CHAPTER 45

管理アクセスの設定

この章では、Telnet、SSH、および HTTPS（ASDM を使用）を介してシステム管理のために ASA にアクセスする方法と、ユーザを認証および許可する方法とログイン バナーを作成する方法について説明します。

この章は、次の項で構成されています。

（注） また、ASA インターフェイスに管理アクセスの目的でアクセスするには、ホスト IP アドレスを許可するアクセス ルールは必要ありません。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。

ASDM、Telnet、または SSH の ASA アクセスの設定

この項では、ASDM、Telnet、または SSH を使用した ASA へのアクセスをクライアントに許可する方法について説明します。次の項目を取り上げます。

ASDM、Telnet、または SSH での ASA アクセスのライセンス要件

次の表に、この機能のライセンス要件を示します。

モデル	ライセンス要件
すべてのモデル	基本ライセンス

ガイドラインと制限事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

IPv6 のガイドライン

IPv6 をサポートします。

モデルのガイドライン

ASASM の場合、スイッチから ASASM へのセッションは Telnet セッションですが、このセクションに従って Telnet アクセスを設定する必要はありません。

その他のガイドライン

- VPN 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。
- ASA への通過ルートとなるインターフェイス以外のインターフェイスへの管理アクセスはサポートされません。たとえば、管理ホストが外部インターフェイスにある場合、外部インターフェイスへの直接管理接続のみ開始できます。このルールの例外は、VPN 接続を介した場合のみです。「VPN トンネルを介した管理アクセスの設定」（P.45-15）を参照してください。
- ASA では、以下のことが可能です。
  - 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。
  - 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 32 の ASDM インスタンスの使用が可能です。
- ASA 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。
- SSL および SSH での XML 管理はサポートされていません。

- （8.4 以降）SSH デフォルト ユーザ名はサポートされなくなりました。**pix** または **asa** ユーザ名とログイン パスワードで SSH を使用して ASA に接続することができなくなりました。SSH を使用するには、[Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authentication] を使用して AAA 認証を設定してから、[Configuration] > [Device Management] > [Users/AAA] > [User Accounts] を選択してローカル ユーザを定義する必要があります。ローカル データベースの代わりに AAA サーバを認証に使用する場合、ローカル認証もバックアップの手段として設定しておくことをお勧めします。
- ASA インターフェイスへの Telnet または SSH 接続を確立できない場合は、「ASDM、Telnet、または SSH の ASA アクセスの設定」（P.45-1）の手順に従って、ASA への Telnet または SSH をイネーブルにしていることを確認します。
- SSH の AES-CTR 暗号化は、ASA 5505、5510、5520、5540、および 5550 を含むシングルコア プラットフォームの AES-128 のみサポートします。

管理アクセスの設定

クライアント IP アドレスを、ASA に Telnet、SSH、または ASDM を使用して接続できるよう指定するには、次の手順を実行します。

手順の詳細

ステップ 1　[Configuration] > [Device Management] > [Management Access] > [ASDM/HTTPS/Telnet/SSH] を選択して、[Add] をクリックします。

[Add Device Access Configuration] ダイアログボックスが表示されます。

ステップ 2　セッションのタイプとして、[ASDM/HTTPS]、[Telnet]、[SSH] のいずれかを選択します。

ステップ 3　[Interface Name] ドロップダウン リストから、管理アクセスに使用するインターフェイスを選択します。

ステップ 4　[IP Address] フィールドに、アクセスを許可するネットワークまたはホストの IP アドレスを入力します。このフィールドには、IPv6 アドレスを入力することもできます。

（注）　その際、IPv6 アドレスの [IP Address] フィールドにコロン（:）を入力すると、[Netmask] フィールドが [Prefix Length] に変わります。

ステップ 5　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るマスクを、[Mask] ドロップダウン リストから選択します。

ステップ 6　[OK] をクリックします。

ステップ 7　HTTP の設定を行います。

a.　[Enable HTTP Server]：HTTP サーバを ASDM アクセス用にイネーブルにします。この設定はデフォルトでイネーブルになっています。

b.　（任意）[Port Number]：デフォルト ポートは 443 です。

c.　（任意）[Idle Timeout]：デフォルトのアイドル タイムアウトは 20 分です。

d.　（任意）[Session Timeout]：デフォルトでは、セッション タイムアウトはディセーブルになっています。ASDM 接続にセッション時間の制限はありません。

e.　（任意）クライアント認証が次のインターフェイス上の ASDM にアクセスする必要があります。ドロップダウン リストでインターフェイスを指定します。

ステップ 8　（任意）Telnet の設定を行います。

a. [Telnet Timeout]：デフォルトのタイムアウト値は 5 分です。

ステップ 9　（任意）SSH の設定を行います。

a. [Allowed SSH Version(s)]：デフォルト値は 1 と 2 です。

b. [SSH Timeout]：デフォルトのタイムアウト値は 5 分です。

c. [DH Key Exchange]：該当するオプション ボタンをクリックして、Diffie-Hellman（DH）キー交換グループ 1 またはグループ 14 を選択します。ASA では、DH グループ 1 およびグループ 14 キー交換の両方の方法がサポートされます。DH グループ キー交換方式が指定されないと、DH グループ 1 のキー交換方式が使用されます。DH キー交換方法の使用方法の詳細については、RFC 4253 を参照してください。

ステップ 10　[Apply] をクリックします。

変更内容が実行コンフィギュレーションに保存されます。

ステップ 11　（SSH で必須）SSH 認証の設定も行う必要があります。

a. [Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authentication] を選択します。

b. [SSH] チェックボックスをオンにします。

c. [Server Group] ドロップダウン リストから、すでに設定されている AAA サーバ グループ名または **LOCAL** データベースを選択します。

d. （任意）AAA サーバ グループを選択する場合は、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ローカル データベースが使用されるように ASA 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、ASA 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。

e. [Apply] をクリックします。

f. LOCAL データベースを選択した場合は、ローカル ユーザを追加します。[Configuration] > [Device Management] > [Users/AAA] > [User Accounts] の順に選択し、[Add] をクリックします。

[Add User Account-Identity] ダイアログボックスが表示されます。

g. [Username] フィールドに、4 ～ 64 文字のユーザ名を入力します。

h. [Password] フィールドに、3 ～ 32 文字の間でパスワードを入力します。パスワードでは大文字と小文字が区別されます。

i. [Confirm Password] フィールドにパスワードを再入力します。

その他のフィールドの詳細については、「ユーザ アカウントのローカル データベースへの追加」（P.33-3）を参照してください。

j. [OK] をクリックし、続いて [Apply] をクリックします。

Telnet クライアントの使用

ASA CLI に Telnet を使用してアクセスするには、ログイン パスワードを入力します。Telnet 認証を設定している場合（「CLI、ASDM、および enable コマンド アクセスの認証の設定」（P.45-22）を参照）、AAA サーバまたはローカル データベースで定義したユーザ名とパスワードを入力します。

SSH クライアントの使用

管理ホスト上の SSH クライアントで、ユーザ名とパスワードを入力します。SSH セッションを開始すると、次の SSH ユーザ認証プロンプトが表示される前に、ASA コンソール上にドット（.）が表示されます。

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

ドットが表示されても、SSH の機能には影響を与えません。コンソールにドットが表示されるのは、ユーザ認証が始まる前で、サーバ キーを生成する場合か、または SSH キー交換中に秘密キーを使用してメッセージを暗号化する場合です。これらのタスクには 2 分以上かかることがあります。ドットは、ASA 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。

パスワードを使用する代わりに公開キーを設定できます。「ユーザ アカウントのローカル データベースへの追加」（P.33-3）を参照してください。

CLI パラメータの設定

この項は、次の内容で構成されています。

CLI パラメータのライセンス要件

次の表に、この機能のライセンス要件を示します。

モデル	ライセンス要件
すべてのモデル	基本ライセンス

ガイドラインと制限事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

ログイン バナーの設定

ユーザが ASA に接続し、ユーザがログインする前または特権 EXEC モードに入る前に表示されるメッセージを設定できます。

制限事項

バナーが追加された後、次の場合は ASA に対する Telnet または SSH セッションが終了する可能性があります。

- バナー メッセージを処理するためのシステム メモリが不足している場合。
- バナー メッセージの表示を試みたときに、TCP 書き込みエラーが発生した場合。

ガイドライン

- セキュリティの観点から、バナーで不正アクセスを防止することが重要です。侵入者を惹き付けるような「welcome」や「please」といった言葉を使用しないでください。次のバナーは、不正アクセスに対して適切な雰囲気を表しています。

  ```
  You have logged in to a secure device. If you are not authorized to access this
  device, log out immediately or risk possible criminal consequences.
  ```

- バナー メッセージのガイドラインについては、RFC 2196 を参照してください。

ログイン バナーを設定するには、次の手順を実行します。

手順の詳細

ステップ 1　[Configuration] > [Device Management] > [Management Access] > [Command Line (CLI)] > [Banner] の順に選択し、CLI に対して作成するバナーのタイプに対応するフィールドに、バナー テキストを入力します。

