
# 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.40-13）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、**aaa authentication ssh console LOCAL** コマンドを使用して AAA 認証を設定し、**username** コマンドを入力してローカル 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.40-1）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。

# Telnet アクセスの設定

クライアント IP アドレスを、ASA に Telnet 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

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **telnet** *source_IP_address mask source_interface*<br><br>**例：**<br>`hostname(config)# telnet 192.168.1.2 255.255.255.255 inside` | アドレスまたはサブネットごとに、ASA が接続を許可する IP アドレスを指定します。<br><br>インターフェイスが 1 つしかない場合は、インターフェイスのセキュリティ レベルが 100 である限り、そのインターフェイスにアクセスするように Telnet を設定することができます。 |
| ステップ 2 | **telnet timeout** *minutes*<br><br>**例：**<br>`hostname(config)# telnet timeout 30` | ASA がセッションを切断するまでに Telnet がアイドル状態を維持する時間の長さを設定します。<br><br>タイムアウトは 1 ～ 1440 分に設定します。デフォルトは 5 分です。デフォルトの期間では一般に短すぎるので、実働前のテストとトラブルシューティングがすべて完了するまでは、長めに設定しておいてください。 |

### 例

次の例は、アドレスが 192.168.1.2 の内部インターフェイスのホストで ASA にアクセスする方法を示しています。

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

次の例は、192.168.3.0 のネットワーク上のすべてのユーザが内部インターフェイス上の ASA にアクセスできるようにする方法を示しています。

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

# 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、**password** コマンドで設定したログイン パスワードを入力します。Telnet 認証を設定している場合（「CLI および ASDM アクセス認証の設定」（P.40-20）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 アクセスの設定

クライアント IP アドレスを指定して、ASA に SSH を使用して接続できるユーザを定義するには、次の手順を実行します。

### 手順の詳細

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **crypto key generate rsa modulus** *modulus_size*<br><br>**例：**<br>`hostname(config)# crypto key generate rsa modulus 1024` | RSA キー ペアを生成します。これは、SSH で必要です。<br>係数の値（ビット単位）は 512、768、1024、または 2048 です。指定するキー係数のサイズが大きいほど、RSA キー ペアの生成にかかる時間は長くなります。値は 1024 にすることをお勧めします。 |
| ステップ 2 | **write memory**<br><br>**例：**<br>`hostname(config)# write memory` | RSA キーを永続的なフラッシュ メモリに保存します。 |
| ステップ 3 | **aaa authentication ssh console LOCAL** | SSH アクセスのローカル認証をイネーブルにします。AAA サーバを使用して認証を設定することもできます。詳細については、「CLI および ASDM アクセス認証の設定」（P.40-20）を参照してください。 |
| ステップ 4 | username *username* **password** *password* | SSH アクセスに使用できるユーザをローカル データベースに作成します。 |
| ステップ 5 | **ssh** *source_IP_address mask source_interface*<br><br>**例：**<br>`hostname(config)# ssh 192.168.3.0 255.255.255.0 inside` | アドレスまたはサブネットごとに、ASA が接続を許可する IP アドレスと、SSH を実行するインターフェイスを指定します。Telnet と異なり、SSH は最も低いセキュリティ レベルのインターフェイスで実行できます。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 6 | （任意）<br>**ssh timeout** *minutes*<br><br>**例：**<br>hostname(config)# ssh timeout 30 | ASA がセッションを切断するまでに SSH がアイドル状態を維持する時間の長さを設定します。<br>タイムアウトは 1 ～ 60 分に設定します。デフォルトは 5 分です。デフォルトの期間では一般に短すぎるので、実働前のテストとトラブルシューティングがすべて完了するまでは、長めに設定しておいてください。 |
| ステップ 7 | （任意）<br>**ssh version** *version_number*<br><br>**例：**<br>hostname(config)# ssh version 2 | SSH バージョン 1 または 2 へのアクセスを制限します。デフォルトでは、SSH はバージョン 1 と 2 の両方を許可します。 |

**例**

次の例は、RSA キーを生成し、アドレスが 192.168.1.2 の内部インターフェイス上のホストで ASA にアクセスする方法を示しています。

```
hostname(config)# crypto key generate rsa modulus 1024
hostnamehostname(config)# write memory
hostname(config)# aaa authentication ssh console LOCAL
WARNING: local database is empty!Use 'username' command to define local users.
hostname(config)# username exampleuser1 password examplepassword1
hostname(config)# ssh 192.168.1.2 255.255.255.255 inside
hostname(config)# ssh timeout 30
```

