CHAPTER 33

AAA のローカル データベースの設定

この章では AAA 用のローカル サーバを設定する方法について説明します。次の情報も上方も含みます。

ローカル データベースに関する情報

次の機能にローカル データベースを使用できます：

- ASDM ユーザごとのアクセス
- コンソール認証
- Telnet 認証および SSH 認証
- **enable** コマンド認証

  この設定は、CLI アクセスにだけ使用され、ASDM ログインには影響しません。
- コマンド許可

  ローカル データベースを使用するコマンド許可を有効にすると、ASA では、ユーザ特権レベルを参照して、どのコマンドが使用できるかが特定されます。コマンド許可がディセーブルの場合は通常、特権レベルは参照されません。デフォルトでは、コマンドの特権レベルはすべて、0 または 15 のどちらかです。ASDM には、コマンドへの割り当てをイネーブルにできる特権レベルが事前に定義されています。割り当てることができるレベルは、15（管理）、5（読み取り専用）、3（監視専用）の 3 種類です。事前定義済みのレベルを使用する場合は、ユーザを 3 種類の特権レベルのいずれかに割り当てます。
- ネットワーク アクセス認証
- VPN クライアント認証

マルチ コンテキスト モードの場合、システム実行スペースでユーザ名を設定し、**login** コマンドを使用して CLI で個々にログインできます。ただし、システム実行スペースではローカル データベースを参照する AAA ルールは設定できません。

（注）　ローカル データベースはネットワーク アクセス許可には使用できません。

フォールバック サポート

ローカル データベースは、複数の機能のフォールバック方式として動作できます。この動作は、ASA から誤ってロックアウトされないようにすることを意図しています。

ログインすると、コンフィギュレーション内で指定されている最初のサーバから、応答があるまでグループ内のサーバが順に 1 つずつアクセスされます。グループ内のすべてのサーバが使用できない場合、ローカル データベースがフォールバック方式（管理認証および許可限定）として設定されていると、ASA はローカル データベースに接続しようとします。フォールバック方式として設定されていない場合、ASA は引き続き AAA サーバにアクセスしようとします。

フォールバック サポートを必要とするユーザについては、ローカル データベース内のユーザ名およびパスワードと、AAA サーバ上のユーザ名およびパスワードとを一致させることを推奨します。これにより、透過フォールバックがサポートされます。ユーザは、AAA サーバとローカル データベースのどちらがサービスを提供しているかが判別できないので、ローカル データベースのユーザ名およびパスワードとは異なるユーザ名およびパスワードを AAA サーバで使用することは、指定するべきユーザ名とパスワードをユーザが確信できないことを意味します。

ローカル データベースでサポートされているフォールバック機能は次のとおりです。

- コンソールおよびイネーブル パスワード認証：グループ内のサーバがすべて使用できない場合、ASA ではローカル データベースを使用して管理アクセスを認証します。これには、イネーブル パスワード認証が含まれる場合があります。
- コマンド許可：グループ内の TACACS+ サーバがすべて使用できない場合、特権レベルに基づいてコマンドを許可するためにローカル データベースが使用されます。
- VPN 認証および許可 : VPN 認証および許可は、通常この VPN サービスをサポートしている AAA サーバが使用できない場合、ASA へのリモート アクセスをイネーブルにするためにサポートされます。管理者である VPN クライアントが、ローカル データベースへのフォールバックを設定されたトンネル グループを指定する場合、AAA サーバ グループが使用できない場合でも、ローカル データベースが必要な属性で設定されていれば、VPN トンネルが確立できます。

グループ内の複数のサーバを使用したフォールバックの仕組み

サーバ グループ内に複数のサーバを設定し、サーバ グループのローカル データベースへのフォールバックをイネーブルにしている場合、ASA からの認証要求に対してグループ内のどのサーバからも応答がないと、フォールバックが発生します。次のシナリオで例証します。

サーバ 1、サーバ 2 の順で、LDAP サーバ グループに 2 台の Active Directory サーバを設定します。リモート ユーザがログインすると、ASA によってサーバ 1 に対する認証が試みられます。

サーバ 1 から認証エラー（「*user not found*」など）が返されると、ASA によるサーバ 2 に対する認証は試みられません。

タイムアウト期間内にサーバ 1 から応答がないと（または認証回数が、設定されている最大数を超えている場合）、ASA によってサーバ 2 に対する認証が試みられます。

グループ内のどちらのサーバからも応答がなく、ASA にローカル データベースへのフォールバックが設定されている場合、ASA によってローカル データベースに対する認証が試みられます。

ローカル データベースのライセンス要件

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。

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

ローカル データベースを認証または許可に使用する場合、ASA からのロック アウトを防止するには、「ロックアウトからの回復」（P.45-35）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