- [session (exec)] バナーは、ユーザが CLI で特権 EXEC モードにアクセスした場合に表示されます。
- [login] バナーは、ユーザが CLI にログインした場合に表示されます。
- [message-of-the-day (motd)] バナーは、ユーザが CLI に初めて接続する場合に表示されます。
- [ASDM] バナーは、ユーザが認証を受けた後 ASDM に接続した場合に表示されます。ユーザは、次のいずれかのオプションを使用して、表示されたバナーを消去できます。
  - [Continue] : バナーを消去し、ログインできます。
  - [Disconnect] : バナーを消去し、接続を終了します。
- 使用できるのは、改行（Enter キー）も含めて ASCII 文字だけです。ただし、改行文字は 2 文字に相当します。
- また、タブ文字は、CLI バージョンでは無視されるため、バナーには使用しないでください。
- RAM およびフラッシュ メモリに関するもの以外、バナーに長さ制限はありません。
- ASA のホスト名またはドメイン名は、**$(hostname)** 文字列と **$(domain)** 文字列を組み込むことによって動的に追加できます。

- システム コンフィギュレーションでバナーを設定する場合は、コンテキスト コンフィギュレーションで **$(system)** という文字列を使用することにより、コンテキスト内でバナー テキストを使用できます。

ステップ 2　[Apply] をクリックします。

新しいバナーが、実行コンフィギュレーションに保存されます。

CLI プロンプトのカスタマイズ

[CLI Prompt] ペインで、CLI セッション時に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 ASA 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。

cluster-unit	（シングルおよびマルチ モード）クラスタ ユニット名を表示します。クラスタの各ユニットは一意の名前を持つことができます。
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 プライオリティを [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。状態には次の値が表示されます。 • [act]：フェールオーバーがイネーブルであり、装置ではトラフィックをアクティブに通過させています。 • [stby]：フェールオーバーはイネーブルです。ユニットはトラフィックを通過させていません。スタンバイ、失敗、または他の非アクティブ状態です。 • [actNoFailove]：フェールオーバーはディセーブルであり、装置ではトラフィックをアクティブに通過させています。 • [stbyNoFailover]：フェールオーバーはディセーブルであり、装置ではトラフィックを通過させていません。この状況は、スタンバイ ユニットでしきい値を上回るインターフェイス障害が発生したときに生じることがあります。 クラスタのユニットのロール（マスターまたはスレーブ）を示します。たとえば、プロンプト ciscoasa/cl2/slave では、ホスト名は ciscoasa、ユニット名は cl2、状態名は slave です。

手順の詳細

[CLI] プロンプトをカスタマイズするには、次の手順を実行します。

ステップ 1　[Configuration] > [Device Management] > [Management Access] > [Command Line (CLI)] > [CLI Prompt] の順に選択し、次のいずれかの操作を行って、プロンプトをカスタマイズします。

- プロンプトに属性を追加する場合は、[Available Prompts] リストで目的の属性をクリックし、[Add] をクリックします。プロンプトには複数の属性を追加できます。属性が [Available Prompts] リストから [Selected Prompts] リストに移動します。

- プロンプトから属性を削除する場合は、[Selected Prompts] リストで属性をクリックし、[Delete] をクリックします。属性が [Selected Prompts] リストから [Available Prompts] リストに移動します。
- コマンド プロンプトに属性が表示される順序を変更する場合は、[Selected Prompts] リストで目的の属性をクリックし、[Move Up] または [Move Down] をクリックして順序を変更します。

変更されたプロンプトが [CLI Prompt Preview] フィールドに表示されます。

ステップ 2　[Apply] をクリックします。

変更されたプロンプトが、実行コンフィギュレーションに保存されます。

コンソール タイムアウトの変更

コンソール タイムアウトでは、接続を特権 EXEC モードまたはコンフィギュレーション モードにしておくことができる時間を設定します。タイムアウトに達すると、セッションはユーザ EXEC モードになります。デフォルトでは、セッションはタイムアウトしません。この設定は、コンソール ポートへの接続を保持できる時間には影響しません。接続がタイムアウトすることはありません。

コンソール タイムアウトを変更するには、次の手順を実行します。

手順の詳細

ステップ 1　新しいタイムアウト値を分単位で定義するには、[Configuration] > [Device Management] > [Management Access] > [Command Line (CLI)] > [Console Timeout] の順に選択します。

ステップ 2　タイムアウトを設定しない場合は、**0** を入力します。デフォルト値は 0 です

ステップ 3　[Apply] をクリックします。

タイムアウト値が変更され、その変更内容が実行コンフィギュレーションに保存されます。

ファイル アクセスの設定

この項では、次のトピックについて取り上げます。

ファイル アクセスのライセンス要件

次の表に、この機能のライセンス要件を示します。

モデル	ライセンス要件
すべてのモデル	基本ライセンス

注意事項と制約事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

FTP クライアント モードの設定

ASA では、FTP サーバとの間で、イメージ ファイルやコンフィギュレーション ファイルのアップロードおよびダウンロードを実行できます。パッシブ FTP では、クライアントは制御接続およびデータ接続の両方を開始します。パッシブ モードではデータ接続の受け入れ側となるサーバは、今回の特定の接続においてリッスンするポート番号を応答として返します。

FTP クライアントをパッシブ モードに設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Device Management] > [Management Access] > [File Access] > [FTP Client] ペインで、[Specify FTP mode as passive] チェックボックスをオンにします。

ステップ 2　[Apply] をクリックします。

FTP クライアントのコンフィギュレーションが変更され、その変更内容が実行コンフィギュレーションに保存されます。

セキュア コピー サーバとしての ASA の設定

ASA 上でセキュア コピー サーバをイネーブルにできます。SSH による ASA へ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 サーバのこの実装には、次の制限があります。

- サーバはセキュア コピーの接続を受け入れまたは終了できますが、開始はできません。
- サーバにはディレクトリ サポートがありません。そのため、リモート クライアント アクセスで ASA の内部ファイル参照はできません。
- サーバではバナーがサポートされません。
- サーバではワイルドカードがサポートされません。

- SSH バージョン 2 接続をサポートするには、ASA のライセンスに VPN-3DES-AES 機能が必要です。

ASA をセキュア コピー サーバとして設定するには、次の手順を実行します。

手順の詳細

ステップ 1　[Configuration] > [Device Management] > [Management Access] > [File Access] > [Secure Copy (SCP) Server] ペインで、[Enable secure copy server] チェックボックスをオンにします。

ステップ 2　[Apply] をクリックします。

変更内容が実行コンフィギュレーションに保存されます。ASA が SCP サーバとして動作するようになり、デバイスとの間でファイルのやり取りが可能になります。

TFTP クライアントとしての ASA の設定

TFTP は、単純なクライアント/サーバ ファイル転送プロトコルで、RFC 783 および RFC 1350 Rev で規定されています。2. ASA を TFTP *クライアント*として設定すると、その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*へ転送できるようになります。設定を行うには、[File] > [Save Running Configuration to TFTP Client or Tools] > [Command Line Interface] を選択します。これにより、コンフィギュレーション ファイルをバックアップし、それらを複数の ASA にプロパゲートできます。

ASA 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 パスは、[Configuration] > [Device Management] > [Management Access] > [File Access] > [TFTP Client] で指定します。このペインで TCP クライアントを設定すれば、それ以降は CLI の **configure net** コマンドおよび **copy** コマンドで、コロン（:）を使用した IP アドレスを指定できます。ただし、ASA と TFTP クライアントの通信に必要となる中間デバイスの認証や設定は、この機能とは別に行われます。

コンフィギュレーション ファイルを TFTP サーバに保存できるように、ASA を TFTP クライアントとして設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Device Management] > [Management Access] > [File Access] > [TFTP Client] ペインで、[Enable] チェックボックスをオンにします。

ステップ 2　[Interface Name] ドロップダウン リストから、TFTP クライアントとして使用するインターフェイスを選択します。

ステップ 3　コンフィギュレーション ファイルの保存先とする TFTP サーバの IP アドレスを [IP Address] フィールドに入力します。

ステップ 4　コンフィギュレーション ファイルの保存先とする TFTP サーバへのパスを [Path] フィールドに入力します。

例：/tftpboot/asa/config3

ステップ 5　[Apply] をクリックします。

変更内容が実行コンフィギュレーションに保存されます。以降、ASA のコンフィギュレーション ファイルの保存には、この TFTP サーバが使用されます。詳細については、「TFTP サーバへの実行コンフィギュレーションの保存」（P.46-28）を参照してください。