次の例は、192.168.3.0 のネットワーク上のすべてのユーザが内部インターフェイス上の ASA にアクセスできるようにする方法を示しています。

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

# SSH クライアントの使用

管理ホストの SSH クライアントで、「SSH アクセスの設定」（P.40-4）で設定した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。

# ASDM での HTTPS アクセスの設定

ASDM を使用するには、HTTPS サーバをイネーブルにし、ASA への HTTPS 接続を許可する必要があります。HTTPS アクセスは、工場出荷時のデフォルト設定の一部として、または **setup** コマンドを使用したときにイネーブルになっています。この項では、ASDM アクセスを手動で設定する方法について説明します。

ASDM への HTTPS アクセスを設定するには、次の手順を実行します。

### 手順の詳細

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **http** *source_IP_address mask source_interface*<br><br>**例：**<br>`hostname(config)# http 192.168.1.2 255.255.255.255 inside` | アドレスまたはサブネットごとに、ASA が HTTPS 接続を許可する IP アドレスを指定します。 |
| ステップ 2 | **http server enable** [*port*]<br><br>**例：**<br>`hostname(config)# http server enable 443` | HTTPS サーバをイネーブルにします。<br>デフォルトでは、*port* は 443 です。ポート番号を変更する場合は、必ず ASDM アクセス URL に変更したポート番号を含めてください。たとえば、ポート番号を 444 に変更する場合は、次のように入力します。<br>**https://10.1.1.1:444** |

### 例

次の例は、HTTPS サーバをイネーブルにし、アドレスが 192.168.1.2 の内部インターフェイス上のホストで ASDM にアクセスする方法を示しています。

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

次の例は、192.168.3.0 のネットワーク上のすべてのユーザが内部インターフェイス上の ASDM にアクセスできるようにする方法を示しています。

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

# 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

| コマンド | 目的 |
|---|---|
| **banner** {**exec** \| **login** \| **motd**} *text*<br><br>**例：**<br>hostname(config)# banner motd Welcome to $(hostname). | ユーザが最初に接続したとき（「今日のお知らせ」（**motd**））、ユーザがログインしたとき（**login**）、ユーザが特権 EXEC モードにアクセスしたとき（**exec**）のいずれかに表示するバナーを追加します。ユーザが ASA に接続すると、まず「今日のお知らせ」バナーが表示され、その後にログイン バナーとプロンプトが表示されます。ユーザが ASA に正常にログインすると、exec バナーが表示されます。<br><br>複数の行を追加する場合は、各行の前に **banner** コマンドを置きます。<br><br>バナー テキストに関する注意事項：<br>• スペースは使用できますが、CLI を使用してタブを入力することはできません。<br>• バナーの長さの制限は、RAM およびフラッシュ メモリに関するもの以外はありません。<br>• ASA のホスト名またはドメイン名は、**$(hostname)** 文字列と **$(domain)** 文字列を組み込むことによって動的に追加できます。<br>• システム コンフィギュレーションでバナーを設定する場合は、コンテキスト コンフィギュレーションで **$(system)** 文字列を使用することによって、コンテキスト内でそのバナー テキストを使用できます。 |

### 例

次は、「今日のお知らせ」バナーの追加方法の例です。

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

# 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。<br>• [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。<br>• [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。<br>• [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。<br>• [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。<br>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、次のコマンドを入力します。

| コマンド | 目的 |
|---|---|
| **prompt** {[**hostname**] [**context**] [**domain**] [**slot**] [**state**] [**priority**] [**cluster-unit**]}<br><br>**例：**<br>`hostname(config)# firewall transparent` | CLI プロンプトをカスタマイズします。 |

## 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

| コマンド | 目的 |
|---|---|
| **console timeout** *number*<br><br>**例：**<br>`hostname(config)# console timeout 0` | 特権セッションが終了するまでのアイドル時間を分単位（0 ～ 60）で指定します。デフォルトのタイムアウトは 0 であり、セッションがタイムアウトしないことを示します。 |

| モデル | ライセンス要件 |
|---|---|
| すべてのモデル | 基本ライセンス |

# 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 Chapter 6, “Configuring Access Rules,” 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。



