AAA サーバーとローカル 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 サーバーについては、ご使用のサーバー 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

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

認証はユーザーを特定する方法です。アクセスが許可されるには、ユーザーは通常、有効なユーザー名と有効なパスワードが必要です。AAA サーバは、ユーザのクレデンシャルとデータベースに保存されている他のユーザ クレデンシャルとを比較します。クレデンシャルが一致した場合は、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は、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 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

許可はポリシーを適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ーが持っているのかを判断します。ユーザーが認証されると、そのユーザー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

アカウンティング

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。これには、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、許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。許可では必ず、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 サーバーおよびサーバーグループ

AAA サーバーは、アクセス制御に使用されるネットワーク サーバーです。認証は、ユーザーを識別します。認可は、認証されたユーザー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装します。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。

外部 AAA サーバーを使用する場合は、まず外部サーバーで使用するプロトコルに応じた AAA サーバーグループを作成し、そのグループにサーバーを追加する必要があります。プロトコルごとに複数のグループを作成し、使用するすべてのプロトコルについてグループを分けることができます。各サーバー グループは、あるサーバーまたはサービスに固有です。

グループの作成方法の詳細については、次のトピックを参照してください。

- RADIUS サーバ グループの設定
- TACACS+ サーバー グループの設定
- LDAP サーバー グループの設定
- RSA SecurID AAA サーバーグループの設定

HTTP Form の使用の詳細については、 VPN 構成ガイドを参照してください。

（注） ASA 9.22.1 以降、Kerberos プロトコルはサポートされていません。AAA サービスに Kerberos を使用できなくなりました。下の 表 に記載されているその他のサポート対象サーバーを使用することをお勧めします。

次の表に、ローカルデータベースを含むサポートされるサーバーのタイプとその用途の概要を示します。

表 *1 : AAA* サーバーでサポートされるサービス

サーバータイプとサービス	認証	許可	アカウンティング
ローカル データベース			
管理者	はい	はい	非対応
VPN ユーザー	はい	非対応	非対応
ファイアウォールセッション（AAA ルール）	はい	はい	非対応
RADIUS			
管理者	はい	はい	はい
VPN ユーザー	はい	はい	はい
ファイアウォールセッション（AAA ルール）	はい	はい	はい
TACACS+			
管理者	はい	はい	はい

サーバータイプとサービス	認証	許可	アカウンティング
VPN ユーザー	はい	非対応	はい
ファイアウォールセッション（AAA ルール）	はい	はい	はい
LDAP			
管理者	はい	非対応	非対応
VPN ユーザー	はい	はい	非対応
ファイアウォールセッション（AAA ルール）	はい	非対応	非対応
SDI（RSA SecurID）			
管理者	はい	非対応	非対応
VPN ユーザー	はい	非対応	非対応
ファイアウォールセッション（AAA ルール）	はい	非対応	非対応
HTTP Form			
管理者	いいえ	非対応	非対応
VPN ユーザー	はい	非対応	非対応
ファイアウォールセッション（AAA ルール）	いいえ	非対応	非対応

注記

- RADIUS：管理者のアカウンティングには、コマンドアカウンティングは含まれません。
- RADIUS：ファイアウォールセッションの認可は、ユーザー固有のアクセスリストでだけサポートされます。このアクセスリストはRADIUS認証応答で受信または指定されます。
- TACACS+：管理者のアカウンティングには、コマンドアカウンティングが含まれます。
- HTTP Form：クライアントレスSSL VPNユーザーセッションの場合に限り、認証とSSO操作がサポートされます。

ローカル データベースについて

ASAは、ユーザー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 サーバーの代わりにローカル データベースを使用して、ユーザー認証、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 ユーザーごとのアクセス
- 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、ASA では、ユーザー特権レベルを参照して使用可能なコマンドが特定されます。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、ユーザーを 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ー名を設定し、**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ーから、応答があるまでグループ内のサーバーが順に 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ー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 サーバー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ーについては、ローカル データベース内のユーザー名およびパスワードと、AAA サーバー上のユーザー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。ユーザーは、AAA サーバー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ー名およびパスワードとは異なるユーザー名およびパスワードを AAA サーバーで使用することは、指定するべきユーザー名とパスワードをユーザー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ー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+ サーバー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 サーバー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 サーバー 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ーを使用したフォールバックの仕組み