マウント ポイントの追加

この項では、次のトピックについて取り上げます。

CIFS マウント ポイントの追加

共通インターネット ファイル システム（CIFS）マウント ポイントを定義するには、次の手順を実行します。

ステップ 1　[Configuration] > [Device Management] > [Management Access] > [File Access] > [Mount-Points] ペインで、[Add] > [CIFS Mount Point] をクリックします。

[Add CIFS Mount Point] ダイアログボックスが表示されます。

ステップ 2　[Enable mount point] チェックボックスをオンにします。

これにより、ASA 上の CIFS ファイル システムが UNIX のファイル ツリーに接続されます。

ステップ 3　[Mount Point Name] フィールドに、既存の CIFS が存在する位置の名前を入力します。

ステップ 4　[Server Name] フィールドまたは [IP Address] フィールドに、マウント ポイントを配置するサーバの名前または IP アドレスを入力します。

ステップ 5　[Share Name] フィールドに、CIFS サーバ上のフォルダの名前を入力します。

ステップ 6　[NT Domain Name] フィールドに、サーバが常駐する NT ドメインの名前を入力します。

ステップ 7　サーバに対するファイル システムのマウントを許可されているユーザの名前を、[User Name] フィールドに入力します。

ステップ 8　サーバに対するファイル システムのマウントを許可されているユーザのパスワードを、[Password] フィールドに入力します。

ステップ 9　[Confirm Password] フィールドにパスワードを再入力します。

ステップ 10　[OK] をクリックします。

[Add CIFS Mount Point] ダイアログボックスが閉じます。

ステップ 11　[Apply] をクリックします。

マウント ポイントが ASA に追加され、その変更内容が実行コンフィギュレーションに保存されます。

FTP マウント ポイントの追加

（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 サーバには、デフォルトで MS-DOS ディレクトリ リスト スタイルがあります。

FTP マウント ポイントを定義するには、次の手順を実行します。

ステップ 1　[Configuration] > [Device Management] > [Management Access] > [File Access] > [Mount-Points] ペインで、[Add] > [FTP Mount Point] をクリックします。

[Add FTP Mount Point] ダイアログボックスが表示されます。

ステップ 2　[Enable] チェックボックスを選択します。

これにより、ASA 上の FTP ファイル システムが UNIX のファイル ツリーに接続されます。

ステップ 3　[Mount Point Name] フィールドに、既存の FTP が存在する位置の名前を入力します。

ステップ 4　[Server Name] フィールドまたは [IP Address] フィールドに、マウント ポイントを配置するサーバの名前または IP アドレスを入力します。

ステップ 5　[Mode] フィールドで、オプション ボタン（[Active] または [Passive]）をクリックして FTP モードを選択します。[Passive] モードを選択した場合、クライアントでは、FTP コントロール接続とデータ接続がともに起動します。サーバは、この接続をリッスンするポートの番号で応答します。

ステップ 6　FTP ファイル サーバへのディレクトリ パス名を [Path to Mount] フィールドに入力します。

ステップ 7　サーバに対するファイル システムのマウントを許可されているユーザの名前を、[User Name] フィールドに入力します。

ステップ 8　サーバに対するファイル システムのマウントを許可されているユーザのパスワードを、[Password] フィールドに入力します。

ステップ 9　[Confirm Password] フィールドにパスワードを再入力します。

ステップ 10　[OK] をクリックします。

[Add FTP Mount Point] ダイアログボックスが閉じます。

ステップ 11　[Apply] をクリックします。

マウント ポイントが ASA に追加され、その変更内容が実行コンフィギュレーションに保存されます。

ICMP アクセスの設定

デフォルトでは、IPv4 または IPv6 を使用して任意の ASA インターフェイスに ICMP パケットを送信できます。この項では、ASA への ICMP 管理アクセスを制限する方法について説明します。ASA への ICMP アクセスを許可するホストとネットワークのアドレスを制限することによって、ASA を攻撃から保護できます。

（注）　ICMP トラフィックに対して ASA の通過を許可する手順については、ファイアウォール コンフィギュレーション ガイドのを参照してください。Chapter 46, “Configuring Access Rules,”

この項は、次の内容で構成されています。

ICMP アクセスに関する情報

IPv6 の ICMP は、IPv4 の ICMP と同じ働きをします。ICMPv6 によって、ICMP 宛先到達不能メッセージなどのエラー メッセージや、ICMP エコー要求および応答メッセージのような情報メッセージが生成されます。また、IPv6 の ICMP パケットは、IPv6 のネイバー探索プロセスやパス MTU ディスカバリに使用されます。

ICMP 到達不能メッセージ タイプ（タイプ 3）の権限を常に付与することを推奨します。ICMP 到達不能メッセージを拒否すると、ICMP パス MTU ディスカバリがディセーブルになって、IPSec および PPTP トラフィックが停止することがあります。パス MTU ディスカバリの詳細については、RFC 1195 および RFC 1435 を参照してください。

ICMP ルールを設定していると、ASA では、ICMP トラフィックに対する最初の照合の後に、すべてのエントリを暗黙の拒否が使用されます。つまり、最初に一致したエントリが許可エントリである場合、ICMP パケットは引き続き処理されます。最初に一致したエントリが拒否エントリであるか、エントリに一致しない場合、ASA によって ICMP パケットは破棄され、syslog メッセージが生成されます。ICMP ルールが設定されていない場合は例外となります。その場合、許可文が想定されます。

ICMP アクセスのライセンス要件

次の表に、この機能のライセンス要件を示します。

モデル	ライセンス要件
すべてのモデル	基本ライセンス

ガイドラインと制限事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

IPv6 のガイドライン

IPv6 をサポートします。

その他のガイドライン

- ASA は、ブロードキャスト アドレス宛ての ICMP エコー要求に応答しません。
- ASA は、トラフィックが着信するインターフェイス宛ての ICMP トラフィックにのみ応答します。ICMP トラフィックは、インターフェイス経由で離れたインターフェイスに送信できません。
- ASA インターフェイスを ping できない場合は、**icmp** コマンドを使用して、IP アドレス用に ASA への ICMP をイネーブルにします。

デフォルト設定

デフォルトでは、IPv4 または IPv6 を使用して任意の ASA インターフェイスに ICMP パケットを送信できます。

ICMP アクセスの設定

ICMP アクセス ルールを設定するには、次の手順を実行します。

手順の詳細

ステップ 1　[Configuration] > [Device Management] > [Management Access] > [ICMP] の順に選択し、[Add] をクリックします。

ステップ 2　次の中から適切なオプション ボタンをクリックして、フィルタリングする IP トラフィックのバージョンを選択します。

- [Both]（IPv4 トラフィックと IPv6 トラフィックをフィルタリングする）
- [IPv4] のみ
- [IPv6] のみ

ステップ 3　[ICMP] テーブルにルールを挿入する場合は、挿入位置の下にあるルールを選択し、さらに [Insert] をクリックします。

右側のペインに [Create ICMP Rule] ダイアログボックスが表示されます。

ステップ 4　[ICMP Type] ドロップダウン リストから、このルールに使用する ICMP メッセージのタイプを選択します。

ステップ 5　ルールを適用する宛先 ASA のインターフェイスを、[Interface] リストから選択します。

ステップ 6　[IP Address] フィールドで、次のいずれかの操作を行います。

- ホストまたはネットワークの IP アドレスを入力します。
- [Any Address] をクリックし、ステップ 9 に進みます。

ステップ 7　[Mask] ドロップダウン リストから、ネットワーク マスクを選択します。

ステップ 8　[OK] をクリックします。

[Create ICMP Rule] ダイアログボックスが閉じます。

ステップ 9　（任意）ICMP の到達不能メッセージに対する制限は、次の各オプションを使用して設定します。ASA をホップの 1 つとして表示するトレースルートに対して ASA の通過を許可するためには、[Configuration] > [Firewall] > [Service Policy Rules] > [Rule Actions] > [Connection Settings] ダイアログボックスの [Decrement time to live for a connection] オプションをイネーブルにするほか、レート制限を大きくする必要があります。

- [Rate Limit] : 到達不能メッセージのレート制限を、1 秒あたり 1 ～ 100 の範囲で設定します。デフォルトは、1 秒あたり 1 メッセージです。
- [Burst Size] : バースト レートを 1 ～ 10 の範囲で設定します。このキーワードは、現在システムで使用されていないため、任意の値を選択できます。

ステップ 10　[Apply] をクリックします。

ICMP ルールが ASA に追加され、その変更内容が実行コンフィギュレーションに保存されます。

VPN トンネルを介した管理アクセスの設定

VPN トンネルがあるインターフェイスで終わっている場合に、別のインターフェイスにアクセスして ASA を管理する必要があれば、そのインターフェイスを管理アクセス インターフェイスとして識別できます。たとえば、外部インターフェイスから ASA に入る場合は、この機能を使用して、ASDM、SSH、Telnet、または SNMP 経由で内部インターフェイスに接続するか、外部インターフェイスから入るときに内部インターフェイスに ping を実行できます。管理アクセスは、IPsec クライアント、IPsec site-to-site、AnyConnect SSL VPN クライアントの VPN トンネル タイプ経由で行えます。