## 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、次のいずれかのコマンドを入力します。

## 手順の詳細

| コマンド | 目的 |
|---|---|
| （IPv4 の場合）<br>**icmp** {**permit** \| **deny**} {**host** *ip_address* \| *ip_address mask* \| **any**} [*icmp_type*] *interface_name*<br><br>**例：**<br>hostname(config)# icmp deny host 10.1.1.15 inside | IPv4 ICMP アクセス ルールを作成します。*icmp_type* を指定しないと、すべてのタイプが識別されます。番号または名前を入力できます。ping を制御するには、echo-reply（0）（ASA からホストへ）または echo（8）（ホストから ASA へ）を指定します。ICMP タイプのリストについては、「ICMP タイプ」（P.44-16）を参照してください。 |
| （IPv6 の場合）<br>**ipv6 icmp** {**permit** \| **deny**} {*ipv6-prefix/prefix-length* \| **any** \| **host** *ipv6-address*} [*icmp-type*] *interface_name*<br><br>**例：**<br>hostname(config)# icmp permit host fe80::20d:88ff:feee:6a82 outside | IPv6 ICMP アクセス ルールを作成します。*icmp_type* を指定しないと、すべてのタイプが識別されます。番号または名前を入力できます。ping を制御するには、echo-reply（0）（ASA からホストへ）または echo（8）（ホストから ASA へ）を指定します。ICMP タイプのリストについては、「ICMP タイプ」（P.44-16）を参照してください。 |

## 例

次の例は、10.1.1.15 のホストを除くすべてのホストで内部インターフェイスへの ICMP の使用を許可する方法を示しています。

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

次の例は、次のコマンドを入力して、10.1.1.15 のアドレスを持つホストに内部インターフェイスへの ping だけを許可する方法を示しています。

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

次に、外部インターフェイスですべての ping 要求を拒否し、すべての packet-too-big メッセージを許可する（パス MTU ディスカバリをサポートするため）方法を示します。

```
hostname(config)# ipv6 icmp deny any echo-reply outside
hostname(config)# ipv6 icmp permit any packet-too-big outside
```

次の例は、ホスト 2000:0:0:4::2 またはプレフィックス 2001::/64 上のホストに対して外部インターフェイスへの ping を許可する方法を示しています。

```
hostname(config)# ipv6 icmp permit host 2000:0:0:4::2 echo-reply outside
hostname(config)# ipv6 icmp permit 2001::/64 echo-reply outside
hostname(config)# ipv6 icmp permit any packet-too-big outside
```

# 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、outside 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 Inside インターフェイスに接続するか、outside インターフェイスから入るときに Inside 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

| コマンド | 目的 |
|---|---|
| **management-access** *management_interface*<br><br>**例：**<br>`hostname(config)# management-access inside` | *management_interface* は、別のインターフェイスから ASA に入るときにアクセスする管理インターフェイスの名前を指定します。 |

# 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。システム管理者の AAA を設定する前に、まずCLI コンフィギュレーション ガイドの該当する AAA サーバの章に示されている手順に従ってローカル データベースまたは AAA サーバを設定します。

この項は、次の内容で構成されています。



## 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。

- Telnet の認証をイネーブルにしていない場合は、ユーザ名を入力しません。ログイン パスワード（**password** コマンドで設定）を入力します。SSH の場合は、ユーザ名とログイン 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。
- 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。

- enable 認証を設定していない場合は、**enable** コマンドを入力するときにシステム イネーブル パスワード（**enable password** コマンドで設定）を入力します。ただし、enable 認証を使用しない場合、**enable** コマンドを入力した後は、特定のユーザとしてログインしていません。ユーザ名を維持するには、enable 認証を使用してください。
- enable 認証を設定する場合（「特権 EXEC モードにアクセスするための認証の設定（enable コマンド）」（P.40-20）を参照）は、ASA によってユーザ名とパスワードの入力を求めるプロンプトが再度表示されます。この機能は、ユーザが入力できるコマンドを判別するためにユーザ名が重要な役割を果たすコマンド許可を実行する場合に特に役立ちます。

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。詳細については、「login コマンドによるユーザの認証」（P.40-21）を参照してください。