サーバー グループ内に複数のサーバーを設定し、サーバー 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ー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。

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

サーバー 1 から認証エラー（「user not found」など）が返されると、ASA によるサーバー 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ーからも応答がなく、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ー アカウントの追加

ユーザーをローカル 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 **[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[User Accounts]** を選択し、次に [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 4 ～ 64 文字の長さのユーザー名を入力します。

ステップ 3 （オプション）8 ～ 127 文字の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。以下を除く任意の ASCII 印刷可能文字（文字コード 32 ～ 126）を組み合わせることができます。

- スペースは使用できません。
- 疑問符は使用できません。
- 3 文字以上連続した、順番に並んだ ASCII 文字または繰り返される ASCII 文字は使用できません。たとえば、次のパスワードは拒否されます。
  - **abc**user1
  - user**543**
  - user**aaaa**
  - user2**666**

フィールドには、アスタリスクだけが表示されます。 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ー名を作成することもできます。

（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、ユーザー名 enable_15 に対するパスワードを変更します。ユーザー名 enable_15 は常に [User Accounts] ペインに表示され、デフォルト ユーザー名を表します。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、そのユーザー名は enable_10 という形式で表示されます。

ステップ 4 パスワードを再度入力します。

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 MSCHAP を認証に使用している場合は、[User authenticated using MSCHAP] チェックボックスをオンにします。

ステップ 6 [Access Restriction] 領域で、ユーザーの管理アクセス レベルを設定します。まず、**[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[AAA Access]** > **[Authorization]** タブの順に移動し、[Perform authorization for exec shell access] オプションをクリックして、管理認可を有効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、このオプションを指定するとユーザーは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、ユーザーはグローバル 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]：ASDM およびローカル コマンド認可用の特権レベルを設定します。範囲は、0（最低）～ 15（最高）です。無制限の管理者アクセス権を付与するには、15 を指定します。事前定義された ASDM ロールでは、管理者用の 15、読み取り専用の 5、およびモニター専用の 3（ユーザーによる [Home] ペインと [Monitoring] ペインの使用を制限する）が使用されます。
- [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、このオプションを指定するとユーザーは SSH、Telnet、およびコンソール ポートを使用できます。ユーザーは設定に 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、ユーザーはグローバル 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、このオプションを指定すると、ユーザー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 （オプション）ユーザー単位で ASA への SSH 接続の公開キー認証をイネーブルにする方法については、ASDM、その他のクライアントの HTTPS アクセスの設定 を参照してください。

ステップ 8 [VPN Policy] をクリックして、このユーザーの VPN ポリシー属性を設定します。VPN 構成ガイドを参照してください。

ステップ 9 [Apply] をクリックします。

ユーザー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。テキスト検索にアスタリスク（「*」）と疑問符（「?」）をワイルドカードとして使用することもできます。

ローカル データベースの認証および認可のテスト

ASA がローカル データベースに接続してユーザーを認証または許可できるかどうか確認するには、次の手順を実行します。

手順

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

ステップ 2 [Servers in the Selected Group] テーブルでテストするサーバーをクリックします。

ステップ 3 [Test] をクリックします。

選択したサーバーに対応する [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 ユーザー名を入力します。

ステップ 6 認証をテストする場合は、ユーザー名のパスワードを入力します。

ステップ 7 [OK] をクリックします。

認証または認可のテスト メッセージが ASA からサーバーへ送信されます。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。

