CHAPTER 13

管理アクセスの設定

この章では、次の項目について説明します。

HTTPS/ASDM

HTTPS/ASDM ペインには、HTTPS を使用した ASDM へのアクセスを許可するすべてのホストまたはネットワークのアドレスを指定するテーブルが用意されています。このテーブルを使用して、アクセスを許可するホストやネットワークを追加または変更できます。

フィールド

- Interface：デバイス マネージャへの管理アクセスを許可するアクセス元のセキュリティ アプライアンス上のインターフェイスを一覧表示します。
- IP Address：アクセスを許可するネットワークまたはホストの IP アドレスを一覧表示します。
- Mask：アクセスを許可するネットワークまたはホストに関連付けられたネットワーク　マスクを一覧表示します。
- Add：新しいホストまたはネットワークを追加するための Add HTTP Configuration ダイアログボックスを表示します。
- Edit：選択したホストまたはネットワークを編集するための Edit HTTP Configuration ダイアログボックスを表示します。
- Delete：選択したホストまたはネットワークを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit HTTP Configuration

Add/Edit HTTP Configuration ダイアログボックスでは、HTTPS でのセキュリティ アプライアンス デバイス マネージャへの管理アクセスが許可されるホストまたはネットワークを追加できます。

フィールド

- Interface Name：セキュリティ アプライアンス デバイス マネージャへの管理アクセスを許可するアクセス元のセキュリティ アプライアンス上のインターフェイスを指定します。
- IP Address：アクセスを許可するネットワークまたはホストの IP アドレスを指定します。
- Mask：アクセスを許可するネットワークまたはホストに関連付けられたネットワーク　マスクを指定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

コマンドライン

この項では、コマンドライン インターフェイス機能について説明します。次の項目を取り上げます。

Banner

Banner ペインでは、当日のお知らせメッセージ、ログイン、セッション バナーを設定できます。

バナーを作成するには、該当するボックスにテキストを入力します。テキストに入力したスペースはそのまま表示されます。タブは ASDM インターフェイスで入力します。コマンドライン インターフェイスからは入力できません。トークンの $(domain) および $(hostname) は、セキュリティ アプライアンスのドメイン名およびホスト名に置き換えられます。

$(hostname) および $(domain) トークンを使用すると、特定のコンテキストで指定したホスト名とドメイン名を画面に表示できます。$(system) トークンを使用して、特定のコンテキストのシステム スペースで設定したバナーを画面に表示できます。

バナーが複数行の場合、行ごとに入力したテキストが既存のバナーの最後に追加されます。テキストが空の場合、復帰記号（CR）がバナーに追加されます。RAM やフラッシュ メモリの容量が許す限り、バナーの長さに制限はありません。ASCII 文字のみ使用できます。改行（Enter キー。2 文字に相当）も使用できます。

Telnet または SSH でセキュリティ アプライアンスにアクセスしたとき、システム メモリが不足してバナー メッセージを表示できなかったり、バナー メッセージを表示するときに TCP 書き込みエラーが発生したりするとセッションは終了します。

バナーを置き換えるには、該当するボックスの内容を変更して **Apply** をクリックします。バナーをクリアするには、該当するボックスの内容をクリアして **Apply** をクリックします。

システム コンテキストでは ASDM のペインからバナー コマンドを使用できませんが、Tools > Command Line Interface から設定できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

CLI Prompt

CLI Prompt ペインでは、CLI セッションで使用するプロンプトをカスタマイズできます。デフォルトでは、プロンプトにはセキュリティ アプライアンスのホスト名が表示されます。マルチコンテキスト モードでは、プロンプトにはコンテキスト名も表示されます。CLI プロンプトには次の項目を表示できます。

context	（マルチモードのみ）現在のコンテキストの名前を表示します。
domain	ドメイン名を表示します。
hostname	ホスト名を表示します。
priority	フェールオーバーの優先順位を pri（プライマリ）または sec（セカンダリ）として表示します。
state	装置のトラフィック通過状態を表示します。状態として次の値が表示されます。 • act：フェールオーバーはイネーブルになっており、装置はアクティブでトラフィックが装置を通過しています。 • stby：フェールオーバーはイネーブルになっており、装置はスタンバイ、障害発生、またはその他の非アクティブ状態で、トラフィックは装置を通過していません。 • actNoFailover：フェールオーバーがイネーブルではなく、装置はアクティブでトラフィックが装置を通過しています。 • stbyNoFailover：フェールオーバーがイネーブルではなく、トラフィックは装置を通過していません。この状態は、スタンバイ装置のしきい値より上でインターフェイスの障害が発生した場合に起こることがあります。

CLI プロンプトを設定するには、次の手順を実行します。

ステップ 1　プロンプトにアトリビュートを追加するには、Available Prompts リストでアトリビュートをクリックしてから **Add** をクリックします。プロンプトには複数のアトリビュートを追加できます。アトリビュートが Available Prompts リストから Selected Prompts リストに移動します。

ステップ 2　プロンプトからアトリビュートを削除するには、Selected Prompts リストでアトリビュートをクリックしてから **Delete** をクリックします。アトリビュートが Selected Prompts リストから Available Prompts リストに移動します。

ステップ 3　コマンド プロンプトにアトリビュートが表示される順序を変更するには、Selected Prompts リストでアトリビュートをクリックし、**Move Up** または **Move Down** をクリックして順序を変更します。

ペインの下部にある CLI Prompt Preview フィールドでコマンド プロンプトのプレビューを確認できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

Console Timeout

Console Timeout ペインでは、管理コンソールの表示時間（分単位）を指定できます。ここで指定した時間が経過すると、コンソールは自動的にシャットダウンします。

Console Timeout フィールドに時間を入力します。制限しない場合は 0 を入力します。デフォルト値は 0 です。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

Secure Shell

Secure Shell ペインでは、特定のホストまたはネットワークだけが SSH プロトコルを使用して、管理アクセスのためにセキュリティ アプライアンスへ接続することを許可するルールを設定できます。ルールでは、特定の IP アドレスおよびネットマスクへの SSH アクセスが制限されます。ルールに準拠した SSH 接続試行は、次に AAA サーバまたは Telnet パスワードによって認証される必要があります。

SSH セッションは、Monitoring > Administration > Secure Shell Sessions を使用して監視できます。

フィールド

Secure Shell ペインでは、次のフィールドが表示されます。

- Allowed SSH Versions：セキュリティ アプライアンスが受け入れる SSH のバージョンを制限します。デフォルトでは、SSH バージョン 1 および SSH バージョン 2 接続が受け入れられます。
- Timeout (minutes)：セキュリティ アプライアンスが SSH セッションを閉じる前にアイドルでいられる分数を 1 ～ 60 で表示します。デフォルトは 5 分です。
- SSH Access Rule：SSH を使用したセキュリティ アプライアンスへのアクセスが許可されるホストおよびネットワークを表示します。このテーブルの行をダブルクリックすると、選択したエントリを対象とした Edit SSH Configuration ダイアログボックスが開きます。
  - Interface：SSH 接続を許可するセキュリティ アプライアンスのインターフェイスの名前が表示されます。
  - IP Address：指定したインターフェイスを介してこのセキュリティ アプライアンスへの接続が許可されている各ホストまたはネットワークの IP アドレスを表示します。
  - Mask：指定したインターフェイスを介してこのセキュリティ アプライアンスへの接続が許可されている各ホストまたはネットワークの IP アドレスのネットマスクを表示します。

- Add：Add SSH Configuration ダイアログボックスが開きます。
- Edit：Edit SSH Configuration ダイアログボックスが開きます。
- Delete：選択した SSH アクセス ルールを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit SSH Configuration

Add SSH Configuration ダイアログボックスでは、新しい SSH アクセス ルールをルール テーブルに追加できます。Edit SSH Configuration ダイアログボックスでは、既存のルールを変更できます。

フィールド

- Interface : SSH 接続を許可するセキュリティ アプライアンス インターフェイスの名前を指定します。
- IP Address：セキュリティ アプライアンスとの SSH 接続の確立が許可されるホストまたはネットワークの IP アドレスを指定します。
- Mask：セキュリティ アプライアンスとの SSH 接続の確立が許可されるホストまたはネットワークのネットマスクです。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Telnet

Telnet ペインでは、ASDM を実行している特定のホストまたはネットワークだけが Telnet プロトコルを使用してセキュリティ アプライアンスに接続できるルールを設定します。

ルールでは、セキュリティ アプライアンス インターフェイスを介した特定の IP アドレスおよびネットマスクへの管理 Telnet アクセスが制限されます。ルールに準拠した接続試行は、事前設定された AAA サーバまたは Telnet パスワードによって認証される必要があります。Telnet セッションは、Monitoring > Telnet Sessions を使用して監視できます。

（注） コンフィギュレーション ファイルには 5 つ以上の Telnet セッションが含まれますが、シングルコンテキスト モードで同時にアクティブになれるのは 5 つまでです。マルチコンテキスト モードでは、コンテキストごとに 5 つの Telnet セッションのみアクティブになれます。

フィールド

Telnet ペインには、次のフィールドが表示されます。

Telnet Rule Table：

- Interface：Telnet 接続を許可するセキュリティ アプライアンス インターフェイス（ASDM を実行している PC またはワークステーションがあるインターフェイス）の名前を表示します。
- IP Address：指定したインターフェイスを介してこのセキュリティ アプライアンスへの接続が許可されている各ホストまたはネットワークの IP アドレスを表示します。

（注）　これは、セキュリティ アプライアンス インターフェイスの IP アドレスではありません。

- Netmask：指定したインターフェイスを介してこのセキュリティ アプライアンスへの接続が許可されている各ホストまたはネットワークの IP アドレスのネットマスクを表示します。