この項は、次の内容で構成されています。

管理インターフェイスのライセンス要件

次の表に、この機能のライセンス要件を示します。

モデル	ライセンス要件
すべてのモデル	基本ライセンス

ガイドラインと制限事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル モードでだけサポートされています。

ファイアウォール モードのガイドライン

ルーテッド モードでサポートされています。

IPv6 のガイドライン

IPv6 をサポートします。

その他のガイドライン

管理アクセス インターフェイスは 1 つだけ定義できます。

管理インターフェイスの設定

管理インターフェイスを設定するには、次の手順を実行します。

手順の詳細

ステップ 1　[Configuration] > [Device Management] > [Management Access] > [Management Interface] ペインの [Management Access Interface] ドロップダウン リストから、セキュリティ レベルの最も高いインターフェイス（内部インターフェイス）を選択します。

ステップ 2　[Apply] をクリックします。

管理インターフェイスが割り当てられ、変更内容が実行コンフィギュレーションに保存されます。

システム管理者用 AAA の設定

この項では、システム管理者の認証とコマンド許可をイネーブルにする方法について説明します。

システム管理者用 AAA に関する情報

この項では、システム管理者用 AAA について説明します。次の項目を取り上げます。

管理認証に関する情報

この項では、管理アクセスの認証について説明します。次の項目を取り上げます。

認証がある場合とない場合の CLI アクセスの比較

ASA へのログイン方法は、認証をイネーブルにしているかどうかによって異なります。

- [No Authentication]：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 パスワードを入力します。（SSH は認証なしでは使用できません）。ユーザ EXEC モードにアクセスします。
- [Authentication]：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。ユーザ EXEC モードにアクセスします。

ログイン後に特権 EXEC モードに入るには、**enable** コマンドを入力します。**enable** の動作は、認証をイネーブルにしているかどうかによって異なります。

- [No Authentication]：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。
- [Authentication]：enable 認証を設定している場合、ASA によってユーザ名とパスワードの入力が再度求められます。この機能は、ユーザが入力できるコマンドを判別するためにユーザ名が重要な役割を果たすコマンド許可を実行する場合に特に役立ちます。

ローカル データベースを使用する enable 認証の場合は、**enable** コマンドの代わりに **login** コマンドを使用できます。**login** によりユーザ名が維持されますが、認証をオンにするための設定は必要ありません。

認証がある場合とない場合の ASDM アクセスの比較

デフォルトでは、ユーザ名のフィールドはブランクにしたまま、パスワードのフィールドにイネーブル パスワードを指定すれば ASDM にログインできます。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ることに注意してください。

HTTP 認証を設定した場合は、ユーザ名をブランクのままにし、イネーブル パスワードを指定して ASDM を使用することはできなくなります。

スイッチから ASA サービス モジュールへのセッションの認証

スイッチから ASASM へのセッションの場合は（**session** コマンドを使用）、Telnet 認証を設定できます。スイッチから ASASM への仮想コンソール接続の場合は（**service-module session** コマンドを使用）、シリアル ポート認証を設定できます。

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、Telnet またはシリアル認証を管理コンテキストで設定した場合、認証はスイッチから ASASM へのセッションにも適用されます。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。

コマンド許可に関する情報

この項では、コマンド許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許可方式」（P.45-18）
- 「ユーザ クレデンシャルの維持について」（P.45-18）
- 「セキュリティ コンテキストとコマンド許可」（P.45-19）

サポートされるコマンド許可方式

次の 2 つのコマンド許可方式のいずれかを使用できます。

- ローカル特権レベル：ASA でコマンド特権レベルを設定します。ローカル ユーザ、RADIUS ユーザ、または LDAP ユーザ（LDAP 属性を RADIUS 属性にマッピングする場合）を CLI アクセスについて認証する場合、ASA はそのユーザをローカル データベース、RADIUS、または LDAP サーバで定義されている特権レベルに所属させます。ユーザは、割り当てられた特権レベル以下のコマンドにアクセスできます。すべてのユーザは、初めてログインするときに、ユーザ EXEC モード（レベル 0 または 1 のコマンド）にアクセスします。ユーザは、特権 EXEC モード（レベル 2 以上のコマンド）にアクセスするために再び **enable** コマンドで認証するか、**login** コマンドでログイン（ローカル データベースに限る）できます。

（注） ローカル データベース内にユーザが存在しなくても、また CLI 認証や **enable** 認証がない場合でも、ローカル コマンド許可を使用できます。代わりに、**enable** コマンドを入力するときにシステム イネーブル パスワードを入力すると、ASA によってレベル 15 に置かれます。次に、すべてのレベルのイネーブル パスワードを作成します。これにより、**enable** *n*（2 ～ 15）を入力したときに、ASA によってレベル *n* に置かれるようになります。これらのレベルは、ローカル コマンド許可を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」（P.45-28）を参照）。**enable** コマンドの詳細については、コマンド リファレンスを参照してください。

- TACACS+ サーバ特権レベル：TACACS+ サーバで、ユーザまたはグループが CLI アクセスについて認証した後で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+ サーバで検証されます。

ユーザ クレデンシャルの維持について

ユーザが ASA にログインする場合、ユーザ名とパスワードを入力して認証される必要があります。ASA は、同じセッションで後ほど認証が再び必要になる場合に備えて、これらのセッション クレデンシャルを保持します。

次の設定が行われている場合、ユーザはログイン時にローカル サーバだけで認証されればよいことになります。その後に続く許可では、保存されたクレデンシャルが使用されます。また、特権レベル 15 のパスワードの入力を求めるプロンプトが表示されます。特権モードを出るときに、ユーザは再び認証されます。ユーザの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 サーバは、ユーザ アクセスの認証を行うように設定されます。
- 特権レベル 15 のコマンド アクセスは、パスワードを要求するように設定されます。
- ユーザのアカウントは、シリアル許可専用（コンソールまたは ASDM へのアクセスなし）として設定されます。
- ユーザのアカウントは、特権レベル 15 のコマンド アクセス用に設定されます。

次の表に、ASA でのクレデンシャルの使用方法を示します。

必要なクレデンシャル	ユーザ名とパスワードによる認証	シリアル許可	特権モード コマンド許可	特権モード終了許可
ユーザ名	Yes	No	No	Yes

必要なクレデンシャル	ユーザ名とパスワードによる認証	シリアル許可	特権モード コマンド許可	特権モード終了許可
パスワード	Yes	No	No	Yes
特権モードのパスワード	No	No	Yes	No

セキュリティ コンテキストとコマンド許可

マルチ セキュリティ コンテキストでコマンド許可を実装する場合の重要な考慮点を次に示します。

- 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。

  コマンド許可を設定する場合は、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。この設定により、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許可を実行できます。

  セキュリティ コンテキストを切り替える場合、管理者は、ログイン時に指定したユーザ名で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可能性があることや、新しいコンテキストではコマンド許可がまったく設定されていない可能性があることを念頭に置いてください。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場合があることを管理者が理解していないと、混乱が生じる可能性があります。この動作は、次の仕組み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。これにより、enable_15 ユーザに対してコマンド許可が設定されていない場合や、enable_15 ユーザの許可が前のコンテキスト セッションでのユーザの許可と異なる場合に、混乱が生じる可能性があります。

  これは、発行される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限り有効となる、コマンド アカウンティングにも影響します。**changeto** コマンドの使用が許可されているすべての管理者は enable_15 ユーザ名を他のコンテキストで使用できるため、enable_15 ユーザ名でログインしたユーザをコマンド アカウンティング レコードで簡単に特定できるとは限りません。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は、enable_15 ユーザ名を使用していたユーザを追跡するために数台のサーバのデータを相関させる必要が生じます。

  コマンド許可を設定する場合は、次の点を考慮します。

  - **changeto** コマンドの使用が許可されている管理者は、実質的に、他のコンテキストそれぞれで enable_15 ユーザに許可されているすべてのコマンドを使用する許可を持ちます。
  - コンテキストごとに別々にコマンドを許可する場合は、**changeto** コマンドの使用許可を持つ管理者に対しても拒否されるコマンドが enable_15 ユーザ名でも拒否されることを、各コンテキストで確認してください。

  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許可を使用できません。

システム管理者用 AAA のライセンス要件

次の表に、この機能のライセンス要件を示します。

モデル	ライセンス要件
すべてのモデル	基本ライセンス

前提条件

AAA サーバまたはローカル データベースの前提条件

AAA サーバまたはローカル データベースでユーザを設定します。AAA サーバに、ASA と通信するように設定する必要があります。次の章を参照してください。

- AAA サーバ：該当する AAA サーバ タイプの章を参照してください。
- ローカル データベース：「ユーザ アカウントのローカル データベースへの追加」（P.33-3）を参照してください。