- **[Monitoring] > [Properties] > [AAA Servers]**

  このペインには、AAA サーバーの統計情報が表示されます。

- **[Tools] > [Command Line Interface]**

  このペインでは、さまざまな非インタラクティブ コマンドを発行し、結果を表示することができます。

ローカル データベースの履歴

表 *2:* 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は、ユーザー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。
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** および **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。 次の画面が変更されました。 **[Configuration]** > **[Device Setup]** > **[Device Name/Password]** > **[Enable Password]** **[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[User Accounts]** > **[Add/Edit User Account]** > **[Identity]**

機能名	プラットフォーム リリース	説明
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 ユーザー データベース（）を使用してAAA SSH認証を有効にしなくても、SSH公開キー認証（）を有効にすることができました。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。ユーザー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ー名を作成できるようになりました。 次の画面が変更されました。 **[Configuration] > [Device Management] > [Management Access] > [ASDM/HTTPS/Telnet/SSH]** **[Configuration] > [Device Management] > [Users/AAA] > [User Accounts] > [Add/Edit User Account]**
すべてのローカル **username** および **enable** パスワードに対する PBKDF2 ハッシュ	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、ユーザー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。 次の画面が変更されました。 **[Configuration] > [Device Setup] > [Device Name/Password] > [Enable Password]** **[Configuration] > [Device Management] > [Users/AAA] > [User Accounts] > [Add/Edit User Account] > [Identity]**

機能名	プラットフォーム リリース	説明
SSH 公開キー認証を使用するユーザーの認証とパスワードを使用するユーザーの認証を区別します。	9.6(3)/9.8(1)	9.6(2) より前のリリースでは、ローカル ユーザー データベース（**ssh authentication**）を使用して AAA SSH 認証を明示的に有効にしなくても、SSH 公開キー認証（**aaa authentication ssh console LOCAL**）を有効にすることができました。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。ユーザーに対して **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ーのローカル認証がデフォルトで有効になります。さらに、明示的に AAA SSH 認証を設定すると、この設定はパスワード付きのユーザー名にのみ適用されます。また、任意の AAA サーバー タイプ（**aaa authentication ssh console radius_1** など）を使用できます。たとえば、一部のユーザーはローカル データベースを使用して公開キー認証を使用し、他のユーザーは RADIUS でパスワードを使用できます。 変更された画面はありません。

より強力なローカルユーザーと有効なパスワード要件	9.17(1)	ローカルユーザーと有効なパスワードについて、次のパスワード要件が追加されました。
		• パスワードの長さ：8 文字以上。以前は、最小値が 3 文字でした。
		• 繰り返し文字と連続文字：3 つ以上の連続した ASCII 文字または繰り返しの ASCII 文字は許可されません。たとえば、次のパスワードは拒否されます。
		  • **abc**user1
		  • user**543**
		  • user**aaaa**
		  • user2**666**
		新規/変更された画面：
		• **[Configuration] > [Device Management] > [Users/AAA] > [User Accounts]**
		• **[Configuration] > [Device Setup] > [Device Name/Password]**

機能名	プラットフォーム リリース	説明
ローカルユーザーのロックアウトの変更	9.17(1)	設定可能な回数のログイン試行に失敗すると、ASA はローカルユーザーをロックアウトする場合があります。この機能は、特権レベル 15 のユーザーには適用されませんでした。また、管理者がアカウントのロックを解除するまで、ユーザーは無期限にロックアウトされます。管理者がその前に **clear aaa local user lockout** コマンドを使用しない限り、ユーザーは 10 分後にロック解除されるようになりました。特権レベル 15 のユーザーも、ロックアウト設定が適用されるようになりました。 新規/変更されたコマンド：**aaa local authentication attempts max-fail** 、**show aaa local user**
SSH および Telnet パスワード変更プロンプト	9.17(1)	ローカルユーザーが SSH または Telnet を使用して ASA に初めてログインすると、パスワードを変更するように求められます。また、管理者がパスワードを変更した後、最初のログインに対してもプロンプトが表示されます。ただし、ASA がリロードすると、最初のログインであっても、ユーザーにプロンプトは表示されません。 新規/変更されたコマンド： **show aaa local user**

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。