（注）　これは、セキュリティ アプライアンス インターフェイスの IP アドレスではありません。

- Timeout：セキュリティ アプライアンスが Telnet セッションを閉じる前にアイドルでいられる分数を 1 ～ 60 で表示します。デフォルトは 5 分です。
- Add：Add Telnet Configuration ダイアログボックスが開きます。
- Edit：Edit Telnet Configuration ダイアログボックスが開きます。
- Delete：選択した項目を削除します。
- Apply：ASDM での変更内容をセキュリティ アプライアンスに送信し、実行中のコンフィギュレーションに適用します。実行中のコンフィギュレーションのコピーをフラッシュ メモリに書き込むには、Save をクリックします。実行中のコンフィギュレーションのコピーをフラッシュ メモリ、TFTP サーバ、またはフェールオーバー スタンバイ装置に書き込むには、***File*** メニューを使用します。
- Reset：変更内容を破棄し、変更前に表示されていた情報、または ***Refresh*** か ***Apply*** を最後にクリックしたときに表示されていた情報に戻します。Reset をクリックした後は、Refresh を使用して、現在実行中のコンフィギュレーションの情報が表示されていることを確認します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Telnet コンフィギュレーションの追加および編集

Telnet ルールの追加

Telnet ルール テーブルにルールを追加するには、次の手順を実行します。

1. **Add** ボタンをクリックし、**Telnet** > **Add** ダイアログボックスを開きます。

2. **Interface** をクリックし、セキュリティ アプライアンス インターフェイスをルール テーブルに追加します。
3. IP Address ボックスに、このセキュリティ アプライアンス インターフェイスを介した Telnet アクセスが許可される、ASDM を実行中のホストの IP アドレスを入力します。

（注）　これは、セキュリティ アプライアンス インターフェイスの IP アドレスではありません。

4. Mask リストで、Telnet アクセスを許可する IP アドレスのネットマスクを選択または入力します。

（注）　これは、セキュリティ アプライアンス インターフェイスの IP アドレスのマスクではありません。

5. 前のペインに戻るには、次のいずれかをクリックします。

- **OK**：変更内容を受け入れて、前のペインに戻ります。
- **Cancel**：変更内容を破棄して、前のペインに戻ります。
- **Help**：詳細情報を表示します。

Telnet ルールの編集

Telnet ルール テーブルのルールを編集するには、次の手順を実行します。

1. **Edit** をクリックし、Telnet > Edit ダイアログボックスを開きます。
2. **Interface** をクリックし、ルール テーブルからセキュリティ アプライアンス インターフェイスを選択します。
3. IP Address フィールドに、このセキュリティ アプライアンス インターフェイスを介した Telnet アクセスが許可される、ASDM を実行中のホストの IP アドレスを入力します。

（注）　これは、セキュリティ アプライアンス インターフェイスの IP アドレスではありません。

4. Mask リストで、Telnet アクセスを許可する IP アドレスのネットマスクを選択または入力します。

（注）　これは、セキュリティ アプライアンス インターフェイスの IP アドレスのマスクではありません。

5. 前のウィンドウに戻るには、次のいずれかのボタンをクリックします。

- **OK**：変更内容を受け入れて、前のペインに戻ります。
- **Cancel**：変更内容を破棄して、前のペインに戻ります。
- **Help**：詳細情報を表示します。

Telnet ルールの削除

Telnet テーブルからルールを削除するには、次の手順を実行します。

1. Telnet ルール テーブルからルールを選択します。
2. **Delete** をクリックします。

変更内容の適用

Add、Edit、または Delete を使用してテーブルを変更した内容は、実行中のコンフィギュレーションにただちに適用されるわけではありません。変更内容を適用または破棄するには、次のいずれかのボタンをクリックします。

1. **Apply**：ASDM での変更内容をセキュリティ アプライアンスに送信し、実行中のコンフィギュレーションに適用します。実行中のコンフィギュレーションのコピーをフラッシュ メモリに書き込むには、**Save** をクリックします。実行中のコンフィギュレーションのコピーをフラッシュ メモリ、TFTP サーバ、またはフェールオーバー スタンバイ装置に書き込むには、**File** メニューを使用します。
2. **Reset**：変更内容を破棄し、変更前に表示されていた情報、または **Refresh** か **Apply** を最後にクリックしたときに表示されていた情報に戻します。Reset をクリックした後は、**Refresh** を使用して、現在実行中のコンフィギュレーションの情報が表示されていることを確認します。

フィールド

- Interface Name：セキュリティ アプライアンスへの Telnet アクセスを許可するインターフェイスを選択します。
- IP Address：セキュリティ アプライアンスへの Telnet が許可されたホストまたはネットワークの IP アドレスを入力します。
- Mask：セキュリティ アプライアンスへの Telnet が許可されたホストまたはネットワークのサブネット マスクを入力します。
- OK：変更内容を受け入れて、前のペインに戻ります。
- Cancel：変更内容を破棄して、前のペインに戻ります。
- Help：詳細情報を表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

ファイル アクセス

この項では、ファイル アクセス機能について説明します。次の項目を取り上げます。

FTP クライアント

FTP Mode ペインでは、FTP モードをアクティブまたはパッシブに設定できます。セキュリティ アプライアンスがイメージ ファイルまたはコンフィギュレーション ファイルを FTP サーバにアップロードしたり、FTP サーバからダウンロードできるようになります。パッシブ FTP クライアントは、コントロール接続とデータ接続を両方とも起動できます。サーバはパッシブ モードでデータ接続の宛先になり、特定の接続の受信時にポート番号に応答します。

フィールド

- Specify FTP mode as passive：FTP モードをアクティブまたはパッシブに設定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

Secure Copy

Secure Copy ペインでは、セキュリティ アプライアンスのセキュア コピー サーバをイネーブルにします。SSH を利用するセキュリティ アプライアンスのアクセスを許可されたクライアントだけが、セキュア コピー接続を確立できます。

制約事項

セキュア コピー サーバの実装には、次の制約事項があります。

- サーバはセキュア コピー接続の受け入れと終了はできますが、起動はできません。
- サーバは、ディレクトリの指定をサポートしていません。そのため、リモート クライアント アクセスでセキュリティ アプライアンスの内部ファイル参照はできません。
- サーバは、バナーをサポートしていません。
- サーバは、ワイルドカードをサポートしていません。
- SSH バージョン 2 で接続するには、セキュリティ アプライアンスのライセンスに VPN-3DES-AES 機能が必要です。

フィールド

- Enable Secure Copy Server：セキュリティ アプライアンスのセキュア コピー サーバをイネーブルにします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

TFTP Client

このペインでは、セキュリティ アプライアンスが TFTP クライアントとして機能するように設定できます。

（注）　このペインでサーバにファイルを書き込むことはありません。このペインでセキュリティ アプライアンスを TFTP クライアントで使用できるように設定してから、***File*** > ***Save Running Configuration to TFTP Server*** をクリックします。

TFTP サーバとセキュリティ アプライアンス

TFTP は RFC783 および RFC1350 Rev. 2 で規定されているシンプルなクライアント / サーバ ファイル転送プロトコルです。このペインでセキュリティ アプライアンスを TFTP *クライアント*として設定すると、実行コンフィギュレーション ファイルのコピーを TFTP *サーバ*に転送できます。転送するには、File > Save Running Configuration to TFTP Client をクリックするか、または Tools > Command Line Interface をクリックします。この方法でコンフィギュレーション ファイルをバックアップし、複数のセキュリティ アプライアンスにプロパゲートできます。

configure net コマンドで TFTP クライアントの IP アドレスを指定し、**tftp-server** コマンドでサーバのインターフェイスとパス / ファイル名を指定すると、そこに実行コンフィギュレーション ファイルが書き込まれます。この情報を実行コンフィギュレーションに適用すると、ASDM で File > Save Running Configuration to TFTP client をクリックすれば、**copy** コマンドで TFTP クライアントにファイル転送できます。

セキュリティ アプライアンスでサポートされる TFTP クライアントは 1 つだけです。TFTP クライアントのフル パスを Configuration > Device Management > Management Access > File Access > TFTP Client で指定します。ここで設定すると、CLI の **configure net** および **copy** コマンドにコロン（:）で IP アドレスを指定できます。ただし、セキュリティ アプライアンスと TFTP クライアントの通信に必要な、中間デバイスの認証または設定は、この機能とは別に実行されます。

show tftp-client コマンドで、現在のコンフィギュレーションに含まれている **tftp-client** コマンド文を一覧表示できます。**no tftp client** コマンドで、クライアントへのアクセスをディセーブルにします。

フィールド

TFTP ペインには次のフィールドがあります。

- Enable：選択すると、コンフィギュレーションに含まれる TFTP クライアントの設定がイネーブルになります。
- Interface Name：セキュリティ アプライアンスのインターフェイス名を選択します。このインターフェイスで TFTP クライアントの設定を使用します。

- IP Address：TFTP サーバの IP アドレスを入力します。
- Path：TFTP クライアントのパスを入力します。先頭にスラッシュ（/）を付け、最後にファイル名を指定します。ここに実行コンフィギュレーションが書き込まれます。

  TFTP クライアントのパスの例：**/tftpboot/security appliance/config3**

（注）　パスの先頭には必ずスラッシュ（/）を付けます。

詳細情報

TFTP の詳細については、使用するソフトウェア バージョンのセキュリティ アプライアンスの技術マニュアルを参照してください。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Mount Points

Mount Points テーブルには、現在ファイル アクセス用に設定されている Common Internet File System（CIFS）および File Transfer Protocol（FTP）のマウント ポイントが表示されます。