ユーザをローカル データベースに追加するには、次の手順を実行します。

手順の詳細

ステップ 1　[Configuration] > [Device Management] > [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。

ステップ 2　[Username] フィールドに、4 ～ 64 文字のユーザ名を入力します。

ステップ 3　[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。フィールドには、アスタリスクだけが表示されます。セキュリティを確保するために、パスワードの長さは 8 文字以上にすることを推奨します。

（注）　[User Accounts] ペインでイネーブル パスワードを設定する場合は（「ホスト名、ドメイン名、およびパスワードの設定」（P.16-1）を参照）、ユーザ名 enable_15 に対するパスワードを変更します。ユーザ名 enable_15 は常に [User Accounts] ペインに表示され、デフォルト ユーザ名を表します。この方法は、ASDM のシステム コンフィギュレーションでイネーブル パスワードを設定する唯一の方法です。CLI で他のイネーブル レベル パスワード（enable password 10 など）を設定すると、そのユーザ名は enable_10 という形式で表示されます。

ステップ 4　[Confirm Password] フィールドにパスワードを再入力します。

セキュリティ上の理由から、パスワードを入力するこの 2 つのフィールドには、アスタリスクだけが表示されます。

ステップ 5　ユーザが属する VPN グループを指定する場合は、[Member of] フィールドにグループ名を入力し、[Add] をクリックします。

VPN グループを削除する場合は、ウィンドウ内からグループを選択し、[Delete] をクリックします。

ステップ 6　[Access Restriction] 領域で、ユーザの管理アクセス レベルを設定します。まず、[Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authorization] タブの [Perform authorization for exec shell access] オプションをクリックして、管理許可をイネーブルにする必要があります。

次のいずれかのオプションを選択します。

- [Full Access (ASDM, Telnet, SSH and console)] : ローカル データベースを使用した管理アクセスの認証を設定する場合（「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）、このオプションを指定するとユーザは ASDM、SSH、Telnet、およびコンソール ポートを使用できます。さらに認証もイネーブルにすると、ユーザはグローバル コンフィギュレーション モードにアクセスできます。
  - [Privilege Level] : ローカル コマンド許可でユーザに適用する特権レベルを選択します。範囲は、0（最低）～ 15（最高）です。詳細については、「コマンド許可の設定」（P.45-27）を参照してください。
- [CLI login prompt for SSH, Telnet and console (no ASDM access)] : ローカル データベースを使用した管理アクセスの認証を設定する場合（「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）、このオプションを指定するとユーザは SSH、Telnet、およびコンソール ポートを使用できます。ユーザは設定に ASDM を使用できません（HTTP 認証を設定している場合）。ASDM 監視は可能です。さらにイネーブル認証も設定すると、ユーザはグローバル コンフィギュレーション モードにアクセスできません。
- [No ASDM, SSH, Telnet, or console access] : ローカル データベースを使用した管理アクセスの認証を設定する場合（「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）、このオプションを指定すると、ユーザは認証用に設定した管理アクセス方式を利用できなくなります（ただし、[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）。

ステップ 7　（任意）ASA への SSH 接続の公開キー認証をユーザ単位でイネーブルにするには、ナビゲーション ペインで次のオプションの 1 をクリックしてください。

- [Public Key Authentication] : Base64 でエンコードされた公開キーに貼り付けます。SSH-RSA raw キーを生成（認証なし）する任意の SSH キー生成ソフトウェア（ssh keygen など）を使用して、キーを生成できます。既存のキーを表示する場合は、キーは SHA-256 ハッシュを使用して暗号化されます。ハッシュ キーをコピーして貼りつける場合は、[Key is hashed] チェックボックスをオンにします。

  認証キーを削除するには、[Delete Key] をクリックして、確認ダイアログボックスを表示します。[Yes] をクリックして認証キーを削除し、[No] をクリックしてそれを保持します。

- [Public Key Using PKF] : [Specify a new PKF key] チェックボックスをクリックして、公開キー ファイル（PKF）でフォーマットされたキー（4096 ビットまで）を貼りつけるかインポートします。Base64 形式でインポートするには大きすぎるキーにはこのフォーマットを使用します。たとえば、ssh の keygen を使用して 4096 ビット キーを生成し、PKF に変換して、このペインでインポートします。既存のキーを表示する場合は、SHA-256 ハッシュを使用して暗号化されます。ハッシュ キーをコピーして貼り付ける必要がある場合は、[Public Key Athentication] ペインからコピーし、[Key is hashed] チェックボックスをオンにした新しい ASA のペインに貼り付けます。

  認証キーを削除するには、[Delete Key] をクリックして、確認ダイアログボックスを表示します。[Yes] をクリックして認証キーを削除し、[No] をクリックしてそれを保持します。