### 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、ブランクのユーザ名と **enable password** コマンドによって設定されたイネーブル パスワードを使用して ASDM にログインできます。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.40-16）
- 「ユーザ クレデンシャルの維持について」（P.40-16）
- 「セキュリティ コンテキストとコマンド許可」（P.40-17）

## 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.40-26）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 |
| 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

この機能により、次を使用できます。

- AAA サーバ：CLI コンフィギュレーション ガイドの該当する AAA サーバの章を参照してください。
- ローカル データベース：“Adding a User Account to the Local Database” section on page 32-4 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.40-1）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 および ASDM アクセス認証の設定」（P.40-20）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“Configuring LDAP Attribute Maps” section on page 32-4 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 認証を設定する（「CLI および ASDM アクセス認証の設定」（P.40-20）を参照）。
- **enable** 認証を設定する（「特権 EXEC モードにアクセスするための認証の設定（enable コマンド）」（P.40-20）を参照）。

### 管理アカウンティングの前提条件

- CLI 認証を設定する（「CLI および ASDM アクセス認証の設定」（P.40-20）を参照）。
- **enable** 認証を設定する（「特権 EXEC モードにアクセスするための認証の設定（enable コマンド）」（P.40-20）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.40-29）を参照してください。

# CLI および ASDM アクセス認証の設定

認証を設定するには、次のコマンドを入力します。

### 手順の詳細

| コマンド | 目的 |
|---|---|
| **aaa authentication** {**telnet** \| **ssh** \| **http** \| **serial**} **console** {**LOCAL** \| *server_group* [**LOCAL**]}<br><br>**例：**<br>`hostname(config)# aaa authentication telnet console LOCAL` | 管理アクセス用のユーザを認証します。**telnet** キーワードを使用すると、Telnet アクセスを制御できます。ASASM の場合、このキーワードは **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.40-15）を参照してください。<br><br>**ssh** キーワードを使用すると、SSH アクセスを制御できます。SSH のデフォルト ユーザ名である asa および pix は現在はサポートされていません。<br><br>**http** キーワードを使用すると、ASDM アクセスを制御できます。<br><br>**serial** キーワードを使用すると、コンソール ポート アクセスを制御できます。ASASM の場合、このキーワードは **service-module** 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.40-15）を参照してください。<br><br>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。<br><br>認証に AAA サーバ グループを使用する場合は、AAA サーバが使用できないときにローカル データベースをフォールバック方式として使用するように ASA を設定できます。サーバ グループ名の後ろに **LOCAL** を指定します（**LOCAL** は大文字と小文字を区別します）。ローカル データベースでは AAA サーバと同じユーザ名およびパスワードを使用することを推奨します。これは、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。<br><br>**LOCAL** だけを入力して、ローカル データベースを認証の主要方式として（フォールバックなしで）使用することもできます。 |

# 特権 EXEC モードにアクセスするための認証の設定（enable コマンド）

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

この項は、次の内容で構成されています。

## enable コマンドの認証の設定

ユーザが **enable** コマンドを入力したときに認証されるように、ASA を設定できます。詳細については、「認証がある場合とない場合の CLI アクセスの比較」（P.40-15）を参照してください。

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

| コマンド | 目的 |
|---|---|
| **aaa authentication enable console** {**LOCAL** \| *server_group* [**LOCAL**]}<br><br>**例：**<br>`hostname(config)# aaa authentication enable console LOCAL` | **enable** コマンドを入力したユーザを認証します。ユーザ名とパスワードの入力を求めるプロンプトがユーザに対して表示されます。<br><br>認証に AAA サーバ グループを使用する場合は、AAA サーバが使用できないときにローカル データベースをフォールバック方式として使用するように ASA を設定できます。サーバ グループ名の後ろに **LOCAL** を指定します（**LOCAL** は大文字と小文字を区別します）。ローカル データベースでは AAA サーバと同じユーザ名およびパスワードを使用することを推奨します。これは、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。<br><br>**LOCAL** だけを入力して、ローカル データベースを認証の主要方式として（フォールバックなしで）使用することもできます。 |