マウント ポイントを追加、変更、または削除するには、次のいずれかの操作を実行します。

- マウント ポイントを追加するには、Add > CIFS Mount Point or Add > FTP Mount Point を選択します。パラメータの詳細については、P.13-13 の「Add or Edit FTP Mount Point ダイアログボックスのフィールド」または P.13-13 の「Add or Edit FTP Mount Point ダイアログボックスのフィールド」を参照してください。
- マウント ポイントを変更するには、テーブルでエントリを選択し、**Edit** をクリックします。エントリをダブルクリックしても編集できます。パラメータの詳細については、P.13-13 の「Add or Edit FTP Mount Point ダイアログボックスのフィールド」または P.13-13 の「Add or Edit FTP Mount Point ダイアログボックスのフィールド」を参照してください。
- マウント ポイントを削除するには、削除するエントリを選択し、**Delete** をクリックします。

（注）　Delete ボタンをクリックすると、ダイアログが表示されなくなり、選択したマウント ポイントがただちにテーブルから削除され、指定したファイル システムにアクセスできなくなります。

適用とリセット。フィールドに対する追加や変更はただちに画面に反映されますが、それをコンフィギュレーションに保存するには Apply をクリックする必要があります。

Add or Edit CIFS Mount Point ダイアログボックスのフィールド

Add or Edit CIFS Mount Point ダイアログボックスには次のフィールドがあります。

- Enable mount point：選択したマウント ポイントへのアクセスをイネーブルまたはディセーブルにします。このオプションをオンにすると、セキュリティ アプライアンスの CIFS ファイル システムが UNIX ファイル ツリーにアタッチされます。反対に、オフにするとマウント ポイントがデタッチされます。
- Mount-Point Name：既存のファイル システムの名前を入力するか変更します。
- Server Name or IP Address：CIFS サーバの事前定義済みの名前（またはドット付き 10 進数形式の IP アドレス）を入力します。
- Share Name：CIFS サーバ内のファイル データにアクセスするためのサーバ共有（フォルダ）の名前を入力します。
- NT Domain Name：事前定義済みの Windows NT ドメイン名を入力します。入力できる最大文字数は 63 文字です。
- User Name：ファイル システムのマウントを認可されているユーザ名を入力します。
- Password：ファイル システムをマウントするために認可されているパスワードを入力します。
- Confirm Password：認可されているパスワードを再入力します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add or Edit FTP Mount Point ダイアログボックスのフィールド

Add or Edit FTP Mount Point ダイアログボックスには次のフィールドがあります。

- Enable mount point：選択したマウント ポイントへのアクセスをイネーブルまたはディセーブルにします。このオプションをオンにすると、セキュリティ アプライアンスの FTP ファイル システムが UNIX ファイル ツリーにアタッチされます。反対に、チェックボックスをオフにするとマウント ポイントがデタッチされます。
- Mount-Point Name：既存の FTP ファイル システムの名前を入力するか変更します。
- Server Name or IP Address：FTP ファイル システム サーバの事前定義済みの名前（またはドット付き 10 進数形式の IP アドレス）を入力します。
- Mode：FTP マウント オプションの FTP 転送モードを Passive または Active から選択します。FTP 転送モードの詳細については、「FTP クライアント」を参照してください。
- Path To Mount：FTP ファイル サーバへのディレクトリ パス名を入力します。スペースは使用できません。
- User Name：ファイル システムのマウントを認可されているユーザ名を入力します。
- Password：ファイル システムをマウントするために認可されているパスワードを入力します。
- Confirm Password：認可されているパスワードを再入力します。

（注）　FTP マウント ポイントの場合、FTP サーバには UNIX のディレクトリ リスト スタイルが必要です。Microsoft FTP サーバのデフォルトは、MS-DOS のディレクトリ リスト スタイルです。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

ICMP

ICMP Rules ペインでは、ICMP ルール テーブルを表示し、セキュリティ アプライアンスへの ICMP アクセスを許可または拒否されるホストまたはネットワークすべてのアドレスを指定します。このテーブルでホストまたはネットワークを追加、変更すると、セキュリティ アプライアンスに送信された ICMP メッセージを許可または禁止できます。

ICMP ルールは、セキュリティ アプライアンス インターフェイスに ICMP トラフィックが着信した場合の制御方法を表示します。ICMP コントロール リストが設定されていない場合、セキュリティ アプライアンスは外部インターフェイスも含め、インターフェイスに着信した ICMP トラフィックをすべて許可します。ただし、デフォルトでは、セキュリティ アプライアンスはブロードキャスト アドレスへの ICMP エコー要求に応答しません。

（注）　**Security Policy** ペインで ICMP トラフィックのアクセス ルールを設定すると、宛先のインターフェイスが保護されていてもセキュリティ アプライアンスを*通過*ルートにできます。

ICMP の到達不能メッセージ タイプ（type 3）の権限は、常に許可にすることをお勧めします。ICMP の到達不能メッセージを拒否すると、ICMP の Path MTU Discovery 機能がディセーブルになり、IPSec および PPTP トラフィックが停止する場合があります。Path MTU Discovery の詳細については、RFC 1195 および RFC 1435 を参照してください。

ICMP コントロール リストを設定すると、セキュリティ アプライアンスでは最初に一致した条件を ICMP トラフィックに適用し、暗黙的にすべてを拒否します。したがって、最初に一致したエントリが許可の場合は、ICMP パケットはそのまま処理されます。最初に一致したエントリが拒否の場合または一致しなかった場合は、セキュリティ アプライアンスで ICMP パケットは破棄され、syslog メッセージが出力されます。例外は ICMP コントロール リストが設定されていない場合です。その場合、**許可**が設定されているものとして処理されます。

フィールド

- Interface：ICMP アクセスが許可されるセキュリティ アプライアンスのインターフェイスを一覧表示します。
- Action：指定したネットワークまたはホストの ICMP 受信メッセージの許可/拒否を表示します。
- IP Address：アクセスを許可 / 拒否するネットワークまたはホストの IP アドレスを一覧表示します。
- Mask：アクセスを許可するネットワークまたはホストに関連付けられたネットワーク　マスクを一覧表示します。
- ICMP Type：ルールを適用する ICMP メッセージ タイプを一覧表示します。表 13-1 に示す ICMP タイプの値がサポートされます。
- Add：Add ICMP Rule ダイアログボックスを表示し、そこから新規の ICMP ルールをテーブルの最後に追加できます。
- Insert Before：ICMP ルールを現在選択されているルールの前に追加します。
- Insert After：ICMP ルールを現在選択されているルールの後に追加します。
- Edit：選択したホストまたはネットワークを編集するための Edit ICMP Rule ダイアログボックスを表示します。
- Delete：選択したホストまたはネットワークを削除します。

表 13-1　ICMP タイプ リテラル

ICMP タイプ	リテラル
0	echo-reply
3	unreachable
4	source-quench
5	redirect
6	alternate-address
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded
12	parameter-problem
13	timestamp-request
14	timestamp-reply
15	information-request
16	information-reply
17	mask-request
18	mask-reply
31	conversion-error
32	mobile-redirect

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit ICMP Rule

Add/Edit ICMP Rule ダイアログボックスでは、ICMP ルールの追加または変更ができます。ICMP ルールには、セキュリティ アプライアンスへの ICMP アクセスが許可 / 拒否されるホストまたはネットワークのアドレスをすべて指定します。

フィールド

- ICMP Type：ルールを適用する ICMP メッセージ タイプを指定します。表 13-2 に示す ICMP タイプの値がサポートされます。
- **Interface**：ICMP アクセスが許可されるセキュリティ アプライアンスのインターフェイスを指定します。
- IP Address：アクセスを許可 / 拒否するネットワークまたはホストの IP アドレスを指定します。
- Any Address：指定したインターフェイスのすべての受信アドレスにアクションを適用します。
- Mask：アクセスを許可するネットワークまたはホストに関連付けられたネットワーク　マスクを指定します。

- Action:指定したネットワークまたはホストの ICMP 受信メッセージの許可/拒否を表示します。
  - Permit：指定したホストまたはネットワーク、およびインターフェイスからの ICMP メッセージを許可します。
  - Deny：指定したホストまたはネットワーク、およびインターフェイスからの ICMP メッセージをドロップします。

表 13-2　ICMP タイプ リテラル

ICMP タイプ	リテラル
0	echo-reply
3	unreachable
4	source-quench
5	redirect
6	alternate-address
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded
12	parameter-problem
13	timestamp-request
14	timestamp-reply
15	information-request
16	information-reply
17	mask-request
18	mask-reply
31	conversion-error
32	mobile-redirect

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Management Interface

Management Interface ペインでは、高度なセキュリティ インターフェイスの管理インターフェイスをイネーブルまたはディセーブルにし、セキュリティ アプライアンスの管理機能を実行できます。管理インターフェイスをイネーブルにすると、IPSec VPN トンネルを使用して固定された IP アドレスを持つ内部インターフェイスで ASDM を実行できます。この機能を使用する場合は、VPN をセキュリティ アプライアンスで設定し、外部インターフェイスにダイナミック IP アドレス割り当てを適用します。たとえば、セキュリティ アプライアンスを自宅から VPN クライアントでアクセスするような場合のセキュリティ管理で役立ちます。

フィールド

- Management Interface : セキュリティ アプライアンスの管理に使用するインターフェイスを指定します。None（デフォルト）を指定すると、管理インターフェイスはディセーブルになります。管理インターフェイスをイネーブルにするには、インターフェイスのセキュリティを最も高く設定し、内部インターフェイスにします。一度に 1 つのインターフェイスだけの管理インターフェイスをイネーブルにできます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

SNMP

SNMP ペインでは、セキュリティ アプライアンスを簡易ネットワーク管理プロトコル（SNMP）管理ステーションから監視できるように設定できます。

ネットワーク管理ステーションを PC またはワークステーションで実行し、スイッチ、ルータ、セキュリティ アプライアンスなど、さまざまなタイプのデバイスのステータスとヘルスを監視する標準的な方法を SNMP で定義できます。

