AAA サーバとローカル データベース

この章では、認証、認可、アカウンティング（AAA は「トリプル A」と読む）について説明します。AAA は、コンピュータ リソースへのアクセスを制御するための一連のサービスで、サービスの課金に必要な情報を提供します。これらの処理は、効果的なネットワーク管理およびセキュリティにとって重要です。

この章では、AAA 機能用にローカル データベースを設定する方法について説明します。外部 AAA サーバについては、ご使用のサーバ タイプに関する章を参照してください。

- AAA とローカル データベースについて （1 ページ）
- ローカル データベースのガイドライン （5 ページ）
- ローカル データベースへのユーザ アカウントの追加 （5 ページ）
- ローカル データベースのモニタリング （7 ページ）
- ローカル データベースの履歴 （8 ページ）

AAA とローカル データベースについて

ここでは、AAA とローカル データベースについて説明します。

認証

認証はユーザを特定する方法です。アクセスが許可されるには、ユーザは通常、有効なユーザ名と有効なパスワードが必要です。AAA サーバは、データベースに保存されている他のユーザ クレデンシャルとユーザの認証資格情報を比較します。クレデンシャルが一致する場合、ユーザはネットワークへのアクセスが許可されます。クレデンシャルが一致しない場合、認証は失敗し、ネットワーク アクセスは拒否されます。

次の項目を認証するように、Cisco ASA を設定できます。

- ASA へのすべての管理接続（この接続には、次のセッションが含まれます）
  - Telnet
  - SSH
  - シリアル コンソール

- ASDM（HTTPS を使用）
- VPN 管理アクセス

- **enable** コマンド
- ネットワーク アクセス層
- VPN アクセス

認証

認可はポリシーを使用するプロセスです。どのようなアクティビティ、リソース、サービスに対するアクセス許可をユーザが持っているのかを判断します。ユーザが認証されると、そのユーザはさまざまなタイプのアクセスやアクティビティを認可される可能性があります。

次の項目を認可するように、ASA を設定できます。

- 管理コマンド
- ネットワーク アクセス層
- VPN アクセス

Accounting

アカウンティングは、アクセス時にユーザが消費したリソースを測定します。そこには、システム時間またはセッション中にユーザが送受信したデータ量などが含まれます。アカウンティングは、許可制御、課金、トレンド分析、リソース使用率、キャパシティプランニングのアクティビティに使用されるセッションの統計情報と使用状況情報のログを通じて行われます。

認証、認可、アカウンティング間の相互作用

認証だけで使用することも、認可およびアカウンティングとともに使用することもできます。認可では必ず、ユーザの認証が最初に済んでいる必要があります。アカウンティングだけで使用することも、認証および認可とともに使用することもできます。

AAA Servers

AAA サーバは、アクセス コントロールに使用されるネットワーク サーバです。認証は、ユーザを識別します。認可は、認証されたユーザがアクセスする可能性があるリソースとサービスを決定するポリシーを実行します。アカウンティングは、課金と分析に使用される時間とデータのリソースを追跡します。

AAA Server Groups

認証、許可、またはアカウンティングに外部 AAA サーバを使用する場合は、まず AAA プロトコルあたり少なくとも 1 つの AAA サーバ グループを作成して、各グループに 1 つ以上のサーバを追加する必要があります。AAA サーバ グループは名前で識別されます。各サーバ グループは、あるサーバまたはサービスに固有です。

次の項を参照してください。

- RADIUS サーバ グループの設定
- TACACS+ サーバ グループの設定
- LDAP サーバ グループの設定

Kerberos、SDI および HTTP フォーム用のサーバ グループも設定できます。これらのグループは VPN 設定で使用されます。これらのグループのタイプについては、『VPN 構成ガイド』を参照してください。

ローカル データベースについて

ASA は、ユーザ プロファイルを取り込むことができるローカル データベースを管理します。AAA サーバの代わりにローカル データベースを使用して、ユーザ認証、認可、アカウンティングを提供することもできます。

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、Cisco 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、Cisco 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。
- 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 アクセス認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設計されています。

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認可するためにローカル データベースが使用されます。
- VPN 認証および認可：VPN 認証および認可は、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 データベースのガイドライン

ローカル データベースを認証または認可に使用する場合、ASA からのロックアウトを必ず防止してください。

ローカル データベースへのユーザ アカウントの追加

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

ステップ 1 ユーザ アカウントを作成します。

username *username* [**password** *password*] [**privilege** *priv_level*]