管理認証の前提条件

ASA において Telnet ユーザ、SSH ユーザ、または HTTP ユーザを認証できるようにするには、その前に ASA との通信を許可されている IP アドレスを特定する必要があります。ASASM の場合、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 ASASM へのセッションは Telnet セッションですが、Telnet アクセスの設定は不要です。詳細については、「ASDM、Telnet、または SSH の ASA アクセスの設定」（P.45-1）を参照してください。

ローカル コマンド許可の前提条件

- **enable** 認証を設定します（「CLI、ASDM、および enable コマンド アクセスの認証の設定」（P.45-22）を参照してください）。

  enable 認証は、ユーザが **enable** コマンドにアクセスした後にユーザ名を保持するためには不可欠です。

  あるいは、設定を必要としない **login** コマンド（これは、認証されている **enable** コマンドと同じでローカル データベースの場合に限る）を使用することもできます。このオプションは **enable** 認証ほど安全ではないため、お勧めしません。

  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。

- 次に示すユーザ タイプごとの前提条件を確認してください。
  - 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の特権レベルを 0 ～ 15 で設定します。
  - RADIUS ユーザ：ユーザの Cisco VSA CVPN3000-Privilege-Level を、0 ～ 15 の値で設定します。
  - LDAP ユーザ：ユーザを特権レベル 0 ～ 15 の間で設定し、次に「LDAP 属性マップの設定」（P.36-5）の説明に従って、LDAP 属性を Cisco VSA CVPN3000-Privilege-Level にマッピングします。

TACACS+ コマンド許可の前提条件

- CLI および **enable** 認証を設定します（「CLI、ASDM、および enable コマンド アクセスの認証の設定」（P.45-22）を参照）。

管理アカウンティングの前提条件

- CLI および **enable** 認証を設定します（「CLI、ASDM、および enable コマンド アクセスの認証の設定」（P.45-22）を参照）。

ガイドラインと制限事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

IPv6 のガイドライン

IPv6 をサポートします。

デフォルト設定

デフォルトのコマンド特権レベル

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

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

すべての特権レベルを表示する方法は、「ローカル コマンド特権レベルの表示」（P.45-29）を参照してください。

CLI、ASDM、および enable コマンド アクセスの認証の設定

CLI、ASDM、および enable コマンドの認証を要求することができます。

前提条件

- 「ASDM、Telnet、または SSH の ASA アクセスの設定」（P.45-1）に従って Telnet、SSH、または HTTP アクセスを設定します。
- SSH アクセスするためは、SSH 認証を設定する必要があります。デフォルトのユーザ名はありません。

手順の詳細

ステップ 1　**enable** コマンドを使用するユーザを認証する場合は、[Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authentication] の順に選択し、次のように設定を行います。

a. [Enable] チェックボックスを選択します。

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. （任意）AAA サーバを選択する場合は、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ローカル データベースが使用されるように ASA 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、ASA 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。

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場合は、[Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authentication] の順に選択し、次のように設定を行います。

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 ASA にアクセスする ASDM クライアントを認証します。HTTP 管理認証では、AAA サーバ グループの SDI プロトコルをサポートしていません。
- [Serial] : コンソール ポートを使用して ASA にアクセスするユーザを認証します。ASASM の場合、このパラメータは **service-module session** コマンドを使用してスイッチからアクセスする仮想コンソールにも影響します。マルチ モード アクセスについては、「スイッチから ASA サービス モジュールへのセッションの認証」（P.45-17）を参照してください。
- [SSH] : SSH を使用して ASA にアクセスするユーザを認証します。
- [Telnet] : Telnet を使用して ASA にアクセスするユーザを認証します。ASASM の場合、このパラメータは **session** コマンドを使用するスイッチからのセッションにも影響します。マルチ モード アクセスについては、「スイッチから ASA サービス モジュールへのセッションの認証」（P.45-17）を参照してください。

b. 対応するチェックボックスを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. （任意）AAA サーバを選択する場合は、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ローカル データベースが使用されるように ASA 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、ASA 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。

ステップ 3　[Apply] をクリックします。

管理許可によるユーザ CLI および ASDM アクセスの制限

ASA を使用すると、RADIUS、LDAP、TACACS+、またはローカル ユーザ データベースを使用して認証する場合に、管理ユーザとリモート アクセス ユーザを区別することができます。ユーザ ロールを区別することで、リモート アクセス VPN ユーザやネットワーク アクセス ユーザが ASA に管理接続を確立するのを防ぐことができます。

（注）　管理許可にはシリアル 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、認証されたユーザはすべて、コンソール ポートにアクセスできます。

手順の詳細

ステップ 1　管理許可をイネーブルにする場合は、[Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authorization] の順に選択し、[Perform authorization for exec shell access] > [Enable] チェックボックスをオンにします。

このオプションを選択すると、RADIUS の管理ユーザ特権レベルのサポートもイネーブルになります。管理ユーザ特権レベルは、ローカル コマンド特権レベルと組み合わせて、コマンド許可に使用できます。詳細については、「ローカル コマンド許可の設定」（P.45-28）を参照してください。

ステップ 2　ユーザを管理認証対象に設定するには、次の各 AAA サーバ タイプまたはローカル ユーザの要件を参照してください。

RADIUS または LDAP（マッピング済み）ユーザ

ユーザが LDAP 経由で認証される場合、ネイティブ LDAP 属性およびその値は Cisco ASA 属性にマッピングされ、特定の許可機能を提供します。Cisco VSA CVPN3000-Privilege-Level を、0 ～ 15 の値で設定します。次に、LDAP 属性を Cisco VAS CVPN3000-Privilege-Level にマッピングします。詳細については、「LDAP 属性マップの設定」（P.36-5）を参照してください。

RADIUS IETF の service-type 属性が、RADIUS 認証および許可要求の結果として access-accept メッセージで送信される場合、この属性は認証されたユーザにどのタイプのサービスを付与するかを指定するために使用されます。

- Service-Type 6（管理）: [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。
- Service-Type 7（NAS プロンプト）: Telnet 認証または SSH 認証のオプションを設定した場合は CLI へのアクセスを許可し、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 モニタリング アクセスは許可します。[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。
- Service-Type 5（発信）: 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いずれのサービスも使用できません（[Serial] オプションは除きます。つまり、シリアル アクセスは許可されます）。リモート アクセス（IPsec および SSL）ユーザは、引き続き自身のリモート アクセス セッションを認証および終了できます。

RADIUS Cisco VSA **privilege-level** 属性（ベンダー ID 3076、サブ ID 220）が access-accept メッセージで送信される場合は、ユーザの権限レベルを指定するために使用されます。

認証されたユーザが ASDM、SSH、または Telnet を使用して ASA に管理アクセスを試みたものの、これを実行するために必要な特権レベルを持っていないと、ASA から syslog メッセージ 113021 が生成されます。このメッセージは、管理者権限が不適切であるためログインに失敗したことをユーザに通知するものです。

TACACS+ ユーザ

「service=shell」で許可が要求され、サーバは PASS または FAIL で応答します。

- PASS（特権レベル 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（特権レベル 2 以上）：Telnet 認証または SSH 認証のオプションを設定した場合は CLI へのアクセスを許可し、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 モニタリング アクセスは許可します。[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。イネーブルの特権レベルが 14 以下に設定されている場合は、**enable** コマンドを使用して特権 EXEC モードにアクセスすることはできません。
- 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いずれのサービスも使用できません（[Serial] オプションは除きます。つまり、シリアル アクセスは許可されます）。

ローカル ユーザ

指定したユーザ名の [Access Restriction] オプションを設定します。アクセス制限のデフォルト値は [Full Access] です。この場合は、[Authentication] タブのオプションで指定されたすべてのサービスに対して、フル アクセスが許可されます。詳細については、「ユーザ アカウントのローカル データベースへの追加」（P.33-3）を参照してください。

ローカル データベース ユーザのパスワード ポリシーの設定

ローカル データベースを使用して CLI または ASDM アクセスの認証を設定する場合は、指定期間を過ぎるとユーザにパスワードの変更を要求し、パスワードの最短長と最低変更文字数などのパスワード標準に従うことを要求するパスワード ポリシーを設定することができます。

パスワード ポリシーはローカル データベースを使用する管理ユーザに対してのみ適用されます。ローカル データベースを使用するその他のタイプのトラフィック（VPN や AAA によるネットワーク アクセスなど）や、AAA サーバによって認証されたユーザには適用されません。