SNMP の用語

- Management station：PC またはワークステーションで実行されるネットワーク管理ステーションです。SNMP プロトコルを使用して、管理対象デバイス上の標準データベースを管理します。ハードウェアの障害など注意が必要なイベントのメッセージも受信できます。
- Agent：SNMP コンテキストでは、管理ステーションがクライアント、セキュリティ アプライアンスで動作する SNMP エージェントがサーバになります。
- OID：SNMP 規格では、システム オブジェクト ID（OID）を設定して、管理ステーションが SNMP エージェントがあるネットワーク デバイスを一意に識別したり、ユーザに分かるように監視情報の発生元を表示したりします。
- MIB：エージェントは Management Information Databases（MIB; 管理情報データベース）と呼ばれる標準データ構造を保持します。これが管理ステーションに蓄積されます。MIB は、パケット、接続、エラー カウンタ、バッファの使用状況、フェールオーバー ステータスなどの情報を収集します。MIB は製品ごとに定義され、通常のネットワーク デバイスで使用される一般的なプロトコルとハードウェア規格も MIB に定義されています。SNMP 管理ステーションから MIB を参照したり、特定のフィールドだけを要求したりできます。一部のアプリケーションでは、管理目的で MIB データを変更する場合があります。
- Trap：エージェントはアラーム条件も監視します。リンク アップ、リンク ダウン、syslog イベントなどトラップに定義したアラーム条件が発生すると、エージェントは指定された管理ステーションにただちに通知します。この通知は SNMP トラップとも呼ばれます。

SNMP

シスコの MIB ファイルおよび OID については、http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml を参照してください。OID は、次の URL からダウンロードすることもできます。ftp://ftp.cisco.com/pub/mibs/oid/oid.tar.gz。

MIB のサポート

セキュリティ アプライアンスは、次の SNMP MIB をサポートしています。

（注）　セキュリティ アプライアンスは、Cisco syslog MIB のブラウジングはサポートしません。

- MIB-II の System グループと Interface グループをブラウジングできます。MIB のブラウジングはトラップの送信とは違います。ブラウジングとは、管理ステーションから MIB ツリーの snmpget や snmpwalk を実行し、値を決定することです。
- Cisco MIB および Cisco Memory Pool MIB を使用できます。

セキュリティ アプライアンスは、次の Cisco MIB をサポートしていません。

- cfwSecurityNotification NOTIFICATION-TYPE
- cfwContentInspectNotification NOTIFICATION-TYPE
- cfwConnNotification NOTIFICATION-TYPE
- cfwAccessNotification NOTIFICATION-TYPE
- cfwAuthNotification NOTIFICATION-TYPE

- cfwGenericNotification NOTIFICATION-TYPE

SNMP CPU 使用状況

セキュリティ アプライアンスは、SNMP を利用する CPU 使用状況のモニタリングをサポートしています。セキュリティ アプライアンスの CPU 使用状況を監視する際、HP OpenView などの SNMP 管理ソフトウェアを利用すると、ネットワーク管理者は容量プランを作成できます。

この機能は、Cisco Process MIB（CISCO-PROCESS-MIB.my）の cpmCPUTotalTable のサポート機能によって組み込まれています。MIB には他に 2 つのテーブル（cpmProcessTable、cpmProcessExtTable）がありますが、今回のリリースではサポートされていません。

cpmCPUTotalTable の各行には、CPU のインデックスと次のオブジェクトが含まれます。

MIB オブジェクト名	説明
cpmCPUTotalPhysicalIndex	このオブジェクトの値は 0 になります。Entity MIB の entPhysicalTable of Entity MIB をセキュリティ アプライアンスの SNMP エージェントがサポートしていないためです。
cpmCPUTotalIndex	このオブジェクトの値は 0 になります。Entity MIB の entPhysicalTable of Entity MIB をセキュリティ アプライアンスの SNMP エージェントがサポートしていないためです。
cpmCPUTotal5sec	直前 5 秒間の CPU 全体のビジー率
cpmCPUTotal1min	直前 1 分間の CPU 全体のビジー率
cpmCPUTotal5min	直前 5 分間の CPU 全体のビジー率

（注）　現在のセキュリティ アプライアンス ハードウェア プラットフォームは単一 CPU だけサポートしているため、セキュリティ アプライアンスが返す cpmCPUTotalTable は 1 行だけで、インデックスは常に 1 になります。

直前の 3 要素の値は、**show cpu usage** コマンドの出力値と同じです。

次の新しい MIB オブジェクトが cpmCPUTotalTable にありますが、セキュリティ アプライアンスではサポートされていません。

- cpmCPUTotal5secRev
- cpmCPUTotal1minRev
- cpmCPUTotal5minRev

フィールド

- Community string (default)：パスワードを入力します。SNMP 管理ステーションはセキュリティ アプライアンスに要求を送信するとき、このパスワードを使用します。SNMP のコミュニティ文字列は、SNMP 管理ステーションと管理対象ネットワーク ノード間で共有される秘密情報です。セキュリティ アプライアンスはパスワードを参照して、受信する SNMP 要求が有効かどうかを決定します。パスワードは、大文字と小文字が区別される最大 32 文字の値です。スペースは使用できません。デフォルトは「public」です。SNMPv2c では、管理ステーションごとに別のコミュニティ文字列を設定できます。コミュニティ文字列がどの管理ステーションにも設定されていない場合、ここで設定した値がデフォルトとして使用されます。
- Contact : セキュリティ アプライアンスのシステム管理者の名前を入力します。テキストは最大 127 文字で、大文字と小文字を区別します。スペースは使用できますが、連続するスペースは 1 桁のスペースに縮められます。

- Security Appliance Location：セキュリティ アプライアンスの場所を指定します。テキストは最大 127 文字で、大文字と小文字を区別します。スペースは使用できますが、連続するスペースは 1 桁のスペースに縮められます。
- Listening Port：SNMP トラフィックが送信されるポートを指定します。デフォルトは 161 です。
- Configure Traps：イベントを設定すると、SNMP トラップを利用して通知できます。
- SNMP Management Station ボックス
  - Interface：SNMP　管理ステーションが存在するセキュリティ　アプライアンスのインターフェイスの名前を表示します。
  - IP Address：SNMP 管理ステーションの IP アドレスを表示します。セキュリティ アプライアンスはこのアドレスを使ってトラップ イベントを送信したり、要求またはポーリングを受信したりします。
  - Community string：管理ステーションのコミュニティ文字列を指定しない場合、Community String (default) フィールドの設定値が使用されます。
  - SNMP Version：管理ステーションに設定されている SNMP のバージョンを表示します。
  - Poll/Trap：この管理ステーションとの通信方式を表示します。ポーリングのみ、トラップのみ、ポーリングとトラップがあります。ポーリングとは、一定間隔で繰り返し送信される管理ステーションの要求をセキュリティ アプライアンスが待つことをいいます。トラップを設定すると、発生した syslog イベントが送信されます。
  - UDP Port：SNMP ホストの UDP ポートです。デフォルト ポートは 162 です。
- Add：Add SNMP Host Access Entry が開き、次のフィールドを設定できます。
- Interface Name：管理ステーションが存在するインターフェイスを選択します。
- IP Address：管理ステーションの IP アドレスを指定します。
- Server Poll/Trap Specification：Poll または Trap を選択します。両方を選択することもできます。
- UDP Port：SNMP ホストの UDP ポートを入力します。このフィールドを指定すると、SNMP ホストのデフォルト UDP ポート番号 162 が上書きされます。
- Help：詳細情報を表示します。
- Edit：Edit SNMP Host Access Entry ダイアログボックスが開き、追加の場合と同じフィールドが表示されます。
- Delete：選択した項目を削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

SNMP ホストのアクセス エントリの追加および編集

SNMP 管理ステーションの追加

SNMP 管理ステーションを追加するには、次の手順を実行します。

1. **Add** をクリックし、**SNMP Host Access Entry** ダイアログボックスを開きます。
2. Interface Name から SNMP 管理ステーションが存在するインターフェイスを選択します。
3. 管理ステーションの IP アドレスを IP Address に入力します。
4. SNMP ホストの UDP ポートを入力します。デフォルトは 162 です。
5. SNMP ホストの Community String パスワードを入力します。管理ステーションのコミュニティ文字列を指定しない場合、SNMP Configuration 画面の Community String (default) フィールドに設定した値が使用されます。
6. **Poll** または **Trap** をクリックして選択します。両方を選択することもできます。
7. 前のペインに戻るには、次のいずれかをクリックします。

- **OK**：変更内容を受け入れて、前のペインに戻ります。
- **Cancel**：変更内容を破棄して、前のペインに戻ります。
- **Help**：詳細情報を表示します。

SNMP 管理ステーションの編集

SNMP 管理ステーションを編集するには、次の手順を実行します。

1. SNMP ペインで、SNMP 管理ステーション テーブルのリスト項目を選択します。
2. **Edit** をクリックし、**Edit SNMP Host Access Entry** を開きます。
3. Interface Name から SNMP 管理ステーションが存在するインターフェイスを選択します。
4. 管理ステーションの IP アドレスを IP Address に入力します。
5. SNMP ホストの Community String パスワードを入力します。管理ステーションのコミュニティ文字列を指定しない場合、SNMP Configuration 画面の Community String (default) フィールドに設定した値が使用されます。
6. SNMP ホストの UDP ポートを入力します。デフォルトは 162 です。
7. **Poll** または **Trap** をクリックして選択します。両方を選択することもできます。
8. SNMP のバージョンを選択します。
9. 前のペインに戻るには、次のいずれかをクリックします。

- **OK**：変更内容を受け入れて、前のペインに戻ります。
- **Cancel**：変更内容を破棄して、前のペインに戻ります。
- **Help**：詳細情報を表示します。