## login コマンドによるユーザの認証

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

この機能を使用すると、ユーザは独自のユーザ名とパスワードでログインして特権 EXEC モードにアクセスすることができるので、システム イネーブル パスワードを全員に提供する必要がなくなります。ユーザがログイン時に特権 EXEC モード（およびすべてのコマンド）にアクセスできるようにするには、ユーザの特権レベルを 2（デフォルト）～ 15 に設定します。ローカル コマンド許可を設定した場合、ユーザは、その特権レベル以下のレベルに割り当てられているコマンドのみを入力できます。詳細については、「ローカル コマンド許可の設定」（P.40-26）を参照してください。

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

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

| コマンド | 目的 |
|---|---|
| **login**<br><br>**例：**<br>`hostname# login` | ローカル データベースからユーザとしてログインします。ASA により、ユーザ名とパスワードの入力を求めるプロンプトが表示されます。パスワードを入力すると、ASA により、ユーザはローカル データベースで指定されている特権レベルに置かれます。 |

# 管理許可によるユーザ CLI および ASDM アクセスの制限

CLI 認証または **enable** 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 属性を RADIUS 属性にマッピングする場合）からの CLI、ASDM、または **enable** コマンドへのアクセスを制限できます。

**（注）** シリアル アクセスは管理認証に含まれないため、**aaa authentication serial console** コマンドを設定している場合は、認証し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

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **aaa authorization exec authentication-server**<br><br>**例：**<br>`hostname(config)# aaa authorization exec authentication-server` | ローカル、RADIUS、LDAP（マッピング済み）、および TACACS+ の各ユーザの管理許可をイネーブルにします。また、RADIUS から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。この特権レベルは、コマンド許可でのローカル コマンドの特権レベルと併用できます。詳細については、「ローカル コマンド許可の設定」（P.40-26）を参照してください。**aaa authorization exec LOCAL** コマンドを使用して、ローカル データベースから属性を取得できるようにします。 |
| 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。<br>• RADIUS または LDAP（マッピング済み）ユーザ：IETF RADIUS 数値型属性の Service-Type を使用します。この属性は、次のいずれかの値にマッピングされます<br>– Service-Type 6（管理）：**aaa authentication console** コマンドで指定されたサービスへのフル アクセスを許可します。<br>– Service-Type 7（NAS プロンプト）：**aaa authentication {telnet \| ssh} console** コマンドを設定した場合は CLI へのアクセスを許可しますが、**aaa authentication http console** コマンドを設定した場合は 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。**aaa authentication enable console** コマンドでイネーブル認証を設定している場合、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。<br>– Service-Type 5（発信）：管理アクセスを拒否します。ユーザは **aaa authentication console** コマンドで指定されたサービスを使用できません（**serial** キーワードを除きます。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。<br>Cisco VSA CVPN3000-Privilege-Level を、0 ～ 15 の値で設定します。次に、**ldap map-attributes** コマンドを使用して 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、“Configuring LDAP Attribute Maps” section on page 32-4 を参照してください。<br>• 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。<br>– PASS、特権レベル 1：設定およびモニタリング セクションへの限定的な読み取り専用アクセス権で ASDM へのアクセスと、権限レベル 1 の **show** コマンドのみへのアクセスを許可します。<br>– PASS、特権レベル 2 以上：**aaa authentication {telnet \| ssh} console** コマンドを設定した場合は CLI へのアクセスを許可しますが、**aaa authentication http console** コマンドを設定した場合は 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。**aaa authentication enable console** コマンドを使用して**イネーブル**認証を設定すると、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。<br>– FAIL：管理アクセスを拒否します。**aaa authentication console** コマンドで指定されたサービスは使用できません（**serial** キーワードを除きます。シリアル アクセスは許可されます）。<br>• ローカル ユーザ：**service-type** コマンドを設定します。デフォルトの **service-type** は **admin** で、**aaa authentication console** コマンドで指定されたサービスへのフル アクセスを許可します。0 ～ 15 の特権レベルでローカル データベース ユーザを設定するには、**username** コマンドを使用します。詳細については、“Adding a User Account to the Local Database” section on page 32-4 を参照してください。 |

# AAA によるユーザ ロールの区別

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。

ユーザ ロールを区別するには、ユーザ名コンフィギュレーション モードで **service-type** 属性を使用します。RADIUS および LDAP の場合（**ldap-attribute-map** コマンドを使用）、Cisco ベンダー固有属性（VSA）の Cisco-Priv-Level を使用して、認証済みのユーザに特権レベルを割り当てることができます。

