスト間で共有するのではなく、コンテキストごとの個別設定となります。

  コマンド許可の設定時に、各セキュリティ コンテキストを個別に設定する必要があります。これにより、セキュリティ コンテキストごとに異なるコマンド許可を実行できるようになります。

  セキュリティ コンテキストの切り替えの際、ログイン時に指定されたユーザ名に許可されるコマンドが、新しいコンテキスト セッションへのログイン時には異なる場合があり、新しいコンテキストではそのコマンド許可がまったく設定されていない場合があることを管理者は理解していてください。コマンド許可がセキュリティ コンテキストによって異なることを理解していないと、混乱を招くもととなります。この動作は、次の点によってより複雑になります。

- **changeto** コマンドで開始される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ていたユーザ名とは関係なく、管理者 ID として常にデフォルト ユーザ名「enable_15」を使用します。enable_15 ユーザに対して共通の許可が設定されていない場合や、この enable_15 ユーザの許可と前のコンテキスト セッションのユーザでの許可とが異なる場合、混乱を生じることがあります。

  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、特定の管理者が発行した各コマンドを正確に対応付けられる場合のみ有効に使用できます。**changeto** コマンドの使用を許可された管理者は他のコンテキストでユーザ名 enable_15 を使用することができるため、コマンド アカウンティング記録を見ても、誰がユーザ名 enable_15 でログインしたのかを容易に特定できないことがあります。コンテキストごとに異なるアカウンティング サーバを使用している場合、ユーザ名 enable_15 の使用者を追跡するには、複数のサーバのデータを照らし合わせる必要があります。

  コマンド許可の設定時には、次の点を考慮してください。

  - **changeto** コマンドの効果的な使用を許可された管理者は、他の各コンテキストでもユーザ enable_15 に許可されたコマンドをすべて使用することができます。
  - コンテキストごとに異なるコマンドを許可する場合、**changeto** コマンドの使用を許可された管理者が使用できないコマンドは、ユーザ名 enable_15 も各コンテキストでこれらのコマンドを使用できないようにします。

  セキュリティ コンテキストを切り替えるとき、管理者はイネーブル EXEC モードを終了して **enable** コマンドを再度入力することにより、必要なユーザ名を使用できるようになります。

（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ていないため、システム実行スペースではコマンド許可は利用できません。

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。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、各コマンドはイネーブル レベル 0 または 15 のどちらか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。

ローカル コマンド許可の前提条件

コマンド許可の設定の一部として、次の作業を完了してください。

- **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.21-14）を参照）。

  login コマンド（認証した **enable** コマンドと同等）を使用する場合には、設定は不要です。ただし、イネーブル認証に比べて安全性が低いので、この方法は推奨しません。

  CLI 認証の設定もできますが、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 イネーブル レベル

デフォルトでは、次のコマンドにイネーブル レベル 0 が割り当てられます。他のコマンドはすべて、イネーブル レベル 15 になります。

- **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 コマンドのいずれかを 15 より低いレベルに変更する場合は、必ず、**configure** コマンドを同じレベルに変更してください。変更しない場合、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。