SNMP 管理ステーションの削除

テーブルから SNMP 管理ステーションを削除するには、次の手順を実行します。

1. SNMP ペインで、SNMP 管理ステーション テーブルの項目を選択します。
2. **Delete** をクリックします。

フィールド

- Interface name：SNMP ホストが存在するインターフェイスを選択します。
- IP Address：SNMP ホストの IP アドレスを入力します。
- UDP Port : SNMP アップデートの送信先にする UDP ポートを入力します。デフォルトは 162 です。

- Community String：SNMP サーバのコミュニティ文字列を入力します。
- SNMP Version：SNMP のバージョンを選択します。
- Server Port/Trap Specification
  - Poll：ポーリング情報を送信します。ポーリングとは、一定間隔で繰り返し送信される管理ステーションの要求をセキュリティ アプライアンスが待つことをいいます。
  - Trap：トラップ情報を送信します。トラップを設定すると、発生した syslog イベントが送信されます。
- OK：変更内容を受け入れて、前のペインに戻ります。
- Cancel：変更内容を破棄して、前のペインに戻ります。
- Help：詳細情報を表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

SNMP Trap Configuration

トラップ

トラップはブラウジングと異なり、特に要求しなくても、リンク アップ、リンク ダウン、syslog イベントなど特定のイベントが発生すると、管理対象デバイスから管理ステーションに「コメント」が送信されます。

セキュリティ アプライアンスの SNMP オブジェクト ID（OID）が、セキュリティ アプライアンスから送信される SNMP イベントに表示されます。セキュリティ アプライアンスのシステム OID は、SNMP のイベント トラップと SNMP の mib-2.system.sysObjectID に表示されます。

セキュリティ アプライアンスで実行される SNMP サービスには、2 つの異なる機能があります。

- 管理ステーション（または SNMP クライアント）が送信した SNMP 要求に応答を返します。
- 管理ステーション、またはセキュリティ アプライアンスの通知を受信するように登録されたその他のデバイスに、トラップ（イベント通知）を送信します。

セキュリティ アプライアンスは、3 タイプのトラップをサポートします。

- ファイアウォール
- ジェネリック
- syslog

トラップの設定

SNMP Trap Configuration を開くと、次のフィールドが表示されます。

- Standard SNMP Traps：送信する標準トラップを選択します。
  - Authentication：認証の標準トラップをイネーブルにします。
  - Cold Start：コールド スタートの標準トラップをイネーブルにします。
  - Link Up：リンク アップの標準トラップをイネーブルにします。

  - Link Down：リンク ダウンの標準トラップをイネーブルにします。
- Entity MIB Notifications
  - FRU Insert：現場交換可能ユニット（FRU）が挿入された場合のトラップ通知をイネーブルにします。
  - FRU Remove：現場交換可能ユニット（FRU）が取り外された場合のトラップ通知をイネーブルにします。
  - Configuration Change：ハードウェア変更が行われた場合のトラップ通知をイネーブルにします。
- IPSec Traps：IPSec トラップをイネーブルにします。
  - Start：IPSec が開始した場合のトラップをイネーブルにします。
  - Stop：IPSec が停止した場合のトラップをイネーブルにします。
- Remote Access Traps：リモート アクセス トラップをイネーブルにします。
  - Session threshold exceeded：リモート アクセスを開こうとしたセッション数が、設定されているセッション数のしきい値を超過した場合のトラップをイネーブルにします。
- Enable Syslog traps：SNMP 管理ステーションへの syslog メッセージの送信をイネーブルにします。
- OK：変更内容を受け入れて、前のペインに戻ります。
- Cancel：変更内容を破棄して、前のペインに戻ります。
- Help：詳細情報を表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Management Access Rules

Management Access Rules ペインでは、インターフェイスに関連付けられるアクセス ルールを定義できます。アクセス ルールが、特定のピア（または複数のピア）とのトラフィックの送受信の許可または拒否を指定するのに対して、管理アクセス ルールは装置へのトラフィックのアクセス コントロールを行います。

たとえば、IKE DoS（サービス拒絶）攻撃を検出するだけでなく、管理アクセス ルールを使用してブロックすることもできます。

フィールド

注 : カーソルをカラムの線に重ねて二重矢印になったら、その矢印を動かしてテーブル カラムの幅を調整できます。カラムの線をクリックして希望のサイズにドラッグします。

- Add：新しい管理アクセス ルールを追加します。
- Edit：管理アクセス ルールを編集します。
- Delete：管理アクセス ルールを削除します。
- Move Up：ルールを上に移動します。ルールは、このテーブルに表示される順序で評価されるため、重複するルールがあると順序によって評価が異なります。
- Move Down：ルールを下に移動します。
- Cut：ルールを切り取ります。
- Copy：ルールのパラメータをコピーします。Paste ボタンを使用すれば、新しいルールを同じパラメータで開始できます。
- Paste: コピーまたは切り取ったルールのパラメータがあらかじめ入力された Add/Edit Rule ダイアログボックスが開きます。そこでルールを変更し、テーブルに追加します。Paste ボタンをクリックすると、選択したルールの上にルールが追加されます。Paste ドロップダウン リストから Paste After 項目を選択すると、選択したルールの後にルールが追加されます。

次の説明では、Management Access Rules テーブルのカラムをまとめています。テーブル行をダブルクリックすれば、カラムの内容を編集できます。ルールは、実行順に表示されます。ルールを右クリックすると、Insert および Insert After 項目と共に、ボタンで表されているオプションがすべて上に表示されます。これらの項目では、選択したルールの前に新しいルールが挿入されるか（Insert）、選択したルールの後ろに新しいルールが挿入されます（Insert After）。

- No：ルールの評価順序を示します。
- Enabled: ルールがイネーブルになっているか、またはディセーブルになっているかを示します。
- Source：Destination Type フィールドで指定された宛先へのトラフィックが許可または拒否される IP アドレス、ネットワーク オブジェクト グループ、インターフェイス IP、または any を指定します。アドレス カラムには、単語 any が付いたインターフェイス名が含まれることがあります（inside: any など）。これは、内部インターフェイスのすべてのホストが、このルールの影響を受けるという意味です。
- Service：ルールで指定されるサービスまたはプロトコルを表示します。
- Action：ルールに適用されるアクションです（Permit または Deny）。
- Logging : アクセスリストのロギングをイネーブルにしている場合、このカラムには、ロギング レベル、およびログ メッセージ間の間隔が秒数で表示されます。
- Time：ルールが適用される時間範囲が表示されます。
- Description: ルールを追加したときに入力した説明が表示されます。暗黙のルールには、「Implicit outbound rule」という説明が含まれます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Management Access Rules

Add/Edit Management Access Rule ダイアログボックスでは、新しい管理ルールの作成、または既存の管理ルールの変更ができます。

- Interface：ルールを適用するインターフェイスを指定します。
- Action：新しいルールのアクション タイプを決定します。Permit または Deny のいずれかを選択します。
  - Permit：すべての一致トラフィックを許可します。
  - Deny：すべての一致トラフィックを拒否します。
- Source：Destination フィールドで指定された宛先へのトラフィックが許可または拒否される IP アドレス、ネットワーク オブジェクト グループ、インターフェイス IP、または any を指定します。

  ...：既存の IP アドレス オブジェクト、IP 名、ネットワーク オブジェクト グループ、またはすべてを選択、追加、編集、削除、または検索できます。
- Destination：Source Type フィールドで指定した送信元からのトラフィックを許可または拒否する IP アドレス、ネットワーク オブジェクト グループ、インターフェイス IP、または any を指定します。

  ...：既存の IP アドレス オブジェクト、IP 名、ネットワーク オブジェクト グループ、またはすべてを選択、追加、編集、削除、または検索できます。
- Service：サービスのリストからポート番号、ポートの範囲、またはウェルノウン サービス名やグループを指定するには、このオプションを選択します。

  ...：事前に設定したリストから既存のサービスを選択、追加、編集、削除、または検索できます。
- Description：（オプション）管理アクセス ルールの説明を入力します。
- Enable Logging：アクセスリストのロギングをイネーブルにします。
  - Logging Level：default、emergencies、alerts、critical、errors、warnings、notifications、informational、または debugging を指定します。
- More Options：ルールの追加設定オプションを表示します。
  - Enable Rule：ルールをイネーブルまたはディセーブルにします。
  - Traffic Direction：どちらの方向のトラフィックにルールを適用するかを決定します。オプションには Incoming と Outgoing があります。
  - Source Service：送信元のプロトコルとサービスを指定します（TCP または UDP サービスのみ）。

    ...：事前に設定したリストから送信元サービスを選択、追加、編集、削除、または検索できます。

    Logging Interval：ロギングが設定されている場合、ロギング間隔を秒単位で指定します。
  - Time Range：このルールに定義されている時間範囲をドロップダウン リストから指定します。

    ...：事前に設定したリストから時間範囲を選択、追加、編集、削除、または検索できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

システム管理者の AAA の設定

この項では、システム管理者の認証とコマンド認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、まずローカル データベースまたは AAA サーバを設定する必要があります（P.12-9 の「ローカル データベースの設定」または P.12-14 の「AAA サーバ グループとサーバの識別」を参照）。

ここでは、次の項目について説明します。

CLI、ASDM の認証の設定とコマンド アクセスのイネーブル化

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用のユーザ名とパスワードを要求するプロンプトを表示します。情報を入力すると、ユーザ EXEC モードにアクセスできます。

特権 EXEC モードに入るには、**enable** コマンドまたは **login** コマンド（ローカル データベースを使用する場合のみ）を入力します。

イネーブル認証を設定した場合、セキュリティ アプライアンスはユーザ名とパスワードを要求するプロンプトを表示します。**イネーブル**認証を設定しない場合、**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** コマンドを入力した後に**イネーブル**認証を使用しないと、特定のユーザとしてログインした状態でなくなります。ユーザ名を保持するには、**イネーブル**認証を使用します。

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。このコマンドはユーザ名を保持しますが、認証を有効にするための設定は必要ありません。