この項は、次の内容で構成されています。

パスワード ポリシーの設定

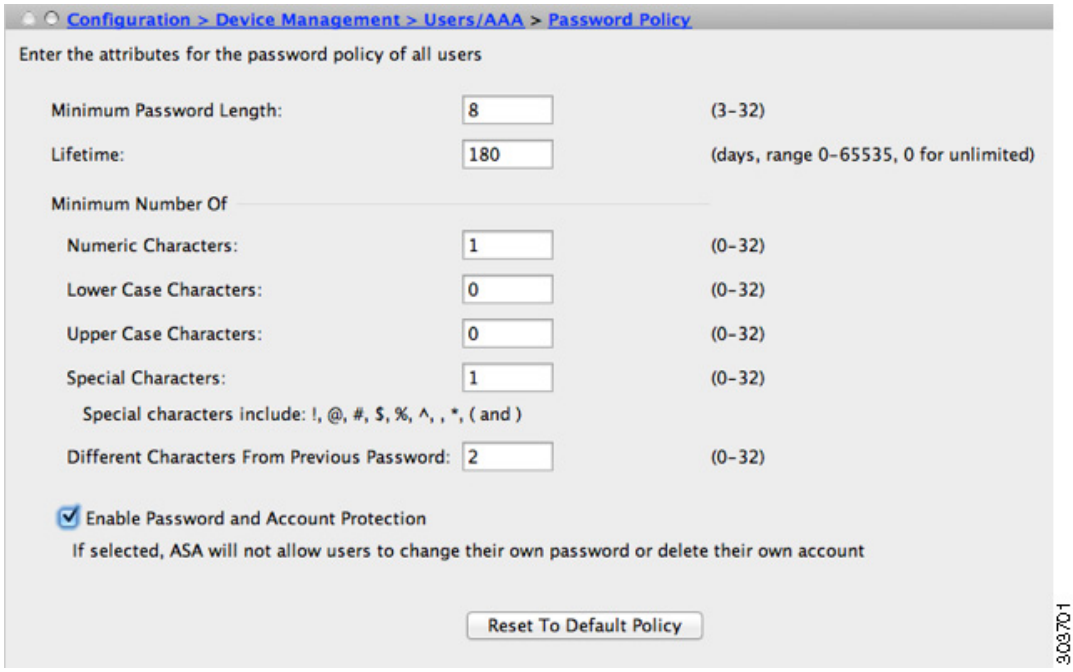
パスワード ポリシーの設定後は、自分または別のユーザのパスワードを変更すると、新しいパスワードに対してパスワード ポリシーが適用されます。あらゆる既存のパスワードは、対象外です。新しいポリシーは、[User Accounts] ペインまたは [Change My Password] ペインによるパスワードの変更に適用されます。

前提条件

- 「CLI、ASDM、および enable コマンド アクセスの認証の設定」（P.45-22）に従って、CLI/ASDM および enable 認証の両方を設定します。ローカル データベースの指定を忘れないでください。

手順の詳細

ステップ 1　**[Configuration] > [Device Management] > [Users/AAA] > [Password Policy]** の順に選択します。



ステップ 2　次のオプションを任意に組み合わせて設定します。

- [Minimum Password Length]：パスワードの最短長を入力します。有効値の範囲は 3 ～ 64 文字です。推奨されるパスワードの最小長は 8 文字です。
- [Lifetime]：リモート ユーザ（SSH、Telnet、HTTP）のパスワードの有効期間を日数で指定します。コンソール ポートのユーザが、パスワードの有効期限切れでロックされることはありません。有効な値は、0 ～ 65536 です。デフォルト値は 0 日です。この場合、パスワードは決して期限切れになりません。

  パスワードの有効期限が切れる 7 日前に、警告メッセージが表示されます。パスワードの有効期限が切れると、リモート ユーザのシステム アクセスは拒否されます。有効期限が切れた後アクセスするには、次のいずれかの手順を実行します。
  - 他の管理者にパスワードを変更してもらいます。
  - 物理コンソール ポートにログインして、パスワードを変更します。
- [Minimum Number Of]：次のタイプの最短文字数を指定します。
  - [Numeric Characters]：パスワードに含まれなければならない数字の最短文字数を入力します。有効な値は、0 ～ 64 文字です。デフォルト値は 0 です
  - [Lower Case Characters]：パスワードに含まれなければならない小文字の最短文字数を入力します。有効値の範囲は 0 ～ 64 文字です。デフォルト値は 0 です
  - [Upper Case Characters]：パスワードに含まれなければならない大文字の最短文字数を入力します。有効値の範囲は 0 ～ 64 文字です。デフォルト値は 0 です
  - [Special Characters]：パスワードに含まれなければならない特殊文字の最短文字数を入力します。有効値の範囲は 0 ～ 64 文字です。特殊文字には、!、@、#、$、%、^、&、*、「(」、「)」があります。デフォルト値は 0 です。
  - [Different Characters from Previous Password]：新しいパスワードと古いパスワードで違わなければならない最小文字数を入力します。有効な値は、0 ～ 64 文字です。デフォルト値は 0 です 文字マッチングは位置に依存しません。したがって、新しいパスワードで使用される文字が、現在のパスワードのどこにも使用されていない場合に限り、パスワードが変更されたとみなされます。

ステップ 3　（任意）[Enable Authentication] チェックボックスをオンにして、ユーザが [User Accounts] ペインではなく、[Change My Password] ペインでパスワードを変更するようにします。デフォルト設定はディセーブルです。どちらの方法でも、ユーザはパスワードを変更することができます。

この機能をイネーブルにすると、[User Accounts] ペインでパスワードを変更しようとしても、次のエラー メッセージが表示されます。

```
ERROR: Changing your own password is prohibited
```

ステップ 4　パスワード ポリシーをデフォルトにリセットするには、[Reset to Default] をクリックします。

ステップ 5　[Apply] をクリックして、設定を適用します。

パスワードの変更

パスワード ポリシーでパスワードの有効期間を設定した場合、有効期間を過ぎるとパスワードを新しいパスワードに変更する必要があります。パスワード ポリシー認証をイネーブルにした場合は、このパスワード変更のスキームが必須です。パスワード ポリシー認証がイネーブルでない場合は、このメソッドを使用することも、[User Accounts] ペインから直接ユーザ アカウントを変更することもできます。

手順の詳細

ステップ 1　[Configuration] > [Device Management] > [Users/AAA] > [Change Password] の順に選択します。

ステップ 2　古いパスワードを入力します。

ステップ 3　新しいパスワードを入力します。

ステップ 4　確認のために新しいパスワードを再度入力します。

ステップ 5　[Make Change] をクリックします。

ステップ 6　[Save] アイコンをクリックして、実行コンフィギュレーションに変更を保存します。

コマンド許可の設定

コマンドへのアクセスを制御する場合、ASA ではコマンド許可を設定でき、ユーザが使用できるコマンドを決定できます。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。

次の 2 つのコマンド許可方式のいずれかを使用できます。

- ローカル特権レベル
- TACACS+ サーバ特権レベル

このコマンド許可の詳細については、「コマンド許可に関する情報」（P.45-17）を参照してください。

この項は、次の内容で構成されています。

- 「TACACS+ コマンド許可の設定」（P.45-32）

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して、コマンドを 16 の特権レベル（0 ～ 15）の 1 つ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 に割り当てられます。各ユーザを特定の特権レベルに定義でき、各ユーザは割り当てられた特権レベル以下のコマンドを入力できます。ASA は、ローカル データベース、RADIUS サーバ、または LDAP サーバ（LDAP 属性を RADIUS 属性にマッピングする場合）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。詳細については、次の項を参照してください。

- 「ユーザ アカウントのローカル データベースへの追加」（P.33-3）
- 「サポートされている認証方式」（P.34-1）
- 「LDAP 属性マップの設定」（P.36-5）

ローカル コマンド許可を設定するには、次の手順を実行します。

手順の詳細

ステップ 1　コマンド許可をイネーブルにする場合は、[Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authorization] の順に選択し、[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 コマンド許可をイネーブルにすると、オプションで、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たり、事前定義済みユーザ アカウント特権をイネーブルにしたりできます。

- 事前定義済みユーザ アカウント特権を使用する場合は、[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。[Yes] をクリックすると、事前定義済みユーザ アカウント特権を使用できるようになります。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 アクセス権）、[Read Only]（特権レベル 5、読み取り専用アクセス権）、[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場合は、[Configure Command Privileges] 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。代わりに、コンフィギュレーション モードを選択し、そのモードで使用可能なコマンドを表示することもできます。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すべてのコマンドを表示できます。コンフィギュレーション モードだけでなく、ユーザ EXEC モードや特権 EXEC モードでも入力が可能で、かつモードごとに異なるアクションが実行されるようなコマンドを使用する場合は、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。特権は、コマンドの show 形式、clear 形式、または configure 形式に対してのみ設定できます。コマンドの configure 形式は、通常、未修正コマンド（**show** または **clear** プレフィックスなしで）または **no** 形式として、コンフィギュレーションの変更を引き起こす形式です。

  コマンドのレベルを変更する場合は、コマンドをダブルクリックするか、[Edit] をクリックします。レベルは 0 ～ 15 の範囲で設定できます。設定できるのは、*main* コマンドの特権レベルだけです。たとえば、すべての **aaa** コマンドのレベルを設定できますが、**aaa authentication** コマンドと **aaa authorization** コマンドのレベルを個別に設定できません。