すべてのイネーブル レベルを表示する手順は、「コマンド イネーブル レベルの表示」（p.21-19）を参照してください。

コマンド イネーブル レベルの指定および許可のイネーブル化

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
```

レベルを変更するコマンドごとに、このコマンドを繰り返します。

このコマンドのオプションの詳細は、次のとおりです。

- **show** | **clear** | **cmd** — コマンドの show、clear、または configure 形式のレベルだけを指定できる任意のキーワードです。コマンドの configure 形式は通常、コマンドの原型（**show** または **clear** のプレフィクスが付いていない状態）または **no** 形式のいずれかで、設定の変更を伴います。これらのキーワードをいずれも使用しない場合、コマンドのすべての形式が対象になります。
- **level** *level* — 0 ～ 15 のレベルを指定します。

- **mode**{**enable** | **configure**} **—** コマンドをユーザ EXEC/ イネーブル EXEC モードとコンフィギュレーション モードの両方で入力できるが、モードによってコマンドの動作が異なる場合は、モードごとにイネーブル レベルを個別に設定できます。
  - **enable —** ユーザ EXEC モードとイネーブル EXEC モードの両方が対象です。
  - **configure — configure terminal** コマンドを使用してアクセスするコンフィギュレーション モードが対象です。
- **command** *command* **—** 設定するコマンドを指定します。*メイン* コマンドのイネーブル レベルだけを設定できます。たとえば、すべての **aaa** コマンドが対象となるレベルは設定できますが、**aaa authentication** コマンドおよび **aaa authorization** コマンドのレベルを個別に設定することはできません。

  また、メイン コマンドとは別にサブ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** コマンドのレベルは設定できますが、**context** コマンドの設定を継承する **allocate-interface** コマンドのレベルは設定できません。

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。

次に、**filter** コマンドの形式を示します。

- **filter**（**configure** オプションの対象）
- **show running-config filter**
- **clear configure filter**

各形式に個別のイネーブル レベルを設定するか、オプションを指定しないで全形式に同じイネーブル レベルを設定します。次に、各形式を個別に設定する例を示します。

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

次に、すべての filter コマンドに同じレベルを設定する例を示します。

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

show privilege コマンドを入力すると、各形式の設定が個別に表示されます。

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 モードで入力する必要がありますが、**enable password** コマンドはコンフィギュレーション モードで入力するので、最上位のイネーブル レベルが必要になります。

```
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** コマンドのレベル設定です。

コマンド イネーブル 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+ コマンド許可をイネーブルにすると、ユーザが CLI にコマンドを入力した時点で FWSM から TACACS+ サーバにコマンドとユーザ名が送信され、そのコマンドが許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許可を設定する場合は、設定が正しいことを確認するまで設定を保存しないでください。設定ミスによって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。再起動しても、ロックアウトされる場合には、「ロックアウトからの回復」（p.21-25）を参照してください。

TACACS+ システムが確実に安定し、信頼性があることを確認してください。必要レベルの信頼性を確保するには通常、完全冗長設定の TACACS+ サーバと、FWSM への完全冗長接続が必要になります。たとえば、TACACS+ サーバ プールに、インターフェイス 1 に接続したサーバと、インターフェイス 2 に接続した別のサーバを設定します。TACACS+ サーバが使用できない場合に備えて、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、ローカル ユーザおよびコマンド イネーブル レベルを設定する必要があります（「コマンド許可の設定」[p.21-15] を参照）。

ここでは、次の内容について説明します。

TACACS+ コマンド許可の前提条件

コマンド許可の設定の一部として、次の作業を完了してください。

- CLI 認証を設定します（「ローカル コマンド許可の設定」[p.21-16] を参照）。
- **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.21-14] を参照）。

TACACS+ サーバ上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。サードパーティ製の 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サーバのマニュアルを参照してください。

Cisco Secure ACS V.3.1 でコマンドを設定する場合は、次の注意事項を参照してください。これらの事項のほとんどは、サードパーティ製のサーバにも適用されます。

- FWSM は、許可するコマンドを「shell」コマンドとして送信するので、TACACS+ サーバ上でコマンドを設定する場合には shell コマンドとして設定してください。

（注）　CiscoSecure ACS には、「pix-shell」と呼ばれるコマンド タイプが含まれていることがあります。FWSM でのコマンド許可には、このタイプを使用しないでください。

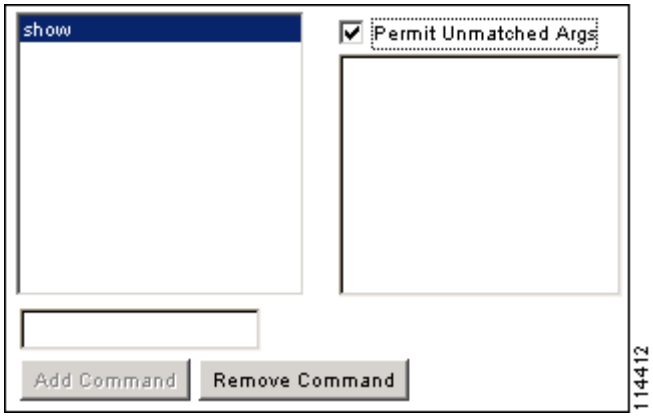
- コマンドの最初の語が、メイン コマンドであると判断されます。その他の文字はすべて引数としてみなされるので、**permit** または **deny** のプレフィクスが必要です。