例：

```
ciscoasa(config)# username exampleuser1 password madmaxfuryroadrules privilege 1
```

username *username* キーワードは、3 ～ 64 文字のスペースと疑問符を除く任意の ASCII 印刷可能文字（文字コード 32 ～ 126）で構成されます。**password** *password* キーワードは、3 ～ 127 文字のスペースと疑問符を除く任意の ASCII 印刷可能文字（文字コード 32 ～ 126）で構成できます。SSH 公開キー認証を使用している場合など、パスワードを指定せずにユーザ名を作成することもできます。**privilege** *priv_level* キーワードでは、0 ～ 15 の範囲で特権レベルを設定します。デフォルトは 2 です。この特権レベルは、コマンド認可で使用されます。

注意 コマンド認可（**aaa authorization console LOCAL** コマンド）を使用していない場合、デフォルトのレベル 2 を使用して特権 EXEC モードにアクセスできます。特権 EXEC モードへのアクセスを制限する場合、特権レベルを 0 または 1 に設定するか、**service-type** コマンドを使用します。

使用頻度の低いこれらのオプションは上記の構文には示されていません。**nopassword** キーワードを使用すると、任意のパスワードを受け入れるユーザアカウントが作成されます。このオプションはセキュアではないため推奨されません。

encrypted キーワード（9.6 以前の場合は 32 文字以内のパスワード用）または **pbkdf2** キーワード（9.6 以降では 32 文字を超えるパスワード用、9.7 以降では長さを問わずすべてのパスワード用）は、パスワードが暗号化されている（MD5 ベースのハッシュまたは PBKDF2（Password-Based Key Derivation Function 2）ハッシュ）ことを示します。既存のパスワードでは、ユーザが新しいパスワードを入力しない限り、MD5 ベースのハッシュが引き続き使用されことに注意してください。**username** コマンド内のパスワードを定義すると、ASA はセキュリティを維持するため、そのパスワードをコンフィギュレーションに保存するときに暗号化します。**show running-config** コマンドを入力すると、**username** コマンドでは実際のパスワードが表示されず、暗号化されたパスワードとその後に **encrypted** または **pbkdf2** キーワードが表示されます。たとえば、パスワードに「test」と入力すると、**show running-config** コマンドの出力には次のように表示されます。

```
username user1 password DLaUiAX3l78qgoB5c7iVNw== encrypted
```

実際に CLI で **encrypted**か **pbkdf2**を入力するのは、同じパスワードを使用していて、あるコンフィギュレーション ファイルを他の ASA にカット アンド ペーストする場合だけです。

ステップ 2 （オプション）ユーザ名属性を設定します。

username *username***attributes**

例：

```
ciscoasa(config)# username exampleuser1 attributes
```

username 引数は、最初の手順で作成したユーザ名です。

デフォルトでは、このコマンドで追加した VPN ユーザには属性またはグループ ポリシーが関連付けられません。**username attributes** コマンドを使用して、明示的にすべての値を設定する必要があります。詳細については、VPN 構成ガイドを参照してください。

ステップ 3 （オプション）管理認可を設定している場合は、**aaa authorization exec** コマンドを使用して、ユーザ レベルを設定します。

service-type {**admin** | **nas-prompt** | **remote-access**}

例：

```
ciscoasa(config-username)# service-type admin
```

admin キーワードは、**aaa authentication console LOCAL** コマンドによって指定されたサービスへのフル アクセスを許可します。デフォルトは **admin** キーワードです。

nas-prompt キーワードは、**aaa authentication** {**telnet** | **ssh** | **serial**} **console** コマンドを設定しているときに CLI へのアクセスを許可しますが、**aaa authentication http console** コマンドを設定しているときは ASDM への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認証をイネーブルにしている場合、ユーザは、**enable** コマンド（または **login** コマンド）を使用して特権 EXEC モードにアクセスできません。

remote-access キーワードは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）。

ステップ 4 （任意） ユーザ単位の ASA への SSH 接続の公開キー認証については、SSH アクセスの設定を参照してください。

ステップ 5 （任意） VPN 認証にこのユーザ名を使用している場合、そのユーザに多くの VPN 属性を設定できます。詳細については、VPN 構成ガイドを参照してください。

例

次の例では、admin ユーザ アカウントに対して特権レベル 15 を割り当てます。

```
ciscoasa(config)# username admin password farscape1 privilege 15
```