（注）　セキュリティ アプライアンスが Telnet、SSH、または HTTP ユーザを認証できるようにするには、まずセキュリティ 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（P.13-5 の「Secure Shell」、P.13-6 の「Telnet」、または P.13-2 の「HTTPS/ASDM」を参照）。これらのペインでは、セキュリティ アプライアンスとの通信が許可される IP アドレスを指定します。

CLI、ASDM、または**イネーブル**認証を設定するには、次の手順を実行します。

ステップ 1　**enable** コマンドを使用するユーザを認証するには、Configuration > Device Management > Users/AAA > AAA Access > Authentication に移動し、次の設定値を設定します。

a. **Enable** チェックボックスをオンにします。

b. Server Group ドロップダウン リストから、サーバ グループ名または LOCAL データベースを選択します。

c. （オプション）AAA サーバを選択する場合、セキュリティ アプライアンスがローカル データベースを AAA サーバが使用不可になった場合のフォールバック方式として使用するように設定できます。**Use LOCAL when server group fails** チェックボックスをオンにします。ローカル

データベースには AAA サーバと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。これは、セキュリティ アプライアンスのプロンプトにはどちらの方式を使用しているか示されないためです。

ステップ 2　CLI または ASDM にアクセスするユーザを認証するには、Configuration > Device Management > Users/AAA > AAA Access > Authentication に移動し、次の設定値を設定します。

a. 次のチェックボックスをオンにします（複数可）。

- **HTTP/ASDM**：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、設定する必要があるのは HTTP 認証だけです。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。HTTP 管理認証では、AAA サーバ グループに SDI プロトコルをサポートしていません。
- **Serial**：コンソール ポート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ユーザを認証します。
- **SSH**：SSH 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ユーザを認証します。
- **Telnet**：Telnet 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ユーザを認証します。

b. オンにしたサービスごとに、Server Group ドロップダウン リストから、サーバ グループ名または LOCAL データベースを選択します。

c. （オプション）AAA サーバを選択する場合、セキュリティ アプライアンスがローカル データベースを AAA サーバが使用不可になった場合のフォールバック方式として使用するように設定できます。**Use LOCAL when server group fails** チェックボックスをオンにします。ローカル データベースには AAA サーバと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。これは、セキュリティ アプライアンスのプロンプトにはどちらの方式を使用しているか示されないためです。

ステップ 3　**Apply** をクリックします。

管理認可を使用したユーザの CLI および ASDM アクセスの制限

CLI または**イネーブル**認証を設定すると、ローカル ユーザ、RADIUS、TACACS+、または LDAP ユーザ（LDAP アトリビュートを RADIUS アトリビュートにマッピングした場合）が CLI、ASDM、または **enable** コマンドにアクセスしないように制限できます。

（注）　管理認可にはシリアル アクセスは含まれないため、Authentication > Serial オプションをイネーブルにすると、認証を受けるユーザはコンソール ポートにアクセスできます。

管理認可を設定するには、次の手順を実行します。

ステップ 1　管理認可をイネーブルにするには、Configuration > Device Management > Users/AAA > AAA Access > Authorization に移動し、**Perform authorization for exec shell access > Enable** チェックボックスをオンにします。

このオプションは、RADIUS の管理ユーザ特権レベルのサポートもイネーブルにします。これはローカル コマンド特権レベルと一緒にコマンド認可に使用できます。詳細については、P.13-33 の「ローカル コマンド認可の設定」を参照してください。

ステップ 2　管理認可対象のユーザを設定するには、次の AAA サーバ タイプまたはローカル ユーザの各要件を参照してください。

- RADIUS or LDAP (mapped) users：Service-Type アトリビュートに次のいずれかの値を設定します。
  - admin：Authentication タブのオプションで指定されたすべてのサービスへのフル アクセスを許可します。
  - nas-prompt：Telnet または SSH 認証オプションを設定した場合は CLI へのアクセスを許可しますが、HTTP オプションを設定した場合は ASDM コンフィギュレーション アクセスを拒否します。ASDM 監視アクセスは許可されます。Enable オプションで**イネーブル**認証を設定した場合、ユーザは **enable** コマンドを使用して特権 EXEC モードにアクセスできません。
  - remote-access：管理アクセスを拒否します。ユーザは、Authentication タブのオプションで指定されたサービスのいずれも使用できません（ただし、Serial オプションは除きます。したがって、シリアル アクセスは許可されます）。
- TACACS+ users：「service=shell」で認可が要求されます。サーバは PASS または FAIL で応答します。
  - PASS, privilege level 1：Authentication タブのオプションで指定されたすべてのサービスへのフル アクセスを許可します。
  - PASS, privilege level 2 and higher：Telnet または SSH 認証オプションを設定した場合は CLI へのアクセスを許可しますが、HTTP オプションを設定した場合は ASDM コンフィギュレーション アクセスを拒否します。ASDM 監視アクセスは許可されます。Enable オプションで**イネーブル**認証を設定した場合、ユーザは **enable** コマンドを使用して特権 EXEC モードにアクセスできません。
  - FAIL：管理アクセスを拒否します。ユーザは、Authentication タブのオプションで指定されたサービスのいずれも使用できません（ただし、Serial オプションは除きます。したがって、シリアル アクセスは許可されます）。
- Local users：Access Restriction オプションを設定します。P.12-10 の「Add/Edit User Account > Identity」を参照してください。デフォルトでは、アクセス制限は Full Access です。これは Authentication タブのオプションで指定されたすべてのサービスへのフル アクセスを許可します。

コマンド認可の設定

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、コマンド認可を設定して、ユーザが使用できるコマンドを決定できます。ログインすると、デフォルトでユーザ EXEC モードにアクセスできますが、このモードで使用できるのは最小限のコマンドだけです。**enable** コマンド（ローカル データベースを使用している場合は **login** コマンド）を入力すると、特権 EXEC モードにアクセスし、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。

ここでは、次の項目について説明します。

コマンド認可の概要

この項では、コマンド認可について説明します。次の項目を取り上げます。

サポートされるコマンド認可方式

2 つのコマンド認可方式のいずれかを使用できます。

- Local privilege levels：セキュリティ アプライアンスでのコマンド特権レベルを設定します。ローカル、RADIUS、または LDAP（LDAP アトリビュートを RADIUS アトリビュートにマッピングしている場合）ユーザが CLI アクセスの認証を受けると、セキュリティ アプライアンスは、そのユーザをローカル データベース、RADIUS サーバ、または LDAP サーバによって定義された特権レベルに置きます。ユーザがアクセスできるのは、ユーザの特権レベル以下のコマンドです。すべてのユーザは、最初にログインしたときユーザ EXEC モードにアクセスします（レベル 0 または 1 のコマンド）。特権 EXEC モード（レベル 2 以上のコマンド）にアクセスするには、ユーザは **enable** コマンドを使用して再度認証を受ける必要があります。または、**login** コマンドでログインできます（ローカル データベースのみ）。

（注） ローカル データベースにユーザがない場合や、CLI 認証または**イネーブル**認証を受けていない場合でも、ローカル コマンド認可を使用できます。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 アプライアンスはユーザをレベル 15 に置きます。このレベルでは、すべてのレベルに対してイネーブル パスワードを作成できます。したがって、**enable** *n*（2 ～ 15）を入力すると、セキュリティ アプライアンスがユーザをレベル *n* に置きます。これらのレベルは、ローカル コマンド認可が有効な場合だけ使用されます。下記の「ローカル コマンド認可の設定」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+ server privilege levels：TACACS+ サーバで、ユーザまたはグループが CLI アクセスの認証を受けた後に使用でき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。

ユーザ クレデンシャルの保持について

ユーザがセキュリティ アプライアンスにログインすると、ユーザ名とパスワードを入力して認証を受けるように要求されます。セキュリティ アプライアンスは、これらのセッション クレデンシャルを、この後セッション内でさらに認証が必要になった場合に備えて保持します。

次のコンフィギュレーションが設定されている場合、ユーザがログイン時に認証を受ける必要があるのはローカル サーバだけです。それ以降のシリアル認可では、保存されたクレデンシャルが使用されます。また、ユーザには、特権レベル 15 のパスワードを要求するプロンプトが表示されます。特権モードから出ると、ユーザは再度認証を受けます。ユーザ クレデンシャルは、特権モードでは保持されません。

- ローカル サーバが、ユーザ アクセスを認証するように設定されている。
- 特権レベル 15 のコマンド アクセスがパスワードを要求するように設定されている。
- ユーザのアカウントが、シリアルのみの認可を受けるように設定されている（コンソールまたは ASDM へのアクセスなし）。
- ユーザのアカウントに特権レベル 15 のコマンド アクセスが設定されている。

次の表に、この場合にセキュリティ アプライアンスがクレデンシャルを使用する方法を示します。

必要なクレデンシャル	ユーザ名および パスワード認証	シリアル 認可	特権モードの コマンド認可	特権モード 終了認可
ユーザ名	あり	なし	なし	あり
パスワード	あり	なし	なし	あり
特権モード パスワード	なし	なし	あり	なし

セキュリティ コンテキストとコマンド認可

コマンド認可を複数のセキュリティ コンテキストで実装する場合、次の重要事項を考慮する必要があります。

- AAA 設定はコンテキストごとに別個であり、コンテキスト間で共有されることはありません。

  コマンド認可の設定時、各セキュリティ コンテキストを別個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施できるようになります。

  セキュリティ コンテキストを切り替えるとき、新しいコンテキスト セッションでは、ログイン時に指定したユーザ名に許可されるコマンドが異なる可能性があること、またはコマンド認可がまったく設定されていない可能性があることを管理者は考慮する必要があります。コマンド認可がセキュリティ コンテキスト間で異なる可能性があることを管理者が理解しておかないと、混乱を招くおそれがあります。この動作は、次の点によってさらに複雑になります。