  たとえば、**show running-configuration aaa-server** コマンドを許可するには、コマンド ボックスに **show running-configuration** を追加し、引数ボックスに **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。

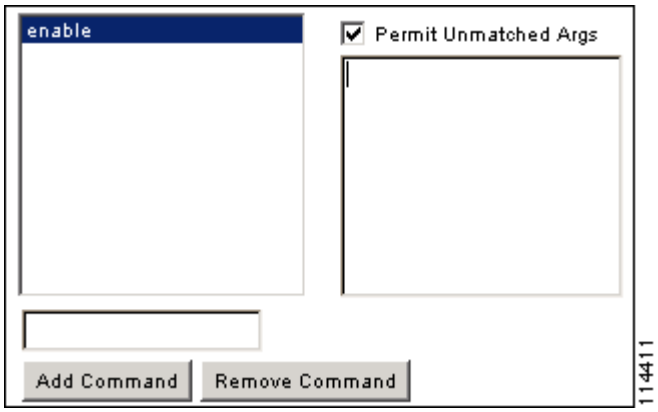
  たとえば、**show** コマンドだけを設定すると、すべての **show** コマンドが許可されます。コマンドのすべての変形（短縮形および CLI の使用方法を示す **?** など）を考慮する必要がないので、この方法を使用することを推奨します（図 21-1 を参照）。

図 21-1　すべての関連コマンドの許可



- **enable** または **help** のように単一語のコマンドの場合には、コマンドの引数がなくても、「Permit Unmatched Args」を選択する*必要があります*（図 21-2 を参照）。

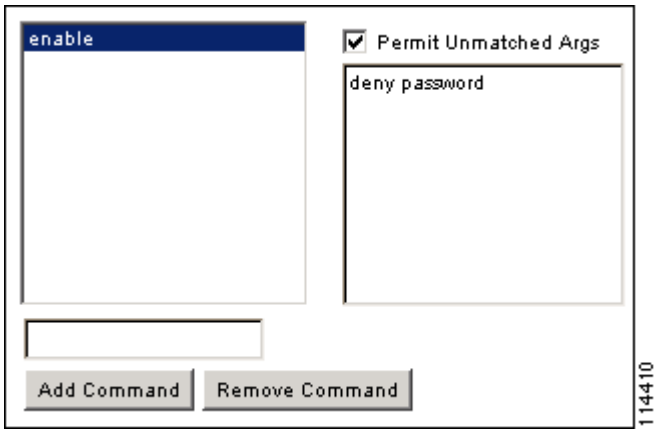
図 21-2　単一ワードのコマンドの許可



- 一部の引数を許可しない場合には、**deny** のプレフィクスを付けて引数を入力します。

  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 ボックスに **enable** を入力し、引数ボックスに **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 21-3 を参照）。

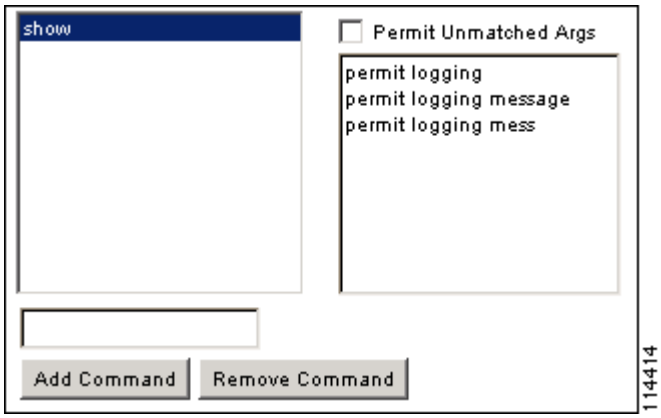
図 21-3　引数の拒否



- コマンドラインにコマンドの短縮形を入力すると、FWSM はプレフィクスとメイン コマンドをフル テキストに拡張しますが、追加の引数は入力されたとおりに TACACS+ サーバに送信されます。