次の例では、管理認可をイネーブルにし、パスワードを指定するユーザ アカウントを作成し、ユーザ名コンフィギュレーション モードを開始して、**nas-prompt** の **service-type** を指定します。

```
ciscoasa(config)# aaa authorization exec authentication-server
ciscoasa(config)# username user1 password gOrgeOus
ciscoasa(config)# username user1 attributes
ciscoasa(config-username)# service-type nas-prompt
```

ローカル データベースのモニタリング

ローカル データベースのモニタリングについては、次のコマンドを参照してください。

- **show aaa-server**

  このコマンドは、設定されたデータベースの統計情報を表示します。AAA サーバ コンフィギュレーションをクリアするには、**clear aaa-server statistics** コマンドを入力します。

- **show running-config aaa-server**

  このコマンドは、AAA サーバの実行コンフィギュレーションを表示します。AAA サーバの統計情報をクリアするには、**clear configure aaa-server** コマンドを入力します。

ローカル データベースの履歴

表 *1:* ローカル データベースの履歴

機能名	プラットフォーム リリース	説明
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。 次のコマンドを導入しました。 **username**、**aaa authorization exec authentication-server**、**aaa authentication console LOCAL**、**aaa authorization exec LOCAL**、**service-type**、**aaa authentication** {**telnet** | **ssh** | **serial**} **console LOCAL**、**aaa authentication http console LOCAL**、**aaa authentication enable console LOCAL**、**show running-config aaa-server**、**show aaa-server**、**clear configure aaa-server**、**clear aaa-server statistics**。
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は、ユーザ単位で有効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。ASA がサポートする Base64 形式（最大 2048 ビット）では大きすぎるキーについては、PKF 形式を使用します。 次のコマンドが導入されました。**ssh authenticaion**。 *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。

機能名	プラットフォーム リリース	説明
ローカルの**username**および**enable** パスワードでより長いパスワード（127文字まで）がサポートされます。	9.6(1)	127 文字までのローカル **username**と**enable**パスワードを作成できます（以前の制限は 32 文字でした）。32 文字以上のパスワードを作成すると、PBKDF2（パスワードベース キー派生関数 2）のハッシュを使用して設定に保存されます。これよりも短いパスワードは引き続き MD5 ベースのハッシュを使用します。 次のコマンドを変更しました。**enable**、**username**
SSH 公開キー認証の改善	9.6(2)	以前のリリースでは、ローカルユーザ データベース（**aaa authentication ssh console LOCAL**）を使用して AAA SSH 認証を同時に有効にすることなく、SSH 公開キー認証を有効にできました（**ssh authentication**）。この設定は修正されたため、AAA SSH 認証を明示的に有効にする必要があります。ユーザが秘密キーの代わりにパスワードを使用できないよう、パスワード未定義のユーザ名を作成できるようになりました。 次のコマンドが変更されました。**ssh authentication**、**username**

機能名	プラットフォーム リリース	説明
すべてのローカル **username**と**enable** パスワードにPBKDF2ハッシュが使用されます。	9.7(1)	長さ制限内のすべてのローカル **username**および**enable** パスワードは、PBKDF2（パスワード ベース キー派生関数 2）のハッシュを使用して設定に保存されます。以前は、32 文字以下のパスワードが MD5 ベースのハッシュ メソッドを使用していました。既存のパスワードでは、ユーザが新しいパスワードを入力しない限り、MD5 ベースのハッシュが引き続き使用されます。ダウングレードのガイドラインについては、『一般操作構成ガイド』の「ソフトウェアおよびコンフィギュレーション」の章を参照してください。 次のコマンドを変更しました。**enable**、**username**
SSH 公開キー認証を使用するユーザの認証とパスワードを使用するユーザの認証を区別します。	9.6(3)/9.8(1)	9.6(2) 以前のリリースでは、SSH 公開キー認証（**ssh authentication**）を有効にして、ローカル ユーザ データベースの AAA SSH 認証（**aaa authentication ssh console LOCAL**）を明示的に有効にしないでおくことができました。9.6(2) では、ASA で AAA SSH 認証を明示的に有効にする必要がありました。このリリースでは、AAA SSH 認証を明示的に有効にする必要はありません。ユーザに対して **ssh authentication** コマンドを設定すると、このタイプの認証を使用するユーザのローカル認証がデフォルトで有効になります。さらに、AAA SSH 認証を明示的に設定すると、パスワードを持つユーザ名のみにこの認証が適用されます。また、AAA サーバ タイプを使用できます（例：**aaa authentication ssh console radius_1**）。たとえば、一部のユーザはローカルデータベースを使用して公開キー認証を使用し、他のユーザは RADIUS でパスワードを使用できます。 変更されたコマンドはありません。