表示されているすべてのコマンドのレベルを変更する場合は、[Select All] をクリックした後に、[Edit] をクリックします。

[OK] をクリックして変更内容を確定します。

ステップ 4　RADIUS の管理ユーザ特権レベルをサポートする場合は、[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、ASA ではローカル データベース ユーザの特権レベルだけがサポートされ、他のタイプのユーザにはデフォルトのレベル 15 がそのまま適用されます。

また、このオプションを設定すると、ローカル ユーザ、RADIUS ユーザ、マッピング済み LDAP ユーザ、TACACS+ ユーザに対する管理許可がイネーブルになります。詳細については、「管理許可によるユーザ CLI および ASDM アクセスの制限」（P.45-23）を参照してください。

ステップ 5　[Apply] をクリックします。

許可設定が割り当てられ、その変更内容が実行コンフィギュレーションに保存されます。

ローカル コマンド特権レベルの表示

次のコマンドを [Tools] > [Command Line Interface tool] に入力すると、コマンドの特権レベルを表示できます。

TACACS+ サーバでのコマンドの設定

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

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

- ASA は、「シェル」コマンドとして許可するコマンドを送信し、TACACS+ サーバでシェル コマンドとしてコマンドを設定します。

（注） Cisco Secure ACS には、「pix-shell」と呼ばれるコマンド タイプが含まれている場合があります。このタイプは ASA コマンド許可に使用しないでください。

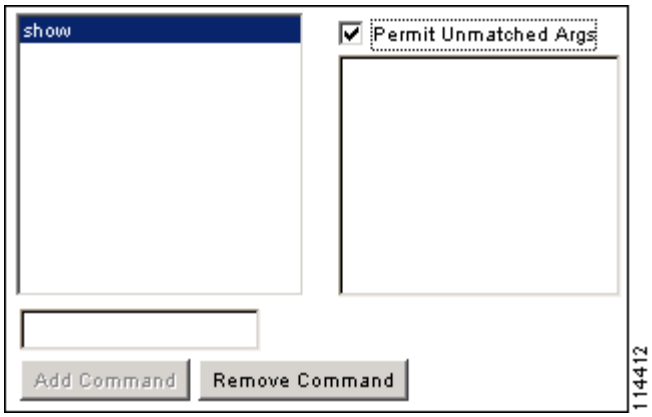
- コマンドの最初のワードは、メイン コマンドと見なされます。その他のワードはすべて引数と見なされます。これは、**permit** または **deny** の後に置く必要があります。

  たとえば、**show running-configuration aaa-server** コマンドを許可するには、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オンにすると、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。

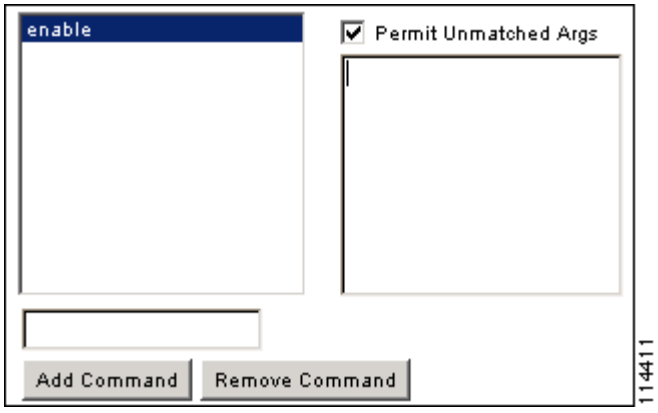
  たとえば、特定の **show** コマンドを設定するだけで、すべての **show** コマンドが許可されます。CLI の使用法を示す疑問符や省略形など、コマンドの変形をすべて予想する必要がなくなるので、この方法を使用することをお勧めします（図 45-1 を参照）。

図 45-1　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 45-2 を参照）。

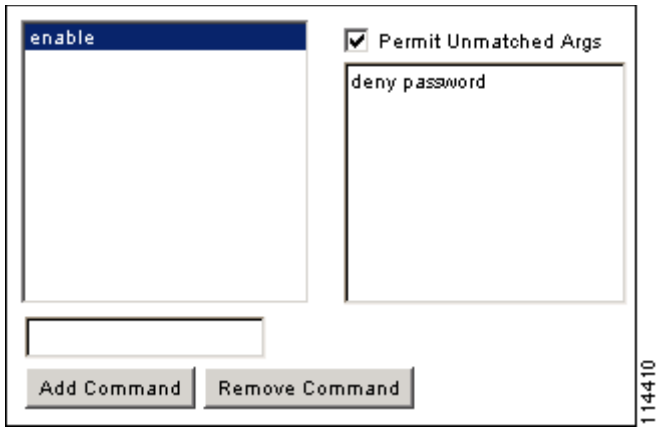
図 45-2　単一ワードのコマンドの許可



- 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 45-3 を参照）。

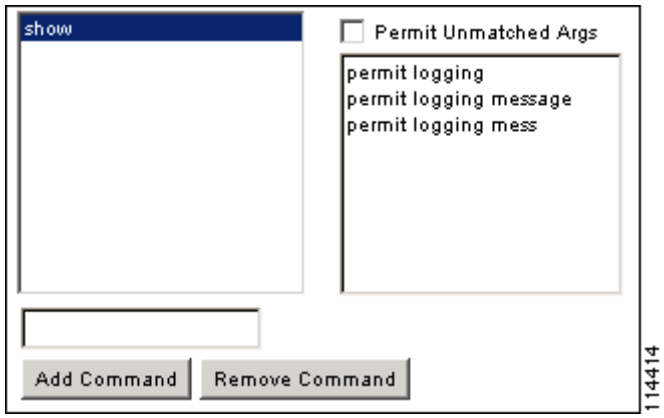
図 45-3　引数の拒否



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

  たとえば、**sh log** と入力すると、ASA 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、ASA 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 45-4 を参照）。

図 45-4　省略形の指定



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

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

TACACS+ コマンド許可の設定

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

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

意図したとおりに機能することが確認できるまで、設定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 ASA 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.45-35）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 ASA への完全冗長接続が必要です。たとえば、TACACS+ サーバ プールに、インターフェイス 1 に接続された 1 つのサーバとインターフェイス 2 に接続された別のサーバを含めます。TACACS+ サーバが使用できない場合にフォールバック方式としてローカル コマンド許可を設定することもできます。この場合は、「コマンド許可の設定」（P.45-27）に示されている手順に従ってローカル 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。

TACACS+ コマンド許可を設定するには、次の手順を実行します。

手順の詳細

ステップ 1　TACACS+ サーバを使用したコマンド許可を実行する場合は、[Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authorization] の順に選択し、[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　（任意）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ローカル データベースが使用されるように ASA を設定できます。設定するには、[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、ASA 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。必ずローカル データベースのユーザ（「ユーザ アカウントのローカル データベースへの追加」（P.33-3）を参照）とコマンド特権レベル（「ローカル コマンド許可の設定」（P.45-28）を参照）を設定してください。

ステップ 4　[Apply] をクリックします。

コマンド許可設定が割り当てられ、その変更内容が実行コンフィギュレーションに保存されます。

管理アクセス 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。ユーザがログインするとき、ユーザが **enable** コマンドを入力するとき、またはユーザがコマンドを発行するときのアカウンティングを設定できます。

コマンド アカウンティングに使用できるサーバは、TACACS+ だけです。

管理アクセスおよびイネーブル 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。

手順の詳細

ステップ 1　ユーザが **enable** コマンドを入力した場合にその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. [Configuration] > [Device Management] > [Users/AAA] >[AAA Access] > [Accounting] の順に選択し、[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 サーバ グループまたは TACACS+ サーバ グループの名前を選択します。

ステップ 2　ユーザが Telnet、SSH、またはシリアル コンソールを使用して ASA にアクセスした場合にその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] 領域で、[Serial]、[SSH]、[Telnet] の中から目的の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 サーバ グループまたは TACACS+ サーバ グループの名前を選択します。

ステップ 3　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] 領域で、[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、TACACS+ サーバ グループの名前を選択します。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。

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際、[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、ASA のアカウンティング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、ASA で処理の対象となりません。

ステップ 4　[Apply] をクリックします。

アカウンティング設定が割り当てられ、その変更内容が実行コンフィギュレーションに保存されます。

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､[Tools] > [Command Line Interface tool] で次の入力をします。

```
hostname# show curpriv
```

例

次に、**show curpriv** コマンドの出力例を示します。

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

表 45-1 に、**show curpriv** コマンドの出力の説明を示します。

表 45-1　show curpriv コマンド出力の説明

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	レベルの範囲は 0 ～ 15 です。ローカル コマンド許可を設定してコマンドを中間特権レベルに割り当てない限り、使用されるレベルはレベル 0 と 15 だけです。
Current Modes	使用可能なアクセス モードは次のとおりです。 • 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