この項は、次の内容で構成されています。



## ローカル認証の使用

ローカル認証を設定するには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **username** *name* {**password** *password*} [**privilege** *priv_level*]<br><br>**例：**<br>`hostname(config)# username admin password mysecret123 privilege 15` | ユーザを作成し、パスワードを指定して、特権レベルを割り当てます。<br><br>**mysecret123** エントリは、保存されているパスワードです。15 は割り当てられる特権レベルで、これは管理ユーザを表します。 |
| ステップ 2 | **service-type** {**admin** \| **nas-prompt** \| **remote-access**}<br><br>**例：**<br>`hostname(config-username)# service-type admin` | サービス タイプを指定します。<br><br>**admin** キーワードは、ユーザにコンフィギュレーション モードへのアクセスを許可します。このオプションでは、ユーザにリモート アクセス経由での接続が許可されます。**nas-prompt** keyword は、ユーザに EXEC モードへのアクセスを許可します。**remote-access** キーワードは、ユーザにネットワーク ユーザへのアクセスを許可します。 |

### 例

次の例では、admin という名前のユーザに service-type として **admin** を指定します。

```
hostname(config)# username admin attributes
hostname(config-username)# service-type admin
```

次の例では、ra-user という名前のユーザに service-type として **remote-access** を指定します。

```
hostname(config)# username ra-user attributes
hostname(config-username)# service-type remote-access
```

## RADIUS 認証の使用

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。サポートされる属性値は、administrative（6）、nas-prompt（7）、Framed（2）、および Login（1）です。認証と許可に使用できるサポートされている RADIUS IETF VSA のリストについては、Table 32-2 on page 32-12 を参照してください。

RADIUS 認証の使用の詳細については、“Configuring RADIUS Servers” section on page 32-14 を参照してください。Cisco Secure ACS のための RADIUS 認証の設定については、Cisco.com にある Cisco Secure ACS のマニュアルを参照してください。

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。許可に使用できるサポートされている RADIUS VSA のリストについては、Table 32-1 on page 32-3 を参照してください。

## LDAP 認証の使用

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。許可に使用できるサポートされている LDAP VSA のリストについては、Chapter 32, “Configuring LDAP Servers for AAA.” を参照してください。

LDAP 許可には、LDAP 属性マッピング機能を使用できます。この機能の例については、“Configuring Authorization with LDAP for VPN” section on page 32-11 を参照してください。

### 例

次の例は、LDAP 属性マップを定義する方法を示しています。この例では、セキュリティ ポリシーによって、LDAP によって認証されているユーザが、ユーザ レコードのフィールドまたはパラメータの title と company を、IETF-RADIUS service-type と privilege-level にそれぞれマップすることを指定しています。

```
hostname(config)# ldap attribute-map admin-control
hostname(config-ldap-attribute-map)# map-name title IETF-RADIUS-Service-Type
hostname(config-ldap-attribute-map)# map-name company Privilege-Level
```

次に、**ldap-attribute-map** コマンドの出力例を示します。

```
ldap attribute-map admin-control
    map-name company Privilege-Level
    map-name title IETF-Radius-Service-Type
```

次の例では、LDAP 属性マップを LDAP AAA サーバに適用します。

```
hostname(config)# aaa-server ldap-server (dmz1) host 10.20.30.1
hostname(config-aaa-server-host)# ldap-attribute-map admin-control
```

**（注）** 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+ 認証の使用

TACACS+ 認証を設定する方法については、“Adding an Authentication Prompt” section on page 32-6 を参照してください。

# 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.40-15）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。



## 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。

- “Adding a User Account to the Local Database” section on page 32-4
- “Supported Authentication Methods” section on page 32-2
- “Configuring LDAP Attribute Maps” section on page 32-4