  たとえば、**sh log** と入力すると、FWSM から TACACS+ サーバにコマンドの完全形である **show logging** が送信されます。ただし、**sh log mess** と入力した場合には、FWSM から TACACS+ サーバに **show logging mess** が送信され、完全形の **show logging message** は送信されません。短縮形を識別できるように、同じ引数について複数のスペルを設定できます（図 21-4 を参照）。

図 21-4　短縮形の指定



- 次の基本コマンドは、すべてのユーザに対して許可することを推奨します。
  - **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許可されている admin ユーザとしてログインします。そうでない場合、意図せずにロックアウトされることがあります。

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+ サーバが使用できない場合、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。フォールバックをイネーブルにするには、**LOCAL**（**LOCAL** はすべて大文字）のあとに、サーバ グループ名を指定します。FWSM のプロンプトでは使用中の方法を判別できないので、ローカル データベースには 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。ユーザがローカル データベースに設定され（「コマンド許可の設定」[p.21-15] を参照）、コマンド イネーブル レベルが設定されていることを確認してください（「ローカル コマンド許可の設定」[p.21-16] を参照）。

コマンド アカウンティングの設定

管理セッション中にシステム管理者が発行したコマンドのアカウンティング　レコードが TACACS+ サーバに送信されるように FWSM を設定することができます。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。最低のイネーブル レベル未満のコマンドは FWSM 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、次のように **aaa accounting command** コマンドを使用します。

```
hostname(config)# aaa accounting command [privilege level] server-tag
```

level は最低のイネーブル レベル、*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先の 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.14-13）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は、以下を参照してください。

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

表 21-1 に、**show curpriv** コマンドの出力の説明を示します。

表 21-1　show curpriv の出力の説明

フィールド	説明
Username	ユーザ名です。デフォルト ユーザとしてログインしている場合、名前は enable_1（ユーザ EXEC）または enable_15（イネーブル EXEC）になります。
Current privilege level	0 ～ 15 のレベルです。ローカル コマンド許可を設定し、コマンドに中間のイネーブル レベルを割り当てた場合をのぞき、使用できるレベルはレベル 0 およびレベル 15 だけです。
Current Mode/s	アクセス モードが表示されます。 • P_UNPR — ユーザ EXEC モード（レベル 0 および 1） • P_PRIV — イネーブル 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回復できます。ただし、設定がすでに保存されている場合には、再びロックアウトされる可能性があります。表 21-2 に、一般的なロックアウトの条件および回復方法を示します。

表 21-2　CLI 認証およびコマンド許可のロックアウト

機能	ロックアウトの条件	説明	対処方法：シングル モード	対処方法：マルチ モード
ローカル CLI 認証	ローカル データベースにユーザが設定されていない。	ローカル データベースにユーザが設定されていない場合、ログインできず、ユーザを追加できません。	ログインし、パスワードと **aaa** コマンドを再設定します。	スイッチから FWSM に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移動し、ユーザを追加します。
TACACS+ コマンド許可 TACACS+ CLI 認証 RADIUS CLI 認証	サーバがダウンしたか、または到達不能で、かつフォールバック方式が設定されていない。	サーバが到達不能な場合、ログインまたはコマンド入力ができません。	1. ログインし、パスワードと aaa コマンドを再設定します。 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、フォールバック方式としてローカル データベースを設定します。	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 に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移動し、ネットワークを再設定します。 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、フォールバック方式としてローカル データベースを設定します。
TACACS+ コマンド許可	十分なレベルを持たないユーザとして、または存在しないユーザとしてログインした場合	コマンド許可をイネーブルにすると、ユーザはそれ以上、コマンドを入力できません。	TACACS+ サーバのユーザアカウントを修正します。 TACACS+ サーバにアクセスできず、FWSM をただち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、パスワードおよび **aaa** コマンドを再設定します。	スイッチから FWSM に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移動し、設定の変更を完了します。TACACS+ の設定を修正するまで、コマンド許可をディセーブルにしておくこともできます。
ローカル コマンド許可	十分なレベルを持たないユーザとしてログインした場合	コマンド許可をイネーブルにすると、ユーザはそれ以上、コマンドを入力できません。	ログインし、パスワードと **aaa** コマンドを再設定します。	スイッチから FWSM に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移動し、ユーザ レベルを変更します。