管理セッション割り当て量の設定

同時に実行できる管理セッションの最大数を設定できます。この最大値に達すると、それ以降のセッションは許可されず、syslog メッセージが生成されます。システム ロックアウトを回避するために、管理セッション割り当て量のメカニズムではコンソール セッションをブロックできません。

管理セッションのクォータを設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Device Management] > [Management Access] > [Management Access Quota] を選択します。

ステップ 2　ASA で許可される ASDM、SSH、および Telnet の同時セッションの最大数を入力します。有効値の範囲は 0 ～ 10000 です。

（注）　クォータ管理セッション数を超えた場合、エラー メッセージが表示され、ASDM が閉じます。

ステップ 3　設定の変更を保存するには、[Apply] をクリックします。

ロックアウトからの回復

状況によっては、コマンド許可や CLI 認証をオンにすると、ASA CLI からロックアウトされる場合があります。通常は、ASA 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 45-2 に、一般的なロックアウト条件と回復方法を示します。

表 45-2　CLI 認証およびコマンド許可のロックアウト シナリオ

機能	ロックアウト条件	説明	対応策：シングル モード	対応策：マルチ モード
ローカル CLI 認証	ローカル データベースにユーザが設定していない。	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 ASA へのセッションを接続します。システム実行スペースから、コンテキストに切り替えてユーザを追加することができます。
TACACS+ コマンド許可 TACACS+ CLI 認証 RADIUS CLI 認証	サーバがダウンしているか到達不能で、フォールバック方式を設定していない。	サーバが到達不能である場合は、ログインもコマンドの入力もできません。	1. ログインし、パスワードと AAA コマンドをリセットします。 2. サーバがダウンしたときにロックアウトされないように、ローカル データベースをフォールバック方式として設定します。	1. ASA でネットワーク コンフィギュレーションが正しくないためサーバが到達不能である場合は、スイッチから ASA へのセッションを接続します。システム実行スペースから、コンテキストに切り替えてネットワークを再設定することができます。 2. サーバがダウンしたときにロックアウトされないように、ローカル データベースをフォールバック方式として設定します。
TACACS+ コマンド許可	十分な特権のないユーザまたは存在しないユーザとしてログインした。	コマンド許可がイネーブルになりますが、ユーザはこれ以上コマンドを入力できなくなります。	TACACS+ サーバのユーザ アカウントを修正します。 TACACS+ サーバへのアクセス権がなく、ASA 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 ASA へのセッションを接続します。システム実行スペースから、コンテキストに切り替えてコンフィギュレーションの変更を完了することができます。また、TACACS+ コンフィギュレーションを修正するまでコマンド許可をディセーブルにすることもできます。
ローカル コマンド許可	十分な特権のないユーザとしてログインしている。	コマンド許可がイネーブルになりますが、ユーザはこれ以上コマンドを入力できなくなります。	ログインし、パスワードと **aaa** コマンドをリセットします。	スイッチから ASA へのセッションを接続します。システム実行スペースから、コンテキストに切り替えてユーザ レベルを変更することができます。

デバイス アクセスのモニタリング

デバイス アクセスをモニタするには、次のペインを参照してください。

パス	目的
[Monitoring] > [Properties] > [Device Access] > [ASDM/HTTPS/Telnet/SSH Sessions]	上部ペインには、ASDM、HTTPS、および Telnet のセッションを介して接続するユーザの接続タイプ、セッション ID、および IP アドレスが示されます。特定のセッションを切断するには、[Disconnect] をクリックします。 下部ペインには、クライアント、ユーザ名、接続ステータス、ソフトウェア バージョン、入力暗号化タイプ、出力暗号化タイプ、入力 HMAC、出力 HMAC、SSH セッション ID、残りのキー データ、残りのキー再生成時間、データベースのキー再生成、時間ベース キー再生成、最後のキー再生成の時間が表示されます。特定のセッションを切断するには、[Disconnect] をクリックします。
[Monitoring] > [Properties] > [Device Access] > [Authenticated Users]	AAA サーバによって認証されるユーザのユーザ名、IP アドレス、ダイナミック ACL、非アクティブ タイムアウト（ある場合）、および絶対タイムアウトが示されます。
[Monitoring] > [Properties] > [Device Access] > [AAA Local Locked Out Users]	ロックアウトされた AAA ローカル ユーザのユーザ名、失敗した認証の試行回数、およびユーザがロックアウトされた回数が示されます。ロックアウトされた特定のユーザをクリアするには、[Clear Selected Lockout] をクリックします。ロックアウトされたすべてのユーザをクリアするには、[Clear All Lockouts] をクリックします。

管理アクセスの機能履歴

表 45-3 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 45-3　管理アクセスの機能履歴

機能名	プラットフォーム リリース	機能情報
管理アクセス	7.0(1)	この機能が導入されました。 次の画面が導入されました。 [Configuration] > [Device Management] > [Management Access] > [ASDM/HTTPS/Telnet/SSH]。 [Configuration] > [Device Management] > [Management Access] > [Command Line (CLI)] >[Banner]。 [Configuration] > [Device Management] > [Management Access] > [CLI Prompt]。 [Configuration] > [Device Management] > [Management Access] > [ICMP]。 [Configuration] > [Device Management] > [Management Access] > [File Access] >[FTP Client]。 [Configuration] > [Device Management] > [Management Access] > [File Access] >[Secure Copy (SCP) Server]。 [Configuration] > [Device Management] > [Management Access] > [File Access] >[Mount-Points]。 [Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authentication]。 [Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authorization]。 [Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Accounting]。
SSH セキュリティが向上し、SSH デフォルト ユーザ名はサポートされなくなりました。	8.4(2)	8.4(2) 以降、pix または asa ユーザ名とログイン パスワードで SSH を使用して ASA に接続することができなくなりました。SSH を使用するには、**aaa authentication ssh console LOCAL** コマンド（CLI）または [Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authentication (ASDM)] を使用して AAA 認証を設定してから、ローカル ユーザを定義する必要があります。定義するには、**username** コマンド（CLI）を入力するか、[Configuration] > [Device Management] > [Users/AAA] > [User Accounts (ASDM)] を選択します。ローカル データベースの代わりに AAA サーバを認証に使用する場合、ローカル認証もバックアップの手段として設定しておくことをお勧めします。

表 45-3　管理アクセスの機能履歴 （続き）

機能名	プラットフォーム リリース	機能情報
ローカル データベースを使用する場合の管理者パスワード ポリシーのサポート	8.4(4.1)、9.1(2)	ローカル データベースを使用して CLI または ASDM アクセスの認証を設定する場合は、指定期間を過ぎるとユーザにパスワードの変更を要求し、パスワードの最短長と最低変更文字数などのパスワード標準に従うことを要求するパスワード ポリシーを設定することができます。 次の画面が導入されました。[Configuration] > [Device Management] > [Users/AAA] > [Password Policy]。
SSH 公開キー認証のサポート	8.4(4.1)、9.1(2)	ASA への SSH 接続の公開キー認証は、ユーザ単位でイネーブルにできます。公開キー ファイル（PKF）でフォーマットされたキーまたは Base64 キーを指定できます。PKF キーは、4096 ビットまで使用できます。Base64 形式（最大 2048 ビット）の ASA サポートには大きすぎるキーには、PKF 形式を使用します。 次の画面が導入されました。 [Configuration] > [Device Management] > [Users/AAA] > [User Accounts] > [Edit User Account] > [Public Key Authentication] [Configuration] > [Device Management] > [Users/AAA] > [User Accounts] > [Edit User Account] > [Public Key Using PKF]。 *PKF キー形式のサポートは 9.1(2) 以降のみです。*
SSH キー交換の Diffie-Hellman グループ 14 のサポート	8.4(4.1)、9.1(2)	SSH キー交換に Diffie-Hellman グループ 14 が追加されました。これまでは、グループ 1 だけがサポートされていました。 次の画面が変更されました。[Configuration] > [Device Management] > [Management Access] > [ASDM/HTTPS/Telnet/SSH]。
管理セッションの最大数のサポート	8.4(4.1)、9.1(2)	同時 ASDM、SSH、Telnet セッションの最大数を設定することができます。 次の画面が導入されました。[Configuration] > [Device Management] > [Management Access] > [Management Session Quota]。
マルチ コンテキスト モードの ASASM において、スイッチからの Telnet 認証および仮想コンソール認証をサポートしました。	8.5(1)	マルチ コンテキスト モードのスイッチから ASASM への接続はシステム実行スペースに接続しますが、これらの接続を制御するために管理コンテキストでの認証を設定できます。
SSH の AES-CTR 暗号化	9.1(2)	ASA での SSH サーバの実装が、AES-CTR モードの暗号化をサポートするようになりました。
SSH キー再生成間隔の改善	9.1(2)	SSH 接続は、接続時間 60 分間またはデータ トラフィック 1 GB ごとに再生成されます。 。