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

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **privilege** [**show** \| **clear** \| **cmd**] **level** *level* [**mode** {**enable** \| **cmd**}] **command** *command*<br><br>**例：**<br>`hostname(config)# privilege show level 5 command filter` | 特権レベルにコマンドを割り当てます。<br>再割り当てする各コマンドに対してこのコマンドを繰り返します。<br>このコマンドのオプションは、次のとおりです。<br>• **show** \| **clear** \| **cmd**：これらのオプション キーワードを使用すると、コマンドの show、clear、または configure 形式に対してだけ特権を設定できます。コマンドの configure 形式は、通常、未修正コマンド（**show** または **clear** プレフィックスなしで）または **no** 形式として、コンフィギュレーションの変更を引き起こす形式です。これらのキーワードのいずれかを使用しない場合は、コマンドのすべての形式が影響を受けます。<br>• **level** *level*：0 ～ 15 のレベル。<br>• **mode** {**enable** \| **configure**}：ユーザ EXEC モードまたは特権 EXEC モードおよびコンフィギュレーション モードでコマンドを入力することができ、そのコマンドが各モードで異なるアクションを実行する場合は、それらのモードの特権レベルを個別に設定することができます。<br>– **enable**：ユーザ EXEC モードと特権 EXEC モードの両方を指定します。<br>– **configure**：**configure terminal** コマンドを使用してアクセスされるコンフィギュレーション モードを指定します。<br>• **command** *command*：設定しているコマンド。設定できるのは、*main* コマンドの特権レベルだけです。たとえば、すべての **aaa** コマンドのレベルを設定できますが、**aaa authentication** コマンドと **aaa authorization** コマンドのレベルを個別に設定できません。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 2 | **aaa authorization exec authentication-server**<br><br>**例：**<br>hostname(config)# aaa authorization exec authentication-server | RADIUS からの管理ユーザ特権レベルをサポートします。<br><br>管理アクセスを認証するユーザに、ユーザ固有のアクセス レベルを強制します（**aaa authentication console LOCAL** コマンドを参照）。<br><br>このコマンドを入力しない場合、ASA 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をすべてデフォルトでレベル 15 に割り当てます。<br><br>このコマンドは、ローカル、RADIUS、LDAP（マッピング済み）、および TACACS+ の各ユーザの管理許可もイネーブルにします。<br><br>**aaa authorization exec LOCAL** コマンドを使用して、ローカル データベースから属性を取得できるようにします。AAA サーバのユーザを管理許可が有効になるように設定する方法については、「管理許可によるユーザ CLI および ASDM アクセスの制限」（P.40-22）を参照してください。 |
| ステップ 3 | **aaa authorization command LOCAL**<br><br>**例：**<br>hostname(config)# aaa authorization command LOCAL | ローカル コマンドの特権レベルの使用をイネーブルにします。ローカル コマンドの特権レベルを使用すると、ローカル データベース、RADIUS サーバ、または LDAP サーバ（マッピングされた属性を持つ）のユーザの特権レベルと比較して検査できます。<br><br>コマンド特権レベルを設定する場合は、このコマンドでコマンド許可を設定しない限り、コマンド許可は実行されません。 |

## 例

**filter** コマンドの形式は次のとおりです。

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

特権レベルを形式ごとに個別に設定することができます。または、このオプションを省略してすべての形式に同じ特権レベルを設定することもできます。次は、各形式を個別に設定する方法の例です。

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

また、次の例では、すべての filter コマンドを同じレベルに設定する例を示します。

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

**show privilege** コマンドは、形式を分けて表示します。

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

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

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

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

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

## ローカル コマンド特権レベルの表示

次のコマンドを使用すると、コマンドの特権レベルを表示できます。

| コマンド | 目的 |
|---|---|
| **show running-config all privilege all** | すべてのコマンドを表示します。 |
| **show running-config privilege level** *level* | 特定のレベルのコマンドを表示します。*level* は 0 ～ 15 の整数です。 |
| **show running-config privilege command** *command* | 特定のコマンドのレベルを表示します。 |

### 例

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

```
hostname(config)# show running-config all privilege all
privilege show level 15 command aaa
privilege clear level 15 command aaa
privilege configure level 15 command aaa
privilege show level 15 command aaa-server
privilege clear level 15 command aaa-server
privilege configure level 15 command aaa-server
privilege show level 15 command access-group
privilege clear level 15 command access-group
privilege configure level 15 command access-group
privilege show level 15 command access-list
privilege clear level 15 command access-list
privilege configure level 15 command access-list
privilege show level 15 command activation-key
privilege configure level 15 command activation-key
....
```

次の例は、特権レベル 10 に対するコマンド割り当てを示しています。

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

次の例は、**access-list** コマンドに対するコマンド割り当てを示しています。

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

## TACACS+ 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推奨します。

- **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*。

- 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オンにしてください。

- 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。

- 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.40-33）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.40-26）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、次のコマンドを入力します。