- **changeto** コマンドで開始した新しいコンテキスト セッションは、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に関係なく、常にデフォルトの「enable_15」というユーザ名を管理者 ID として使用します。ユーザ enable_15 に対してコマンド認可が設定されていない場合、またはユーザ enable_15 の認可が前のコンテキスト セッションのユーザの認可とは異なる場合、この動作は混乱の原因になる可能性があります。

  この動作は、コマンド アカウンティングにも影響します。コマンド アカウンティングが役立つのは、発行された各コマンドを正確に特定の管理者に関連付けられる場合だけであるためです。**changeto** コマンドの使用権限を持つすべての管理者が切り替え後のコンテキストでユーザ名 enable_15 を使用できるため、コマンド アカウンティング レコードはユーザ名 enable_15 としてログインしたのは誰かを明確に識別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 サーバを使用する場合、ユーザ名 enable_15 を使用しているのが誰かを追跡するには、複数のサーバからのデータを相互に関連付ける必要があります。

  コマンド認可の設定時、次の点を考慮してください。

  - **changeto**　コマンドの使用権限を持つ管理者は、切り替え後の各コンテキストでユーザ enable_15 に許可されているすべてのコマンドを使用する権限があります。
  - コンテキストごとに異なるコマンドを認可する場合、各コンテキストで、**changeto** コマンドの使用権限を持つ管理者に拒否されているコマンドの使用を、ユーザ名 enable_15 に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とき、管理者は特権 EXEC モードを出て、**enable** コマンドを再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 コマンドはサポートされていないため、コマンド認可はシステム実行スペースでは使用できません。

ローカル コマンド認可の設定

ローカル コマンド認可では、コマンドを 16 の特権レベル（0 ～ 15）のいずれかに割り当てることができます。デフォルトでは、各コマンドは特権レベル 0 または 15 に割り当てられています。各ユーザを特定の特権レベルに定義することができ、ユーザはその特権レベル以下であれば、どのコマンドでも入力できます。セキュリティ アプライアンスは、ローカル データベース、RADIUS サーバ、または LDAP サーバ（LDAP アトリビュートを RADIUS アトリビュートにマッピングしている場合）に定義されているユーザ特権レベルをサポートしています。P.12-25 の「LDAP Attribute Map の設定」を参照してください。

ここでは、次の項目について説明します。

ローカル コマンド認可の前提条件

コマンド認可の設定の一部として次の操作を実行します。

- **イネーブル**認証を設定します（P.13-28 の「CLI、ASDM の認証の設定とコマンド アクセスのイネーブル化」を参照）。

  イネーブル認証は、ユーザが **enable** コマンドにアクセスした後もユーザ名を保持するために必須です。

  または、設定の必要がない **login** コマンドを使用できます（ローカル データベースの場合のみで、認証を受けた **enable** コマンドと同じ）。この方法は**イネーブル**認証ほどセキュアではないため、お勧めしません。

  CLI 認証も使用できますが、必須ではありません。
- 次のユーザ タイプごとの前提条件を参照してください。
  - ローカル データベース ユーザ：ローカル データベース内の各ユーザを特権レベル 0 ～ 15 に設定します。

    ローカル データベースを設定するには、P.12-9 の「ローカル データベースの設定」を参照してください。
  - RADIUS ユーザ：ユーザを Cisco VSA CVPN3000-Privilege-Level の値 0 ～ 15 に設定します。
  - LDAP ユーザ：ユーザを特権レベル 0 ～ 15 に設定してから、LDAP アトリビュートを Cisco VAS CVPN3000-Privilege-Level にマッピングします（P.12-25 の「LDAP Attribute Map の設定」を参照）。

デフォルトのコマンド特権レベル

デフォルトで、次のコマンドは特権レベル 0 に割り当てられています。その他のすべてのコマンドはレベル 15 に割り当てられています。

- **show checksum**
- **show curpriv**
- **enable**
- **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、必ず **configure** コマンドもそのレベルに移動します。移動しないと、ユーザが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。

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

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

ステップ 1　コマンド認可をイネーブルにするには、Configuration > Device Management > Users/AAA > AAA Access > Authorization に移動し、**Enable authorization for command access > Enable** チェックボックスをオンにします。

ステップ 2　Server Group ドロップダウン リストから、**LOCAL** を選択します。

ステップ 3　ローカル　コマンド認可をイネーブルにすると、特権レベルを個々のコマンドまたはコマンド　グループに手動で割り当てるオプション、または事前定義済みユーザ アカウント特権をイネーブルにするオプションを使用できます。

- 事前定義済みユーザ アカウント特権を使用するには、**Set ASDM Defined User Roles** をクリックします。

  ASDM Defined User Roles Setup ダイアログボックスに、コマンドとそのレベルが表示されます。事前定義済みユーザ アカウント特権を使用するには、**Yes** をクリックします。事前定義済みユーザ アカウント特権には、Admin（特権レベル 15、すべての CLI コマンドへのフル アクセス）、Read Only（特権レベル 5、読み取り専用アクセス）、Monitor Only（特権レベル 3、Monitoring セクションへのアクセス権のみ）があります。
- コマンド レベルを手動で設定するには、**Configure Command Privileges** ボタンをクリックします。

  Command Privileges Setup ダイアログボックスが表示されます。Command Mode ドロップダウン リストから **--All Modes--** を選択すると、すべてのコマンドを表示できます。または、コンフィギュレーション モードを選択して、そのモードで使用可能なコマンドを表示できます。たとえば、**context** を選択すると、コンテキスト コンフィギュレーション モードで使用可能なコマンドをすべて表示できます。コマンドをコンフィギュレーション モードだけでなく、ユーザ EXEC や特権 EXEC モードでも入力でき、そのコマンドがモードごとに異なるアクションを実行する場合、これらのモードに対して別個に特権レベルを設定できます。

  Variant カラムには、show、clear、または cmd が表示されます。コマンドの show、clear、または configure 形式に対してのみ特権を設定できます。コマンドの configure 形式では、通常、変更されないコマンド（**show** または **clear** プレフィックスなし）または **no** 形式のどちらかとして、コンフィギュレーションの変更が発生します。

  コマンドのレベルを変更するには、コマンドをダブルクリックするか、**Edit** をクリックします。0 ～ 15 のレベルを設定できます。特権レベルを変更できるのは *main* コマンドだけです。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** コマンドや **aaa authorization** コマンドのレベルを別個に設定することはできません。

  表示されているすべてのコマンドのレベルを変更するには、**Select All** をクリックして **Edit** をクリックします。

  OK をクリックして変更を受け入れます。

ステップ 4　RADIUS の管理ユーザ特権レベルをサポートするには、**Perform authorization for exec shell access > Enable** チェックボックスをオンにします。

このオプションを設定しないと、セキュリティ アプライアンスはローカル データベース ユーザの特権レベルだけをサポートし、他のタイプのユーザにはデフォルトのレベル 15 を使用します。

また、このオプションは、ローカル、RADIUS、LDAP（マッピング済み）、および TACACS+ のユーザに対する管理認可をイネーブルにします。詳細については、P.13-29 の「管理認可を使用したユーザの CLI および ASDM アクセスの制限」を参照してください。

ステップ 5　**Apply** をクリックします。

TACACS+ コマンド認可の設定

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

TACACS+ サーバを使用したコマンド認可の設定時には、意図したとおりに機能することを確認してからコンフィギュレーションを保存してください。誤ったコンフィギュレーションによりロックアウトされた場合は、通常、セキュリティ アプライアンスを再起動してアクセス権を回復できます。それでもロックアウトされる場合は、P.13-40 の「ロックアウトからの回復」を参照してください。

TACACS+ システムの安定性と信頼性が十分であることを確認してください。必要な信頼性のレベルとして、通常は TACACS+ サーバ システム、およびセキュリティ アプライアンスへの接続に完全な冗長性が求められます。たとえば、使用する TACACS+ サーバ プールに、インターフェイス 1 に接続する 1 台のサーバとインターフェイス 2 に接続するもう 1 台のサーバを含めます。また、TACACS+ サーバが使用できない場合のフォールバック方式としてローカル コマンド認可も設定できます。この場合、P.13-30 の「コマンド認可の設定」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、次の項目について説明します。

TACACS+ コマンド認可の前提条件

CLI および**イネーブル**認証を設定します（P.13-28 の「CLI、ASDM の認証の設定とコマンド アクセスのイネーブル化」を参照）。

TACACS+ サーバのコマンドの設定

Cisco Secure Access Control Server（ACS）TACACS+ サーバのコマンドを、グループまたは個別ユーザに対する共有プロファイル コンポーネントとして設定できます。サードパーティの TACACS+ サーバの場合、コマンド認可サポートの詳細については、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 でのコマンドの設定については次のガイドラインを参照してください。このガイドラインの多くは、サードバーティのサーバに対しても適用されます。

- セキュリティ アプライアンスは、コマンドを「シェル」コマンドとして認可されるように送信するため、TACACS+ サーバでもそのコマンドはシェル コマンドとして設定してください。

（注）　Cisco Secure ACS には、「pix-shell」というコマンド タイプが含まれている場合があります。このタイプのコマンドはセキュリティ アプライアンスのコマンド認可には使用しないでください。

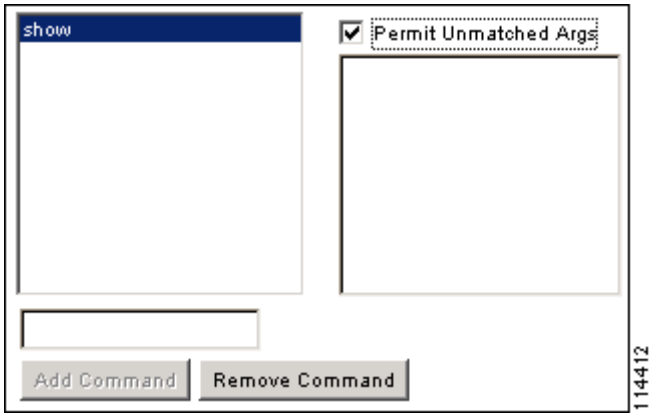
- コマンドの最初の語は、メイン コマンドと見なされます。それ以降の語はすべて引数と見なされ、その前に **permit** または **deny** を付ける必要があります。