ステップ 8　[VPN Policy] をクリックして、このユーザの VPN ポリシー属性を設定します。VPN コンフィギュレーション ガイドの “Configuring VPN Policy Attributes for a User” section on page 74-13 を参照してください。

ステップ 9　[Apply] をクリックします。

ユーザがローカル データベースに追加され、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。

ヒント　[Configuration] > [Device Management] > [Users/AAA] > [User Accounts] ペインの各カラムで特定のテキストを検索できます。[Find] ボックスに検索する特定のテキストを入力し、[Up] または [Down] 矢印をクリックします。また、アスタリスク（*）および疑問符（?）をテキスト検索でワイルドカード文字として使用できます。

次の例では、Linux または Macintosh システムの SSH の共有キーを生成して、ASA にインポートします。

ステップ 1　コンピュータで 4096 ビットの ssh rsa 公開キーおよび秘密キーを生成します。

```
jcrichton-mac:~ john$ ssh-keygen -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/john/.ssh/id_rsa):
/Users/john/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase): pa$$phrase
Enter same passphrase again: pa$$phrase
Your identification has been saved in /Users/john/.ssh/id_rsa.
Your public key has been saved in /Users/john/.ssh/id_rsa.pub.
The key fingerprint is:
c0:0a:a2:3c:99:fc:00:62:f1:ee:fa:f8:ef:70:c1:f9 john@jcrichton-mac
The key's randomart image is:
+--[ RSA 4096]----+
| .               |
|  o  .           |
|+...  o          |
|B.+.....         |
|.B ..+  S        |
|  =   o          |
|   + . E         |
|  o o            |
| ooooo           |
+-----------------+
```

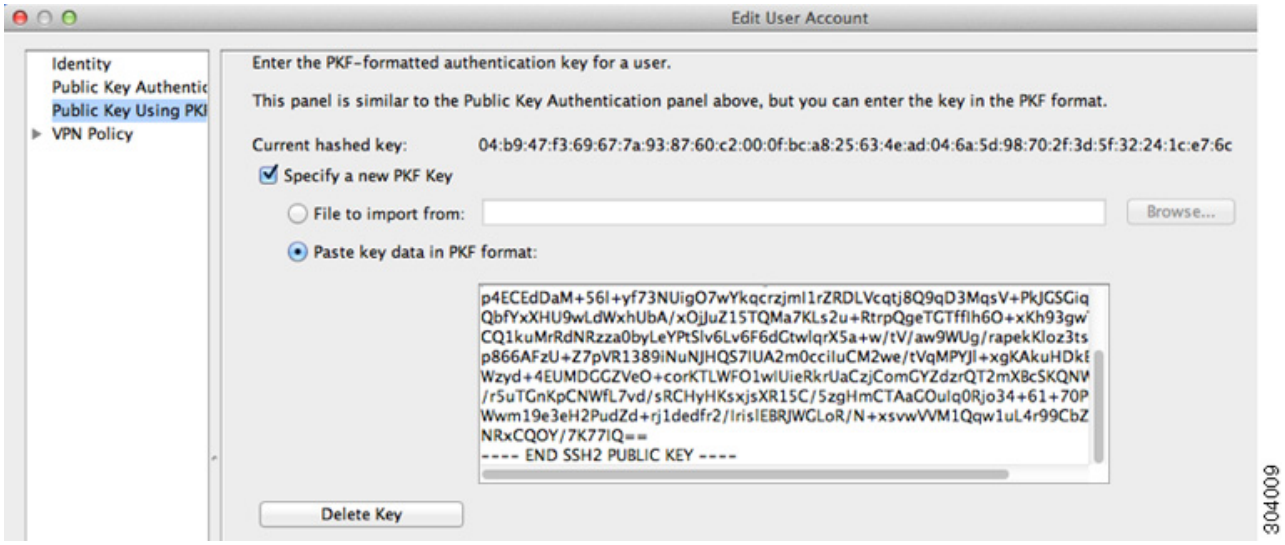
ステップ 2　PKF 形式にキーを変換します。

```
jcrichton-mac:~ john$ cd .ssh
jcrichton-mac:.ssh john$ ssh-keygen -e -f id_rsa.pub
---- BEGIN SSH2 PUBLIC KEY ----
```

```
Comment: "4096-bit RSA, converted by ramona@rboersma-mac from OpenSSH"
AAAAB3NzaC1yc2EAAAADAQABAAACAQDNUvkgza37lB/Q/fljpLAv1BbyAd5PJCJXh/U4LO
hleR/qgIROjpnDaS7Az8/+sjHmq0qXC5TXkzWihvRZbhefyPhPHCi0hIt4oUF2ZbXESA/8
jUT4ehXIUE7FrChffBBtbD4d9FkV8A2gwZCDJBxEM26ocbZCSTx9QC//wt6E/zRcdoqiJG
p4ECEdDaM+56l+yf73NUigO7wYkqcrzjmI1rZRDLVcqtj8Q9qD3MqsV+PkJGSGiqZwnyIl
QbfYxXHU9wLdWxhUbA/xOjJuZ15TQMa7KLs2u+RtrpQgeTGTffIh6O+xKh93gwTgzaZTK4
CQ1kuMrRdNRzza0byLeYPtSlv6Lv6F6dGtwlqrX5a+w/tV/aw9WUg/rapekKloz3tsPTDe
p866AFzU+Z7pVR1389iNuNJHQS7IUA2m0cciIuCM2we/tVqMPYJl+xgKAkuHDkBlMS4i8b
Wzyd+4EUMDGGZVeO+corKTLWFO1wIUieRkrUaCzjComGYZdzrQT2mXBcSKQNWlSCBpCHsk
/r5uTGnKpCNWfL7vd/sRCHyHKsxjsXR15C/5zgHmCTAaGOuIq0Rjo34+61+70PCtYXebxM
Wwm19e3eH2PudZd+rj1dedfr2/IrislEBRJWGLoR/N+xsvwVVM1Qqw1uL4r99CbZF9NghY
NRxCQOY/7K77IQ==
---- END SSH2 PUBLIC KEY ----
jcrichton-mac:.ssh john$
```