### 手順の詳細

| コマンド | 目的 |
|---|---|
| **aaa authorization command** *tacacs+_server_group* [**LOCAL**]<br><br>**例：**<br>`hostname(config)# aaa authorization command group_1 LOCAL` | TACACS+ サーバを使用してコマンド許可を実行します。<br><br>TACACS+ サーバを使用できない場合は、ローカル データベースをフォールバック方式として使用するように ASA を設定できます。フォールバックをイネーブルにするには、サーバ グループ名の後ろに **LOCAL** を指定します（**LOCAL** は大文字と小文字を区別します）。ASA は、どちらの方式を使用しているかを示すプロンプトを表示しないため、ローカル データベースと TACACS+ サーバで同じユーザ名とパスワードを使用することをお勧めします。必ずローカル データベースのユーザ（“Adding a User Account to the Local Database” section on page 32-4 を参照）とコマンド特権レベル（「ローカル コマンド許可の設定」（P.40-26）を参照）を設定してください。 |

# 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

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **aaa accounting** {**serial** \| **telnet** \| **ssh** \| **enable**} **console** *server-tag*<br><br>**例：**<br>`hostname(config)# aaa accounting telnet console group_1` | 管理アクセスに対する AAA アカウンティングのサポートをイネーブルにします。<br><br>有効なサーバ グループ プロトコルは RADIUS と TACACS+ です。 |
| ステップ 2 | **aaa accounting command** [**privilege** *level*] *server-tag*<br><br>**例：**<br>`hostname(config)# aaa accounting command privilege 15 group_1` | コマンド アカウンティングをイネーブルにします。TACACS+ サーバだけがコマンド アカウンティングをサポートします。<br><br>**privilege** *level* は最小特権レベルで、*server-tag* は、ASA がコマンド アカウンティング メッセージを送信する TACACS+ サーバ グループの名前です。 |

# 現在のログイン ユーザの表示

現在のログイン ユーザを表示するには、次のコマンドを入力します。

```
hostname# show curpriv
```

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

**表 40-1　show curpriv 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。 |

表 40-1　show curpriv コマンド出力の説明 （続き）

| フィールド | 説明 |
|---|---|
| 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 Mode/s | 使用可能なアクセス モードは次のとおりです。<br>• P_UNPR：ユーザ EXEC モード（レベル 0 と 1）<br>• P_PRIV：特権 EXEC モード（レベル 2 ～ 15）<br>• P_CONF：コンフィギュレーション モード |

# ロックアウトからの回復

状況によっては、コマンド許可や CLI 認証をオンにすると、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 40-2 に、一般的なロックアウト条件と回復方法を示します。

表 40-2　CLI 認証およびコマンド許可のロックアウト シナリオ

| 機能 | ロックアウト条件 | 説明 | 対応策：シングル モード | 対応策：マルチ モード |
|---|---|---|---|---|
| ローカル CLI 認証 | ローカル データベース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<br>TACACS+ CLI 認証<br>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。<br>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。<br>2. サーバがダウンしたときにロックアウトされないように、ローカル データベースをフォールバック方式として設定します。 |

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

| 機能 | ロックアウト条件 | 説明 | 対応策：シングル モード | 対応策：マルチ モード |
|---|---|---|---|---|
| TACACS+ コマンド許可 | 十分な特権のないユーザまたは存在しないユーザとしてログインした。 | コマンド許可がイネーブルになりますが、ユーザはこれ以上コマンドを入力できなくなります。 | TACACS+ サーバのユーザ アカウントを修正します。<br>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。 |

# 管理アクセスの機能履歴

表 40-3 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。

**表 40-3　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。<br>次のコマンドを導入しました。<br>**show running-config all privilege all、show running-config privilege level、show running-config privilege command、telnet、telnet timeout、ssh、ssh timeout、http、http server enable、asdm image disk、banner、console timeout、icmp、ipv6 icmp、management access、aaa authentication console、aaa authentication enable console、aaa authentication telnet \| ssh console、service-type、login、privilege、aaa authentication exec authentication-server、aaa authentication command LOCAL、aaa accounting serial \| telnet \| ssh \| enable console、show curpriv、aaa accounting command privilege**。 |
| 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。 |
| 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。 |