  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オンにすると、明示的に拒否されたものを除き、コマンドのすべての引数を許可できます。

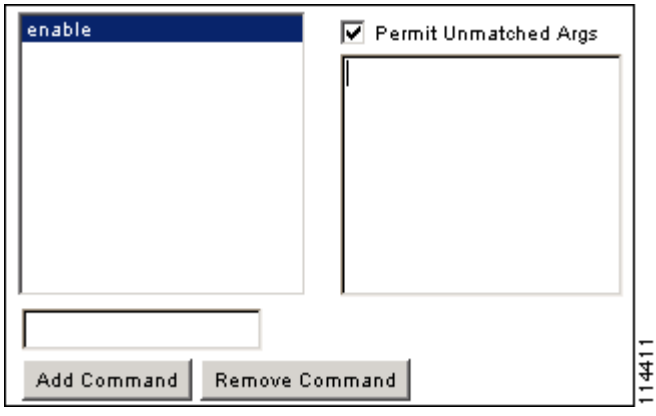
  たとえば、**show** コマンドだけを設定して、すべての **show** コマンドを許可できます。省略形や CLI の使用方法を表示する **?** など、コマンドのバリアントすべてを想定する必要がないため、この方法を使用することをお勧めします（図 13-1 を参照）。

図 13-1　関連するすべてのコマンドの許可



- 1 語のコマンドの場合、コマンドに引数がない場合も含め、一致しない引数（**enable** や **help** など）を許可する必要があります（図 13-2 を参照）。

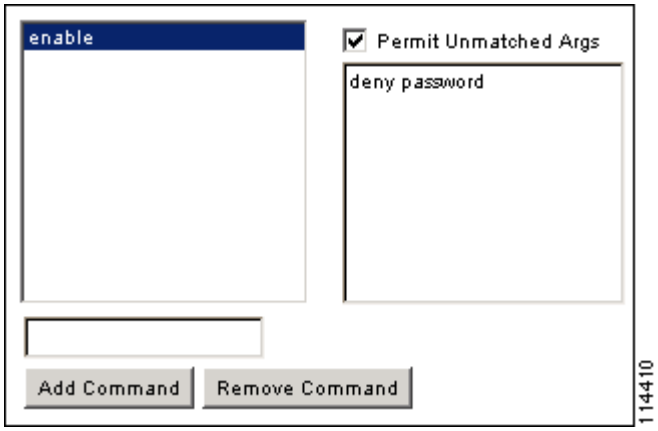
図 13-2　1 語のコマンドの許可



- 許可しない引数がある場合は、**deny** の後にその引数を入力します。

  たとえば、**enable** は許可するが、**enable password** は許可しない場合、コマンド ボックスに **enable** を入力し、引数ボックスに **deny password** と入力します。必ず Permit Unmatched Args チェックボックスをオンにし、**enable** 単体は許可されるようにします（図 13-3 を参照）。

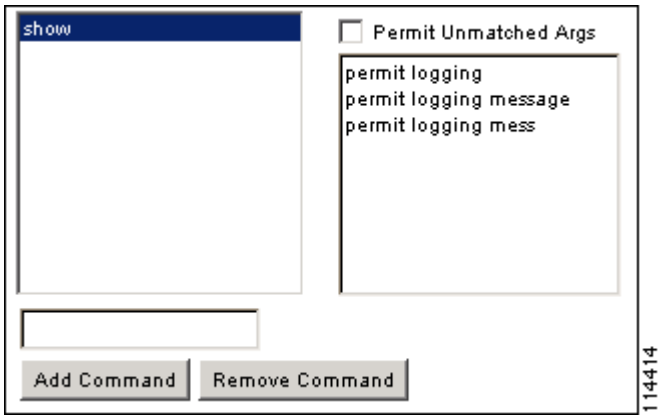
図 13-3　引数の不許可



- コマンドラインでコマンドの省略形を使用する場合、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 コマンドをフル テキストで展開しますが、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 アプライアンスはコマンド全体（**show logging**）を TACACS+ サーバに送信します。ただし、**sh log mess** と入力すると、セキュリティ アプライアンスは **show logging mess** を TACACS+ サーバに送信しますが、コマンドを **show logging message** と展開することはありません。省略形を想定し、同じ引数の複数のスペルを設定できます（図 13-4 を参照）。

図 13-4　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+ コマンド認可をイネーブルにする前に、TACACS+ サーバに定義されている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行するために必要なコマンド認可を受けていることを確認します。たとえば、すべてのコマンドが認可された admin ユーザとしてログインする必要があります。それ以外の場合、予期せずロックアウトされる場合があります。

TACACS+ コマンド認可を設定するには、次の手順を実行します。

ステップ 1　TACACS+ サーバを使用したコマンド認可を実行するには、Configuration > Device Management > Users/AAA > AAA Access > Authorization に移動し、**Enable authorization for command access > Enable** チェックボックスをオンにします。

ステップ 2　Server Group ドロップダウン リストから、AAA サーバ グループ名を選択します。

ステップ 3　（オプション）AAA サーバを使用できない場合の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セキュリティ アプライアンスを設定できます。**Use LOCAL when server group fails** チェックボックスをオンにします。ローカル データベースには AAA サーバと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。これは、セキュリティ アプライアンスのプロンプトにはどちらの方式を使用しているか示されないためです。

ステップ 4　**Apply** をクリックします。

管理アクセス アカウンティングの設定

管理アクセスのアカウンティングをイネーブルにするには、次の手順を実行します。

ステップ 1　アカウンティングの対象にできるのは、最初にセキュリティ アプライアンスの認証を受けたユーザだけです。そのため、P.13-28 の「CLI、ASDM の認証の設定とコマンド アクセスのイネーブル化」に従って認証を設定します。

ステップ 2　ユーザが **enable** コマンドを入力したときにアカウンティングをイネーブルにするには、次の手順を実行します。

a. Configuration > Device Management > Users/AAA > AAA Access > Accounting に移動し、**Require accounting to allow accounting of user activity > Enable** チェックボックスをオンにします。

b. Server Group ドロップダウン リストから、RADIUS または TACACS+ サーバ グループ名を選択します。

ステップ 3　ユーザが Telnet、SSH、またはシリアル コンソールを使用してセキュリティ アプライアンスにアクセスしたときにユーザのアカウンティングをイネーブルにするには、次の手順を実行します。

a. Require accounting for the following types of connections 領域の下で、Serial、SSH、Telnet に対応するチェックボックスをオンにします（複数可）。

b. 接続タイプごとに、Server Group ドロップダウン リストから RADIUS または TACACS+ サーバ グループ名を選択します。

ステップ 4　コマンド アカウンティングを設定するには、次の手順を実行します。

a. Require command accounting 領域の下で、**Enable** をオンにします。

b. Server Group ドロップダウン リストから、TACACS+ サーバ グループ名を選択します。RADIUS はサポートされていません。

CLI で **show** コマンド以外のいずれかのコマンドを入力したときに、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。

c. Command Privilege Setup ダイアログボックスを使用してコマンド特権レベルをカスタマイズする場合（P.13-34 の「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」を参照）、Privilege level ドロップダウン リストで最小特権レベルを指定することで、セキュリティ アプライアンスのアカウンティング対象のコマンドを制限できます。セキュリティ アプライアンスは、最小の特権レベル未満のコマンドはアカウンティングしません。

ステップ 5　**Apply** をクリックします。

ロックアウトからの回復

コマンド認可または CLI 認証を有効にすると、状況によってはセキュリティ アプライアンス CLI からロックアウトされることがあります。通常は、セキュリティ アプライアンスを再起動するとアクセス権を回復できます。ただし、コンフィギュレーションをすでに保存していると、ロックアウトされることがあります。表 13-3 に、一般的なロックアウト状況と回復方法を示します。

表 13-3　CLI 認証とコマンド認可のロックアウト シナリオ

機能	ロックアウト状況	説明	回避策：シングルモード	回避策：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含まれていない。	ローカル データベースにユーザが含まれていない場合、ログインできず、ユーザを追加することはできません。	ログインし、パスワードと各 **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 アプライアンスのセッションを開始します。システム実行スペースから、該当するコンテキストに変更し、ユーザを追加できます。
TACACS+ コマンド認可 TACACS+ CLI 認証 RADIUS CLI 認証	サーバが停止または到達不能で、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の入力はできません。	1. ログインし、パスワードと各 AAA コマンドをリセットします。 2. 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、サーバが停止してもロックアウトされないようにします。	1. セキュリティ アプライアンスのネットワーク コンフィギュレーションが正しくないために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 アプライアンスのセッションを開始します。システム実行スペースから、該当するコンテキストに変更し、ネットワーク設定値を再設定できます。 2. 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、サーバが停止してもロックアウトされないようにします。
TACACS+ コマンド認可	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。	コマンド認可をイネーブルにしたにもかかわらず、ユーザがどのコマンドも入力できないことが判明しました。	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、ただちにセキュリティ アプライアンスを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、パスワードと各 **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 アプライアンスのセッションを開始します。システム実行スペースから、該当するコンテキストに変更し、コンフィギュレーションの変更を完了できます。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た。	コマンド認可をイネーブルにしたにもかかわらず、ユーザがどのコマンドも入力できないことが判明しました。	ログインし、パスワードと各 **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 アプライアンスのセッションを開始します。システム実行スペースから、該当するコンテキストに変更し、ユーザ レベルを変更できます。