ステップ 3　キーをクリップボードにコピーします。

ステップ 4　ASDM で、[Configuration] > [Device Management] > [Users/AAA] > [User Accounts] を選択し、ユーザ名を選択して [Edit] をクリックします。[Public Key Using PKF] をクリックして、ウィンドウにキーを貼り付けます。



ステップ 5　ユーザが ASA に SSH できることを確認（テスト）します。

```
jcrichton-mac:.ssh john$ ssh test@10.86.118.5
The authenticity of host '10.86.118.5 (10.86.118.5)' can't be established.
RSA key fingerprint is 39:ca:ed:a8:75:5b:cc:8e:e2:1d:96:2b:93:b5:69:94.
Are you sure you want to continue connecting (yes/no)? yes
```

次のダイアログボックスが、パスフレーズを入力するために表示されます。

一方、端末セッションでは、以下が表示されます。

```
Warning: Permanently added '10.86.118.5' (RSA) to the list of known hosts.
Identity added: /Users/john/.ssh/id_rsa (/Users/john/.ssh/id_rsa)
Type help or '?' for a list of available commands.
asa>
```

ローカル データベースの認証および許可のテスト

ASA がローカル データベースに接続して、ユーザを認証または許可できることを確認するには、次の手順を実行します。

ステップ 1　[Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] > [AAA Server Groups] テーブルで、サーバが含まれるサーバ グループをクリックします。

テーブル内の該当する行が選択されます。

ステップ 2　[Selected Group] テーブルの [Servers] から、テストするサーバをクリックします。

テーブル内の該当する行が選択されます。

ステップ 3　[Test] をクリックします。

選択したサーバに対応する [Test AAA Server] ダイアログボックスが表示されます。

ステップ 4　実行するテストのタイプ（[Authentication] または [Authorization]）をクリックします。

ステップ 5　[Username] フィールドにユーザ名を入力します。

ステップ 6　認証をテストする場合は、そのユーザ名に対応するパスワードを [Password] フィールドに入力します。

ステップ 7　[OK] をクリックします。

認証または許可のテスト メッセージが ASA からサーバへ送信されます。テストが失敗した場合は、ASDM によりエラー メッセージが表示されます。

ローカル データベースのモニタリング

ローカル データベースをモニタするには、次のペインを確認します：

パス	目的
[Monitoring] > [Properties] > [AAA Servers]	設定済みデータベースの統計情報を表示します。
[Monitoring] > [Properties] > [AAA Servers]	AAA サーバ実行コンフィギュレーションを表示します。

ローカル データベースの機能履歴

表 33-1 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 33-1　ローカル データベースの機能履歴

機能名	プラットフォーム リリース	機能情報
AAA のローカル データベース設定	7.0(1)	AAA 用にローカル データベースを設定する方法について説明します。 次の画面が導入されました。 [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] [Configuration] > [Device Management] > [Users/AAA] > [User Accounts]
SSH 公開キー認証のサポート	9.1(2)	ASA への SSH 接続の公開キー認証がユーザ単位でイネーブルにできるようになりました。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] *8.4(4.1) でも使用可能。PKF キー形式は 9.1(2) でのみサポートされます。*